

# **Introduction to Cyber Security**

## **(FCS)**



**Uttarakhand Open University, Haldwani- 263139**

Toll Free Number: 18001804025

Email: [info@ouu.ac.in](mailto:info@ouu.ac.in)

<http://ouu.ac.in>

<b>Title</b>	Introduction to Cyber Security
<b>Author</b>	<b>Dr. Jeetendra Pande</b> , Assistant Professor-School of CS & IT, Uttarakhand Open University, Haldwani
<b>ISBN:</b> 978-93-84813-96-3	
 Uttarakhand Open University, 2017	
© Uttarakhand Open University, 2017. This work by Uttarakhand Open University is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License. It is attributed to the sources marked in the References, Article Sources and Contributors section.	
<b>Published By :</b> Excel Paper Converters, Haldwani	<b>Qty : 2834</b>

# Index

<b>1.1 INTRODUCTION .....</b>	<b>8</b>
1.1.1 HISTORY OF INTERNET .....	8
1.1.1.1 <i>Internet Addresses</i> .....	10
1.1.1.2 <i>DNS</i> .....	12
1.1.1.3 <i>Internet Infrastructure</i> .....	13
1.1.1.4 <i>World Wide Web</i> .....	14
<b>1.2 INTRODUCTION TO CYBER CRIME.....</b>	<b>15</b>
1.2.1 CLASSIFICATION OF CYBER CRIMES.....	16
1.2.2 REASONS FOR COMMISSION OF CYBER CRIMES .....	18
<b>1.3 MALWARE AND ITS TYPE .....</b>	<b>19</b>
1.3.1 ADWARE.....	19
1.3.2 SPYWARE .....	19
1.3.3 BROWSER HIJACKING SOFTWARE.....	19
1.3.4 VIRUS.....	19
1.3.5 WORMS .....	20
1.3.6 TROJAN HORSE .....	20
1.3.7 SCAREWARE .....	21
<b>1.4 KINDS OF CYBER CRIME .....</b>	<b>21</b>
1.4.1 CYBER STALKING .....	21
1.4.2 CHILD PORNOGRAPHY .....	22
1.4.3 FORGERY AND COUNTERFEITING.....	22
1.4.4 SOFTWARE PIRACY AND CRIME RELATED TO IPRs .....	22
1.4.5 CYBER TERRORISM .....	22
1.4.6 PHISHING.....	22
1.4.7 COMPUTER VANDALISM .....	22
1.4.8 COMPUTER HACKING .....	22
1.4.9 CREATING AND DISTRIBUTING VIRUSES OVER INTERNET.....	23
1.4.10 SPAMMING .....	23
1.4.11 CROSS SITE SCRIPTING.....	23
1.4.12 ONLINE AUCTION FRAUD .....	24
1.4.13 CYBER SQUATTING.....	24
1.4.14 LOGIC BOMBS.....	24
1.4.15 WEB JACKING .....	24
1.4.16 INTERNET TIME THEFTS .....	24

1.4.17 DENIAL OF SERVICE ATTACK.....	24
1.4.18 SALAMI ATTACK .....	24
1.4.19 DATA DIDDLING .....	25
1.4.20 EMAIL SPOOFING.....	25
<b>2.1 AUTHENTICATION .....</b>	<b>26</b>
<b>2.2 ENCRYPTION.....</b>	<b>27</b>
<b>2.3 DIGITAL SIGNATURES .....</b>	<b>28</b>
<b>2.4 ANTIVIRUS.....</b>	<b>29</b>
<b>2.5 FIREWALL .....</b>	<b>30</b>
<b>2.6 STEGANOGRAPHY .....</b>	<b>31</b>
<b>3.1 COMPUTER FORENSICS .....</b>	<b>33</b>
<b>3.2 WHY SHOULD WE REPORT CYBER CRIME?.....</b>	<b>36</b>
<b>4.1 INTRODUCTION .....</b>	<b>40</b>
<b>4.2 SOME RECENT CYBER CRIME INCIDENTS .....</b>	<b>40</b>
<b>5.1 INTRODUCTION .....</b>	<b>47</b>
<b>5.2 COUNTER CYBER SECURITY INTIATIVES IN INDIA.....</b>	<b>47</b>
<b>6.1 GENERATING SECURE PASSWORD .....</b>	<b>52</b>
6.1.1 GUIDELINE FOR SETTING SECURE PASSWORD.....	52
<b>6.2 USING PASSWORD MANAGER .....</b>	<b>55</b>
6.2.1 WHAT IS A PASSWORD MANAGER? .....	56
6.2.2 WHY YOU SHOULD USE IT? .....	56
6.2.3 HOW DOES IT WORK?.....	56
6.2.4 SOME POPULAR PASSWORD MANAGERS.....	56
<b>6.3 ENABLING TWO-STEP VERIFICATION .....</b>	<b>62</b>
<b>6.4 SECURING COMPUTER USING FREE ANTIVIRUS .....</b>	<b>72</b>
<b>7.1 CONFIGURING FIREWALL ON MAC COMPUTER .....</b>	<b>75</b>
7.1.1 TURNING ON AND CONFIGURING THE MAC OS X FIREWALL.....	75
<b>7.2 WORKING WITH WINDOWS FIREWALL IN WINDOWS .....</b>	<b>78</b>
7.2.1 FIREWALL IN WINDOWS 7 .....	78
7.2.2 CONFIGURING WINDOWS FIREWALL .....	79
7.2.3 HOW TO START & USE THE WINDOWS FIREWALL WITH ADVANCED SECURITY.....	83

7.2.3.1 How to Access the Windows Firewall with Advanced Security .....	83
7.2.3.2 What Are The Inbound & Outbound Rules?.....	84
7.2.3.3 What Are The Connection Security Rules?.....	86
7.2.3.4 What Does the Windows Firewall with Advanced Security Monitor? .....	87
<b>8.1 FINDING THE BEST BROWSER ACCORDING TO THE USERS REQUIREMENT .....</b>	<b>89</b>
<b>9.1 SAFE BROWSING .....</b>	<b>94</b>
9.1.1 HOW DO I KNOW IF A WEBSITE IS SECURE? .....	94
<b>9.2 TIPS FOR BUYING ONLINE.....</b>	<b>95</b>
<b>9.3 CLEARING CACHE FOR BROWSERS .....</b>	<b>96</b>
9.3.1 CLEARING CACHE FOR CHROME BROWSERS ABOVE VERSION 10.....	96
9.3.2 CLEARING CACHE FOR CHROME BROWSERS FROM VERSION 1 TO 9.....	99
9.3.3 CLEARING CACHE FOR SAFARI FOR IOS, IPHONE AND IPAD.....	102
9.3.4 CLEARING CACHE FOR SAFARI FOR MAC OS X.....	103
9.3.5 CLEARING CACHE FOR SAFARI FOR WINDOWS .....	104
9.3.6 CLEARING CACHE FOR INTERNET EXPLORER 9, 10 AND 11 .....	106
9.3.7 CLEARING CACHE FOR INTERNET EXPLORER 8.....	108
9.3.8 CLEARING CACHE FOR FIREFOX .....	111
9.3.9 CLEARING CACHE FOR FIREFOX 33 .....	112
9.3.10 CLEARING CACHE FOR OPERA .....	114
9.3.11 CLEARING CACHE FOR CCLEANER .....	115
<b>10.1 WHAT IS WIRELESS LAN? .....</b>	<b>117</b>
<b>10.2 MAJOR ISSUES WITH WLAN.....</b>	<b>118</b>
10.2.1 SECURE WLAN.....	118
10.2.2 WI-FI AT HOME.....	118
<b>11.1 SAFE BROWSING GUIDELINES FOR SOCIAL NETWORKING SITES .....</b>	<b>123</b>
11.1.1GENERAL TIPS ON USING SOCIAL NETWORKING PLATFORMS SAFELY .....	124
11.1.2 POSTING PERSONAL DETAILS .....	125
11.1.3 FRIENDS, FOLLOWERS AND CONTACTS.....	125
11.1.4 STATUS UPDATES .....	126
11.1.5 SHARING ONLINE CONTENT .....	126
11.1.6 REVEALING YOUR LOCATION .....	126
11.1.7 SHARING VIDEOS AND PHOTOS .....	127
11.1.8 INSTANT CHATS.....	127
11.1.9 JOINING AND CREATING GROUPS, EVENTS AND COMMUNITIES .....	127

<b>11.2 EMAIL SECURITY TIPS .....</b>	<b>128</b>
<b>12.1 INTRODUCTION .....</b>	<b>130</b>
<b>12.2 SMARTPHONE SECURITY GUIDELINES.....</b>	<b>131</b>
12.2.1 PURSES, WALLETS, SMARTPHONES .....	131
12.2.2 PLATFORMS, SETUP AND INSTALLATION .....	132
12.2.2.1 <i>Platforms and Operating Systems</i> .....	132
12.2.2.2 <i>Feature Phones</i> .....	132
12.2.2.3 <i>Branded and locked smartphones</i> .....	133
12.2.2.4 <i>General Setup</i> .....	133
12.2.2.5 <i>Installing and updating applications</i> .....	133
12.2.3 COMMUNICATING SECURELY(THROUGH VOICE AND MESSAGES) WITH A SMARTPHONE .....	134
12.2.3.1 <i>Secure Voice Communication</i> .....	134
12.2.3.2 <i>Sending Messages Securely</i> .....	137
12.2.3.3 <i>Storing Information on your Smartphone</i> .....	138
12.2.3.4 <i>Sending Email from your Smartphone</i> .....	139
12.2.3.5 <i>Capturing Media with your Smartphone</i> .....	139
12.2.3.6 <i>Accessing the Internet Securely from your Smartphone</i> .....	140
12.2.3.7 <i>Advanced Smart Phone Security</i> .....	141
REFERENCES.....	144

# INTRODUCTION TO CYBER SPACE

## 1.1 INTRODUCTION

Internet is among the most important inventions of the 21<sup>st</sup> century which have affected our life. Today internet have crosses every barrier and have changed the way we use to talk, play games, work, shop, make friends, listen music, see movies, order food, pay bill, greet your friend on his birthday/ anniversary, etc. You name it, and we have an app in place for that. It has facilitated our life by making it comfortable. Gone are the days when we have to stand in a long queue for paying our telephone and electricity bills. Now we can pay it at a click of a button from our home or office. The technology have reached to an extent that we don't even require a computer for using internet. Now we have internet enabled smartphone, palmtops, etc. through which we can remain connected to our friends, family and office 24x7. Not only internet has simplified our life but also it has brought many things within the reach of the middle class by making them cost effective. It was not long back, while making an ISD or even a STD call, the eyes were stricken on the pulse meter. The calls were very costly. ISD and STD were used to pass on urgent messages only and the rest of the routine communication was done using letters since it was a relatively very cheap. Now internet have made it possible to not only talk but use video conference using popular applications like skype, gtalk etc. at a very low price to a level where a one hour video chat using internet is cheaper than the cost of sending a one page document from Delhi to Bangalore using speed-post or courier service. Not only this, internet has changed the use of the typical devices that were used by us. Television can be used not only for watching popular tv shows and movies but can be used for calling/ video chatting with friend using internet. Mobile phone is not only used for making a call but viewing a latest movie. We can remain connected to everyone, no matter what our location is. Working parents from office can keep eye on their children at home and help them in their homework. A businessman can keep eye on his staff, office, shop, etc with a click of a button. It has facilitated our life in more than one way. Have you ever wondered from where this internet came? Let us discuss the brief history of internet and learn how this internet was invented and how it evolved to an extent that now we cannot think of our lives without it.

### 1.1.1 History of Internet

I don't know what the cold war between USA and Russia gave to the world, but defiantly the internet is one of those very useful inventions whose foundation was laid during cold war

days. Russia Launched the world's first satellite, SPUTNIK into the space on 4<sup>th</sup> October, 1957. This was clearly the victory of Russia over the cyber space and as a counter step, Advanced Research Projects Agency, the research arm of Department of Defence, United States, declared the launch of ARPANET(Advanced Research Projects Agency NETwork) in early 1960's. This was an experimental network and was designed to keep the computers connected to the this network to communicate with each other even if any of the node, due to the bomb attack, fails to respond. The first message was sent over the ARPANET, a packing switching network, by Leonard Kleinrock's laboratory at University of California, Los Angeles (UCLA). You will be surprised to know that the fist message that was sent over internet was "LO". Actually they intended to send work "LOGIN" and only the first two letters reached its destination at second network node at Stanford Research Institute (SRI) and before the last three letters could reach the destination the network was down due to glitch. Soon the error was fixed and the message was resent and it

The major task that ARPANET have to play is to develop rules for communication i.e. protocols for communicating over ARPANET. The ARPANET in particular led to the development of protocols for internetworking, in which multiple separate networks could be joined into a network of networks. It resulted in the development if TCP/IP protocol suite, which specifies the rules for joining and communicating over APRANET.

Soon after, in 1986 NSF(national Science Foundation) backbone was created to and five US universities' computing centres were connected to form NSFnet. The participating Universities were:

- Princeton University -- John von Neumann National Supercomputer Center, JvNC
- Cornell University -- Cornell Theory Center, CTC
- University of Illinois at Urbana-Champaign -- National Center for Supercomputing Applications, NCSA
- Carnegie Mellon University -- Pittsburgh Supercomputer Center, PSC
- General Atomics -- San Diego Supercomputer Center, SDSC

NFSnet, the successor of ARPAnet, become popular by 1990 and ARPANET was decommissioned. There were many parallel networks developed by other Universities and other countries like United Kingdom. In 1965, National Physical Laboratory(NPL) proposed a packing switching network. Michigan Educational Research Information Triad formed MERIT network in 1966 which was funded and supported by State of Michigan and the

National Science Foundation (NSF). France also developed a packet switching network, known as CYCLADES in 1973.

Now there were many parallel systems working on different protocols and the scientist were looking for some common standard so that the networks could be interconnected. In 1978, TCP/IP protocol suits were ready and by 1983, the TCP/IP protocol were adopted by ARPANET.

In 1981, the integration of two large network took place. NFS developed Computer Science Network(CSNET) and was connected to ARPANET using TCP/IP protocol suite. Now the network was not only popular among the research community but the private played also took interest in the network. Initially NFS supported speed of 56 kbit/s. It was upgraded to 1.5 Mbit/s in 1988 to facilitate the growth of network by involving merit network, IBM, MCA and the state of Michigan.

After the corporates took realized the strength and merit of this network, they participated in the development of the network to ripe its benefits. By late 1980s many Internet Service Providers(ISPs) emerged to provide the backbone for carrying the network traffic. By 1991, NFSNET was expanded and was upgraded to 45Mbit/s. Many commercial ISPs provided backbone service and was popular among the corporate. To facilitate the commercial use of the network, NFSNET was decommissioned in 1995 and now the Internet could carry commercial traffic.

Now more and more Universities and research centres throughout the world connected to it. Now this network was very popular among the research community and in 1991 National Research and Education Network (NREN) was founded and the World Wide Web was released. Initially the role of internet was only limited to file transfer. The credit of internet what we see it today goes to Tim Berners-Lee who introduced www. With the advent of www, there was a transformation on how the network was used. Now this web of information can be used to retrieve any information available over the internet. Software called, browser was developed to browse the internet. It was developed by researchers at University of Illinois in 1992 and named as Mosaic. This browser enables to browse the internet the way we browse it today.

### **1.1.1 Internet Addresses**

With so many devices connected to the internet, we require some mechanism to uniquely identify every device that is connected to the internet. Also we require some centralized

system which takes care of this mechanism so that the signs which are used to identify each device are not duplicate; else the whole purpose is defeated. To take care of this, we have a centralized authority known as Internet Assigned Numbers Authority (IANA), which is responsible for assigning a unique number known as IP(Internet Protocol) address. An IP address is a 32-bit binary number which is divided into four octets and each octet consists of 8 binary digits and these octet are separated by a dot(.). An example of an IP address is

**11110110.01011010.10011100.1111100**

Each 8-bits in an octet can have two binary values i.e. 0 and 1. Therefore, each octet can have minimum value 0. i.e. 00000000 to maximum value 256 i.e. 11111111 and in total have  $2^8 = 256$  different combinations.

Again to remember this 32-bit address in binary is bit difficult, so for the better understanding of the human being, it is expressed in a decimal format. But this decimal format is for human understanding only and the computer understands it in binary format only. In decimal, the above IP address is expressed as 123.45.78.125

These octets are used to create and separate different classes. An IP address consists of two parts viz. **Network** and **Host**. Network part identifies the network different network and the host part identifies a device of a particular network.

This address uniquely identifies a devices connected to the internet similar to the postal system where we identify any house by fist identifying the county, then state, district, post office, cluster/block and finally the house number. These IP addresses are classified into five categories based on the availability of IP range. These categories/classes are:

*Table 1: IP Address Classes*

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.

IANA decentralises that task of assigning the IP addresses by allocating the large chunk of IP addresses to five Regional Internet Registries (RIRs), which are further responsible to

allocate the IP addresses in their zone. These RIRs along with their area of operations are listed below:

- APNIC- This RIR is responsible for serving the Asia Pacific region
- AfriNIC- This RIR is responsible for serving the African region
- ARIN- This RIR is responsible for serving North America and several Caribbean and North Atlantic islands
- LACNIC- This RIR is responsible for serving Latin America and the Caribbean, and
- RIPE NCC- This RIR is responsible for serving Europe, the Middle East, and parts of Central Asia

For liaison and coordinating between these five RIRs, there is an organization called Number Resource Organization(NRO). These organizations are

#### **1.1.1.2 DNS**

Whenever we browse any website in the internet, we type name something like www.uou.ac.in and we rarely deal with IP address like 104.28.2.92 but the fact is even if we type http:\\ 104.28.2.92 in the URL, it will land us to the same webpage. The fact is we are very comfortable using and remembering the names instead of a number. Moreover, these IP address changes over time and some of the sites have multiple IP address. Also, the transfer of the data over internet is only possible using IP addresses because the routing of the packet of data sent over internet is done using IP address. There is a server called Domain Name System(DNS) which takes care of this translation job to simplify and to save us from remembering these changing IP address numbers, the DNS. Whenever you type an address like http:\\www.uou.ac.in, there is a process called DNS name resolution, takes place in the background. The computer keeps the track of recently visited sites and locally maintains a database in DNS cache. In case, the IP address of the site you have requested for is not found in the DNS cache of your local computer, then the next probable place to find it is DNS server of your Internet Service Provider(ISP). These DNS servers of ISP also maintain the cache of the recently visited pages. Just in case, the information is not found here also, the DNS server of the ISP forward the query to the root nameservers. The root name servers publish the root zone file to other DNS servers and clients on the Internet. The root zone file describes where the authoritative servers for the DNS top-level domains (TLD) are located. There are currently 13 rootname servers. They are:

- A - VeriSign Global Registry Services

- B - University of Southern California - Information Sciences Institute
- C - Cogent Communications
- D - University of Maryland
- E - NASA Ames Research Center
- F - Internet Systems Consortium, Inc.
- G - U.S. DOD Network Information Center
- H - U.S. Army Research Lab
- I - Autonomica/NORDUnet
- J - VeriSign Global Registry Services
- K - RIPE NCC
- L - ICANN
- M - WIDE Project

These root nameservers directs the query to the appropriate Top-Level Domain(TLD) nameservers by reading the last part of the URL first. In our example the url was <http://www.uou.ac.in>. The last part is .in. Some of the examples of TLD name servers are .com, .biz, .org, .us, .in, etc. These TLD nameservers acts as a switchboard and direct the query to the appropriate authoritative nameserver maintained by each domain. These authoritative nameserver maintains DNS records along with other useful information. This address record is returned back to the requesting host computer via TLD nameservers, nameservers, ISP's DNS server. These intermediary server keeps the record of this IP address in their DNS cache, so that if the same request is encountered again , they don't have to go through this process again. If the same URL is requested again, the DNS cache of the local host computer will return the IP address of the URL.

### **1.1.1.3 Internet Infrastructure**

Internet, as the name suggests, in a network of network i.e. it is a collection of several small, medium and large networks. This clearly indicates to one fact, nobody is a single owner of the internet and it is one of the proven example of collaborative success. Now you must be surprised how such a large network which is spread across the continents can run without the any problem. Yes it is correct that to monitor such a large network, we require an international body which can frame the rules, regulation and protocols to join and use this network. Therefore, an international organization, known as “The Internet Society” was formed in 1992 to take care of such issues.

Let us now discuss, how this internet works? How the email you sent to your friend is received by your friend's computer located at another country/continent. When you are working in your laptop/desktop in your home without connecting to the internet, your computer is a standalone system. But, whenever you connect to the internet by dialling to your Internet Service Provider(ISP) using your modem, you become the part of the network. The ISP is the link between the internet backbone, through which the entire data route, and the user. The ISP connects to the internet backbone at Network Access Points(NAP). These NAPs are the provided by the large telecommunication companies at various regions. These large telecommunication companies connect the countries and the continents by building and maintaining the large backbone infrastructure to route data from NAP to NAP. ISPs are connected to this backbone at NAP and are responsible build and manage network locally. So when you dial internet through modem, you first become part of the local ISP, which in turn connects to the internet backbone through NAP. The data is routed through this backbone and sent to the destination NAP, where the ISP of your friend's network is located. As soon as your friend dials his modem to connect to the internet, the data is delivered to your friend's computer.

#### **1.1.1.4 World Wide Web**

Sometimes we interchangeably use the term internet and world wide web or simply the web, as it is popularly known as. But web is only one of the several the utilities that internet provides. Some of the popular service that internet provides other then web is e-mail, usenet, messaging service, FTP, etc. The web use HTTP protocol to communicate over internet and to exchange information. The web was developed at CERN (European de Reserches Nucleaires), Switzerland) by a UK scientist Tim Berners-Lee in 1989. It consists of all the public web sites and all the devices that access the web content. WWW is an information sharing model which is developed to exchange information over the internet. There are plenty of public websites, which is a collection of web pages, available over the internet. These web-pages contain plenty of information in a form of text, videos, audio and picture format. These web pages are access using a application software called a web browser. Some of the examples of the popular web browser are: Internet explorer, Chrome, Safari, Firefox, etc.

So this was a little introduction about internet and how it functions. Now let us discuss about cyber crime.

## 1.2 INTRODUCTION TO CYBER CRIME

The internet was born around 1960's where its access was limited to few scientist, researchers and the defence only. Internet user base have evolved exponentially. Initially the computer crime was only confined to making a physical damage to the computer and related infrastructure. Around 1980's the trend changed from causing the physical damaging to computers to making a computer malfunction using a malicious code called virus. Till then the effect was not so widespread because internet was only confined to defence setups, large international companies and research communities. In 1996, when internet was launched for the public, it immediately became popular among the masses and they slowly became dependent on it to an extent that it has changed their lifestyle. The GUIs were written so well that the user doesn't have to bother how the internet was functioning. They have to simply make a few clicks over the hyper links or type the desired information at the desired place without bothering where this data is stored and how it is sent over the internet or whether the data can be accessed by another person who is connected to the internet or whether the data packet sent over the internet can be sniffed and tampered. The focus of the computer crime shifted from merely damaging the computer or destroying or manipulating data for personal benefit to financial crime. These computer attacks are increasing at a rapid pace. Every second around 25 computers become victim to cyber attack and around 800 million individuals are effected by it till 2013. CERT-India have reported around 308371 Indian websites to be hacked between 2011-2013. It is also estimated that around \$160 million are lost per year due to cyber crime. This figure is very conservative as most of the cases are never reported.

According to the 2013-14 report of the standing committee on Information Technology to the 15th Lok Sabha by ministry of communication and information technology, India is a third largest number of Internet users throughout the world with an estimated 100 million internet users as on June, 2011 and the numbers are growing rapidly. There are around 22 million broadband connections in India till date operated by around 134 major Internet Service Providers(ISPs).

Before discussing the matter further, let us know what the cyber crime is?

The term **cyber crime** is used to describe a unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal activity. It is often

committed by the people of destructive and criminal mindset either for revenge, greed or adventure.

### **1.2.1 Classification of Cyber Crimes**

The cyber criminal could be internal or external to the organization facing the cyber attack.

Based on this fact, the cyber crime could be categorized into two types:

- *Insider Attack:* An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The motive of the insider attack could be revenge or greed. It is comparatively easy for an insider to perform a cyber attack as he is well aware of the policies, processes, IT architecture and weakness of the security system. Moreover, the attacker have an access to the network. Therefore it is comparatively easy for a insider attacker to steal sensitive information, crash the network, etc. In most of the cases the reason for insider attack is when a employee is fired or assigned new roles in an organization, and the role is not reflected in the IT policies. This opens a vulnerability window for the attacker. The insider attack could be prevented by planning and installing an Internal intrusion detection systems (IDS) in the organization.
- *External Attack:* When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. The organization which is a victim of cyber attack not only faces financial loss but also the loss of reputation. Since the attacker is external to the organization, so these attackers usually scan and gathering information. An experienced network/security administrator keeps regular eye on the log generated by the firewalls as external attacks can be traced out by carefully analysing these firewall logs. Also, Intrusion Detection Systems are installed to keep an eye on external attacks.

The cyber attacks can also be classified as structured attacks and unstructured attacks based on the level of maturity of the attacker. Some of the authors have classified these attacks as a form of external attacks but there is precedence of the cases when a structured attack was performed by an internal employee. This happens in the case when the competitor company wants the future strategy of an organization on certain points. The attacker may strategically gain access to the company as an employee and access the required information.

- *Unstructured attacks:* These attacks are generally performed by amateurs who don't have any predefined motives to perform the cyber attack. Usually these amateurs try to test a tool readily available over the internet on the network of a random company.
- *Structure Attack:* These types of attacks are performed by highly skilled and experienced people and the motives of these attacks are clear in their mind. They have access to sophisticated tools and technologies to gain access to other networks without being noticed by their Intrusion Detection Systems(IDSs). Moreover, these attacker have the necessary expertise to develop or modify the existing tools to satisfy their purpose. These types of attacks are usually performed by professional criminals, by a country on other rival countries, politicians to damage the image of the rival person or the country, terrorists, rival companies, etc.

Cyber crimes have turned out to be a low-investment, low-risk business with huge returns. Now-a-days these structured crimes are performed are highly organized. There is a perfect hierarchical organizational setup like formal organizations and some of them have reached a level in technical capabilities at par with those of developed nation. They are targeting large financial organizations, defence and nuclear establishments and they are also into online drugs trading.

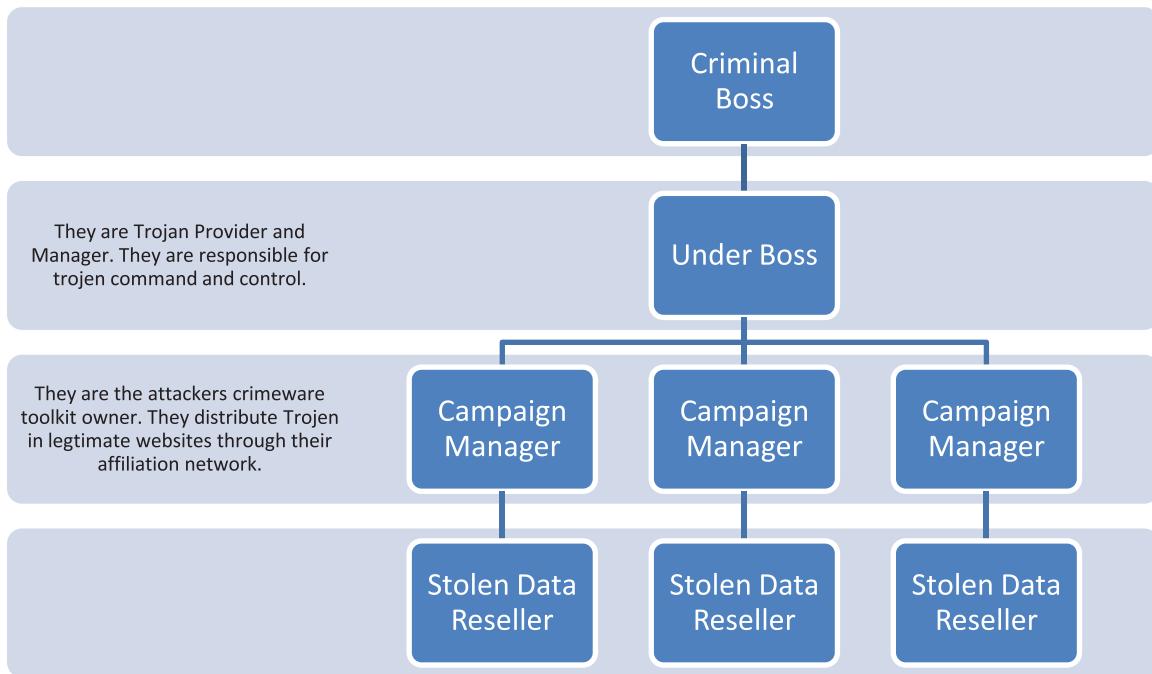


Figure 1 : Hierarchical Organisational Structure

The role of all the people in the hierarchy remain changing and it is based on the opportunity. If a hacker who have hacked sensitive data from an organization may use it for financially exploiting the organisation himself. In case, the hacker himself have the technical expertise for it, he will do it himself, otherwise he may find a buyer who is interested in that data and have the technical expertise.

There are some cyber criminals offers on-demand and service. The person, organization or a country may contact these cyber criminals for hacking an organization to gain access to some sensitive data , or create massive denial-of –service attack on their competitors. Based on the demand of the customer the hackers write malware, virus, etc to suit their requirements. An organization effected by a cyber attack, not only faces financial loss, but its reputation is also adversely affected, and the competitor organization will definitely benefit by it.

### **1.2.2 Reasons for Commission of Cyber Crimes**

There are many reasons which act as a catalyst in the growth of cyber crime. Some of the prominent reasons are:

- a. *Money*: People are motivated towards committing cyber crime to make quick and easy money.
- b. *Revenge*: Some people try to take revenge with other person/organization/society/ caste or religion by defaming its reputation or bringing economical or physical loss. This comes under the category of cyber terrorism.
- c. *Fun*: The amateur do cyber crime for fun. They just want to test the latest tool they have encountered.
- d. *Recognition*: It is considered to be pride if someone hack the highly secured networks like defense sites or networks.
- e. *Anonymity*- Many times the anonymity that a cyber space provides motivates the person to commit cyber crime as it is much easier to commit a cyber crime over the cyber space and remain anonymous as compared to real world.

It is much easier to get away with criminal activity in a cyber world than in the real world. There is a strong sense of anonymity than can draw otherwise respectable citizens to abandon their ethics in pursuit of personal gain.

- f. *Cyber Espionage*: At times the government itself is involved in cyber trespassing to keep eye on other person/network/country. The reason could be politically, economically or socially motivated.

## **1.3 MALWARE AND ITS TYPE**

Malware stands for “*Malicious Software*” and it is designed to gain access or installed into the computer without the consent of the user. They perform unwanted tasks in the host computer for the benefit of a third party. There is a full range of malwares which can seriously degrade the performance of the host machine. There is a full range of malwares which are simply written to distract/annoy the user, to the complex ones which captures the sensitive data from the host machine and send it to remote servers. There are various types of malwares present in the Internet. Some of the popular ones are:

### **1.3.1 Adware**

It is a special type of malware which is used for forced advertising. They either redirect the page to some advertising page or pop-up an additional page which promotes some product or event. These adware are financially supported by the organizations whose products are advertised.

### **1.3.2 Spyware**

It is a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine. Mostly it gathers the browsing habits of the user and the send it to the remote server without the knowledge of the owner of the computer. Most of the time they are downloaded in to the host computer while downloading freeware i.e. free application programmes from the internet. Spywares may be of various types; It can keeps track of the cookies of the host computer, it can act as a keyloggers to sniff the banking passwords and sensitive information, etc.

### **1.3.3 Browser hijacking software**

There is some malicious software which are downloaded along with the free software offered over the internet and installed in the host computer without the knowledge of the user. This software modifies the browsers setting and redirect links to other unintentional sites.

### **1.3.4 Virus**

A virus is a malicious code written to damage/harm the host computer by deleting or appending a file, occupy memory space of the computer by replicating the copy of the code, slow down the performance of the computer, format the host machine, etc. It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc. A virus may be present in a computer but it cannot activate itself without the human intervention.

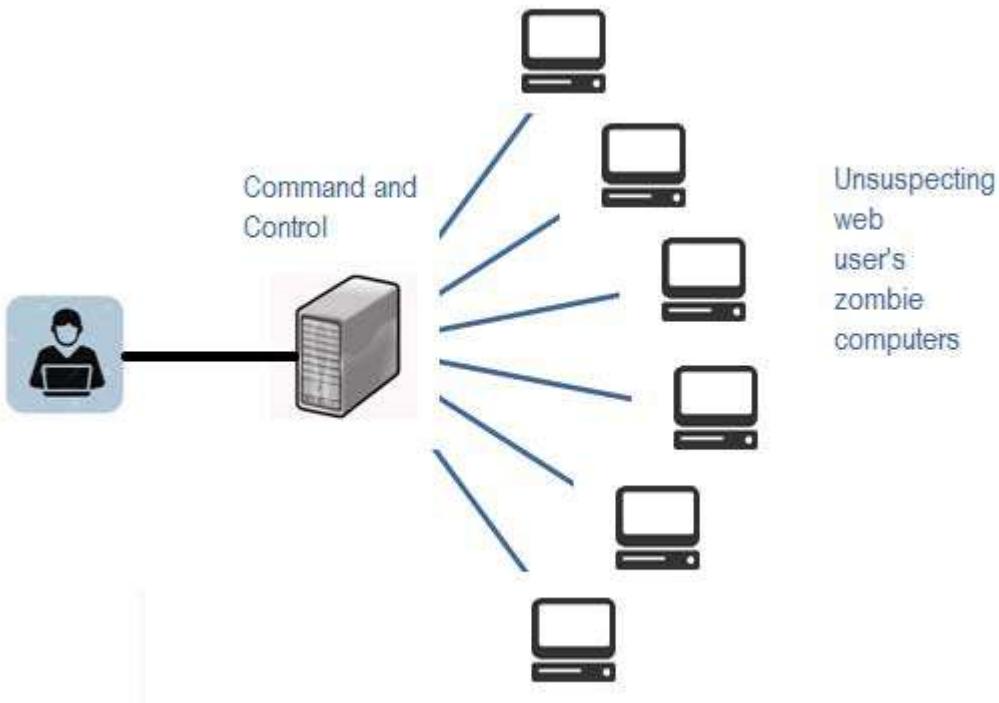
Until and unless the executable file(.exe) is execute, a virus cannot be activated in the host machine.

### 1.3.5 Worms

They are a class of virus which can replicate themselves. They are different from the virus by the fact that they does not require human intervention to travel over the network and spread from the infected machine to the whole network. Worms can spread either through network, using the loopholes of the Operating System or via email. The replication and spreading of the worm over the network consumes the network resources like space and bandwidth and force the network to choke.

### 1.3.6 Trojan Horse

Trojan horse is a malicious code that is installed in the host machine by pretending to be useful software. The user clicks on the link or download the file which pretends to be a useful file or software from legitimate source. It not only damages the host computer by manipulating the data but also it creates a backdoor in the host computer so that it could be controlled by a remote computer. It can become a part of *botnet*(robot-network), a network of computers which are infected by malicious code and controlled by central controller. The computers of this network which are infected by malicious code are known as zombies. Trojans neither infect the other computers in the network nor do they replicate.



*Figure 2: A typical botnet*

### **1.3.7 Scareware**

Internet has changed how we talk, shop, play etc. It has even changed the way how the criminal target the people for ransom. While surfing the Internet, suddenly a pop-up alert appears in the screen which warns the presence of dangerous virus, spywares, etc. in the user's computer. As a remedial measure, the message suggests the user download the full paid version of the software. As the user proceeds to download, a malicious code, known as scareware is downloaded into the host computer. It holds the host computer hostage until the ransom is paid. The malicious code can neither be uninstalled nor can the computer be used till the ransom is paid. A sample message alert of a scareware is shown below in Fig 3<sup>1</sup>



*Figure 3: Sample Warning Message of a Scareware<sup>1</sup>*

## **1.4 KINDS OF CYBER CRIME**

Various types of cyber crimes are:

### **1.4.1 Cyber Stalking**

It is an act of stalking, harassing or threatening someone using Internet/computer as a medium. This is often done to defame a person and use email, social network, instant messenger, web-posting, etc. as a medium as it offers anonymity. The behaviour includes false accusations, threats, sexual exploitation to minors, monitoring, etc.

---

<sup>1</sup> Image courtesy: <https://www.flickr.com/photos/alamagordo/2372928527>

#### **1.4.2 Child Pornography**

It is an act of possessing image or video of a minor (under 18), engaged in sexual conduct.

#### **1.4.3 Forgery and Counterfeiting**

It is a use of computer to forgery and counterfeiting is a document. With the advancement in the hardware and the software, it is possible to produce counterfeit which matches the original document to such an extent that it is not possible to judge the authenticity of the document without expert judgement.

#### **1.4.4 Software Piracy and Crime related to IPRs**

Software piracy is an illegal reproduction and distribution for personal use or business. It comes under crime related to IPR infringement. Some of the other crimes under IPR infringement are: download of songs, downloading movies, etc.

#### **1.4.5 Cyber Terrorism**

It is defined as the use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives.

#### **1.4.6 Phishing**

It is a process of acquiring personal and sensitive information of an individual via email by disguising as a trustworthy entity in an electronic communication. The purpose of phishing is identity theft and the personal information like username, password, and credit card number etc. may be used to steal money from user account. If a telephone is used as a medium for identity theft, it is known as *Vishing* (voice phishing). Another form of phishing is *Smishing*, in which sms is used to lure customers.

#### **1.4.7 Computer Vandalism**

It is an act of physical destroying computing resources using physical force or malicious code.

#### **1.4.8 Computer Hacking**

It is a practice of modifying computer hardware and software to accomplish a goal outside the creator's original purpose. The purpose of hacking a computer system may vary from simply demonstrations of the technical ability, to sealing, modifying or destroying information for social, economic or political reasons. Now the corporate are hiring hackers, a person who is engaged in hacking computers, to intentionally hack the computer of an organization to find and fix security vulnerabilities.

The hackers may be classified as:

- White Hat: white hat hackers are the persons who hack the system to find the security vulnerabilities of a system and notify to the organizations so that a preventive action can be taken to protect the system from outside hackers. White hat hackers may be paid employee of an organization who is employed to find the security loop-holes, or may be a freelancer who just wants to prove his mantle in this field. They are popularly known as ethical hackers.
- Black Hat: in contrast to the white hat, the black hat hack the system with ill intentions. They may hack the system for social, political or economically motivated intentions. They find the security loopholes in the system, and keep the information themselves and exploit the system for personal or organizational benefits till the organization whose system is compromised is aware of this, and apply security patches. They are popularly known as crackers.
- Grey Hat: Grey hat hackers find out the security vulnerabilities and report to the site administrators and offer the fix of the security bug for a consultancy fee.
- Blue hat: A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed.

#### **1.4.9 Creating and distributing viruses over internet**

The spreading of a virus can cause business and financial loss to an organization. The loss includes the cost of repairing the system, cost associated with the loss of business during downtime and cost of loss of opportunity. The organization can sue the hacker, if found, for the sum of more than or equivalent to the loss borne by the organization.

#### **1.4.10 Spamming**

Sending of unsolicited and commercial bulk message over the internet is known as spamming.

An email can be classified as spam, if it meets following criteria:

- a. Mass mailing:- the email is not targeted to one particular person but to a large number of peoples.
- b. Anonymity:- The real identity of the person not known
- c. Unsolicited:- the email is neither expected nor requested for the recipient.

These spams not only irritate the recipients and overload the network but also waste the time and occupy the valuable memory space of the mailbox.

#### **1.4.11 Cross Site Scripting**

It is an activity which involves injecting a malicious client side script into a trusted website. As soon as the browser executes the malicious script, the malicious script gets access to the cookies and other sensitive information and sent to remote servers. Now this information can be used to gain financial benefit or physical access to a system for personal interest.

#### **1.4.12 Online Auction Fraud**

There are many genuine websites who offers online auction over internet. Taking the advantage of the reputation of these websites, some of the cyber criminals lure the customers to online auction fraud schemes which often lead to either overpayment of the product or the item is never delivered once the payment is made.

#### **1.4.13 Cyber Squatting**

It is an act of reserving the domain names of someone else's trademark with intent to sell it afterwards to the organization who is the owner of the trademark at a higher price.

#### **1.4.14 Logic Bombs**

These are malicious code inserted into legitimate software. The malicious action is triggered by some specific condition. If the conditions holds true in future, the malicious action begins and based on the action defined in the malicious code, they either destroy the information stored in the system or make system unusable.

#### **1.4.15 Web Jacking**

The hacker gain access to a website of an organization and either blocks it or modify it to serve political, economical or social interest. The recent examples of web jacking are some of the websites of the educational institutes were hacked by Pakistani hackers and an animation which contains Pakistani flags were flashed in the homepage of these websites. Another example is Indian hackers hacked website of Pakistani railways and flashed Indian flag in the homepage for several hours on the occasion of Independence Day of India in 2014.

#### **1.4.16 Internet Time Thefts**

Hacking the username and password of ISP of an individual and surfing the internet at his cost is Internet Time Theft.

#### **1.4.17 Denial of Service Attack**

It is a cyber attack in which the network is chocked and often collapsed by flooding it with useless traffic and thus preventing the legitimate network traffic.

#### **1.4.18 Salami Attack**

It is an attack which proceeds with small increments and final add up to lead to a major attack. The increments are so small that they remain unnoticed. An example of salami attack is gaining access to online banking of an individual and withdrawing amount in such a small amounts that it remains unnoticed by the owner. Often there is default trigger set in the banking website and transactions below say, Rs. 1000 withdrawal are not reported to the owner of the account. Withdrawing amount of Rs. 1000 over a period of time will lead to total withdrawal of a large sum.

#### **1.4.19 Data Diddling**

It is a practice of changing the data before its entry into the computer system. Often, the original data is retained after the execution on the data is done. For example, DA or the basic salary of the person is changed in the payroll data of an individual for pay calculation. Once the salary is calculated and transferred to his account, the total salary is replaced by his actual salary in the report.

#### **1.4.20 Email Spoofing**

It is a process of changing the header information of an e-mail so that its original source is not identified and it appears to an individual at the receiving end that the email has been originated from source other than the original source.

# CYBER SECURITY TECHNIQUES

There are many cyber security techniques to combat the cyber security attacks. The next section discusses some of the popular techniques to counter the cyber attacks.

## 2.1 AUTHENTICATION

It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be. A typical method for authentication over internet is via username and password. With the increase in the reported cases of cyber crime by identity theft over internet, the organizations have made some additional arrangements for authentication like *One Time Password*(OTP), as the name suggest it is a password which can be used one time only and is sent to the user as an *SMS* or an email at the mobile number/email address that he have specified during the registration process. It is known as two-factor authentication method and requires two type of evidence to authentication an individual to provide an extra layer of security for authentication. Some other popular techniques for two-way authentication are: biometric data, physical token, etc. which are used in conjunction with username and password.

The authentication becomes more important in light of the fact that today the multinational organizations have changed the way the business was to be say, 15 years back. They have offices present around the Globe, and an employee may want an access which is present in a centralized sever. Or an employee is working from home and not using the office intranet and wants an access to some particular file present in the office network. The system needs to authenticate the user and based on the credentials of that user, may or may not provide access to the user to the information he requested. The process of giving access to an individual to certain resources based on the credentials of an individual is known as authorization and often this process is go hand-in-hand with authorization. Now, one can easily understand the role of strong password for authorization to ensure cyber security as an easy password can be a cause of security flaw and can bring the whole organization at high risk. Therefore, the password policy of an organization should be such that employees are forced to use strong passwords (more than 12 characters and combination of lowercase and uppercase alphabets along with numbers and special characters) and prompt user to change their password frequently. In some of the bigger organizations or an organization which deals in sensitive information like defence agencies, financial institutions, planning commissions, etc. a hybrid authentication

system is used which combines both the username and password along with hardware security measures like biometric system, etc. Some of the larger organizations also use *VPN*(Virtual Private Network), which is one of the method to provide secure access via hybrid security authentication to the company network over internet.

## 2.2 ENCRYPTION

It is a technique to convert the data in unreadable form before transmitting it over the internet. Only the person who have the access to the key and convert it in the readable form and read it. Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key. The decoding of the complex code to original text using key is known as decryption. If the same key is used to lock and unlock the data, it is known as symmetric key encryption.

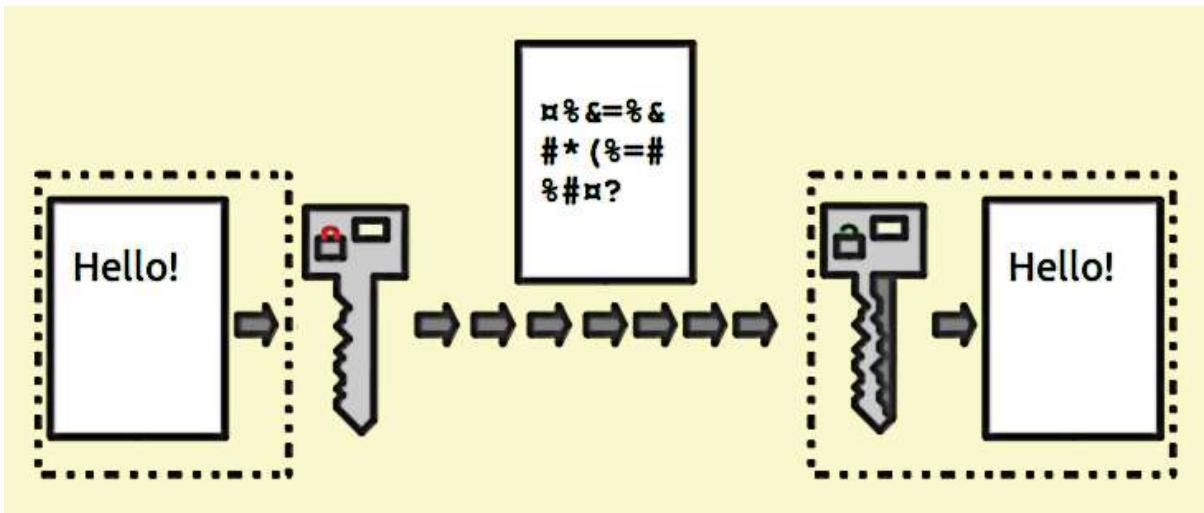


Figure 4: Encryption<sup>2</sup>

In symmetric key encryption, the after coding of data, the key is sent to the destination user via some other medium like postal service, telephone, etc. because if the key obtained by the hacker, the security of the data is compromised. Key distribution is a complex task because the security of key while transmission is itself an issue. To avoid the transfer of key a method called asymmetric key encryption, also known as public key encryption, is used. In

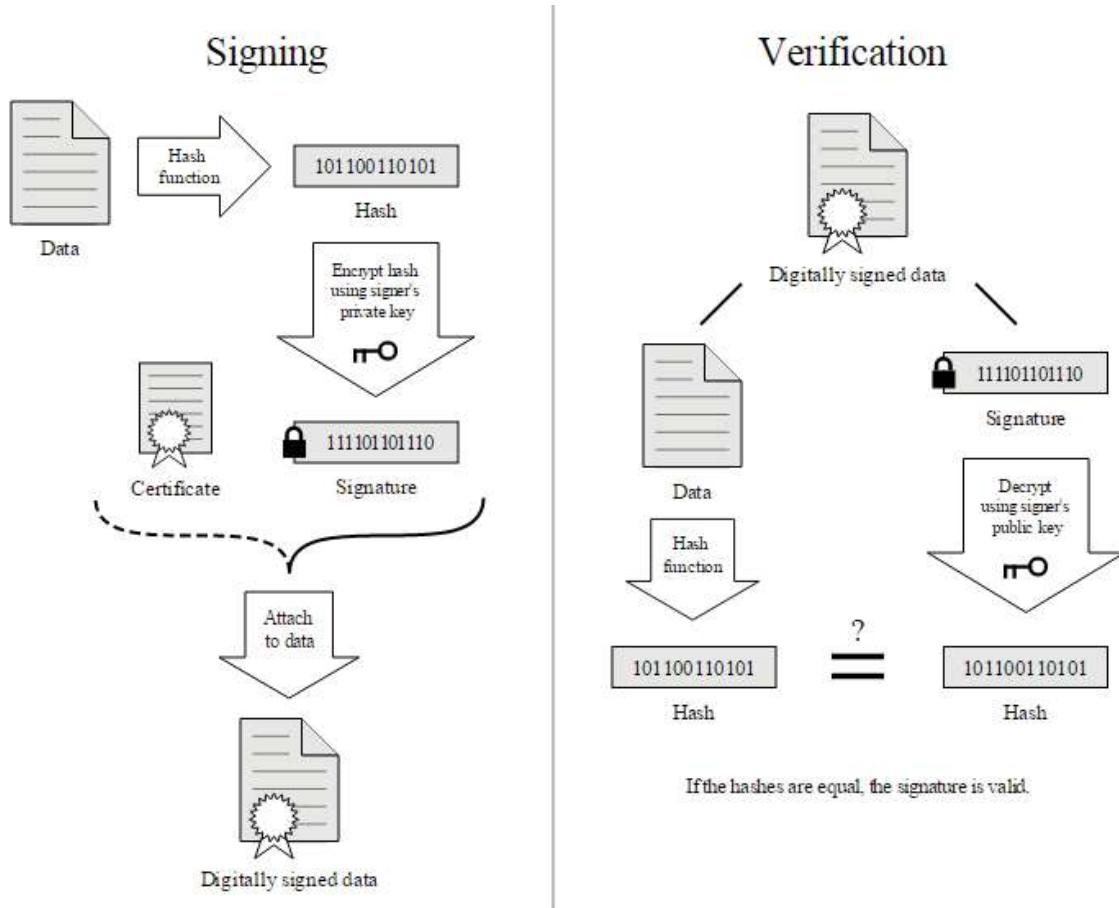
<sup>2</sup> Image courtesy: [https://upload.wikimedia.org/wikipedia/commons/b/bc/Public\\_key\\_encryption\\_keys.png](https://upload.wikimedia.org/wikipedia/commons/b/bc/Public_key_encryption_keys.png)

asymmetric key encryption, the key used to encrypt and decrypt data are different. Every user posse's two keys viz. public key and private key. As the name suggest, the public key of every user is known to everyone but the private key is known to the particular user, who own the key, only. Suppose sender A wants to send a secret message to receiver B through internet. A will encrypt the message using B's public key, as the public key is known to everyone. Once the message is encrypted, the message can safely be send to B over internet. As soon as the message is received by B, he will use his private key to decrypt the message and regenerate the original message.

## **2.3 DIGITAL SIGNATURES**

It is a technique for validation of data. Validation is a process of certifying the content of a document. The digital signatures not only validate the data but also used for authentication. The digital signature is created by encrypting the data with the private key of the sender. The encrypted data is attached along with the original message and sent over the internet to the destination. The receiver can decrypt the signature with the public key of the sender. Now the decrypted message is compared with the original message. If both are same, it signifies that the data is not tempered and also the authenticity of the sender is verified as someone with the private key(which is known to the owner only) can encrypt the data which was then decrypted by his public key. If the data is tempered while transmission, it is easily detected by the receiver as the data will not be verified. Moreover, the massage cannot be re-encrypted after tempering as the private key, which is posses only by the original sender, is required for this purpose.

As more and more documents are transmitted over internet, digital signatures are essential part of the legal as well as the financial transition. It not only provides the authentication of a person and the validation of the document, it also prevents the denial or agreement at a later stage. Suppose a shareholder instructs the broker via email to sell the share at the current price. After the completion of the transaction, by any chance, the shareholder reclaims the shares by claiming the email to be forge or bogus. To prevent these unpleasant situations, the digital signatures are used.



*Figure 5: Digital signature<sup>3</sup>*

## 2.4 ANTIVIRUS

There are verities of malicious programs like virus, worms, trojan horse, etc that are spread over internet to compromise the security of a computer either to destroy data stored into the computer or gain financial benefits by sniffing passwords etc. To prevent these malicious codes to enter to your system, a special program called an anti-virus is used which is designed to protect the system against virus. It not only prevents the malicious code to enter the system but also detects and destroys the malicious code that is already installed into the system. There are lots of new viruses coming every day. The antivirus program regularly updates its database and provides immunity to the system against these new viruses, worms, etc.

---

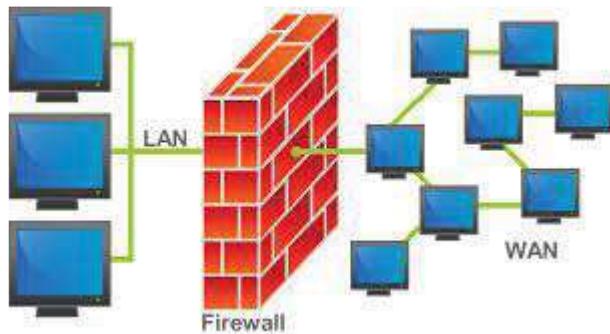
<sup>3</sup> Image courtesy: [https://upload.wikimedia.org/wikipedia/commons/2/2b/Digital\\_Signature\\_diagram.svg](https://upload.wikimedia.org/wikipedia/commons/2/2b/Digital_Signature_diagram.svg)



*Figure 6: Different antivirus available on the market<sup>4</sup>*

## 2.5 FIREWALL

It is a hardware/software which acts as a shield between an organization's network and the internet and protects it from the threats like virus, malware, hackers, etc. It can be used to limit the persons who can have access to your network and send information to you.



*Figure 7: Firewall<sup>5</sup>*

There are two type of traffic in an organization viz. inbound traffic and outbound traffic. Using firewall, it is possible to configure and monitor the traffic of the ports. Only the packets from trusted source address can enter the organization's network and the sources which are blacklisted and unauthorized address are denied access to the network. It is important to have firewalls to prevent the network from unauthorized access, but firewall does not guarantee this until and unless it is configured correctly. A firewall can be implemented using hardware as well as software or the combination of both.

---

<sup>4</sup> Image courtesy: <https://www.flickr.com/photos/thomasguest/3027199004>

<sup>5</sup> Image courtesy: <https://upload.wikimedia.org/wikipedia/commons/5/5b/Firewall.png>

- Hardware Firewalls: example of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet.
- Software Firewalls: These firewalls are installed and installed on the server and client machines and it acts as a gateway to the organizations' network.

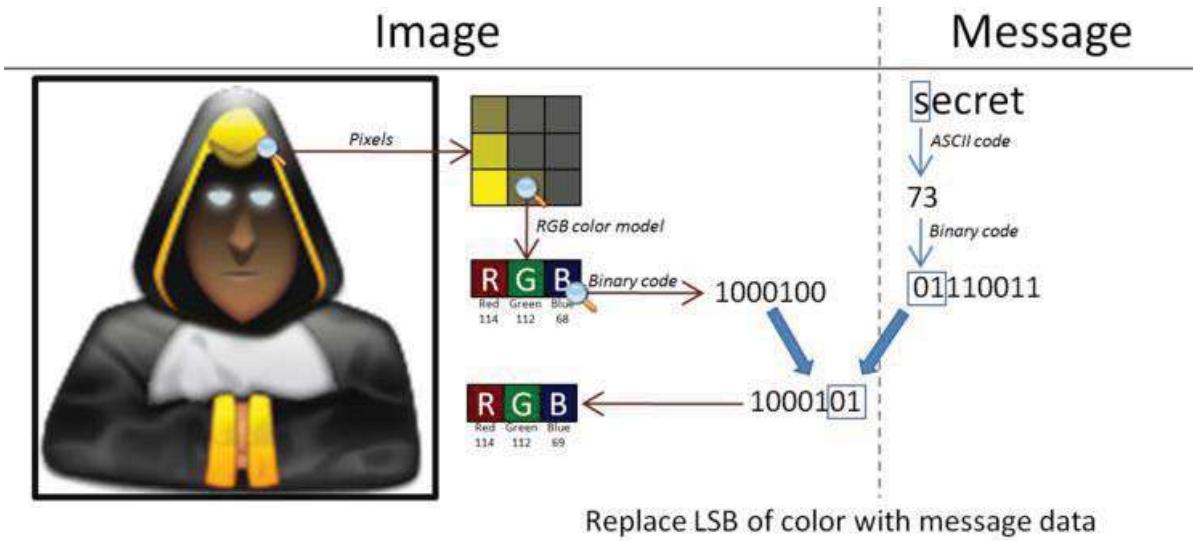
In the operating system like Windows 2003, Windows 2008 etc. it comes embedded with the operating system. The only thing a user need to do is to optimally configure the firewall according to their own requirement. The firewalls can be configured to follow “rules” and “policies” and based on these defined rules the firewalls can follow the following filtering mechanisms.

- Proxy- all the outbound traffic is routed through proxies for monitoring and controlling the packet that are routed out of the organization.
- Packet Filtering- based on the rules defined in the policies each packet is filtered by their type, port information, and source & destination information. The example of such characteristics is IP address, Domain names, port numbers, protocols etc. Basic packet filtering can be performed by routers.
- Stateful Inspection: rather than going through all the field of a packet, key features are defined. The outgoing/incoming packets are judged based on those defined characteristics only.

The firewalls are an essential component of the organizations' network. They not only protect the organization against the virus and other malicious code but also prevent the hackers to use your network infrastructure to launch DOS attacks.

## **2.6 STEGANOGRAPHY**

It is a technique of hiding secret messages in a document file, image file, and program or protocol etc. such that the embedded message is invisible and can be retrieved using special software. Only the sender and the receiver know about the existence of the secret message in the image. The advantage of this technique is that these files are not easily suspected.



*Figure 8: Steganography<sup>6</sup>*

There are many applications of steganography which includes sending secret messages without ringing the alarms, preventing secret files from unauthorized and accidental access and theft , digital watermarks for IPR issues, etc.

Let us discuss how the data is secretly embedded inside the cover file( the medium like image, video, audio, etc which is used for embed secret data) without being noticed. Let us take an example of an image file which is used as a cover mediem. Each pixel of a high resolution image is represented by 3 bytes(24 bits). If the 3 least significant bits of this 24 bits are altered and used for hiding the data, the resultant image, after embedded the data into it, will have unnoticeable change in the image quality and only a very experienced and tranined eyes can detect this change. In this way, evcery pixel can be used to hide 3 bits of information.

Similerly, introducing a white noise in an audio file at regular or random interval can be used to hide data in an audio or video files. There are various free softwares available for Steganography. Some of the popular ones are: QuickStego, Xiao, Tucows, OpenStego, etc.

---

<sup>6</sup> Image courtesy: [https://upload.wikimedia.org/wikipedia/commons/b/b8/Seformatbmp-embedding\\_full.png](https://upload.wikimedia.org/wikipedia/commons/b/b8/Seformatbmp-embedding_full.png)

# INVESTIGATING CYBER CRIMES: INTRODUCTION TO CYBER FORENSIC

In the preceding chapters, we have discussed the prevention techniques for cyber attack. What if one has encountered a cyber attack? What Next? The next step is to report the cyber crime. But if a person is exposed to cyber forensic principles, the chances that the person accidentally destroys the vital cyber evidences are minimized.

## 3.1 COMPUTER FORENSICS

Cyber forensic is a branch of science which deals with tools and techniques for investigation of digital data to find evidences against a crime which can be produced in the court of law. It is a practice of preserving, extracting, analyzing and documenting evidence from digital devices such as computers, digital storage media, smartphones, etc. so that they can be used to make expert opinion in legal/administrative matters.

The computer forensic plays a vital role in an organization as our dependency on computing devices and internet is increasing day-by-day. According to a survey conducted by University of California<sup>7</sup>, 93% of all the information generated during 1999 was generated in digital form, on computers, only 7% of the remaining information was generated using other sources like paper etc. It is not always easy to collect evidences as the data may be tampered, deleted, hidden or encrypted. Digital forensic investigation is a highly skilled task which needs the expertise of various tools, techniques and guidelines for finding and recovering the digital evidences from the crime scene or the digital equipments used in the crime. With digital equipments like smartphone, tablets, palmtops, smart tv, etc having increasing processing capabilities and computation speed, the possibility of use of these devices in cyber crime cannot be ruled out. A forensic investigator must not only have deep understanding of the working of these devices and also hands-on exposure to the tools for accurate data retrieval so that the value and integrity of the data is preserved.

---

<sup>7</sup> [http://www.isfs.org.hk/publications/ComputerForensics\\_part1.pdf](http://www.isfs.org.hk/publications/ComputerForensics_part1.pdf)

A computer can be used intentionally or unintentionally to cyber crime. The intentional use is to use your computer to send hate mails or installing cracked version of an otherwise licenced software into your computer. Unintentional use is the computer you are using contains virus and it is spread into the network and outside the network causing major loss to someone in financial terms. Similllerly a computer can be directly used to commit a digital crime. For example, your computer is used to access the sensitive and classified data and the data is sent someone inside/outside the network who can use this data for him own benefit. The indirect use of computer is when while downloading a crack of a software, a trozan horse is stored in the computer, while creates a backdoor in the network to facilitate hacker. Now the hacker logs into your computer and use it for committing cyber crime. An experienced computer forensic investigator plays a crucial role in distinguishing direct and indirect attack. Computer forensic experts are also useful for recovery of accidental data loss, to detect industrial espionage, counterfeiting, etc.

In large organization, as soon as a cyber crime is detected by the incident handling team, which is responsible for monitoring and detection of security event on a computer or computer network, initial incident management processes are followed<sup>8</sup>. This is an in-house process. It follows following steps:

1. *Preparation:* The organization prepares guidelines for incident response and assigns roles and the responsibilities of each member of the incident response team. Most of the large organizations earn a reputation in the market and any negative sentiment may negatively affect the emotions of the shareholders. Therefore, an effective communication is required to declare the incident. Hence, assigning the roles based on the skill-set of a member is important.
2. *Identification:* based on the traits the incident response team verifies whether an event had actually occurred. One of the most common procedures to verify the event is examining the logs. Once the occurrence of the event is verified, the impact of the attack is to be assessed.
3. *Containment:* based on the feedback from the assessment team, the future course of action to respond to the incident is planned in this step.

---

<sup>8</sup> <http://countuponsecurity.com/2012/12/21/computer-security-incident-handling-6-steps/>

4. *Eradication*: In this step, the strategy for the eradication or mitigate of the cause of the threat is planned and executed.
5. *Recovery*: it is the process of returning to the normal operational state after eradication of the problem.
6. *Lesson Learned*: if a new type of incident is encounter, it is documented so that this knowledge can be used to handle such situations in future.

The second step in the process is forensic investigation is carried out to find the evidence of the crime, which is mostly performed by 3<sup>rd</sup> party companies. The computer forensic investigation involves following steps:

1. *Identify incident and evidence*: this is the first step performed by the system administrator where he tries to gather as much information as possible about the incident. Based on this information the scope and severity of the attack is assessed. Once the evidence of the attack is discovered, the backup of the same is taken for the investigation purpose. The forensic investigation is never performed on the original machine but on the data that is restored from the backup.
2. *Collect and preserve evidence*: Various tools like Helix, WinHex, FKT Imager, etc. are used to capture the data. Once the backup of the data is obtained, the custody of the evidence and the backup is taken. MD5(message digest) hash of the backup is calculated and matched with the original one to check the integrity of the data. Other important sources of information like system log, network information, logs generated by Intrusion Detection Systems(IDS), port and process information are also captured.
3. *Investigate*: The image of the disk is restored from the backup and the investigation is performed by reviewing the logs, system files, deleted and updates files, CPU uses and process logs, temporary files, password protected and encrypted files, images, videos and data files for possible steganographic message, etc.
4. *Summarize and Presentation*: The summery of the incident is presented in chronological order. Based on the investigation, conclusions are drawn and possible cause is explained.

While carrying out the digital forensic investigation, rules and procedure must be applied. Specially while capturing the evidence. It should be ensured that the actions that are taken for capturing the data do not change the evidence. The integrity of the data should be maintained. It must be ensured that the devices used for capturing the backup are free from contamination.

Moreover, all the activities related to seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review<sup>9</sup>. Prevention is always better than cure. It is always recommended to fine tune your intrusion detection system like firewall occasionally perform penetration tests on your network to avoid pray to hacker. Last but not the least, report the crime.

### **3.2 WHY SHOULD WE REPORT CYBER CRIME?**

Some of the companies do not report a cyber crime incident because they fear this will harm their reputation amongst its shareholders. Some of the data are very sensitive and its disclosure may impact their business negatively. But, the fact is until and unless a cyber crime incident is reported, the cyber criminals will never be grabbed by the law enforcement agencies. This will further worsen the conditions and encourage the criminals to repeat these types of incidents with the same or the other organizations. So it is very important to identify and prosecute them. This will help not only to identify the existing threats to the economy and the infrastructure but also new threats are identified. Depending on the scope of a cyber crime, the cyber crime should be reported to nearest cyber cell of your locality, state cyber cell, central investigating agencies like CBI, IB or the international bodies like Interpol.

Some of the addresses of the cyber coordinating units are:

<b>Assam</b> <b>Address:</b> CID HQ,Dy.SP., Assam Police <b>Contact Details:</b> Ph: +91-361-252-618, +91 9435045242 <b>E-mail id:</b> ssp_cod@assampolice.com	<b>Haryana</b> <b>Address:</b> Cyber Crime and Technical Investigation Cell, Joint Commissioner of Police, Old S.P.Office complex,Civil Lines, Gurgaon <b>E-mail:</b> jtcp.ggn@hry.nic.in
<b>Mumbai</b> <b>Address:</b> Cyber Crime Investigation Cell, Office of Commissioner of Police office,Annex -3 Building, 1st floor, Near Crawford Market, Mumbai-01.	<b>Chennai</b> <b>Address:</b> Asst. Commr. of Police, Cyber Crimes Cell, Vepery, Chennai <b>Contact Details:</b> 04423452348, 04423452350

<sup>9</sup> <http://www.isfs.org.hk/publications/011009/Collins-CIO&CeO.pdf>

<p><b>Contact Details:</b> +91-22-22630829, +91-22-22641261</p> <p><b>Web site:</b> <a href="http://www.cybercellmumbai.com">http://www.cybercellmumbai.com</a></p> <p><b>E-mail id:</b> officer@cybercellmumbai.com</p> <p><b>Thane</b></p> <p><b>Address:</b> 3rd Floor, Police Commissioner Office, Near Court Naka, Thane West, Thane 400601.</p> <p><b>Contact Details:</b> +91-22-25424444</p> <p><b>Web site:</b> <a href="http://www.thanepolice.org">www.thanepolice.org</a></p> <p><b>E-Mail:</b> police@thanepolice.org</p>	<p><b>E-mail id:</b> cybercrimechn@yahoo.com</p> <p><b>For Rest of Tamil Nadu,</b></p> <p><b>Address:</b> A-Wing, III rd Floor, Rajaji Bhawan, Besant Nagar, Chennai-600090</p> <p><b>Contact Details:</b> 044-24461959, 24468889, 24463888</p> <p><b>E-mail id:</b> hobechohn@cbi.gov.in</p>
<p><b>Bangalore</b> (for whole of the Karnataka)</p> <p><b>Address:</b> Cyber Crime Police Station, C.O.D Headquarters, Carlton House, # 1, Palace Road, Bangalore - 560 001</p> <p><b>Contact Details:</b> +91-80-2220 1026, +91-80-2294 3050, +91-80-2238 7611 (FAX)</p> <p><b>Web site:</b> <a href="http://www.cyberpolicebangalore.nic.in">http://www.cyberpolicebangalore.nic.in</a></p> <p><b>Email-id:</b> ccps@blr.vsnl.net.in, ccps@kar.nic.in</p>	<p><b>Hyderabad</b></p> <p><b>Address:</b> Cyber Crime Police Station, Crime Investigation Department, 3rd Floor, D.G.P. office, Lakdikapool, Hyderabad – 500004</p> <p><b>Contact Details:</b> +91-40-2324 0663, +91-40-2785 2274, +91-40-2785 2040, +91-40-2329 7474 (Fax)</p> <p><b>Website:</b> <a href="http://www.cidap.gov.in/cybercrimes.aspx">http://www.cidap.gov.in/cybercrimes.aspx</a></p> <p><b>E-mailid:</b> cidap@cidap.gov.in, info@cidap.gov.in, cybercell_hyd@hyd.appolice.gov.in</p>
<p><b>Delhi</b></p> <p><b>CBI Cyber Crime Cell:</b> Superintendent of Police, Cyber Crime Investigation Cell, Central Bureau of Investigation, 5th Floor, Block</p>	<p><b>Pune</b></p> <p><b>Address :</b> Deputy Commissioner of Police(Crime), Office of the Commissioner Office, 2, Sadhu Vaswani Road, Camp,Pune 411001</p>

<p>No.3, CGO Complex, Lodhi Road, New Delhi – 3</p> <p><b>Contact Details:</b> +91-11-4362203, 011-26851998 011-26515229, +91-11-4392424</p> <p><b>Web site:</b> <a href="http://cbi.nic.in">http://cbi.nic.in</a></p> <p><b>Asst. Commissioner of Police,</b> Cyber Crime Cell, EOW, Crime Branch, 2nd Floor, Police Training School, Malaviya Nagar, New Delhi-110 017</p> <p><b>E-Mail:</b> cbiccic@bol.net.in, dcp-eow-dl@nic.in</p>	<p><b>Contact Details:</b> +91-20-26123346, +91-20-26127277 +91-20-2616 5396, +91-20-2612 8105 (Fax)</p> <p><b>Website:</b> <a href="http://www.punepolice.gov.in">www.punepolice.gov.in</a></p> <p><b>E-Mail:</b> crimecomp.pune@nic.in, punepolice@vsnl.com</p>
<p><b>Himachal Pradesh</b></p> <p><b>Address :</b> CID Office ,Dy.SP, Himachal Pradesh</p> <p><b>Contact Details:</b> +91-94180 39449</p> <p><b>E-mail:</b> soodbrijesh9@gmail.com</p>	<p><b>Gujarat</b></p> <p>DIG, CID, Crime and Railways. Fifth Floor, Police Bhavan Sector 18, Gandhinagar 382 018</p> <p><b>Contact Details:</b> +91-79-2325 4384, +91-79-2325 0798, +91-79-2325 3917 (Fax)</p>
<p><b>Jharkhand</b></p> <p><b>Address:</b> IG-CID,Organized Crime, Rajarani Building, Doranda Ranchi – 834002</p> <p><b>Contact Details:</b> +91-651-2400 737, +91-651-2400 738</p> <p><b>E-mail:</b> a.gupta@jharkhandpolice.gov.in</p>	<p><b>Kerala</b></p> <p><b>Address :</b> Hitech Cell, Police Head Quarters, Thiruvananthapuram</p> <p><b>Contact Details:</b> +91-471 272 1547, +91-471 272 2768</p> <p><b>E-mail:</b> hitechcell@keralapolice.gov.in</p>
<p><b>Jammu</b></p> <p><b>Address:</b> SSP-Crime, CPO Complex,Panjtirthi, Jammu-180004</p> <p><b>Contact Details:</b> +91-191-257-8901</p>	<p><b>Orissa</b></p> <p><b>Address:</b> CID,Crime Branch, Orissa</p> <p><b>Contact Details:</b> +91 94374 50370</p> <p><b>E-mail:</b> splcidcb.orpol@nic.in</p>

<b>E-mail:</b> <a href="mailto:sspcrmjmu-jk@nic.in">sspcrmjmu-jk@nic.in</a>	
<b>Meghalaya</b>  <b>Address:</b> SCRB,Superintendent of Police Meghalaya  <b>Contact Details:</b> +91 98630 64997  <b>E-mail:</b> <a href="mailto:scrb-meg@nic.in">scrb-meg@nic.in</a>	<b>Punjab</b>  <b>Address:</b> Cyber Crime Police Station, DSP Cyber Crime, S.A.S Nagar,Patiala, Punjab  <b>Contact Details:</b> +91 172 2748 100
<b>Bihar</b>  <b>Address:</b> Cyber Crime Investigation Unit, Dy.S.P.Kotwali Police Station, Patna  <b>Contact Details:</b> +91 94318 18398  <b>E-mail:</b> <a href="mailto:cciu-bih@nic.in">cciu-bih@nic.in</a>	<b>West Bengal</b>  <b>Address:</b> CID, Cyber Crime, West Bengal  <b>Contact Details:</b> +9133 24506163  <b>E-mail:</b> <a href="mailto:occyber@cidwestbengal.gov.in">occyber@cidwestbengal.gov.in</a>
<b>Uttar Pradesh</b>  <b>Address:</b> Cyber Complaints Redressal Cell, Nodal Officer Cyber Cell Agra, Agra Range 7,Kutchery Road, Baluganj,Agra-232001, Uttar Pradesh  <b>Contact Details:</b> +919410837559  <b>E-mail:</b> <a href="mailto:info@cybercellagra.com">info@cybercellagra.com</a>	<b>Uttarakhand</b>  <b>Address:</b> Special Task Force Office Sub Inspector of Police, Dehradoon  <b>Contact Details:</b> +91 135 264098, +91 94123 70272  <b>E-mail:</b> <a href="mailto:dgc-police-us@nic.in">dgc-police-us@nic.in</a>

# SOME RECENT CYBER SECURITY ATTACKS

## 4.1 INTRODUCTION

The proliferation of Internet amongst the population is getting deep day-by-day. This not only increase the scope of e-governance and e-commerce in the area of healthcare, banking, power distribution, etc. but also expose these sectors to cyber threats like hacking, credential thefts, data tempering, account hijacking, etc. According to a report, there were around 62,189 cyber security incidents, originating mainly from Countries including US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE, in the period from Jan-May, 2014. Also, around 10,000 Indian government sites were compromised in this period. India has a serious shortage of IT Security professional to deal with such threats in effective manner. According to a report, India needs around one million cyber security professionals to deal with cyber threats effectively.

## 4.2 SOME RECENT CYBER CRIME INCIDENTS

In the current section, we will discuss some of the common cyber crimes and frauds incidents over internet so that you could appreciate how these little ignorance could lead to a big disaster.

1. Paypal, an international online money transfer service, which allows you to safely transfer money through an Internet using various encryption techniques and provides an alternative to other traditional payment methods like cheques, money orders, etc. It has an active user base of over 100 million active users in 190 countries and performs over 9 million payments daily. It is one of the popular medium of payment over online auction sites like ebay etc. It is a convenient medium for trading particularly of the buyers and sellers are from different countries and have different currencies.

Romanian Hacker TinKode aka Razvan Cerniaianu, exploited a loophole in the code of the chargeback process of PayPal. Due to this, a user can double its money on every attempt. Suppose the user has Rs.1000, then using this loophole, the amount will be doubled to Rs.2000 in the first attempt. Now this Rs. 2000 will be doubled to Rs. 4000 in the second attempt. Further Rs. 4000 will be doubled to Rs. 8000. Like wise this process will continue endlessly.

2. In Australia, a website called MP3/WMA Land, which offers a large number of pirated songs, music video clips for free download to its users. This resulted in heavy financial losses to the artists and the producers of those songs. The complain was loudeged by an organizations called Music Industry Piracy Investigations.

The owners of the website, Ng, Tran and Le, who were the students of Australian University, were framed for Australia's largest copyright infringement case(Urbas, 2012).

3. One of the intresting case of online stalking was registered by Mrs. Ritu Kohli at Delhi Police (Kaur, 2013). She reported that someone is using her identity over the Internet in the website [www.mirc.com](http://www.mirc.com) for chatting, and distributed her address and phone number. As a result she received a large number of phone calls from all over including Dubai, Ahemdabad, Mumbai, etc. at odd hours. This caused a lot of mental frustration and she decided to report the case. Based on her complain, Delhi Police traced the IP address and finally traced the address of accused, Manish Kathuria and arrested him.

A Dubai based NRI was blackmailed, and by the time the case was reported, he had already approximatly 1.25 crore to the accused (Madhya Pradesh State Cyber Police, 2013). The NRI met a girl over Internet and after a series of long chatting sessions, the girl won the love and trust of the NRI. In the meantime, she introduces him with several of her friends. Due to some reasons, the relation could not last long. After some time, one of the girl's friend, who was introduced to him by the girl, reports him that due to the mental stress of the broken relationship, the girl have committed suicide and police is investigating the case. Many fake copies of the letters from CBI, High Court of Calcutta, New York police and Punjab University etc. were also sent to the NRI. The NRI sought help from the girl's friend, who in turn introduced her with a law firm based at Kolkata. The owner of the law firm agreed to take this case. A huge sum of money was demanded by the law firm and a total of more than 1.26 crore were transferred on different occassions and he still demanded more money. The NRI smell something fishy and reported the case to Mumbai Police. The NRI forwarded all the email that he received from the girl, her friend and the owner of the law firm. After the forensic investigation for the email, the IP address of all the three persons were found to be originated from the same source. After investigation, it was found that the identity of the girl and her friends were all virtual i.e. they does not exist. The owner of the law firm was the mastermind who assumed false identity of all the persons and created this false story to blackmail the NRI.

4. Iran's nuclear facility at Natanz was attacked by virus, *Stuxnet* which is believed to be developed by US (Shubert, 2011). It was not possible to inject the virus through the Internet as the network of the the Iran's nuclear facility is a private network and was isolated from rest of the world. The virus first infected the third party utility which is used by Natanz facility and gained access to the network. The virus was designed to attack a specific system software which controls the operation of Siemens controllers. The virus speeds up or slow down the centrifuges and thus wearing them out prematurely. Moreover, it hijacked the system and send false signals about the health and status of the nuclear plant. Therefore, by the time the effect of the virus was detected, it was too late and the virus have done much harm to the nuclear facility.
5. A trojan mail was used to hack the user name and the password of the current account of Mumbai based firm RPG Group and siphoned off Rs. 2.41 crore by Real Time Gross Settlement(RTGS) (Narayan, 2013). Th bank officials suspected when they notice the huge amount of money transfer. They confirmed they came from the company's officials who denied the transfer of the money to the designated accounts. Based on the names and the address of the account holders who have received the money, the police came to know that the account holders have permitted the main accused to use their account in return of huge commission.
6. Chennai police cracked a case of credit card fraud, where two BPO employees with the help of the son of the accused, increased the credit card limit and the communication address of the credit card owner (Madhya Pradesh State Cyber Police, 2013). They illegally hacked into their company's computer to find out the details of the credit card owner. They credit card company was cheated for about 7 lakhs before the incident was noticed. Due to the chance of the communication address, the owner of credit card could not receive monthly statements generated at the month's end. The case was registered with the Chennai police. After the digital forensic investigation of the BPO's computer system, it was found that its two employees have illegally accessed to the computer to steal the customer record.
7. A case of copyright infringement was lodged in Andhra Pradesh (Nandanwar, 2013). A well known mobile service operator company launched a promotional campaign, in which it offered a mobile phone at a very low cost to its customers with a lock-in period of 3-years. The software of the phone was configured in such a way that, in the lock-in period the sim of any other company cannot work with the handset. A competitor of that company lured the existing customers of the company which gave

the mobile phone to “unlocked” the phone by cracking the software of the mobile so that any other sim can be used with the handset. The company reported the crime and the case were registered under copyright infringement u/s 63 of copyrights act.

8. A gang of criminals is active over the cyber space, which steals the credit card data of the cardholders from the POS at shopping malls, petrol pumps, resturants, hotels, etc. and use these cards to book air tickets online. According to the reports, over 15000 credit cards were fraudulently used by these criminals to book online tickets which account for approximatly Rs. 17 crore revenue loss. These criminals use public infrastructure like cyber cafe, etc. to book these tickets so that it is difficult to trace them. The fraud came to the notice when the customers who were charged for booking an airticket and these customers reported at the card issuing banks claming that these tickets were never booked by them.
9. In the year 2000, a worm known as Love Bug worm or VBS/Loveletter, which specially target Windows operating system based computer system, caused damage costing approx. Rs. 22,000 crore. An spam mail containing “ILOVEYOU” in the subject line and LOVE-LETTER-FOR-YOU.TXT.vbs as an attachment is received. If the user clicked the attachment, the machine gets infacted and the worm start searching all the drive of the computer and start currupting the files. It also start forwarding the copies of the email to all the outlook contacts added in the addressbook of the user. Nearly 10% machines connected to the Internet were infacted within no time (Madhya Pradesh State Cyber Police, 2013). Many large organizations which includes British parliament, Pentagon have to shut down the email system to stop this worm spreading into their network.
10. Online degree fraud are very popular these days over internet where accredited online degrees are offered by fake Universities (Gollin, 2003). These diploma mills offer to turn your work experience into a degree in exchange of money. The transcripts are also issued to the students on the basis of self evaluation. Its only when the students is rejected on account of fake degree, he realize that he fell pray to online fraud.
11. Can you belive a fake tweet message can cost \$136 billion loss within seconds (Fisher, 2013). The US stock markets crashed in response to a fake twitter message send via hacked twitter account of Associated Press, USA which reported two explosions in the White House and that President Barack Obama had been injured. Later, Syrian Electronic Army, a terrorist group claimed responsibility on its own Twitter feed for the AP hack. The hacking was performed by sending a phishing e-

mail. As soon as the link in the phishing e-mail was clicked, a spyware was installed in the computer and the information stored in the system were sent to remote servers. Using this information the account of AP was hacked and the hoax was created which effected sentiments of the investor of NY Stock Exchange and resulted in heavy loss.

12. Recently a new virus, which infects the Point of Sale(POS) machines and steals the payment record of credit card of the customers. These confidential data like PIN codes, credit card numbers, expiration date, CCV number, etc. are tracked and sent to the hackers so that this information can be misused for committing financial frauds (US-CERT, 2014).
13. The people with ill intentions are not only looking for your private and confidential data, but are in search of your communication infrastructure so that your identity can be used for hiding their identity so that they are not caught after creating neusence. The terrorist outfit Indian Mujahideen(IM) used the unprotected wi-fi network of a Mumbai based US citizen, Kenneth Haywood. They hacked his wi-fi network used send an e-mail, which contains his IP address, to a news agency just 5 minutes before the Ahemdabad blast (Chowdhury, Nair, & Johnson, 2008).
14. The terrorist used open wi-fi network of Matunga's Khalsa College of Arts, Science and Commerce, Mumbai to send a terror mail to media house (The Indian Express, 2008). The terrorists remotely access the router and deleted the system logs after using the network so that it becomes difficult for the investigating to trace the origin of the email.
15. Pune based software engineer, Asma Sandip Thorve was arrested by economic offences wing of Pune police for illegally steeling source code of the software product and other confidential information of Brainvisa Technologies due to which the company lost Rs. 46.5 crores (Times of India, 2009).
16. There is a new type of crime evolving over internet where a prospective business partner will offer you a homebased business oppourtunity with no investment and very lucrative commission (Castillo, 2007). Once the person agrees to work with the company, the prospective business partner will ask for the details like address, phone numbers, photo identity, date of birth, etc. After some time, the person will receive parcel at the address with repackging instructions along with the list of addresses where these parcels are to be dispatched abroad. Actually these goods are purchased using stolen credit cards and the goods are delivered at the address provided by the person. The person will be held responsible if address of the delivery of the goods is

traced by the investigators. The real trouble begins when your commision arrives. It is in the form of third party cheque and is of the higher amount then you expected. Some days latter an instruction to return the excess amount electronically is received. Once the excess fund is electronically transferred, the bank will discover that the cheque is fake and the person will be help responsible for this act.

17. Some of the customers of ICICI bank were victim phishing attack (Nair, 2009). Some of the customers received an email from a person who claimed to be an official of ICICI bank. He asked the customers to update their account information using a link which redirects the customers to a page which is very similler to ICICI bank's webpage. The case was registered by the bank officials when this fraud came to the knowledge of the bank when some of the customers got suspecious and informed the IT department of the bank to verify the source of such email. The bank officials were suprized to find out that the website, which was very closely resembling the bank's official website. If the customer used that link to update his account credentials by logging into the fake website using their user id and the password, these details would reached the hackers and they can later use this information to login into the customer's account and transfer money aur pruchase goods online.
18. The cyber criminals have targeted the gas filling station in the US to skim the credit card and debit card data. The hacker planted bluetooth enabled credit card skimmers in most of the gas stations locted in the Southern United States. The customer data which includes information like account number, PIN, CVV, etc eas used by the hackers to withdraw more than \$2 million from the ATM mostly located at Manhattan.
19. The hackers used the tools used by the law enforcement agencies to parse data from iPhones to steel the private photographs of female celebreties in the US (Hazen, 2014). The hackers are belived to be using software called Elcomsoft Phone Password Breaker and iBrute to log into apple's site and download the backupfiles into their machines.
20. There are many incidents were non- friendly countries launch cyber attacks to gain access to the sensitive information. One such event is Russia is suspected for his involvement in hacking of US financial system (Farberov, 2014). One of the leading banks JPMorgan Chase was reported to be attacked by Russian hackers. The hackers were successful in steeling the sensitive data from the bank's server.
21. Recently, a Chinese mobile company, Xiaomi was found guilty for sending the sensitive data to Chinese servers (Kumar, 2014). This information includes sms,

photographs, contact list, etc. without the knowledge of the users. It's not the first time that a Chinese company was suspected for espionage and US government have banned the use of Chinese equipments in some of its major establishments.

# CYBER SECURITY INITIATIVES IN INDIA

## 5.1 INTRODUCTION

With the growth of internet, the dependence on computers has increased exponentially. The challenge is to protect critical information infrastructure, like civil aviation sector, Railways' passenger reservation system and communication network, port management, companies and organisations in power, oil and natural gas sectors, banking and finance, telecom sector, etc. from cyber attacks. India is ranked fourth among the top 50 countries in terms of the number of cyber crime complaints reported to the Internet Crime Complaint Centre (IC3), preceded only by the US, Canada and the UK based on the 2014 IC3 annual report (The Telegraph, 2015).

Shortage of trained cyber security workforce is of serious concern to India. In comparison to China, US and Russia that have 125000, 91080 and 7300 trained cyber experts respectively; India has merely 556 cyber experts deployed in various government agencies (Joshi, 2013). India is considered an IT superpower that is a major exporter of software and hosts major ITES-based outsourced businesses. Therefore, IT constitutes a major share of Indian economy. Recently, European Union has picked holes in India's data security system and suggested that a joint expert group be set up to propose ways on how the country should tighten measures for qualifying as a data secure nation (Sen, 2013). Therefore, India needs look seriously into upgrading its Information Security infrastructure and reframe cyber policies to get data secure status from EU. This is crucial for India to retain high-end outsourced business, which has a potential of increasing from the existing \$20 billion to \$50 billion.

## 5.2 COUNTER CYBER SECURITY INITIATIVES IN INDIA

To counter cyber security attacks, Government of India have taken some initiatives which are listed below:

1. **National Counter Terrorism Center(NCTC):** After 26/11 attack in 2008, suddenly the Indian government realized the importance of Counter terrorism initiatives and proposed National Counter Terrorism Center(NCTC) to provide intelligence inputs to the decision makers to plan for counter terrorist activities. The NCTC is supposed to coordinate between various State and Central govt. agencies and serve as a single and

effective point of control and coordination of all counter terrorism measures. It is modeled on the American NCTC and Britain's Joint Terrorism Analysis Centre and will derive its powers from the Unlawful Activities Prevention Act, 1967 (Mrunal, 2012).

2. **National Information Security Assurance Programme (NISAP):** To create the awareness among the people in the government and critical sector organization, CERT-In has taken an initiative called National Information Security Assurance Programme (NISAP), to develop and implement information security policy and information security best practices based on ISO/IEC 27001 for protection of their infrastructure. CERT-in has established the facility for Computer Forensics for investigation of cyber crimes and to provide hands on training to the law enforcement agencies and judiciary. This infrastructure is being augmented to include network forensics and mobile forensics investigation facility. CERT-In is cooperating with defence, banks, judiciary and law enforcement agencies in training their officials as well as extending the support in investigation of cyber crimes (Srinath, 2006).
3. **Computer Emergency Response Team-India(CERT-In):** The Indian Computer Emergency Response Team was created in 2004 by Department of Information Technology. The purpose of creating CERT-In was to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country and is also responsible for overseeing administration of the IT act (CERT-In, 2014).
4. **Indo US Cyber Security Forum (IUSCSF):** The India-US Cyber Security Forum was established in 2001 and is dedicated to protecting the critical infrastructure of the knowledge-based economy. The members of the forum are various government and private sector organizations, both from India and the United States, working under the Forum's auspices, have identified risks and common concerns in cyber security and crafted an action-oriented work plan on securing networked information systems. The Forum focuses on cyber-security, cyber-forensics and related research and works towards enhancing co-operation among law enforcement agencies on both sides in dealing with cyber crime. Defence services of both the countries will enhance their interaction through exchange of experience in organizational, technological, and procedural aspects. Ongoing co-operation between India's STQC and the US National Institute of Standards and Technology (NIST) will expand to new areas including harmonization of standards. CII and their US counterpart have decided to set up an

India Information Sharing and Analysis Centre (ISAC) and India Anti-Bot Alliance ('bot' refers to software that can be tasked to invade computers and undertake malicious activities remotely on behalf of hackers) (Press Information Bureau, 2006).

5. **National Critical Information Infrastructure Protection Centre (NCIIPC) of India:** It is declared as a nodal agency for the protection of critical information infrastructure of India and is responsible for all measures including R&D for protection of critical information infrastructure. Some of the activities that NCIIPC performs are (Chander, 2013):
  - a. Identification of Critical Sub-sectors
  - b. Study of Information Infrastructure of identified critical sub-sectors
  - c. Issue of Daily / Monthly cyber alerts / advisories
  - d. Malware Analysis
  - e. Tracking zombies and Malware spreading IPs
  - f. Cyber Forensics activities
  - g. Research and Development for Smart and Secure Environment.
  - h. Facilitate CII owners in adoption of appropriate policies, standards, best practices for protection of CII.
  - i. Annual CISO Conference for Critical Sectors.
  - j. Awareness and training
  - k. 24X7 operation and helpdesk
6. **National Intelligence Grid (Natgrid) project of India:** It is the integrated intelligence grid developed by C-DAC-Pune connecting databases of core security agencies of the Government of India (C-DAC, 2014). It is a counter terrorism measure that collects and collates a host of information from government databases including tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel (Yasmeen, 2013). This combined data will be made available to 11 central agencies, which are: Research and Analysis Wing, the Intelligence Bureau, Central Bureau of Investigation, Financial intelligence unit, Central Board of Direct Taxes, Directorate of Revenue Intelligence, Enforcement Directorate, Narcotics Control Bureau, Central Board of Excise and Customs and the Directorate General of Central Excise Intelligence.
7. **Crime and Criminal Tracking Networks and Systems (CCTNS) project of India:** It is a project under National e-Governance Plan(NeGP) covering all 28 States and 7

UTs which aims at creation of a nation-wide networking infrastructure for evolution of IT-enabled sophisticated tracking system around 'investigation of crime and detection of criminals (PTI, 2013). The goals of the CCTNS are to facilitate collection, storage, retrieval, analysis, transfer and sharing of data and information at the police station and between the police station and the State Headquarters and the Central Police Organizations. CCTNS would provide a comprehensive database for crimes and criminals, and it would be easier for the law enforcement agencies to track down a criminal moving from one place to another.

8. **National Cyber Coordination Centre (NCCC):** National Cyber Coordination Centre is a proposed cyber security and e-surveillance agency in India. It is intended to screen communication metadata and co-ordinate the intelligence gathering activities of other agencies. Some of the components of NCCC include a cyber attack prevention strategy, cyber attack investigations and training, etc.
9. **Botnet Cleaning Center:** As a part of the Digital India programme, the Government is setting up a centre that will detect malicious programmes like 'botnets' and help people remove such harmful softwares from their devices. "The Government is setting up 'botnet' cleaning and malware analysis centre" according to media reports. Botnet is a network of malicious software. It can steal information, take control of device function and carry out cyber attacks like Distributed Denial-of-Service (DDoS).
10. **E-mail policy of Government of India:** In present date Email is considered to be as the major source of communication between individuals and organization as well. The same applies to Govt. of India (GOI) as well. E-mail has become major mode of communications for the entire government. With the increasing use of Emails to communicate among different Govt. Agencies, the Email Policy was laid down by Government of India (GOI) in October 2013. Here we will cover some of the important clause of policy, readers are advised to download policy from Department of Electronics and IT website.
11. **Ministry of Home Affairs (MHA):** The Ministry of Home Affairs (MHA) is a ministry of the Government of India. An interior ministry, it is mainly responsible for the maintenance of internal security and domestic policy. Readers are advised to read annual report of the Ministry of Home Affairs. The Ministry of Home Affairs (MHA) has multifarious responsibilities, the important among them being-internal security, border management, CentreState relations, administration of Union Territories, management of Central Armed Police Forces, disaster management, etc.

**12. National Crime Records Bureau (NCRB):** NCRB shall endeavour to empower

Indian Police with Information Technology and Criminal Intelligence to enable them to effectively & efficiently enforce the law & improve public service delivery. This shall be achieved through coordination with police forces at National & International level, upgradation of crime analysis technology, developing IT capability & IT enabled solutions.

**13. Data Security Council of India (DSCI):** Data Security Council of India (DSCI) is a

premier industry body on data protection in India, setup by NASSCOM, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together national governments and their agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives. To further its objectives, DSCI engages with governments, regulators, industry associations and think tanks on policy matters. To strengthen thought leadership in cyber security and privacy, DSCI develops best practices and frameworks, publishes studies, surveys and papers. It builds capacity in security, privacy and cyber forensics through training and certification program for professionals and law enforcement agencies and engages stakeholders through various outreach initiatives including events, awards, chapters, consultations and membership programs. DSCI also endeavours to increase India's share in the global security product and services market through global trade development initiatives. These aim to strengthen the security and privacy culture in the India.

# GUIDELINES FOR SECURE PASSWORD, TWO STEP VERIFICATION AND USING FREE ANTIVIRUS

## 6.1 GENERATING SECURE PASSWORD

### 6.1.1 Guideline for setting secure Password<sup>10</sup>

Choosing the right password is something that many people find difficult, there are so many things that require passwords these days that remembering them all can be a real problem. Perhaps because of this a lot of people choose their passwords very badly. The simple tips below are intended to assist you in choosing a good password.

#### Basics

- ✓ Use at least eight characters, the more characters the better really, but most people will find anything more than about 15 characters difficult to remember.
- ✓ Use a random mixture of characters, upper and lower case, numbers, punctuation, spaces and symbols.
- ✓ Don't use a word found in a dictionary, English or foreign.
- ✓ Never use the same password twice.

#### Things to avoid

- ✓ Don't just add a single digit or symbol before or after a word. e.g. "apple1"
- ✓ Don't double up a single word. e.g. "appleapple"
- ✓ Don't simply reverse a word. e.g. "elppa"
- ✓ Don't just remove the vowels. e.g. "ppl"
- ✓ Key sequences that can easily be repeated. e.g. "qwerty", "asdf" etc.
- ✓ Don't just garble letters, e.g. converting e to 3, L or i to 1, o to 0. as in "z3r0-10v3"

#### Tips

- ✓ Choose a password that you can remember so that you don't need to keep looking it up, this reduces the chance of somebody discovering where you have written it down.
- ✓ Choose a password that you can type quickly, this reduces the chance of somebody discovering your password by looking over your shoulder.

#### Bad Passwords

---

<sup>10</sup> [http://www.lockdown.co.uk/?pg=password\\_guide](http://www.lockdown.co.uk/?pg=password_guide)

- ✓ Don't use passwords based on personal information such as: name, nickname, birthdate, wife's name, pet's name, friends name, home town, phone number, social security number, car registration number, address etc. This includes using just part of your name, or part of your birthdate.
- ✓ Don't use passwords based on things located near you. Passwords such as "computer", "monitor", "keyboard", "telephone", "printer", etc. are useless.
- ✓ Don't ever be tempted to use one of those oh so common passwords that are easy to remember but offer no security at all. e.g. "password", "letmein".
- ✓ Never use a password based on your username, account name, computer name or email address.

## **Choosing a password**

- ✓ Use good password generator software.
- ✓ Use the first letter of each word from a line of a song or poem.
- ✓ Alternate between one consonant and one or two vowels to produce nonsense words. eg. "taupouti".
- ✓ Choose two short words and concatenate them together with a punctuation or symbol character between the words. eg. "seat%tree"

## **Changing your password**

- ✓ You should change your password regularly, I suggest once a month is reasonable for most purposes.
- ✓ You should also change your password whenever you suspect that somebody knows it, or even that they may guess it, perhaps they stood behind you while you typed it in.
- ✓ Remember, don't re-use a password.

## **Protecting your password**

- ✓ Never store your password on your computer except in an encrypted form. Note that the password cache that comes with windows (.pwl files) is NOT secure, so whenever windows prompts you to "Save password" don't.
- ✓ Don't tell **anyone** your password, not even your system administrator
- ✓ Never send your password via email or other unsecured channel
- ✓ Yes, write your password down but don't leave the paper lying around, lock the paper away somewhere, preferably off-site and definitely under lock and key.
- ✓ Be very careful when entering your password with somebody else in the same room.

## **Remembering your password**

Remembering passwords is always difficult and because of this many people are tempted to write them down on bits of paper. As mentioned above this is a very bad idea. So what can you do?

- ✓ Use a secure password manager, see the downloads page for a list of a few that won't cost you anything.
- ✓ Use a text file encrypted with a strong encryption utility.
- ✓ Choose passwords that you find easier to remember.

## **Bad Examples**

- ✓ "fred8" - Based on the users name, also too short.
- ✓ "christine" - The name of the users girlfriend, easy to guess
- ✓ "kciredref" - The users name backwards
- ✓ "indescribable" - Listed in a dictionary
- ✓ "iNdesCribaBle" - Just adding random capitalisation doesn't make it safe.
- ✓ "gandalf" - Listed in word lists
- ✓ "zeolite" - Listed in a geological dictionary
- ✓ "qwertyuiop" - Listed in word lists
- ✓ "merde!" - Listed in a foreign language dictionary

## **Good Examples**

None of these good examples are actually good passwords, that's because they've been published here and everybody knows them now, always choose your own password don't just use somebody else's.

- ✓ "mItWdOtW4Me" - Monday is the worst day of the week for me.

## **How would a potential hacker get hold of my password anyway?**

There are four main techniques hackers can use to get hold of your password:

1. **Steal it.** That means looking over your shoulder when you type it, or finding the paper where you wrote it down. This is probably the most common way passwords are compromised, thus it's very important that if you do write your password down you keep the paper extremely safe. Also remember not to type in your password when somebody could be watching.
2. **Guess it.** It's amazing how many people use a password based on information that can easily be guessed. Psychologists say that most men use 4 letter obscenities as passwords and most women use the names of their boyfriends, husbands or children.
3. **A brute force attack.** This is where every possible combination of letters, numbers and symbols in an attempt to guess the password. While this is an extremely labour intensive task, with modern fast processors and software tools this method is not to be underestimated. A Pentium 100 PC might typically be able to try 200,000 combinations every second this would mean that a 6 character password containing just upper and lower case characters could be guessed in only 27½ hours.
4. **A dictionary attack.** A more intelligent method than the brute force attack described above is the dictionary attack. This is where the combinations tried are first chosen from words available in a dictionary. Software tools are readily available that can try every word in a dictionary or word list or both until your password is found. Dictionaries with hundreds of thousands of words, as well as specialist, technical and foreign language dictionaries are available, as are lists of thousands of words that are often used as passwords such as "qwerty", "abcdef" etc.

## 6.2 USING PASSWORD MANAGER<sup>11</sup>

We use passwords to ensure security and the confidentiality of our data. One of the biggest modern day crimes is identity theft, which is easily accomplished when passwords are compromised. The need of the hour is good password management. Have you ever thought of an alternative to remembering your passwords and not repeatedly entering your login credentials? Password managers are one of the best ways to store, back up and manage your passwords. A good password is hard to remember and that's where a password manager

---

<sup>11</sup> <http://opensourceforu.efytimes.com/2015/01/peek-top-password-managers/>

comes in handy. It encrypts all the different passwords that are saved with a master password, the only one you have to remember.

### **6.2.1 What is a password manager?**

A password manager is software that helps a user to manage passwords and important information so that it can be accessed any time and anywhere. An excellent password manager helps to store information securely without compromising safety. All the passwords are saved using some kind of encryption so that they become difficult for others to exploit.

### **6.2.2 Why you should use it?**

If you find it hard to remember passwords for every website and don't want to go through the 'Forgot password?' routine off and on, then a password manager is what you are looking for. These are designed to store all kinds of critical login information related to different websites.

### **6.2.3 How does it work?**

Password managers may be stored online or locally. Online password managers store information in an online cloud, which can be accessed any time from anywhere. Local password managers store information on the local server, which makes them less accessible. Both have their own advantages, and the manager you use would depend on your need.

Online password managers use browser extensions that keep data in a local profile, syncing with a cloud server. Some other password managers use removable media to save the password so that you can carry it with you and don't have to worry about online issues. Both these options can also be combined and used as two-factor authentication so that data is even more secure.

### **6.2.4 Some popular Password managers**

The passwords are saved using different encryptions based on the services that the companies provide. The best password managers use a 256-bit (or more) encryption protocol for better security, which has been accepted by the US National Security Agency for top secret information handling. If you have considered using a password manager and haven't decided on one, this section features the top five.

1. **KeePassX:** KeePassX is an open source, cross-platform and light weight password management application published under the terms of the GNU General Public License. It was built based on the Qt Libraries. KeePassX stores information about user names, passwords and other login information in a secure database. KeePassX uses its own random password generator, which makes it easier to create strong

passwords for better security. It also includes a powerful and quick search tool with which a keyword of a website can be used to find login credentials that have been stored in the database. It allows users to customise groups, making it more user friendly. KeePassX is not limited to storing only usernames and passwords but also free-form notes and any kind of confidential text files.

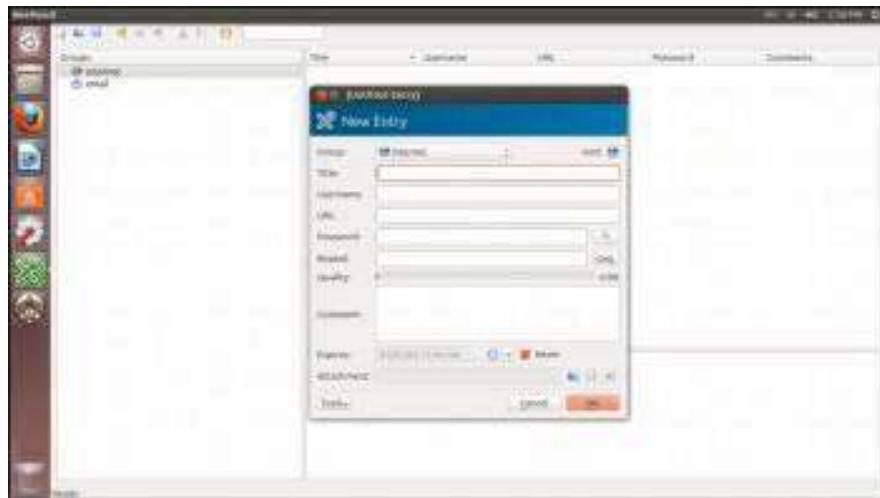


Figure 9: KeePassX

### Features

- *Simple user interface:* The left pane tree structure makes it easy to distinguish between different groups and entries, while the right pane shows more detailed information.
- *Portable media access:* Its portability makes it easy to use since there's no need to install it on every computer.
- *Search function:* Searches in the complete database or in every group.
- *Auto fill:* There's no need to type in the login credentials; the application does it whenever the Web page is loaded. This keeps it secure from key loggers.
- *Password generator:* This feature helps to generate strong passwords that make it difficult for dictionary attacks. It can be customised.
- *Two factor authentication:* It enables the user to either unlock the database by a master password or by a key from a removable drive.
- *Adds attachments:* Any type of confidential document can be added to the database as an attachment, which allows users to secure not just passwords.

- *Cross-platform support*: It works on all supported platforms. KeePassX is an open source application, so its source code can be compiled and used for any operating system.
  - *Security*: The password database is encrypted with either the AES encryption or the Twofish algorithm, which uses 256-bit key encryption.
  - *Expiration date*: The entries can be expired, based on a user defined date.
  - *Import and export of entries*: Entries: from PwManager or Kwallet can be imported, and entries can be exported as text files.
  - *Multi-language support*: It supports 15 languages.
2. **Clipperz**: Clipperz is a Web-based, open source password manager built to store login information securely. Data can be accessed from anywhere and from any device without any installation. Clipperz also includes an offline version when an Internet connection is not available.



Figure 10: Clipperz

## Features

- *Direct login*: Automatically logs in to any website without typing login credentials, with just one click.
- *Offline data*: With one click, an encrypted local copy of the data can be created as a HTML page.
- *No installation*: Since it's a Web-based application, it doesn't require any installation and can be accessed from any compatible browser.

- *Data import*: Login data can be imported from different supported password managers.
  - *Security*: The database is encrypted using JavaScript code on the browser and then sent to the website. It requires a passphrase to decrypt the database without which data cannot be accessed.
  - *Support*: Works on any operating system with a major browser that has JavaScript enabled.
3. Password Gorilla: Password Gorilla is an open source, cross-platform, simple password manager and personal vault that can store login information and notes. Password Gorilla is a Tcl/Tk application that runs on Linux, Windows and Mac OS X. Login information is stored in the database, which can be accessed only using a master password. The passwords are SHA256 protected and the database is encrypted using the Twofish algorithm. The key stretching feature makes it difficult for brute force attacks.



Figure 11: Password Gorilla

### Features

- *Portable*: Designed to run on a compatible computer without being installed.
- *Import of database*: Can import the password database saved in the CSV format.
- *Locks the database when idle*: It automatically locks the database when the computer is idle for a specific period of time.
- *Security*: It uses the Twofish algorithm to encrypt the database.
- *Can copy credentials*: Keyboard shortcuts can be used to copy login credentials to the clipboard.

- *Auto clear*: This feature clears the clipboard after a specified time.
  - *Organises groups*: Groups and sub-groups can be created to organise passwords for different websites.
4. **Gpassword Manager**: Gpassword Manager is a simple, lightweight and cross-platform utility for managing and accessing passwords. It is published under the terms of the Apache License. It allows users to securely store passwords/URLs in the database. The added entries can be marked as favourites, which then can be accessed by right-clicking the system tray icon. The passwords and other login information shown in the screen can be kept hidden based on user preferences.

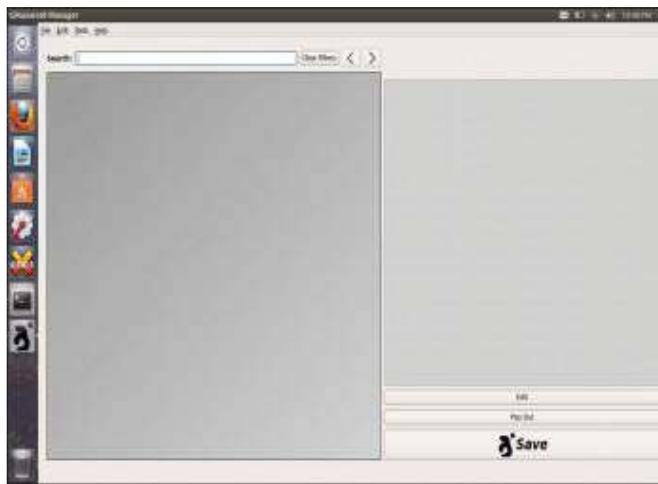


Figure 12: Gpassword manager

#### Features

- *Access to favourite sites*: A list of favourite Web pages can be accessed quickly from the convenient ‘tray’ icon.
  - *Quick fill*: Passwords and other information can be clicked and dragged onto forms for quick filling out.
  - *Search bar*: The quick search bar allows users to search passwords that are needed.
  - *Password generator*: Passwords with user-defined options can be generated with just a click.
  - *Quick launch*: Favourite websites can be launched by right-clicking the tray icon.
5. **Password Safe**: Password Safe is a simple and free open source application initiated by Bruce Schneier and released in 2002. Now Password Safe is hosted on

SourceForge and developed by a group of volunteers. It's well known for its ease of use. It is possible to organise passwords based on user preference, which makes it easy for the user to remember. The whole database backup and a recovery option are available for ease of use. Passwords are kept hidden, making it difficult for shoulder surfing. Password Safe is licensed under the Artistic licence.



Figure 13: Password Safe

### Features

- *Ease of use:* The GUI is very simple, enabling even a beginner to use it.
- *Multiple databases:* It supports multiple databases. And different databases can be created for each category.
- *Safe decryption:* The decryption of the password database is done in the RAM, which leaves no trace of the login details in the hard drive.
- *Password generator:* Supports the generation of strong, lengthy passwords.
- *Advanced search:* The advanced search function allows users to search within the different fields.
- *Security:* Uses the Twofish algorithm to encrypt the database.

## 6.3 ENABLING TWO-STEP VERIFICATION<sup>12</sup>

Every day, tens of thousands of personal accounts are hacked. Personal information is compromised, passwords are cracked, and lives are put in jeopardy. If you ever use one password for multiple accounts, you are exponentially increasing your vulnerability to being hacked. Thankfully, Google has launched its **2-step verification system**: anytime an unknown device is used to sign into your Google account, the user has to provide a verification code *in addition* to the password. So it's not enough for hackers to just get your password; they'll also need physical control of your phone or computer to access your account.

**Step 1:** Sign into your Gmail account. Click on a thumbnail of your avatar on the right side of the top menu bar, and then click "Account" to update your settings.

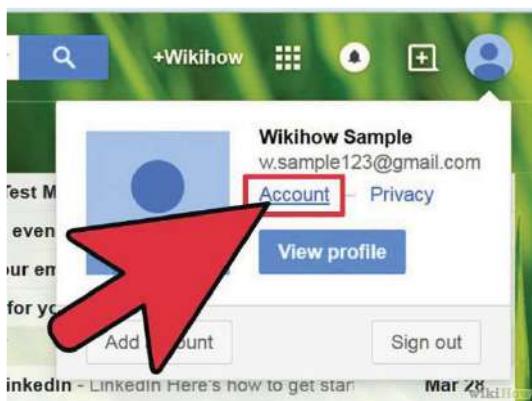


Figure 14: Account setting

**Step 2:** You will land on your Account Settings page. Scroll down until you find a blue bar that says "signing in".

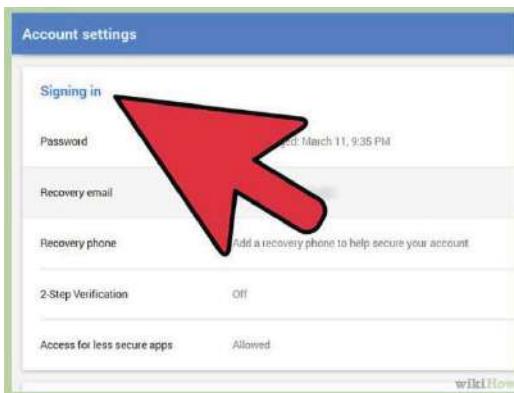


Figure 15: Signing in

<sup>12</sup> <http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License

**Step 3:** In the 2-step verification section, you'll see if you already have 2-step verification turned on. If it says "OFF," click "Edit" to set the feature up.

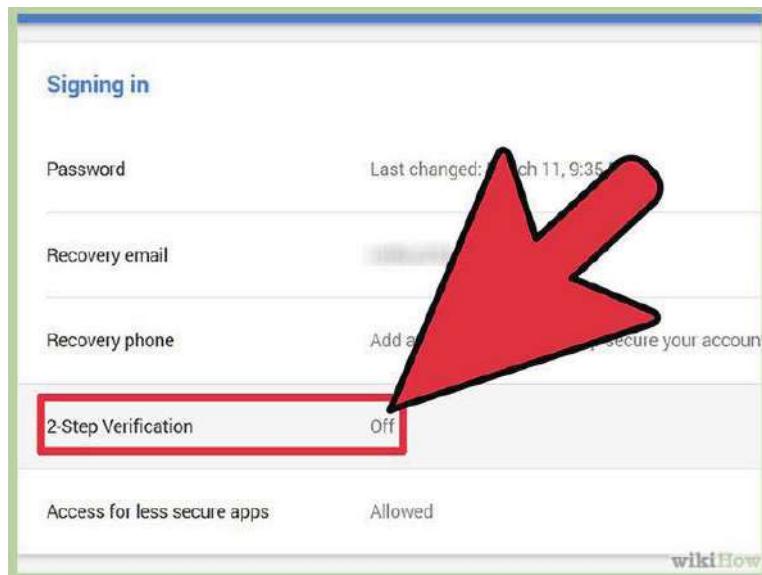


Figure 16: Turning on two steps verification<sup>13</sup>

**Step 4:** You'll see a page that briefly walks through the steps of setting up 2-step verification. Hover over the steps for more detail. Once you're ready, click "Start setup."

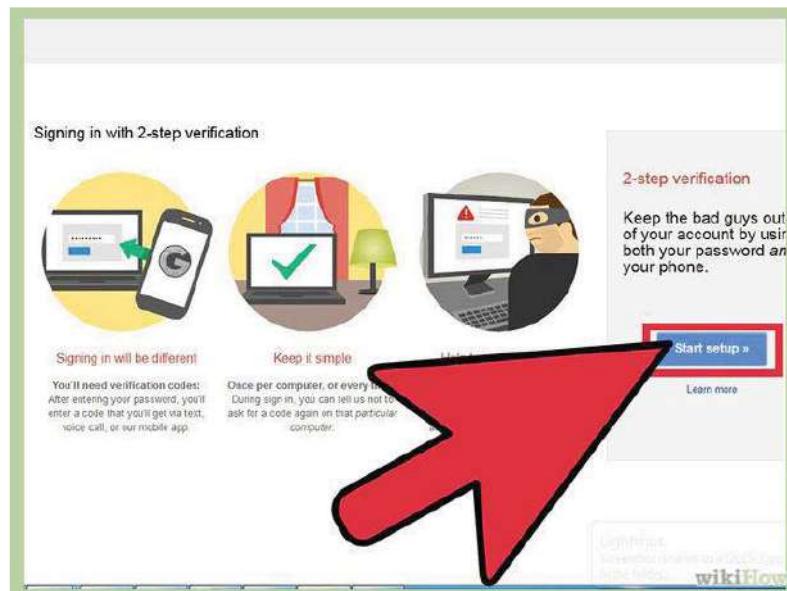


Figure 17: Start setup

**Step 5:** Type in your cell phone number. This will be the phone associated with your Google account. Anytime you sign into your Google account from an unknown device (e.g., a public

<sup>13</sup> Image courtesy: Figure 14 to 30 are adopted from <http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License.

computer), Google will send a verification code to your phone and you will need to enter that before you can sign in.

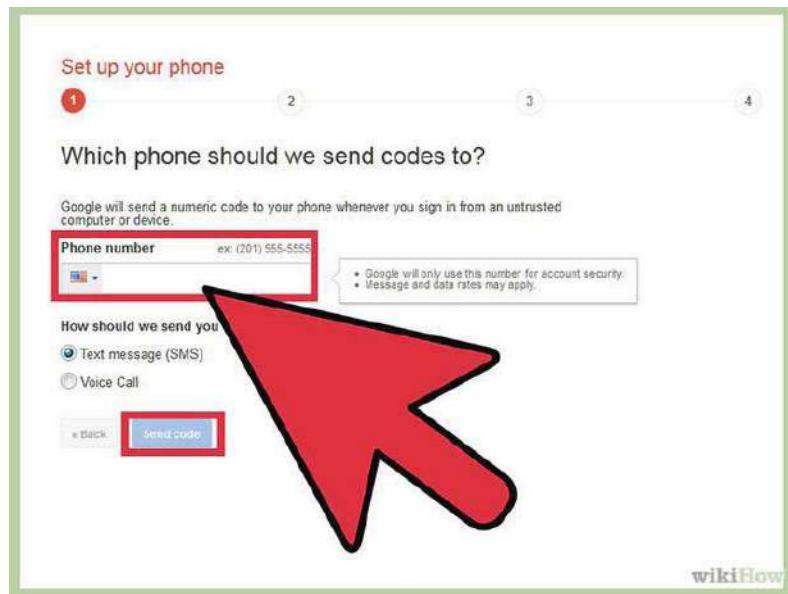


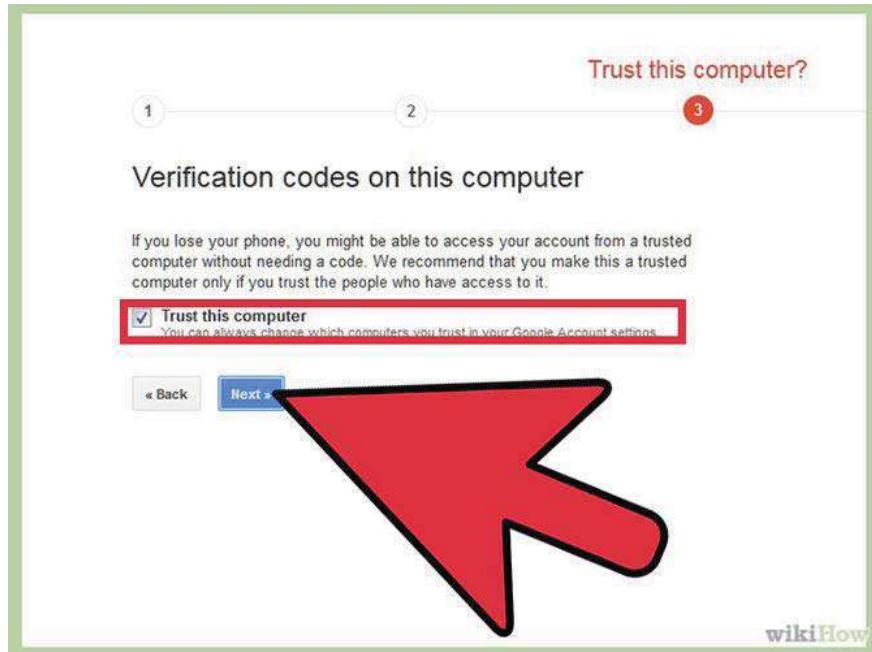
Figure 18: Entering mobile number for verification

**Step 6:** Select whether you'd like to receive a text message or Google Voice call with your verification code. Press submit. Then wait for the code to arrive to your phone and enter it in.



Figure 19: Entering varification code

**Step 7: Decide whether to trust this device.** If you are turning on 2-step verification from a personal computer or trusted device, check the "trust this device" box. You will only be asked to enter a verification code when you sign into this account once per 30 days.



*Figure 20: Setting up trust setting of the computer*

**Step 8:** Press OK, and you have just set up 2-step verification for your Google account! Skip any additional steps that seem unfamiliar or confusing for now -- we will address all of them in successive sections of this article.

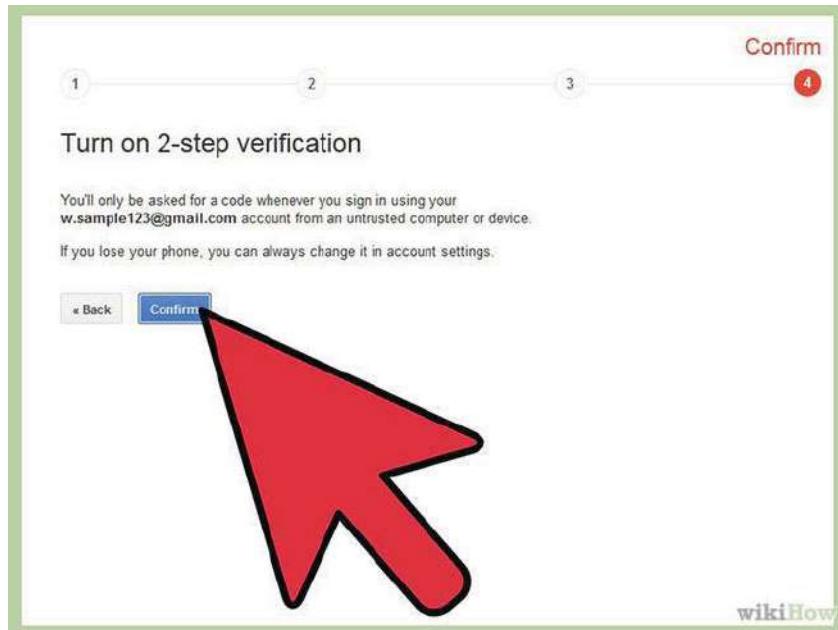


Figure 21: Confirmation

**Step 9:** Print a list of backup verification codes and store it in a secure but accessible place, like your wallet. If you ever need to sign into your Google account but don't have your primary phone with you, you can enter one of these codes instead.

- Go to your 2-step verification settings page.
- Under "How to receive codes," click on the "Show backup codes" link. Print this page.



Figure 22: Saving the page

### Method 1 of 2: Application-Specific Passwords

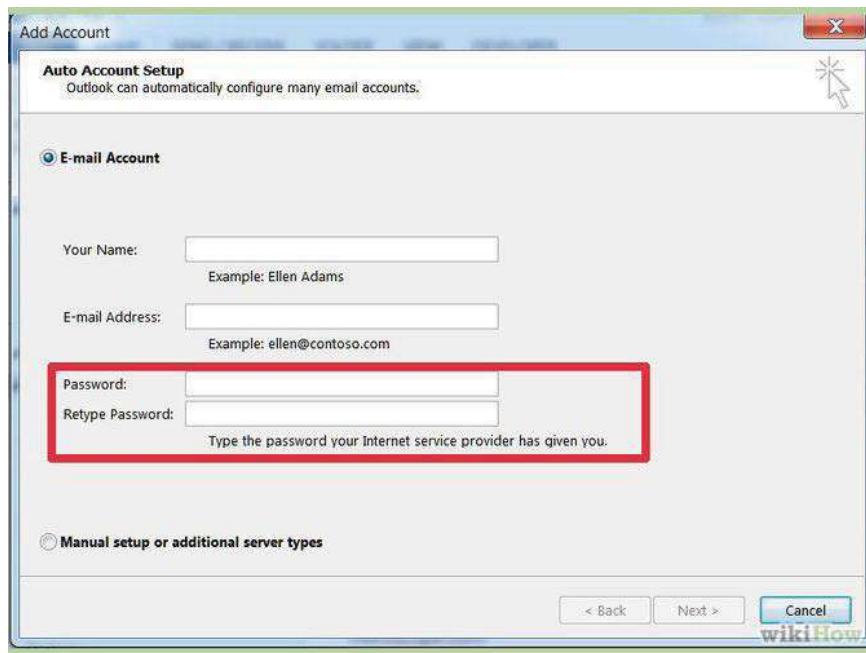


Figure 23: Setting up application specific password

**Step 1:** Understand the need for application-specific passwords. With 2-step verification, Google has you covered every time you sign into your account from a web browser. However, if you use your Google account with other applications, such as Microsoft Outlook or a mobile device's mail application, those systems cannot ask you for a verification code. Therefore, you will need to sign into those systems *once* with an application-specific password. You will only need to re-enter an application-specific password if you choose to reset it and generate a new one for that device.

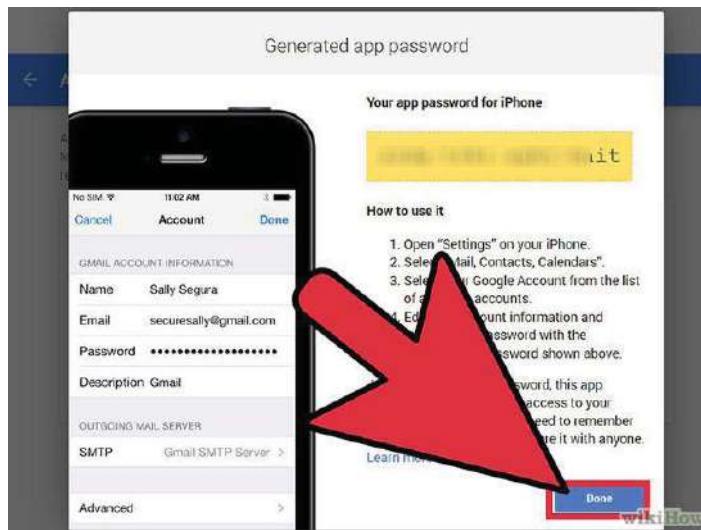


Figure 24: Generating app password

**Step 2:** Generate application-specific passwords for your devices. Go to your 2-step verification settings page or click "Edit" next to 2-step verification on the Security Account Settings page (steps 1-3 above). Scroll down and click on "Manage application-specific passwords."

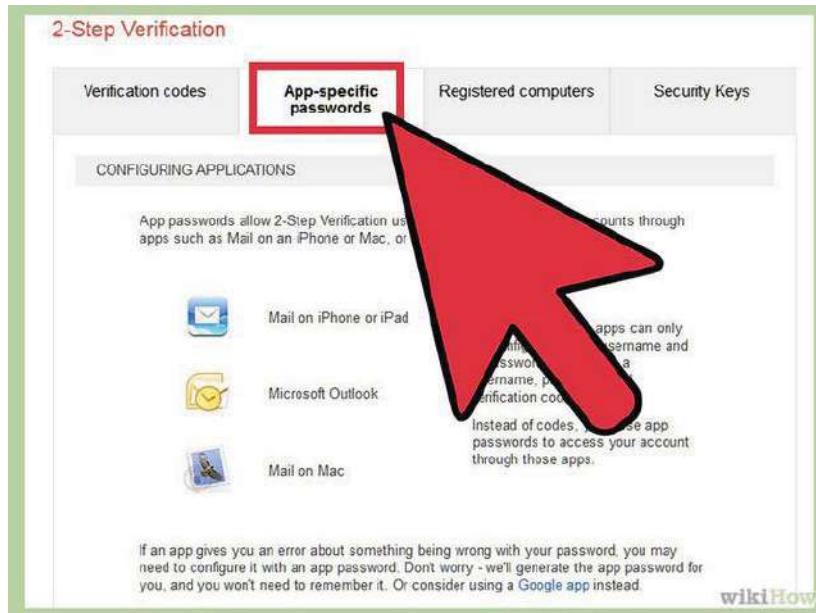


Figure 25: Managing application specific passwords

**Step 3:** At the top of the page, you will see a list of sites, applications and devices to which you have granted some level of access to your account. If you allowed a third-party website (e.g., LinkedIn, Twitter, Foursquare) to comb your Gmail Contacts to find friends, for example, you will see that listed. If you use other Google applications, you will also see those listed. Feel free to revoke access to any site or program you no longer wish to use.

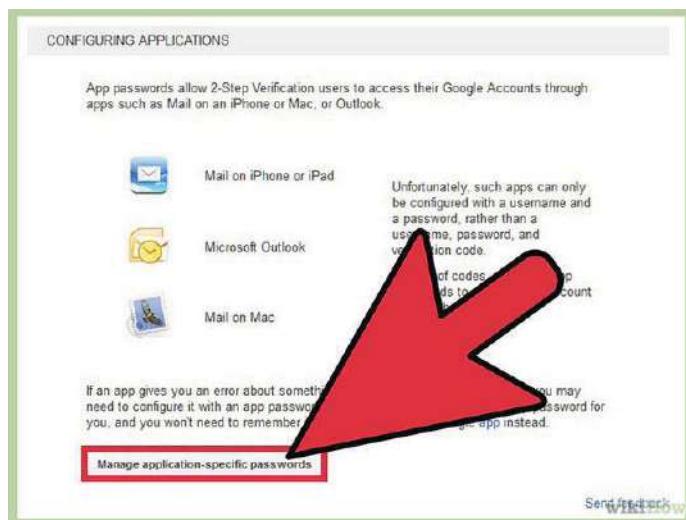


Figure 26: Configuring applications

**Step 4:** Scroll down to the field at the bottom for entering the name of a device. Enter in something that will help you remember what this application-specific password is for -- e.g., Mail App on iPhone, Google App on iPhone, Chrome Sync, Outlook, Thunderbird, or whatever describes your application. Click "Generate password". You should generate a new application-specific password for *each* application.



Figure 27: Generating app password

**Step 5:** Open up the application. Go to the settings page where you enter in your Google Account information. Type in your Google account name as usual. Now instead of your account password, type in the application-specific password in the password field. You have now granted this application full access to your Google account. You will only need to enter this password once. There is no need to write it down or memorize it, and it will not be displayed by Google again.



Figure 28: Testing the password

**Step 6:** Click "Done" on your web browser once you have successfully entered the application-specific password.

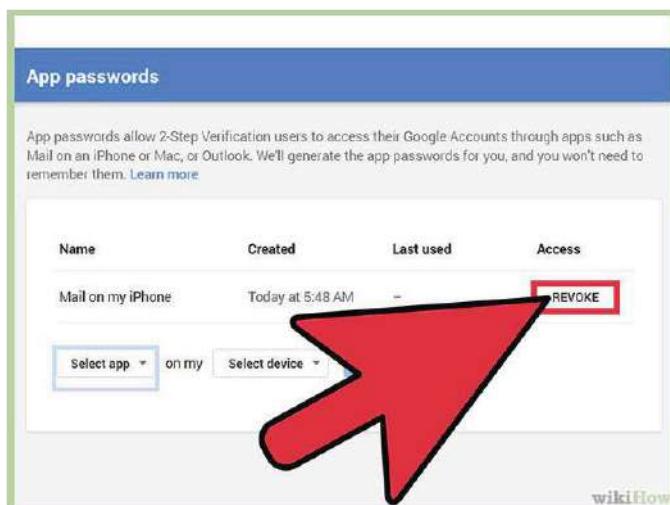


Figure 29: Revoke the password

**Step 7:** Know how to revoke an app's access to your Gmail account. If you don't want to use an app anymore, or you lost your phone and want to stop anyone who has it from accessing your Gmail, simply click on the "Revoke" button in your application-specific password settings page.

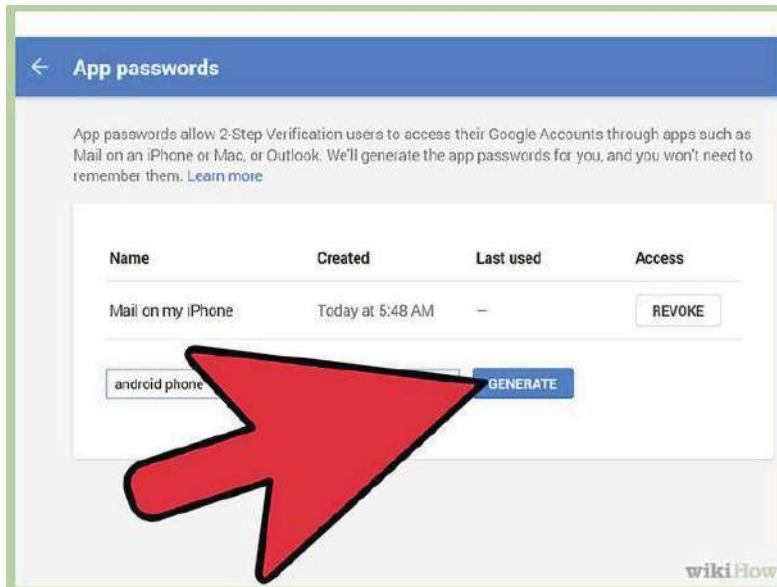


Figure 30: Generating password for android phone

**Step 8:** Create new application-specific passwords for *each* application that you connect your Google Account to! This means if you sync your Google Account to two mail apps and a chat client, you should have *three* application-specific passwords.

### Method 2 of 2: If You Lose Your Phone

If you lose your phone and have 2-step verification turned on, you *can* still access your Gmail account. You also can and should follow these steps to stop strangers from gaining access to your Google accounts.

**Step 1:** Revoke your current application-specific passwords. If you have a smartphone with apps linked to your Google account, they will automatically be signed out. When you get a new phone, you can generate new application-specific passwords (see previous section) and enter them into your new devices.

**Step 2:** Change your Gmail password. Even if someone else has your verification code, they can't get into your Gmail account without your new password. While it's unlikely that the person who has your phone also has cracked your Gmail password, you can never be too sure. If you are logged into Google from any web browser on your mobile device, you'll now also automatically be signed out.

**Step 3:** Add a backup phone number if you have a second mobile device. Go to your 2-step verification settings page and click "Add a phone number" in the "Backup phones" section.

**Step 4:** If you don't have a backup phone, use your list of printable backup codes to access your account. On your 2-step verification settings page, click "Show backup codes". If you haven't done so already, print out this page and keep it in a safe but accessible place -- such as your wallet.

**Step 5:** If you get phone and change your phone number, be sure to revoke access to your previous number on the 2-step verification settings page.

## 6.4 SECURING COMPUTER USING FREE ANTIVIRUS<sup>14</sup>

As computers become more and more integrated in to our lives, we end up leaving many sensitive data on our computer-from passwords, official email id, bank account to personal notes, business plans and other confidential information. So, good security software is a must for everyone. Here is a list of 11 free anti-virus software and its common features which you can select (home users) for your online security. All are listed in alphabetical order

**1. Avast Antivirus**– Avast is one of the best free anti-virus software available that provides a complete protection against security threats. This full-featured antivirus package has the following feature: Built in Anti-spyware, Anti-Rootkit, Web shield, Strong self protection, P2P and IM shield, Anti-Virus kernel, resident protection, Network shield, Automatic update, System integration, Windows 64 bit support, Integrated Virus Cleaner. It can be downloaded from <https://www.avast.com/index>

**2. AVG Antivirus** – AVG anti-virus free edition provides basic antivirus and anti-spyware protection for Windows. Following features included in the free edition: Anti-virus , anti-spyware and Safe surf feature. It can be downloaded from <http://free.avg.com/>

**3. Avira AntiVir Personal** - Avira is a comprehensive, easy to use antivirus program, designed to reliable free of charge virus protection to home-users. Features included are: Protection from virus worms and Trojans, Anti-rootkit, Anti-fishing, Anti dialers. It can be downloaded from <http://www.free-av.com/>

**4. BitDefender** - Free Edition uses the same ICSA Labs certified scanning engines found in Pro version of BitDefender , allowing you to enjoy basic virus protection for no cost at all. Features includes: On demand Virus Scanner and Remover and Scheduled scanning. It can be downloaded from <http://www.bitdefender.com/PRODUCT-14-en--BitDefender-Free-Edition.html>

---

<sup>14</sup> [http://shaifulaueo.blogspot.in/p/free-antivirus\\_13.html](http://shaifulaueo.blogspot.in/p/free-antivirus_13.html)

**5. Blink Personal** – An all-in one security suite with antivirus limited for one year. Blink personal Security suite features – Antivirus and Anti spyware, Anti root kit, Built-in Firewall protection and Identity protection. It can be downloaded from <http://free-antivirus.eeye.com/>

**6. Calmwin antivirus**–An open source, free Antivirus program for Windows 98/Me/2000/XP/2003 and Vista. Features include - high detection rates for viruses and spyware; automatic downloads of regularly updated Virus Database, Standalone virus scanner. It does not include an on-access real-time scanner. It can be downloaded from <http://www.calmwin.com/>

**7. Comodo Antivirus** - has all the functionality of a paid AV without the price – Features includes- Detects and remove viruses from computers and networks. On Access Scanning conducts a real-time, scheduled virus scan. Host Intrusion Detection allows you to Intercept viruses, spyware, and other malware before they infect your computer. Get updates of the latest virus definitions everyday so you can stay protected against the latest threats. It can be downloaded from <http://antivirus.comodo.com/>

**8. Moon Secure Antivirus** - Aims to be the best Free Antivirus for Windows under GPL license. It offers multiple scan engines, Net shield, Firewall, On access, on Exec scanner and rootkits preventions plus features from Commercial Antivirus applications. It can be downloaded from <http://sourceforge.net/projects/moonav/>

**9. PCTools Antivirus**- with PC Tools AntiVirus Free Edition you are protected against the most nefarious cyber-threats attempting to gain access to your PC and personal information. It protects you from Virus, worm, Trojan and has Smart Updates, IntelliGuard Protection, file guard and email guard. It can be downloaded from <http://www.pctools.com/free-antivirus/>

**10. Rising Antivirus** – Rising Antivirus Free Edition is a solution with no cost to personal users for the life of the product while still provides the same level of detection and protection capability as RISING Antivirus . It protects your computers against all types of viruses, Trojans, worms, rootkits and other malicious programs. Ease of use and Smartupdate technology make it an "install and forget" product and entitles you to focus on your own jobs with your computer. It can be downloaded from <http://www.freerav.com/>

**11. Threatfire Lite** – Provides Comprehensive protection against viruses, worms, Trojans, spyware, rootkits, keyloggers & buffer overflows. And have Real-time behavior-based malware detection, malware quarantine & removal, etc. It can be downloaded from <http://www.threatfire.com/download/>

## **ACTIVITY**

1. Compare the feature of some of the popular free antivirus.
2. What is the difference between free antivirus and paid antivirus? Is it safe to use free antivirus in your machine?
3. Use the guidelines to for generating secure passwords and evaluate whether your current passwords can be considered as safe or unsafe passwords.
4. Based on the above guidelines, change your unsafe passwords to safe ones.
5. Find out some popular password managers and evaluate them based on their characteristics'.
6. Based on the above comparison, choose one of the best password managers for yourself.
7. Create two step verification for your Gmail account.
8. Find out how many sites, other than Gmail provide two steps verification.

## **RECOMENDED VIDEOS**

<https://www.youtube.com/watch?v=WprjZyY8ZuY>

<https://www.youtube.com/watch?v=mYhJyVKjai4>

<https://www.youtube.com/watch?v=MFyPg2Flf8s>

<https://www.youtube.com/watch?v=iNWUtj9qhPo>

<https://www.youtube.com/watch?v=A9O0zYv-5d0>

[https://www.youtube.com/watch?v=cdRbvO\\_MXh4](https://www.youtube.com/watch?v=cdRbvO_MXh4)

[https://youtu.be/Xhmae4\\_fG2o](https://youtu.be/Xhmae4_fG2o)

<https://youtu.be/COU5T-Wafa4>

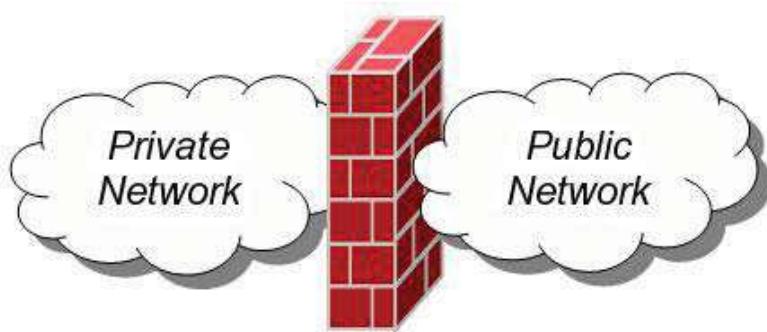
<https://youtu.be/cUH3tQbGj4A>

<https://youtu.be/hYyWgPXfx9U>

## 7.1 CONFIGURING FIREWALL ON MAC COMPUTER<sup>15</sup>

Every Mac ships with a built-in firewall - a service that can be configured to disallow information from entering your Mac. But what is a firewall, and why do you need to use it on your Mac?

Every time you request information from the Internet, such as a web page or email message, your Mac sends data packets to request the information. Servers receive the packets, and then send other packets back to your Mac. This all happens in a matter of seconds. Once your Mac has reassembled the packets, you'll see something, like an email message or web page.



*Figure 31: Firewall*

A firewall can help prevent bad packets from entering your Mac. Hackers love to run automated applications that can scan thousands of computers (including your Mac) for open ports that can be exploited. To ensure that random individuals do not gain unauthorized access to your Mac, you should enable Mac OS X's built-in firewall. It will close your Mac's open ports and disallow random network scans.

### 7.1.1 Turning on and Configuring the Mac OS X Firewall

Here's how to turn on and configure your Mac's built-in firewall:

1. From the Apple menu, select **System Preferences**. The window shown below appears.

---

<sup>15</sup> Content and image courtesy(figure 31 to 35): <http://www.macinstruct.com/node/165> available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License



Figure 32: System preference dashboard

2. Select **Security & Privacy**.
3. Click the **Firewall** tab.
4. Click the lock icon and authenticate with your administrator username and password.

The window shown below appears.

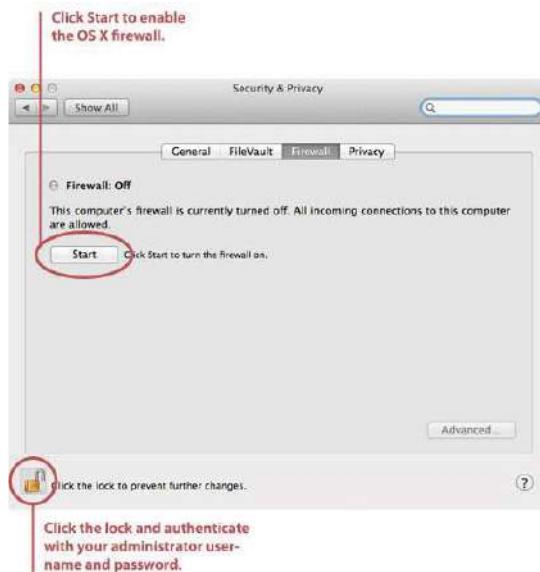


Figure 33: Security and privacy dashboard

5. Click **Start**. The firewall turns on - you'll know it's enabled when you see the green light and the **Firewall: On** message, as shown below.



Figure 34: Turning on firewall

6. Click **Advanced**. The window shown below appears.

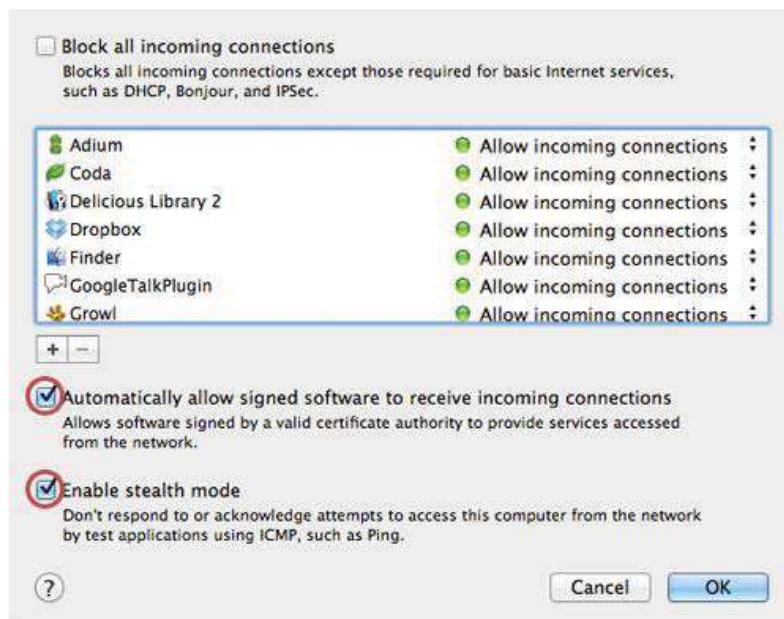


Figure 35: Configuring firewall

7. Select the **Automatically allow signed software to receive incoming connections** checkbox. This allows the applications on your Mac to communicate with the outside world.
8. Select the **Enable stealth mode** checkbox. This prevents your Mac from responding to port scans and ping requests.
9. Click **OK** to close the *Advanced* settings.
10. Close System Preferences. Your Mac is now protected by the built-in firewall!

## 7.2 WORKING WITH WINDOWS FIREWALL IN WINDOWS7<sup>16</sup>

### 7.2.1 Firewall in Windows 7

Windows 7 comes with two firewalls that work together. One is the **Windows Firewall**, and the other is **Windows Firewall with Advanced Security (WFAS)**. The main difference between them is the complexity of the rules configuration. Windows Firewall uses simple rules that directly relate to a program or a service. The rules in WFAS can be configured based on protocols, ports, addresses and authentication. By default, both firewalls come with predefined set of rules that allow us to utilize network resources. This includes things like browsing the web, receiving e-mails, etc. Other standard firewall exceptions are File and Printer Sharing, Network Discovery, Performance Logs and Alerts, Remote Administration, Windows Remote Management, Remote Assistance, Remote Desktop, Windows Media Player, Windows Media Player Network Sharing Service.

With firewall in Windows 7 we can configure inbound and outbound rules. By default, all outbound traffic is allowed, and inbound responses to that traffic are also allowed. Inbound traffic initiated from external sources is automatically blocked.

Sometimes we will see a notification about a blocked program which is trying to access network resources. In that case we will be able to add an exception to our firewall in order to allow traffic from the program in the future.

Windows 7 comes with some new features when it comes to firewall. For example, "full-stealth" feature blocks other computers from performing operating system fingerprinting. OS fingerprinting is a malicious technique used to determine the operating system running on the host machine. Another feature is "boot-time filtering". This features ensures that the firewall is working at the same time when the network interface becomes active, which was not the case in previous versions of Windows.

When we first connect to some network, we are prompted to select a network location. This feature is known as Network Location Awareness (NLA). This feature enables us to assign a network profile to the connection based on the location. Different network profiles contain different collections of firewall rules. In Windows 7, different network profiles can be

---

<sup>16</sup> Contents and image courtesy( Figure 31 o 43):<http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advanced-security> available under Creative Commons Attribution-Noncommercial-Share Alike 4.0 International.

configured on different interfaces. For example, our wired interface can have different profile than our wireless interface. There are three different network profiles available:

- Public
- Home/Work - private network
- Domain - used within a domain

We choose those locations when we connect to a network. We can always change the location in the Network and Sharing Center, in Control Panel. The Domain profile can be automatically assigned by the NLA service when we log on to an Active Directory domain. Note that we must have administrative rights in order to configure firewall in Windows 7.

### 7.2.2 Configuring Windows Firewall

To open Windows Firewall we can go to **Start > Control Panel > Windows Firewall**.

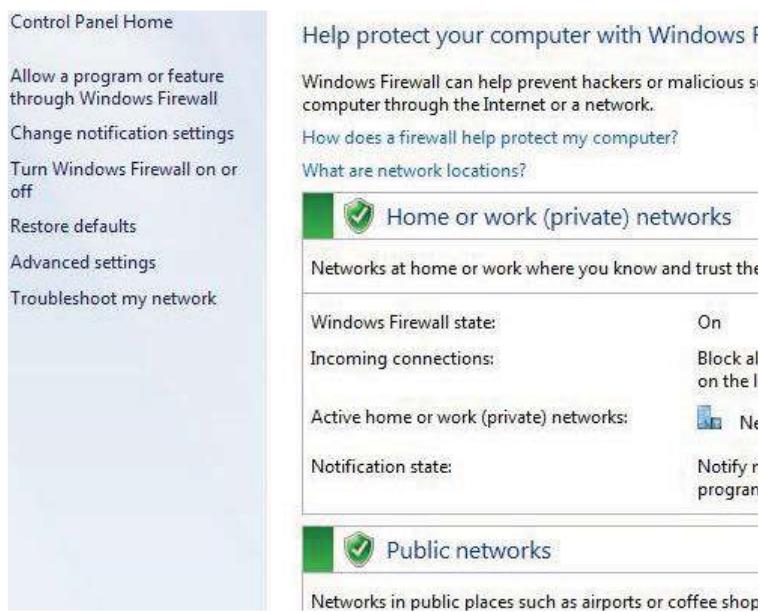


Figure 36: Control panel dashboard on Windows machine

By default, Windows Firewall is enabled for both private (home or work) and public networks. It is also configured to block all connections to programs that are not on the list of allowed programs. To configure exceptions we can go to the menu on the left and select "Allow a program or feature through Windows Firewall" option.

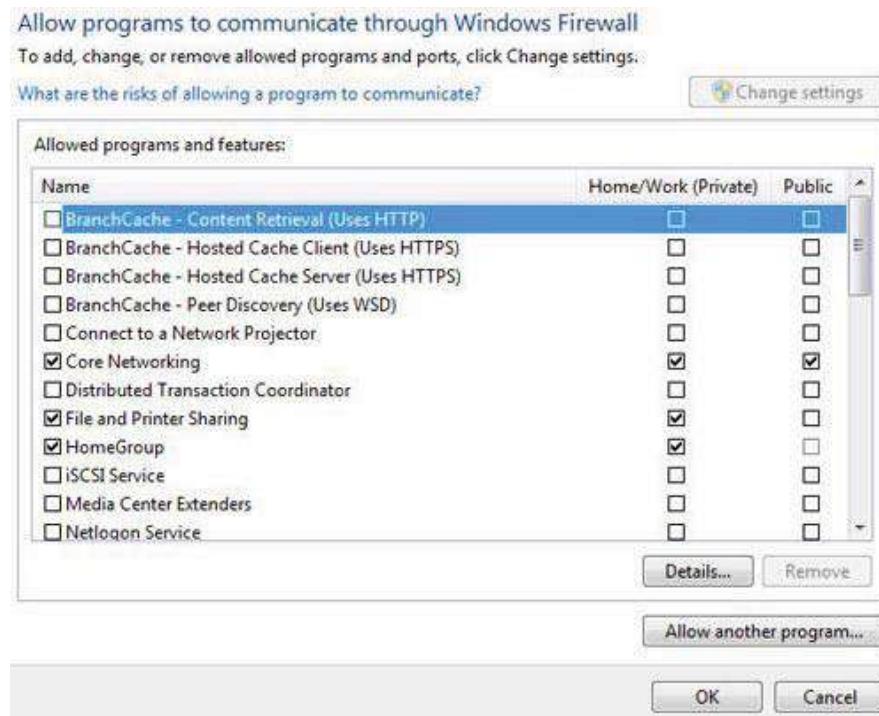


Figure 37: Configuring firewall setting

## Exceptions

To change settings in this window we have to click the "Change settings" button. As you can see, here we have a list of predefined programs and features that can be allowed to communicate on private or public networks. For example, notice that the Core Networking feature is allowed on both private and public networks, while the File and Printer Sharing is only allowed on private networks. We can also see the details of the items in the list by selecting it and then clicking the Details button.

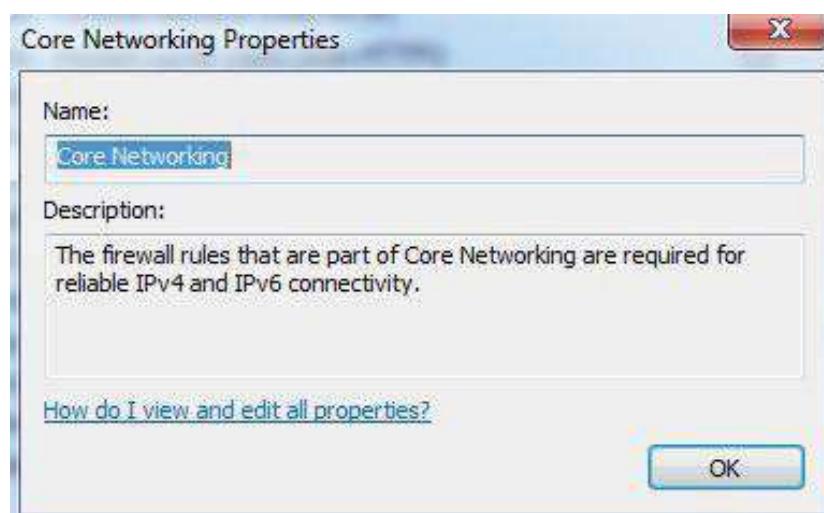


Figure 38: Setting exceptions

## Details

If we have a program on our computer that is not in this list, we can manually add it by clicking on the "Allow another program" button.



Figure 39: Selecting programs not present in the list

## Add a Program

Here we have to browse to the executable of our program and then click the Add button. Notice that we can also choose location types on which this program will be allowed to communicate by clicking on the "Network location types" button.



Figure 40: Adding a program

## Network Locations

Many applications will automatically configure proper exceptions in Windows Firewall when we run them. For example, if we enable streaming from Media Player, it will automatically configure firewall settings to allow streaming. The same thing is if we enable Remote Desktop feature from the system properties window. By enabling Remote Desktop feature we actually create an exception in Windows Firewall.

Windows Firewall can be turned off completely. To do that we can select the "Turn Windows Firewall on or off" option from the menu on the left.

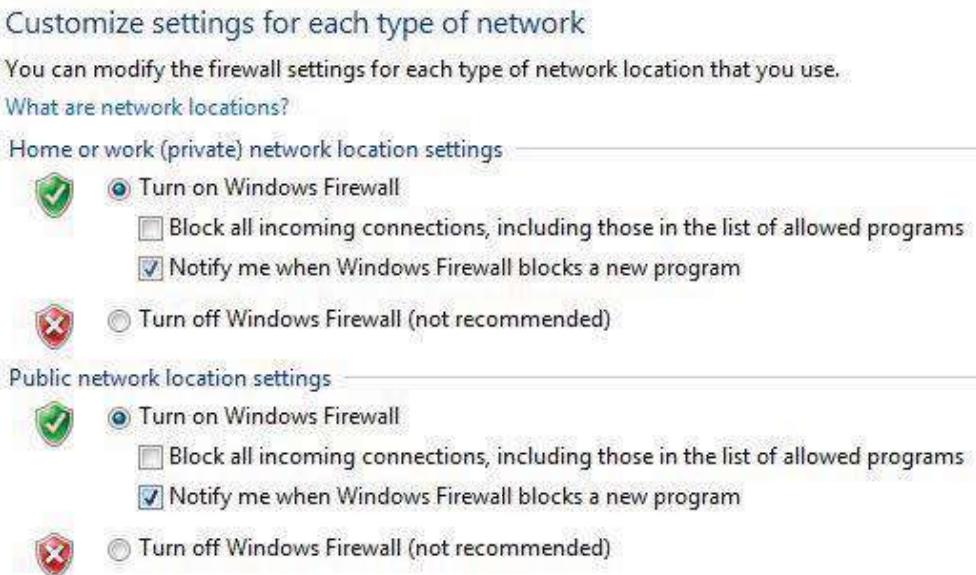


Figure 41: Customize settings

## Firewall Customization

Note that we can modify settings for each type of network location (private or public). Interesting thing here is that we can block all incoming connections, including those in the list of allowed programs.

Windows Firewall is actually a Windows service. As you know, services can be stopped and started. If the Windows Firewall service is stopped, the Windows Firewall will not work.

Service Name	Description	Status	Startup Type
Windows Event Log	This service ...	Started	Automatic
Windows Firewall	Windows Fi...	Started	Automatic
Windows Font Cache S...	Optimizes p...	Started	Automatic (D...)
Windows Image Acquisi...	Provides im...		Manual

Figure 42: Enabling firewall from Windows services

## Firewall Service

In our case the service is running. If we stop it, we will get a warning that we should turn on our Windows Firewall.



Figure 43: Firewall notification

## Warning

Remember that with Windows Firewall we can only configure basic firewall settings, and this is enough for most day-to-day users. However, we can't configure exceptions based on ports in Windows Firewall any more. For that we have to use Windows Firewall with Advanced Security, which will be covered in next section.

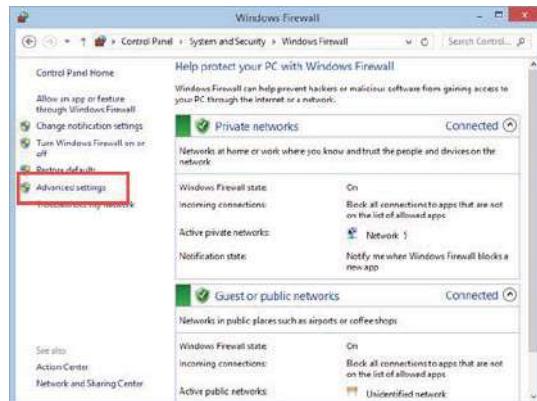
### 7.2.3 How to Start & Use the Windows Firewall with Advanced Security<sup>17</sup>

The *Windows Firewall with Advanced Security* is a tool which gives you detailed control over the rules that are applied by the *Windows Firewall*. You can view all the rules that are used by the *Windows Firewall*, change their properties, create new rules or disable existing ones. In this tutorial we will share how to open the *Windows Firewall with Advanced Security*, how to find your way around it and talk about the types of rules that are available and what kind of traffic they filter.

#### 7.2.3.1 How to Access the Windows Firewall with Advanced Security

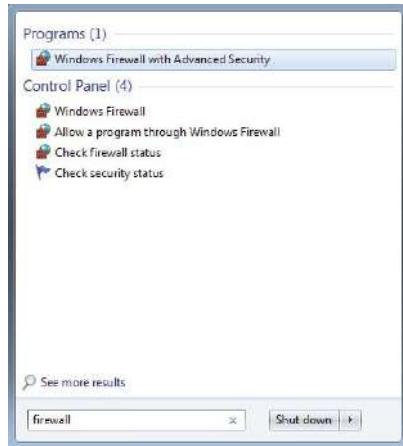
You have several alternatives to opening the *Windows Firewall with Advanced Security*:

One is to open the standard Windows Firewall window, by going to "*Control Panel -> System and Security -> Windows Firewall*". Then, click or tap *Advanced settings*.



<sup>17</sup> <http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advanced-security>

In Windows 7, another method is to search for the word *firewall* in the *Start Menu* search box and click the "*Windows Firewall with Advanced Security*" result.



In Windows 8.1, *Windows Firewall with Advanced Security* is not returned in search results and you need to use the first method shared above for opening it.

The *Windows Firewall with Advanced Security* looks and works the same both in Windows 7 and Windows 8.1. To continue our tutorial, we will use screenshots that were made in Windows 8.1.



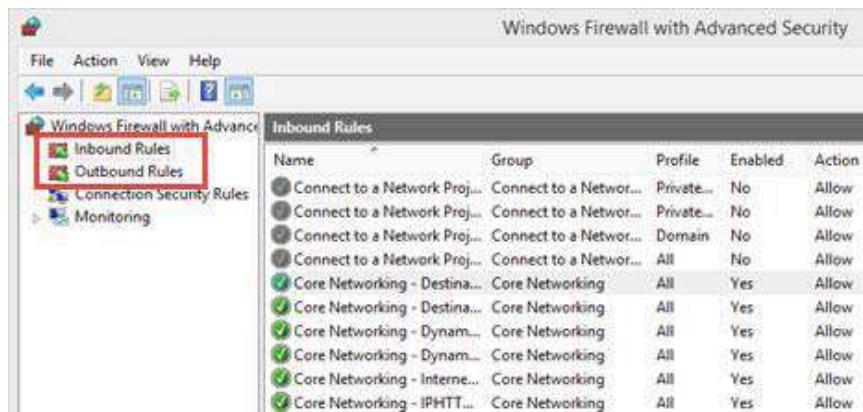
### 7.2.3.2 What Are The Inbound & Outbound Rules?

In order to provide the security you need, the *Windows Firewall* has a standard set of inbound and outbound rules, which are enabled depending on the location of the network you are

connected to. Inbound rules are applied to the traffic that is coming from the network and the Internet to your computer or device. Outbound rules apply to the traffic from your computer to the network or the Internet.

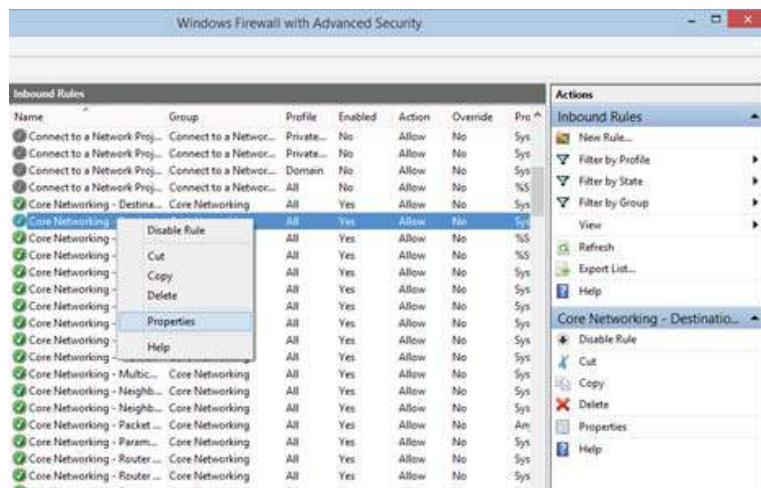
These rules can be configured so that they are specific to: computers, users, programs, services, ports or protocols. You can also specify to which type of network adapter (e.g. wireless, cable, virtual private network) or user profile it is applied to.

In the *Windows Firewall with Advanced Security*, you can access all rules and edit their properties. All you have to do is click or tap the appropriate section in the left-side panel.

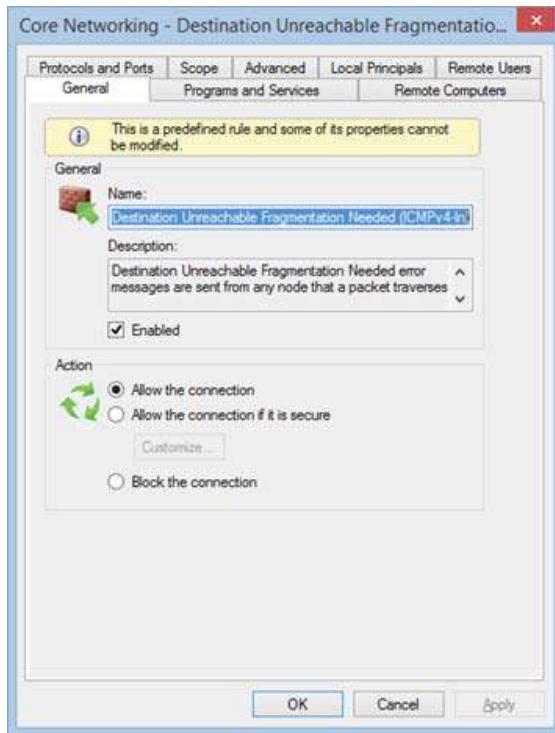


The rules used by the *Windows Firewall* can be enabled or disabled. The ones which are enabled or active are marked with a green check-box in the *Name* column. The ones that are disabled are marked with a gray check-box.

If you want to know more about a specific rule and learn its properties, right click on it and select *Properties* or select it and press *Properties* in the column on right, which lists the actions that are available for your selection.



In the *Properties* window, you will find complete information about the selected rule, what it does and in when it is applied. You will also be able to edit its properties and change any of the available parameters.



#### 7.2.3.3 What Are The Connection Security Rules?

Connection security rules are used to secure traffic between two computers while it crosses the network. One example would be a rule which defines that connections between two specific computers must be encrypted.

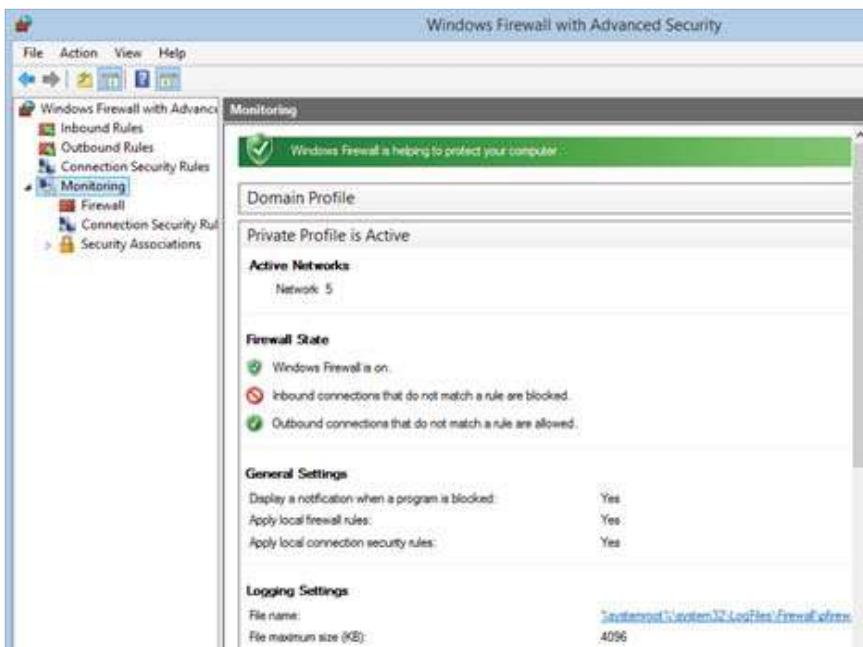
Unlike the inbound or outbound rules, which are applied only to one computer, connection security rules require that both computers have the same rules defined and enabled.

If you want to see if there are any such rules on your computer, click or tap "*Connection Security Rules*" on the panel on the left. By default, there are no such rules defined on Windows computers and devices. They are generally used in business environments and such rules are set by the network administrator.



#### **7.2.3.4 What Does the Windows Firewall with Advanced Security Monitor?**

The *Windows Firewall with Advanced Security* includes some monitoring features as well. In the *Monitoring* section you can find the following information: the firewall rules that are active (both inbound and outbound), the connection security rules that are active and whether there are any active security associations.



You should note that the *Monitoring* section shows only the active rules for the current network location. If there are rules which get enabled for other network locations, you will not see them in this section.

The above section discussed on how to setup a firewall on two Operating Systems viz. Windows and Mac. Linux have many variants therefore it is not possible to discuss how to configure firewall on Linux. There are some links in the Recommended Videos section which discuss the procedure of setting up firewall in various variant of Linux.

#### **Activity**

1. Setup and configure a firewall in your system.
2. Find some some of the free and commercially available firewalls over internet.

#### **RECOMENDED VIDEOS**

<https://www.youtube.com/watch?v=krbivwp4t3U>

<https://www.youtube.com/watch?v=H0g8xJMnT68>

**For linux**

<https://www.youtube.com/watch?v=hkzHtEnFZpc>

[https://www.youtube.com/watch?v=o0a09CQi\\_48](https://www.youtube.com/watch?v=o0a09CQi_48)

<https://www.youtube.com/watch?v=wbzP2-qvc4o>

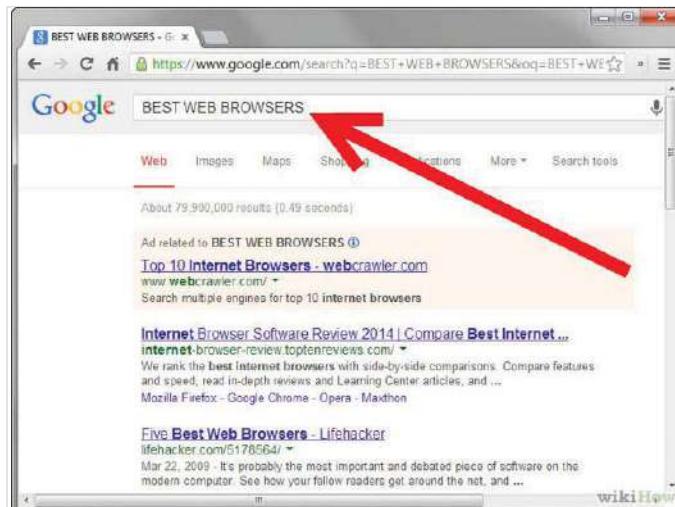
# CHOOSING BEST BROWSER TO SUIT YOUR REQUIREMENTS

## 8.1 FINDING THE BEST BROWSER ACCORDING TO THE USERS REQUIREMENT<sup>18</sup>

Browsers are the key to the Internet these days, at least for most tasks. There are many, many browsers for every platform and operating system, so the choice can be tough. However, this should help narrow the search.

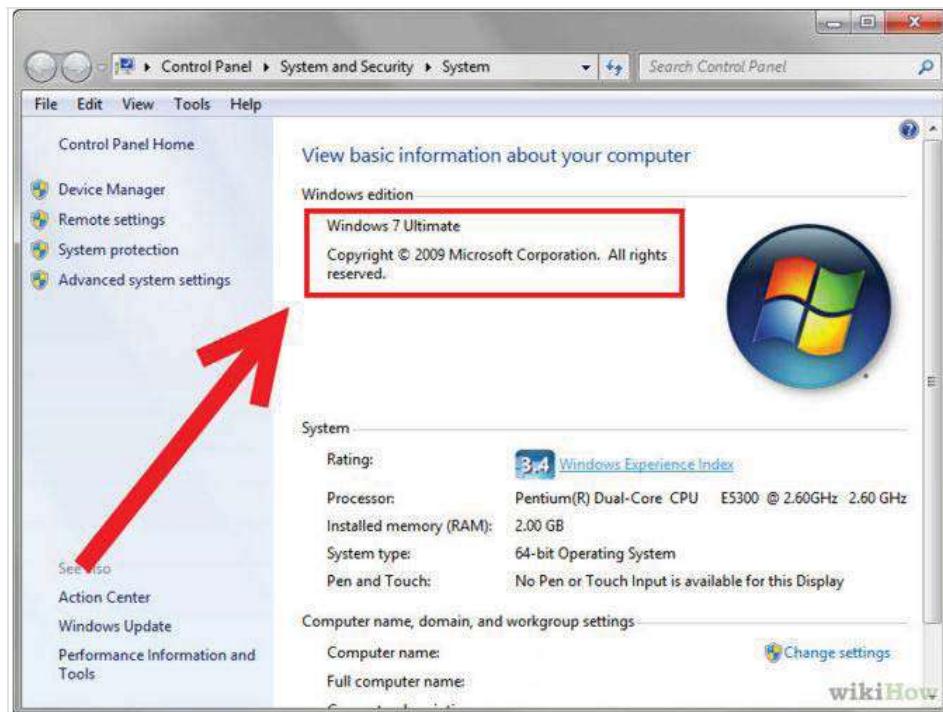


**Step 1:** Determine the age of your computer. How old is your computer? Is it a mobile device? Know your systems specifications as this may be more suited to some browsers than others.

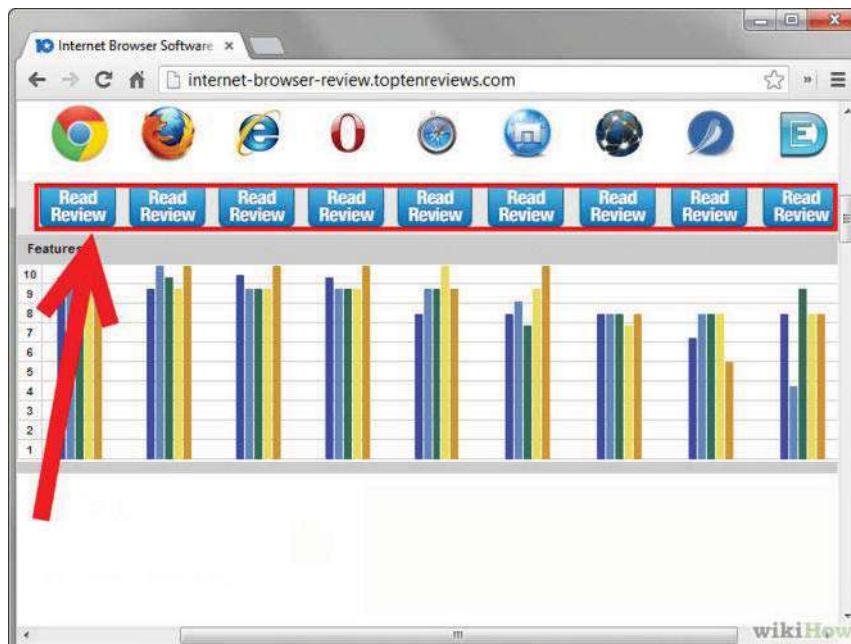


<sup>18</sup> <http://www.wikihow.com/Choose-an-Internet-Browser>

**Step 2:** Think about your ideal browser; what would it be able to do? You may want it to be quite simple, handling only the bare necessities. You may want some basic features like web feed reading, bookmarking (favorites), or search boxes. Some browsers have a lot more, and that's where it starts to get confusing.



**Step 3:** Make sure you know what platform you are on. Some browsers are only available to a certain operating system, or not available to one operating system.



**Step 4:** Research browsers. Tabbed browsers include Safari (runs on OS X, iPhone and is new to Windows), Firefox (general purpose with the most plug-ins), Opera(supports torrents, handles e-mail and runs on mobile devices), Konqueror (dual purpose file manager), Seamonkey (includes HTML editor and e-mail client), Off By One (tiny) and Flock (social networking).

The screenshot shows a comparison chart titled "Internet Browser Software" from [internet-browser-review.toptenreviews.com](http://internet-browser-review.toptenreviews.com). The chart compares seven browsers: Chrome, Firefox, Internet Explorer, Opera, Konqueror, Mozilla, and Flock. It includes a legend for speed ratings (10-9 Excellent, 8-6 Good, 5-4 Average, 3-2 Poor, 1-0 Bad) and a "Print/Email" button. The "Features" section is highlighted with a red arrow pointing to it.

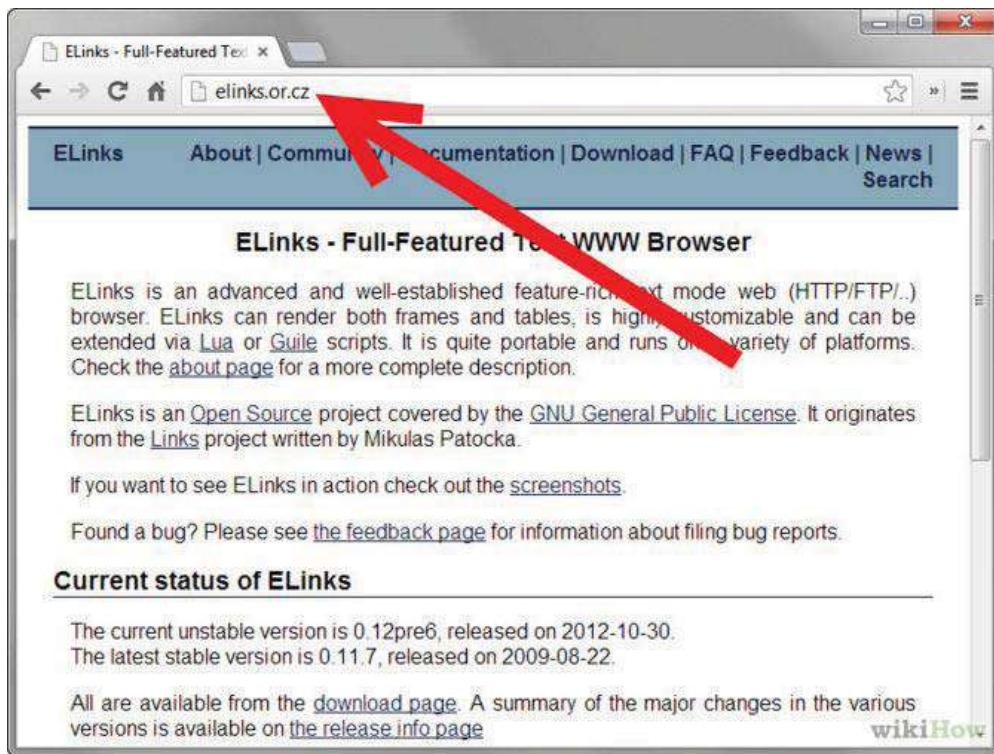
	Chrome	Firefox	Internet Explorer	Opera	Konqueror	Mozilla	Flock
Initial Startup Time	4	6.3	4.3	5.1	4.2	8	9
Average Startup	4.3	6.3	4	4.4	3.7	6.9	4
Navigation Time	4.4	5.7	4.5	4.8	3.8	3.2	11
Features	✓	✓	✓	✓	✓	✓	✓
Tabbed Browsing	✓	✓	✓	✓	✓	✓	✓
Add-ons	✓	✓	✓	✓	✓	✓	✓
Integrated Search Engine	✓	✓	✓	✓	✓	✓	✓
Save Tabs	✓	✓	✓	✓	✓	✓	✓
Customization Options	✓	✓	✓	✓	✓	✓	✓
Bookmarks	✓	✓	✓	✓	✓	✓	✓
RSS Feeds	✓	✓	✓	✓	✓	✓	✓
Zoom	✓	✓	✓	✓	✓	✓	✓
Find-On Page Function	✓	✓	✓	✓	✓	✓	✓
Password Manager	✓	✓	✓	✓	✓	✓	✓
Autofill	✓	✓	✓	✓	✓	✓	✓
Automatic Updates	✓	✓	✓	✓	✓	✓	✓

**Step 5:** See the features of all browsers you have found, and compare with what you want.

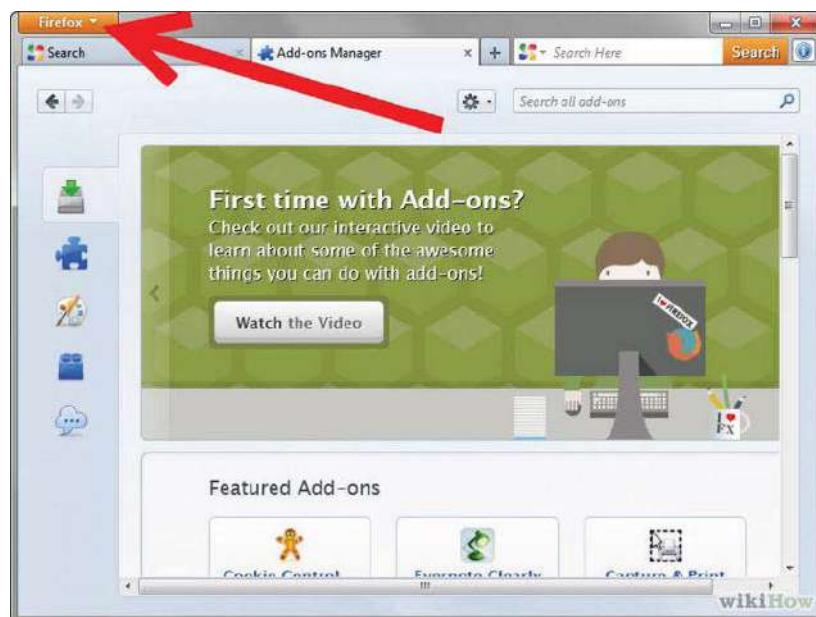
The screenshot shows the homepage of the Off By One Web Browser at [offbyone.com/offbyone/](http://offbyone.com/offbyone/). The page features a banner with the text "Yes, Another Free Web Browser". The left sidebar contains links like Home, Overview, FAQ, Help, Download, and Search. The main content area has a heading "The Browser Has Landed" and text about the browser's features, including its compatibility with Windows 95-XP and its tabbed browsing interface. A sidebar on the right offers a download link for "Free PC Software".

**Step 6:** Consider alternative lower-memory browsers, if you have low computer memory.

Consider Off by One, Dillo, SkipStone and NetSurf.



**Step 7:** Consider a text-based browser, if you want an even faster-than-fast(maximum speed/hyperdrive) experience. Consider ELinks.



**Step 8:** Find out if you can add features you may want or if there is an easy method to doing so such as an existing plugin or extension in the case of Firefox.



**Step 9:** Download and install your new browser!

### Activity

1. Compare the various browsers based on their characteristics'.

### RECOMMENDED VIDEOS:

<https://www.youtube.com/watch?v=sr7mgYD2tAc>

<https://www.youtube.com/watch?v=-jHs-RYD7gc>

<https://www.youtube.com/watch?v=gNiz4kfSZnw>

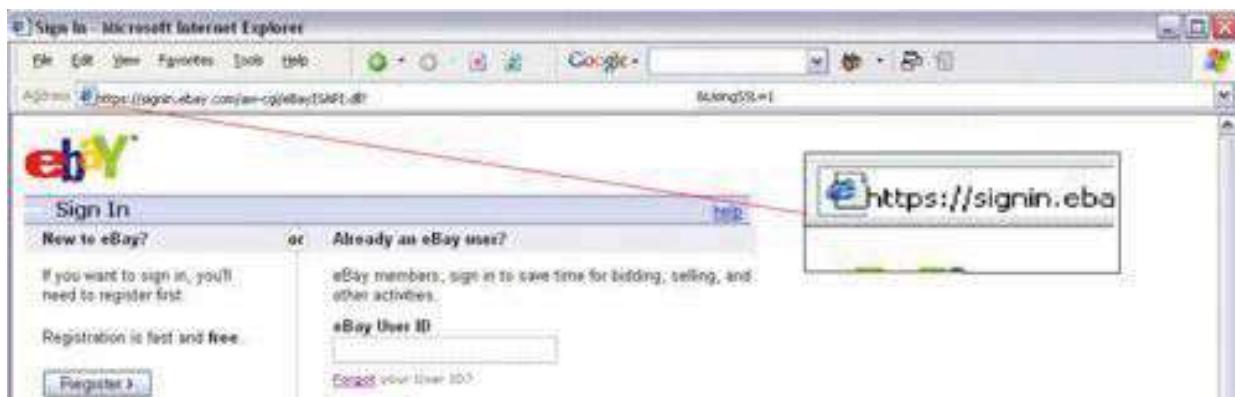
# GUIDELINES FOR SAFE INTERNET BROWSING

## 9.1 SAFE BROWSING

Internet security is a matter of great concern for internet users. It is important to **know if a website is secure** or not while surfing the internet<sup>19</sup>. A **secure website** creates a safe connection between the website and the web browser so that entered data, such as personal information, credit card details, banking information, etc, is not accessible to unauthorized entities. When the browser opens a secured connection, "https" can be seen in the URL instead of just http. To **know if a website is secure** or not, look for the locked yellow colour padlock symbol on the lower right corner of the browser window.

### 9.1.1 How do I know if a website is secure?

Some web sites use a secure connection between the web site and your browser. This may be important to you, for instance, if you want to pay online for a product or a service and have to enter credit card information or other personal information. To know if your browser is viewing a secure web site, you can look in the lower right part of the window. There is a small box in the frame of the window to the left of the area that describes which zone you are in (usually the Internet zone, with a globe icon). If you see a yellow padlock icon, the web site you are viewing is a "secure web site." If the box is empty, the web site does not have a secure connection with your browser.



<sup>19</sup> <http://ccm.net/faq/2-how-do-i-know-if-a-website-is-secure>

## **9.2 TIPS FOR BUYING ONLINE<sup>20</sup>**

Shopping online can be cheaper and more convenient for you and for businesses. However, make sure you understand your rights and the risks before you shop online or bid in an online auction.

**I. Pay securely:** Don't make any payment unless:

- You are on a secure website, and
- You can make a secure payment.

This will protect you against fraud and unauthorised credit card transactions. A secure website address will always:

- begin with 'https://', not 'http://'
- display the image of a closed padlock (usually in the bottom right corner of your browser window).

**Only make a payment if you can see both of these things.** Never give out your bank account details, credit card number or other personal details if you are not certain that the business is a reputable trader.

**II. Know the business:** Only buy from websites you know and trust. Check that the company has a physical street address and landline phone number. If the company operates from overseas, you might have trouble getting a refund or repair.

**III. Know the product:** Make sure you check whether:

- the product is legal
- the product will work in Australia
- any warranties or guarantees offered are valid in Australia
- the product has an authorised repairer nearby.

**IV. Check the contract:** Make sure you read and understand:

- the terms and conditions of sale
- the refund policy
- the delivery details
- returns and repairs policies, including any associated costs.

**V. Check the full cost:** Be aware of the full cost of your purchase. Additional costs may include:

- currency conversion
- taxes

---

<sup>20</sup> <https://www.qld.gov.au/law/your-rights/consumer-rights-complaints-and-scams/consumer-advice-rights-and-responsibilities/tips-to-become-a-smarter-shopper/tips-for-buying-online/>

- postage and delivery fees
- packaging.

It might end up being cheaper to buy the product at a local shop.

VI. **Protect your privacy:** Only buy online if you are comfortable with a business's privacy policy. Do not give out information unless they require it to complete the sale. Remember, if a deal sounds too good to be true, it probably is.

VII. **Keep records:** Always write down any reference numbers and print out copies of:

- the order form (both before and after you confirm the order)
- receipts (can come by email or in a pop-up window).

Always make sure all charges are correct by checking the receipt against your:

- credit card statement
- merchant account statement (such as PayPal)
- bank statement.

The charges may be converted from another currency.

VIII. **Online auction sites:** Most online auction sites (like eBay) offer a dispute resolution process for buyers and sellers. This should be your first step to resolve a dispute if:

- you did not receive the items you bought
- you did not receive payment for items you sold
- you received items that were significantly different from their description.

The eBay website has an example of this facility.

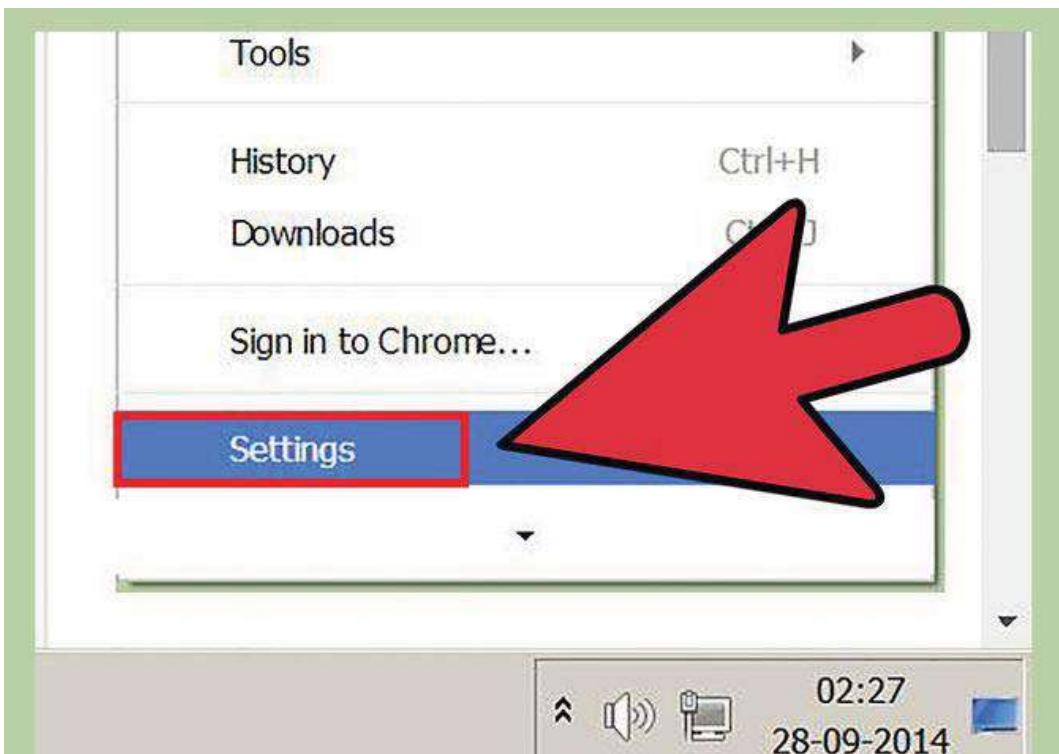
## 9.3 CLEARING CACHE FOR BROWSERS

Your internet browser's cache stores certain information (snapshots) of webpages you visit on your computer or mobile device so that they'll load more quickly upon future visits and while navigating through websites that use the same images on multiple pages so that you do not download the same image multiple times<sup>21</sup>. Occasionally, however your cache can prevent you from seeing updated content, or cause functional problems when stored content conflicts with live content. You can fix many browser problems simply by clearing your cache. This article contains instructions with screenshots on how to clear the cache for all major browsers.

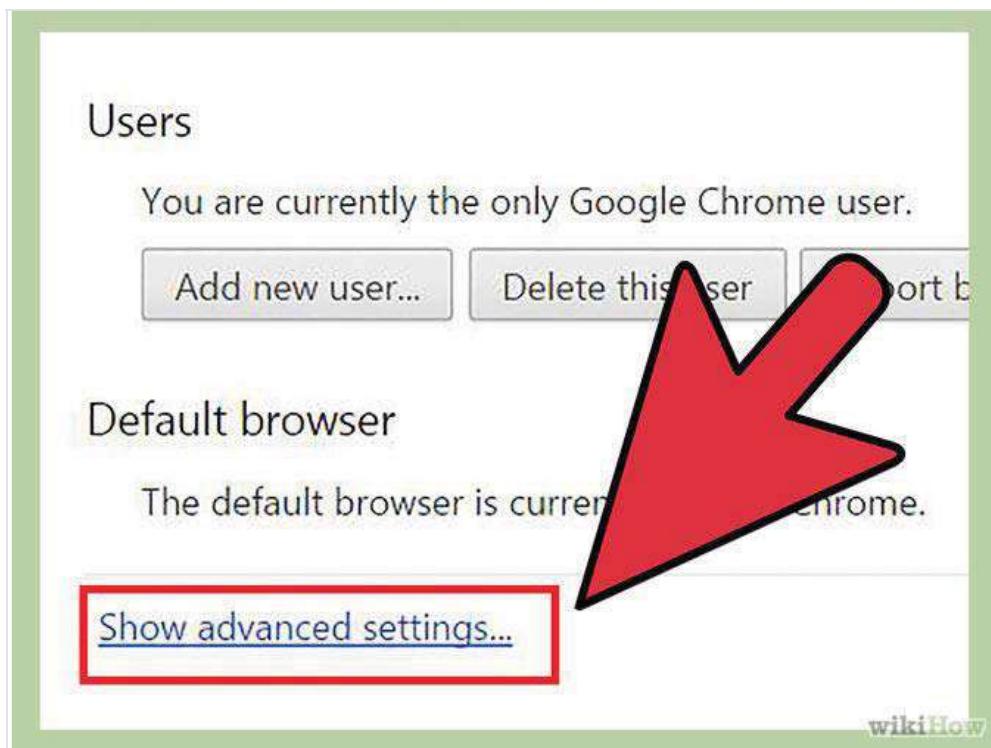
### 9.3.1 Clearing cache for Chrome Browsers above version 10

---

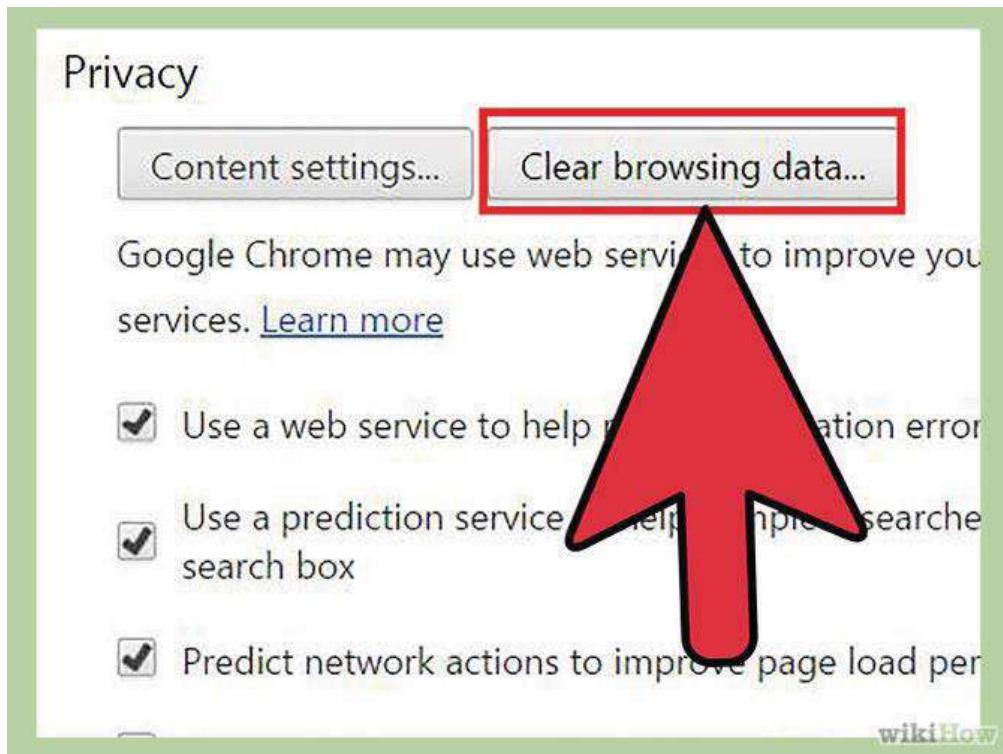
<sup>21</sup> <http://www.wikihow.com/Clear-Your-Browser%27s-Cache>



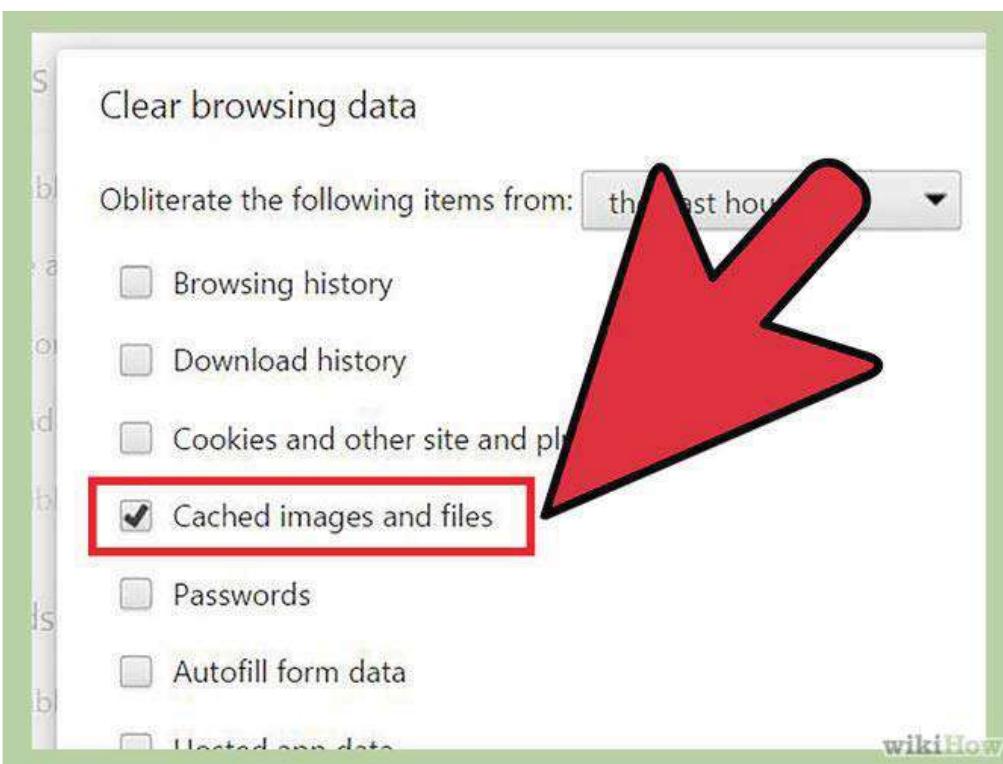
**Step 1:** Open the settings on Chrome. Click the menu icon in the upper right corner of the browser to the right. Click settings on the bottom of the menu.



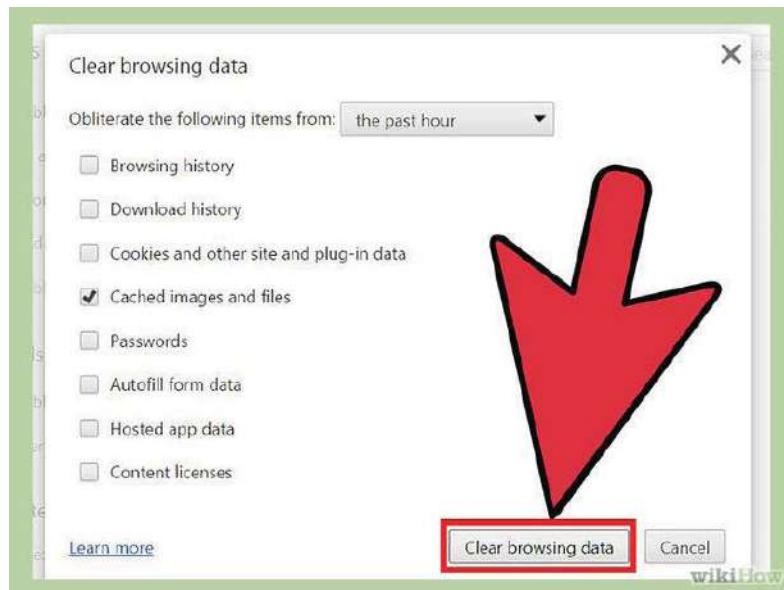
**Step 2:** From settings, click "Show advanced settings. It's located at the very bottom of the settings section.



**Step 3:** Scroll to the privacy section and click "Clear browsing data."

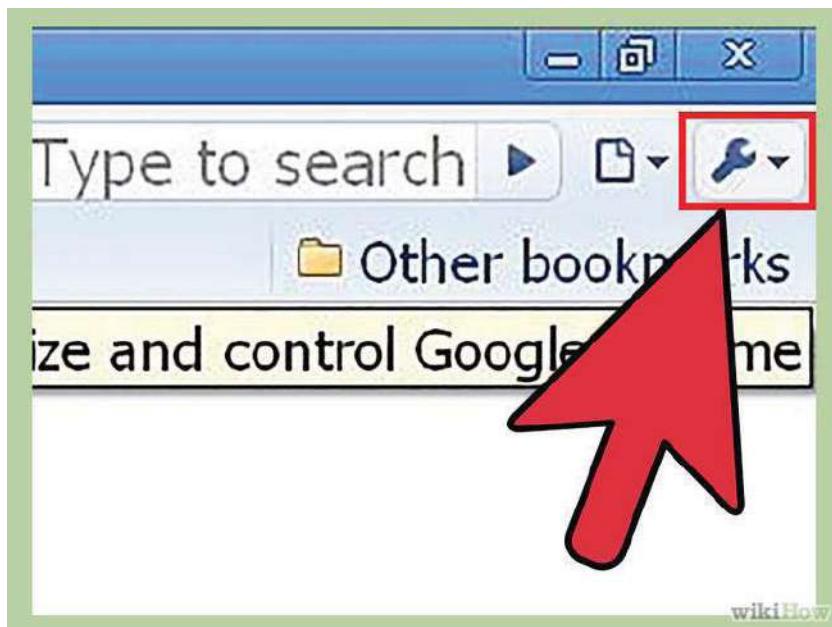


**Step 4:** Select "Cached images and files". Uncheck all other options to avoid deleting browser history, cookies and other things you may wish to retain. Change "Obliterate the following items from" to "the beginning of time".

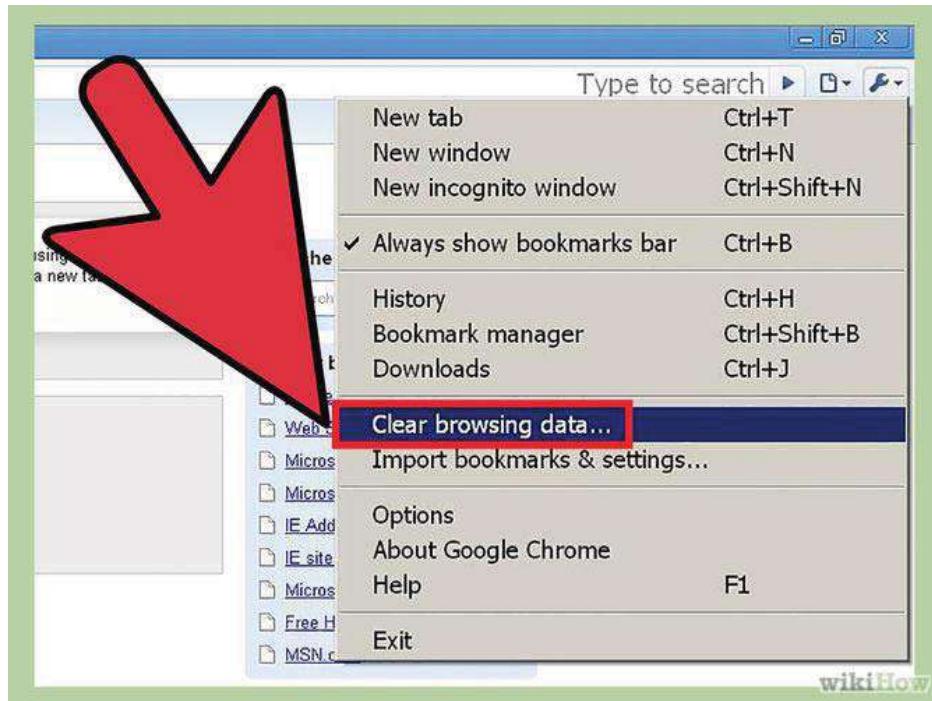


**Step 5:** Press "Clear browsing data". You are done!

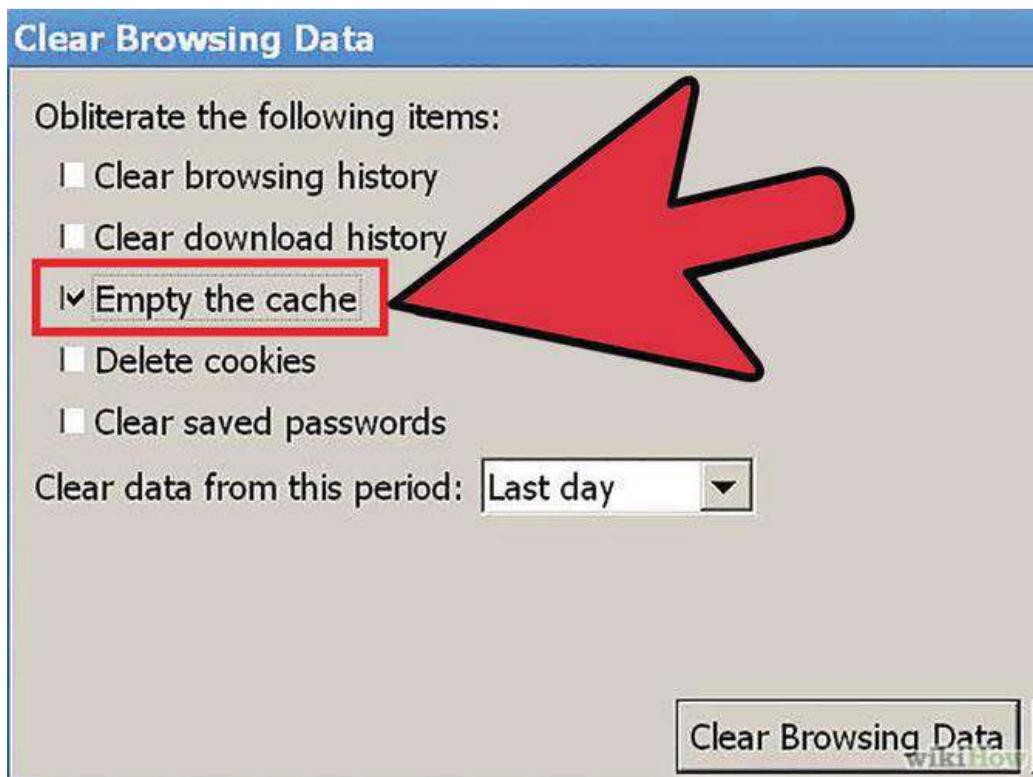
### 9.3.2 Clearing cache for Chrome Browsers from version 1 to 9



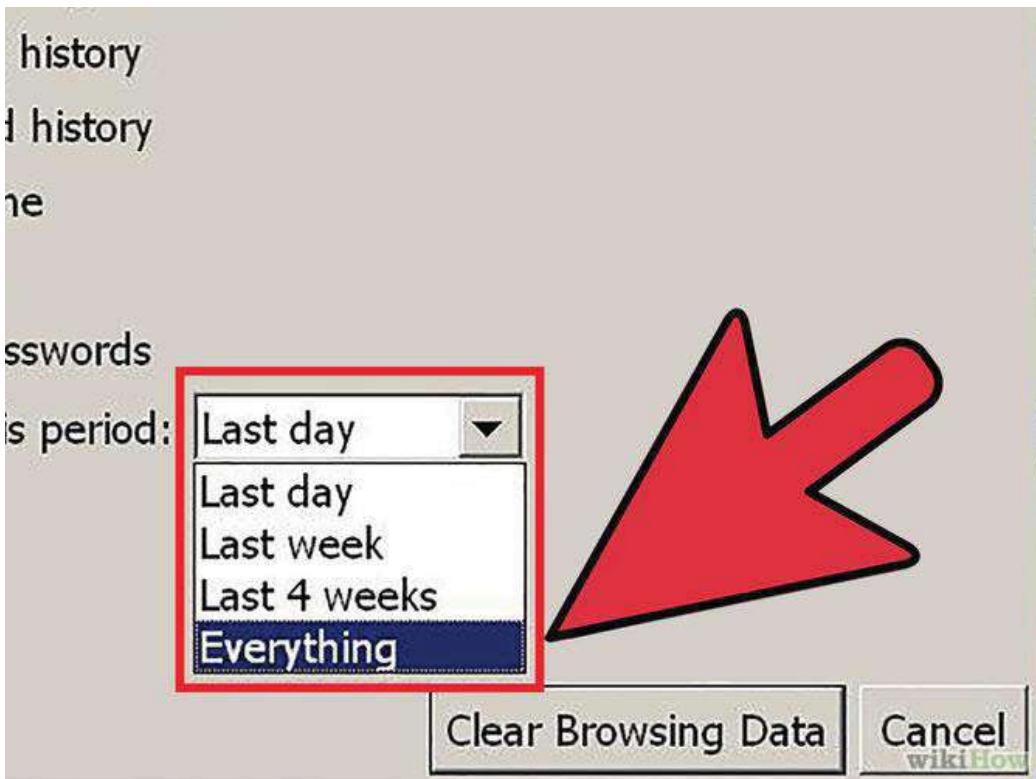
**Step 1:** Once your browser is open, select the Tools menu (the wrench in the upper-right corner) and select Options (Preferences on Mac).



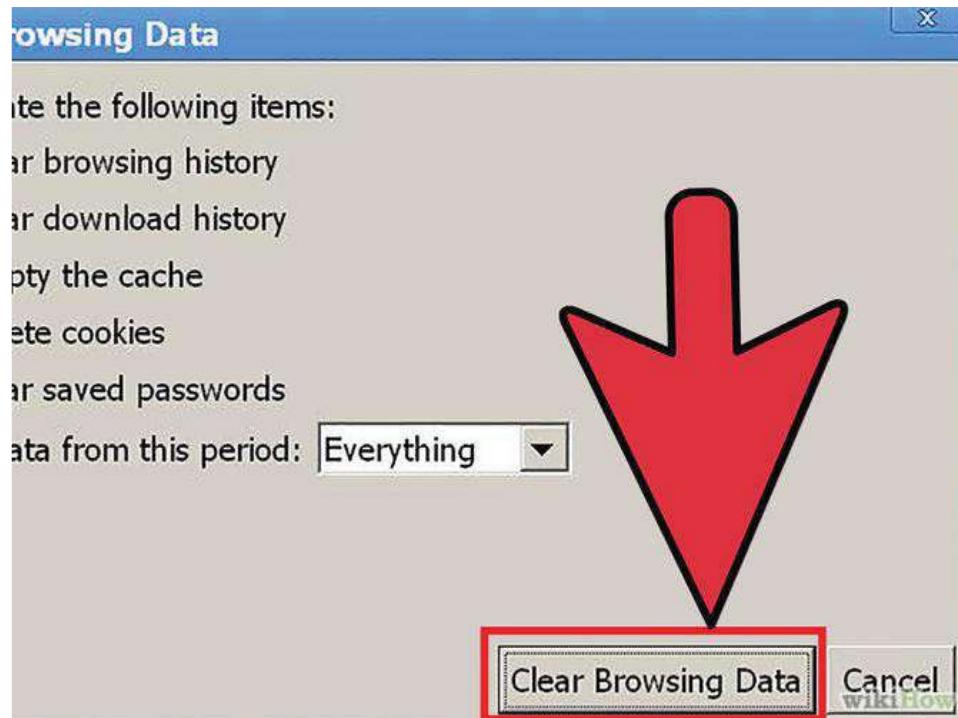
**Step 2:** On the Under the Hood tab, click the **Clear Browsing data** button.



**Step 3:** Select the **Empty the cache** check-box.



**Step 4:** You can also choose the period of time you wish to delete cached information using the Clear data from this period dropdown menu.



**Step 5:** Click the Clear Browsing Data button.

### 9.3.3 Clearing cache for Safari for iOS, iPhone and iPad



**Step 1:** Click on Settings from the home page.

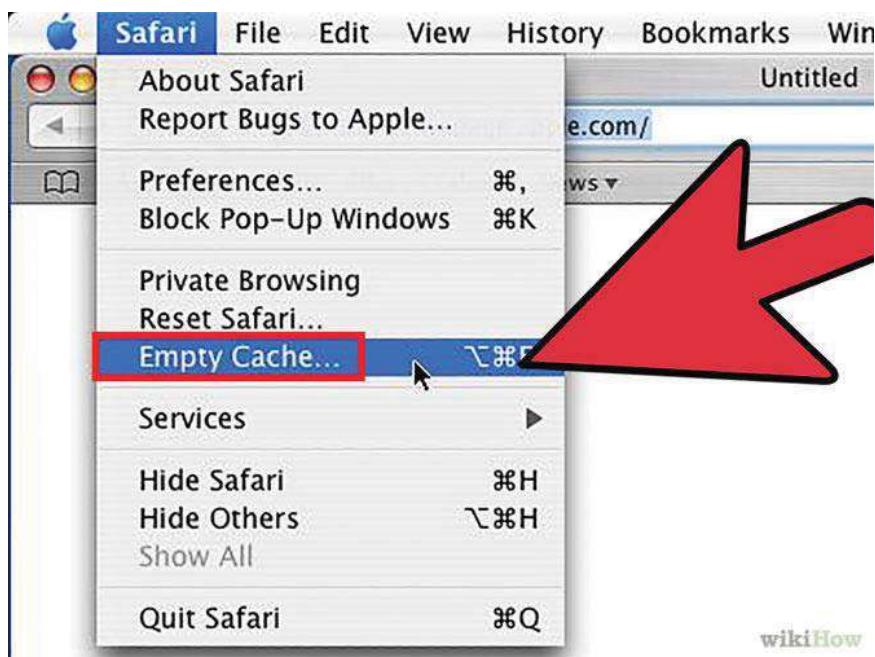


**Step 2:** Scroll down until you see "Safari." Click on it to bring up the option page.

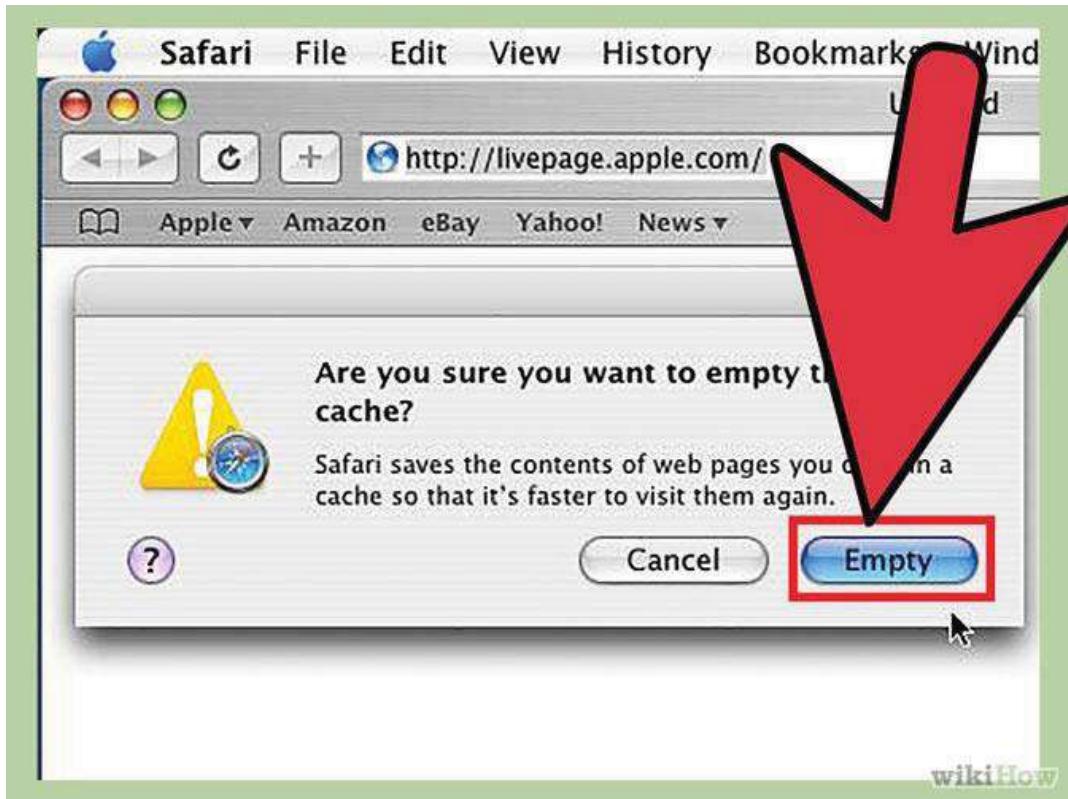


**Step 3:** Click "**Clear Cookies and Data**". A popup box will appear. Click "Clear Cookies and Data" again to confirm your choice.

#### 9.3.4 Clearing cache for Safari for Mac OS x

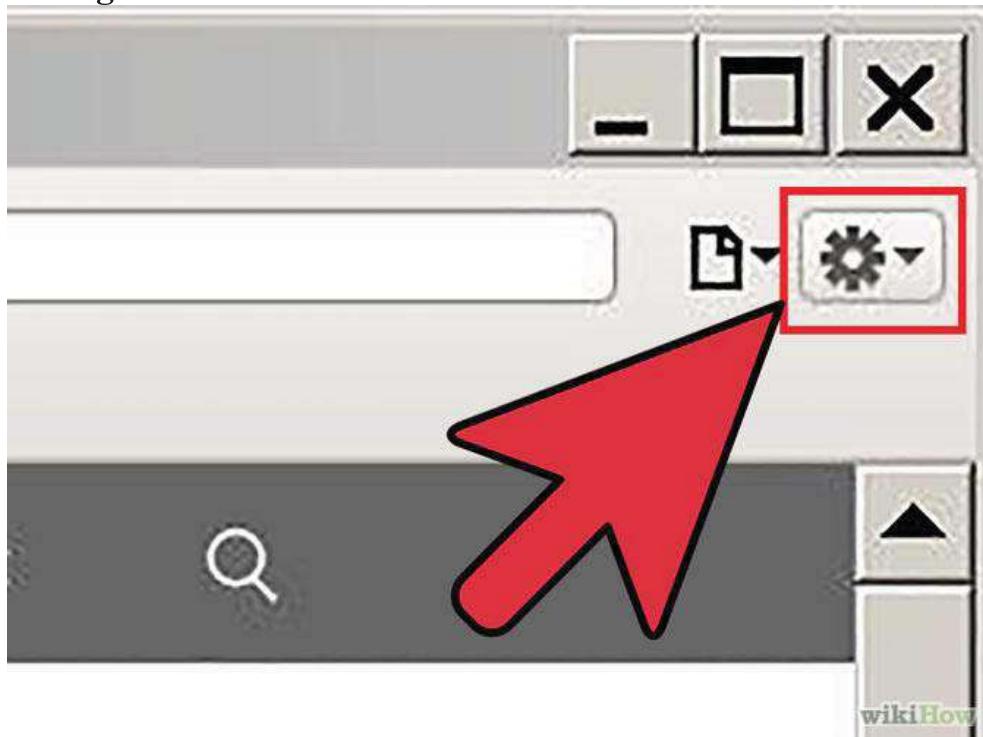


**Step 1:** Once your browser is open, click the Safari menu and select Empty Cache.

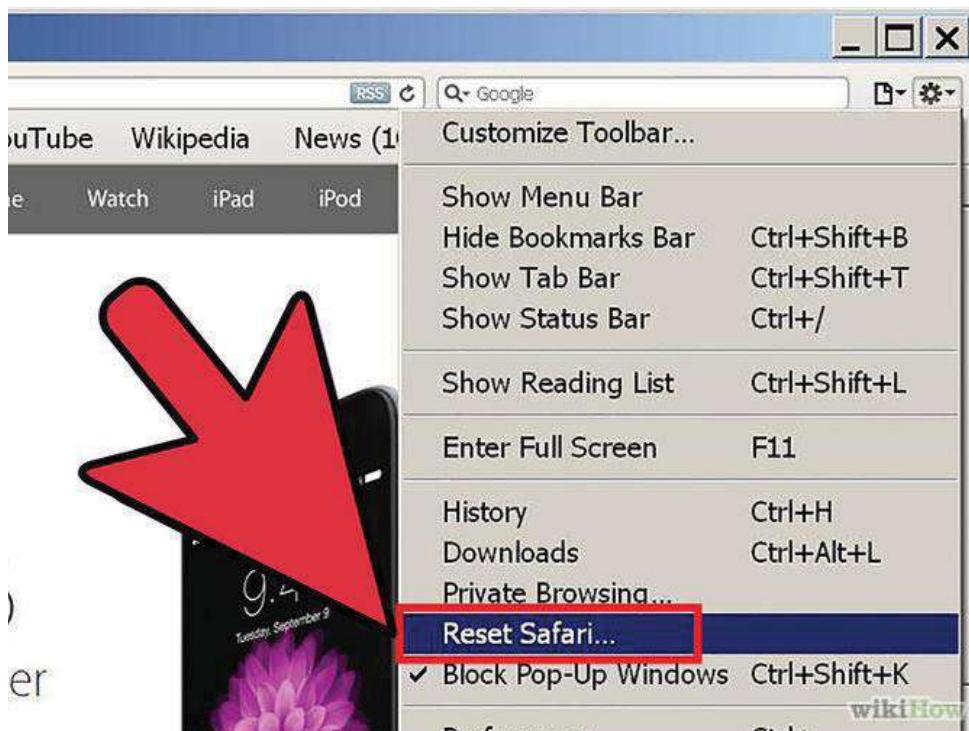


Step 2: Click Empty.

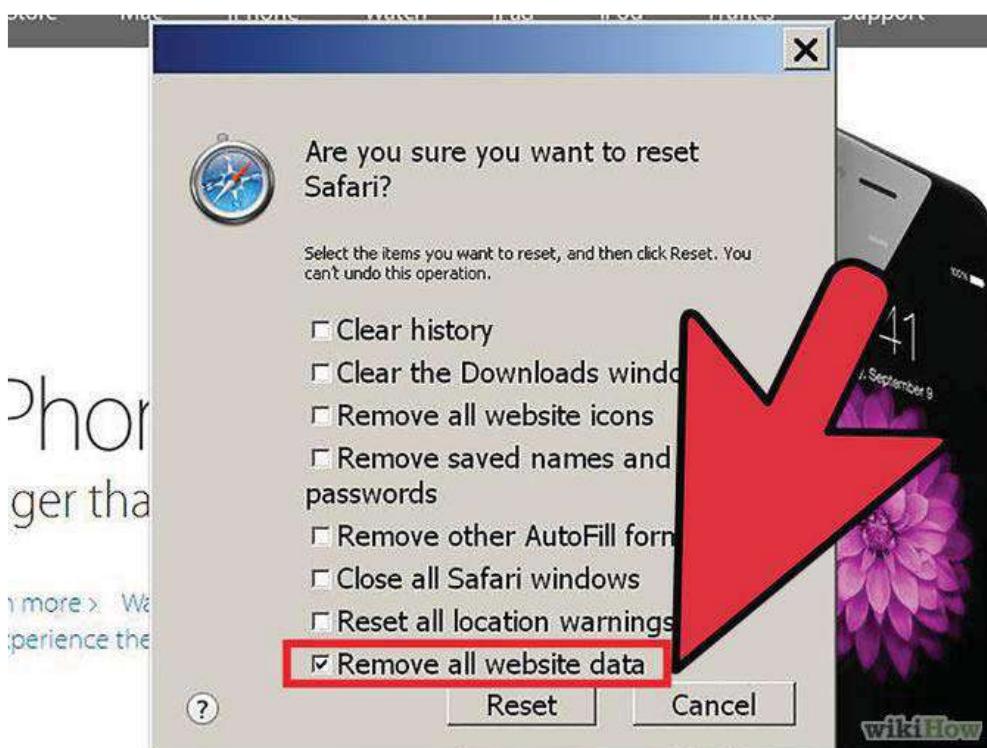
#### 9.3.5 Clearing cache for Safari for windows



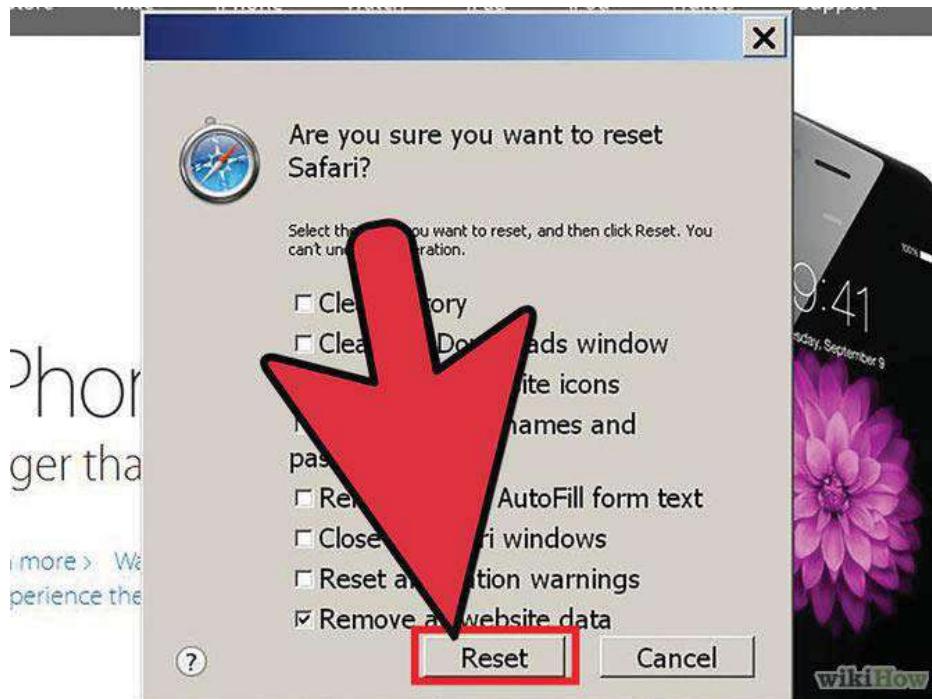
**Step 1:** Once your browser is open, click the gear icon on the top right.



**Step 2:** Select "Reset Safari..." This will prompt a screen to open.

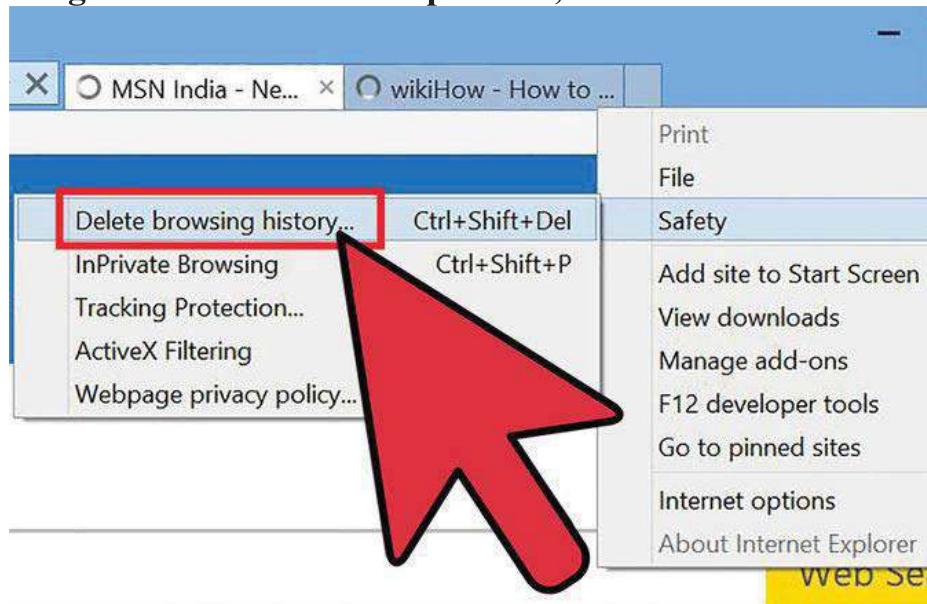


**Step 3:** Select "**Remove all website data**" at the very bottom of the prompt. Check or uncheck any other categories you want reset.



**Step 4:** Click “Reset”.

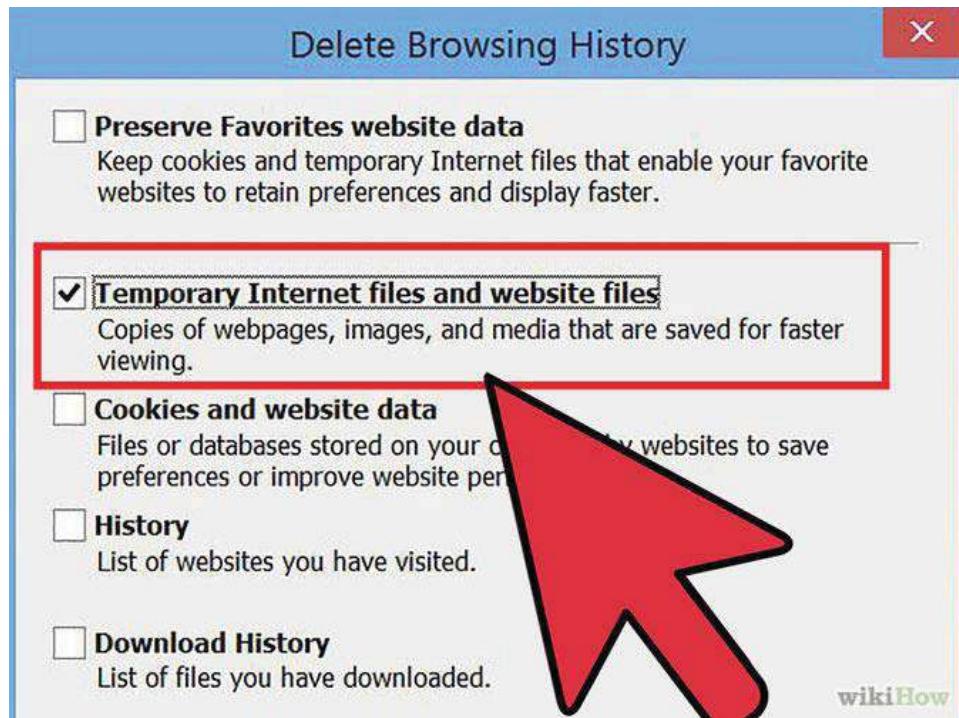
### 9.3.6 Clearing cache for Internet explorer 9, 10 and 11



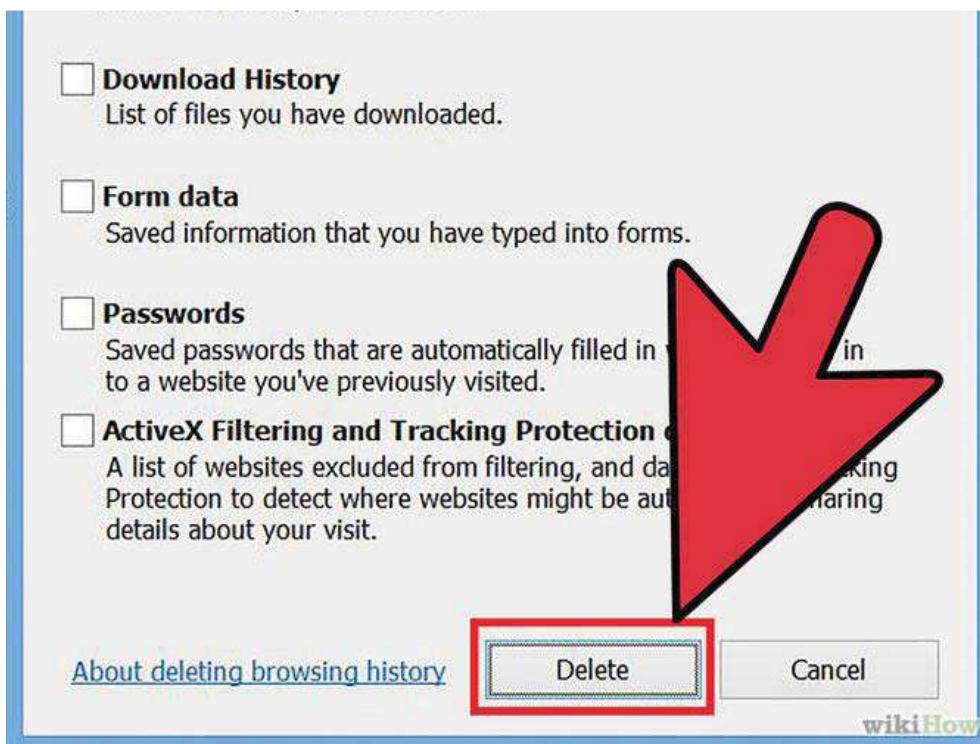
hopping World Cup 2014

wikiHow

**Step 1:** Once your browser is open, click the gear icon at the top right to open the **Settings** menu. Then, select **Safety** and **Delete Browsing History**.

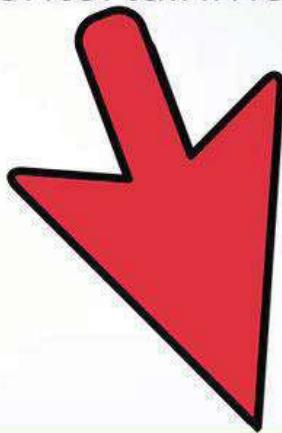


**Step 2:** Select Temporary Internet Files. You will also need to uncheck all of the other boxes, especially Preserve Favorites website data. This option makes the window also delete objects from websites in your Favorites folder, which is necessary to completely clear your cache.



**Step 3:** Click the Delete button near the bottom of the window to perform the operations (i.e. clear your cache by deleting temporary files).

entertainment lifestyle shopping



Internet Explorer has finished deleting the selected browsing history.

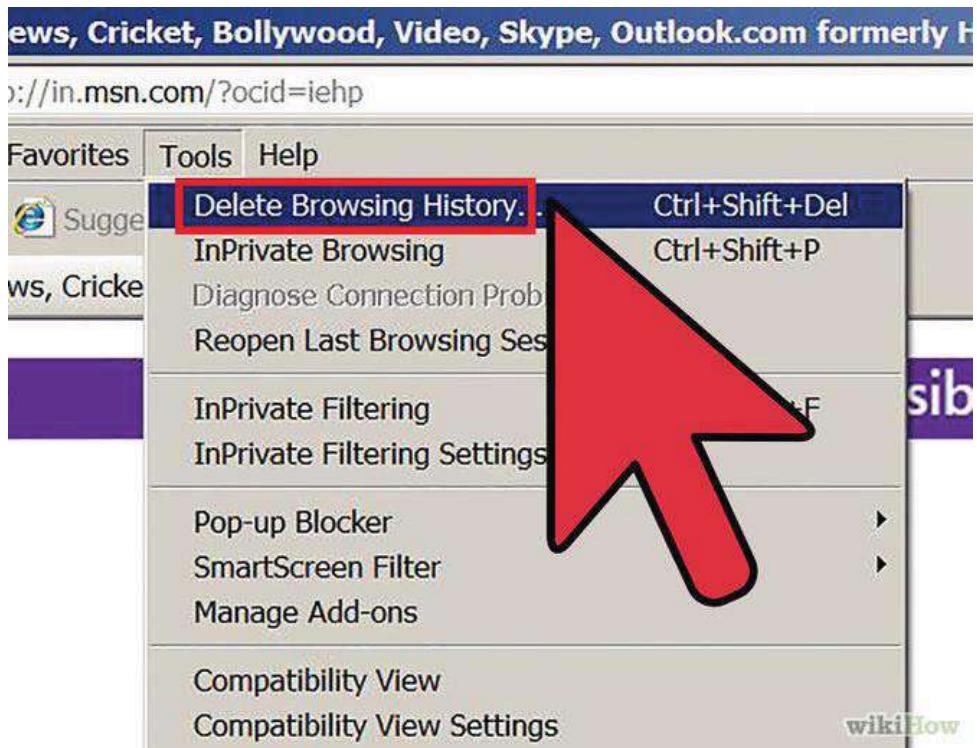
wikiHow

**Step 4:** Your computer will work for a moment, and then the process will be complete. You've successfully cleared Internet Explorer 9's Cache!

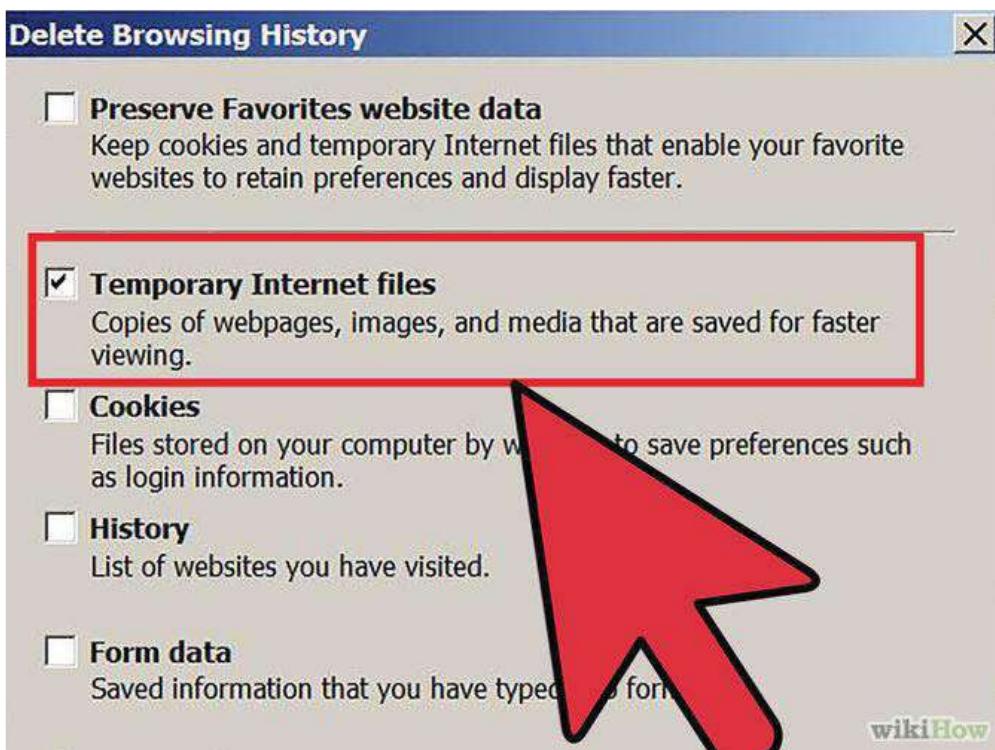
### 9.3.7 Clearing cache for Internet explorer 8



**Step 1:** Once your browser is open, click the **Tools** menu.



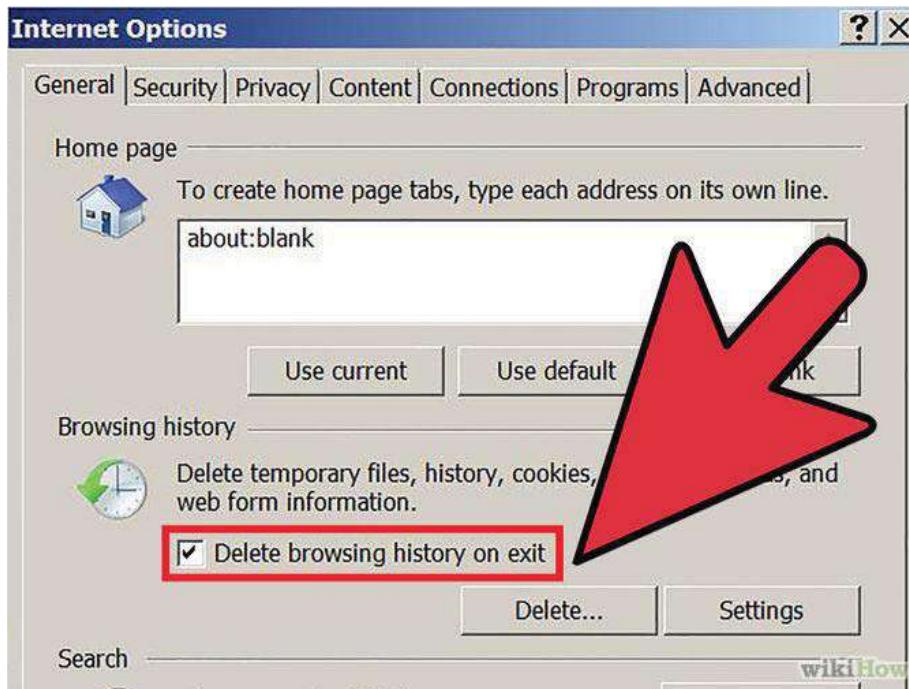
Step 2: Click on **Delete Browsing History**.



Step 3: Select **Temporary Internet Files**.



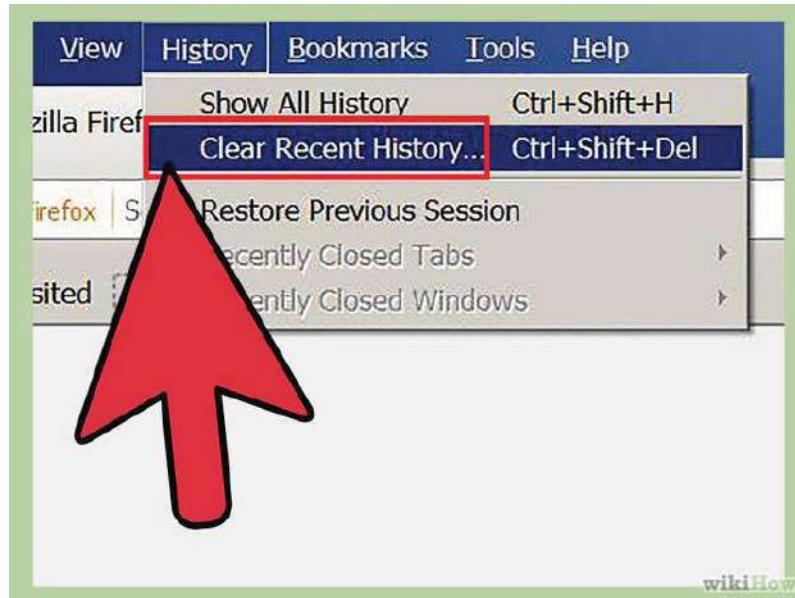
**Step 4:** Click the **Delete** button near the bottom of the window to delete your temporary files (i.e. clear your cache).



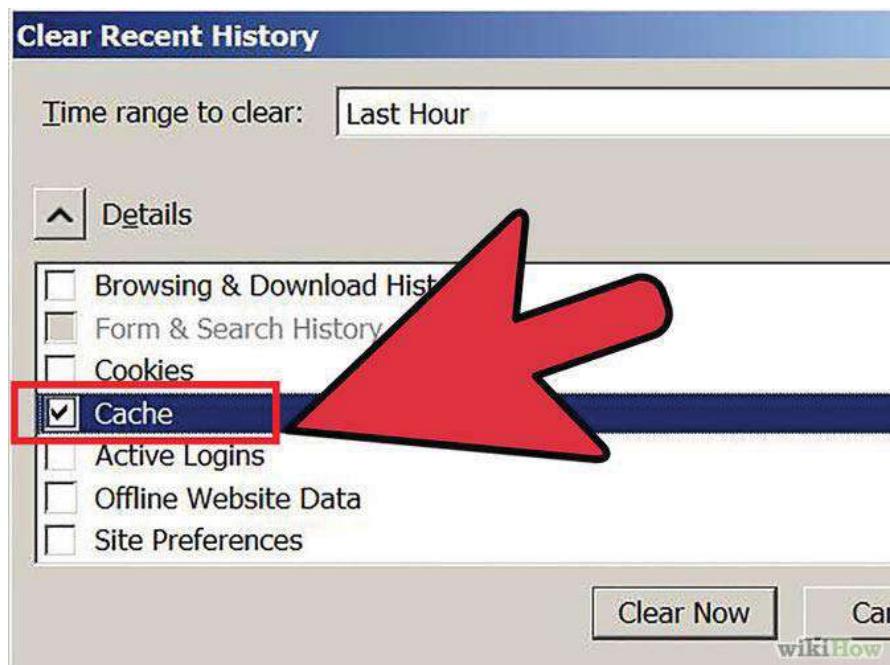
**Step 5:** Set your cache to delete every time you close Internet Explorer. If you want the browser to automatically clear the cache whenever you close it, close the 'Delete Browsing History' window, select '**Internet Options**' from the Tools menu, and check the '**Delete Browsing history on exit**' checkbox.

Note: IE8 has a "feature" which retains some cookies even after you clear your cache if you do not UNCHECK the "Preserve Favorites Website Data." If you truly need to clear your cache, you will want to uncheck this!

### 9.3.8 Clearing cache for Firefox



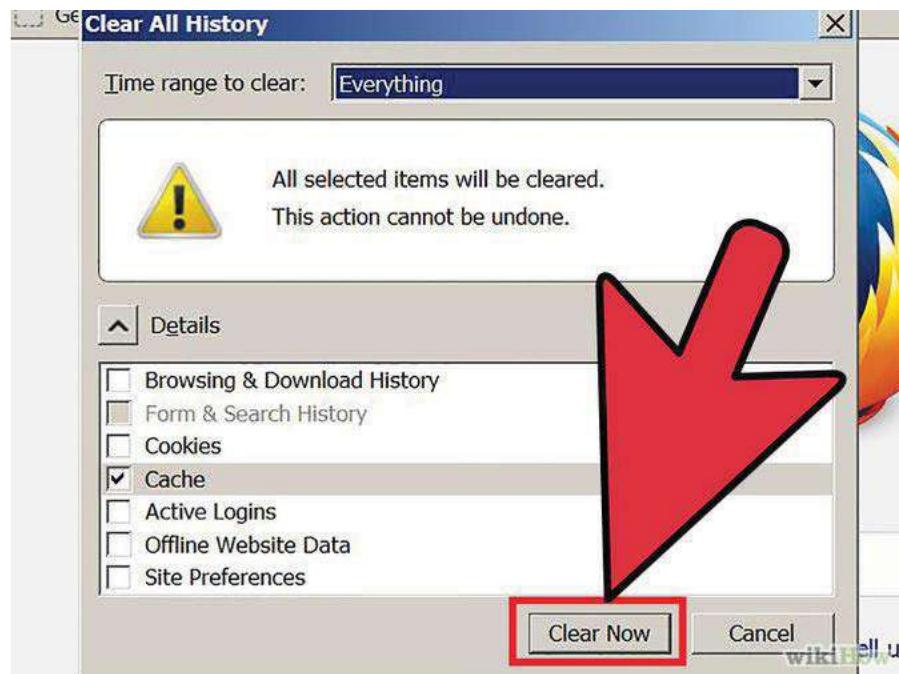
**Step 1:** On a PC, click the "Firefox" menu in the top left corner. Next, select the right arrow next to "History >", and click "**Clear Recent History**".



**Step 2:** Make sure "Details" is expanded, then select "**Cache**" from the list. Uncheck everything else.

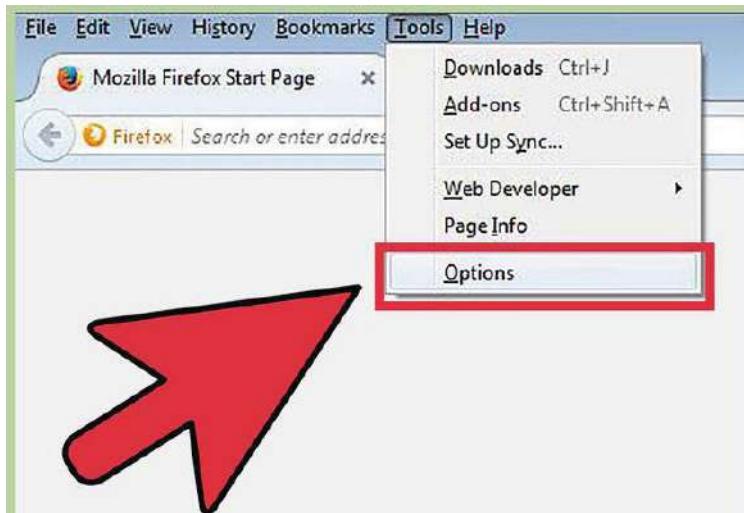


**Step 3:** In the "Time Range to Clear" drop down, select "Everything".

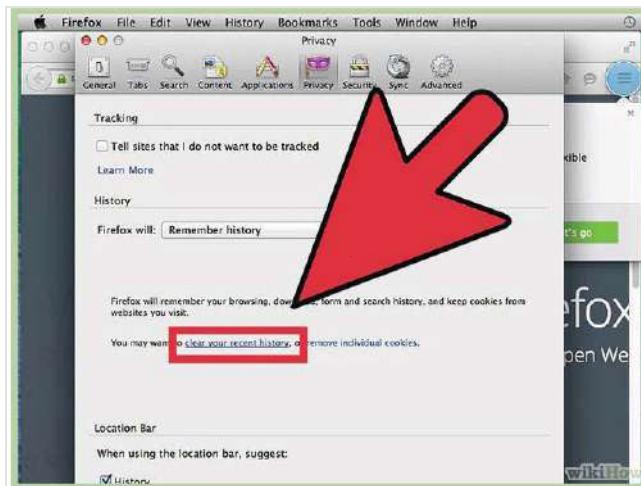


**Step 4:** Select "Clear Now". Your computer will work for a moment, and the process will be complete. You've successfully cleared Firefox's Cache!

### 9.3.9 Clearing cache for Firefox 33



**Step 1:** Click the Menu button ("hamburger button" - the one with three horizontal lines) and then choose Options.

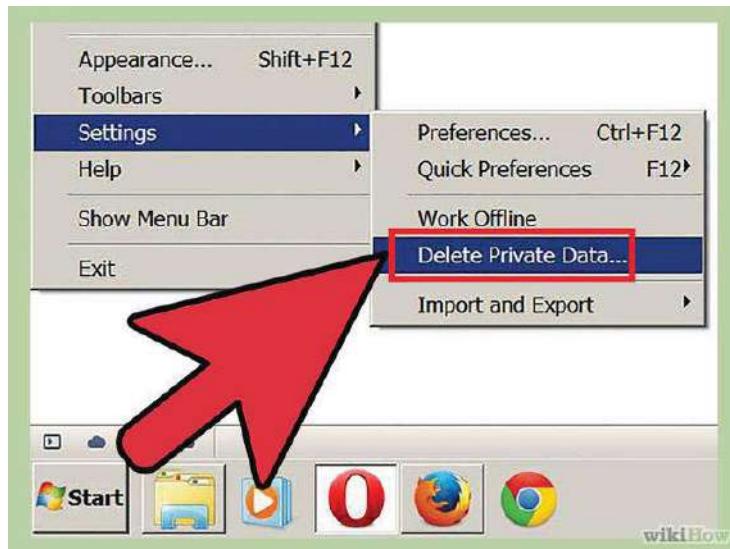


**Step 2:** Firefox for Mac: On a Mac, choose Preferences from the Firefox menu and then continue as instructed below. With the Options window now open, click the Privacy tab. In the History area, click the clear your recent history link.

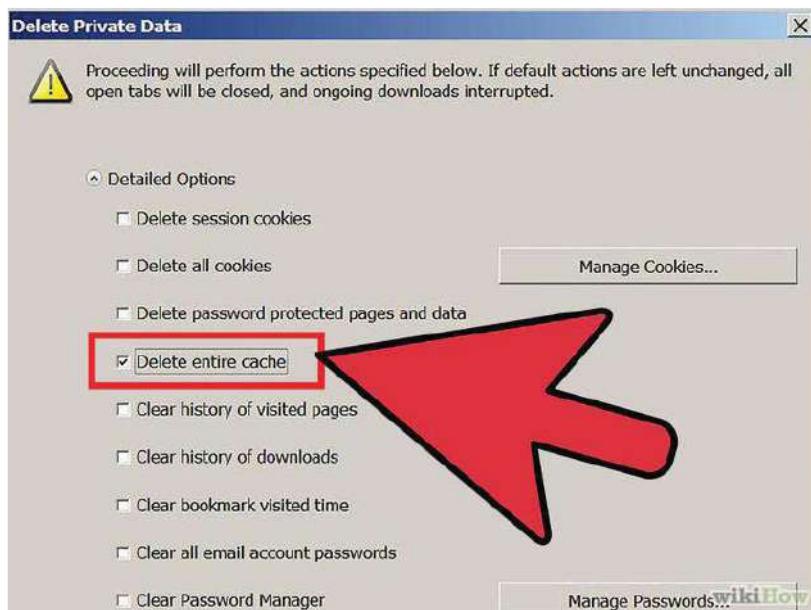


**Step 3:** If you wish to clear other kinds of stored data, feel free to check the appropriate boxes. They will be cleared with the cache in the next step.

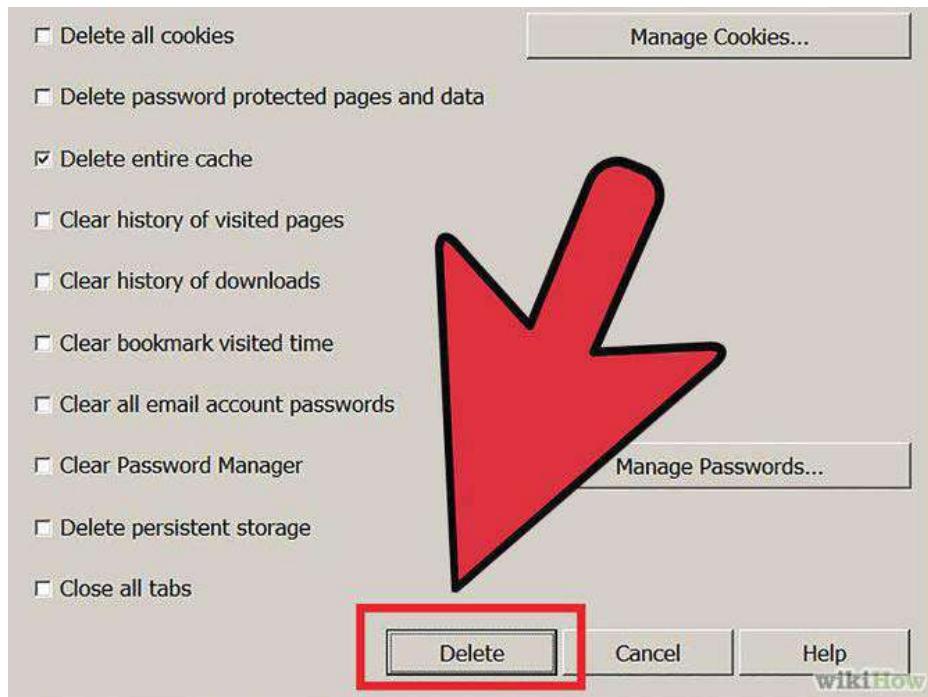
### 9.3.10 Clearing cache for opera



**Step 1:** Once your browser is open, select the "Settings" menu and click "Delete private data".

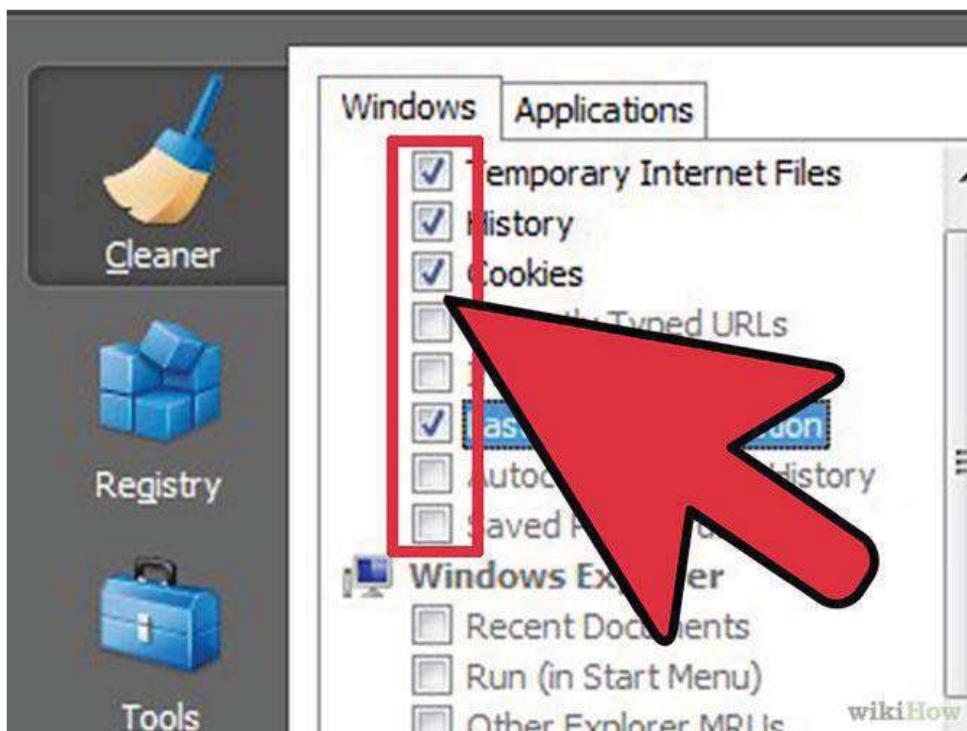


**Step 2:** Make sure the "Delete entire cache" box is checked. Make sure any unwanted categories are left **unchecked**.



Step 3: Press “Delete”.

### 9.3.11 Clearing cache for Ccleaner



**Ccleaner-** This is a computer maintenance tool that lets you scan and delete browser cache and cookies. Launch it, go to Cleaner tab and make sure to check the Temporary internet files for the browser you have.

## **Activity**

- a. Perform the cache clearing operation on your system browser.
- b. Perform the cache clearing operation on the browser of your smartphone.
- c. Install CCleaner in your system and use it to perform cache clearing operation.
- d. Find out whether the popular websites you visit daily are secure or not.
- e. Can you find any banking site that does not use https://
- f. Can you find some social networking site that does not use https://
- g. Can you list down some important points that should be kept in mind before going for online shopping.

# WIRELESS SECURITY

This chapter is about different kind of Best Practices that should be followed when using Wireless LAN.

## 10.1 WHAT IS WIRELESS LAN?

The Wireless LAN or WLAN is becoming a popular way to connect devices such as computers these days. In offices and homes, WLAN has become an alternative way of communication compared to wired LAN. The convenience to connect different devices is both cost effective and easily maintainable. The Wikipedia says: “Wireless LANs have become popular in the home due to ease of installation, and the increasing to offer wireless access to their customers; often for free.”

The other factors why WLANs are becoming more acceptable are:

1. No need to be connected physically with each other through any medium such as cables.  
You can roam around freely in office premises, home or around.
2. WLANs are cost effective. Cabling all the way in the offices, hotels etc are not needed.  
So it's cheap and provides same quality of service.
3. Unreachable spots where a cable is hardly accessible, WLAN signals can reach out such as big installations like airports. Also surfing outdoors is also convenient. Just install the device called Access Points (AP) and you are done.
4. Less interruption and easy trouble shooting in case of failures as compared to cabled networks.
5. More secure as most of APs support best encryption methods which protect them from sniffing and other attacks.



Figure 44: A typical Wireless network

## **10.2 MAJOR ISSUES WITH WLAN**

Having said that, WLAN are also as prone to various attacks as their counterpart wired LANs are. Actually WLANs are easier to hack as compared to wired LANs, if not properly configured, due to its easy accessibility around the installation. No need to be in contact of physical wires to hack can be done from anywhere. Its convenience can turn into serious risk to the organization if not configured properly. Major attacks include such as, Sniffing, Key cracking, DoS (Denial of Service), Deauthentication attacks, War driving etc. This chapter is not focused on attacks, we shall mainly concentrate on best practices- how to install and use WLAN securely which can thwart a number of above mentioned attacks.

### **10.2.1 Secure WLAN**

Wireless Security mainly depends on these 3 factors:

- How much is your wireless network secured in terms of encryption being used.
- Monitoring for suspicious and unusual activities.
- User awareness and education.

These are the combination of various approaches ranging from corporate to home networks.

These are also for users how to remain safe while surfing.

### **10.2.2 Wi-Fi at home**

Using a Wi-Fi at home is not a luxury anymore it has become a necessity. However, when the question of security comes into the scene, the first thought that would arise in my mind is how you can protect something which you cannot see, neither can you feel it? Protecting a home wireless network is altogether a different side of the coin as compared to wired networks. Most of wireless network device vendor's and Internet Service provider do not provide any security settings by default and leave the customer to fend for herself. So make sure, your network is secured from being maliciously used.

There is no silver bullet that will protect your wireless network infrastructure. These are, however, some countermeasures listed below that should be used in conjunction with each other to secure your wireless network to the highest level:

**1. Use most secure possible encryption:** The first and most necessary step- use industry standard encryptions. The old (however generally used) WEP-Wired Equivalent Privacy, has been known to be broken. Even you use complex passwords it can be broken and decrypted within minutes or hours. WEP uses 40 bit or 128 bits RC4 ciphers to encrypt the channel.

Instead use secure protocols such as WPA 2 – Wi-Fi Protected Access- 2, which uses strong 128 bits AES ciphers and is typically considered more robust encryption strategy available.

**Attacks mitigated:** WEP Key cracking, Sniffing, Capturing/Eavesdropping

**2. Use Firewall:** All the wireless routers come with built-in firewalls. Enable them with all the security features. You should block any anonymous ping requests and place restrictions on website browsing, if required. Define additional security policies and apply them.

**Attacks mitigated:** Fingerprinting, System compromise

**3. Have a monitoring system in place:** There's a saying- prevention is better than a cure. If you are able to detect some suspicious activities before it penetrates your network, you can block them or take precautionary measures. Deploy WIPS/WIDS for monitoring suspicious activities.

**Attacks mitigated:** Scanning, DoS

**4. Don't use default credentials:** Every wireless router comes with a set of default username/password. Sometimes, people don't change them and keep using them for long time. Username and passwords are used by computers or other devices to connect to wireless router. If any hacker is able to guess them, he can connect to your network easily. Studies show that majority of users use the same combination of username/passwords as set by manufacturers. Some default username combinations are: admin/admin, admin/password or admin/““.

**Attacks mitigated:** Unauthorized access, War driving

**5. Disable Auto-connect feature:** Some devices or the computers/laptops have ‘Let this tool manage your wireless networks’ or ‘Connect automatically to available network’. Such users having this auto-connect feature enabled are prone to Phishing attack or Rogue AP attack. Attackers keep their APs alive and kicking for such kind of unsuspecting users. They also use luring names as ‘HotSpot’, ‘SecureConnect’, ’GovtNetworks’ etc. The user will never suspect them and keep surfing the wireless network happily. Also if you have not changed the default password of your router, the attacker will try to use this feature on their machine and automatically connect using the easily guessable default passwords.

**Attacks mitigated:** Phishing, Sniffing, Rouge AP association

**6. Don't use public Wi-Fi spots to surf sensitive websites:** Free and open wireless networks available on airports, cafes, railway stations are not very secure by nature. They do

not use any encryption to secure the channel between your laptop to the router. So any information which is not by default going on HTTPS from your laptop/smart phone is susceptible to sniffing and even more your session could be hijacked because the unencrypted channel may leak the active session ID used by your website. Recently to demonstrate these types of attacks one researcher developed a tool Firesheep [<http://codebutler.github.com/firesheep/>]. All the attacker needs to do is to just install this tool in Firefox and start sniffing the communications on a public unencrypted Wi-Fi. Some applications like Facebook encrypts the login page [HTTPS] but internal pages are served on unencrypted [HTTP] channel so your session ID can be leaked.

**Attacks mitigated:** Sniffing, Session Hijacking

**7. Change the default SSID:** Although this will not prevent hackers breaking into a network, using a default SSID acts as an indication that the user is careless. So he may be an obvious target to explore further to see if he still uses the default passwords as well?

**Attacks mitigated:** War driving

**8. Restrict access by assigning static IP addresses and MAC filtering:** Disable automatic IP assigning feature and use private static IPs to the legitimate devices you want to connect. This will help you in blocking unwanted devices from being connected to your network. Also, enable MAC filtering- router remembers MAC of each and every device connected to it and saves it as list. You can use this facility to restrict access. Only a set of trusted devices can be allowed to connect. However MAC spoofing is still possible but it raises an extra bar for your wireless network.

**9. Turn off your router when not in use:** Last but not least, a little obvious, but it will save your network from all the attacks for that time period.

#### 1.7.2.3 Wi-Fi in a Corporate/Enterprise Network

Due to the nature of activity and criticality of information, it is very important that Corporate / Enterprise networks have a higher degree of security.

The following are good to have:

- Defining an adequate organization wide Information Security policy & procedures for wireless network

- SSID's should not be associated with the organization, AP vendor or any other related information which would be easy to guess or associate with the current organization
- Enable WPA2 Enterprise encryption with RADIUS authentication and use of EAP protocol like EAP-TTLS, TLS etc.
- Implementation of PKI infrastructure. CA signed certificates to authenticate the server to client and vice versa
- Filtering of clients based on unique identifier like MAC Address
- Isolated 'Guest' wireless network with no interface / connection to the corporate network
- Limiting the radius of Wi-Fi network by reducing the power output of the AP
- Allocating IP Address to the employee and guest machines only after successful authentication
- Periodically changing the keys & passwords
- Use of VPN while accessing corporate information from Public Wi-Fi network
- Client side utilities like DecaffeintID can help in detecting changes in ARP table and serve as common man's IDS to protect against attacks like 'hole196' and DoS.
- Implementation of Wireless IDS. Wireless IDS is a new concept. The key features of Wireless IDS are:
  - Prevention against Rogue AP's
  - Detection & prevention against DoS attacks
  - Assistance in locating the approximate physical location of the attacker
  - Assistance in enforcing the Organization's Information Security policy on wireless networks
  - Detection of use of scanning tools like Kismet & NetStumbler

## ACTIVITY

1. What are the precautions one should take using a wi-fi network at public place?
2. How to secure home network?
3. How to secure enterprise network?
4. Find more about the terms over internet:
  - IDS
  - DOS
  - Kismet
  - NetStumbler

## **RECOMENDED VIDEOS**

[https://www.youtube.com/watch?v=\\_WHynHcXm7c](https://www.youtube.com/watch?v=_WHynHcXm7c)

[https://www.youtube.com/watch?v=Jmszt\\_\\_J204](https://www.youtube.com/watch?v=Jmszt__J204)

<https://www.youtube.com/watch?v=aktovPyT0iM>

[https://www.youtube.com/watch?v=CStMHLQWa\\_8](https://www.youtube.com/watch?v=CStMHLQWa_8)

<https://www.youtube.com/watch?v=a9q-tDRCTtc>

<https://www.youtube.com/watch?v=xex1h93fnl8>

<https://www.youtube.com/watch?v=a9q-tDRCTtc>

# EMAIL AND SOCIAL MEDIA SECURITY

## 11.1 SAFE BROWSING GUIDELINES FOR SOCIAL NETWORKING SITES<sup>22</sup>

Online communities have existed since the invention of the internet. First there were bulletin boards and email lists, which gave people around the world opportunities to connect, to communicate and to share information about particular subjects. Today, social networking websites have greatly expanded the range of possible interactions, allowing you to share messages, pictures, files and even up-to-the-minute information about what you are doing and where you are. These functions are not new or unique – any of these actions can also be performed via the internet without joining a social networking site.

Although these networks can be very useful, and promote social interaction both online and offline, when using them you may be making information available to people who want to abuse it. Think of a social networking site as being like a huge party. There are people there that you know, as well as some that you don't know at all. Imagine walking through the party with all your personal details, and up-to-the-minute accounts of what you are thinking, written on a big sign stuck on your back so that everyone can read it without you even knowing. Do you really want everyone to know all about you?

Remember that social networking sites are owned by private businesses, and that they make their money by collecting data about individuals and selling that data on, particularly to third party advertisers. When you enter a social networking site, you are leaving the freedoms of the internet behind and are entering a network that is governed and ruled by the owners of the site. Privacy settings are only meant to protect you from other members of the social network, but they do not shield your data from the owners of the service. Essentially you are giving all your data over to the owners and trusting them with it.

If you work with sensitive information and topics, and are interested in using social networking services, it is important to be very aware of the privacy and security issues that they raise. Human rights advocates are particularly vulnerable to the dangers of social networking sites and need to be extremely careful about the information they reveal about themselves AND about the people they work with.

---

<sup>22</sup> <https://securityinabox.org/en/guide/social-networking>

Before you use any social networking site it is important to understand how they make you vulnerable, and then take steps to protect yourself and the people you work with. This guide will help you understand the security implications of using social networking sites.

### **11.1.1General Tips on using Social Networking platforms safely**

Social media have become an evident part of our life. We share out updates with our friends, family and anyone who is concerned using social media. But the hackers can use this information to steal sensitive data and hack your account. Given below are some of the general tips on using social media.

➤ **Always ask the questions:**

- ✓ Who can access the information I am putting online?
  - ✓ Who controls and owns the information I put into a social networking site?
  - ✓ What information about me are my contacts passing on to other people?
  - ✓ Will my contacts mind if I share information about them with other people?
  - ✓ Do I trust everyone with whom I'm connected?
- Always make sure you use **secure passwords** to access social networks. If anyone else does get into your account, they are gaining access to a lot of information about you and about anyone else you are connected to via that social network. Change your passwords regularly as a matter of routine.
- Make sure you understand the default **privacy settings** offered by the social networking site, and how to change them.
- Consider using **separate accounts/identities**, or maybe different pseudonyms, for different campaigns and activities. Remember that the key to using a network safely is being able to trust its members. Separate accounts may be a good way to ensure that such trust is possible.
- Be careful when accessing your social network account in public internet spaces. **Delete your password and browsing history** when using a browser on a public machine.
- **Access social networking sites using https://** to safeguard your username, password and other information you post. Using https:// rather than http:// adds another layer of security by encrypting the traffic from your browser to your social networking site.
- Be careful about putting too much information into **your status updates** – even if you trust the people in your networks. It is easy for someone to copy your information.

- Most social networks allow you to integrate information with other social networks. For example you can post an update on your Twitter account and have it automatically posted on your Facebook account as well. Be particularly **careful when integrating your social network accounts!** You may be anonymous on one site, but exposed when using another.
- Be cautious about how safe your content is on a social networking site. **Never rely on a social networking site as a primary host for your content** or information. It is very easy for governments to block access to a social networking site within their boundaries if they suddenly find its content objectionable. The administrators of a social networking site may also decide to remove objectionable content themselves, rather than face censorship within a particular country.

### **11.1.2 Posting Personal Details**

Social networking sites ask you for a good deal of data about yourself to make it easier for other users to find and connect to you. Perhaps the biggest vulnerability this creates for users of these sites is the possibility of identity fraud, which is increasingly common. In addition, the more information about yourself you reveal online, the easier it becomes for the authorities to identify you and monitor your activities. The online activities of diaspora activists from some countries have led to the targeting of their family members by the authorities in their homelands.

Ask yourself: is it necessary to post the following information online?

- ✓ birth dates
- ✓ contact phone numbers
- ✓ addresses
- ✓ details of family members
- ✓ sexual orientation
- ✓ education and employment history

### **11.1.3 Friends, Followers and Contacts**

The first thing you will do after filling in your personal details with any social networking application is establish connections to other people. Presumably these contacts are people you know and trust – but you may also be connecting to an online community of like-minded individuals that you have never met. The most important thing to understand is what information you are allowing this online community to have.

When using a social network account such as Facebook, where a lot of information about yourself is held, consider only connecting to people you know and trust not to misuse the information you post.

#### **11.1.4 Status Updates**

On Twitter and Facebook and similar networks, the status update answers the questions: What am I doing right now? What's happening? The most important thing to understand about the status update is who can actually see it. The default setting for the status update on most social networking applications is that anyone on the internet can see it. If you only want your contacts to see the updates, you need to tell the social networking application to keep your updates hidden from everyone else.

To do this in Twitter, look for “Protect Your Tweets”. In Facebook, change your settings to share your updates with “Friends Only”. Even if you switch to those settings, consider how easy it is for your information to be reposted by followers and friends. Agree with your network of friends on a common approach to passing on the information posted in your social networking accounts. You should also think about what you may be revealing about your friends that they may not want other people to know; it's important to be sensitive about this, and to ask others to be sensitive about what they reveal about you.

There have been many incidents in which information included in status updates has been used against people. Teachers in the US have been fired after posting updates about how they felt about their students; other employees have lost their jobs for posting about their employers. This is something that nearly everyone needs to be careful about.

#### **11.1.5 Sharing Online Content**

It's easy to share a link to a website and get your friend's attention. But who else will be paying attention, and what kind of reaction will they have? If you share (or "like") a site that opposes some position taken by your government, for example, agents of that government very might well take an interest and target you for additional surveillance or direct persecution.

If you want your contacts (and of course the administrators of the social networking platform you use) to be the only ones who can see the things you share or mark as interesting, be sure to check your privacy settings.

#### **11.1.6 Revealing your Location**

Most social networking sites will display your location if that data is available. This function is generally provided when you use a GPS-enabled phone to interact with a social network, but don't assume that it's not possible if you aren't connecting from a mobile. The network your computer is connected to may also provide location data. The way to be safest about it is to double-check your settings.

Be particularly mindful of location settings on photo and video sharing sites. Don't just assume that they're not sharing your location: double-check your settings to be sure.

### **11.1.7 Sharing Videos and Photos**

Photos and videos can reveal people's identities very easily. It's important that you have the consent of the subject/s of any photo or video that you post. If you are posting an image of someone else, be aware of how you may be compromising their privacy. Never post a video or photo of anyone without getting their consent first.

Photos and videos can also reveal a lot of information unintentionally. Many cameras will embed hidden data (metadata tags), that reveal the date, time and location of the photo, camera type, etc. Photo and video sharing sites may publish this information when you upload content to their sites.

### **11.1.8 Instant Chats**

Many social networking sites have tools that allow you to have discussions with your friends in real time. These operate like Instant Messaging and are one of the most insecure ways to communicate on the internet, both because they may reveal who you are communicating with, and what you are communicating about.

*Connecting to the site via https is a minimum requirement for secure chatting, but even this is not always a guarantee that your chat is using a secure connection. For example, Facebook chat uses a different channel to HTTPS (and is more prone to exposure).*

It is more secure to use a specific application for your chats, such as Pidgin with an Off-the-record plugin, which uses encryption. Read the 'Pidgin – secure instant messaging' hands-on guide.

### **11.1.9 Joining and Creating Groups, Events and Communities**

What information are you giving to people if you join a group or community? What does it say about you? Alternatively, what are people announcing to the world if they join a group or community that you have created? How are you putting people at risk?

When you join a community or group online it is revealing something about you to others. On the whole, people may assume that you support or agree with what the group is saying or doing, which could make you vulnerable if you are seen to align yourself with particular political groups, for example. Also if you join a group with a large number of members that you don't know, then this can compromise any privacy or security settings that you have applied to your account, so think about what information you are giving away before joining. Are you using your photo and real name so strangers can identify you?

Alternatively, if you set up a group and people choose to join it, what are they announcing to the world by doing so? For example, perhaps it is a gay and lesbian support group that you have set up to help people, but by joining it people are openly identifying themselves as gay or gay-friendly, which could bring about dangers for them in the real world.

## 11.2 EMAIL SECURITY TIPS<sup>23</sup>

1. Don't open email attachments that you are not expecting, or which have come from someone you do not know. When you open such an email, make sure that your anti-virus software is up-to-date and pay close attention to any warnings from your browser or email program.
2. You can use anonymity software which can help you hide your chosen email service from anyone who might be monitoring your internet connection. A good, free software programme to do this is *Tor* (Find out more about Tor browser using Google). If you don't want to give away information about your identity through your email, do not register a username or 'Full Name' that is related to your personal or professional life.
3. You can avoid getting spam (unwanted or junk email) by guarding your email address and distributing it sparingly. Also, never open or reply to any emails you consider to be spam, because spammers will take this as a proof of the legitimacy of the address and will just send you more spam. Consider using a spam filter, but remember that it needs to be monitored as it may mistake a genuine email for spam.
4. You should try to avoid your emails being mistaken for spam by the recipients. Spam filters will block messages with certain words in the subject heading. It is worth scanning your spam folder for subject lines that are getting blocked.

---

<sup>23</sup> <https://survival.tacticaltech.org/internet/email/tips>

5. Beware of email scams. Many scam emails pretend to come from a bank, Ebay, Paypal, or other online shops. If you get an email telling you that your account is in danger of being shut down, or that you need to take immediate action by updating your account information, be very suspicious: these messages are usually scams. Another frequent scam has you receiving an email from someone you know which says that they have had an emergency and asks you to send them money. This person's email account is likely to have been compromised by a scammer.
6. Pay close attention if your browser suddenly gives you messages about invalid security certificates when you attempt to access a secure webmail account. It could mean that someone is tampering with the communication between your computer and the server in order to intercept your messages.

## ACTIVITY

1. What are anonymous accounts? Find some browsers which supports anonymouity.
2. After going though the above section, find out whether you were following the above safe practices while handling your social medial account? Find the gaps?
3. Based on the above recommendations, adjust your social media account settings.

## RECOMENDED VIDEOS

<https://www.youtube.com/watch?v=EFHfg1bfgVc>

<https://www.youtube.com/watch?v=tkgLHoafeFk>

[https://www.youtube.com/watch?v=QUyla\\_nMJis](https://www.youtube.com/watch?v=QUyla_nMJis)

<https://www.youtube.com/watch?v=-CeuqCHX7tE>

<https://www.youtube.com/watch?v=xCHTmzfsGmI>

# SMARTPHONE SECURITY

## 12.1 INTRODUCTION<sup>24</sup>

Advances in technology now mean that mobile phones can provide services and features similar to desktop or laptop computers. These Smartphones offer many new ways to communicate and capture and disseminate media. To provide these new functionalities, the smartphones not only use the mobile network, but also connect to the internet either via a wi-fi connection (similar to a laptop at an internet cafe) or via data connections through the mobile network operator.

So while you can, of course, make phone calls with a smartphone, it is better to view smartphones as small computing devices. This means that the other material in this toolkit is relevant to your use of your smartphone as well as your computer.

Smartphones usually support a wide range of functionality – web browsing, email, voice and instant messaging over the internet, capturing, storing and transmitting audio, videos and photos, enabling social networking, multi-user games, banking and many other activities. However, many of these tools and features introduce new security issues, or increase existing risks. For instance, some smartphones have built-in geo-location (GPS) functionality, which means they can provide your precise location to your mobile network operator by default, and to many applications you use on your phone (such as social networking, mapping, browsing and other applications). As mentioned before, mobile phones already relay your location information to your mobile network operator (as part of the normal functions of the phone). However, the additional GPS functionality not only increases the precision of your location information, it also increases the amount of places where this information might be distributed.

It's worth reviewing all the risks associated with mobile phones discussed in our guide How to use mobile phones as securely as possible as all of them are also relevant to smartphone use. That guide also covers issues of eavesdropping, interception of SMS or phone calls, SIM card related issues, and best practices.

In this guide we'll take a look at the additional security challenges posed by smartphones.

---

<sup>24</sup> <https://securityinabox.org/en/guide/smartphones>

## 12.2 SMARTPHONE SECURITY GUIDELINES

### 12.2.1 Purses, Wallets, Smartphones

We have an intuitive understanding of the value of keeping our purse or wallet safe, because so much sensitive information is stored in them, and losing them will compromise our privacy and safety. People are less aware of the amount of personal information being carried in their smartphones, and consider losing a phone a nuisance rather than a risk. If you also think that a smartphone is a computing device which is always connected to a network and is continually carried around, it also highlights the important difference between a holder of discrete, passive information (like a wallet), and an active and interactive item like a smartphone.

*A simple exercise can help illustrate this:*

Empty the content of your wallet or purse, and take account of sensitive items. Typically you may find:

- Pictures of loved ones (~5 pictures)
- Identification cards (driver's license, membership cards, social security cards)
- Insurance and health information (~2 cards)
- Money (~5 bills)
- Credit/Debit cards (~3 cards)

Now, examine the contents of your smartphone. A typical smartphone user may find some of the above in higher quantities, and in some cases much more valuable items:

- Pictures of loved ones (~100 pictures)
- Email applications and their passwords
- Emails (~500 emails)
- Videos (~50 videos)
- Social networking applications and their passwords
- Banking applications (with access to the bank accounts)
- Sensitive documents
- Sensitive communication records
- A live connection to your sensitive information

The more you use smartphones, the more you need to become aware of the associated risks and take appropriate precautions. Smartphones are powerful amplifiers and distributors of your personal data. They are designed to provide as much connectivity as possible and to link to social networking services by default. This is because your personal data is valuable information that can be aggregated, searched and sold.

It can be disastrous if you lose your phone without having a backup of your most important data (such as your contacts) in a secure location. Besides backing up your data, make sure you also know how to restore the data. Keep a hard copy of the steps you need to take so you can do it quickly in an emergency.

In this chapter we'll start by introducing some smartphone basics – a description of various platforms and some basic setup procedures for securing your information and communication. The remaining parts of this chapter will cover specific precautions related to common uses of smartphones.

## **12.2.2 Platforms, Setup and Installation**

### **12.2.2.1 Platforms and Operating Systems**

At the time of writing, the most common smartphones in use are Apple's iPhone and Google's Android, followed by Blackberry and Windows phones. The key difference between Android and other operating systems is that Android is, mostly, an Open Source (*FOSS*) system, which allows the operating system to be audited independently to verify if it properly protects users' information and communication. It also facilitates development of security applications for this platform. Many security-aware programmers develop Android applications with user safety and security in mind. Some of these will be highlighted later in this chapter.

Regardless what type of smartphone you are using, there are issues that you should be aware of when you use a phone which connects to the internet and comes with features such as *GPS* or wireless networking capacities. In this chapter we focus on devices with the Android platform, because, as mentioned above, it's easier to secure data and communications. Nonetheless, basic setup guides and some applications for devices other than Android phones are provided, too. Blackberry phones have been presented as "secure" messaging and email devices. This is because messages and emails are securely channeled through Blackberry servers, out of the reach of potential eavesdroppers. Unfortunately, more and more governments are demanding access to these communications, citing need for guarding against potential terrorism and organised crime. India, United Arab Emirates, Saudi Arabia, Indonesia and Lebanon are examples of governments which have scrutinized the use of Blackberry devices and demanded access to user data in their countries.

### **12.2.2.2 Feature Phones**

Another category of mobiles are often called 'feature phones'. Recently, feature phones have increased their functionalities to include those of some smartphones. But generally, feature phones' operating systems are less accessible, therefore there are limited opportunities for

security applications or improvements. We do not specifically address feature phones, although many measures discussed here make sense for feature phones too.

#### **12.2.2.3 Branded and locked smartphones**

Smartphones are usually sold branded or locked. Locking smartphones means that the device can only be operated with one carrier, whose SIM card is the only one that will work in the device. Mobile network operators usually brand a phone by installing their own firmware or software. They may also disable some functionalities or add others. Branding is a means for companies to increase revenue by channelling your smartphone use, often also collecting data about how you are using the phone or by enabling remote access to your smartphone.

For these reasons, we recommend that you buy an unbranded smartphone if you can. A locked phone poses a higher risk since all your data is routed through one carrier, which centralises your data streams and makes it impossible to change SIM cards to disseminate the data over different carriers. If your phone is locked, ask someone you trust about unlocking it.

#### **12.2.2.4 General Setup**

Smartphones have many settings which control the security of the device. It is important to pay attention to how your smartphone is set up. In the Hands-on Guides below we will alert you to certain smartphone security settings that are available but not active by default, as well as those which are active by default and make your phone vulnerable.

#### **12.2.2.5 Installing and updating applications**

The usual way to install new software on your smartphone is to use the iPhone Appstore or Google Play store, log in with your user credentials, and download and install a desired application. By logging-in you associate your usage of the online store with the logged-in user account. The owners of the application store keep records of this user's browsing history and application choices.

The applications which are offered in the official online store are, supposedly, verified by store owners (Google or Apple), but in reality this provides weak protection against what applications will do after being installed on your phone. For example, some applications may copy and send out your address book after you install them on your phone. On Android phones each application needs to request, during the installation process, what it will be permitted to do when it is in use. You should pay close attention to what permissions are requested, and if these permissions make sense for the function of the app you are installing. For example, if you are considering a "news reader" application and you find out that it requests the rights to send your contacts over a mobile data connection to a third party, you

should look for alternative applications with appropriate access and rights.)ites. Some users may want to consider these alternative sites to minimize online contact with Google. One of the alternative store is **F-Droid** ('Free Droid'), which only provides *FOSS* applications. However please remember that you should trust the site before you download any apps from it. For inexperienced users we recommend that you use Google Play store.

If you don't want to (or are unable to) go online to access apps, you can transfer apps from someone else's phone by sending *.apk* files (short for 'android application package') via bluetooth. Alternatively you could download the .apk file to your device's Micro SD card or use a usb cable to move it there from a PC. When you have received the file, simply long tap on the filename and you will be prompted to install it. (**Note:** be especially careful while using Bluetooth.

### **12.2.3 Communicating Securely(Through Voice and Messages) with a Smartphone**

#### **12.2.3.1 Secure Voice Communication**

##### *Basic telephony*

In order to send or receive any calls or communications to your phone, the signal towers nearest you are alerted by your phone of its presence<sup>25</sup>. As a result of those alerts and communications the network service provider knows the precise geographic location of your mobile phone at any given time.

**About Anonymity:** If you are conducting sensitive phone conversations or sending sensitive SMS messages, beware of the above tracking 'feature' of all mobile phones. Consider adopting the steps below:

- Make calls from different locations each time, and choose locations that are not associated with you.
- Keep your phone turned off, with the battery disconnected, go to the chosen location, switch your phone on, communicate, switch the phone off and disconnect the battery. Doing this habitually, each time you have to make a call, will mean that the network cannot track your movements.
- Change phones and SIM cards often. Rotate them between friends or the second-hand market.

---

<sup>25</sup> <https://securityinabox.org/en/guide/mobile-phones>

- Use unregistered pre-paid SIM cards if this is possible in your area. Avoid paying for a phone or SIM cards using a credit card, which will also create a connection between these items and you.

**About eavesdropping:** Your phone can be set to record and transmit any sounds within the range of its microphone without your knowledge. Some phones can be switched on remotely and brought into action in this way, even when they look as though they are switched off.

- Never let people whom you don't trust get physical access to your phone; this is a common way of installing spying software on your phone.
- If you are conducting private and important meetings, switch your phone off and disconnect the battery. Or don't carry the phone with you if you can leave it where it will be absolutely safe.
- Make sure that any person with whom you communicate also employs the safeguards described here.
- In addition, don't forget that using a phone in public, or in places that you don't trust, makes you vulnerable to traditional eavesdropping techniques, or to having your phone stolen.

**About interception of calls:** Typically, encryption of voice communications (and of text messages) that travel through the mobile phone network is relatively weak. There are inexpensive techniques which third parties can use to intercept your written communications, or to listen to your calls, if they are in proximity to the phone and can receive transmissions from it. And of course, mobile phone providers have access to all your voice and text communications. It is currently expensive and/or somewhat technically cumbersome to encrypt phone calls so that even the mobile phone provider can't eavesdrop – however, these tools are expected to become cheaper soon. To deploy the encryption you would first have to install an encryption application on your phone, as well as on the device of the person with whom you plan to communicate. Then you would use this application to send and receive encrypted calls and/or messages. Encryption software is currently only supported on a few models of so-called 'smart' phones.

Conversations between Skype and mobile phones are not encrypted either, since at some point, the signal will move to the mobile network, where encryption is NOT in place<sup>26</sup>. Using Internet through your Smartphone over mobile data connections or WiFi can provide more secure ways to communicate with people, namely by using VoIP and employing means to secure this channel of communication. Some smartphone tools can even extend some of this security beyond VoIP, to mobile phone calls as well (See **Redphone** below).

*Here we list a few tools and their pros and cons:*

### **Skype**

The most popular commercial VoIP application, Skype, is available for all smartphone platforms and works well if your wireless connectivity is reliable. It is less reliable on mobile data connections.

Skype is a non Open-Source software what makes it very difficult to independently confirm its level of security. Additionally, Skype is owned by Microsoft, which has a commercial interest in knowing when you use Skype and from where. Skype also may allow law enforcement agencies retrospective access to all your communications history.

### **Other VoIP tools**

Using VoIP is generally free (or significantly cheaper than mobile phone calls) and leaves few data traces. In fact, a secured VoIP call can be the most secure way to communicate.

**RedPhone** is a Free and Open-Source Software application that encrypts voice communication data sent between two devices that run this application. It is easy to install and very easy to use, since it integrates itself into your normal dialing and contact scheme. But people you want to talk to also need to install and use RedPhone. For ease of use, RedPhone uses your mobile number as a way to identify you to your contacts. Unfortunately, this makes it more difficult to use RedPhone without a functioning mobile service plan, even on devices capable of using WiFi to connect to the Internet. RedPhone also uses a central server, which puts the administrators of the service in a powerful position by allowing them to see much of the meta-data related to your encrypted VoIP calls.

**CSipSimple** is a powerful VoIP client for Android phones that is well maintained and comes with many easy set-up wizards for different VoIP services.

---

<sup>26</sup> <https://securityinabox.org/en/guide/smartphones>

**Open Secure Telephony Network (OSTN)** and the server provided by the Guardian project, **ostel.co**, currently offers one of the most secure means to communicate via voice. Knowing and trusting the entity that operates the server for your VoIP communication needs is an important consideration.

When using CSipSimple, you never directly communicate with your contact, instead all your data is routed through the Ostel server. This makes it much harder to trace your data and find out who you are talking to. Additionally, Ostel doesn't retain any of this data, except the account data that you need to log in. All your speech is securely encrypted and even your meta data, which is usually very hard to disguise, is blurred since traffic is proxied through the ostel.co server. If you download CSipSimple from ostel.co it also comes preconfigured for use with ostel, which makes it very easy to install and use.

*Tool Guides* for CSipSimple and Ostel.co are forthcoming. In the meantime, more information can be found by following the links above.

#### **12.2.3.2 Sending Messages Securely**

You should use precautions when sending SMS and using instant messaging or chatting on your smartphone.

##### **SMS**

SMS communication is insecure by default. Anyone with access to a mobile telecommunication network can intercept these messages easily and this is an everyday occurrence in many situations. Don't rely on sending unsecured SMS messages in critical situations. There is also no way of authenticating SMS messages, so it is impossible to know if the contents of a message was changed during delivery or if the sender of the message really is the person they claim to be.

##### **Securing SMS**

**TextSecure** is a *FOSS* tool for sending and receiving secure SMS on Android phones. It works both for encrypted and non-encrypted messages, so you can use it as your default SMS application. To exchange encrypted messages this tool has to be installed by both the sender and the recipient of a message, so you will need to get people you communicate with regularly to use it as well. TextSecure automatically detects when an encrypted message is received from another TextSecure user. It also allows you to send encrypted messages to more than one person. Messages are automatically signed making it nearly impossible to tamper with the contents of a message. In our TextSecure hands-on guide we explain in detail the features of this tool and how to use it.

## **Secure Chat**

Instant messaging and chatting on your phone can produce a lot of information that is at risk of interception. These conversations might be used against you by adversaries at a later date. You should therefore be extremely wary about what you reveal when you are writing on your phone while instant messaging and chatting.

There are ways to chat and instant message securely. The best way is to use end-to-end encryption, as this will enable you to make sure the person on the other end is who you want.

We recommend ChatSecure as a secure text chat application for the Android phones. ChatSecure offers easy and strong encryption for your chats with *Off-the-Record* Messaging protocol. This encryption provides both authenticity (you can verify that you are chatting with the right person) and the independent security of each session so that even if the encryption of one chat session is compromised, other past and future sessions will remain secure.

ChatSecure has been designed to work together with Orbot, so your chat messages can be routed through the *Tor* anonymizing network. This makes it very hard to trace it or even find out that it happened.

For iPhones, the **ChatSecure** client provides the same features, although it is not easy to use it with the *Tor* network.

Whichever application you will use always consider which account you use to chat from. For example when you use Google Talk, your credentials and time of your chatting session are known to Google. Also agree with your conversation partners on not saving chat histories, especially if they aren't encrypted.

### **12.2.3.3 Storing Information on your Smartphone**

Smartphones come with large data storage capacities. Unfortunately, the data stored on your device can be easily accessible by third parties, either remotely or with physical access to the phone. You can take steps to encrypt any sensitive information on your phone by using specific tools.

#### ***Date Encryption Tools***

The **Android Privacy Guard (APG)** allows OpenGPG encryption for files and emails. It can be used to keep your files and documents safe on your phone, as well when emailing.

#### ***Recording Password Securely***

You can keep all your needed passwords in one secure, encrypted file by using **Keepass**. You will only need to remember one master password to access all the others. With Keepass you

can use very strong passwords for each account you have, as KeePass will remember them for you, and it also comes with a password generator to create new passwords. You can synchronise KeePass password databases between your phone and your computer. We recommend that you synchronise only those passwords that you will actually use on your mobile phone. You can create a separate smaller password database on the computer and synchronise this one instead of coping an entire database with all the passwords that you use to your smartphone. Also, since all the passwords are protected by your master password, it is vital to use very strong password for your KeePass database.

#### **12.2.3.4 Sending Email from your Smartphone**

In this section we will briefly discuss the use of email on smartphones. In the first instance, consider if you really need to use your smartphone to access your email. Securing a computer and its content is generally simpler than doing so for a mobile device such as a smartphone. A smartphone is more susceptible to theft, monitoring and intrusion.

If it is absolutely vital that you access your email on your smartphone, there are actions you can take to minimize the risks.

- Do not rely on smartphone as your primary means for accessing your email. Downloading (and removing) emails from an email server and storing them only on your smartphone is not advised. You can set up your email application to use only copies of emails.
- If you use email encryption with some of your contacts, consider installing it on your smartphone, too. The additional benefit is that encrypted emails will remain secret if the phone falls into wrong hands.

Storing your private encryption key on your mobile device may seem risky. But the benefit of being able to send and store emails securely encrypted on the mobile device might outweigh the risks. Consider creating a mobile-only encryption key-pair (using **APG**) for your use on your smartphone, so you do not copy your encryption private key from your computer to the mobile device. Note that this requires that you ask people you communicate with to also encrypt emails using your mobile-only encryption key.

#### **12.2.3.5 Capturing Media with your Smartphone**

Capturing pictures, video or audio with your Smartphone can be a powerful means to document and share important events. However, it is important to be careful and respectful of privacy and safety of those pictured, filmed or recorded. For example, if you take photos or record video or audio of an important event, it might be dangerous to you or to those who

appear in the recordings, if your phone fell into the wrong hands. In this case, these suggestions may be helpful:

- Have a mechanism to securely upload recorded media files to protected online location and remove them from the phone instantly (or as soon as you can) after recording.
- Use tools to blur the faces of those appearing in the images or videos or distort the voices of audio or videos recordings and store only blurred and distorted copies of media files on your mobile device.
- Protect or remove meta information about time and place within the media files.

**Guardian Project** has created a *FOSS* app called **ObscuraCam** to detect faces on photos and blur them. You can choose the blurring mode and what to blur, of course. Obscuracam also deletes the original photos and if you have set up a server to upload the captured media, it provides easy functionality to upload it.

#### **12.2.3.6 Accessing the Internet Securely from your Smartphone**

As discussed in our guide **How to keep your Internet communication private** and our guide **How to remain anonymous and bypass censorship on the Internet**, access to content on the Internet, or publishing material online such as photos or videos, leaves many traces of who and where you are and what you are doing. This may put you at risk. Using your smartphone to communicate with the Internet magnifies this risk.

##### ***Through Wi-Fi or Mobile Data***

Smartphones allow you to control how you access the Internet: via a wireless connection provided by an access point (such as an internet cafe), or via a mobile data connection, such as GPRS, EDGE, or UMTS provided by your mobile network operator.

Using a WiFi connection reduces the traces of data you may be leaving with your mobile phone service provider (by not having it connected with your mobile phone subscription). However, sometimes a mobile data connection is the only way to get online. Unfortunately mobile data connection protocols (like EDGE or UMTS) are not open standards. Independent developers and security engineers cannot examine these protocols to see how they are being implemented by mobile data carriers.

In some countries mobile access providers operate under different legislation than internet service providers, which can result in more direct surveillance by governments and carriers.

Regardless of which path you take for your digital communications with a smartphone, you can reduce your risks of data exposure through the use of anonymising and encryption tools.

### ***Anonymity of your Smartphone***

To access content online anonymously, you can use an Android app called **Orbot**. Orbot channels your internet communication through Tor's anonymity network.

Another app, Orweb, is a web browser that has privacy enhancing features like using proxies and not keeping a local browsing history. Orbot and Orweb together circumvent web filters and firewalls, and offer anonymous browsing.

### ***Proxies***

The mobile version of *Firefox* – **Firefox mobile** can be equipped with proxy add-ons, which direct your traffic to a proxy server. From there your traffic goes to the site you are requesting. This is helpful in cases of censorship, but still may reveal your requests unless the connection from your client to the proxy is encrypted. We recommend the **Proxy Mobile** add-on (also from **Guardian Project**, which makes proxying with Firefox easy. Is also the only way to channel Firefox mobile communications to Orbot and use the *Tor* network.

### **12.2.3.7 Advanced Smart Phone Security**

#### ***Get Full Access to your Smartphone***

Most Smartphones are capable of more than their installed operating system, manufacturers' software (firmware), or the mobile operators' programmes allow. Conversely, some functionalities are 'locked in' so the user is not capable of controlling or altering these functions, and they remain out of reach. In most cases those functionalities are unnecessary for smartphone users. There are however, some applications and functionalities that can enhance the security of data and communications on a smartphone. Also there are some other existing functionalities that can be removed to avoid security risks.

For this, and other reasons, some smartphone users choose to manipulate the various software and programs running the smartphone in order to gain appropriate privileges to allow them to install enhanced functionalities, or remove or reduce other ones.

The process of overcoming the limits imposed by mobile carriers, or manufacturers of operating systems on a smartphone is called rooting (in case of Android devices), or jailbreaking (in case of iOS devices, like iPhone or iPad). Typically, successful rooting or jailbreaking will result in your having all the privileges needed to install and use additional

applications, make modifications to otherwise locked-down configurations, and total control over data storage and memory of the smartphone.

**WARNING:** Rooting or jailbreaking may not be a reversible process, and it requires experience with software installation and configuration. Consider the following:

- There is a risk of making your smartphone permanently inoperable, or 'bricking' it (i.e. turning it into a 'brick').
- The manufacturer or mobile carrier warranty may be voided.
- In some places, this process maybe illegal.

But if you are careful, a rooted device is a straightforward way to gain more control over your smartphone to make it much more secure.

### *Alternative Firmwares*

Firmware refers to programmes that are closely related to the particular device. They are in cooperation with the device's operating system and are responsible for basic operations of the hardware of your smartphone, such as the speaker, microphone, cameras, touchscreen, memory, keys, antennas, etc.

If you have an Android device, you might consider installing a firmware alternative to further enhance your control of the phone. Note that in order to install alternative firmware, you need to root your phone.

An example of an alternative firmware for an Android phone is **Cyanogenmod** which, for example, allows you to uninstall applications from the system level of your phone (i.e. those installed by the phone's manufacturer or your mobile network operator). By doing so, you can reduce the number of ways in which your device can be monitored, such as data that is sent to your service provider without your knowledge.

In addition, Cyanogenmod ships by default with an OpenVPN application, which can be tedious to install otherwise. VPN (Virtual Private Network) is one of the ways to securely proxy your internet communication (see below).

Cyanogenmod also offers an Incognito browsing mode in which history of your communication is not recorded on your smartphone.

### ***Full Device Encryption***

If your phone is rooted you may consider encrypting its entire data storage or creating a volume on the Smartphone to protect some information on the phone.

**Luks Manager** allows easy, on-the-fly strong encryption of volumes with an user-friendly interface. We highly recommend that you install this tool before you start storing important data on your Android device and use the Encrypted Volumes that the Luks Manager provides to store all your data.

### ***Virtual Private Network(VPN) Security***

A VPN provides an encrypted tunnel through the internet between your device and a VPN server. This is called a tunnel, because unlike other encrypted traffic, like https, it hides all services, protocols, and contents. A VPN connection is set up once, and only terminates when you decide.

Note that since all your traffic goes through the proxy or VPN server, an intermediary only needs to have access to the proxy to analyze your activities. Therefore it is important to carefully choose amongst proxy services and VPN services. It is also advisable to use different proxies and/or VPNs since distributing your data streams reduces the impact of a compromised service.

## **ACTIVITIES**

1. Find out more about jailbreaking over internet.
2. Find and use the feature of “off-the –record” option in your chat application and observe what difference it makes.
3. Download and use Skype to make a video call to your friend.
4. Find out more about ***ObscuraCam*** over internet.

## **RECOMENDED VIDEOS**

<https://www.youtube.com/watch?v=KCObM4PBTvK>

<https://www.youtube.com/watch?v=V8bCyRCqK0k>

## References

- Barry M. Leiner, V. G. (s.j.). *Brief History of the Internet*. Onttrek Dec. 20, 2015 uit <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet> available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.
- Bunting, S., & Wei, W. (2006). *The Official EnCE: EnCase Certified Examiner Study Guide*. Wiley Publishing Inc.
- Castillo, F. (2007). *Reshipping Fraud - A Home Business Con*.
- C-DAC. (2014). *National Intelligence Grid : NATGRID*.
- CERT-In. (2014). *Indian Computer Emergency Response Team*.
- Chander, M. (2013). *National Critical Information Infrastructure Protection Centre (NCIIPC): Role, Charter & Responsibilities*.
- Chowdhury, S., Nair, S., & Johnson. (2008). *The curious case of Ken Haywood*. The Indian Express.
- Cone, M. (2011, Dec. 17). *How to Configure Your Mac's Firewall*. Onttrek Oct. 24, 2015 uit MACINSTRUCT: <http://www.macinstruct.com/node/165> available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.
- Cyber Crime Investigation Cell, Mumbai.* (s.j.). Onttrek Dec. 20, 2015 uit <http://cybercellmumbai.gov.in/>
- (2014). *CYBER CRIME, CYBER SECURITY AND RIGHT TO PRIVACY*. New Delhi: LOK SABHA SECRETARIAT.
- CYBER SECURITY MANIFESTO 2.0.* (2012, Oct. 01). Onttrek Sep. 26, 2015 uit cybersecuritymanifesto: <http://cybersecuritymanifesto.com/>
- Email tips.* (s.j.). Onttrek Oct. 29, 2015 uit Digital Survival: <https://survival.tacticaltech.org/internet/email/tips> available under a Creative Commons Attribution-Share Alike 3.0 Unported License.

Farberov, S. (2014). *Russian hackers attacked US financial system stealing gigabytes of data in suspected retaliation for Ukraine sanctions*. Mail Online.

Fisher, M. (2013). *Syrian hackers claim AP hack that tipped stock market by \$136 billion. Is it terrorism?* The Washington Post.

Gallagher, S. (2013, Oct. 02). *We are not who we are*. Onttrek Sep. 26, 2015 uit Security Blog: <https://securityblog.redhat.com/tag/two-factor-authentication/> available under a Creative Commons Attribution-ShareAlike 3.0 Unported License.

Glass, E. (2003). *The NTLM Authentication Protocol and Security Support Provider*. Onttrek Sep. 26, 2015 uit Sourceforge: <http://davenport.sourceforge.net/ntlm.html> available under permission by the owner to use, copy, modify, and distribute this document for any purpose and without any fee.

Gollin, G. (2003). *Unconventional University Diplomas from Online Vendors: Buying a Ph.D. University That Doesn't Exist*.

Gonsalves, A. (2014). *How hackers used Google to steal corporate data*. [www.infoworld.com](http://www.infoworld.com).

Gordon, S., & Ford, R. (2003). *Cyberterrorism?* Onttrek Dec. 20, 2015 uit <http://www.symantec.com/avcenter/reference/cyberterrorism.pdf>

(1998). How Email Works. In P. Grall, *How Internet Works* (bl. 85). Que Corporation.

Gupta, A. (2011, March 01). *Digital Forensic Analysis Using BackTrack, Part 1*. Onttrek Sep. 26, 2015 uit opensourceforu: <http://opensourceforu.efytimes.com/2011/03/digital-forensic-analysis-using-backtrack-part-1/> available under Creative Commons Attribution-NonCommercial 3.0 Unported License.

*Hacker (computer security)*. (Nov.). Onttrek Dec. 20, 2015 uit 2015: [http://en.wikipedia.org/wiki/Hacker\\_\(computer\\_security\)](http://en.wikipedia.org/wiki/Hacker_(computer_security)) available under the Creative Commons Attribution-ShareAlike License.

Havercan, P. (2015, July 17). *A plain person's guide to Secure Sockets Layer*. Onttrek Sep. 26, 2015 uit <http://peter.havercan.net/computing/plain-persons-guide-to-secure-sockets-layer.html> available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Hazen, S. (2014). *Hackers Used Police Tool to Steal Celeb Photos*. NEWSER.

*How do I know if a website is secure?* (2015, Oct.). Onttrek Oct. 29, 2015 uit ccm.net: <http://ccm.net/faq/2-how-do-i-know-if-a-website-is-secure> available under the Creative Commons Attribution - NonCommercial - ShareAlike 3.0 France license.

*How it works.* (2010, Jan. 17). Onttrek Sep. 26, 2015 uit Wikidot: <http://pychatter.wikidot.com/how-it-works> available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License.

*How to Choose an Internet Browser.* (s.j.). Onttrek Oct. 29, 2015 uit WikiHow: <http://www.wikihow.com/Choose-an-Internet-Browser> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License

*How to Clear Your Browser's Cache.* (s.j.). Onttrek Oct. 29, 2015 uit WikiHow: <http://www.wikihow.com/Clear-Your-Browser%27s-Cache> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License

*How to Reveal a Fake Facebook Account.* (s.j.). Onttrek Sep. 27, 2015 uit [www.wikihow.com](http://www.wikihow.com/Reveal-a-Fake-Facebook-Account): <http://www.wikihow.com/Reveal-a-Fake-Facebook-Account> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License

*How to Set up 2 Step Verification in Gmail.* (s.j.). Onttrek Oct. 24, 2015 uit WikiHow: <http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License

*How to Set up 2 Step Verification in Gmail.* (s.j.). Onttrek Oct. 29, 2015 uit <http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail> available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License.

*Introduction to Digital Forensics.* (2011, Nov. 16). Onttrek Sep. 28, 2015 uit Wikibooks: [https://en.wikibooks.org/wiki/Introduction\\_to\\_Digital\\_Forensics](https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics) available under the Creative Commons Attribution-ShareAlike License

ISFS. (2004, April). *Computer Forensics.* Onttrek Dec. 20, 2015 uit [http://www.isfs.org.hk/publications/ComputerForensics\\_part1.pdf](http://www.isfs.org.hk/publications/ComputerForensics_part1.pdf)

Kaur, R. P. (2013). Statistics of Cyber Crime in India: An Overview. *International Journal Of Engineering And Computer Science*, 2 (8).

*Kerberos Authentication.* (s.j.). Onttrek Sep. 26, 2015 uit Interactiva: <http://computers.interactiva.org/Security/Authentication/Kerberos/> available under a Creative Commons Attribution-ShareAlike 3.0 Unported License

Kessler, G. C. (2001, Sep.). *Steganography: Hiding Data Within Data*. Onttrek Dec. 20, 2015 uit <http://www.garykessler.net/library/steganography.html>

Kessler, G. C. (2005, Dec.). *The Role of Computer Forensics in Law Enforcement*. Onttrek Dec. 20, 2015 uit [http://www.garykessler.net/library/role\\_of\\_computer\\_forensics.html](http://www.garykessler.net/library/role_of_computer_forensics.html)

Kumar, M. (2014). *Xiaomi Phones Secretly Sending Users' Sensitive data to Chinese Servers*. The Hacker News.

Leung, C. (s.j.). *Binding a Corporate Information Protection Strategy*. Onttrek Dec. 20, 2015 uit <http://www.isfs.org.hk/publications/011009/Collins-CIO&CeO.pdf>

Lucas, I. (2009, July 10). *Password Guidelines*. Onttrek Oct. 24, 2015 uit Lockdown.co.uk: [http://www.lockdown.co.uk/?pg=password\\_guide](http://www.lockdown.co.uk/?pg=password_guide) available under a Creative Commons Attribution-ShareAlike 2.0 License

Madhya Pradesh State Cyber Police. (2013). *Recent Examples of Cyber Crime & E-Commerce Fraud Related Investigations in India*.

Mcafee. (2014). *Net Losses: Estimating the Global Cost of Cybercrime*. Santa Clara.

Mehnle, J. (2010, April 17). *Sender Policy Framework*. Onttrek Sep. 28, 2015 uit Openspf: <http://www.openspf.org/Introduction> available under Creative Commons CC BY-SA 2.5

Mrunal. (2012). *National Counter Terrorism Center (NCTC): Meaning, functions, Controversy*.

Nair, S. (2009). *Selected Case Studies on Cyber Crime*.

Nandanwar, R. (2013). *Case Study of Recent Examples of Cyber Crime and E-Commerce Fraud related Investigations involving IPR and Copyright Act*.

Narayan, V. (2013). *Mumbai bank hacked, Rs 2.4 crore siphoned off in 3 hours*. Mumbai: The Economic Times.

Nelson, B., Phillips, A., & Steuart, C. (2009). *Guide to Computer Forensics and Investigations*. Cengage Learning.

*Networking in Windows 7*. (s.j.). Onttrek Oct. 24, 2015 uit <http://www.utilizewindows.com/>: <http://www.utilizewindows.com/7/networking/452-working-with-windows-firewall-in-windows-7> available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

NK, V. (2015, Jan. 24). *A Peek into the Top Password Managers*. Onttrek Oct. 24, 2015 uit opensourceforu.com: <http://opensourceforu.efytimes.com/2015/01/peek-top-password-managers/> available under Creative Commons Attribution-NonCommercial 3.0 Unported License.

Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). *First Responders guide to Computer Forensic*. CERT Training and Education.

*Password Authentication Protocol*. (2015, July 17). Onttrek Sep. 26, 2015 uit WIKIPEDIA: [https://en.wikipedia.org/wiki/Password\\_Authentication\\_Protocol](https://en.wikipedia.org/wiki/Password_Authentication_Protocol) available under the Creative Commons Attribution-ShareAlike License.

Press Information Bureau. (2006). *India-US cyber security Forum - Fact Sheet*.

*PROTECT THE SENSITIVE FILES ON YOUR COMPUTER*. (s.j.). Onttrek Oct. 29, 2015 uit SECURITY IN-A-BOX: <https://securityinabox.org/en/guide/secure-file-storage> available under a Creative Commons Attribution-Share Alike 3.0 Unported License.

*PROTECT YOURSELF AND YOUR DATA WHEN USING SOCIAL NETWORKING SITES*. (s.j.). Onttrek Oct. 29, 2015 uit securityinabox.org: <https://securityinabox.org/en/guide/social-networking> available under a Creative Commons Attribution-Share Alike 3.0 Unported License.

PTI. (2013). <http://www.thehindu.com/news/national/govt-launches-crime-tracking-pilot-project/article4272857.ece>. The Hindu.

Quirk, S. (2014, Mar. 13). *Concordia Password Security Policy*. Onttrek Sep. 26, 2015 uit <http://kb.cu-portland.edu/Password+Security> available under a Creative Commons Attribution 3.0 License.

Ranger, S. (2014, June 09). *Organised cybercrime groups are now as powerful as nations*. Onttrek Dec. 20, 2015 uit <http://www.zdnet.com/organised-cybercrime-groups-are-now-as-powerful-as-nations-7000030323/>

*Recognise scam or hoax emails and websites.* (s.j.). Onttrek Sep. 27, 2015 uit <https://www.communications.gov.au/what-we-do/internet/stay-smart-online/your-identity/recognise-scam-or-hoax-emails-and-websites> available under a Creative Commons Attribution 3.0 International License.

Rocha, L. (2012, Dec. 21). *COMPUTER SECURITY INCIDENT HANDLING – 6 STEPS*. Onttrek Dec. 20, 2015 uit Count Upon Security: <http://countuponsecurity.com/2012/12/21/computer-security-incident-handling-6-steps/>

Rusen, C. A. (2014, Sep. 09). *How to start & use the Windows firewall with advance security*. Onttrek Oct. 24, 2015 uit DigitalCitizen: <http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advanced-security> available under Creative Commons Attribution-Noncommercial-Share Alike 4.0 International.

Rusen, C. A. (2014, Sep. 26). *How to Start & Use The Windows Firewall with Advanced Security*. Onttrek Oct. 29, 2015 uit <http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advanced-security> available under Creative Commons Attribution-Noncommercial-Share Alike 4.0 International.

*Selecting a strong password.* (2015, Sep. 10). Onttrek Sep. 26, 2015 uit Wordpress: <https://en.support.wordpress.com/selecting-a-strong-password/> available under a Creative Commons Sharealike license.

Shubert, A. (2011). *Cyber warfare: A different way to attack Iran's reactors*. CNN.

Singh, G., Sharma, A., Rampal, K., Kular, R., Gupta, S., Sarita, R., et al. (2013). *India Risk Survey 2013*. Pinkerton and Federation of Indian Chambers of Commerce and Industry (FICCI).

Srinath, B. J. (2006). *Cyber Security Awareness for Protection of National Information Infrastructure*. Dept. of Information Technology. Ministry of Communication & Information Technology, Govt. of India.

Stewart, W. (2000, Jan. 07). *How Email Works*. Onttrek Sep. 28, 2015 uit <http://www.livinginternet.com/>: <http://www.livinginternet.com/e/ew.htm> available under a Creative Commons Attribution Share Alike License

Swain, B. (2009, July). *What are malware, viruses, Spyware, and cookies, and what differentiates them?* Onttrek Dec. 20, 2015 uit <http://www.symantec.com/connect/articles/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them>

Talukder, M. i. (s.j.). *Free Antivirus*. Onttrek Oct. 29, 2015 uit [http://shaifulaueo.blogspot.in/p/free-antivirus\\_13.html](http://shaifulaueo.blogspot.in/p/free-antivirus_13.html) available under a Creative Commons Attribution 3.0 license.

*The Home Computer Security Centre*. (2009, july 10). Onttrek Oct. 29, 2015 uit <http://www.lockdown.co.uk>: [http://www.lockdown.co.uk/?pg=password\\_guide](http://www.lockdown.co.uk/?pg=password_guide) available under a Creative Commons Attribution-ShareAlike 2.0 License.

The Indian Express. (2008). *Latest terror mail traced to Mumbai college*. Mumbai: The Indian Express.

*The Invention of Internet*. (s.j.). Onttrek Dec. 20, 2015 uit <http://www.history.com/topics/inventions/invention-of-the-internet>

*The Telegraph*. (2015, Dec. 06). Onttrek Dec. 17, 2015 uit [http://www.telegraphindia.com/1151207/jsp/business/story\\_57045.jsp#.VnJcINJ95dg](http://www.telegraphindia.com/1151207/jsp/business/story_57045.jsp#.VnJcINJ95dg)

Times of India. (2009). *Another techie held for duping Brainvisa*. Pune: Times of India.

*Tips for buying online*. (2015, Oct. 02). Onttrek Oct. 29, 2015 uit Tips for buying online: <https://www.qld.gov.au/law/your-rights/consumer-rights-complaints-and-scams/consumer-advice-rights-and-responsibilities/tips-to-become-a-smarter-shopper/tips-for-buying-online/> available under a Creative Commons Attribution 3.0 Australia (CC BY) licence.

*Understanding Authentication*. (2008, Feb. 14). Onttrek Sep. 26, 2015 uit Go4Experts: <http://www.go4expert.com/articles/understanding-authentication-t8842/> available under Creative Commons with Attribution Required.

Urbas, G. (2012). Copyright, Crime and Computers: New Legislative Frameworks for Intellectual Property Rights Enforcement. *Journal of International Commercial Law and Technology*, 7 (1), 11-26.

US-CERT. (2014). *Backoff Point-of-Sale Malware:Alert (TA14-212A)*. United States Computer Emergency Readiness Team.

US-CERT. (2008). *Computer Forensics*. Onttrek Dec. 20, 2015 uit <https://www.us-cert.gov/sites/default/files/publications/forensics.pdf>

*USE MOBILE PHONES AS SECURELY AS POSSIBLE.* (s.j.). Onttrek Oct. 29, 2015 uit <https://securityinabox.org/en/guide/smartphones> available under a Creative Commons Attribution-Share Alike 3.0 Unported License.

Verma, D. (2012, Nov. 05). *How To Identify Fake Email And Trace Sender's Location*. Onttrek Sep. 27, 2015 uit <http://www.usethistip.com>: <http://www.usethistip.com/2012/11/how-to-identify-fake-email-and-trace.html> available under a Creative Commons Attribution 3.0 License.

*What Is A Software Patch?* (2013, Nov. 08). Onttrek oct. 29, 2015 uit OSSWATCH: <http://oss-watch.ac.uk/resources/softwarepatch> available under a Creative Commons Attribution-ShareAlike 4.0 International License.

*Working With Windows Firewall in Windows 7.* (s.j.). Onttrek Oct. 29, 2015 uit <http://www.utilizewindows.com>: <http://www.utilizewindows.com/7/networking/452-working-with-windows-firewall-in-windows-7>

Yasmeen, A. (2013). *Natgrid will deter terror*. The Hindu dated 15 Dec. 2013.

# **Notes**

## **Notes**

**978-93-84813-96-3**

# उत्तराखण्ड मुक्त विश्वविद्यालय, हल्द्वानी

## साइबर स्पेस

### 1.1 परिचय

21वीं शताब्दी की एक अत्यन्त महत्वपूर्ण खोज ने हमारे जीवन को सबसे ज्यादा प्रभावित किया है और वह खोज है इन्टरनेट। इन्टरनेट की निर्बाध पहुँच ने हमारे बात करने, गेम खेलने, कार्य करने, खरीद-फरोख्त करने, मित्र बनाने, संगीत सुनने, फिल्में देखने, खान-पान का सामान घर मंगाने, बिलों का भुगतान करने, अपने मित्रों और परिजनों को जन्म दिवस/तीज-त्यौहारों और शुभ अवसरों पर बधाई देने आदि के तरीकों को पूरी तरह बदल दिया है। कोई ऐसा कार्य-कलाप शायद ही बचा हो, जिसके लिए कोई ऐप न हो। इसने हमारे दैनिक जीवन को सुविधाजनक बना दिया है। टेलीफोन या बिजली के बिल भुगतान के लिए लम्बी-लम्बी कतारों में खड़े होना, बीते दिनों की बात हो गई है। अब हम अपने घर या ऑफिस से केवल एक बटन क्लिक करके यह काम कर सकते हैं। टेक्नॉलाजी के विस्तार ने इंटरनेट के इस्तेमाल के लिए कम्प्यूटर की आवश्यकता को भी समाप्त कर दिया है। अब हमारे पास इंटरनेट से चलने वाले स्मार्टफोन, पामटॉप आदि ऐसे यंत्र हैं, जिनसे हम अपने दोस्तों और परिवार से चौबीसों घण्टे जुड़े रह सकते हैं। इन्टरनेट ने हमारे रोजमरा के कार्यों को न केवल आसान बनाया है बल्कि यह इतना किफायती हो गया है कि हर मध्यमवर्गीय व्यक्ति की पहुँच के अन्दर आ गया है। कुछ समय पहले की ही तो बात है, जब हम आईएसडी (अन्तर्राष्ट्रीय काल) या एसटीडी कॉल करते वक्त पल्स-मीटर व पल्स गिनते रहते थे, कि कहीं बिल ज्यादा न आ जाए। कॉल बहुत महंगी थीं, आईएसडी और एसटीडी का उपयोग केवल अत्यंत अर्जेट मैसेज और वह भी तत्काल देने के लिए होता था और बांकी संदेश या सम्पर्क तो पत्रों के माध्यम से होता था, क्योंकि यह माध्यम अपेक्षाकृत काफी सस्ता था। इंटरनेट के माध्यम से न केवल बात करना सम्भव हो गया है बल्कि स्काइप, जीचैट जैसे लोकप्रिय एप्लीकेशन्स के उपयोग द्वारा बहुत कम कीमत पर अब वीडियो कान्फ्रैंसिंग भी की जा सकती है। एक घण्टे की वीडियो चैट का खर्चा स्पीड पोस्ट या कूरियर सेवा के जरिए एक पृष्ठ का दस्तावेज दिल्ली से बंगलौर भेजने की कीमत से भी कम आता है। यही नहीं हमारे उपयोग के कुछ विशिष्ट उपकरण भी इंटरनेट के जरिए चलाए जा सकते हैं। टेलीविजन

अब केवल लोकप्रिय धारावाहिक और फ़िल्में देखने का साधन मात्र नहीं रह गए हैं बल्कि इन्टरनेट का इस्तेमाल करके इन पर अब अपने मित्रों के साथ वीडियो चैट भी की जा सकती है। मोबाइल फोन पर बात करने के अलावा, नई से नई फ़िल्में भी देखी जा सकती हैं। हम कहीं भी हों, सभी से सम्पर्क में रह सकते हैं। काम—काजी माता—पिता अपने ऑफिस से अपने बच्चों पर नजर रख सकते हैं और उनके होमवर्क में मदद कर सकते हैं। कारोबारी एक बठन को विलक करके अपने कर्मचारियों, ऑफिस, दुकान आदि पर नजर रख सकते हैं। इन्टरनेट ने हमारे दैनिक कार्यों को अनेक तरीकों से आसान बना दिया है। कभी आपने सोचा है कि ये इन्टरनेट आया कहाँ से है? आइये, अब हम इन्टरनेट के सक्षिप्त इतिहास पर चर्चा करते हैं और यह जानने का प्रयास करते हैं कि इसकी खोज कैसे हुई, कैसे इसका इस सीमा तक विकास हुआ, कि इसके बिना हम अपने जीवन की कल्पना तक नहीं कर सकते।

### 1.1.1 इन्टरनेट का इतिहास

यह तो नहीं बताया जा सकता कि रूस और अमरीका के बीच शीतयुद्ध ने दुनिया को क्या दिया। लेकिन, इन्टरनेट एक ऐसी उपयोगी खोज अवश्य रही, जिसकी आधारशिला इस शीतयुद्ध के दौरान रखी गई। रूस ने 4 अक्टूबर, 1967 को दुनियां का पहला उपग्रह “स्पूतनिक” अन्तरिक्ष में छोड़ा (प्रक्षेपित)। यह निश्चय ही सोवियत रूस की अन्तरिक्ष पर विजय थी और इसके जवाब में, अमरीका के रक्षा विभाग के अनुसंधान संस्थान, एडवान्स रिसर्च प्राजेक्ट एजेंसी (एआरपीए यानि अर्पा) ने 1960 के दशक के प्रारम्भ में अर्पानेट (एडवान्स रिसर्च प्राजेक्ट एजेंसी नेट) लॉच (शुरू) करने की घोषणा की। यह परीक्षण के तौर पर बनाया गया एक नेटवर्क था। इसे इस तरह डिजाइन किया गया था कि बम से हमला होने पर यदि इस नेटवर्क की कोई नोड (गन्थि) रिस्पॉड (प्रत्युत्तर) करने में असफल रहे, तो भी कम्प्यूटर संचार व्यवस्था (कम्प्युनिकेशन) बनाए रखने के लिए नेटवर्क से जुड़े रहें। पैकिंग—स्थिरणिंग नेटवर्क वाले इस अर्पानेट से पहला संदेश, यूनिवर्सिटी ऑफ कैलीफोर्निया, लॉस एन्जिलिस (यूसीएलए) स्थित लियोनार्ड क्लीनरॉक प्रयोगशाला द्वारा भेजा गया था। आपको यह जानकर हैरत होगी कि इन्टरनेट पर भेजा गया पहला संदेश “लो” (एलओ) था। दरअसल, “लौगिन” शब्द भेजना चाहते थे, लेकिन शुरू के दो अक्षर “एल ओ” (लो) ही अपने गन्तव्य यानि स्टैनफोर्ड रिसर्च इन्स्टीट्यूट (एसआरआई) स्थित नोड (ग्रंथि) पर पहुँचे और इससे पहले कि अन्तिम तीन अक्षर (जीआईएन) गन्तव्य पर पहुंच पाते पल्सों में अनियमित अन्तराल (गिलच) की वजह से इन्टरनेट डाउन हो गया था। शीघ्र ही इस खामी को दूर कर लिया गया और संदेश सफलतापूर्वक फिर से भेज दिया गया।

अर्पानेट को संचार के नियम बनाने की अहम भूमिका सौंपी गई थी। उसे अर्पानेट पर कम्प्युनिकेशन (संदेशों के आदान—प्रदान) के लिए प्रोटोकोल तैयार करने थे। अपार्टनेट ने नेटवर्कों के नेटवर्क में अनेक

अन्य नेटवर्कों को जोड़ने से संबंधित प्रोटोकोल तैयार किए। इसके फलस्वरूप टीसीपी/आईपी प्रोटोकोल के सैट (सुइट्स) बनाए गए। इनमें उन नियमों को सपष्ट किया गया जिनके तहत अर्पनेट से जुड़कर संदेशों का प्रेषण/ग्रहण (कम्युनिकेशन) किया जा सकता था।

1986 में एनएसएफ (नेशनल साइंस फाउन्डेशन) बैकबोन की स्थापना की गई और एनएसएफ नेट स्थापित करने के लिए पांच विश्वविद्यालयों के कम्प्यूटिंग केन्द्रों को परस्पर कनेक्ट (जोड़ा) किया गया। इस नेट में शामिल होने वाले विश्वविद्यालय इस प्रकार थे :—

- प्रिंसटन विश्वविद्यालय—जॉनवोन नेशनल सुपर कम्प्यूटरसेंटर, जेवीएनसी
- कॉरनेल विश्वविद्यालय—कौरनेल थ्यौरी सेन्टर
- अरबाना—चैम्पेन रिथ्त इलिनॉइस विश्वविद्यालय—नेशनल सेन्टर फॉर सुपर कम्प्यूटर एप्लीकेशन्स, एनसीएसए
- कार्नेगी मैलॉन विश्वविद्यालय—पिट्स—बर्ग सुपर कम्प्यूटर सेन्टर, पीएससी
- जनरल एटोमिक्स सैन डिएगो सुपरकम्प्यूटर सेन्टर, एसडीएससी

अर्पनेट की जगह लेने वाला एनएफस्नैट 1990 तक काफी लोकप्रिय हो गया था और अर्पनेट को बंद कर दिया गया था। तब तक कई विश्वविद्यालय और युनाइटेड किंगडम जैसे देश अपना—अपना नेटवर्क स्थापित कर चुके थे। 1965 में नेशलन फिजिकल लेबोरेट्री ने पैकिंग—स्विंचिंग नेटवर्क का प्रस्ताव किया। मिशीगन एजूकेशनल रिसर्च इन्फॉर्मेशन ट्रिआड ने 1966 में मैरिट (एमईआरआईटी) नेटवर्क स्थापित किया। इसे मिशीगन राज्य और एनएसएफ ने धन और सहायता उपलब्ध कराई। फ्रान्स ने भी 1973 में साइक्लोडस (सीवाईसीएलएईएस) नामक अपना स्विचिंग—पैकिंग नेटवर्क तैयार किया।

अब अलग—अलग प्रोटोकोल पर काम करने वाले अनेक समानान्तर नेटवर्क बन चुके थे। वैज्ञानिक एक ऐसे सांझा स्टैन्डर्ड (मानक) की तलाश में थे जिसके द्वारा इन नेटवर्कों को आपस में कनेक्ट किया जा सके। 1978 में, टीसीपी/आईपी प्रोटोकोल के सैट बनाए गए और 1983 तक, अर्पनेट ने इन टीसीपी/आईपी प्रोटोकोल को अपना लिया था।

1981 में दो बड़े नेटवर्कों को परस्पर कनेक्ट किया गया। एनएफएस द्वारा कम्प्यूटर साइंस नेटवर्क (सीएसनेट) स्थापित कर इसे टीसीपी/आईपी प्रोटोकाल सेट का इस्तेमाल करके अर्पनेट से कनेक्ट कर दिया गया। अब तक नेटवर्क शोधार्थियों (रिसर्च कम्प्यूनिटी) में काफी लोकप्रिय हो चुका था और निजी क्षेत्र में भी इसमें रुचि दिखाने लगी थी। प्रारम्भ में एनएफएस में इन्टरनेट की स्पीड 56 केबिट्स/प्रति सेकंड थी, जिसे 1988 में मैरिट नेटवर्क, आईबीएम, एमसीए और मिशीगन राज्य के कनेक्ट हो जाने 1.5 एमबिट्स/सेकंड तक अपग्रेड कर दिया गया। इससे नेटवर्क के विस्तार में सहायता मिली।

उद्योग जगत को इस नेटवर्क की ताकत और खूबियों का अहसास होने पर वे भी इसका फायदा उठाने के लिए इसके विस्तार में सहयोग करने लगे। नेटवर्क ट्रैफिक को सुगम बनाने के लिए इन्टरनेट सेवा प्रदाता यानि इन्टरनेट सर्विस प्रोवाइडर (आईएसपी) भी इस क्षेत्र में आने लगे। 1991 तक एनएसएफ नेट का काफी विस्तार हो चुका था और इसकी स्पीड 45 एमबिट्स तक अपग्रेड की जा चुकी थी। अनेक कारोबारी आईएसपी बैकबोन सेवा उपलब्ध कराने लगे थे और ये उद्योग जगत में लोकप्रिय हो गए थे। नेटवर्क का वाणिज्यिक उपयोग सहज बनाने के लिए, 1995 में एनएसएफ नेट बंद कर दिया गया और अब कमर्शियल ट्रैफिक के लिए इन्टरनेट का उपयोग होने लगा।

अब पूरी दुनिया के अधिक से अधिक विश्वविद्यालय और अनुसंधान केन्द्र इन्टरनेट से जुड़ गए हैं। अब तक यह नेटवर्क काफी लोकप्रिय हो चुका था और 1991 में नेशनल रिसर्च एण्ड एजूकेशन नेटवर्क (एनईआरएन यानि नर्न) की स्थापना हुई तथा वर्ल्ड वाइड वेब का सपना साकार हो गया। आज जो इन्टरनेट हम इस्तेमाल करते हैं इसका श्रेय टिमबार्नर्स-ली को जाता है। इन्होंने ही की शुरुआत की थी। इसके चलते इन्टरनेट जगत में क्रान्ति आ गई।

सूचना के इस तंत्र का उपयोग करके, अब हम इन्टरनेट से कोई भी सूचना या जानकारी प्राप्त कर सकते हैं। ब्राउजर नाम का सॉफ्टवेयर भी विकसित हुआ और इसका उपयोग इन्टरनेट ब्राउज करने के लिए किया जाने लगा। इलिनॉइस विश्वविद्यालय के अनुसंधानकर्ताओं ने 1992 में इसे तैयार किया था और इसका नाम मोजाइक रखा था। आज हम इन्टरनेट ब्राउज करने के लिए इसी ब्राउजर का इस्तेमाल करते हैं।

### 1.1.1.1 इन्टरनेट एड्रेसेज

चूंकि इन्टरनेट से बहुत से उपकरण (डिवाइस) कनेक्ट रहते हैं। इसलिए यह आवश्यक हो जाता है कि ऐसा तंत्र (मैकेनिज्म) हो जो इन्टरनेट से जुड़े प्रत्येक डिवाइस को अनन्य रूप से पहचान सके। इसके अलावा इस डिवाइस को संभालने के लिए एक सेन्ट्रलाइज्ड सिस्टम भी होता है, जो यह सुनिश्चित करता है कि प्रत्येक डिवाइस की अलग पहचान हो अन्यथा नेटवर्क बनाने का उद्देश्य ही समाप्त हो जाएगा। यह कार्य एक सेन्ट्रलाइज्ड अथॉरिटी (प्राधिकरण) करता है। जिसे इन्टरनेट असाइन्ड नम्बर्स अथॉरिटी (आईएएनए) कहते हैं। जो प्रत्येक डिवाइस को एक युनीक (अनन्य) नम्बर देता है, जो आईपी (इन्टरनेट प्रोटोकोल) नम्बर कहलाता है। इस आईपी एड्रेस में 32 बिट वाले बाइनेरी (द्विचर) नम्बर होते हैं, जिन्हें चार अष्टकों (ऑकटेट) में विभाजित किया जाता है। प्रत्येक ऑकटेट में 8 बाइनेरी नम्बर होते हैं और इन ऑकटेट को डॉट (.) द्वारा अलग किया जाता है। आईपी एड्रेस का एक उदाहरण नीचे दिया गया है—

एक ऑक्टेट के प्रत्येक 8 बिट्स में दो बाइनरी वैल्यू अर्थात् 0 और 1 होती है। अतः प्रत्येक ऑक्टेट की न्यूनतम वैल्यू 0 और अधिकतम वैल्यू 256 अर्थात् 11111111 और कुल मिलाकर  $2^8=256$  अलग-अलग संचय (कॉम्बिनेशन) हो सकते हैं।

इस 32 बिट्स एड्रेस को याद रखना बड़ा मुश्किल है। आसानी से याद रखने और समझने के लिए इसे दाशमिक (डेसीमल) फार्मेट में व्यक्त किया जाता है। लेकिन यह दाशमिक केवल समझने के लिए ही है। कम्प्यूटर तो केवल बाइनरी फार्मेट ही समझता है। उपरोक्त आईपी ऐड्रेस को दाशमिक फॉर्मेट में इस प्रकार अभिव्यक्त किया जाता है :— 123.45.78.125

अलग-अलग क्लास बनाने और उन्हें अलग करने के लिए इन आक्टेट का उपयोग किया जाता है। आईपी ऐड्रेस दो भागों में होता है— नेटवर्क और होस्ट। नेटवर्क वाला भाग यह बताता है कि यह कौन सा नेटवर्क है और होस्ट वाला भाग उस नेटवर्क के डिवाइस को इंगित करता है। यह एड्रेस उसी तरह एक डिवाइस की पहचान करता है जिस तरह कि पोस्ट ऑफिस सिस्टम किसी मकान की। जैसे— सबसे पहले देश, फिर राज्य, जिला, पोस्ट ऑफिस और फिर कलस्टर/ब्लॉक और अन्त में मकान नम्बर। इन आईपी ऐड्रेस को आईपी रेन्ज की उपलब्धता के आधार पर पांच वर्गों (कैटेगरी) में रखा गया है।

#### तालिका 1 : आईपी ऐड्रेस के वर्ग

क्लास	ऐड्रेस रेजेंस	सपोर्ट
क्लास ए	1.0.0.1 से 126.255.255.254	हास्ट 127 नेटवर्क्स में से प्रत्येक पर 16 मिलियन होस्ट बिट्स को सपोर्ट करता है।
क्लास बी	128.1.0.1 से 191.255.255.254	16000 नेटवर्क्स में से प्रत्येक पर 65000 बिट्स को सपोर्ट करता है।
क्लास सी	192.0.1.7 से 223.255.254.254	21 मिलियन नेटवर्क में से प्रत्येक पर 254 होस्ट को सपोर्ट करता है।
क्लास डी	224.0.0.0 से 239.255.255.255	मल्टीकास्ट ग्रुप के लिए रिजर्व
क्लास ई	240.0.0.0 से 254.255.255.255.254	भविष्य में उपयोग अथवा अनुसंधान एवं विकास के लिए रिजर्व

आईएएनए ने पांच रीजनल (क्षेत्रीय) इन्टरनेट रजिस्ट्री (आर आई आर) को आईपी एड्रेस आबंटित करने का काम सौंपा है। इसके लिए इन्हें बहुत बड़ी संख्या में आईपी एड्रेस सौंपे गए हैं। ये रीजनल इन्टरनेट रजिस्ट्रियां अपने—अपने ज़ोन (क्षेत्र) में आईपी एड्रेस आबंटित करती हैं। इन आरआईआर का नाम और कार्य-क्षेत्र इस प्रकार है:—

- एपीएनआईसी— यह आरआईआर एशिया—प्रशान्त क्षेत्र के लिए कार्य करता है।
- एफ्रीएनआईसी— यह आरआईआर अफ्रीकी क्षेत्र के लिए कार्य करता है।
- एआरआईएन— यह आरआईआर उत्तरी अमरीका और अनेक कैरेबियन तथा उत्तरी अटलांटिक द्वीप समूहों के लिए कार्य करता है।
- एलएसीएनआईबी— यह आइरआईआर दक्षिणी अमरीका कैरेबियन द्वीपों के लिए कार्य करता है।

तथा

- आरआईपीई—एनसीसी— यह आरआईआर यूरोप, मध्यपूर्व एवं मध्य एशिया के कुछ भागों के लिए कार्य करता है। इन पांच आरआईआर के बीच सम्पर्क (लाइजन) और तालमेल के लिए एक संगठन बनाया गया है जिसे नम्बर रिसोर्स ऑर्गनाइजेशन (एनआरओ) कहा जाता है।

### 1.1.1.2 डीएनएस

जब भी हम इन्टरनेट पर कोई वेबसाइट ब्राउज करते हैं, हम धनवन्धनपद जैसा कोई नाम टाइप करते हैं पर शायद ही कभी 104.28.2.92 जैसा कोई आईपी एड्रेस टाइप करते हों। लेनिक यदि हम जजचरूध104.28.2.92 भी न्तर में टाइप करें तो भी हम उसी वेबपेज पर पहुँचेंगे। दरअसल, इसका कारण यह है कि हम संख्याओं की बजाए शब्दों में किसी नाम को आसानी से याद रख सकते हैं। इसके अलावा, आईपी एड्रेस समय बीतने पर बदलते भी रहते हैं और कुछ साइट्स ऐसी होती हैं जिनके अनेक आईपी एड्रेस हाते हैं। साथ ही, डाटा—पैक इन्टरनेट आईपी—एड्रेस के इस्तेमाल से ही भेजे जाते हैं। इसमें सर्वर का इस्तेमाल होता है जिसे डोमेन नेम सिस्टम (डीएनएस) कहते हैं जो इसे आसान बनाने के लिए अनुवाद (ट्रान्सलेशन) का काम करता है और हमें इन बदलते आईपी एड्रेसेज को यानि डीएनएस को याद नहीं रखना पड़ता। जब भी हम जजचरूधनवन्धनपद जैसा कोई एड्रेस टाइप करते हैं तो बैकग्राउन्ड में एक प्रक्रिया स्वयं शुरू हो जाती है जिसे जीएनएस नेम रिजॉल्यूशन कहते हैं। कम्प्यूटर हाल ही में विजिट की गई साइट्स का डीएनएस कैश (गुप्त भण्डार) में डाटाबेस रखता है। यदि, कोई साइट जिस पर आप जाना चाहते हैं, वह आपके स्थानीय कम्प्यूटर के डीएनएस डाटा बेस में नहीं है तो उसके मिलने की अगली सम्भावना, आपके इंटरनेट सर्विस प्रोवाइडर (आईएसपी) के डीएनएस सर्वर में होगी। आईएसपी के ये

डीएनएस सर्वर भी हाल ही म देखी गई साइटों के कैशे रखते हैं। यदि यह सूचना वहां भी नहीं मिलती है तो आईएसपी का डीएनएस सर्वर इसे रुट नेम सर्वर से प्राप्त करता है। रुट नेम सर्वर रुट जोन फाइलों को अन्य डीएनएस सर्वरों और इन्टरनेट पर अन्य क्लाइन्टों को प्रेषित करता है। रुट जोन फाइल यह बताती है कि डीएनएस टॉप-लेवल डोमेन (टीएलडी) के लिए अथॉरिटिव सर्वर कहां अवस्थित है। वर्तमान में, 13 रुट नेम सर्वर हैं:-

- ए— बेरीसाइन ग्लोबल रजिस्ट्री सर्विसेज,
  - बी— युनिवर्सिटी ऑफ कैलीफोर्निया, इन्फॉर्मेशन साइंस इन्स्टीट्यूट
  - सी— कोजेन्ट कम्प्यूनिकेशन्स
  - डी— युनिवर्सिटी ऑफ मैरीलैण्ड
  - ई— नासा एम्स रिवर्च सेन्टर
  - एफ— इन्टरनेट सिस्टम कन्सोर्टियम इन्कॉर्पोरेशन
  - जी— यूएस.डी. ओडी नेटवर्क इन्फॉर्मेशन सेन्टर
  - एच— यूएस. आर्मी रिसर्च लैब
  - आई— आटोनौमिका / नॉर्डनेट
  - जे— वेरीसाइन ग्लोबल रजिस्ट्री सर्विसेज
  - के— आरआईपीई एनसीसी
  - एल— आसीएएनएन
  - एम— वाइड (डब्ल्यू आई डी ई) प्रोजेक्ट

ये रुट नेम सर्वर प्रश्न (क्वैरी) को समुचित टॉप-लेवल डोमेन (टीएलडी) को भेजता है। रुट नेम सर्वर टीएलडी को तलाशने के लिए सबसे पहले यूआरएल के अंतिम भाग को रीड (पढ़ता) करता है। हमारे उदाहरण में यूआरएल जेजचरक्षूनवनंबण्पद है। इसका अन्तिम भाग ण्पद है। टीएलडी के कुछ उदाहरण ण्बवउएण्ड्रग्रुण ण्वतहए ण्पद आदि हैं। ये टीएलडी नेम सर्वर स्विच बोर्ड की तरह काम करते हैं और क्वैरी को प्रत्येक डोमेन द्वारा अनुरक्षित समुचित अथॉरिटेटिव नेम सर्वर को भेज (डॉयरेक्ट) देते हैं। ये अथॉरिटेटिव नेम सर्वर अन्य उपयोगी जानकारी के अलावा डीएनएस रिकॉर्ड भी रखते हैं। एड्रेस रिकॉर्ड टीएलडी नेमसर्वर आईएसपी के डीएनएस सर्वर के जरिए अनुरोध भेजने वाले होस्ट कम्प्यूटर को वापस भेज दिये जाते हैं। ये बीच के सर्वर इस आईपी एड्रेस का रिकॉर्ड अपने कैशे में सेव रखते हैं ताकि यदि ऐसा ही अनुरोध दुबारा प्राप्त हो तो उन्हें उक्त प्रक्रिया को फिर से न दोहराना पड़े। यदि इसी यूआरएल का अनुरोध दुबारा प्राप्त होता है, तो बेर्स्ट कम्प्यूटर का डीएनएस कैशे यूआरएल का आईपी एड्रेस स्वयं दर्शा देगा।

### **1.1.1.3 इन्टरनेट का बुनियादी ढांचा (इन्फ्रास्ट्रक्चर)**

जैसा कि नाम से पता चलता है, यह नेटवर्कों का एक नेटवर्क है यानि यह छोटे, मझौले और बड़े नेटवर्कों का एक व्यवस्थित समूह है। इससे एक तथ्य का साफ पता चलता है कि इन्टरनेट पर किसी एक का स्वामित्व नहीं है। यह सामूहिक सफलता का एक स्वयंसिद्ध उदाहरण है। आपके दिमाग में यह प्रश्न अवश्य ही कौंधता होगा कि सभी महाद्वीपों में फैला यह विशाल नेटवर्क बिना किसी समस्या के कैसे काम करता है। हाँ यह बिल्कुल सही है कि इतने विशाल नेटवर्क की निगरानी के लिए एक अन्तर्राष्ट्रीय निकाय की आवश्यकता पड़ी होगी, जो इस नेटवर्क में शामिल होने के लिए नियम, विनियम और प्रोटोकोल बनाएगी। इसीलिए, इन मुद्दों से निपटने के लिए 1992 में एक अन्तर्राष्ट्रीय संगठन का गठन किया गया, जिसे “दी इन्टरनेट सोसायटी” नाम दिया गया है।

अब हम इस पर चर्चा करेंगे कि इन्टरनेट किस प्रकार काम करता है। आपके द्वारा भेजी गई ई-मेल किसी अन्य देश/महाद्वीप में बैठे आपके मित्र के कम्प्यूटर पर कैसे प्राप्त होती है। जब आप इन्टरनेट पर कनेक्ट हुए बिना अपने लैपलॉप/डिस्कटॉप पर काम करते हैं तो आपके कम्प्यूटर अपने तक सीमित कम्प्यूटर की तरह काम करता है। लेकिन, जब भी आप अपने मॉडम का इस्तेमाल करके अपने इन्टरनेट सर्विस प्रोवाइडर (आईएसपी) को डायल करके इन्टरनेट से कनेक्ट होते हैं, तो आप उस नेटवर्क का हिस्सा बन जाते हैं। आईएसपी उस इन्टरनेट बैकबोन के लिंक की तरह काम करता है जिसके जरिए डाटा एक उपयोगकर्ता से दूसरे उपयोगकर्ता के बीच रुट होते हैं। आईएसपी नेटवर्क एक्सेस प्वाइन्ट्स (एनएपी) पर इन्टरनेट बैंक बोन से कनेक्ट होते हैं। विभिन्न क्षेत्रों में दूरसंचार से जुड़ी बड़ी कम्पनियां ये एनएपी उपलब्ध कराती हैं। एनएपी से एनएपी को डाटा रुट करने के लिए, ये दूरसंचार कम्पनियां विशाल बैक-बोन इन्फ्रास्ट्रक्चर स्थापित करती हैं और इनका अनुरक्षण करती हैं। इस बैक-बोन के एनएपी पर आईएसपी कनेक्ट रहते हैं। और इन आईएसपी का दायित्व स्थानीय स्तर पर नेटवर्क तैयार करना तथा इस नेटवर्क को मैनेज करना होता है। इसलिए जब आप मॉडम के जरिए इन्टरनेट डायल करते हैं तो स्थानीय आईएसपी के नेटवर्क से जुड़ जाते हैं, जो आगे एनएपी के माध्यम से आपको इन्टरनेट बैक-बोन से कनेक्ट कर देता है। आपका डाटा इस बैक-बोन के माध्यम से रुट होता है और उस गत्तव्य एनएपी को पहुंच जाता है, जहाँ आपके मित्र के नेटवर्क का आईएसपी मौजूद है। जैसे ही आपका मित्र अपने मॉडल के जरिए इन्टरनेट से कनेक्ट होता है, आपका डाटा आपके मित्र के कम्प्यूटर में पहुंच जाता है।

### **1.1.1.4 वर्ल्ड वाइड वेब**

कई बार हम इन्टरनेट और वर्ल्ड वाइड वेब अथवा इसके प्रचलित नाम “वेब” शब्द का उपयोग भी करते हैं। लेकिन वेब तो उन अनेक उपयोगिताओं में से एक है जो हमें इन्टरनेट के जरिए प्राप्त होती है।

इन्टरनेट द्वारा प्रदत्त कुछेक सेवाओं में ईमेल, यूजनेट, मैसेजिंग सेवा, एफटीपी आदि हैं। वैब पर कम्प्यूनिकेट करने और सूचनाओं के आदान-प्रदान के लिए भज्ज प्रोटोकोल का उपयोग किया जाता है। युनाइटेड किंगडम, के वैज्ञानिक टिम बार्नर्स-ली ने 1989 में सर्व (यूरोपियन डे रिसर्चेज न्यूकेलियर्स) में वेब का विकास किया था। इसमें वेब कन्टेन्ट (विषय वस्तु) तक पहुँचने के लिए प्रयुक्त सभी डिवाइस और सभी प्रकार की पब्लिक वेबसाइट शामिल हैं। सूचना साझा करने वाला एक मॉडल है, जो इन्टरनेट पर सूचनाओं के अदान-प्रदान के लिए विकसित किया गया है। एक वेबसाइट में अनेक वेबपेज होते हैं और ये वेबसाइट इन्टरनेट पर उपलब्ध रहती हैं। इन वेबपेजों पर टेक्स्ट, वीडियो, आडियो तथा पिक्चर फार्मेट में सूचनाओं का भण्डार उपलब्ध है। वेब ब्राउजर नाम के एप्लीकेशन सॉफ्टवेयर का इस्तेमाल करके इन वेब पेजों पर पहुँचा जा सकता है। इन्टरनेट एक्सप्लोरर, क्रोम, सफारी, फायरफाक्स आदि ऐसे ही कुछ प्रचलित ब्राउजर हैं। यह इन्टरनेट के बारे में और इसके कार्य करने के तरीके पर एक संक्षिप्त परिचय था। अब हम साइबर अपराधों पर चर्चा करेंगे।

## 1.2 साइबर अपराध (साइबर क्राइम)

### परिचय

इन्टरनेट 1960 के दशक में अस्तित्व में आया था। उस समय इसका उपयोग कुछेक वैज्ञानिकों, शोधकर्ताओं और रक्षा विभाग तक ही सीमित था। लेकिन इसके बाद से इन्टरनेट का उपयोग करने वालों की संख्या में जबर्दस्त विस्तार हुआ है। प्रारम्भ में कम्प्यूटर से जुड़े अपराध कम्प्यूटरों और इनके बुनियादी ढांचे को भौतिक नुकसान पहुँचाने तक सीमित थे। 1980 के दशक में कम्प्यूटरों को भौतिक नुकसान पहुँचाने की आपराधिक प्रवृत्ति दुर्भावनापूर्ण कोड यानि वायरस का इस्तेमाल करके कम्प्यूटर के कार्यकारण को बाधित (मैलफंक्शन) करने में बदल गयो। लेकिन इसका प्रभाव ज्यादा व्यापक नहीं था, क्योंकि इन्टरनेट का उपयोग केवल फ़िफेन्स सेट-अप, बड़ी अन्तर्राष्ट्रीय कम्पनियों और शोध संस्थानों तक ही सीमित था। 1996 में इन्टरनेट आम लोगों को सुलभ कराया गया और यह बहुत जल्दी उनमें इतना अधिक लोकप्रिय हो गया कि वे धीरे-धीरे इस पर पूरी तरह निर्भर हो गये। यहाँ तक कि इन्टरनेट ने जनसाधारण की जीवनशैली को ही बदल दिया। ग्राफिक यूजर इन्टरफ़ेस (जीयूआई) इस प्रकार लिखे गए थे यानि यूजर के लिए फ़ॉन्ट-एण्ड इस प्रकार तैयार गया था कि यूजर को यह सोचने की जरूरत ही नहीं थी कि इन्टरनेट किस प्रकार काम करता है। यूजर को तो केवल हाइपरलिंक पर क्लिक करना होता है या फिर नियत जगह पर अपनी अपेक्षित सूचना टाइप करनी होती है। वह यह सोचता ही नहीं है कि ये डाटा कहाँ स्टोर किए जाते हैं और इन्हें इन्टरनेट पर कैसे भेजा जाता है या इन्टरनेट पर कनेक्ट कोई अन्य व्यक्ति भी इस डाटा पैकेट तक पहुँच बना रहा है, अथवा इन्टरनेट द्वारा भेजे गए डाटा पैकेट से छेड़-छाड़ भी की जा

सकती है। अब कम्प्यूटर क्राइम केवल कम्प्यूटर को या कम्प्यूटर के कार्यकरण (फंक्शनिंग) को नुकसान पहुँचाने तक ही सीमित नहीं रह गया है, अब व्यक्तिगत हित और वित्तीय अपराधों के लिए भी इस तरह के कृत्य किए जा रहे हैं। ये कम्प्यूटर अपराध तेजी से बढ़ रहे हैं। हर एक सैकेन्ड में लगभग 25 कम्प्यूटर इस तरह के अपराधों के शिकार बन रहे हैं। 2013 तक लगभग 800 मिलियन यानि 80 करोड़ लोग इन कम्प्यूटर हमलों से प्रभावित हो चुके थे। सीईआरटी—इंडिया की रिपोर्ट के अनुसार 2011–13 के बीच लगभग 308371 भारतीय वेबसाइट हैकिंग का शिकार बनी थीं। अनुमान है कि साइबर हमलों की वजह से हर वर्ष लगभग 160 मिलियन डॉलर का नुकसान होता है। ज्यादातर मामलों की जानकारी ही नहीं मिलतीं, इसलिए कहा जा सकता है कि ये आंकड़े भी पूरी कहानी नहीं बताते।

15वीं लोकसभा में सूचना और संचार प्रौद्योगिकी मंत्रालय से संबद्ध स्थाई समिति की 2013–14 की रिपोर्ट के अनुसार, भारत दुनिया में इन्टरनेट का उपयोग करने वाला तीसरा सबसे बड़ा देश है और 20 जून 2011 में भारत में 100 मिलियन इन्टरनेट उपयोगर्ता थे तथा इनकी संख्या तेजी से बढ़ रही है। भारत में लगभग 22 मिलियन ब्रॉडबैन्ड कनेक्शन हैं और 134 बड़े इन्टरनेट सेवा प्रदाता (आईएसपी) हैं।

हम इस पर और आगे चर्चा करें कि इससे पहले हमें यह जान लेना चाहिए कि साइबर क्राइम (अपराध) है क्या?

साइबर क्राइम शब्द एक ऐसे गैर—कानून कृत्य को कहते हैं, जिसमें आपराधिक कृत्य को अंजाम देने के लिए कम्प्यूटर अथवा कम्प्यूटर उपकरण जैसे कि स्मार्टफोन, टेबलेट्स, पर्सनल डिजिटल असिस्टेंट्स (पीडीए) आदि का एकल या नेटवर्क के एक पार्ट के रूप में इस्तेमाल किया जाता है या इन्हें साइबर अपराध का लक्ष्य बनाया जाता है। विनाशक और आपराधिक सोच वाले व्यक्ति बदले की भावना, लालच अथवा अपनी मौज के लिए ऐसे कृत्य करते हैं।

### 1.2.1 साइबर अपराधों का वर्गीकरण

साइबर अपराधी उस संगठन के अन्दर का व्यक्ति भी हो सकता है, जिस संगठन पर साइबर हमला हुआ है या फिर उस संगठन से बाहर का भी हो सकता है। इस तथ्य के आधार पर साइबर अपराध (क्राइम) को दो वर्गों में बांटा जा सकता है।?

#### □ इनसाइडर अटैक:

किसी ऐसे व्यक्ति द्वारा कम्प्यूटर सिस्टम अथवा नेटवर्क पर हमला, जिसे सिस्टम तक पहुँच का अधिकार हो, इनसाइडर अटैक कहलाता है। आमतौर पर इस प्रकार का हमला ऐसे कर्मचारी या ठेकेदार द्वारा किया जाता है जो उस संगठन से असन्तुष्ट या नाराज हो। इनसाइडर अटैक का कारण बदला या लालच हो सकता है। चूंकि ऐसा व्यक्ति संगठन की नीतियों, प्रक्रियाओं, आईटी इन्फ्रास्ट्रक्चर (सूचना प्रौद्योगिकी ढांचा)

और सिक्यूरिटी सिस्टम की कमजोरियों से भलीभाँति वाकिफ होता है, इसलिए, वह व्यक्ति साइबर अटैक जैसा कृत्य आसानी से अंजाम दे सकता है। इसके अलावा अटैक करने वाले की नेटवर्क तक पहुँच होती है, इसलिए, इनसाइडर अटैकर (हमला करने वाला) महत्वपूर्ण एवं गोपनीय सूचना आसानी से चुरा सकता है, नेटवर्क आदि को क्रैश कर सकता है। ज्यादातर मामलों में इनसाइडर अटैक का कारण ऐसे व्यक्ति होते हैं, जिन्हें संगठन ने निकाल दिया हो या कोई ऐसा काम सौंप दिया हो जो उस संगठन की आईटी नीति के अनुरूप न हो। इससे अटैकर का कम्पनी की कमजोरी का पता चल जाता है। संगठन में आन्तरिक घुसपैठ खोजी प्रणाली, यानि इन्टरनल इन्ट्रयूजन डिटेक्शन सिस्टम (आईडीएस) स्थापित करके इस तरह के इनसाइडर अटैक की रोकथाम की जा सकती है।

#### □ एक्स्टर्नल अटैक :

यदि अटैकर को संगठन के किसी अन्दरुनी व्यक्ति ने यह कार्य सौंपा हो या किसी बाहरी व्यक्ति ने इस कृत्य को अंजाम दिया हो, इन दोनों ही मामलों में अटैकर संगठन से बाहर का व्यक्ति है, तो यह एक्स्टरनल अटैक कहलाएगा। साइबर अटैक के शिकार संगठन को वित्तीय नुकसान पहुँचने के अलावा उसकी प्रतिष्ठा को भी धक्का लगता है। ऐसे अटैकर (हमलाकर्ता) आमतौर पर बारीकी से जांच (स्कैन) करके जानकारी जुटाते हैं। अनुभवी नेटवर्क/सिक्यूरिटी एडमिनिस्ट्रेटर फायर-वॉल लॉग्स का सावधानीपूर्वक विश्लेषण करके एक्स्टरनल अटैक का पता लगा सकते हैं। इसके लिए वे फायरवॉल द्वारा सृजित (जनरेटेड) लॉग्स पर नियमित रूप से नजर रखते हैं। इसके साथ ही, एक्स्टर्नल अटैक पर नजर रखने के लिए इन्ट्रयूजन डिटेक्शन सिस्टम भी लगाए जाते हैं।

साइबर हमलों को अटैकर की महारत के स्तर के आधार पर स्ट्रक्चर अटैक और अनस्ट्रक्चर अटैक के रूप में भी वर्गीकृत किया जा सकता है। कुछ विद्वानों ने इन हमलों को एक्स्टर्नल अटैक (बाहरी हमले) के रूप में परिभाषित किया है, लेकिन ऐसे भी मामले सामने आए हैं जहां संगठन के किसी अन्दर के व्यक्ति ने यह कृत्य किया है। ऐसा तब होता है, जब कोई प्रतिस्पर्धी कम्पनी कुछ खास मुद्दों पर अपनी प्रतिद्वन्द्वी कम्पनी को भावी रणनीति (कार्यनीति) को जानना चाहती है। अटैकर सुनियोजित तरीके से एक कर्मचारी के तौर पर प्रतिद्वन्द्वी कम्पनी में अपनी पैठ बनाता है और अपेक्षित जानकारी हासिल करता है।

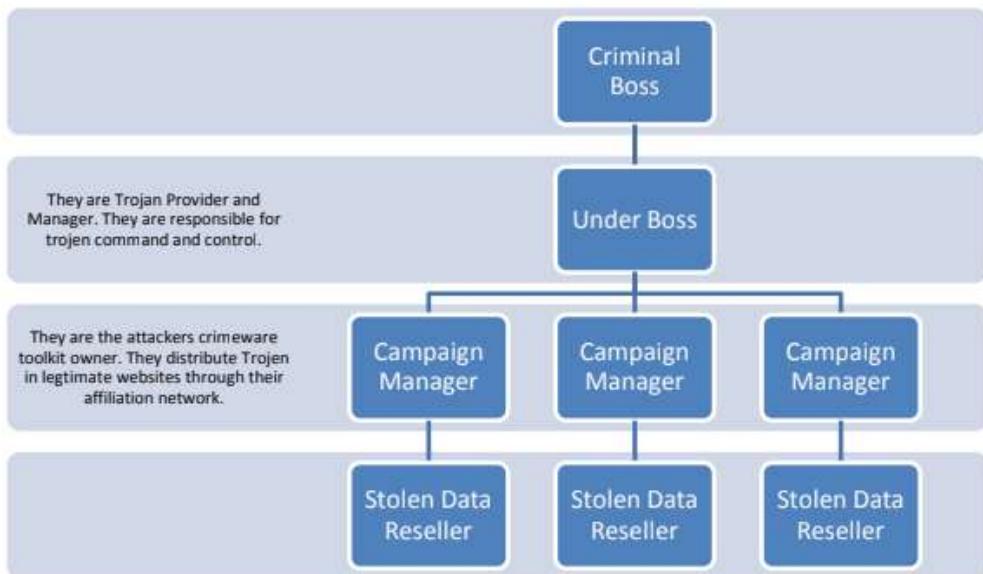
#### □ अनस्ट्रक्चर अटैक :

इस तरह के अटैक अनाड़ी (एमेच्यौर) अटैकर करते हैं। साइबर अटैक के पीछे इन लोगों की पूर्वनियत मंशा नहीं होती है। आमतौर ये अटैकर इन्टरनेट पर उपलब्ध टूल का परीक्षण करने के लिए किसी भी कम्पनी के नेटवर्क पर साइबर अटैक करते हैं।

## □ स्ट्रक्चर अटैक :

इस प्रकार के हमले अत्यन्त दक्ष और अनुभवी लोगों द्वारा किए जाते हैं और इन हमलों के पीछे उनकी मंशा पहले से तय होती है। इन लोगों के पास अत्याधुनिक टूल्स और प्रौद्योगिकी होती है जिसके उपयोग से ये किसी भी संस्थान के नेटवर्क में उस संस्थान के इन्टर्यूजन डिटेक्शन सिस्टम (आईईडी) की नजरों से बचकर सैन्ध लगा सकते हैं। इसके अलावा ये लोग मौजूदा टूल्स को अपने उद्देश्य के अनुसार अपग्रेड करने और नए टूल्स बनाने में दक्ष होते हैं। ये हमले पेशेवर अपराधियों द्वारा अंजाम दिए जाते हैं। कोई देश अपने प्रतिद्वन्द्वी देश पर, उनके राजनेताओं पर उनकी प्रतिष्ठा कम करने के लिए अटैक करा सकता है आतंकवादी और प्रतिद्वन्द्वी कम्पनियां आदि भी इन पेशेवर अपराधियों का उपयोग करती हैं।

साइबर अपराध कम खर्चीला है इसमें जोखिम भी कम है और मनमाफिक परिणाम भी मिलते हैं। आजकल ये स्ट्रक्चर्ड अपराध अत्यंत सुसंगठित गिरोहों द्वारा किए जाते हैं। औपचारिक संगठन की तरह ही इनका भी एक श्रेणीबद्ध (हीयरआर्कियल) संगठनात्मक सेट—अप होता है। कुछ संगठन तो ऐसे हैं जो तकनीकी क्षमता के क्षेत्र में विकसित देशों को भी टक्कर दे सकते हैं। ये संगठन वित्तीय संस्थानों, रक्षा संस्थानों और परमाणु प्रतिष्ठानों को अपना निशाना बनाते हैं। कुछ ऐसे संगठन भी हैं जो नशे का कारोबार करते हैं।



चित्र 1 : श्रेणीबद्ध संगठनात्मक ढांचा

इस सुसंगठित गिरोह में प्रत्येक सदस्य की भूमिका अवसर के आधार पर बदलती रहती है। यदि कोई हैकर किसी संगठन से संवेदी आंकड़े या जानकारी हैक कर लेता है तो वह अपने स्वयं के फायदे के लिए भी संगठन का वित्तीय शोषण कर सकता है। यदि हैकर के पास हैक करने (सेंध लगाने) की अपनी

तकनीकी क्षमता है तो वह स्वयं यह कार्य कर सकता है अन्यथा वह कोई ऐसा ग्राहक तलाशेगा जिसे इन आंकड़ों में रुचि हो और उसके पास तकनीकी विशेषता हो।

कई ऐसे साइबर अपराधी हैं जो अपनी सेवाएं देने के लिए तत्पर रहते हैं। कोई व्यक्ति, संगठन अथवा देश किसी संगठन की महत्वपूर्ण जानकारी चुराने के लिए अथवा अपने प्रतिद्वन्द्वी संस्थान की सेवाओं को बुरी तरह बाधित करने के लिए इन पेशेवर साइबर अपराधियों से सम्पर्क कर सकते हैं। अपने ग्राहक की जरूरत के अनुसार य हैकर मेलवेयर, वायरस आदि कोड करते हैं। साइबर अटैक से प्रभावित संगठन को न केवल वित्तीय नुकसान पहुँचता है बल्कि उसकी साख पर भी बुरा प्रभाव पड़ता है, प्रतिद्वन्द्वी संगठन निश्चय ही इसका फायदा उठायेगा।

### 1.2.2 साइबर क्राइम (अपराध) को बढ़ावा देने वाले कारण

ऐसे अनेक कारण हैं जो साइबर अपराधों की वृद्धि में उत्प्रेरक (फैटेलस्ट) की तरह काम करते हैं:-

(क) **पैसा**- आसानी से जल्दी से धन प्राप्त करने की लालसा भी साइबर अपराध को बढ़ावा देती है।

(ख) **बदला**- कुछ लोग अपने प्रतिद्वन्द्वी/संगठन/समाज/जाति अथवा धर्म से बदला लेने की भावना से उन्हें वित्तीय नुकसान पहुँचाने या उन्हें बदनाम करने अथवा भौतिक नुकसान पहुँचाने का प्रयास करते हैं। इस प्रकार का अपराध साइबर आतंकवाद की श्रेणी में आता है।

(ग) **मौज-मस्ती**:- अनाड़ी (एमेच्यौर) हैकर अपनी मौज-मस्ती के लिए साइबर अपराध करते हैं। वे इन्टरनेट पर मिले हैकिंग के नए टूल को जांचने के लिए भी ये अपराध करते हैं।

(घ) **गर्व**- यदि कोई डिफेन्स साइट्स अथवा नेटवर्क जैसे अत्यंत सुरक्षित नेटवर्क को हैक कर लें तो वह इसे गर्व की बात मानता है।

(ङ) **गुमनामी (एनोनिमिटी)**:- साइबर जगत (स्पेस) में गुमनामी की बहुत गुंजाइश है और यह गुमनामी कई साइबर अपराध के लिए व्यक्ति को प्रेरित करती है। साइबर जगत में गुमनाम बने रह कर अपराध को अंजाम देना आसान है, जबकि वास्तविक दुनियाँ में ऐसा करना मुश्किल है।

साइबर जगत में आपराधिक कृत्य के बाद बच निकलना वास्तविक दुनिया की तुलना में अपेक्षाकृत आसान है। गुमनामी की यह मजबूत भावना ऐसे लोगों को भी निहित स्वार्थ के लिए अपनी सारी नैतिकता भूल कर अपराध के लिए प्रेरित कर सकती है, जो अन्यथा एक सम्माजनक जीवन जी रहे थे।

(च) **साइबर गुप्तचरी (एस्पियोनेज)**:- कई बार सरकार स्वयं भी अन्य व्यक्तियों/नेटवर्क/देश पर नजर रखने के लिए साइबर घुस-पैठ (ट्रेसपासिंग) में शामिल रहती है। इसके कारण राजनीति, अर्थव्यवस्था, सामाजिकता आदि से प्रेरित हो सकते हैं।

### **1.3 मैलवेयर और इसके प्रकारः—**

मैलवेयर शब्द “मैलेसियम सॉफ्टवेयर” से बना है। इसे इस तरह डिजाइन किया जाता है कि इसे उपयोगकर्ता की जानकारी के बिना नेटवर्क में प्रवेश कराके कम्प्यूटर सिस्टम में स्थापित किया जा सकता है। यह किसी अन्य पक्ष के फायदे के लिए मेजबान (होस्ट) कम्प्यूटर में अवांछित दखललंदाजी करता है। ऐसे मेलवैयर्स की पूरी एक श्रृंखला है जो होस्ट मशीन के कार्यकरण को गम्भीर नुकसान पहुंचा सकते हैं। कम्प्यूटर के उपयोगकर्ता के कार्य में व्यवधान डालने/परेशान करने वाले साधारण मैलवेयर से लेकर अत्यंत जटिल मैलवेयर, जो होस्ट मशीन से महत्वपूर्ण जानकारी चारकर दूरदराज के सर्वर को भेजने में सक्षम हैं, जैसे अनेक मैलवयर हैं। इन्टरनेट पर अनेक प्रकार के मैलवेयर हैं। कुछ ज्ञात मैलवेयर इस प्रकार हैं:—

#### **1.3.1 एडवेयर**

यह एक विशेष प्रकार का मैलवेयर है, जो उपयोगकर्ता के सिस्टम पर जबरन विज्ञापन डिस्प्ले करता है। इस प्रकार के मैलवेयर किसी विज्ञापन पेज पर री-डाइरेक्ट कर देते हैं, या किसी विज्ञापन या आयोजन से संबंधित विज्ञापन पेज को बीच-बीच में पॉप-अप करते रहते हैं। इन एडवेयर्स को वे संस्थान पैसा मुहैया करते हैं, जिनके उत्पादों का विज्ञापन किया जा रहा है।

#### **1.3.2 स्पाइवेयर**

यह एक खास तरह का मैलवेयर है, जिसे उपयोगकर्ता की अनुमति से अथवा बिना अनुमति के लक्षित कम्प्यूटर में स्थापित (इन्स्टॉल) कर दिया जाता है और इसे लिखित मशीन से संवेदी सूचनाएं चुराने के लिए डिजाइन किया जाता है। ज्यादातर मामलों में यह उपयोगकर्ता की ब्राउजिंग हैबिट (आदतों) को जानकर और यह सूचना कम्प्यूटर के मालिक की जानकारी के बिना रिमोट सर्वर को भेजत है। ज्यादातर मामलों में यह देखा गया है कि इन्टरनेट से फ्रीवेयर यानि मुफ्त में मिलने वाले एप्लीकेशन प्रोग्राम डाउनलोड करते समय ऐसे स्पाइवेयर भी डाउनलोड हो जाते हैं। स्पाइवेयर कई प्रकार के होते हैं; ये होस्ट कम्प्यूटर की कुकीज पर नजर (ट्रैक) रख सकते हैं, ये बैंकिंग पासवर्ड और संवेदनशील सूचना आदि का पता लगाने के लिए की-लॉगर की तरह भी काम कर सकते हैं।

#### **1.3.3 ब्राउजर हॉइजैकिंग साफ्टवेयर**

कुछ ऐसे भी नुकसान-देय (मैलिसियस) साफ्टवेयर भी हैं जो इन्टरनेट पर उपलब्ध फ्री सॉफ्टवेयर के साथ डाउनलोड होकर उपयोगकर्ता (यूजर) की जानकारी के बिना उसके कम्प्यूटर में स्थापित हो जाते हैं।

इस तरह के सॉफ्टवेयर ब्राउजर की सैटिंग बदल कर लिंक को अवांछित साइट्स पर री-डाइरेक्ट करते हैं।

#### 1.3.4 वायरस

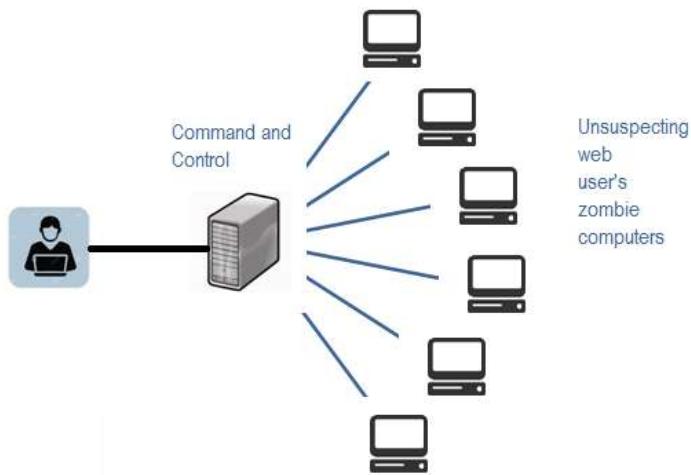
वायरस एक ऐसा मैलिसियस कोड है जो होस्ट कम्प्यूटर को नष्ट करने/नुकसान पहुँचाने के लिए तैयार किया जाता है। यह वायरस किसी फाइल को डिलीट कर सकता है या इसके साथ किसी बेकार फाइल को जोड़ सकता है, कोड की अनेक कॉपी (प्रतिलिपि) बनाकर कम्प्यूटर के मेमोरी स्पेस को भर सकता है, कम्प्यूटर को स्लो (धीमा) कर सकता है, होस्ट मशीन को फार्मेट कर सकता है, इत्यादि। वायरस ईमेल अटैचमेन्ट, पैन ड्राइव, डिजिटल इमेजेज, ई-ग्रीटिंग, ऑडियो अथवा वीडियो विलप्स आदि के माध्यम से एक मशीन से दूसरी मशीन में फैल सकता है। हो सकता है कि किसी कम्प्यूटर में वायरस हो पर यह स्वतः एकटीवेट नहीं हो सकता। यह तभी एकटीवेट होगा, जब उपयोगकर्ता एकजीक्यूटेबल फाइल (मगम) को एकजीक्यूट करेगा, इसीलिए होस्ट मशीन में वायरेस एकटीवेट नहीं किया जा सकता।

#### 1.3.5 वॉर्म्स

ऐसे भी कई वायरस हैं जो स्वतः रिप्लीकेट होने में सक्षम होते हैं। ये वायरस इस मायने में अलग होते हैं कि इन्हें नेटवर्क के जरिए ट्रेवल करने और संक्रमित मशीन से पूरे नेटवर्क में फैलने के लिए इन्सानी दखल की आवश्यकता नहीं पड़ती। वॉर्म्स आपरेटिंग सिस्टम की खामियों का फायदा उठाकर या ईमेल के द्वारा फैल सकते हैं। वॉर्म्स के नेटवर्क्स में प्रसार होने और इनके रिप्लीकेट होने से नेटवर्क के स्पेस और बैन्डविड्थ की खपत (कन्ज्यूम) बहुत होती और अन्ततः नेटवर्क चोक (जाम) होने लगता है।

#### 1.3.6 ट्रोजन हॉर्स

ट्रोजन हॉर्स एक ऐसा मैलीसियस कोड है जो एक उपयोगी सॉफ्टवेयर सा प्रतीत होता है लेकिन ऐसा है नहीं। यूजर धोखे में आकर किसी ऐसी लिंक को विलक करता है या ऐसी फाइल या सॉफ्टवेयर डाउनलोड कर लेता है, जो किसी वैध स्रोत से उपयोगी साफ्टवेयर जैसा प्रतीत होता है। यह ट्रोजन हॉर्स आंकड़ों से छेड़छाड़ करके न केवल होस्ट कम्प्यूटर को नुकसान पहुँचाता है बल्कि होस्ट कम्प्यूटर में चोर दरवाजा (बैकडोर) बनाकर इसका नियंत्रण एक रिमोट कम्प्यूटर को सौंप देता है। और इस तरह होस्ट कम्प्यूटर मैलीसियस कोड से संक्रमित कम्प्यूटरों के उस नेटवर्क यानि “बोटनेट” (रोबोट-नेटवर्क) का हिस्सा बन जाता है जिसका नियंत्रण एक सेन्ट्रल कन्ट्रोलर के हाथ में है।



चित्र 2 : बोटनेट

### 1.3.7 स्केअर वेयर

इन्टरनेट ने हमारे बात करने, खरीदारी करने और गेम खेलने के तौर-तरीके बदल दिए हैं। इसी तरह से इसने फिरौती के लिए लोगों को बधक बनाने के अपराधियों के तरीकों को भी बदल दिया है। इन्टरनेट सर्फ करते समय, अचानक एक पॉप-अप डिस्प्ले होता है जो उपयोगकर्ता के कम्प्यूटर में खतरनाक वायरस, स्पाइवेयर आदि होने की चेतावनी देता है। और इससे बचने के लिए साफ्टवेयर के पेड वर्जन को डाउनलोड करने की सलाह देता है। जैसे ही यूजर डाउनलोड करता ह, इसके साथ ही स्केअर वेयर नामक मैलिसियस कोड होस्ट कम्प्यूटर में डाउनलोड हो जाता है। यह स्केअर वेयर होस्ट कम्प्यूटर को बधक बना कर फिरौती की मांग करता है। इस मैलिसियस कोड को अनइन्स्टॉल नहीं किया जा सकता और जब तक फिरौती नहीं मिल जाती कम्प्यूटर काम नहीं करेगा। स्केअर-वेयर के मैसेज अलर्ट का एक नमूना नीचे चित्र-3 में दिया गया है:-



चित्र 3 : स्केअर वेयर द्वारा चेतावनी का नमूना

## **1.4 साइबर क्राइम के प्रकार**

विभिन्न प्रकार के साइबर अपराध इस प्रकार हैं:—

### **1.4.1 साइबर स्टॉकिंग**

इन्टरनेट/कम्प्यूटर के माध्यम से किसी का गुपचुप पीछा करने (स्टॉकिंग), परेशान करने अथवा धमकी देने जैसे कृत्य को साइबर स्टॉकिंग कहते हैं। बहुधा यह कृत्य किसी को बदनाम करने के लिए किया जाता है। चूंकि इन्टरनेट के इस्तेमाल से अपराधी अपनी पहचान छुपाने में सफल रहता है। अतः वह ईमेल, सोशल नेटवर्क, इन्स्टैट मैसेन्जर वबपोस्टिंग आदि के जरिए ऐसा कृत्य करता है। अपराधी झूठे आरोप लगाना, धमकियां देने, किशोरों के यौन उत्पीड़न, निगरानी आदि जैसे तरीके अपनाता है।

### **1.4.2 चाइल्ड पोर्नोग्राफी**

इसके अन्तर्गत अश्लील यौन—आचरण में रत कम उम्र (18 वर्ष से कम) के बच्चों के चित्र अथवा वोडियो रखना और प्रसारित करना शामिल हैं।

### **1.4.3. जालसाजी और जाली दस्तावेज बनाना (फोरजरी तथा काउन्टरफीटिंग)**

कम्प्यूटर का उपयोग करके जालसाजी करना और नकली दस्तावेज बनाना इस अपराध के अन्तर्गत आता है। हार्डवेयर और सॉफ्टवेयर क्षेत्र में प्रगति के चलते, जाली दस्तावेज तैयार करना बहुत आसान हो गया है। इस प्रकार बनाए गए जाली दस्तावेज हूब्हू मूल दस्तोवेज की तरह होते हैं। कोई विशेषज्ञ ही इनमें भेद कर सकता है।

### **1.4.4. साफ्टवेयर पायरेसी और आईपीआर से जुड़े अपराध**

व्यक्तिगत उपयोग या बिजनेस करने के लिए सॉफ्टवेयर की गरकानूनी तरीके से नकल तैयार करना सॉफ्टवेयर पायरेसी कहलाता है। यह आईपीआर उल्लंघन से जुड़े अपराधों की श्रेणी में आता है। आईपीआर (बौद्धिक सम्पदा अधिकार) उल्लंघन के अन्तर्गत गाने डाउनलोड करना, मूवी डाउनलोड करना आदि भी शामिल हैं।

### **1.4.5 सायबर टैररिज्म (आतंकवाद)**

राजनीतिक अथवा सामाजिक हित साधने के लिए सरकार को, नागरिकों को अथवा नागरिकों के किसी वर्ग को धमकाने अथवा अवपीड़ित करने के लिए कम्प्यूटर संसाधनों का इस्तेमाल करना सायबर आतंकवाद कहलाता है।

#### 1.4.6 फिशिंग

दूरसंचार के इलेक्ट्रॉनिक माध्यम में किसी प्रतिष्ठित संस्थान या साइट का छद्मवेश धारण करके, ईमेल के जरिए किसी की व्यक्तिगत एवं महत्वपूर्ण जानकारी हासिल करने की प्रक्रिया को फिशिंग कहते हैं। फिशिंग का उद्देश्य यूजरनेम, पासवर्ड और क्रेडिट कार्ड नम्बर आदि जैसी व्यक्तिगत सूचना चुराना होता है। इन सूचनाओं का इस्तेमाल यूजर के खाते से पैसा चुराने में किया जा सकता है। जानकारी प्राप्त करने के लिए टेलीफोन का इस्तेमाल किया गया है तो इसे “विशिंग” (वॉयस फिशिंग) कहा जाता है। फिशिंग का एक और रूप स्मिशिंग है। इसमें कस्टमर के लिए एसएमएस का उपयोग किया जाता है।

#### 1.4.7 कम्प्यूटर बैन्डलिज्म (बर्बरता)

भौतिक बल या नुकसानदायक कोड के जरिए कम्प्यूटिंग संसाधनों को ध्वस्त करने का कृत्य कम्प्यूटर बैन्डलिज्म कहलाता है।

#### 1.4.8 कम्प्यूटर हैकिंग

कम्प्यूटर के हार्डवेयर और सॉफ्टवेयर में बदलाव करने की प्रक्रिया को कम्प्यूटर हैकिंग कहते हैं। मशीन के मूल प्रयोजन के अलावा किसी और कार्य को निष्पादित करने के लिए यह कृत्य किया जाता है। कम्प्यूटर हैकिंग का उद्देश्य अपनी तकनीकी क्षमता का प्रदर्शन करने से लेकर सामाजिक, आर्थिक अथवा राजनीतिक कारणों की वजह से सूचना चुराने, सूचना में बदलाव करने और सूचना विनष्ट करने आदि तक कुछ भी हो सकता है। अब उद्योग जगत भी हैकर्स की सेवाएं लेने लगा है। कम्प्यूटर हैकिंग के काम में नियुक्त व्यक्ति कम्प्यूटर सिस्टम की सुरक्षा संबंधी कमजोरियों का पता लगाने और इन्हें दुरुस्त करने के लिए इरादतन कम्प्यूटर हैक करता है।

हैकर्स को निम्नानुसार वर्गांकृत किया जा सकता है:-

##### □ व्हाइट हैट :

व्हाइट हैट हैकर्स उन व्यक्तियों को कहते हैं जो सिस्टम की सुरक्षा कमजोरियों का पता लगा कर संस्थान को बताते हैं ताकि बाहरी हैकरों से सिस्टम, को बचाने के लिए यथोचित कदम उठाए जा सकें। व्हाइट हैट हैकर उस संस्थान का कर्मचारी भी हो सकता है जिसे यह काम सौंपा गया है या फिर कोई

ऐसा व्यक्ति भी हो सकता है जो हैकिंग के क्षेत्र में अपनी दक्षता दिखाना चाहता हो। ऐसे लोगों को ऐथिकल हैकर कहा जाता है।

#### □ ब्लैक हैट :

इसके विपरीत, ब्लैक हैट हैकर्स गलत इरादे से सिस्टम हैक करते हैं। ये हैकर्स सामाजिक, आर्थिक अथवा राजनीतिक हित साधन के लिए सिस्टम हैक कर सकते हैं। ये लोग सिस्टम की सुरक्षा संबंधी खामियों का पता लगाकर तब तक उस संस्थान या संगठन का अपने या अपने संगठन के फायदे के लिए दोहन/शोषण करते रहते हैं जब तक कि हैकिंग के शिकार संगठन को इसकी जानकारी न मिल जाये और वह अपने सिस्टम की सुरक्षा को दुरुस्त न कर ले। ब्लैक हैट हैकर्स को आमतौर पर क्रैकर्स कहा जाता है।

#### □ ग्रे हैट :

ग्रे हैट हैकर्स सुरक्षा खामियों का पता लगाकर साइट के एडमिनिस्ट्रेटर को सूचित करते हैं और सुरक्षा खामी को दुरुस्त करने की पेशकश करते हैं और बदले में परामर्शशुल्क या पारितोषिक की अपेक्षा रखते हैं।

#### □ ब्ल्यू हैट :

ब्ल्यू हैट हैकर वह व्यक्ति होता है जिसका कम्प्यूटर सिस्टम की सुरक्षा की देखभाल करने वाली फर्म से कोई नाता नहीं होता है बल्कि सिस्टम लॉच करने से पहले इसके बग—टेस्ट के लिए इसकी सेवाएं ली जाती हैं जो सिस्टम की सुरक्षा को भेदता है ताकि इन सुरक्षा कमजोरियों को दूर किया जा सके।

### **1.4.9 वायरस बनाना और इन्हें इन्टरनेट के जरिए फैलाना :**

किसी संगठन के कम्प्यूटर सिस्टम में वायरस के प्रसार से उसे कारोबारी और वित्तीय नुकसान उठाना पड़ सकता है। सिस्टम की मरमत कराने का खर्च, सिस्टम डाउन रहने के दौरान कारोबार को हुए नुकसान की लागत, अवसर हाथ से निकल जाने पर हुआ नुकसान ये सभी वित्तीय नुकसान में शामिल हैं। संगठन अपने नुकसान के बराबर या इससे अधिक की धनराशि की भरपाई के लिए हैकर पर कूननी कार्रवाई कर सकता है।

### **1.4.10 स्पैमिंग**

इन्टरनेट के जरिए थोक में अवांछित और वाणिज्यिक संदेश (मैसेज) भेजना स्पैमिंग कहलाता है। यदि निम्नलिखित लक्षण किसी ई—मेल में नजर आएं तो इस ईमेल को स्पैम की श्रेणी में रखा जा सकता है:-

(क) मासमेलिंग:- यह ई—मेल किसी एक व्यक्ति को नहीं बल्कि अनेक व्यक्तियों को भेजी जाती है।

(ख) एनोनिमिटी:- भेजने वाले की पहचान गुप्त रहती है।

(ग) अनसोलिसिटेडः— ऐसी ईमेल का ना तो इन्तजार रहता है और ना ही इसके लिए कोई अनुरोध किया गया होता है।

ऐसी ई-मेल से प्राप्तकर्ता परेशान ही नहीं होता बल्कि इनसे नेटवर्क भी आवरलोड होता और है मेलबॉक्स भी चोक होने लगता है।

#### **1.4.11 क्रॉस साइट स्क्रिप्टिंगः—**

इस प्रक्रिया में किसी भरोसेमंद वेबसाइट में उसी की तरह तैयार की गई वेबसाइट को मिला दिया जाता है। जैसे ही उपयोगकर्ता इस नुकसानदेय स्क्रिप्ट को विलक करता है, यह स्क्रिप्ट कुकीज तक पहुंच कर संवेदी (सेन्सिटिव) जानकारी चुरा कर रिमोट सर्वर को भेज देती है। अब इस जानकारी से वित्तीय फायदे या अपने हित के लिए उस सिस्टम का प्रयोग करना आसान हो जाता है।

#### **1.4.12 ऑनलाइन ऑक्सन (नीलामी) फ्रॉड**

इन्टरनेट पर ऑनलाइन ऑक्सन की सुविधा देने वाली कई प्रामाणिक वेबसाइट्स हैं। इन वेबसाइट्स की प्रतिष्ठा का फायदा उठाकर कुछ सायबर अपराधी ग्राहकों को ऑनलाइन ऑक्सन की जाली स्कीमों से फंसाते हैं इसका परिणाम यह निकलता है कि या तो ग्राहक उत्पाद का अधिक भुगतान करता है या फिर भुगतान हो जाने पर सामान डिलीवर ही नहीं होता।

#### **1.4.13 सायबर स्क्वाटिंग**

किसी अन्य के ट्रेडमार्क के डोमेन नाम को अपने लिए आरक्षित (रिजर्व) करने और बाद में ट्रेडमार्क के स्वामित्व वाले संस्थान को ऊंची कीमत पर उसे बेचने के इरादे से यह कृत्य किया जाता है।

#### **1.4.14 लॉजिक बौम्ब**

ये वो मैलिसियस (नुकसान देय) कोड हैं, जिन्हें वैध (युक्ति संगत) साफ्टवेयर में प्रविष्ट (इन्सर्ट) कर दिया जाता है और नुककान पहुँचाने का कार्य तब शुरू करता है, जब निर्धारित शर्त (लॉजिक) पूरी होनी हो। साफ्टवेयर के उपयोग दौरान आगे चल कर जब भी कोड के लिए निर्धारित लॉजिक सम्पन्न होगा, यह मैलासियस कोड अपना कार्य शुरू कर देगा। और सिस्टम में सुरक्षित सूचना नष्ट कर देगा और सिस्टम को नाकाम बना देगा।

#### **1.4.15 वेब जैकिंग**

हैकर राजनीतिक, आर्थिक या सामाजिक हित साधन के उद्देश्य से किसी संस्थान की वेबसाइट को हैक करके या तो इसे ब्लॉक कर देता है या इसमें बदलाव कर देता है। शिक्षण संस्थानों की वेब साइट्स को पाकिस्तानी हैकर्स द्वारा हैक करके इनके होम पेज पर पाकिस्तानी झाण्डे से युक्त एक एनीमेशन चित्र लगा देना, वेब जैकिंग के हालिया उदाहरण हैं। 2014 में भारत के स्वतंत्रता दिवस के अवसर पर भारतीय हैकरों

ने पाकिस्तान रेलवे की वेबसाइट को हैक करके इसके होम पेज पर भारतीय ध्वज डिस्प्ले कर दिया था जो कई घण्टों तक इस होमपेज पर बना रहा। यह भी वेब जैकिंग का एक और उदाहरण है।

#### 1.4.16 इन्टरनेट टाइम थैफ्ट्स

किसी व्यक्ति के इन्टरनेट सर्विस प्रोवाइडर (आईएसपी) या यूजरनेम और पासवर्ड हैक करके उस व्यक्ति के खर्च पर इन्टरनेट सर्फ करना इन्टरनेट टाइम थैफ्ट कहलाता है।

#### 1.4.17 डिनायल ऑफ सर्विस (सेवाएं बाधित करना) अटैक

यह एक ऐसा सायबर अटैक (हमला) है, जिसमें नेटवर्क पर बेकार के ट्रैफिक की बाढ़ लाकर इसे जाम कर दिया जाता है और इस तरह आवश्यक नेटवर्क ट्रैफिक के प्रवाह को रोक दिया जाता है।

#### 1.4.18 सलामी अटैक

इस तरह के अटैक में अत्यन्त छोटे-छोटे टुकड़ों में अटैक किया जाता है और जब अन्त में इन सब को मिला कर जोड़ा जाता है तो यह एक बड़ा नुकसान बन चुका होता है। ये क्रमिक अटैक इतने छोटे होते हैं कि प्रायः नजरन्दाज हो जाते हैं। सलामी अटैक का एक उदाहरण है— किसी व्यक्ति की ऑनलाइन बैंकिंग में सेंध (एक्सेस) लगा कर इतनी छोटी-छाटी धनराशि चुराना कि जिसे खाते का मालिक (वह व्यक्ति) नोटिस ही न कर पाए। बहुधा बैंकिंग वेबसाइट में डिफाल्ट ट्रिगर सेट होता है और एक निश्चित सीमा से कम के लेनदेन की जानकारी खाताधारक को नहीं दी जाती। मान लो कि तय सीमा एक हजार रुपये है तो इससे कम के विझॉल की जानकारी खाताधारक को नहीं मिलेगी। और यदि 1000 रु. कि राशि क्रमिक रूप से चुराई जा रही है तो कुछ समय बाद कुल मिलाकर उसके खाते से एक बड़ी राशि निकल चुकी होगी।

#### 1.4.19 डाटा डिडलिंग

आंकड़ों को कम्प्यूटर सिस्टम में ऐन्टर (प्रविष्ट) करने से पहले इन्हें बदलने की प्रक्रिया को डाटा डिडलिंग कहते हैं। बहुधा, डाटा प्रोसेसिंग की प्रक्रिया पूरी होने के बाद मूल डाटा (आंकड़े) पुनः रिप्लेस कर दिए जाते हैं। उदाहरण के लिए, वेतन गणना के लिए किसी व्यक्ति के डीए अथवा मूलवेतन को उस व्यक्ति के पे-रोल (वेतन शीट) में बदल दिया जाता है। वेतन की गणना और उस व्यक्ति के खाते में इसके पहुंचने के बाद कल वेतन के स्थान पर उसके वास्तविक वेतन को रिप्लेस कर दिया जाता है।

#### 1.4.20 ईमेल स्फूर्फिंग

इस प्रक्रिया में किसी ई-मेल की हैडर इन्फोर्मेशन (शीर्ष पर अंकित सूचना) को बदल दिया जाता है ताकि ई-मेल के मूल स्रोत (ओरिजिनल सोर्स) का पता न लगे और प्राप्तकर्ता को यह इस रूप में प्राप्त होती है कि यह ई-मेल मूल ओरिजिनल सोर्स से नहीं बल्कि किसी अन्य सोर्स से आई है।

## साइबर सुरक्षा की तकनीकें

साइबर सुरक्षा पर हमले से निपटने के लिए साइबर सुरक्षा की अनेक तकनीकें हैं।

### 2.1 प्रमाणीकरण (अर्थाँटिकेशन)

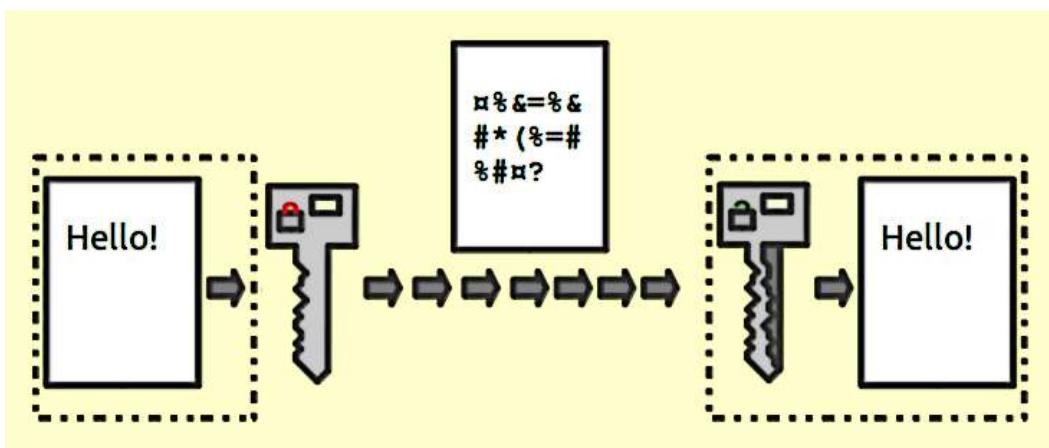
यह किसी व्यक्ति की पहचान जानने की एक प्रक्रिया है, ताकि यह सुनिश्चित किया जा सके कि यह वही व्यक्ति है जैसा कि उसने अपने आप को बताया है। इन्टरनेट पर प्रमाणीकरण का एक खास तरीका यूजरनेम और पासवर्ड है। इन्टरनेट पर यूजरनेम और पासवर्ड चुराकर साइबर अपराधों को अंजाम देने के मामलों में बढ़ोत्तरी को देखते हुए, संस्थानों ने वन टाइम पासवर्ड (ओटीपी) जैसे प्रमाणीकरण की अतिरिक्त व्यवस्था की है। जैसा कि नाम से ही स्पष्ट है, यह पासवर्ड केवल एक बार ही प्रयुक्त होता है और यह पासवर्ड यूजर को उसके उस मोबाइल/ईमेल एड्रेस पर एसएमएस अथवा ईमेल के जरिए भेजा जाता है, जो उसने पंजीकरण (रजिस्ट्रेशन) प्रक्रिया के दौरान दर्ज कराया है। इसे टू-फैक्टर अर्थाँटिकेशन (दोहरी प्रमाणीकरण प्रक्रिया कहते हैं। इसमें किसी व्यक्ति को प्रमाणित करने के लिए दो प्रकार के सबूतों की आवश्यकता होती है। इसका उद्देश्य प्रमाणीकरण के लिए सुरक्षा की एक अतिरिक्त पर्त (लेयर) की व्यवस्था करना है। टू-वे अर्थाँटिकेशन की कुछ अन्य प्रचलित तकनीकें हैं:- बायोमैट्रिक डाटा, फिजिकल टोकन आदि। यूजरनेम और पासवर्ड के साथ ही जोड़कर इन तकनीकों का प्रयोग किया जाता है।

आज से लगभग 15 वर्ष पहले कारोबार करने का जो तरीका था, बहुराष्ट्रीय संगठनों ने उसे बदल दिया है। इसे देखते हुए प्रमाणीकरण का महत्व और बढ़ गया है। इनके कार्यालय दुनिया के अलग देशों में हैं। इनका कोई कर्मचारी जो किसी अन्य देश में अवस्थित है और उसे उस संगठन के सेन्ट्रलाइज्ड (केन्द्रीयकृत) सर्वर जो किसी तीसरे देश में मौजूद है, पर एक्सेस (पहुंच) चाहिए अथवा कोई कर्मचारी जो घर से काम (वर्क फ्रॉम होम) करता है, और अपने ऑफिस का इन्टरनेट प्रयोग नहीं करता है, लेकिन उसे ऑफिस के नेटवर्क पर उपलब्ध कोई खास फाइल पर काम करना है। ऐसी स्थिति में, सिस्टम उस यूजर के विवरण (क्रेडेन्शियल्स) के आधार पर उसका प्रमाणीकरण चाहेगा और प्रमाणिकता की पुष्टि होने पर ही यूजर को फाइल तक पहुंचने देगा, अन्यथा नहीं। उस व्यक्ति के क्रेडेन्शियल्स के आधार पर कुछ निश्चित संसाधनों (रिसोर्सेज) पर पहुँच प्रदान करने की प्रक्रिया का ऑथोराइजेशन कहते हैं। आमतौर पर अर्थाँटिकेशन और ऑथोराइजेशन की प्रक्रिया साथ-साथ चलती है। अब यह भलीभांति स्पष्ट है कि किसी संगठन की साइबर सुरक्षा सुनिश्चित करने में मजबूत (स्ट्रॉंग) पासवर्ड को अहम भूमिका होती है। कोई आसान सा पासवर्ड सुरक्षा को नुकसान पहुंचा कर उस पूरे संगठन को बड़े जोखिम में डाल सकता है। इसलिए किसी भी संगठन की पासवर्ड नीति इस प्रकार की होनी चाहिए कि उसके कर्मचारी स्ट्रॉंग पासवर्ड (12 से अधिक अक्षर (कैरेक्टर) और लोअरकेस तथा अपरकेस का कॉम्बिनेशन (मिश्रण) साथ ही कुछ

विशिष्ट अंक और अक्षर भी शामिल हों) का उपयोग करने के लिए बाध्य हों और साथ ही समय—समय पर पासवर्ड बदलते रहें। कुछ बड़े संगठनों अथवा संवेदनशील संगठनों जैसे कि रक्षा संस्थान, वित्तीय संस्थान, योजना आयोग आदि, प्रमाणीकरण की मिश्रित प्रणाली (हाइब्रिड अर्थाँन्टिकेशन सिस्टम) का प्रयोग करते हैं। इसमें यूजरनेम और पासवर्ड के साथ—साथ हार्डवेयर की सुरक्षा के लिए बायोमैट्रिक सिस्टम आदि का भी प्रयोग किया जाता है। कुछ बड़े संगठन वीपीएन (वर्चुअल प्राइवेट नेटवर्क) का भी इस्तेमाल करते हैं। यह कम्पनी को इन्टरनेट पर हाइब्रिड सिक्युरिटी अर्थाँन्टिकेशन के द्वारा सुरक्षित पहुँच उपलब्ध कराने का एक तरीका है।

## 2.2 एनक्रिप्शन (कोडीकरण)

इन्टरनेट पर डाटा के प्रसारण के पहले इन्हें अपठनीय स्वरूप में बदलने की प्रक्रिया को एनक्रिप्शन कहते हैं। केवल वही व्यक्ति इन एनक्रिप्टेड डाटा को पठनीय रूप में बदल कर पढ़ सकता है, जिसके पास इसकी कुंजी (की) होगी। औपचारिक रूप से एनक्रिप्शन को इस प्रकार परिभाषित किया जा सकता है—“मैथमैटिकल एल्गोरिथिम का उपयोग करके आंकड़ों को जटिल कोडों में परिवर्तित करके डाटा लॉक करने की प्रक्रिया एनक्रिप्शन कहलाती है।” ये कोड इतने जटिल होते हैं कि सर्वाधिक शक्तिशाली कम्प्यूटर को भी इन्हें ब्रेक करने में कई वर्ष लग जाएंगे। इस सुरक्षित कोड को इन्टरनेट पर गंतव्य तक सही—सलामत प्रसारित किया जा सकता है। प्राप्तकर्ता “की” का इस्तेमाल करके डाटा डिकोड कर सकता है। “की” का प्रयोग करके जटिल कोड को मूल—पाठ में बदलने की प्रक्रिया को डिक्रिप्शन कहते हैं यदि डाटा लॉक और अनलॉक करने के लिए एक ही “की” का इस्तेमाल हो तो इसे साइमैट्रिक “की” एनक्रिप्शन कहते हैं।



चित्र 4 : एनक्रिप्शन<sup>1</sup>

<sup>1</sup> Image courtesy: [https://upload.wikimedia.org/wikipedia/commons/b/bc/Public\\_key\\_encryption\\_keys.png](https://upload.wikimedia.org/wikipedia/commons/b/bc/Public_key_encryption_keys.png)

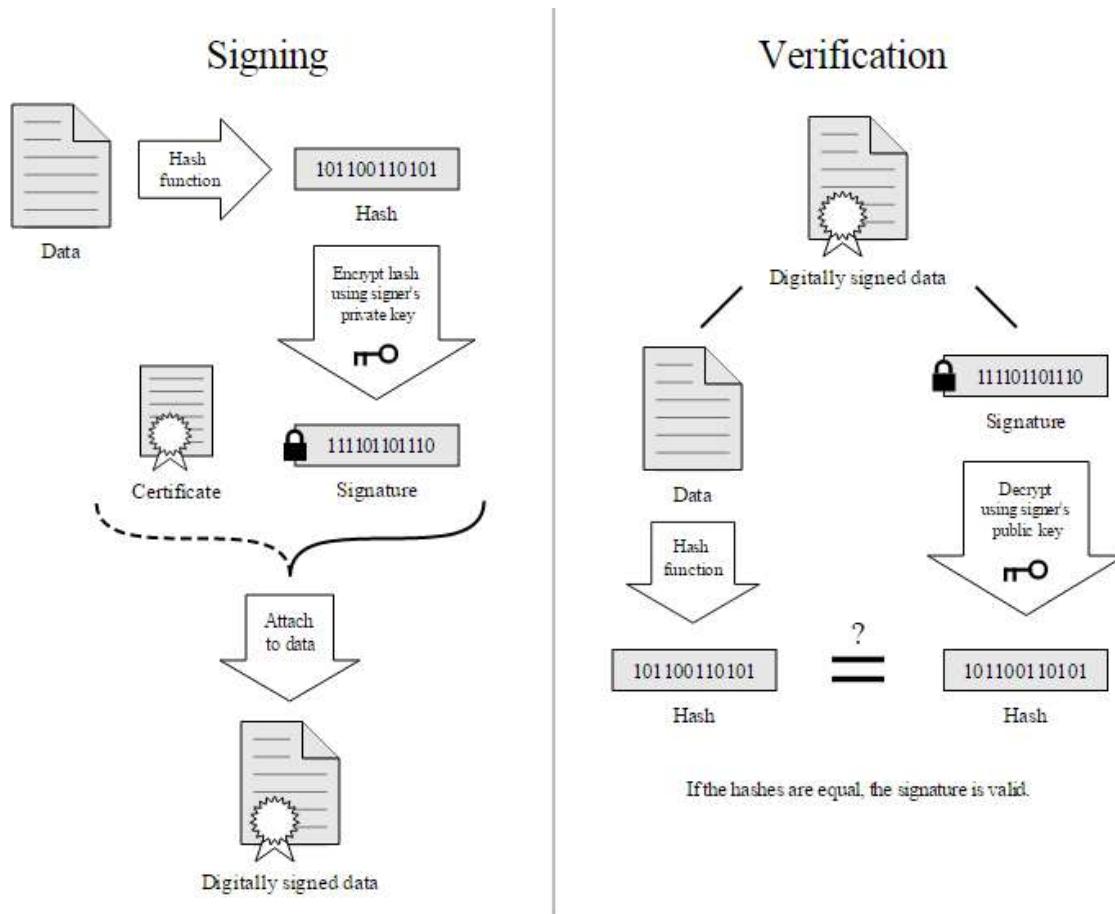
साइमैट्रिक “की” एनक्रिशन में, डाटा कोडिंग के बाद “की” डाक सेवा, टेलीफोन आदि के जैसे किसी अन्य माध्यम के जरिए गन्तव्य पर भेजी जाती है, क्योंकि, यदि किसी हैकर को ये “की” प्राप्त हो गई तो डाटा सुरक्षा खतरे में पड़ जाएगी। “की” के हस्तांतरण से बचने के लिए, असिमैट्रिक “की” एनक्रिप्शन जिसे पब्लिक की एनक्रिप्शन भी कहते हैं, पद्धति का उपयोग किया जाता है। एसिमैट्रिक “की” एनक्रिप्शन में, डाटा एनक्रिप्ट और डिक्रिप्ट करने के लिए अलग—अलग “की” होती हैं। प्रत्येक यूजर के पास दोनों “की” यानि पब्लिक “की” और प्राइवेट “की” होती है। जैसा कि नाम से स्पष्ट है प्रत्येक यूजर की पब्लिक “की” की जानकारी सबको होती है, लेकिन प्राइवेट “की” की जानकारी केवल उस खास यूजर को होती है, जिसके पास वह “की” है। मान लो कि प्रेषक “ए” प्राप्तकर्ता (रिसीवर) “बी” को कोई गुप्त संदेश (सीक्रेट मैसेज) भेजना चाहता है। “ए” “बी” की पब्लिक “की” का इस्तेमाल करके संदेश एनक्रिप्ट करेगा, क्यों पब्लिक “की” सबकी जानकारी में है। संदेश एनक्रिप्ट होने के बाद इसे इन्टरनेट के जरिए “बी” को सही स्थान पर भेज दिया जाएगा। जैसे ही यह संदेश “बी” को मिलेगा वह अपनी प्राइवेट “की” का इस्तेमाल करके संदेश को मूल—पाठ में परिवर्तित कर लेगा।

## 2.3 डिजिटल सिग्नेचर

यह आंकड़ों के वैधीकरण (वेलिडेशन) की एक टेक्नीक है। किसी दस्तावेज (डॉक्यूमेन्ट) की विषयवस्तु (कन्टेन्ट) के प्रमाणीकरण की प्रक्रिया को वेलीडेशन कहते हैं। डिजिटल सिग्नेचर केवल डाटा वेलिडेट नहीं करते बल्कि इन्हें प्रमाणित भी करते हैं। प्रेषक (सेन्डर) की प्राइवेट “की” से डाटा एनक्रिप्शन के द्वारा डिजिटल सिग्नेचर बनाए जाते हैं। मूल संदेश (ओरिजिनल मैसेज) के साथ एनक्रिप्ट किए डाटा को संलग्न करके इन्हें इंटरनेट पर गन्तव्य (डेस्टीनेशन) को भेजा जाता है। प्राप्तकर्ता (रिसीवर) प्रेषक की पब्लिक “की” का उपयोग करके सिग्नेचर डिक्रिप्ट कर सकता है। अब, डिक्रिप्ट किए गए मैसेज का मूल मैसेज से मिलान किया जाता है। यदि दोनों में कोई फर्क नहीं है, तो इससे पता लगता है डाटा के साथ छेड़—छाड़ (टैम्परिंग) नहीं हुई है, साथ ही सेन्डर की प्रमाणिकता भी सत्यापित हो जाती है, क्योंकि जिसके पास प्राइवेट “की” है (जो कि केवल ओनर को मालूम है) वही डाटा एनक्रिप्ट कर सकता है, जिसे बाद में पब्लिक “की” के द्वारा डिक्रिप्ट किया गया है। यदि प्रेषण (ट्रान्समिशन) के दौरान डाटा से छेड़—छाड़ की गई है तो इसका आसानी से पता चल जाएगा क्योंकि डाटा का सत्यापन नहीं होगा। इसके अलावा, मैसेज को फिर से एनक्रिप्ट नहीं किया जा सकता, क्योंकि एनक्रिप्शन के लिए जरूरी प्राइवेट “की” तो मूल प्रेषक (ओरिजिनल सेन्डर) के पास है।

ज्यादातर डॉक्यूमेन्ट अब इन्टरनेट के जरिए भेजे जाने लगे हैं, इसलिए वैज्ञानिक डिजिटल सिग्नेचर वैधानिक तथा वित्तीय लेन—देन का अनिवार्य हिस्सा बन गए हैं। इससे न केवल व्यक्ति की प्रामाणिकता

और डॉक्यूमेंट की वैधता सिद्ध होती है, बल्कि कभी बाद में समझौता या अनुबंध का नकारने की सम्भावना भी समाप्त हो जाती है। उदाहरण के लिए, कोई शेयर धारक ई-मेल के जरिए अपने ब्रोकर को आदेश देता है कि वर्तमान मूल्य पर मेरे शेयर बेच दो। लेन-देन पूरा हो जाने के बाद, शेयर होल्डर यह कह कर कि ई-मेल जाली या बोगस थी अपने शेयरों पर फिर दावा कर सकता है। ऐसी विवादास्पद स्थितियों को रोकने के लिए, डिजिटल सिग्नेचर का उपयोग किया जाता है।



चित्र 5 : डिजिटल सिग्नेचर<sup>2</sup>

## 2.4 एन्टीवायरस

कम्प्यूटर की सुरक्षा को भेदने के लिए इन्टरनेट पर वायरस, वॉर्म्स, ट्रोजन हॉर्स आदि जैसे कई मैलिसियस प्रोग्राम प्रेषित किए जाते हैं। ये प्रोग्राम कम्प्यूटर में मौजूद डाटा को नष्ट कर सकते हैं या पासवर्ड आदि चुरा कर वित्तीय नुकसान पहुंचा सकते हैं। सिस्टम में इन मैलिसियस प्रोग्राम की पहुंच को

<sup>2</sup> Image courtesy: [https://upload.wikimedia.org/wikipedia/commons/2/2b/Digital\\_Signature\\_diagram.svg](https://upload.wikimedia.org/wikipedia/commons/2/2b/Digital_Signature_diagram.svg)

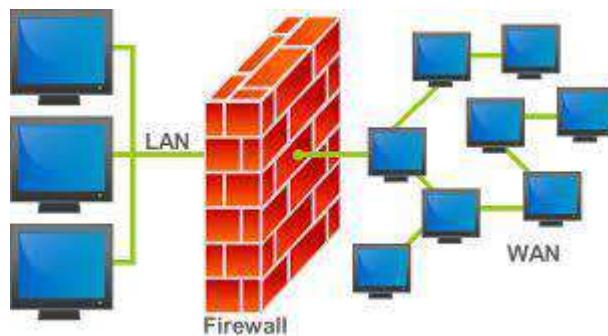
रोकने के लिए एक एन्टी-वायरस नाम के विशेष प्रोग्राम का उपयोग किया जाता है। सिस्टम को वायरस से सुरक्षित रखने के लिए इन्हें बनाया गया है। यह न केवल वायरस को सिस्टम में प्रवेश करने से रोकता है। बल्कि सिस्टम में पहले से मौजूद मैलिसियस कोड को भी नष्ट करता है। हर दिन नए-नए वायरस इंटरनेट से प्रसारित होते रहते हैं। एन्टी-वायरस अपने डाटाबेस को निरन्तर अपडेट करता रहता है और इन वायरस, बॉर्क्स आदि से सिस्टम को बचाता रहता है।



चित्र 6 : बाजार में उपलब्ध एन्टी-वायरस<sup>3</sup>

## 2.5 फायरवॉल

यह एक हार्डवेयर/साफ्टवेयर है जो संगठन के नेटवर्क और इंटरनेट के बीच कवच (शील्ड) की तरह काम करता है और वायरस, मैलवेयर, हैकर्स आदि के खतरों से इसे बचाता है। यह केवल उन्हीं व्यक्तियों को आपके नेटवर्क में प्रवेश पाने और सूचना भेजने की अनुमति देता है, जिन्हें आपने प्राधिकृत किया हो।



चित्र 7 : फायरवॉल<sup>4</sup>

किसी भी संगठन में दो तरह का ट्रैफिक होता है, यानि इन बाउन्ड ट्रैफिक और आउट बाउन्ड ट्रैफिक। फायरवॉल के इस्तेमाल से, पोर्ट के ट्रैफिक को कन्फिगर करना और मॉनीटर करना सम्भव हो जाता है।

<sup>3</sup> Image courtesy: <https://www.flickr.com/photos/thomasguest/3027199004>

<sup>4</sup> Image courtesy: <https://upload.wikimedia.org/wikipedia/commons/5/5b/Firewall.png>

केवल विश्वसनीय (ट्रस्टेड) स्रोतों से डाटा पैकेट संगठन के नेटवर्क में प्रवेश कर सकते हैं और काली सूची में डाले गए स्रोतों तथा अनाधिकृत एड्रेस से डाटा पैकेट नेटवर्क में प्रवेश नहीं कर सकते हैं। नेटवर्क में अनाधिकृत प्रवेश रोकने के लिए फायरवॉल होना बहुत जरूरी है। लेकिन यदि फायरवॉल को सही तरीके से कन्फिगर नहीं किया गया तो फायरवाल ऐसा कर पायेगा इसकी कोई गारण्टी नहीं है। फायरवॉल हार्डवेयर और सॉफ्टवेयर का अथवा दोनों का एक साथ साथ संयोजन करके स्थापित की जा सकती है।

#### □ **हार्डवेयर फायरवॉल:**—

हार्डवेयर फायरवाल्स का उदाहरण वे राउटर हैं, जिनके माध्यम से किसी संगठन का नेटवर्क बाहरी नेटवर्क अर्थात् इन्टरनेट से कनेक्ट होता है।

#### □ **सॉफ्टवेयर फायरवॉल्स:**—

ये फायरवॉल्स सर्वर और क्लाइन्ट मशीनों में इन्स्टॉल किए जाते हैं और उस संगठन के नेटवर्क के गेटवे की तरह काम करते हैं।

विन्डोज 2003 और विन्डोज 2008 आदि जैसे ओपरेटिंग सिस्टम में ये फायरवॉल इम्बेडेड (अन्तर्निहित) होती है। यूजर को केवल अपनी जरूरत के अनुसार फायरवॉल को ईष्टतम (ऑप्टिमली) कन्फिगर करना होता है। फायरवाल्स “नियमों” और “नीतियों” के पालन के लिए कन्फिगर किया जाता है और इन परिभाषित (तयशुदा) नियमों के आधार पर फायरवाल फिल्टरिंग के लिए निम्नलिखित तंत्र (मैकेनिज्म) अपना सकती हैं:—

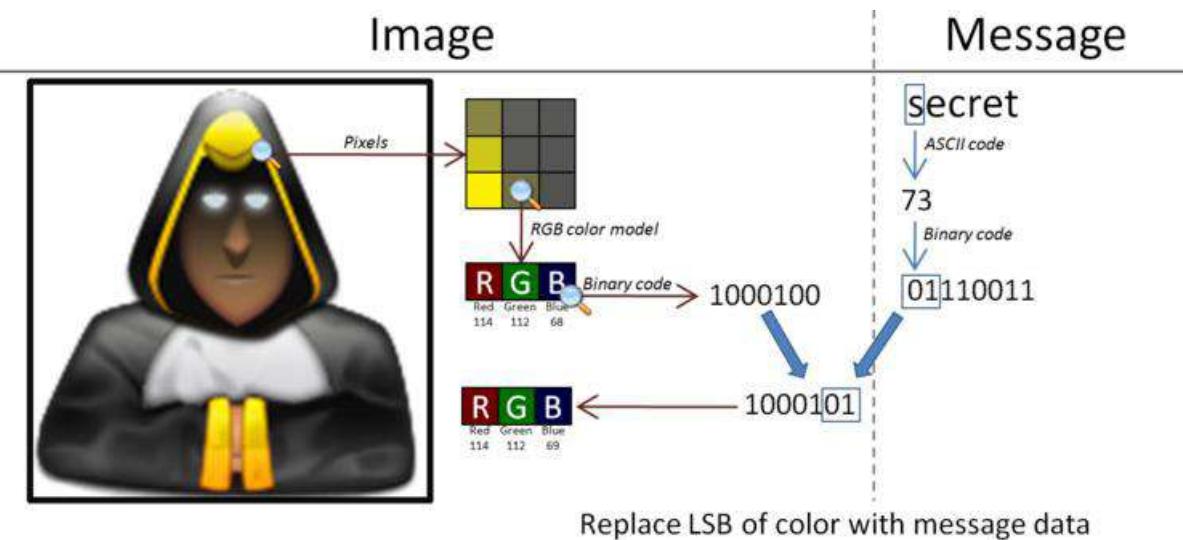
□ **प्रॉक्सी** :— संगठन से बाहर रुट किए जाने वाले ट्रैफिक पर नियंत्रण और निगरानी के लिए इस आउट बाउन्ड ट्रैफिक को प्रॉक्सी से होकर गुजरना होगा।

□ **पैकेट फिल्टरिंग** :— नीतियों में तय नियमों के आधार पर प्रत्येक पैकेट को उसके टाइप, पोर्ट इन्फोर्मेशन और सोर्स तथा डेर्सीनेशन इन्फोर्मेशन के अनुसार फिल्टर किया जाता है। इन विशेषताओं के उदाहरण आईपी एड्रेस, डोमेन नेम, पोर्ट नम्बर्स, प्रोटोकोल आदि हैं। पैकेट फिल्टरिंग का बुनियादी (बेसिक) कार्य राउटर करते हैं।

□ **स्टेटफुल इन्स्पैक्शन** :— किसी डाटा पैकेट की सभी पहचानों को परखने की बजाय, कुछ प्रमुख विशेषताएं तय कर दी जाती हैं। आउट गोइंग/इनकमिंग पैकेट्स को केवल इन तयशुदा विशेषताओं के आधार पर परखा जाता है। फायरवाल्स संगठन के नेटवर्क का एक अनिवार्य अंग होती है ये संगठन के नेटवर्क को वायरस तथा अन्य मैलिसियस कोड से तो बचाती ही है, साथ ही किसी हैकर को डीओएस (डॉस) अटैक के लिए आपके नेटवर्क का उपयोग करने से भी रोकती हैं।

## 2.6 स्टेगैनोग्राफी

किसी डॉक्यूमेंट फाइल, इमेज फाइल और प्रोग्राम अथवा प्रोटोकॉल आदि में गुप्त संदेश छुपाने की तकनीक को स्टेगैनोग्राफी कहते हैं। इस तकनीक से छुपाया गया संदेश दिखाई नहीं देता और एक विशेष सॉफ्टवेयर का उपयोग कर इसे निकाल लिया जाता है। इमेज में छिपे संदेश की जानकारी केवल पष्क (सैन्डर) और प्राप्तकर्ता (रिसीवर) को होती है। इस टैक्नीक का फायदा यह है कि इस तरह की फाइलों पर आसानी से शक नहीं होता।



चित्र 8 : स्टेगैनोग्राफी<sup>5</sup>

स्टेगैनोग्राफी के अनेक इस्तेमाल हैं। इनमें बिना शक पैदा किए गुप्त संदेश भेजना, गोपनीय फाइलों को अनाधिकृत और अनायास एक्सेस तथा चोरी से बचाना, आईपीआर से संबंधित विषयों के लिए डिजिटल वाटरमार्क आदि शामिल हैं।

अब हम इस विषय पर चर्चा करेंगे कि डाटा कवर फाइल (ईमेल, वीडियो, ऑडियो आदि) के अन्दर किस प्रकार गोपनीय तरीके से इम्बेड किए जाते हैं। हम एक ईमेज फाइल का उदाहरण लेंगे जिसे कवर फाइल की तरह इस्तेमाल किया गया है। हाई रिजॉल्यूशन इमेज के प्रत्येक पिक्सल में 3 बाइट्स (24 बिट्स) होते हैं। इस 24 बिट्स में से यदि 3 सबसे कम फर्क डालने वाले बिट्स में छेड़-छाड़ करके डाटा छुपा दिया जाए तो डाटा इम्बेड करने के बाद इमेज की क्वालिटी में होने वाला बदलाव नजर ही नहीं आएगा और केवल अत्यन्त अनुभवी और पैनी नजर ही इस बदलाव को भौंव पायेगी। इस प्रकार, प्रत्येक पिक्सल में 3 बिट्स की सूचना छुपायी जा सकती है।

<sup>5</sup> Image courtesy: [https://upload.wikimedia.org/wikipedia/commons/b/b8/Seformatbmp-embedding\\_full.png](https://upload.wikimedia.org/wikipedia/commons/b/b8/Seformatbmp-embedding_full.png)

इसी प्रकार, किसी ऑडियो फाइल में नियमित अथवा अनियमित अन्तराल पर व्हाइट नॉइज डालकर ऑडियो अथवा वीडियो फाइल में डाटा छिपाए जा सकते हैं। स्टेगेनोग्राफी के लिए अनेक फ्री साफ्टवेयर उपलब्ध हैं। किंवदं स्टेगो, शियाओं, टुकाउज, ओपस्टेगो आदि ऐसे ही कुछ प्रचलित सॉफ्टवेयर हैं।

—□—

# सायबर अपराधों की जांच—पड़ताल : सायबर अपराध—विज्ञान एक परिचय

पिछले अध्यायों में हमने सायबर अटैक के रोकथाम की तकनीकों पर चर्चा की थी। यदि किसी को सायबर अटैक झेलना पड़ा तो उसका अलग कदम क्या होगा? अगला कदम यह होगा कि वह इस कृत्य की रिपोर्ट दर्ज कराए। यदि उस व्यक्ति को सायबर फोरेन्सिक (अपराध—विज्ञान) का ज्ञान है तो सायबर अपराध से जुड़े महत्वपूर्ण सबूतों के अनजाने में नष्ट होने की सम्भावना कम रहेगी।

## 3.1 कम्प्यूटर फोरेन्सिक (अपराध—विज्ञान)

सायबर अपराध—विज्ञान की वह शाखा है, जिसमें सायबर अपराध के खिलाफ ऐसे सबूत जुटाने के लिए डिजिटल डाटा के अन्वेषण हेतु आवश्यक टूल्स और तकनीकों का अध्ययन किया जाता है, जिन्हें अदालत में प्रस्तुत किया जा सके। इस विज्ञान में कम्प्यूटर, डिजिटल स्टोरेज मीडिया, स्मार्टफोन आदि जैसे डिजिटल उपकरणों से सबूत हासिल करने, उनका विश्लेषण करने और उन्हें दस्तावेजों के रूप में सहेजने तथा संरक्षित करने के तौर—तरीकों को समझाया जाता है ताकि कानूनी/प्रशासनिक मामलों में विशेषज्ञता—युक्त राय प्रस्तुत करने के लिए इनका उपयोग किया जा सके।

चूंकि कम्प्यूटिंग उपकरणों और इन्टरनेट पर हमारी निर्भरता दिन प्रतिदिन बढ़ती जा रही है इसलिए किसी भी संगठन में कम्प्यूटर फोरेन्सिक की भूमिका भी अहम होती जा रही है। कैलिफोर्निया विश्वविद्यालय द्वारा कराए गए एक सर्वे के अनुसार 1999 के दौरान केवल 7: सूचना ही पेपरों पर तैयार की गई थी शेष 93: के लिए कम्प्यूटर का इस्तेमाल हुआ था। सबूत जुटाना बहुधा आसान नहीं होता क्योंकि डाटा डिलीट किए जा सकते हैं, छुपाये जा सकते हैं या फिर ये एनक्रिप्टेड फार्मेट में हो सकते हैं। डिजिटल फोरेन्सिक जांच—पड़ताल एक अत्यन्त कुशलता वाला कार्य है। इसमें अपराध के स्थल अथवा अपराध के लिए इस्तेमाल किए गए डिजिटल उपकरणों से डिजिटल सबूत तलाशने और हासिल करने के लिए विभिन्न टूल्स, टैक्नीक और दिशा—निर्देशों का प्रत्यक्ष एवं प्रायोगिक ज्ञान होना अत्यन्त जरूरी है। चूंकि स्मार्ट फोन, टेबलेट्स, पामटॉप्स, स्मार्ट टीवी आदि जैसे डिजिटल उपकरणों की प्रोसेसिंग (प्रसंस्करण) क्षमता और कमप्यूटिंग स्पीड अच्छी—खासी होती है, इसलिए अपराधों में इनके इस्तेमाल की सम्भावना से इन्कार नहीं किया जा सकता। फोरेन्सिक जाँचकर्ता को इन उपकरणों के कार्यकरण (वर्किंग) की गहरी जानकारी के साथ ही इन उपकरणों से सटीक आंकड़ों (सूचना) को हासिल करने के टूल्स की भी प्रत्यक्ष और प्रायोगिक जानकारी होना जरूरी है ताकि सूचना (डाटा) की अहमियत और विश्वसनीयता को बनाए रखा जा सके।

सायबर क्राइम में कम्प्यूटर का इस्तेमाल इरादतन और गैर-इरादतन दोनों तरह से हो सकता है। आपके कम्प्यूटर का उपयोग हेट मेल भेजने के लिए करना अथवा आपके कम्प्यूटर में किसी लाइसेंसशुदा सॉफ्टवेयर का चोरी किया गया वर्जन स्थापित (इन्स्टॉल) करना इरादतन क्राइम की श्रेणी में आएगा जबकि आपके कम्प्यूटर में मौजूद वायरस का नेटवर्क में या नेटवर्क के बाहर किसी डिजिटल उपकरण में फैल जाना और उससे कोई बड़ा वित्तीय नुकसान होना गैर-इरादतन अपराध की श्रेणी में आएगा। इसी प्रकार, किसी डिजिटल क्राइम में कम्प्यूटर का सीधे प्रयोग किया जा सकता है। उदाहरण के लिए, आपके कम्प्यूटर का प्रयोग संवेदी और गोपनीय डाटा हासिल करने और नेटवर्क में/नेटवर्क के बाहर किसी उस व्यक्ति को भेजने के लिए किया जा सकता है, जो अपने फायदे के लिए इन डाटा का उपयोग कर सकता है। किसी सॉफ्टवेयर का फेकवर्जन डाउनलोड करते समय ट्रोजन होर्स कम्प्यूटर में इन्स्टाल हो जाता है जो आपके कम्प्यूटर में चोर दरवाजा (बैकडोर) बना कर किसी हैकर को नेटवर्क हैक करने का मौका दे सकता है, यह कम्प्यूटर का अप्रत्यक्ष प्रयोग कहलाएगा। अब हैकर आपके कम्प्यूटर में लॉग-इन करके साइबर क्राइम के लिए इसका इस्तेमाल कर सकता है। एक अनुभवी कम्प्यूटर फारेन्सिक इन्वेस्टीगेटर (जांचकर्ता) प्रत्यक्ष और अप्रत्यक्ष अटैक में अन्तर समझ सकता है। कम्प्यूटर फोरेन्सिक विशेषज्ञ औद्योगिक जासूसी, जालसाजी आदि का पता लगाने के लिए अनायास लुप्त डाटा भी खोजने में समर्थ होते हैं। बड़े संस्थानों में उनके किसी कम्प्यूटर अथवा नेटवर्क की सुरक्षा में सेंध के मामलों की निगरानी के लिए गठित इन्सीडेन्ट हन्डलिंग टीम को जैसे ही किसी सायबर क्राइम का पता लगता है, वह इस घटना की प्रारम्भिक जांच के लिए संगठन की बनाई अपनी प्रक्रिया का पालन करती है। इस प्रक्रिया के निम्नलिखित चरण हैं:—

## 1. तैयारी—

संगठन सायबर घटना होने पर कार्रवाई के लिए दिशा-निर्देश तैयार करता है और इन्सीडेन्ट रिस्पॉन्स टीम के प्रत्येक सदस्य की भूमिका और दायित्व तय करता है। ज्यादातर बड़े संस्थानों की बाजार में अपनी साथ होती है और इस भरोसे पर सवाल उठने से उस संस्थान के शेयरों-धारकों का भरोसा कम होने लगता है। इसलिए सायबर क्राइम जैसी घटना की जानकारी देने के लिए एक कारगर तंत्र होना जरूरी है। अतः टीम के सदस्य की दक्षता के आधार पर उसका दायित्व तय करना काफी महत्वपूर्ण हो जाता है।

## 2. आइडेन्टीफिकेशन (शिनाख्त)

इन्सीडेन्ट रिस्पॉन्स टीम लक्षणों के आधार पर यह पता लगाती है कि वास्तव में घटना घटी है या नहीं। घटना की सत्यता जाँचने की सबसे आम प्रक्रिया है, लॉग्स की जांच करना। जब यह पुर्खता हो जाता है कि घटना हुई है तब इस साइबर अटैक के प्रभाव (इम्पैक्ट) का आकलन किया जाता है।

### **3. कन्टेनमेन्ट (अवरोधन)**

इस चरण में, असेसमेंट (आकलन) टीम से प्राप्त फीडबैक के आधार पर भविष्य में ऐसी घटनाओं को रोकने की रणनीति बनाई जाती है।

### **4. उन्मूलन (इरेडिकेशन)**

इस चरण में, खतरों को समाप्त करने अथवा कम करने की रणनीति बनाई जाती है और लागू की जाती है।

### **5. रिकवरी (संभालना):—**

इस चरण में, समस्या के समाधान (उन्मूलन) के बाद फिर से सामान्य कार्य संचालन शुरू करने की प्रक्रिया शामिल है।

### **6. भविष्य के लिए सबकः—**

यदि घटना पहली बार घटी है या नई तरह की है, तो इसका ब्यौरा दर्ज कर लिया जाता है ताकि भविष्य में ऐसी ही घटना घटने पर पिछली घटना के अनुभवों और ज्ञान के द्वारा इससे निपटा जा सके।

अगले कदम के तौर पर, अपराध के सबूत जुटाने के लिए फोरेन्सिक जांच-पड़ताल का सहारा लिया जाता है। अधिकांश मामलों में यह जांच-पड़ताल किसी अन्य कम्पनी द्वारा कराई जाती है। कम्प्यूटर फोरेन्सिक इन्वेस्टीगेशन में निम्नलिखित चरण शामिल हैं:—

#### **1. घटना और सबूतां की शिनाख्त करना:—**

सिस्टम एडमिनिस्ट्रेटर सबसे पहले यही काम करता है। वह घटना के बारे में हर सम्भव जानकारी जुटाने का प्रयास करता है। इस जानकारी के आधार पर अटैक का दायरा और उसकी प्रचण्डता का आकलन किया जाता है। अटैक का सबूत मिलते ही, जांच-पड़ताल के लिए इसका बैकअप ले लिया जाता है। फोरेन्सिक जांच-पड़ताल कभी भी मूल मशीन पर नहीं, बल्कि बैक-अप के द्वारा री-स्टोर किए गए डाटा पर की जाती है।

#### **2. सबूत जुटाना और संरक्षित रखना:—**

डाटा कैचर करने के लिए हेलिक्स, विनाफेक्स, एफकेटी इमेज जैसे अनेक टूल्स का इस्तेमाल किया जाता है। डाटा का बैक-अप लेने के बाद, सबूत और बैक-अप को अभिरक्षित कर लिया जाता है। डाटा की विश्वसनीयता परखने के लिए, बैक-अप के एमडी5 (मैसेज डाइजेस्ट) हैस की गणना करके इसका मूल

डाटा से मिलान किया जाता है। सिस्टम लॉग, नेटवर्क इन्फॉर्मेशन, इन्ड्रियूजन डिटेक्शन सिस्टम (आईडीएस) द्वारा तैयार किए गए लॉग, पोर्ट तथा पोर्ट इन्फॉर्मेशन भी अभिरक्षित कर लिये जाते हैं।

### 3. जांच-पड़ताल:-

स्टेगेनोग्राफिक संदेशों आदि की संभावना तलाशने के लिए लॉग्स, सिस्टम फाइल्स, डिलीट और अपडेट की गई फाइलों, सीपीयू के उपयोग और प्रोसेस लॉग्स, टेम्परेरी फाइलों, पासवर्ड द्वारा सुरक्षित एनक्रिप्टेड फाइलों, इमेजेज, वीडियो, और डाटा फाइलों की समीक्षा करके जांच-पड़ताल की जाती है।

### 4. समराइजेशन और प्रेजेन्टेशन:-

घटना का सार संक्षेप काल-क्रमानुसार तैयार करके प्रस्तुत किया जाता है। जांच-पड़ताल के आधार पर निष्कर्ष निकाला जाता है और सम्भावित कारणों को समझा/समझाया जाता है।

डिजिटल फोरेन्सिक जाँच पड़ताल के दौरान, विशेष रूप से सबूत जुटाते समय नियमों और पद्धतियों का पालन अवश्य किया जाए। यह सुनिश्चित किया जाए कि डाटा कैचर करने की प्रक्रिया से सबूतों में कोई बदलाव न आए। आकड़ों की विश्वसनीयता सुरक्षित रहे। यह सुनिश्चित किया जाए कि बैकअप लेने के लिए उपयोग किए जाने वाले उपकरण पूरी तरह संक्रमण मुक्त हों। इसके अलावा, डिजिटल सबूतों को जब्त करने, सबूतों को हासिल करने और इन्हें ट्रान्सफर करने से संबंधित सभी क्रिया-कलापों को लिपिबद्ध किया जाए, संरक्षित किया जाए और समीक्षा के लिए उपलब्ध कराया जाए। बीमारी से परहेज भला। फायरवॉल जैसे डिटेक्शन सिस्टम को समय-समय पर दुरुस्त करते रहें और हैकरों के हमले से बचने के लिए अपने नेटवर्क का पैनीट्रेशन टेस्ट (भेदन परीक्षण) करते रहे। इन सबके अलावा, अपराध की रिपोर्ट अवश्य दर्ज कराएं।

## 3.2 सायबर अपराध की रिपोर्ट क्यों लिखाएं?

कुछ कम्पनियां अपने शेयरधारकों के बीच कम्पनी की ख्याति को नुकसान पहुँचने के डर से सायबर क्राइम की रिपोर्ट दर्ज नहीं करते हैं। कुछ डाटा अत्यंत गोपनीय होते हैं और इनके खुलासे से उनका कारोबार प्रभावित हो सकता है। लेकिन, सच्चाई यह है कि जब तक सायबर क्राइम की रिपोर्ट दर्ज नहीं कराई जाएगी, सायबर अपराधी पकड़े नहीं जाएंगे। इससे स्थिति और खराब होगी, और सायबर अपराधी उसी कम्पनी अथवा किसी अन्य कम्पनी में बेखौफ ऐसे अपराध करते रहेंगे। इसलिए इन अपराधियों का पता लगाना और उन्हें दण्डित करना अत्यंत आवश्यक है। इससे न केवल अर्थव्यवस्था के लिए मौजूदा खतरे बल्कि नए खतरों को भी पहचानने में मदद मिलेगी। सायबर अपराध के दायरे के अनुसार, नजदीक के सायबर सैल, स्टेट (राज्य) सायबर सैल, सीबीआई, आईबी जैसी केन्द्रीय जांच एजेंसियों अथवा इन्टरपोल जैसे अन्तर्राष्ट्रीय निकायों में इनकी रिपोर्ट दर्ज कराई जानी चाहिए।

कुछ सायबर समन्वय इकाइयों के पते इस प्रकार हैं:-

<b>टसम</b>	<b>हरियाणा</b>
<p><b>पता :</b> सीआईडी मुख्या., डिप्टी एस पी, असम पुलिस, कॉन्टेक्ट नं. -फो 91-361-252-618, 91 9435045242</p> <p><b>ईमेल—</b> चक्रवरक/दचवसपबम</p>	<p><b>पता :</b> साइबर क्राइम एण्ड टैक्नीकल इन्वेस्टीगेशन सेल, ज्वाइन्ट कमिश्नर ऑफ पुलिस, ओल्ड एसपी ऑफिस कॉम्प्लेक्स, सिविल लाइन, गुरुग्राम</p> <p><b>ई—मेल:</b> पजबचण्हहदमीतलण्दपबण्पद</p>
<b>मुम्बई</b>	<b>चेन्नई</b>
<p><b>पता :</b> साइबर क्राइम इन्वेस्टीगेशन सेल, आफिस ऑफ कमिश्नर ऑफ पुलिस, एनेक्सी-3 बिल्डिंग प्रथम तल नीयर क्राफर्ड मार्केट, मुम्बई-01</p> <p><b>कॉन्टेक्ट नं.</b> 91-22-22630829 91-22-22641261</p> <p><b>वेबसाइट :</b> जेजचरुधूबलइमबमससउनउइंप्पबवउ</p> <p><b>ईमेल :</b> वापिबमत/बलइमतबमससउनउइंप्पबवउ</p>	<p><b>पता :</b> असिस्टेंट कमिश्नर ऑफ पुलिस, साइबर क्राइम सेल, वेपेरी, चेन्नई-7</p> <p><b>कॉन्टेक्ट नं. :</b> 04423452348, 04423452350</p> <p><b>ई—मेल:</b> बलइमतबतपउमबीद/लवीववण्बवउ</p>
<b>थाने</b>	<b>शेष तमिलनाडु</b>
<p><b>पता :</b> तीसरा तल, पुलिस कमिश्नर ऑफिस, नियर कोर्ट नाका, थाने वेस्ट, थाने- 400601</p> <p><b>कॉन्टेक्ट नं.</b> 91-22-25424444</p> <p><b>वेबसाइट :</b> ज्ञांदमचवसपबमण्वतह</p> <p><b>ई—मेल :</b> चवसपबम/ज्ञांदमचवसपबमण्वतह</p>	<p><b>पता :</b> ए-विंग, तीसरा तल, राजाजी भवन, बेसेन्ट नगर, चेन्नई-600090</p> <p><b>कॉन्टेक्ट नं.—</b> 044-244619590, 24468889, 24463888</p> <p><b>ई—मेल:</b> वेइमवबीद/बझ.हवअण्पद</p>
<b>बंगलौर (पूरा कर्नाटक)</b>	<b>हैदराबाद</b>
<p><b>पता :</b> सायबर क्राइम पुलिस स्टेशन, सीओडी मुख्यालय कार्लटन हाउस 1, पैलेस रोड, बंगलौर-560001</p> <p><b>कॉन्टेक्ट नं.</b> 91-80-2220 1026, 91-80-2294 3050, 91-80-2238 7611 (फैक्स)</p> <p><b>वेबसाइट:</b> जेजचरुधूबलइवतचवसपबमइंदहसवतण्वण्दपबण्पद</p> <p><b>ई—मेल:</b> बबचसमइसतण्डेकण्दमजण्पदए बमचवेमांतण्दपबण्पद</p>	<p><b>पता :</b> साइबर क्राइम पुलिस स्टेशन, क्राइम इन्वेस्टीगेटिंग डिपॉर्टमेंट, तीसरा तल, डीजीपी ऑफिस, लकड़ी का पुल, हैदराबाद-500004</p> <p><b>कॉन्टेक्ट नं.</b> 91-40-23240663, 91-40-27852274, 91-40-27852040, 91-40-23297474 (फैक्स)</p> <p><b>वेबसाइट:</b> जेजचरुधूबपकंचण्हवअण्पदध्वलइमतबतपउमणेंग</p> <p><b>ई—मेल:</b> बपकंच/बपकंचण्हवअण्पदए</p>

	<p>पदवि / बपकंचण्हवअण्पदए बलइमतबमससत्रीलकममीलकंचचसवसपबमण्हवअण्पद</p>
<b>दिल्ली</b>  <b>सीबीआई सायबर क्राइम सेल :</b> सुपरिन्टेन्डेन्ट ऑफ पुलिस सायबर क्राइम इन्वेस्टीगेशन सेल, सेन्ट्रल ब्यूरो ऑफ इन्वेस्टीमेशन, पांचवा तल, ब्लॉक नं. 3, सीजीओ कॉम्प्लेक्स लोधी रोड, नई दिल्ली-3 कॉन्ट्रेक्ट नं. 91-11-4362203, 011-26851998, 011-26515229, 011-4392424  <b>वेबसाइट :</b> जेजचरूद्धबइपण्दपबण्पद  <b>सहायक पुलिस आयुक्त, सायबर क्राइम सेल, ईओडब्ल्यू क्राइम ब्रांच, दूसरा तल, पुलिस ट्रेनिंग स्कूल, मालवीय नगर, नई दिल्ली-110017   <b>ईमेल:</b> बइपबपब/इवसण्दमजण्पद   कबचमवूकसबण्दपबण्पद</b>	<p><b>पुणे</b> पता : डिप्टी कमिश्नर ऑफ पुलिस (क्राइम), ऑफिस ऑफ दी कश्मिनर, 2, साधु वासवानी रोड, कैम्प, पुणे कॉन्ट्रेक्ट नं. 91-20-26123346, 91-20-26127277, 91-20-26128105 (फैक्स)   <b>वेबसाइट:</b> एचनदचवससबम/हवअण्पद   <b>ईमेल:</b> बतपउमबउच/दपबण्पद   चनदमचवसपबम/अेदसण्बवउ</p>
<b>हिमाचल</b>  <b>पता :</b> सीआईडी ऑफिस, डी.एस.पी. हिमाचल प्रदेश <b>कॉन्ट्रेक्ट नं. :</b> 91-9418039449  <b>ई-मेल:</b> ववकइतपरमौ/हउंपसण्बवउ	<p><b>गुजरात</b> डीआईजी, सीआईडी, क्राइम एण्ड रेलवे, फिपथ फ्लोर, पुलिस भवन, सैक्टर 18, गांधीनगर- 382618   <b>कॉन्ट्रेक्ट नं.-</b> 91-79-23254384, 91-79-23250798, 91-79-23253917 (फैक्स)</p>
<b>झारखण्ड</b>  <b>पता :</b> आईजी, सीआईडी क्राइम, राजारानी बिल्डिंग, डोरण्डा, रांची-834002  <b>कॉन्ट्रेक्ट नं.:</b> 916512400737, 91-6512400738  <b>ई मेल :</b> हनचजं/रींतांदकवचसपबमण्हवअण्पद	<p><b>केरल</b> पता : हाइटेक सेल, पुलिस हेडकवार्टर, तिरुअनन्तपुरम   <b>कॉन्ट्रेक्ट नं.</b> 914712721547, 914712722768   <b>ई-मेल:</b> पेजमबीबमसस/पमतंसंचवसपबमण्हवअण्पद</p>
<b>जम्मू</b>  <b>पता :</b> एसएसपी क्राइम, सीपीओ कॉम्प्लेक्स, पंजतीर्थ, जम्मू-180004  <b>कॉन्ट्रेक्ट नं.:</b> 911912578901	<p><b>उड़ीसा</b> पता : सीआईडी, क्राइम ब्रांच, उड़ीसा   <b>कॉन्ट्रेक्ट नं.:</b> 919437450370   <b>ईमेल:</b> चसबपकबइण्वतचवस/दपबण्पद</p>

<b>ईमेल:</b> चबतउरउन / दपबण्पद	
<b>मेघालय</b>  पता : एससीआरबी, सुपरिन्टेन्डॉन्ट ऑफ पुलिस, मेघालय  कॉन्ट्रेक्ट नं.: 919863064997  <b>ई मेल:</b> बतइ.उमह / दपबण्पद	<b>पंजाब</b>  पता : सायबर क्राइम पुलिस स्टेशन, डीएसपी सायबर क्राइम, एसएएस नगर, पटियाला, पंजाब कॉन्ट्रेक्ट नं. 911722748100
<b>बिहार</b>  पता : सायबर क्राइम इन्वेस्टीगेशन यूनिट, डीएस.पी. कोतवाली पुलिस स्टेशन, पटना  कॉन्ट्रेक्ट नं.:— 919431818398  <b>ईमेल:</b> बबपन.इपी / दपबण्पद	<b>पश्चिम बंगाल</b>  पता : सीआईडी, सायबर क्राइम, पश्चिम बंगाल।  कान्ट्रेक्ट नं.: 913324506163  <b>ईमेल:</b> बबबलइवत / बपकूममजइमदहंसणहवअण्पद
<b>उत्तर प्रदेश</b>  पता : सायबर कम्पलेन रीईसल सेल, नोउल ऑफिसर सायबर सेल आगरा, रेज 7, कचहरी रोड, बालूगंज, आगरा— 232001, उत्तर प्रदेश  कॉन्ट्रेक्ट नं.: 919410837559  <b>ईमेल:</b> पदवि / बलइमतबमससंहंतण्बवउ	<b>उत्तराखण्ड</b>  पता : स्पेशल टास्क फोर्स ऑफिस सब इन्स्पेक्टर ऑफ पुलिस, देहरादून  कॉन्ट्रेक्ट नं.: 91135264098, 919412370272  <b>ईमेल:</b> कहब.चवसपबम.ने / दपबण्पद

-□-

# हाल ही में साइबर सुरक्षा पर हुए हमले

## 4.1 परिचय:

इन्टरनेट का उपयोग दिन-पर-दिन तेजी से बढ़ता जा रहा है। इसके चलते स्वास्थ्य देखभाल, बैंकिंग, विद्युत वितरण आदि के क्षेत्र में ई-गवर्नेंस, ई-कॉर्मर्स का दायरा तो बढ़ ही रहा है लेकिन साथ ही हैकिंग, व्यक्तिगत जानकारी की चोरी, डाटा टैम्परिंग, एकाउन्ट हाइजॉकिंग आदि जैसे खतरे भी इन क्षेत्रों में बढ़ रहे हैं। एक रिपोर्ट के अनुसार जनवरी-मई 2014 के दौरान, साइबर सुरक्षा पर हमले की 62189 घटनाएं हुई थीं और ये हमले मुख्यतया अमरीका, यूरोप, ब्राजील, तुर्की, चीन, पाकिस्तान, बंगलादेश, अलजीरिया और यूएई से हुए थे। साथ ही, भारत सरकार की 10,000 साइटें इन हमलों का निशाना बनी थीं। ऐसे हमलों से निपटने के लिए, भारत में आईटी क्षेत्र के सुरक्षा पेशेवरों की भारी कमी है। एक रिपोर्ट के अनुसार साइबर खतरों से निपटने के लिए भारत को लगभग 10 लाख साइबर सुरक्षा पेशेवरों की आवश्यकता है।

## साइबर अपराध की कुछ ताजा घटनाएं

इस खण्ड में हम साइबर अपराध और धोखाधड़ी की कुछ आम घटनाओं पर चर्चा करेंगे ताकि आप यह समझ सकें कि किस तरह थोड़ी सी ना समझी एक बड़े नुकसान का कारण बन सकती है।

- पेपैल, अन्तर्राष्ट्रीय स्तर पर ऑनलाइन मनी ट्रान्सफर की सेवा देने वाली कम्पनी है, जो अनेक प्रकार की एनक्रिप्शन तकनीकों का इस्तेमाल करके आपको इन्टरनेट के माध्यम से सुरक्षित रूप से मनी ट्रान्सफर की सुविधा देती है और चैक, मनीआर्डर आदि जैसे भुगतान के पारम्परिक तरीकों का एक विकल्प प्रदान करती है। इसके 190 देशों में 10 करोड़ से ज्यादा यूजर हैं और इसके माध्यम से प्रतिदिन लगभग 90 लाख भुगतान होते हैं। यह ईबे आदि ऑनलाइन ऑक्सन साइटों पर भुगतान का एक लोकप्रिय माध्यम है। यह विभिन्न देशों के खरीददार और विक्रेताओं को अलग-अलग मुद्राओं में व्यापार की सहायता प्रदान करती है।

रोमानिया के एक हैकर टिन्कोडे उर्फ रजवान कारनैन ने पेपैल की चार्जबैक प्रक्रिया के कोड में एक लूपहोल (कमजोरी) का फायदा उठाया। इसके द्वारा कोई भी यूजर प्रत्येक अटैम्ट (प्रयास) पर अपना पैसा दो गुना कर सकता है। मान लो किसी यूजर के पास 1000 रु. है। वह इस लूपहोल का फायदा उठाकर पहले अटैम्ट पर इस राशि को 2000 रु. बना लेगा। यह 2000 रु. दूसरे अटैम्ट में 4000 रु. हो जाएंगे और अगले अटैम्ट में 8000 रु। इस तरह यह प्रक्रिया निरन्तर चलती रहेगी।

- आस्ट्रेलिया में, एमपी3/डबल्यूएमए लैण्ड नाम की वेबसाइट अपने यूजर्स को पायरेटेड (चुराए गए) गाने, म्यूजिक वीडियो विलप्स आदि को मुफ्त में डाउनलोड करने की सुविधा देती थी। इससे इन

गानों के निर्माताओं और कलाकारों को भारी वित्तीय नुकसान उठाना पड़ रहा था। म्यूजिक इन्डस्ट्री पायरेसी इन्वेस्टीमेशन नामक संगठन ने इसकी शिकायत दर्ज कराई।

इस वेबसाइट के मालिक ना ट्रान और ली, जो आस्ट्रेलियाई विश्वविद्यालय के छात्र थे इस वेब साइट को चला रहे थे। उन पर आस्ट्रेलिया के सबसे बड़े कॉपीराइट इन्फ्रांजमेंट (लिप्याधिकार उल्लंघन) मामल में मुकदमा चलाया गया (अरबास, 2012)

3. ऑनलाइन स्टॉकिंग (परेशान करना) का एक दिलचस्प मामला श्रीमती ऋतु कोहली द्वारा दिल्ली पुलिस में दर्ज कराया गया था (कौर 2015) उन्होंने बताया कि कोई अज्ञात व्यक्ति इन्टरनेट के द्वारा एप्पतबण्वर वेबसाइट पर चैटिंग के लिए उसकी आइडेन्टिटी (प्रोफाइल) का उपयोग कर रहा है और उसने उसका पता तथा फोन नं. कई लोगों को दे दिया है। और अब, दुबई, अहमदाबाद, मुम्बई आदि कई जगहों से रात-बेरात फोन आ रहे हैं। इन हरकतों ने उसे मानसिक रूप से परेशान कर दिया है। अन्ततः उसे यह रिपोर्ट दर्ज करानी पड़ी है। महिला की शिकायत के आधार पर दिल्ली पुलिस ने आईपी ऐड्रेस का पता लगाकर आरोपी व्यक्ति मनीश कथूरिया को खोज निकाला और गिरफ्तार कर लिया।

दुबई में रहने वाले एक प्रवासी भारतीय को ब्लैकमेल किया गया। पुलिस में रिपोर्ट दर्ज कराने तक वह लगभग 125 करोड़ रुपये ब्लैकमेलर को दे चुका था (मध्य प्रदेश स्टेट सायबर पुलिस, 2013)। इस प्रवासी भारतीय की इन्टरनेट पर एक लड़की से मुलाकात हुई थी और अनेक बार चैटिंग के बाद, लड़की ने प्रवासी भारतीय का भरोसा और प्यार जीत लिया। इस बीच, इस लड़की ने अपने कई दोस्तों से इन्टरनेट पर ही उसका परिचय करवाया। कुछ कारणों की वजह से ये रिश्ता ज्यादा नहीं चला। कुछ समय बाद, लड़की की एक मित्र, जिसका परिचय उस लड़की ने ही करवाया था, ने बताया कि रिश्ता टूट जाने की वजह से लड़की ने मानसिक तनाव के चलते आत्महत्या कर ली है और पुलिस मामले की पड़ताल कर रही है। सीबीआई, कलकत्ता हाईकोर्ट, न्यूयार्क पुलिस, पंजाब पुलिस आदि के पत्रों की कई जाली प्रतियां इस प्रवासी भारतीय को भेजी गईं। प्रवासी भारतीय ने लड़की की मित्र से मदद मांगी, जिसने कोलकत्ता स्थित एक लॉ फर्म से उसकी मुलाकात करवाई। लॉ फर्म का मालिक इस केस को लेने के लिए तैयार हो गया और बदले में एक बड़ी राशि की मांग की। अलग-अलग अवसरों पर 1.26 करोड़ रुपये से ज्यादा की राशि लॉ फर्म को ट्रान्सफर (अंतरित) भी कर दी गई लेकिन फर्म और ज्यादा पैसा मांगने लगी। अब प्रवासी भारतीय को दाल में कुछ काला नजर आने लगा और उसने इस घटना की जानकारी मुम्बई पुलिस को दी। उसने लड़की के मित्र और लॉ फर्म से प्राप्त ईमेल मुम्बई पुलिस को फार्वर्ड (अग्रेषित) कर दीं। ई मेल की फॉरेन्सिक जांच के बाद पता चला कि तीनों व्यक्तियों का आईपी ऐड्रेस एक ही है और ये एक ही स्रोत (स्टोर्स) से जनरेट

की गई है। आगे खोज—बीन के बाद पता चला कि लड़की और उसके मित्र सभी वर्चुअल (आभासी) हैं यानि इनका अस्तित्व ही नहीं है। लॉ फर्म का मालिक ही वह शातिर दिमाग है जिसने ये झूठी प्रोफाइल और कहानी प्रवासी भारतीय को ब्लैक मेल करने के लिए गढ़ी थी।

4. ईरान के नटान्ज स्थित परमाणु संयंत्र पर “स्टक्सनेट” वायरस का हमला हुआ था। माना जाता है कि यह वायरस अमरीका ने तैयार किया था (शुमर्ट, 2011)। चूंकि ईरान के परमाणु संयंत्र का अपना निजी नेटवर्क था और यह शेष दुनिया के नेटवर्क से कनेक्ट नहीं था, इसलिए इन्टरनेट के द्वारा इस नेटवर्क में वायरस पहुंचाना सम्भव नहीं था। इस वायरस ने पहले उस थर्ड पार्टी की यूटिलिटी को संक्रमित किया, जिसका उपयोग नटान्ज परमाणु संयंत्र करता था और इस प्रकार वह संयंत्र के नेटवर्क में पहुंच गया। वायरस को एक ऐसे खास सिस्टम सॉफ्टवेयर को अपना निशाना बनाने के लिए डिजाइन किया गया था, जो साइमन्स कन्ट्रोलरों के ऑपरेशन (कार्य—संचालन) को नियंत्रित करता था। वायरस सेन्ट्रीफ्यूजों की स्पीड को अनायास तेज या धीमी कर देता था और इस प्रकार उन्हें स्थायी तौर पर नाकाम बना रहा था। इसके अलावा, वायरस ने संयंत्र को अपने कब्जे (हाइजैक) में ले लिया था तथा संयंत्र के संचालन—स्वास्थ्य के बारे में झूठे सिग्नल भेजता था। जब तक वायरस के प्रभाव का पता चलता, बहुत देर हो चुकी थी और वायरस परमाणु संयंत्र को बहुत नुकसान पहुंचा चुका था।
5. मुम्बई स्थित आरपीजी ग्रुप फर्म के चालू खाते का यूजर नेम और पासवर्ड हैक करने के लिए ट्रोजन मेल का इस्तेमाल किया गया था और इस तरीके से रीयल टाइम ग्रोस सैटलमेंट (आरटीजीएस) के द्वारा 2.41 करोड़ रुपये उड़ा लिये गए (नारायण, 2013)। बैंक कर्मचारियों को संदेह तब हुआ जब उन्होंने भारी भरकम राशि का ट्रान्सफर देखा। उन्होंने इस बारे में जब कम्पनी के अधिकारियों से बात की तो उन्होंने बताए गए खाते में किसी भी राशि के ट्रान्सफर से इनकार किया। खाताधारकों के नाम और पते के आधार पर पुलिस को पता चला कि खाताधारकों ने भारी—भरकम कमीशन के बदले में आरोपियों को अपना खाता इस्तेमाल करने की अनुमति दी थी।
6. चेन्नई पुलिस ने क्रेडिट कार्ड धोखा—धड़ी के ऐसे मामले का राज खोला था, जिसमें दो बीपीओ कर्मचारियों ने आरोपी के पुत्र की मदद से क्रेडिट कार्ड धारक की क्रेडिट लिमिट बढ़ा दी और उसका पता भी बदल दिया (मध्यप्रदेश स्टेट सायबर पुलिस, 2013)। उन्होंने क्रेडिट कार्ड धारक के विवरण का पता लगाने के लिए अपनी कम्पनी के कम्प्यूटर में सेंध लगाई। घटना का पता चलने तक क्रेडिट कार्ड कम्पनी को लगभग 7 लाख रुपये का चूना लग चुका था। पत्र व्यवहार का पता बदल दिए जाने के कारण, कार्ड धारक को महीने के अन्त में जनरेट होने वाला मासिक स्टेटमेंट भी नहीं मिला। चेन्नई पुलिस में मामला दर्ज किया गया। बीपीओं के कम्प्यूटर की फोरेंसिक जांच करने पर पता चला कि कम्प्यूटर रिकार्ड चुराने के लिए कम्पनी के दो कर्मचारियों ने कम्प्यूटर में सेंध लगाई थी।

7. आन्ध्रप्रदेश में लिप्याधिकार उल्लंघन (कॉपीराइट इन्फ्रिंजमेंट) का एक मामला दर्ज किया गया था (नंदूरबार, 2013) मोबाइल सेवा चलाने वाली एक जानी-मानी कम्पनी ने एक प्रमोशनल अभियान की शुरूआत की, जिसके अन्तर्गत उसने अपने ग्राहकों को 3 वर्ष के लॉक-इन पीरियड के साथ अत्यन्त कम कीमत पर मोबाइल फोन देने की पेशकश की थी। फोन के सॉफ्टवेयर को इस प्रकार कन्फिगर किया गया था कि लॉक-इन पीरियड के दौरान मोबाइल हैण्डसेट में किसी अन्य कम्पनी का सिम काम नहीं करेगा। कम्पनी के एक प्रतिद्वन्द्वी ने कम्पनी के मौजूदा ग्राहकों को लालच देने के लिए एक मोबाइल फोन दिया जिससे कम्पनी के मोबाइल को उसका सॉफ्टवेयर क्रेक करके “अनलॉक” किया जा सकता था और उस फोन में कोई भी सिम का इस्तेमाल किया जा सकता था। कम्पनी ने इसकी रिपोर्ट दर्ज कराई और कॉरीराइट एक्ट की धारा 63 के तहत कॉपीराइट उल्लंघन का ममला दर्ज किया गया।
8. साइबर जगत में सक्रिय अपराधियों का एक गिरोह शॉपिंग मॉल, पेट्रोल पम्प, रेस्टरॉ, होटल्स आदि में लगे पीओएस से कार्डधारकों के क्रेडिट कार्ड डाटा चुरा कर इन कार्ड का इस्तेमाल ऑनलाइन एयरटिकट बुकिंग के लिये करता था। रिपोर्टों के अनुसार, इन अपराधियों ने ऑनलाइन टिकट बुक करने के लिए 15000 से ज्यादा जाली क्रेडिट कार्डों का उपयोग किया। जिससे लगभग 17 करोड़ रुपये के राजस्व का नुकसान हुआ। ये अपराधी ऑनलाइन टिकट बुक करने के लिए सायबर कैफै जैसी सार्वजनिक सुविधाओं का पयोग करते थे। इससे उन्हें खोजना मुश्किल हो रहा था। इस जालसाजी का पता तब लगा जब इस जालसाजी के शिकार ग्राहकों को ऑनलाइन टिकट बुकिंग की स्टेटमेंट प्राप्त हुई और इन ग्राहकों ने कार्ड जारी करने वाले बैंकों को बताया कि उन्होंने ये टिकट कभी बुक ही नहीं किए।
9. वर्ष 2000 में, “लव बग” अथवा “वीबीएस/लव लैटर” नाम के एक वॉर्म ने बिन्डोज ऑपरेटिंग सिस्टम पर आधारित कम्प्यूटरों को विशेष रूप से अपना निशाना बनाया और अनुमानत: 22000 करोड़ रु. की लागत का नुकसान पहुंचाया। इन कम्प्यूटरों पर “आई लव यू” सबजक्ट लाइन के साथ अथवा लव-लैटर-फॉर-यू जज्जअडे के रूप में अटैचमेंट के साथ एक स्पैम मेल आती थी। जैसे ही यूजर इस अटैचमेंट को क्लिक करता था, कम्प्यूटर संक्रमित हो जाता था और यह वॉर्म कम्प्यूटर की सभी ड्राइव को सर्च करना और फाइलों को करप्ट करना शुरू कर देता था। साथ ही, यूजर की एड्रेस बुक में शामिल सभी आउट बुक कार्टेक्ट को इस ई मेल की कॉपी फॉरवर्ड करना शुरू कर देता था। कुछ ही समय में इन्टरनेट से कनेक्ट लगभग 10: कम्प्यूटर इस वॉर्म से संक्रमित हो गए थे (मध्यप्रदेश स्टेट सायबर पुलिस, 2013)। ब्रिटिश पार्लियामेंट, पेन्टागन जैसे बड़े संगठनों को अपने नेटवर्क में इस वॉर्म को फैलने से रोकने के लिए ई मेल सिस्टम को बन्द करना पड़ा था।

10. इन्टरनेट पर इन दिनों ऑनलाइन डिग्री की धोखाधड़ी काफी चल रही है। इसमें जाली विश्वविद्यालयों द्वारा मान्यता प्राप्त डिग्री प्रदान करने की जालसाजी की जा रही है (गोलिन, 2013)। डिप्लोमा प्रदान करने वाली ये कम्पनियां पैसा लेकर आपके कार्य अनुभव के बल पर डिप्लोमा/डिग्रियां देने का दावा करती है। छात्रों को स्व-मूल्यांकन के आधार पर डिग्री की प्रतिलिपि जारी भी कर दी जाती है। छात्र को ऑनलाइन धोखाधड़ों का पता तब लगता है जब डिग्री को जाली होने के कारण निरस्त कर दिया जाता है।
11. क्या कोई विश्वास करेगा कि इन्टरनेट के जरिए एक झूठी खबर भेज कर 136 अरब डालर का नुकसान पहुंचाया जा सकता है? ऐसा हुआ है। एसोसिएटेड प्रेस (ए.पी.) यूएस. के ट्रिवटर एकाउन्ट को हैक करके एक फेक ट्रिवटर मैसेज वायरल किया गया था। इसमें बताया गया था कि “हाइट हाउस में एक विस्फोट हुआ है और राष्ट्रपति बराक ओबामा घायल हो गए हैं।” बाद में एक आतंकवादी ग्रुप, सीरियन इलेक्ट्रॉनिक आर्मी ने स्वतः ए.पी. के ट्रिवटर एकाउन्ट को हैक करने और यह संदेश भेजने का दावा किया। एक फेक ई-मेल भेज कर यह हैकिंग की गई थीं जैसे ही फिशिंग ई-मेल की लिंक को विलक किया गया, एक स्पाइवेयर कम्प्यूटर में इन्स्टॉल हो गया और कम्प्यूटर में रखी सारी जानकारी एक रिमोट सर्वर को भेज दी गई। इस जानकारी का उपयोग करके “एपी” का ट्रिवटर एकाउन्ट हैक किया गया और यह अफवाह फैलाई गई, जिसके चलते न्यूयार्क स्टोक एक्सचेंज के निवेशकों का विश्वास डगमगाया और भारी नुकसान हुआ।
12. हाल ही में, एक नया वायरस प्वाइन्ट ऑफ सेल्स (पीओएस) मशीनों को संक्रमित कर रहा है। यह वायरस ग्राहक क क्रेडिट कार्ड के भुगतान रिकार्ड चुराता है। पिन कोड, क्रेडिट कार्ड नम्बर, कार्ड की एक्सपायरी डेट, सीसीवी नम्बर आदि जैसे गोपनीय डाटा ट्रैक करके हैकर को भेज दिए जाते हैं ताकि वित्तीय धोखा-धड़ी के लिए इस जानकारी का दुरुपयोग किया जा सके (यूएस-सीईआरटी, 2014)
13. गलत इरादे वाले लोग न कवेल आपकी निजी और गोपनीय जानकारी (डाटा) की तलाश में रहते हैं, बल्कि आपके कम्प्यूनिकेशन इन्फ्रास्टक्चर को भी खोजते हैं, ताकि अपनी पहचान छुपाने के लिए आपकी पहचान का उपयोग कर सकें और अपराध करने के बाद पकड़े न जा सके। इंडियन मुजाहिदीन (आईएम) नामक आतंकवादी गुट ने मुम्बई स्थित अमरीकी नागरिक, कैनेथ हेवुड के अनप्रोटेक्टेड (असंरक्षित) वाई-फाई को हैक करके एक ई-मेल उसके आईपी एड्रेस से एक न्यूज एजेंसी को भेजी थी। यह ई-मेल अहमदाबाद ब्लास्ट से 5 मिनट पहले भेजी गई थी। (चौधरी, नायर और जॉनसन, 2008)।
14. आतंकवादियों ने एक मीडिया हाउस को आतंकी मेल भेजने के लिए मुम्बई के माटुंगा कॉलेज, ऑफ आर्ट्स, साइंस एण्ड कॉर्मर्स के ओपन वाई-फाई का इस्तेमाल किया था (दी इंडियन एक्सप्रेस, 2008)

आतंकवादियों ने नेटवर्क का इस्तेमाल करने के बाद दर से ही राउटर में सेंध लगाकर सिस्टम लॉग को डिलीट कर दिया ताकि जाँच एजेंसिया ई—मेल के ओरिजनल स्रोत का पता न लगा सकें।

15. पुणे पुलिस की आर्थिक अपराध शाखा ने सॉफ्टवेयर इंजीनियर, आस्मा संदीप थोर्वे को ब्रेनवीजा टैक्नेलॉजिज के सॉफ्टवेयर प्रोडक्ट का सोर्स कोड और अन्य गोपनीय सूचना गैरकानूनी तरीके से चुराने के अपराध में गिरफ्तार किया था। इस गैर कानूनी कृत्य की वजह से कम्पनी को 46.5 करोड़ रु. का नुकसान हुआ था (टाइम्स ऑफ इंडिया, 2009)।
16. इन्टरनेट पर एक नए तरीके का अपराध उभर रहा है जिसमें प्रत्याशित बिजनेस पार्टनर आपको घर से ही कारोबार करने की पेशकश कर रहा है, आपको कोई पैसा भी नहीं लगाना है और आकर्षक कमीशन भी मिलेगा (कैस्टिलो, 2007)। यदि वह व्यक्ति कम्पनी के साथ काम करने को तैयार हो जाता है तो यह प्रत्याशित पार्टनर पता, फोन नम्बर, फोटो पहचान, जन्मतिथि आदि जैसा विवरण मांगेगा। कुछ समय बाद उस व्यक्ति को उसके पते पर पार्सल मिलेगा और साथ ही सामान को फिर से पैक करने के अनुदेश तथा पतों की एक सूची जहां विदेशों में ये सामान भेजे जाने हैं, भी प्राप्त होंगे। दरअसल ये सारा सामान चुराए गए क्रेडिट कार्ड से खरीदा गया होता है और बिजनेस पार्टनर द्वारा उपलब्ध कराए गए पते पर डिलीवर करना होता है। यदि जाँच एजेंसी सामान की डिलीवरी के पता तलाश लेगी तो वह व्यक्ति पकड़ा जाएगा। असली परेशानी तब शुरू होती है, जब कमीशन आता है। यह कमीशन थर्ड पार्टी चक के रूप में होता है और चैक की राशि आपकी उम्मीद से ज्यादा होती है। कुछ दिन बाद आपको वह अधिक राशि इलैक्ट्रॉनिकली लौटाने को कहा जाता है, जैसे ही फण्ड ट्रान्सफर हो जाता है, बैंक को पता लगता है कि वह चैक तो जाली थी और आप इसके दोषी पाए जाते हैं।
17. आईसीआईसीआई बैंक के कई ग्राहकों को फिशिंग अटैक का शिकार बनाया गया था। (नायर, 2009)। कुछ ग्राहकों को अपने आपको आईसीआईसीआई बैंक का अधिकारी बताने वाले एक व्यक्ति से ईमेल प्राप्त हुई थी। उसने ग्राहकों को एक लिंक का इस्तेमाल करके अपने खातों की सूचना अपडेट करने को कहा। यह लिंक ग्राहकों को एक ऐसे वेबपेज पर रीडाइरेक्ट करता था, जो हू—बहू आईसीआईसीआई के वेबपेज की तरह था। जब कुछ ग्राहकों को संदेह हुआ और उन्होंने बैंक के आईटी डिपार्टमेंट इस ईमेल के सोर्स की सत्यता जांचने को कहा तो बैंक अधिकारियों को इस जाल—साजी का पता लगा और उन्होंने मामला दर्ज कराया। बैंक अधिकारी यह देख कर हैरान रह गए की नकली वेबसाइट उनके बैंक की अधिकारिक वेबसाइट से काफी—कुछ मिलती—जुलती है। यदि ग्राहक इस लिंक का उपयोग कर अपने यूजर नेम और पासवर्ड द्वारा लाग—इन करके अपना एकाउन्ट

अपडेट करते तो ये सारी डिटेल हैकर तक पहुंच जाती और वो बाद में ग्राहकों के खातों से लॉग—इन करके पैसा ट्रांसफर कर लेते या ऑनलाइन खरीददारी करते।

18. सायबर अपराधियों ने क्रेडिट कार्ड और डेबिट कार्ड डाटा स्किम करने के लिए अमरीका में गैस फिलिंग स्टेशनों को अपना निशाना बनाया था। हैकर ने अमरीका के दक्षिण भाग में अवस्थित अधिकतर गैस स्टेशनों में चोरी छिपे ब्ल्यू टूथ संचालित (इनेबल्ड) क्रेडिट कार्ड स्किमर लगा दिए थे। ग्राहकों के खाता नम्बर, पिन, सीवीवी आदि जैसी जानकारी चुरा कर मैनहट्टन स्थित अधिकांश एटीएम से 2 मिलियन डॉलर से ज्यादा की राशि निकाली गई थी।
19. आईफोन से डाटा निकालने के लिए पुलिस एजेंसियों द्वारा उपयोग किए जाने वाले टूल्स का प्रयोग करके हैकरों ने अमरीकी की सुप्रसिद्ध महिलाओं के निजी फोटोग्राफ चुराए थे (हैजन, 2014)। माना जाता है कि हैकर एल्कॉमसॉफ्ट फोन पासवर्ड ब्रेकर और आईब्रट नामक सॉफ्टवेयर का इस्तेमाल करके एप्पल की साइट में सेंध लगाते हैं और मशीन में मौजूद बैकअप फाइलों को डाउनलोड कर लेते थे।
20. ऐसी बहुत से घटनाएं हुई हैं, जहां किसी गैर-मित्र राष्ट्र ने संवेदनशील सूचनाओं तक पहुंच बनाने के लिए सायबर अटैक किया है। अमरीका के फाइनेन्शियल सिस्टम की हैकिंग में रूस का हाथ होने का शक, ऐसी ही एक घटना है (फारबेरोव, 2014)। जानकारी मिली थी कि रूसी हैकरों ने एक अग्रणी बैंक जेपी मोर्गन चेज पर सायबर हमला किया था। हैकर बैंक के सर्वर से संवेदी डाटा चुराने में सफल रहे थे।
21. हाल ही में, चीन की एक मोबाइल कम्पनी, शिओमी को चीन के सर्वरों को संवेदी डाटा भेजने का दोषी पाया गया था (कुमार, 2014)। उपयोगकर्ता की जानकारी के बिना, एसएमएस, फोटोग्राफ्स, कॉन्टेक्ट लिस्ट आदि जैसी जानकारी इनमें शामिल थी। ऐसा पहली बार नहीं हुआ है कि चीन की किसी कम्पनी पर जासूसी का शक हुआ हो। अमरीका ने अपने कुछ प्रमुख प्रतिष्ठानों में चीन के उपकरणों के इस्तेमाल पर प्रतिबन्ध लगा दिया है।

# भारत में सायबर सुरक्षा पहल

## 5.1 परिचय

इन्टरनेट के प्रसार से कम्प्यूटरों पर निर्भरता बहुत अधिक बढ़ गई है। सिविल एविएशन सैक्टर (नागरिक उड़ान क्षेत्र), रेलवे का यात्री आरक्षण सिस्टम और संचार नेटवर्क, बंदरगाह प्रबन्धन, बिजली, तेल और प्राकृतिक गैस क्षेत्र की कम्पनियों और संस्थानों, बैंकिंग तथा वित्त, दूरसंचार क्षेत्र जैसे संगठनों के महत्वपूर्ण सूचना तंत्र की सायबर हमले से सुरक्षा एक बड़ी चुनौती है। इन्टरनेट क्राइम कम्पलेन सेन्टर (आईसी 3) को मिली सायबर अपराध की शिकायतों के अनुसार शीर्ष के 50 देशों में भारत का स्थान चौथा है। आईसी 3 की 2014 की रिपोर्ट के अनुसार भारत से ऊपर केवल अमरीका, कनाडा और यूके हैं। (दी टेलीग्राफ, 2015)। भारत में सायबर सुरक्षा के क्षेत्र में प्रशिक्षित मानव शक्ति की कमी गम्भीर चिन्ता का विषय है। चीन, अमरीका और रूस में क्रमशः 125000, 91080 और 23000 प्रशिक्षित सायबर विशेषज्ञ हैं जबकि भारत में इनकी संख्या मात्र 556 है। जो विभिन्न सरकारी एजेंसियों में नियुक्त हैं। (जोशी, 2013)। भारत को आईटी के क्षेत्र में महाशक्ति माना जाता है यानि यह सॉफ्टवेयर का एक प्रमुख निर्यातक है और आईटीईएस— आधारित आउट सोर्स बिजनेस का एक बड़ा केन्द्र है। इस तरह भारत की अर्थव्यवस्था में सूचना प्रौद्योगिकी का योगदान बहुत अधिक है। हाल ही में, यूरोपियन यूनियन (ईयू) ने भारत के डाटा सिक्यूरिटी सिस्टम में खामियां निकाली हैं। उसने देश में सायबर सुरक्षा को मजबूत बनाने के लिए एक संयुक्त विशेषज्ञ दल के गठन का प्रस्ताव किया है ताकि भारत डाटा सेक्योर देश का दर्जा हासिल कर सके (सेन, 2013)। इसलिए, भारत को अपने सूचना सुरक्षा से संबंधित बुनियादी ढांचे को अपग्रेड करने तथा सायबर सुरक्षा नीति को और दुरुस्त बनाने पर गम्भीरता से विचार करना चाहिये ताकि वह ईयू से डाटा सेक्योर नेशन का दर्जा प्राप्त कर सके। आउटसोर्स बिजनेस का केन्द्र बने रहने के लिए यह बहुत जरूरी है क्योंकि इस बिजनेस के मौजूदा 20 अरब से बढ़कर 50 अरब डॉलर तक पहुँचने की सम्भावना है।

## 5.2 भारत में प्रतिकारक (काउन्टर) सायबर सुरक्षा पहल

भारत सरकार ने सायबर सुरक्षा पर हमले का जवाब देने के लिए कुछ पहल की हैं जो इस प्रकार हैं—

### 1. नेशनल काउन्टर टैररिज्म सेन्टर (एनसीटीसी) :

2008 में 26/11 हमले के बाद, सरकार ने काउन्टर टैररिज्म पहल के महत्व को समझा और आतंकवादी कृत्यों से निपटने और जवाब देने की योजना बनाने के लिए रणनीतिकारों को खुफिया जानकारी उपलब्ध कराने के उद्देश्य से नेशनल काउन्टर टैररिज्म सेन्टर (एनसीटीसी) स्थापित करने का प्रस्ताव किया। एनसीटीसी विभिन्न राज्य एजेंसियों और केन्द्र सरकार के बीच तालमेल बैठाएगी और आतंकवाद के

प्रतिकार से संबोधन सभी कार्यवाइयों के बीच समन्वय और नियंत्रण के एक कारगर केन्द्र की तरह काम करेगी। इसे अमरीका के एनसीटीसी और ब्रिटेन के ज्वाइन्ट टैररिज्म एनालिसिस सेंटर की तर्ज पर डिजाइन किया गया है। इसे गैरकूननी कार्यकलाप रोकथाम अधिनियम, (यूएपीए) 1967 के द्वारा शक्तियां प्रदान की गई है। (मृणाल, 2012)

## **2. राष्ट्रीय सूचना सुरक्षा आश्वासन कार्यक्रम (एनआईएसएपी):-**

सरकार और महत्वपूर्ण क्षेत्र के संस्थानों में कार्यरत लोगों को जागरूक बनाने के लिए सीईआरटी—इन ने नेशनल इन्फॉर्मेशन सिक्यूरिटी एश्योरेंश प्रोग्राम (एनआईएसएपी) नाम से एक पहल शुरू की है। इसका उद्देश्य आईएसओ/आईईसी 27001 पर आधारित सूचना सुरक्षा नीति तथा सूचना सुरक्षा के बेहतरीन तौर-तरीके विकसित करना और इन्हें लागू करना है ताकि ये लोग अपने सूचना ढाँचे को सुरक्षित बना सकें। सीईआरटी—इन ने सायबर अपराध की जांच-पड़ताल और कानून लागू करने वाली एजेंसियों तथा न्यायपालिका के लोगों को कार्यगत (हैन्डस ऑन) प्रशिक्षण प्रदान करने के लिए कम्प्यूटर फॉरेन्सिक की सुविधाएं स्थापित की हैं। प्रशिक्षण के इस बुनियादी ढाँचे को और मजबूत किया जा रहा है ताकि नेटवर्क फॉरेन्सिक और मोबाइल फॉरेन्सिक जांच पड़ताल की सुविधा को भी इसमें शामिल किया जा सके। सीआईआरटी—इन डिफेन्स, बैंक, न्यायपालिका तथा कानून लागू करने वाली एजेंसियों के कार्मिकों को प्रशिक्षण देने में सहयोग कर रही है तथा साथ ही सायबर-अपराधों की जांच-पड़ताल में भी सहायता प्रदान कर रही है (श्री नाथ, 2006)।

## **3. कम्प्यूटर इमरजेंसी रिस्पॉन्स टीम— इंडिया (सीईआरटी—इन):-**

सूचना और प्रौद्योगिकी विभाग ने 2004 में इंडियन कम्प्यूटर इमरजेंसी रिस्पॉन्स टीम का गठन किया था। इस टीम का गठन का उद्देश्य, कम्प्यूटर सुरक्षा से जुड़ी घटनाओं पर कार्रवाई करना, सुरक्षा कमजोरियों से अवगत कराना तथा परे देश में आईटी सुरक्षा के कारगर तौर-तरीकों को बढ़ावा देना है और इसे सूचना प्रौद्योगिकी (आईटी) अधिनियम की निगरानी का दायित्व भी सौंपा गया है (सीईआरटी—इन 2014)।

## **4. भारत—अमरीका सायबर सुरक्षा फोरम (आईयूएससीएसएफ):-**

भारत—अमरीका सायबर सुरक्षा फोरम सन् 2001 में स्थापित किया गया था और यह पूरी तरह से केवल ज्ञान—आधारित अर्थव्यवस्था के महत्वपूर्ण ढाँचे की सुरक्षा के लिए गठित किया गया है। भारत और अमरीका के विभिन्न सरकारी और निजी क्षेत्र के संगठन इस फोरम के सदस्य बनाए गए हैं। ये सदस्य फोरम के तत्वावधान में काम करते हैं। फोरम ने सायबर सुरक्षा से जुड़े जोखिमों और साझा सरोकारों का पता लगाया है तथा नेटवर्क आधारित सूचना सिस्टमों को सुरक्षित बनाने के लिए एक ठोस कार्य-योजना तैयार की है। फोरम सायबर सुरक्षा, सायबर फॉरेन्सिक और इससे संबंधित शोध के प्रति समर्पित है तथा दोनों देशों की सायबर अपराधों से निपटने वाली पुलिस एजेंसियों के बीच सहयोग बढ़ाने की दिशा में कार्य करता है।

दोनों देशों के रक्षा सेवा संगठन, प्रौद्योगिकी और प्रक्रियागत पहलुओं पर अपने—अपने अनुभवों के आदान—प्रदान के जरिए परस्पर सम्पर्क बढ़ाएंगे। भारत के एसटीक्यूसी और अमरीका के नेशनल इन्स्टीट्यूट ऑफ स्टैन्डर्ड्स एण्ड टेक्नॉलॉजी (एनआईएसटी) के बीच मौजूदा सहयोग का विस्तार किया जाएगा ताकि दोनों देशों के मानकों को सुसंगत बनाया जा सके तथा नए क्षेत्रों को इसमें शामिल किया जा सके। सीआईआई और इसके अमेरिकी समकक्ष ने एक इंडिया इन्फॉर्मेशन शेयरिंग एण्ड एनालिसिस सेन्टर (आईएसएसी) तथा इंडिया एन्टी-बॉट एलायन्स ('बॉट' से तात्पर्य उस साफ्टवेयर से है, जो हैकर्स की तरफ से कम्प्यूटर में सेंध लगा कर, रिमोट नियंत्रण के जरिए नुकसान पहुंचाने का कृत्य करता है) स्थापित करने का निर्णय लिया है। (पत्र सूचना कार्यालय, 2006)।

#### **5. भारतीय राष्ट्रीय क्रिटिकल इन्फॉर्मेशन इन्फ्रास्ट्रक्चर प्रोटेक्शन सेन्टर (एनसीआईपीसी):—**

भारत के क्रिटिकल इन्फॉर्मेशन इन्फ्रास्ट्रक्चर के संरक्षण के लिए इसे नोडल (केन्द्रोयकृत) एजेंसी के रूप में घोषित किया गया है और सूचना प्रौद्योगिकी के महत्वपूर्ण ढांचे की सुरक्षा के लिए अनुसंधान एवं विकास सहित सभी कदम जरूरी उठाने का दायित्व इसे सौंपा गया है।

एनसीआईपीसी के कुछ कार्यकलाप इस प्रकार हैं:—

- क. महत्वपूर्ण सब—सैक्टरों की पहचान करना,
- ख. पहचान किए गए महत्वपूर्ण सब—सैक्टरों के सूचना ढांचे की समीक्षा करना।
- ग. दैनिक / मासिक सायबर संकट सूचना / चेतावनी जारी करना,
- घ. मैलवेयर विश्लेषण
- ङ. जूम्बी और मैलवेयर फैलाने वाले आईपी एड्रेसेज की निगरानी करना।
- च. सायबर फोरेन्सिक कार्यकलाप
- छ. चुस्त—दुरुस्त और सुरक्षित माहौल के लिए अनुसंधान और विकास
- ज. सीआईआई के संरक्षण के लिए सीआईआई मालिकों को समुचित नीतियां मानक और बेहतरीन तौर—तरीके अपनाने के लिए प्रेरित करना।
- झ. क्रिटिकल सैक्टरों के वास्ते वार्षिक सीआईएसओ सम्मेलन।
- ट. जागरूकता और प्रशिक्षण
- ठ. चौबीसों घण्टे तत्पर हैल्पडेस्क।

#### **6. भारतीय राष्ट्रीय इन्टेलिजेंस ग्रिड (नैटग्रिड) परियोजना:—**

सी—डैक पुणे ने इस एकीकृत इन्टैलीजेंस ग्रिड का विकास किया है। इसमें भारत सरकार की सुरक्षा एजेंसियों के डाटा बेस को कनेक्ट किया गया है (सी—डैक, 2014)। यह आतंकवाद के प्रतिकार की दिशा में एक ऐसा उपाय है, जिसमें सरकार के डाटाबेस से कर तथा बैंक खातों का विवरण, क्रेडिट कार्ड से लेन—देन, वीजा और इमिग्रेशन रिकार्ड तथा रेल और हवाई यात्रा द्वारा विजिट किए गए स्थलों का विवरण

जैसी अनेक तरह की जानकारी जुटा कर इनका सम्पर्क निकाला जाता है (यास्मीन, 2013)। यह संयुक्त डाटा 11 केन्द्रीय एजेंसियों जैसे रिसर्च एण्ड एनालिसिस विंग, इन्टैलीजेंस ब्यूरो, सीबीआई, फाइनेन्सियल इन्टैलीजेंस यूनिट, केन्द्रीय प्रत्यक्ष कर बोर्ड, राजस्व आसूचना निदेशालय, प्रवर्तन निदेशालय, नारकोटिक्स कन्ट्रोल ब्यूरो, बोर्ड ऑफ एक्साइज एण्ड कस्टम, केन्द्रीय आसूचना महानिदेशालय को उपलब्ध कराया जाता है।

#### **7. भारतीय क्राइम एण्ड क्रिमिनल ट्रैकिंग नेटवर्क एण्ड सिस्टम्स (सीसीटीएनएस) परियोजना:-**

राष्ट्रीय ई-प्रशासन योजना (एनईजीपी) के तहत बनाई गई इस परियोजना के तहत सभी 28 राज्यों और 7 केन्द्र शासित प्रदेशों को शामिल किया जाएगा। इसका उद्देश्य अपराधों की जांच-पड़ताल और अपराधियों को तलाशने के लिए सूचना प्रौद्योगिकी से संचालित अत्याधुनिक निगरानी प्रणाली के विकास हेतु नेटवर्किंग का एक राष्ट्रव्यापी बुनियादी ढांचा तैयार किया जाएगा (पीटीआई, 2013)। सीसीटीएनएस डाटा और सूचना जुटाने, कम्प्यूटरों से इन्हें पुनः हासिल करने, इनका विश्लेषण करने और पुलिस स्टेशन तथा पुलिस स्टेशनों एवं राज्यम मुख्यालयों एवं केन्द्रीय पुलिस संगठनों के बीच इन्हें अंतरित करने और साझा करने की सुविधा प्रदान करेगा। सीसीटीएनएस अपराधों और अपराधियों के बारे में व्यापक डाटाबेस उपलब्ध कराएगा। इससे कानून व्यवस्था को बनाए रखने वाली संस्थाओं को बार-बार अपनी जगह बदलने वाले अपराधियों को ट्रैक करने में मदद मिलेगी।

#### **8. राष्ट्रीय साइबर समन्वयन केन्द्र (एनसीसीसी):-**

इस भावी परियोजना में सायबर सुरक्षा और ई-सर्वेलांस के लिए भारत में एक एजेंसी स्थापित करने का प्रस्ताव है। यह एजेंसी मुख्यतया कम्पूनिकेशन मैटाडाटा की स्क्रीनिंग और आसूचना (इन्टैलीजेंस) जुटाने वाली अलग-अलग एजेंसियों के बीच तालमेल कायम करेगी। एनसीसीसी को सौंपे जाने वाले विषयों में सायबर हमले के रोकथाम की कार्यनीति, सायबर हमले की जांच पड़ताल और प्रशिक्षण आदि शामिल हैं।

#### **9. बॉटनेट क्लीनिंग सेन्टर:-**

डिजिटल इंडिया प्रोग्राम के एक भाग के रूप में, सरकार एक केन्द्र स्थापित करने जा रही है जो “बॉटनेट” जैसे मैलेसियस प्रोग्राम को खोजेगी और लोगों को ऐसे नुकसानदेय सॉफ्टवेयरों को अपने उपकरणों से हटाने में सहायता देगी। मीडिया में प्रकाशित रिपोर्ट के अनुसार, “सरकार बॉटनेट क्लीनिंग मैलवेयर एनालिसिस सेन्टर स्थापित करने जा रही है।” बॉटनेट मैलासियस साफ्टवेयर का एक नटवर्क है, जो सूचना चुरा सकता है, उपकरण के फंक्शन को अपने कब्जे में ले सकता है और डिस्ट्रीब्यूटेड डिनायल-ऑफ-सर्विसेज (डीडॉस) जैसे सायबर हमले कर सकता है।

#### **10. भारत सरकार की ईमेल नीति:-**

आज लोगों के बीच और विभिन्न संगठनों के बीच पत्र व्यवहार के लिए या सम्पर्क के लिए ईमेल एक प्रमुख साधन बन गया है। और यही बात सरकार (भारत सरकार) पर भी लागू होती है। पूरी सरकार के लिए संचार का माध्यम ईमेल बन गया है। विभिन्न सरकारी एजेंसियों के बीच संचार का माध्यम ईमेल को देखते हुए, भारत सरकार ने अक्टूबर, 2013 में ई-मेल नीति तैयार की। यहां हम ईमेल नीति के कुछ महत्वपूर्ण प्रावधानों पर चर्चा करने जा रहे हैं। आपसे अनुरोध है कि इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी विभाग की वेबसाइट से इस नीति को डाउनलोड कर लें।

#### **11. गृह मंत्रालय (एमएचए):-**

गृह मंत्रालय भारत सरकार का एक मंत्रालय है। आंतरिक मंत्रालय के तौर पर इसका दायित्व देश की आंतरिक सुरक्षा को कायम रखना और घरेलू नीतियों को लागू करना है। गृह मंत्रालय की जिम्मेदारी बहुआयामी है। इसमें सबसे महत्वपूर्ण आन्तरिक सुरक्षा, सीमा प्रबंधन, राज्यों और केन्द्र के बीच सम्बन्ध, केन्द्रशासित प्रदेशों का प्रशासन, केन्द्रीय सशस्त्र पुलिस बल का प्रबंधन और आपदा प्रबंधन आदि हैं।

### **12. राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (एनसीआरबी):-**

एनसीआरबी भारतीय पुलिस को कानूनों को कारगरता और कुशलता से लागू करने और सार्वजनिक सेवाओं की सहज सुलभता सुनिश्चित करने के लिए सूचना प्रौद्योगिकी तथा आपराधिक खुफिया जानकारी उपलब्ध कराकर सशक्त बनाने की दिशा में काम करेगा। यह लक्ष्य हासिल करने के लिए राष्ट्रीय और अन्तर्राष्ट्रीय स्तर पर पुलिस बलों के साथ तालमेल, अपराध विश्लेषण की तकनीकों का उन्नयन, सूचना प्रौद्योगिकी के विकास तथा सूचना प्रौद्योगिकी संचालित समाधानों को मजबूत बनाया जाएगा।

### **13. भारतीय डाटा सुरक्षा परिषद (डीएससीआई):-**

नैसकॉम द्वारा स्थापित भारतीय डाटा सुरक्षा परिषद भारत में डाटा प्रोटेक्शन का एक प्रमुख औद्योगिक निकाय है। परिषद सायबर सुरक्षा और निजता (पाइवेसी) के क्षेत्र में सर्वश्रेष्ठ तौर—तरीके, मानक—और अनेक पहलें लागू करके सायबर जगत को सुरक्षित और भरोसेमंद बनाने के प्रति कटिबद्ध है। डीएससीआई राज्य सरकारों और उनकी एजेंसियों, डाटा संरक्षण प्राधिकरणों, औद्योगिक संगठनों, जन सहयोग के लिए विद्वत समुदायों, दूरदर्शी नेतृत्व, क्षमता निर्माण तथा आउटरीच (सामुदायिक पहुँच) प्रयासों को साथ लाने का एक मंच बना है। अपने उद्देश्यों को आगे बढ़ाने के लिए, डीएससीआई सरकारों, नियम नियामकों, औद्योगिक संगठनों और नीतिगत मामलों से जुड़े विद्वानों के सम्पर्क में रहता है। सायबर सुरक्षा और निजता के क्षेत्र में दूरदर्शी नेतृत्व को मजबूत बनाने के लिए, डीएससीआई सर्वश्रेष्ठ कार्यपद्धतियाँ और फ्रेमवर्क तैयार करता है, अध्ययनों और सर्वेक्षणों पर दस्तावेज प्रकाशित करता है। परिषद पेशेवरों और कानून लागू करने वाली एजेंसियों के प्रशिक्षण तथा प्रमाणन कार्यक्रम आयोजित करके सुरक्षा, निजता और सायबर फोरेन्सिक के क्षेत्र में क्षमता निर्माण का कार्य करती है और समारोह, पुरस्कार, विचार—विनिमय, परामर्श और सदस्यता कार्यक्रमों के साथ—साथ विभिन्न सम्पर्क प्रयासों के जरिए हितधारकों की सेवाएं लेती है। डीएससीआई विश्व के साथ व्यापार वृद्धि की पहल के माध्यम से विश्वबाजार में सुरक्षा उत्पाद और सेवाओं के क्षेत्र में भारत की भागीदारी बढ़ाने के लिए भी प्रयासरत है। इसका उद्देश्य भारत में सुरक्षा और निजता की संस्कृति को मजबूत बनाना है।

# सुरक्षित पासवर्ड बनाने के दिशा-निर्देश, द्वि-चरणीय सत्यापन और फ्री एन्टी वायरस का उपयोग

## 6.1 सुरक्षित पासवर्ड बनाना

### 6.1.1 सुरक्षित पासवर्ड सेट करने के दिशा-निर्देशः—

कई लोगों को सही पासवर्ड चुनने में दिक्कत होती है। आजकल पासवर्ड बनाने के लिए कई चीजें जोड़नी होती हैं और उन्हें याद रखना वास्तव में एक समस्या है। शायद इसी वजह बहुत से लोग अपना पासवर्ड ठीक से नहीं चुनते। नीचे कुछ सामान्य से नुस्खे दिए गए हैं, जिनके जरिए आप एक अच्छा पासवर्ड चुन सकेंगे।

#### मूल बातें

- कम से कम आठ कैरेक्टर का उपयोग करें, जितने ज्यादा कैरेक्टर (वर्णाक्षर) होंगे उतना ही अच्छा पासवर्ड बनेगा, लेकिन यह भी ध्यान रखें कि ज्यादातर लोग लगभग 15 कैरेक्टर से ज्यादा याद नहीं रख पाते।
- कैरेक्टर का चयन रैण्डम (यादृच्छ यानि कहीं भी कोई भी) होना चाहिए, अपर और लोअर केस (यानि ब्लॉक लैटर और स्माल लैटर का मिश्रण), अंकों, पंक्चुएशन (विसर्ग चिन्ह), स्पेस और सिम्बल का उपयोग करें।
- शब्द कोश में मिलने वाले शब्दों, अंग्रेजी अथवा अन्य विदेशी भाषाओं के शब्दों का प्रयोग न करें।
- एक ही पासवर्ड कभी भी दोबारा प्रयोग न करें।

#### इनसे बचें

- किसी शब्द के पहले या बाद में केवल एक अंक या सिम्बल न जोड़ें। उदाहरण— "apple1"
- एक ही शब्द को डबल-अप न करें। उदाहरण— "appleapple"
- किसी शब्द को उल्टा न लिखें। उदाहरण— "elppa"
- किसी शब्द से केवल वोवेल (स्वर) हटा कर कामन चलाएं। उदाहरण— "ppl"

- की सीक्वेंस जिन्हे आसानी से दोहराया जा सकता है। उदाहरण— "Qwerty", "asdfg" आदि।
- केवल अक्षरों को गार्बल न करें। उदाहरण में को 3 में, ₹ अथवा € को 1, 0 का ₹ में बदलना जैसा कि 3ro या Lov3 आदि।

## नुस्खे

- ऐसा पासवर्ड चुनें, जिसे आप याद रख सकते हैं ताकि आपको इसे नोट न करना पड़े। इससे किसी को यह पता नहीं लगेगा कि आपने पासवर्ड कहां नोट कर रखा है।
- ऐसा पासवर्ड चुने जिसे आप तेजी से टाइप कर सकते हैं। इससे आपके पीछे से झांकने वाले व्यक्ति को आपका पासवर्ड समझने का मौका नहीं मिलेगा।

## खराब पासवर्ड

- अपने नाम, प्रचलित नाम, जन्मतिथि, पत्नी के नाम, अपने पालतू पशु—पक्षी के नाम, दोस्त के नाम, होम टाउन के नाम, फोन नं., सोशल सिक्यूरिटी नम्बर, कार रजिस्ट्रेशन नम्बर, पता आदि जैसी व्यक्तिगत सूचना के नाम पर पासवर्ड न बनाएं। इसमें नाम का कोई हिस्सा या जन्मतिथि के कुछ अंक आदि भी शामिल हैं।
- अपने आसपास की चीजों के आधार पर पासवर्ड न बनाए। जैसे— कम्प्यूटर, मॉनीटर, कीबोर्ड, टेलीफोन, प्रिन्टर आदि।
- अत्यन्त सामान्य शब्दों को भी पासवर्ड न बनाएं। इन्हें याद रखना तो आसान होता है पर ये सुरक्षित नहीं हैं जैसे "password" "letmein" आदि।
- अपने यूजर नेम, एकाउन्ट नेम, कम्प्यूटरनेम ईमेल एड्रेस को आधार बनाकर कभी पासवर्ड न बनाएं

## पासवर्ड का चयन

- किसी अच्छे पासवर्ड जनरेटर सॉफ्टवेयर का प्रयोग करें।
- किसी गाने का, कविता की किसी लाइन के प्रत्येक शब्द के पहले अक्षर का प्रयोग करें।
- प्रत्येक व्यंजन (कन्सोनेट) के बीच एक या दो स्वर (वोवल) डाल कर कोई अर्थहीन (नॉनसेन्स) शब्द बनाएं। उदाहरण "taoupouti"
- कोई दो छोटे शब्द चुनें और इनके बीच कोई विसर्ग (पंक्त्युएशन) या निशान (सिम्बल) डाल दें। उदाहरण "seat%tree"

## **पासवर्ड बदलना**

- समय—समय पर पासवर्ड बदलते रहें। सुझाव है कि महीने में एक बार पासवर्ड अवश्य बदलें।
- जब भी आपको शक हो कि किसी को पासवर्ड का पता चल गया है, इसे अवश्य बदलें।
- याद रखें कि पासवर्ड का री—यूज न करें।

## **पासवर्ड को सुरक्षित बनाना**

- कभी भी पासवर्ड को कम्प्यूटर में स्टोर न करें। यदि ऐसा करना हो तो एनक्रिप्टेड फार्म में स्टोर करें।
- ध्यान रखें कि विन्डोज के साथ आने वाला पासवर्ड कैशे (चूसपिसमें) सुरक्षित नहीं है। इसलिए यदि विन्डोज “सेव पासवर्ड” का ऑप्शन दें, तो इसे नकार दें।
- अपना पासवर्ड किसी को यहां तक कि अपने एडमिनिस्ट्रेटर तक को भी न बताएं।
- कभी भी अपना पासवर्ड ईमेल अथवा किसी अन्य असुरक्षित चैलन के जरिए न भेजें।
- हाँ, अपना पासवर्ड लिख लें, पर इस कागज को लापरवाही से यहां—वहां न छोड़ें। किसी ऐसी सुरक्षित जगह पर रखें, जहां किसी की नजर न पड़े। बेहतर होगा कि इसे ताला लगा कर रखें।
- यदि आपके कमरे में कोई अन्य व्यक्ति मौजूद है, तो पासवर्ड एण्टर करते समय बहुत सावधान रहें।

## **पासवर्ड याद रखना**

- पासवर्ड याद रखना मुश्किल होता है, इसलिए बहुत से लोग इसे कागज के टुकड़े पर नोट कर लेते हैं। यह अच्छा नहीं है। तो अब करें क्या?
- सेक्यॉर पासवर्ड मैनेजर का प्रयोग करें। ऐसे ही कुछ पासवर्ड मैनेजर हैं, इनके डाउनलोड्स देख लें, इसके लिए आपको कोई कीमत नहीं चुकानी है।
- स्ट्रॉग एन्क्रिप्शन साप्टवेयर से एनक्रिप्ट की गई टैक्स्ट फाइल का प्रयोग करें।
- ऐसा पासवर्ड चुनें जिसे याद रखना आसान हो।

## **खराब उदाहरण**

- "Fred8" —यूजर नेम पर आधारित है और बहुत छोटा है।
- "christine" —यूजर की गर्लफैण्ड का नाम, आसानी से अनुमान लगाया जा सकता है।
- "kciredref" —यूजर नेम विपरीत क्रम में लिखा गया है।

- "indescribable" — शब्दकोश में है।
- "indescribable" — बीच—बीच में ब्लॉक लैटर—यूज करने से यह सुरक्षित नहीं हो गया है।
- "Gandalf" — शब्द सूची में दिया गया है।
- "Zeolicte" — भौवैज्ञानिक शब्दकोश में है।
- "Qwertyuiop" — की बोर्ड के क्रम में है।
- "merde" — विदेशी भाषा के शब्दकोश में है।

## अच्छे पासवर्ड के उदाहरण

- नीचे दिए गए अच्छे उदाहरण दरअसल अच्छे उदाहरण नहीं माने जा सकते क्योंकि इन्हें यहां छाप दिया गया है। अपना पासवर्ड स्वयं चुनें, किसी और का पासवर्ड प्रयोग न करें।  
"mitwdotw4me"- Mondoy is the worst day for me.
- कोई सम्भावित हैकर ऐसे किसी का पासवर्ड हॉसिल कर सकता है?  
हैकर किसी का पासवर्ड प्राप्त करने के लिए चार तकनीकों का इस्तेमाल कर सकता है।

### 1. चुराना:-

जब आप इसे टाइप करें, आपके पीछे से झांक कर या जहाँ आपने लिख कर रखा है उसे तलाश कर। यह पासवर्ड हासिल करने का सबसे आम तरीका है। इसलिए, जरूरी है कि आप यदि पासवर्ड लिख कर रखते हैं तो इसे पूरी तरह सुरक्षित जगह पर रखें। साथ ही यह भी ध्यान रखें कि जब आप पासवर्ड टाइप कर रहे हो तो कोई इसे देख न सके।

### 2. अनुमान लगाना:-

हैरत की बात है कि ज्यादातर लोग ऐसे पासवर्ड चुनते हैं, जिनका आसानी से अनुमान लगाया जा सकता है। मनोवैज्ञानिकों का कहना है कि ज्यादातर पुरुष पासवर्ड में अभद्र शब्दों का चयन करते हैं और महिलाएं अपने प्रेमी, पति या बच्चे के नाम को चुनती हैं।

### 3. ब्रूट फोर्स अटैक:-

इस प्रक्रिया में, पासवर्ड हासिल करने के लिए हर सम्भव तरीका अपनाया जाता है जैसे कि अक्षरों और अंकों तथा गणितीय चिन्हों को परस्पर किस प्रकार मिलाकर पासवर्ड बनाया है, इनके सम्भवतः कितने मिले जुले शब्द बन सकते हैं इसकी गणना की जाती है। यह अत्यंत श्रमसाध्य प्रक्रिया है, लेकिन आधुनिक फास्ट प्रोसेसर और साप्टवेयर टूल्स को देखते हुए इसे कम करके नहीं आंका जा सकता। पेन्टियम 100

कम्प्यूटर एक सेकेन्ड में 200000 काम्बिनेशन को जाँच सकता है यानि 6 करैक्टर के पासवर्ड जिसमें अपर केस और लोअर केस के करैक्टर को मिलाया गया है, जानने में उसे केवल 27.30 घण्टे लगेंगे।

#### 4. डिक्षनरी अटैक:-

ब्रूट फोर्स अटैक से भी ज्यादा बुद्धिमत्तापूर्ण अटैक डिक्षनरी अटैक है। इसमें पासवर्ड बनाने के लिए चयन किए गए मिश्रण को सबसे पहले डिक्षनरी में उपलब्ध शब्दों में तलाशा जाता है। ऐसे साप्टवेयर उपलब्ध हैं, जो लाखों शब्दों वाले शब्दकोश, साथ ही विशिष्ट, तकनीकी और विदेशी भाषा के शब्दकोशों को खंगाल कर आपके पासवर्ड को खोज सकते हैं इसके अलावा छूतजला छबकमठि आदि जैसे हजारों पासवर्ड को तलाश सकते हैं।

### 6.2 पासवर्ड मैनेजर का इस्तेमाल:-

हम अपने डाटा की सुरक्षा और गोपनीयता के लिए पासवर्ड का प्रयोग करते हैं। पासवर्ड पता लगा कर अपराध को अंजाम देना आजकल आम हो गया है। इसलिये अच्छा पासवर्ड बनाना समय की मांग है। आपने कभी अपने पासवर्ड को याद रखने और बार-बार अपना विवरण न देने के बारे में सोचा है? पासवर्ड मैनेजर, पासवर्ड स्टोर करने, इसे मैनेज करने और इसका बैकअप रखने का एक सर्वश्रेष्ठ तरीका है। अच्छा पासवर्ड याद रखना मुश्किल होता है और यहीं, पासवर्ड मैनेजर की आवश्यकता पड़ती है। पासवर्ड मैनेजर उन सभी पासवर्ड को मास्टर पासवर्ड से एनक्रिप्ट कर देता है जिन्हें सेव कर लेता है। आप को केवल मास्टर पासवर्ड को याद रखना है।

#### 6.2.1 पासवर्ड मैनेजर क्या है?

पासवर्ड मैनेजर एक साप्टवेयर है जो यूजर को पासवर्ड और महत्वपूर्ण सूचना संभालने में मदद करता है ताकि कभी भी और कहीं वह इनका उपयोग कर सकें। एक उत्कृष्ट पासवर्ड मैनेजर सुरक्षा से कोई समझौता किए बिना सूचना संरक्षित और स्टोर करने में मदद करता है। मैनेजर सभी पासवर्ड को किसी न किसी रूप में एनक्रिप्ट करके सेव करता है, ताकि कोई अन्य इनका दुरुपयोग न कर सके।

#### 6.2.2 इसका प्रयोग क्यों करें?

यदि आपको प्रत्येक वेबसाइट का पासवर्ड याद रखना परेशानी भरा लगता है और आप बार-बार “फोरगॉट पासवर्ड” प्रश्न से नहीं गुजरना चाहते, तो पासवर्ड मैनेजर ही आपकी यह परेशानी हल कर सकता है। इन्हें अलग-अलग वेबसाइटों से संबंधित सभी प्रकार की महत्वपूर्ण लॉगइन सूचनाओं को स्टोर करने के लिए डिजाइन किया गया है।

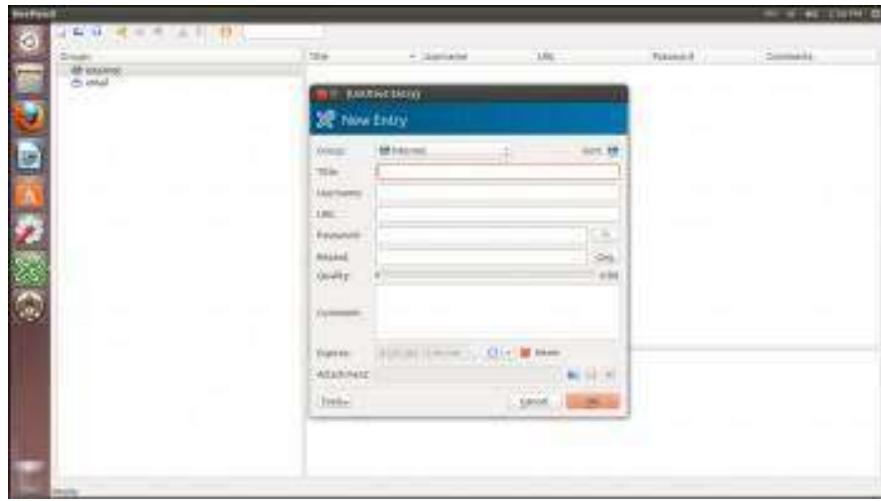
### **6.2.3 यह किस तरह काम करता है?**

पासवर्ड मैनेजर ऑनलाइन अथवा लोकल सर्वर दोनों में स्टोर किए जा सकते हैं। ऑनलाइन पासवर्ड मैनेजर सूचना को ऑनलाइन क्लाउड में स्टोर करते हैं, जिसे आप कहीं भी कभी भी हासिल कर सकते हैं। लोकल पासवर्ड मैनेजर लोकल सर्वर पर स्टोर करते हैं, इसलिए ये थोड़ा कम एक्सेसिबल होते हैं। दोनों के अपने-अपने फायदे हैं। आप कौन सा चाहेंगे, यह आपकी जरूरत पर निर्भर करेगा। ऑनलाइन पासवर्ड मैनेजर ब्राउजर एक्सटेंशनों का इस्तेमाल करते हैं जो डाटा को क्लाउड सर्वर से सिंक करके लोकल प्रोफाइल में रखते हैं। कुछ अन्य पासवर्ड मैनेजर पासवर्ड सेव करने के लिए रिमूवेबल मीडिया का इस्तेमाल करते हैं, आप ऑनलाइन समस्याओं की चिन्ता किए बिना इसे अपने साथ कहीं भी ले जा सकते हैं। इन दोनों विकल्पों को एक साथ भी इस्तेमाल किया जा सकता है। इस तरह आप दोहरे सत्यापन के जरिए डाटा को और ज्यादा सुरक्षित बना सकते हैं।

### **6.2.4 कुछ लोकप्रिय पासवर्ड मैनेजर**

पासवर्ड अलग-अलग एनक्रिप्शन का इस्तेमाल करके सेव किए जाते हैं और यह कम्पनी द्वारा प्रदत्त सेवाओं पर निर्भर करता है। बढ़िया पासवर्ड मैनेजर बेहतर सुरक्षा के लिए 256-बिट (या अधिक) एनक्रिप्शन प्रोटोकॉल का प्रयोग करते हैं। अमरीका की राष्ट्रीय सुरक्षा एजेंसी ने भी अत्यन्त गोपनीय सूचनाओं को संभालने के लिए इसे मंजूरी दी है। यदि आप पासवर्ड मैनेजर इस्तेमाल करने की सोच रहे हैं और अभी तक यह तय नहीं किया है किसे चुना जाए तो पांच विकल्प नीचे दिए गए हैं:-

- की पास एक्स:**- की पास एक्स एक मुक्त सोर्स, क्रॉस-प्लेटफार्म और बहुत कम डिवाइस स्पेस धेरने वाली पासवर्ड मैनेजमेंट एप्लीकेशन है। इसे जीएनयू जनरल पब्लिक लाइसेंस की शर्तों के तहत उपलब्ध कराया गया है। इसे क्यूटी लायब्रेरीज के आधार पर बनाया गया है। की पास एक्स यूजर नेम, पासवर्ड तथा अन्य लॉगइन जानकारी एक सुरक्षित डाटा बेस में स्टोर करता है। की पास एक्स अपना खुद का ऐण्डम पासवर्ड जनरेटर प्रयोग करता है, जिससे बेहतर सुरक्षा के लिए स्ट्रॉंग पासवर्ड बनाना आसान हो जाता है। इसमें शक्तिशाली तथा तुरन्त सर्च करने वाला एक टूल भी दिया गया है जिसकी सहायता से किसी वेबसाइट के की-वर्ड का उपयोग करके डाटाबेस में स्टोर किए गए लॉगइन क्रेडेन्शियल खोजे जा सकते हैं। यह यूजर को गुप्त कर्स्टमाइज करने की सुविधा भी देता है तथा इसे और ज्यादा यूजर फ्रैन्डली बनाता है। की पास एक्स केवल यूजरनेम और पासवर्ड ही सेव नहीं करता बल्कि नोट्स और किसी भी प्रकार की गुप्त टेक्स्ट फाइलों से भी युक्त है।



चित्र 9 : की पास एक्स

### विशेषताएं

- आसान यूजर इन्टरफ़ेस : इसका लैपट पैन ट्री स्ट्रक्चर अलग—अलग ग्रुप्स और एन्ट्रीज में अन्तर करना आसान बनाता है, जबकि राइट पैन विस्तार से सूचना दिखाता है।
- पोर्टेबल मीडिया एक्सेस : इसकी यह विशेषता इसे और ज्यादा उपयोगी बनाती है क्योंकि इस सुविधा के चलते इसे हर—एक कम्प्यूटर में इन्स्टॉल करना जरूरी नहीं है।
- सर्च फंक्शन: पूरे डाटाबेस और प्रत्येक ग्रुप को सर्च करता है।
- ऑटोफ़िल: लॉगइन क्रेडेन्शियल में टाइप करने की जरूरत नहीं है; वेब पेज जब भी लोड किया जाता है, एप्लीकेशन यह कार्य खुद कर देता है। यह सुविधा इसे की लॉगर्स से सुरक्षित बनाती है।
- पासवर्ड जनरेटर: यह विशेषता स्ट्रॉग पासवर्ड जनरेट करने में मदद करती है और डिक्शनरी अटैक की सम्भावना नहीं रहती। इसे कर्स्टमाइज किया जा सकता है।
- टू फैक्टर अथॉन्टिकेशन: इसकी सहायता से यूजर मास्टर पासवर्ड या रिमूवेबल ड्राइव की एक की से डाटाबेस अनलॉक कर सकता है।
- एड्स अटैचमेंट: किसी भी तरह के गोपनीय डॉक्यूमेंट को अटैचमेंट के रूप में जोड़ा जा सकता है और इस तरह पासवर्ड के अलावा डॉक्यूमेंट को भी सैक्योर बनाया जा सकता है।
- क्रॉस—प्लेट फॉर्म सपार्ट:— यही सभी सपोर्टेड प्लेटफार्म पर काम करता है। की पास एक ओपन सोर्स एप्लीकेशन है; इसलिए सोर्स कोड कम्पाइल किया जा सकता है और किसी भी ऑपरेटिंग सिस्टम में उपयोग किया जा सकता है।

- सुरक्षा: पासवर्ड डाटाबेस को एईएस एनक्रिप्शन अथवा ट्रॉफिश एल्गोरिथम, जो 256-बिट की एनक्रिप्शन का इस्तेमाल करता है, के द्वारा एनक्रिप्ट किया गया है।
- एस्क्वाइरेशन डेट: यूजर द्वारा तय तारीख के अनुसार एन्ट्रीज को एक्सपायर किया जा सकता है।
- एन्ट्रीज के एक्सपोर्ट और इम्पोर्ट की सुविधा: पीडब्ल्यू मैनेजर अथवा केवैलेट के द्वारा एन्ट्रीज इम्पोर्ट और टैक्स्ट फाइल के रूप में एक्सपोर्ट की जा सकती है।
- मल्टी-लैंग्वेज सपोर्ट: यह 15 भाषाओं को सपोर्ट करता है।

**2. किलपर्ज़:**— किलपर्ज वेब-आधारित, ओपनसोर्स वाला पासवर्ड मैनेजर है, जिसे लॉगइन इन्फोर्मेशन सुरक्षित रूप से स्टोर करने के लिए बनाया गया है। इसकी सहायता से बिना किसी डिवाइस, बिना किसी इंस्टालेशन के कहीं से भी डाटा तक पहुंचा जा सकता है। किलपर्ज में इसका एक ऑलनलाइन वर्जन भी जोड़ा गया है, जो इन्टरनेट कनेक्शन न होने पर भी काम करेगा।



**चित्र 10 : किलपर्ज**

#### **विशेषताएँ:**—

- लॉगइन क्रेडेन्शियल टाइप किए बिना, केवल एक किलक से किसी भी वेबसाइट में लॉगइन किया जा सकता है।
- ऑफलाइन डाटा : केवल एक किलक से एचटीएमल पेज के रूप में डाटा की एनक्रिप्टेड लोकल कॉपी तैयार की जा सकती है।
- कोई इन्टॉलेशन नहीं : यह एक वेब आधारित एप्लीकेशन है, इसके लिए किसी इन्स्टॉलेशन की जरूरत नहीं है और किसी भी कम्पैटिबल ब्राउजर के द्वारा इसे एक्सेस किया जा सकता है।

- सुरक्षा : डाटा को ब्राउजर पर जावा स्क्रिप्ट कोड का प्रयोग करके एनक्रिप्ट किया जाता है और फिर वेबसाइट पर भेजा जाता है। डाटाबेस को पासफ्रेज के बिना डिक्रिप्ट नहीं किया जा सकता और इसके बिना आप डाटा नहीं पढ़ पायेंगे।
- डाटा इम्पोर्ट: अलग—अलग डाटा मैनेजर से सपोर्ट वाले लॉगइन डाटा इम्पोर्ट किए जा सकते हैं।
- सपोर्ट: जावा स्क्रिप्ट से चलने वाले ब्राउजरों से युक्त किसी भी ऑपरेटिंग सिस्टम पर काम करने में सक्षम है।

**3. पासपर्ड गोरिल्ला:**— यह एक ओपन सोर्स सॉफ्टवेयर है। इसमें क्रॉस—प्लेट फॉर्म, सिम्पल पासवर्ड मैनेजर और निजी वॉल्ट की सुविधा उपलब्ध है, जिसमें लॉगइन इन्फॉर्मेशन और नोट्स स्टोर किए जा सकते हैं। पासपर्ड गोरिल्ला टीसीएस/टीके एप्लीकेशन है जो लिनक्स, विन्डोज और मैक ओएसएक्स पर काम करतो है। लॉगइन इन्फॉर्मेशन डाटाबेस में स्टोर की जाती है जिसे केवल मास्टर पासवर्ड के द्वारा ही एक्सेस किया जा सकता है। पासपर्ड एसएचए 250 द्वारा प्रोटेक्टेड होते हैं और डाटाबेस टूफिस एलगोरिथिम के प्रयोग द्वारा सेक्योर किए जाते हैं। इसकी स्ट्रेचिंग खूबी ब्रूट फोर्स अटैक से बचाती है।



**चित्र 11. पासवर्ड गोरिल्ला**

### विशेषताएं

- पोर्टेबल: बिना इन्स्टॉल किए कम्प्यूटर पर रन करने के लिए डिजाइन।
- कम्प्यूटर का इस्तेमाल न होने पर डाटाबेस लॉक करता है : यदि कम्प्यूटर कुछ खास समय तक एकिटव न रहे तो डाटाबेस खुद-ब-खुद लॉक हो जाता है।
- सुरक्षा : डाटाबेस को एनक्रिप्ट करने के लिए टूफिश एल्गोरिथिम का उपयोग करता है।
- क्रेडेंशियल कॉपी करने में सक्षम : विलपबोर्ड पर लॉगइन कॉपी करने के लिए की बोर्ड शॉर्टकट के इस्तेमाल की सुविधा।
- ऑटो क्लीअर: एक नियत समय के बाद यह खूबी विलपबोर्ड को क्लीयर कर देती है।

- ग्रुप बनाने की सुविधा : अलग-अलग वेबसाइटों के पासवर्ड व्यवस्थित करने के लिए ग्रुप और सब-ग्रुप (उप समूह) बनाए जा सकते हैं।

**4. जी पासवर्ड मैनेजर** :— यह पासवर्ड एक्सेस करने (पढ़ने) और इस सम्भलाने का एक असान, कम स्पेस धेरने और क्रॉस प्लेटफार्म उपलब्ध कराने वाला एक सॉफ्टवेयर है। इसे अपाचे लाइसेंस की शर्तों के तहत उपलब्ध कराया गया है। यह पासवर्ड/ यूआरएल डाटा बेस में सुरक्षित रूप से स्टोर करने की सुविधा देता है। इसमें आप एडेड एन्ट्रीज को फेवरट (पसंदीदा) के तौर पर मार्क करके सेव कर सकते हैं। और सिस्टम द्वे आइकान को राइट क्लिक करके एक्सेस कर सकते हैं। यदि आप चाहें तो स्क्रीन पर नजर आने वाले पासवर्ड तथा अन्य लॉगइन सूचनाओं को हिडन भी कर सकते हैं।



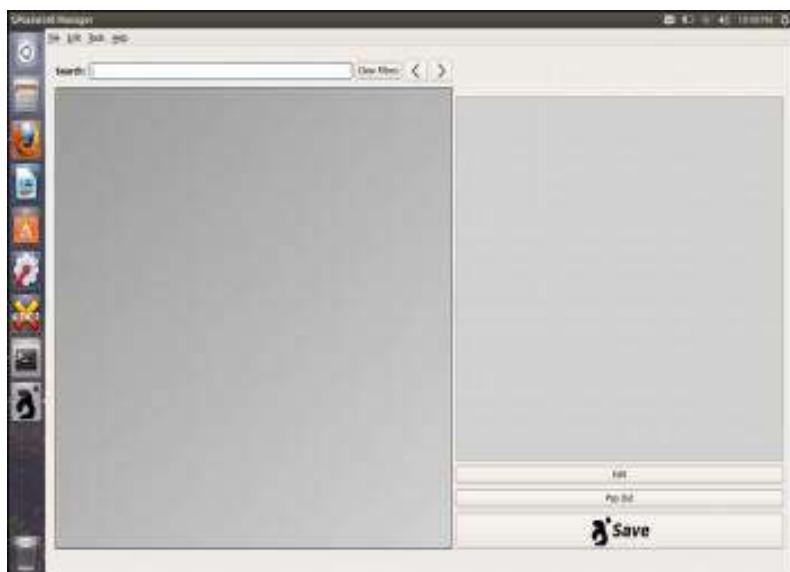
चित्र 12 : जी पासवर्ड मैनेजर

#### विशेषताएँ:-

- पसंदीदा साइटों तक एक्सेस : इसमें “द्रे” आइकन से तुरन्त पसंदीदा साइटों को तलाशने की सुविधा दी गई है।
- किवक फ़िल: फॉर्म में पासवर्ड या किसी इन्फोर्मेशन को फ़िल करने के लिए इन्हें क्लिक और ड्रेग करके वहां फ़िल करने की सुविधा दी गई है।
- सर्चबार : यूजर को अपनी जरूरत के अनुसार पासवर्ड तुरन्त सर्च करने की सुविधा दी गई है।
- पासवर्ड जनरेटर: यूजर द्वारा तय विकल्पों के अनुसार पासवर्ड जनरेट किए जा सकते हैं।
- किवक लॉच: द्रे आईकॉन को क्लिक करके पसंदीदा साइट खोल सकते हैं।

**5. पासवर्ड सेफ** :— यह आसान सा एक ओपन सोर्स एप्लीकेशन है जो निःशुल्क उपलब्ध है। ब्रस श्नीअर ने इसकी पहल की थी और 2002 में यह रिलीज हुआ था। अब वॉलन्टीर्स के एक समूह ने इसे डेवलप करके सोर्सफोर्ज कर होस्ट किया है। यह उपयोग करने में बहुत असान है। यूजर के प्रीफरेन्स के आधार

पर पासवर्ड आर्गनाइज करना सम्भव है, जिससे यूजर को इन्हें याद रखना आसान हो जाता है। पूरे डाटाबेस का बैकअप लेने और रिकवरी की सुविधा ने इसका प्रयोग और आसान बना दिया है। पासवर्ड हिडन रहते हैं अतः चोरी—छुपे पासवर्ड जानना आसान नहीं होता। आप्टिस्टिक लाइसेंस के तहत पासवर्ड सेफ को लाइसेंस प्राप्त है।



**चित्र 13 : पासवर्ड सेफ**

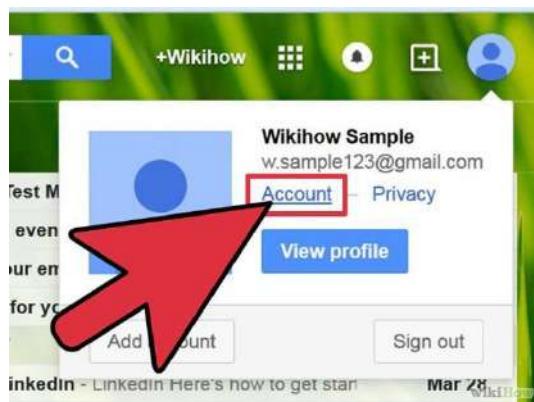
#### विशेषताएं

- प्रयोग करने में आसान : जीयूआई इतना आसान है कि कोई नौसिखिया (बिगिनर) भी इसका इस्तेमाल कर सकता है।
- मल्टीपल डाटाबेस: यह मल्टीपल डाटाबेस को भी सपोर्ट करता है और हर एक कैटेगरी के लिए अलग—अलग डाटाबेस बना सकते हैं।
- सेफडिक्रिप्शन: पासवर्ड डाटाबेस का डिक्रिप्शन रैम में होता है, इसके चलते हार्ड ड्राइव में लॉग—इन डिटेल का लेशमात्र भी विवरण नहीं रहता।
- पासवर्ड जनरेटर: स्ट्रांग और लम्बे पासवर्ड जनरेशन की सुविधा है।
- एडवान्स सर्च: यजर को अलग—अलग फील्ड के अन्दर एडवान्सड सर्च फंक्शन के जरिए सर्च की सुविधा प्रदान करता है।
- सिक्यूरिटी: डाटाबेस के एन्क्रिप्शन के लिए टूफिश एल्गोरिथिम का इस्तेमाल करता है।

#### 6.3 टू—स्टेप वेरिफिकेशन अपनाना:-

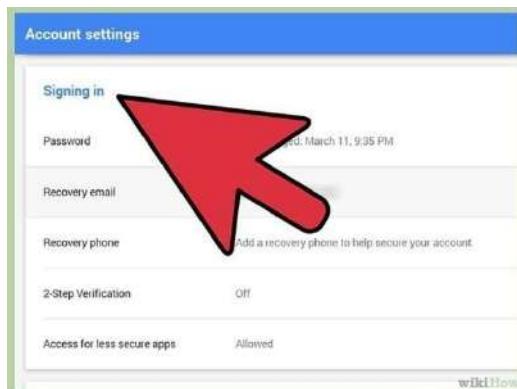
रोज दसियों हजार पर्सनल एकाउन्ट हैं। पर्सनल इन्फोर्मेशन चुरा ली जाती है, पासवर्ड क्रैक कर लिए जाते हैं और जिन्दगियां खतरे में पड़ जाती हैं। यदि आप अपने सभी एकाउन्ट्स के लिए एक ही पासवर्ड यूज करते हैं तो हैकिंग को आमंत्रण दे रहे हैं। शुक्र है कि गूगल ने 2-स्टेप वेरीफिकेशन प्रणाली शुरू की है। जब भी कोई अनजान डिवाइस गूगल एकाउन्ट में साइनआउट किया जाएगा, यूजर को पासवर्ड के अलावा वेरीफिकेशन कोड भी देना होगा। अब हैकर केवल आपका पासवर्ड हासिल करके आपके एकाउन्ट में लॉगइन नहीं कर सकता, उसे आपके फोन अथवा कम्प्यूटर पर भी प्रत्यक्ष तौर पर कब्जा करना होगा, तभी वह आपका एकाउन्ट एक्सेस कर पाएगा।

**स्टेप-1:**— अपने जी मेल एकाउन्ट में साइन इन करें। टॉप मैन्यू बार के राइट साइड पर अपने अवैटार के थम्बनेल पर विलक करें और उसके बाद अपनी सेटिंग्स को अपडेट करने के लिए “एकाउन्ट” पर विलक करें।



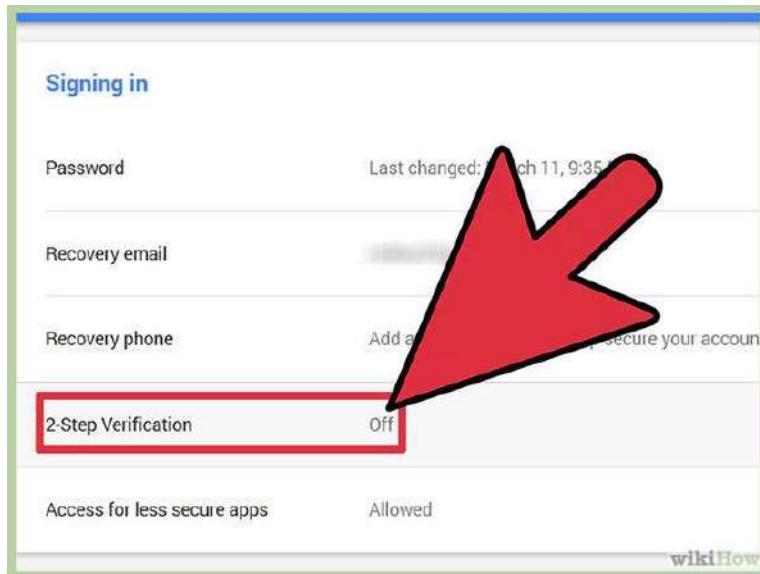
#### चित्र 14 : एकाउन्ट सेटिंग

**स्टेप-2 :** आप अपने एकाउन्ट पेज पर पहुंच जाएंगे। स्क्रोल-डाउन करें, आपको एक ब्ल्यूबार नजर आएगा, जिस पर अंकित होगा— “साइनिंग इन”



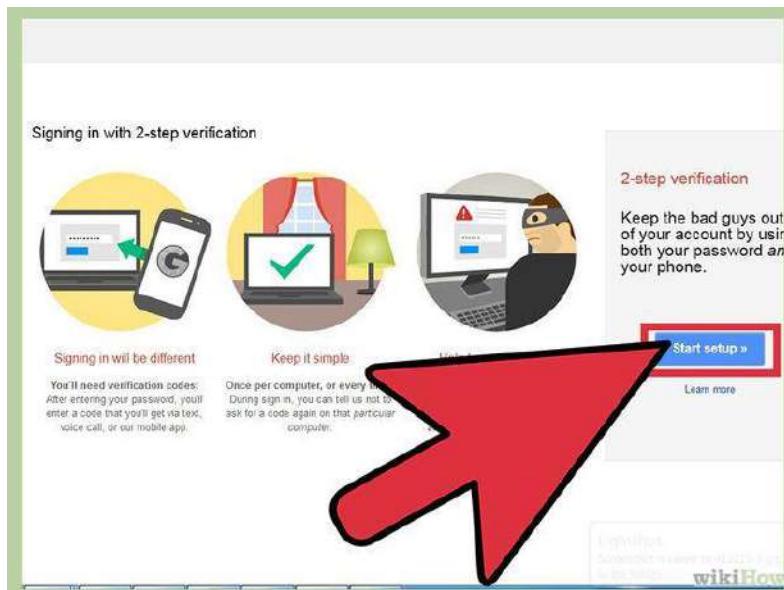
#### चित्र 15 : साइनिंग इन

**स्टेप-3 :** 2-स्टेप वेरीफिकेशन सैक्षण आप को बताएगा कि आपका 2-स्टेप वैरिफिकेशन “आन” है या “ऑफ”। यदि यह “ऑफ” बताता है, तो अगले फीचर पर जाने के लिए “एडिट” को बिलक करें।



**चित्र 16 : टर्निंग “ऑन” दू स्टेप वेरीफिकेशन**

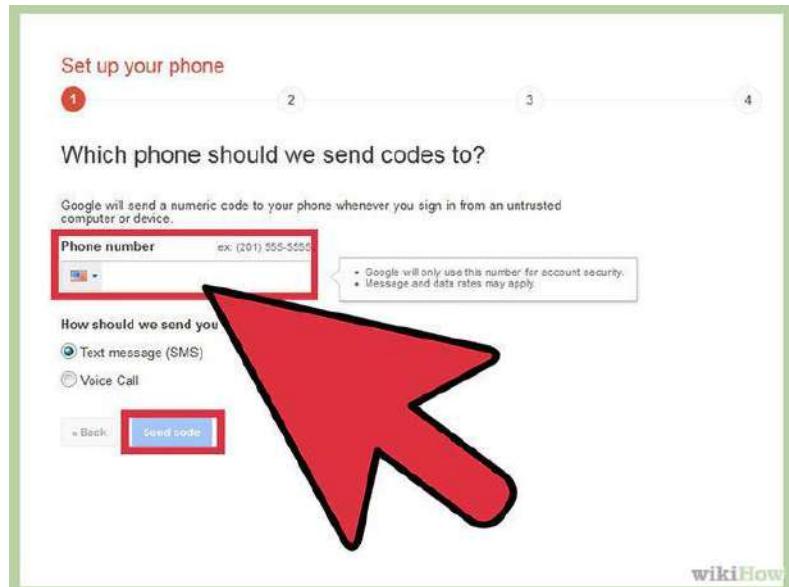
**स्टेप-4 :** आपको एक पेज नजर आएगा जो कुछ समय के लिए सेडिंग अप 2 स्टेप वेरीफिकेशन के अलग-अलग स्टेप्स पर रुकते हुए गुजरेगा। और ज्यादा विवरण के लिए इन स्टेप्स पर नजर रखें। जब आप तैयार हो जाएं, “स्टार्ट सेटअप” पर बिलक करें।



**चित्र 17 : स्टार्ट सेटअप**

**स्टेप-5 :** अपना मोबाइल नम्बर टाइप करें, यह नम्बर आपके गूगल एकाउन्ट से जुड़ जाएगा। जब भी आप किसी अनजान डिवाइस (यानि सार्वजनिक कम्प्यूटर) से अपने गूगल एकाउन्ट में साइन इन करेंगे,

गूगल आपके इस फोन पर एक वेरीफिकेशन कोड भेजेगा। आपको तभी साइन इन किया जाएगा जब आप ये कोड प्रविष्ट करेंगे।



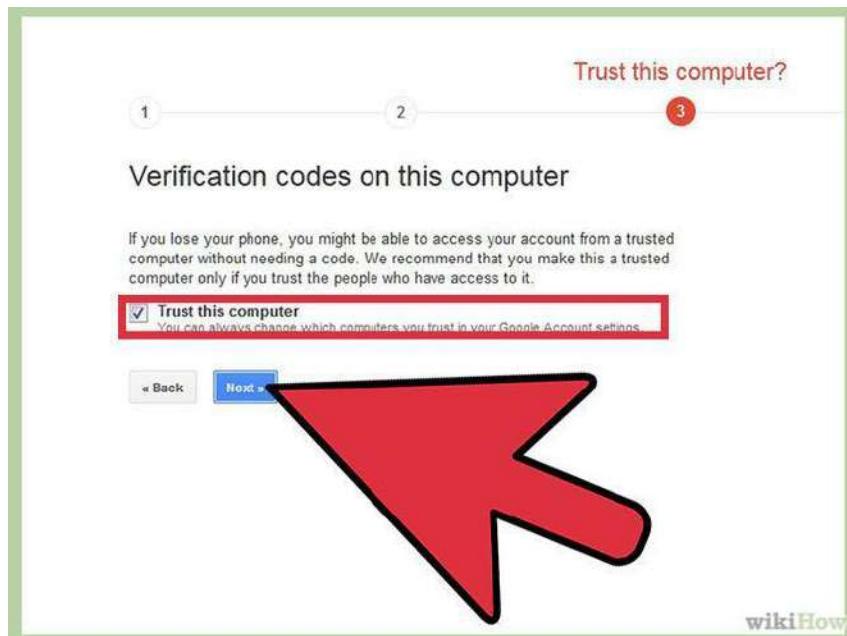
चित्र 18 : वेरीफिकेशन के लिए मोबाइल नम्बर एन्टर करना

**स्टेप-6 :** सलेक्ट करें कि आप अपने वेरीफिकेशन कोड के साथ क्या रिसीव करना चाहेंगे, टैक्स्ट मैसेज या गूगल वॉइस कॉल। अब आप अपने फोन पर कोड आने का इंतजार करें। कोड मिलने पर इसे एन्टर करें।



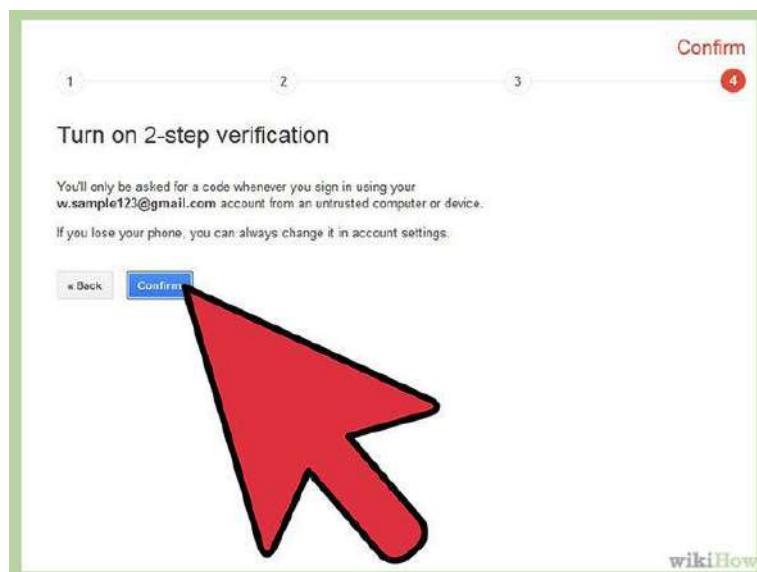
चित्र 19 : वेरीफिकेशन कोड एन्टर करना

**स्टेप-7 :** इस डिवाइस पर विश्वास करें या नहीं— यदि आप 2-स्टेप वेरीफिकेशन अपने पर्सनल कम्प्यूटर अथवा भरोसेमंद डिवाइस से “आन” कर रहे हैं तो “ट्रस्ट दिस डिवाइस” बॉक्स को टिक करें। अब आपको इस डिवाइस पर अपने एकाउन्ट में साइनइन करने के लिए हर 30 दिन में केवल एक बार वेरीफिकेशन कोड एन्टर करना होगा।



### चित्र 20 : कम्प्यूटर ट्रस्ट सैट अप करना

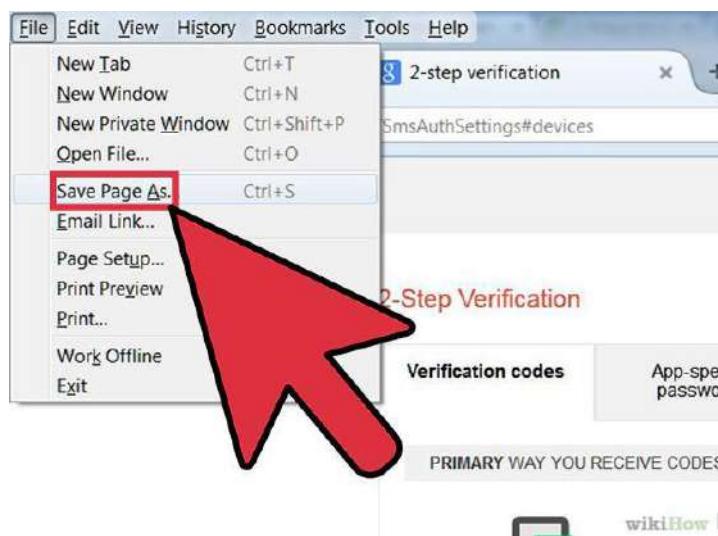
**स्टेप-8 :** अब ओके दबाएं। आपने अपने गूगल एकाउन्ट के लिए 2-स्टेप वेरीफिकेशन “ऑन” कर लिया है। उन स्टेप्स को स्किप कर दें जो आपके लिए अपरिचित या भ्रम पैदा करने वाले हों। हम इन सभी स्टेप्स पर इस आर्टिकल के अगले खण्डों में चर्चा करेंगे।



## चित्र 21 : कन्फर्मेशन

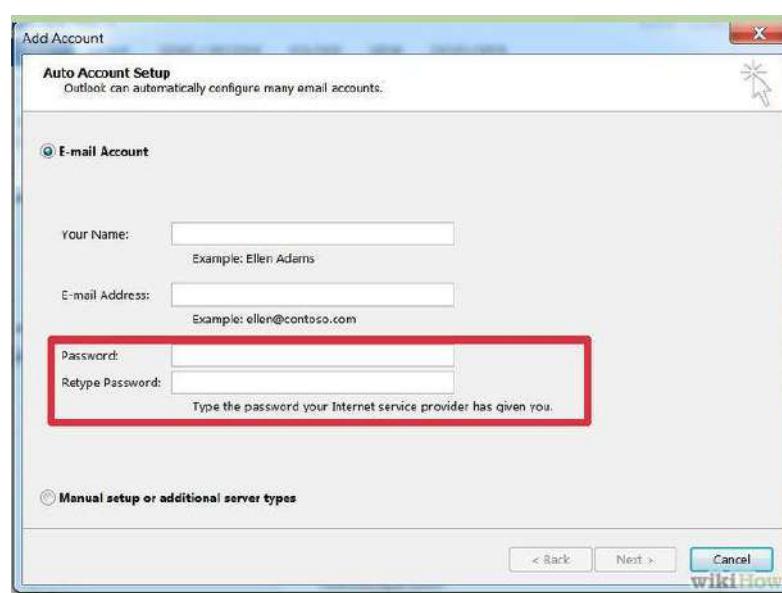
स्टेप-9 : वेरिफिकेशन कोड का एक प्रिन्ट ले लें और इसे किसी सुरक्षित स्थान जैसे कि अपने पर्स में सुरक्षित रख लें। अब यदि आपको अपने गूगल-एकाउन्ट पर साइन इन करना है और आपका फोन इस वक्त आपके पास नहीं है, आप इनमें से कोई कोड एन्टर करके साइन इन कर सकते हैं।

- अपने 2-स्टेप वेरिफिकेशन पेज पर जाएं।
- “हाऊ टू रिसीव कोड्स” के तहत “शो बैकअप कोड्स” लिंक पर क्लिक करें। इस पेज को प्रिंट कर लें।



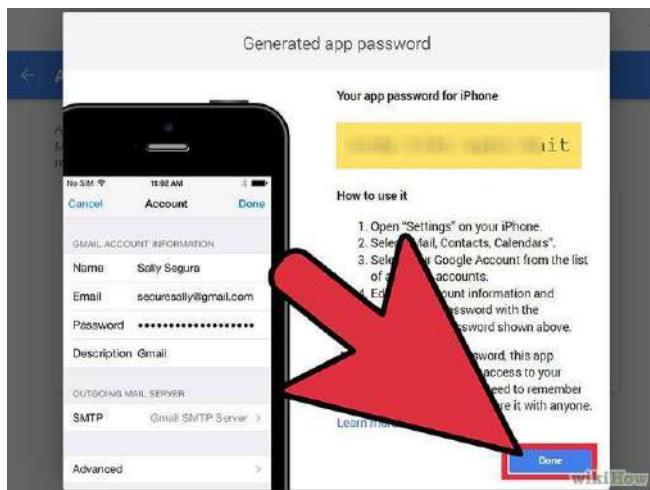
## चित्र 22 : पेज सेव करना

### 2 का मैथड 1 : एप्लिकेशन— स्पेसिफिक पासवर्ड



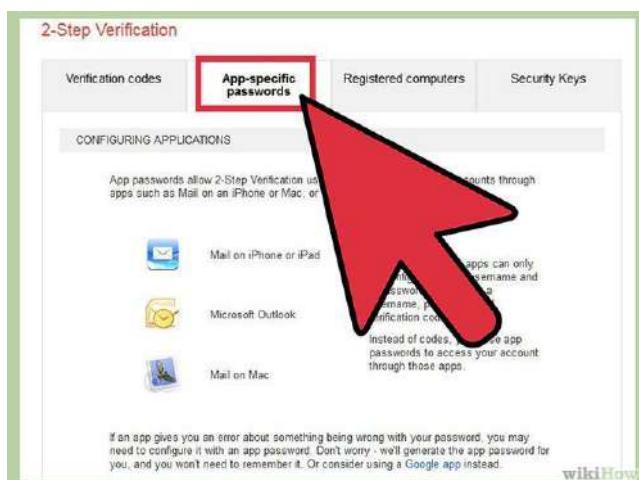
### चित्र 23 : एप्लिकेशन स्पेसिफिक पासवर्ड सेट करना

**स्टेप-1 :** एप्लिकेशन स्पेसिफिक पासवर्ड क्यों? यह समझना जरूरी है। गूगल जब भी आप किसी ब्राउजर से साइन इन करते हैं, आपको कवर कर लेता है। लेकिन, यदि आप किसी अन्य एप्लिकेशन जैसे कि माइक्रोसॉफ्ट आउट लुक या किसी मोबाइल डिवाइस की एप्लीकेशन से साइनइन करते हैं, ये सिस्टम आपसे वेरिफिकेशन कोड नहीं मांग पाते हैं। इसलिए, आपको एक बार एप्लीकेशन—स्पेसिफिक पासवर्ड से इन सिस्टम पर साइन इन करना होगा। आपको केवल एक एप्लिकेशन—स्पेसिफिक पासवर्ड री—एन्टर करना होगा और उस खास डिवाइस के लिए आप एक नया पासवर्ड बना लेंगे। इसके लिए “री—सेट इट” पर जाए और एक नया पासवर्ड बना लें।



### चित्र 24 : एप पासवर्ड जनरेटर करना

**स्टेप-2 :** एप्लीकेशन—स्पेसिफिक पासवर्ड जनरेट करना। 2—स्टेप वेरिफिकेशन पेज पर जाएं अथवा सिक्योरिटी सेटिंग्स पेज पर 2—स्टेप वेरिफिकेशन के बगल में नजर आ रहे ‘एडिट’ को क्लिक करें (उपरोक्त स्टेप्स 1—3)। स्क्रोल—डाउन करें और ‘मैनेज एप्लीकेशन—स्पेसिफिक पासवर्ड’ पर क्लिक करें।



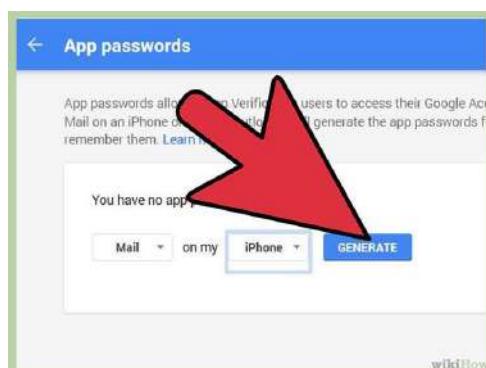
### चित्र 25 : एप्लिकेशन स्पेसिफिक पासवर्ड जनरेट करना

**स्टेप-3 :** पेज के टॉप पर आपको साइट्स की एक सूची नजर आएगी, इसमें एप्लीकेशन्स और डिवाइसेज भी दिए गए होंगे ये वो सूची है जिन्हें आपने अपने एकाउन्ट को कुछ हद तक एक्सेस की अनुमति दी है। उदाहरण के लिए, यदि आपने किसी अन्य वेबसाइट (जैसे कि लिंकेडिन, ट्रिवटर, फोरस्क्वायर) को अपने जीमेल कान्टेक्ट्स को तलाशने की अनुमति दी है, तो वह इस सूची में नजर आएगी। यदि आप गूगल की कोई और एप्लीकेशन यूज करते हैं तो वह भी नजर आएंगी। अब यदि आप किसी साइट या प्रोग्राम जो लिस्ट में शामिल है को और आगे यूज नहीं करना चाहते हैं तो आप उन्हें एक्सेस करने से रोक सकते हैं।



### चित्र 26 : एप्लीकेशन कन्फिगर करना

**स्टेप-4 :** डिवाइस का नाम एन्टर करने के लिए इस फ़ील्ड पर स्क्रोल-डाउन करके बॉटम पर पहुँचें। अब इस जगह वह नाम एन्टर करें, जिससे आप यह याद रख सकें कि किस डिवाइस के लिए आपने एप्लीकेशन-स्पेसिफिक पासवर्ड जनरेट किया है। जैसे कि मेल एप ऑन आइफोन, गुगल एप ऑन आईफोन, क्रोम सिंक, आउटलुक, थन्डरबर्ड अथवा कोई भी ऐसा नाम जो आपके एप्लीकेशन को इंगित कर सके। “जनरेट पासवर्ड” बिल्कुल करें। इस प्रकार आप प्रत्येक एप्लीकेशन के लिए एक नया एप्लीकेशन स्पेसिफिक पासवर्ड जनरेट कर पाएंगे।



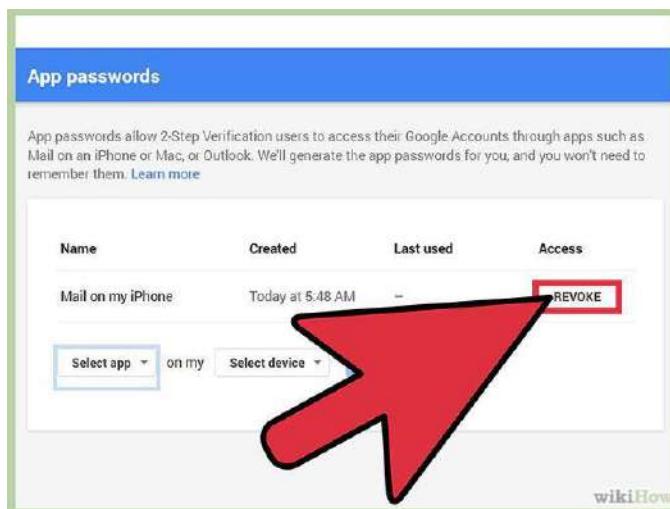
### चित्र 27 : जनरेटिंग एप पासवर्ड

स्टेप-5 : एप्लीकेशन खोलें। सेटिंग पेज पर जाएं, जहां आप अपना गूगल एकाउन्ट एन्टर करते हैं। गूगल एकाउन्ट का नाम टाइप करें। अब अपने एकाउन्ट पासवर्ड की बजाय एप्लीकेशन-स्पेसिफिक पासवर्ड को पासवर्ड फ़ील्ड में टाइप करें। अब आपने इस एप्लीकेशन को अपना गूगल एकाउन्ट एक्सेस करने की अनुमति दे दी है। आपको यह पासवर्ड केवल एक ही बार एन्टर करना होगा। अब इसे नोट डाउन करने या याद रखने की जरूरत नहीं होगी और गूगल दुबारा इसे डिस्प्ले नहीं करेगा।



### चित्र 28 : पासवर्ड टेस्ट करना

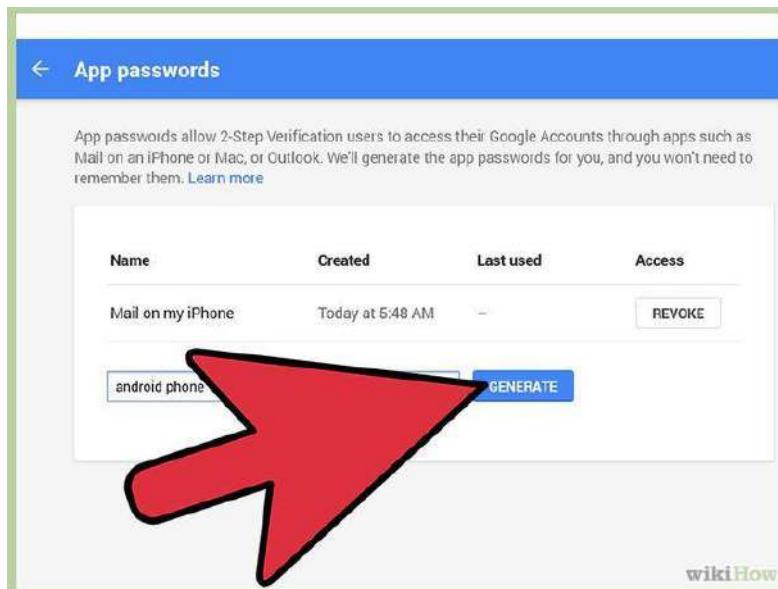
स्टेप-6 : एप्लीकेशन स्पेसिफिक पासवर्ड एन्टर करने के बाद अपने ब्राउजर पर “डन” को विलक करें।



### चित्र 29 : पासवर्ड रिवोक करना

स्टेप-7 : किसी एप्प को अपने जीमेल एकाउन्ट को एक्सेस करने से मना कैसे करें? यदि किसी एप को अब यूज नहीं करना चाहते हैं या आपका फोन खो गया है और चाहते हैं कि जिसके पास भी आपका फोन

है वह आपके जी मेल एकाउन्ट को एक्सेस न कर पाए तो आपको बस इतना करना है कि आप एप्लीकेशन—स्पेसिफिक पासवर्ड सैटिंग पेज पर जाकर “रीवोक” बटन को विलक कर दें।



### चित्र 30 : एन्ड्रॉइड फोन के लिए पासवर्ड जनरेट करना

**स्टेप-8 :** अपने गूगल एकाउन्ट से कनेक्ट करने वाले प्रत्येक एप्लीकेशन के लिए नया एप्लीकेशन—स्पेसिफिक पासवर्ड जनरेट करें। इसका मतलब है, यदि आप अपने गूगल एकाउन्ट को दो मेल एप्स और एक चैट एकाउन्ट से सिन्क कर रहे हैं तो आपको तीन एप्लीकेशन—स्पेसिफिक पासवर्ड जनरेट करने चाहिए।

### मैथड 2 का 2 : यदि आपका फोन खो जाएः—

यदि आपका फोन खो गया है और 2-स्टेप वेरीफिकेशन “ऑन” है आप तब भी अपना जी मेल एकाउन्ट एक्सेस कर सकते हैं। कोई अन्जान व्यक्ति इस फोन पर आपके एकाउन्ट एक्सेस न कर सके इसके लिए आप नीचे दिए गए तीन कदम उठाएः—

**स्टेप-1 :** अपने मौजूदा एप्लीकेशन—स्पेसिफिक पासवर्ड रिवोक कर दें। यदि आपका स्मार्ट फोन आपके जी मेल एकाउन्ट से सिंक है, तो वह स्वतः साइन आउट हो जाएगा। जब आप नया फोन ले आएं, तो आप नया एप्लीकेशन स्पेसिफिक पासवर्ड जनरेट कर लें (पिछला सैक्षण देखें) और उसे अपने नए डिवाइस में एन्टर कर लें।

**स्टेप-2 :** अपना जी मेल पासवर्ड बदल दें। यदि किसी के पास आपका वेरीफिकेशन पासवर्ड है भी, तो भी वह आपके नए पासवर्ड के बिना आपका जी मेल एकाउन्ट नहीं खोल पाएगा। हालांकि ऐसी सम्भावना नहीं है कि जिसके पास आपका फोन है वह आपका जी मेल पासवर्ड क्रेक कर लेगा, फिर भी गफलत में नहीं

रहना चाहिए। यदि आप किसी वेब ब्राउजर से अपने मोबाइल डिवाइस पर गूगल में लॉग इन है, आपको भी स्वतः साइन आउट कर दिया जाएगा।

**स्टेप-3 :** यदि आपके पास एक और मोबाइल डिवाइस है तो एक बैकअप फोन नं. ऐड कर दें। अपने 2-स्टेप वेरीफिकेशन सैटिंग पेज पर जाएं और “बैक अप फोन” में “ऐड ए फोन नम्बर” पर क्लिक करें।

**स्टेप- 4 :** यदि आपके पास बैकअप फोन नहीं है, तो अपने एकाउन्ट को एक्सेस करने के लिए अपने प्रिन्टेबल बैकअप लिस्ट का प्रयोग करें। आपके 2-स्टेप वेरीफिकेशन पेज पर, “शो बैकअप कोड्स” पर क्लिक करें। यदि आप पहले ऐसा नहीं कर पाये हैं, तो इस पेज का प्रिन्ट आउट ले लें और अपनी पहुंच के अन्दर किसी सुरक्षित जगह जैसे कि आप का पर्स में रख लें।

**स्टेप-5 :** यदि आपने अपना फोन नं. बदल लिया है, तो ध्यान रखें कि 2-स्टेप वेरीफिकेशन पेज पर अपने पिछले फोन नम्बर की एक्सेस रिवोक करना न भूलें।

## 6.4 फ्री एन्टीवायरस द्वारा अपने कम्प्यूटर को सुरक्षित बनाना

हमारे रोजमर्रा के कामों में कम्प्यूटर का उपयोग दिन-प्रतिदिन बढ़ता जा रहा है। हम पासवर्ड, ऑफिसियल ई मेल आईडी, बैक एकाउन्ट, पर्सनल नोट्स, बिजनेस प्लान तथा अन्य गोपनीय जानकारी जैसे संवेदी डाटा अपने कम्प्यूटर में रखने लगे हैं। इसलिए सुरक्षा हेतु एक अच्छा सैक्यूरिटी सॉफ्टवेयर नितान्त आवश्यक हो गया है। यहां 11 फ्री एन्टीवायरस की सूची और इनकी सामान्य विशेषताएं दी गई हैं। इनम से कोई एक आप अपनी ऑनलाइन सिक्यूरिटी के लिए चुन सकते हैं। यह सूची वर्णक्रम में है:-

### 1. अवास्ट एन्टीवायरस:

यह एक बेहतरीन फ्री एन्टीवायरस है जो ऑनलाइन खतरों से पूरी सुरक्षा प्रदान करता है। इस एन्टीवायरस के फुल-फीचर पैकेज की ये विशेषताएं हैं:- बिल्ट-इन एन्टो स्पायवेयर, एन्टी रुटकिट वेब शील्ड, स्ट्रांग सेल्फ प्रोटेक्शन, पी2पी और आईएम शील्ड, एन्टी-वायरस कार्नेल, रेजीडेन्ट प्रोटेक्शन, नेटवर्क शील्ड, आटेमिटिक अपडेट, सिस्टम इन्टीग्रेशन विन्डोज 64 बिट सपोर्ट, इन्टीग्रेटेड वायरस क्लीनर। इसे <https://www.avast.com/index> से डाउनलोड किया जा सकता है।

### 2. एवीजी एन्टीवायरस :

एवीजी एन्टीवायरस के फ्री एडीशन में बेसिक एन्टीवायरस और एन्टी-स्पायवेयर प्रोटेक्शन सुविधा दी गई है। इसके अलावा सेफ सर्फ फीचर भी इसकी एक खूबी है। इसे <http://free.avg.com/> से डाउनलोड कर सकते हैं।

### 3. एवीरा एन्टीवायरस पर्सनल :

यह होम यूजर्स के लिए एक अच्छा एन्टीवायरस है। इसे इस्तेमाल करना आसान है, भरोसेमंद है और कोई पैसा भी नहीं देना पड़ता। इसके द्वारा वायरस, वॉर्म्स और ट्राजन के हमले से आप बच सकते हैं। एन्टी-रुटकिट, एन्टी फिशिंग, एन्टीडायलर जैसी सुविधाएं भी इसमें ह इसे <http://www.av.com/> से डाउनलोड कर सकते हैं।

#### **4. बिटडिफेन्डर :**

इसका फ्री एडीशन उसी आईसीएस लैब द्वारा प्रमाणित स्कैनिंग इन्जन का प्रयोग करता है जो बिटडिफेन्डर के प्रो वर्जन में है। इसमें बिना कोई कीमत चुकाए आप बेसिक वायरस प्रोटेक्शन की सुविधा ले सकते हैं। ऑन डिमांड वायरस स्कैनर तथा रिमूव और शेड्यूल स्कैनिंग जैसे प्रोग्राम भी इसमें हैं इसे <http://www.bitdefender.com/> PRO/PRODUCT-14-en-oit bitdefender-free-edition.html से डाउनलोड किया जा सकता है।

#### **5. ब्लिंक पर्सनल :**

यह एन्टीवायरस के साथ-साथ एक ऑल-इन-वन सिक्यूरिटी पैकेज है, जिसे आप एक वर्ष तक यूज कर सकते हैं। ब्लिंक सिक्यूरिटी पैकेज में एन्टीवायरस और एन्टी स्पाइवेयर एन्टी रुटकिट, बिल्ट इन फायरवाल प्रोटेक्शन और आइडेन्टी प्रोटेक्शन जैसे फीचर भी शामिल हैं। इसे <http://free-antivrvs.eeye.com/> से डाउनलोड कर सकते हैं।

#### **6. कामविन एन्टीवायरस :**

यह विन्डोज 98/एमई/2000/एक्सपी/2003 और विस्टा के लिए एक ओपन सोर्स फ्री एन्टीवायरस प्रोग्राम है। इसमें वायरस और स्पाइवेयर को तलाशने की क्षमता, नियमित रूप से अपडेटेड वायरस के डाटाबेस को डाउनलोड करने, पूर्ण रूप से वायरस स्कैन जैसी खूबियां इसमें शामिल हैं। इसमें ऑन-एक्सेस रीयल-टाइम स्कैनर की सुविधा नहीं है। इसे <https://www.clamwin.com/> से डाउनलोड कर सकते हैं।

#### **7. कोमोडो एन्टीवायरस :**

इसमें वो सभी फंक्शन मौजूद हैं, जो एक खरीदे गए एन्टीवायरस में मिलते हैं। इसकी विशेषताओं में—कम्प्यूटर और नेटवर्क में वायरस खोजने और हटाने, एक्सेस करन पर आपके कम्प्यूटर को संक्रमित करने से पहले ही तत्काल वायरस स्कैन केज, वायरस, स्पाइवेयर और अन्य मैलवेयर को इन्टरसैट करने के लिए होस्ट इन्ट्रयूजन डिटेक्शन करने के प्रोग्राम भी शामिल हैं। आपको नवीन वायरस की डेफिनेशन भी रोज प्रदान करता है, ताकि आप ताजा खतरों से सुरक्षित रहें। इसे <https://antivirus.comodo.com/> से डाउनलोड कर सकते हैं।

#### **8. मून सिक्योर एन्टीवायरस :**

जीपीएल लाइसेंस के तहत विन्डोज के लिए सर्वश्रेष्ठ फ्री—एन्टीवायरस बनने की ओर अग्रसर है। इसमें मल्टीपल स्कैन इंजिन, नेटशील्ड, फायरवॉल, ऑन एक्सेस स्कैन रुटकिट्स प्रिवेन्शन की सुविधा के अलावा बाजार में उपलब्ध एन्टीवायर एप्लीकेशनों की अनेक खूबियां भी इसमें उपलब्ध हैं। [bls](http://sourceforge.net/projets/moonav/) <http://sourceforge.net/projets/moonav/> से डाउनलोड कर सकते हैं।

## 9. पीसी टूल्स एन्टीवायरस :

पीसी टूल्स एन्टीवायरस के इस फ्री संस्करण से आप अपने कम्प्यूटर और पर्सनल इन्फोर्मेशन को साइबर-खतरों के जघन्य हमलों से बचा सकते हैं। ये आपको वायरस, वॉर्म्स, ट्रोजन से सुरक्षा प्रदान करता है तथा स्मार्ट अपडेट, इन्टेलीगार्ड प्रोटेक्शन, फाइनल गार्ड और ईमेल गार्ड जैसी सेवाएं भी इसमें उपलब्ध हैं। इसे <http://www.pclools.com/free-antivirus> से डाउनलोड कर सकते हैं।

## 10. टाइजिंग एन्टीवायरस :

इस एन्टीवायरस का फ्री एडीशन सभी प्रकार वायरस, वॉर्म्स, ट्रोजन रुटकिट्स तथा अन्य प्रकार नुकसानदेह प्रोग्राम से तब तक संरक्षण प्रदान करता रहता है, जब तक यह आपके डिवाइस में है और इसकी कोई कीमत भी आपको नहीं चुकानी है। आसान प्रयोग और स्मार्ट अपडेट टैक्नॉलौजी इसकी एक ऐसी विशेषता है कि आप इसे इन्स्टॉल कीजिये और निश्चिन्त होकर अपने कम्प्यूटर पर काम में मशागूल हो जाइये। इसे <http://www.freeav.com/> से डाउनलोड कर सकते हैं।

## 11. थ्रेटफायर लाइट :

यह एन्टीवायरस वॉर्म्स, ट्रोजन, स्पायवेयर, रुटकिट्स, वायरस, की लॉगर्स एण्ड बफर ओवरफलो जैसे खतरों से व्यापक सुरक्षा प्रदान करता है। साथ ही मेलवेयर के बिहैवियर से उनका पता लगाने, मैलवेयर क्वारंटाइन और रिमूव करने आदि जैसे प्रोग्राम भी इसमें अन्तर्निहित हैं। इसे <http://www.threatscre.com/downlond/> से डाउनलोड कर सकते हैं।

## अभ्यास

1. कुछ प्रमुख एन्टीवायरस की विशेषताओं की तुलना करें।
2. फ्री एन्टीवायरस और पेड एन्टीवायरस में क्या अन्तर है? क्या अपने डिवाइस में फ्री एन्टीवायरस उपयोग करना सुरक्षित है?
3. सेक्योर पासवर्ड जनरेट करने के दिशा-निर्देशों का यूज करें और इस आधार पर आकलन कर बनाएं कि क्या आपका पासवर्ड सेक्योर माना जा सकता है।
4. उपरोक्त दिशा-निर्देशों का पालन करते हुए अपने अनसेफ पासवर्ड को सेफ पासवर्ड में बदलें।
5. कुछ लोकप्रिय पासवर्ड मैनेजर खोज लें और उनकी विशेषता के आधार पर तुलना करें।

6. उपरोक्त तुलना के आधार पर अपने लिए एक बेहतरीन पासवर्ड मैनेजर चुनें।
7. अपने जी मेल एकाउन्ट के लिए 2-स्टेप वेरीफिकेशन क्रिएट करें।
8. जी मेल के अलावा और कितनी साइटें 2-स्टेप वेरीफिकेशन अपनानी हैं?

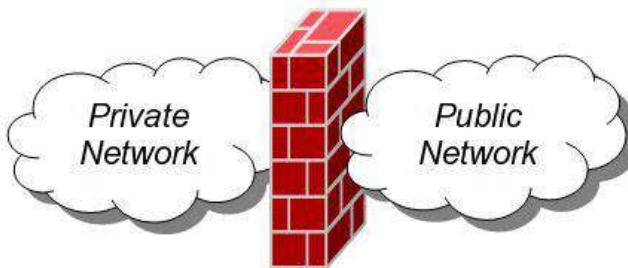
अनुशंसित वीडियो

—□—

## मैक कम्प्यूटर पर फायरवॉल कन्फिगर करना

मैक कम्प्यूटर बिल्ट-इन फायरवाल के साथ मिलते हैं<sup>6</sup>। यह सुविधा कन्फिगर करनी पड़ती है ताकि अवांछित सूचना आपके कम्प्यूटर में न आए। लेकिन फायरवाल है क्या, और आपको अपने मैक में इसे इस्तेमाल क्यों करना है?

जब भी आप इंटरनेट से कोई सूचना तलाशते हैं, आपका मैक उस सूचना को तलाशने के लिए डाटा पैकेट प्रेषित करता है। सर्वर में डाटा पैकेट रिसीव होता है और सर्वर से आपके मैक को एक अन्य डाटा पैकेट प्रेषित किया जाता है। यह सब कुछ सेकेन्ड्स में हो जाता है। जैसे ही आपका मैक इस पैकेट को रीअसेम्बल करता है, आपको अपेक्षित सूचना ईमेल अथवा वेबपेज के रूप में दिखाई दे जाती है।



चित्र 31 : फायरवॉल

फायरवॉल बैड पैकेट्स (हानिकारक डाटा) को आपके कम्प्यूटर में एंटर करने से रोकती है। हैकर्स ऑटोमेटेड एप्लीकेशन्स का प्रयोग करते हैं, जो हजारों कम्प्यूटर (आपके कम्प्यूटर सहित) स्कैन कर सकते हैं और ओपन पोर्ट तलाश कर उनका दुरुपयोग कर सकते हैं। यह सुनिश्चित करने के लिए कि कोई अनजान व्यक्ति आपके मैक को एक्सेस न कर सके, आपको मैक ओएस एक्स की फायरवॉल इनेबल करनी होगी ये आपके मैक के ओपन पार्ट्स को क्लोज करके रैण्डम नेटवर्क स्कैन को रोक देगी।

### 7.1.1 मैक ओएसएक्स फायरवॉल कन्फिगर करना और ऑन करना :

मैक फायरवॉल किस प्रकार कन्फिगर और ऑन करें:

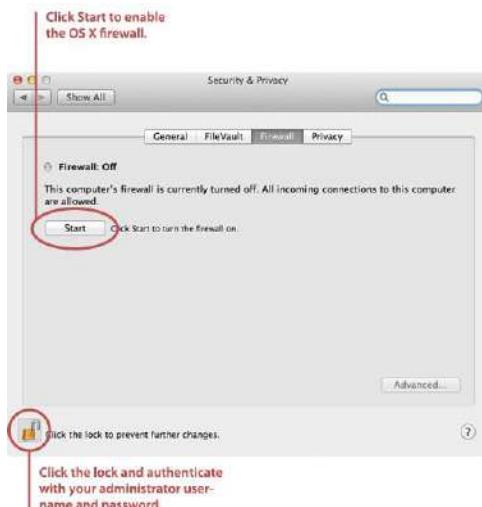
1. एप्पल मेनू से सिस्टम प्रीफेरेंस सलेक्ट करें। नीचे दी गई विन्डो नजर आएगी।

<sup>6</sup> Content and image courtesy(figure 31 to 35): <http://www.macinstruct.com/node/165> available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License



**चित्र 32 : सिस्टम प्रीफरेंस डैशबोर्ड**

2. सिक्यूरिटी एण्ड प्राइवेसी सलेक्ट करें।
3. फायरवॉल टैब विलक करें।
4. लॉक आइकॉन को विलक करें और अपने एडमिनिस्ट्रेटर के यूजर नेम और पासवर्ड से अथॉन्टिकेट करें।  
नीचे दी गई विन्डो नजर आएगी।



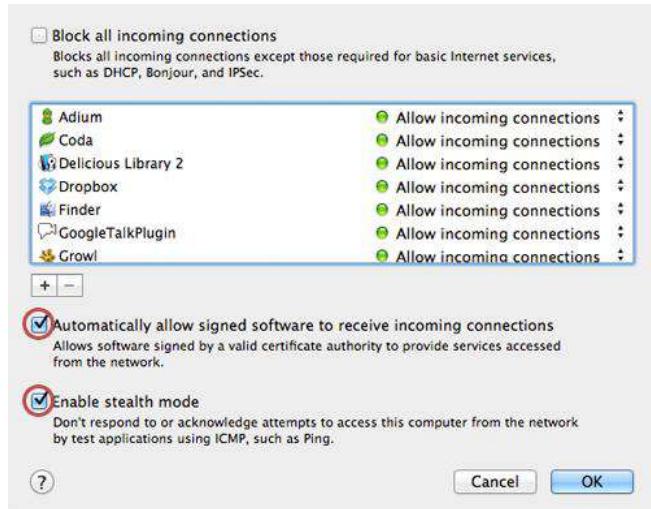
**चित्र 33 : सिक्यूरिटी और प्राइवेसी डैश बोर्ड**

5. स्टार्ट किलक करें। फायरवॉल ऑन हो जाएगी आपको ग्रीन लाइट ऑन नजर आएगी और जैसा कि नीचे दिखाया गया है फायरवॉल ऑन मैसेज भी आएगा।



**चित्र 34 : फायरवॉल ऑन करना**

6. एडवान्स्ड को विलक करें। नीचे दिखाई गई विन्डो नजर आएगी।



### चित्र 35 : फायरवॉल कन्फिगर करना

7. ऑटोमेटिकली एलाइ साइन्ड सॉफ्टवेयर टू रिसीव इनकमिना कनेक्शन चैक बॉक्स को सलेक्ट करें। इससे आपके मैक की एप्लीकेशन बाहरी नेटवर्क के साथ सम्पर्क को नहीं रोकेगी।
8. इनेबल्ड स्टील्थ मोड चैक बॉक्स को सलेक्ट करें। इससे आपका मैक पोर्ट स्कैन और पिंग रिक्वेस्ट्स को इजाजत नहीं देगा।
9. एडवान्स सैटिंग्स को बन्द करने के लिए ओके क्लिक करें।
10. सिस्टम प्रीफरेन्सेज को क्लोज करें। आपका मैक बिल्ट-इन फायरवॉल के द्वारा संरक्षित हो चुका है।

## 7.2 विन्डोज 7 में विन्डोज फायरवॉल को समझाना:—

### 7.2.1 विन्डोज 7 में फायरवॉल:—

विन्डोज 7 में दो फायरवॉल एक साथ मिलती हैं। इनमें से एक विन्डोज फायरवॉल और दूसरी विन्डोज फायरवॉल विथ एडवान्स सिक्यूरिटीज (डब्ल्यूएफएएस) है। इन दोनों में अन्तर, कन्फ्यूगिरेशन के नियमों की जटिलता का है। विन्डोज फायरवॉल प्रोग्राम अथवा किसी सर्विस से सीधे जुड़े आसान नियमों को यूज करती है। जबकि डब्ल्यूएफएएस के नियमों को प्रोटोकोल, पोर्ट्स, एड्रेस और अर्थान्तिकेशन के अनुसार कन्फिगर किया जा सकता है। बाईडिफॉल्ट, दोनों फायरवॉल पहले से निर्धारित नियमों के अनुसार कार्य करती हैं, जो हमें नेटवर्क रिसोर्सेज को इस्तेमाल करने से नहीं रोकती। इसमें वेब ब्राउज करना, ई मेल रिसीव करना आदि शामिल हैं। इसके अलावा, फाइल एण्ड प्रिन्टर शेयरिंग, नेटवर्क डिस्कवरी, परफॉर्मेन्स लॉग्स और अलर्ट, रिमोट एडमिनिस्ट्रेशन, विन्डोज रिमोट मैनेजमेंट, रिमोट असिस्टेंस, रिमोट डैस्क टॉप, विन्डोज मीडिया प्लेयर, विन्डोज मीडिया प्लेयर शेयरिंग सर्विस भी निर्बाध एकिटव रहती हैं।

विन्डोज 7 में निहित फायरवॉल से हम इनबाउंड और आउटबाउंड रूल्स को कन्फिगर कर सकते हैं। बाई डिफॉट, सभी आउट बाउंड ट्रैफिक के लिए कोई रोक नहीं है और उनके जवाब में इन बाउंड ट्रैफिक भी बिना रोकटोक प्रवेश करेगा। लेकिन, बाहरी सोर्स से स्वतः जनरेट होने वाला ट्रैफिक खुद-ब-खुद ब्लॉक हो जाएगा। कई बार हम ऐसा नोटिफिकेशन देखते हैं कि फलॉ-फलॉ ट्रैफिक जो नेटवर्क रिसोर्सेज को एक्सेस करना चाहता था, उसे ब्लॉक कर दिया गया है। ऐसे मामलों में, हम अपनी फायरवॉल में कुछ अपवाद जोड़ सकते हैं कि भविष्य में इन प्रोग्राम को ब्लॉक न किया जाए। जब हम फायरवॉल की बात करते हैं, तो विन्डोज 7 में कुछ नए फीचर दिए गए हैं। उदाहरण के लिए—“फुल स्टील्थ” अन्य कम्प्यूटरों के ऑपरेटिंग सिस्टम को फिंगर प्रिंटिंग (सटीक पहचान) की इजाजत नहीं देता। फिर प्रिंटिंग एक ऐसी मैलीसियस (गलत इरादे वाली) टैक्नीक है, जो होर्स्ट मशीन के ऑपरेटिंग सिस्टम को पकड़ने के लिए इस्तेमाल की जाती है। “बूट टाइम फिल्टरिंग” एक और टैक्नीक है, जो यह सुनिश्चित करती है कि फॉयरवॉल तभी काम करे जब नेटवर्क पर कनेक्ट होते हैं, हम नेटवर्क की लोकेशन की जानकारी पाते हैं। इसे नेटवर्क लोकेशन अवेयरनेश (एलएनए) कहा जाता है। इस फीचर से हम लोकेशन के आधार पर कनेक्शन से उस नेटवर्क के लिए एक नेटवर्क प्रोफाइल तय करते हैं। अलग-अलग नेटवर्क प्रोफाइल में अलग-अलग फायर-वॉल रूल्स होते हैं। विन्डोज 7 में, अलग-अलग प्रोफाइल्स को अलग-अलग इन्टरफेस पर कन्फिगर किया जा सकता है। उदाहरण के लिए हमारे वायरलेस इन्टरफेस कुछ और तथा वायर्ड इन्टरफेस कुछ और हो सकते हैं। आजकल तीन अलग-अलग नेटवर्क प्रोफाइल्स उपलब्ध हैं:—

#### □ पब्लिक

#### □ होमवर्क— प्राइवेट नेटवर्क

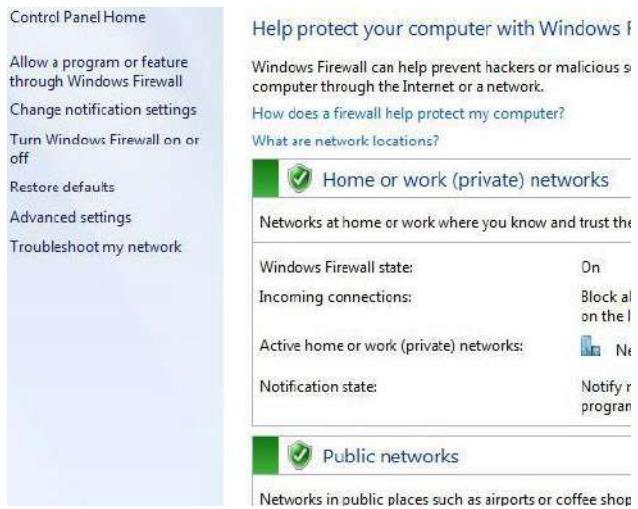
#### □ डोमेन— किसी खास डोमेन में यूज होने वाली

जब हम किसी नेटवर्क से कनेक्ट होते हैं, हम इन लोकेशन का चयन करते हैं। हम चाहें तो नेटवर्क में लोकेशन और शेयरिंग सेन्टर बदल सकते हैं। जब हम किसी एक्टिव डायरेक्ट्री डोमेन पर लॉगइन करते हैं तो एनएलए सर्विस डोमेन प्रोफाइल स्वतः तय कर देता है। ध्यान रखें, विन्डोज 7 में फायरवॉल कन्फिगर करने के लिए हमें एडमिनिस्ट्रेटिव राइट्स होने चाहिए।

### 7.2.2 विन्डोज फायरवॉल कन्फिगर करना<sup>7</sup>

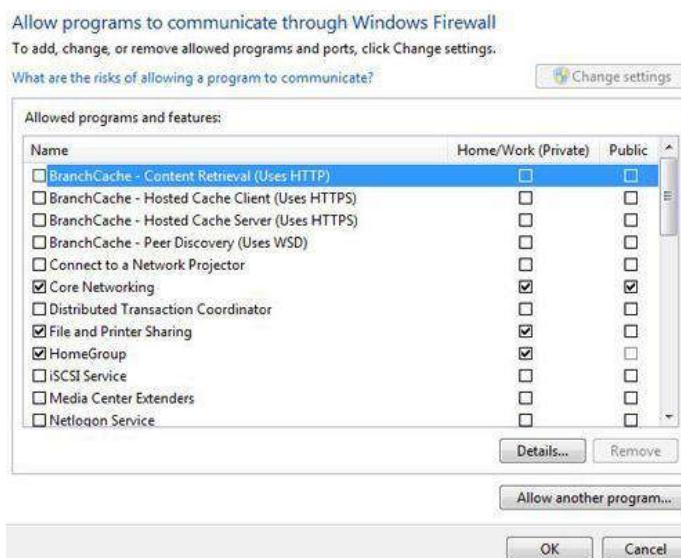
<sup>7</sup> Contents and image courtesy( Figure 31 o 43):<http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advanced-security> available under Creative Commons Attribution-Noncommercial-Share Alike 4.0 International.

विन्डोज की फायरवॉल को ओपन करने के लिए हमें स्टार्ट झ कन्ट्रोल पैनल झ विन्डोज फायरवॉल पर जाना होगा।



**चित्र 36 : विन्डोज मशीन पर कन्ट्रोल पैनल डैशबोर्ड**

प्राइवेट (होम अथवा वर्क) तथा पब्लिक नेटवर्क्स दोनों के लिए फायरवॉल बाई डिफाल्ट इनेबल्ड होती है। ये उन सभी प्रोग्राम को ब्लॉक करती है जो एलाउड प्रोग्राम की सूची में नहीं हैं। हम इनमें से जिन्हें शामिल करना चाहते हैं, उन्हें इनेबल करने के लिए “एलाउ ए प्रोग्राम और फीचर थू विन्डोज फायरवॉल” ऑप्शन पर जाना होगा।



**चित्र 37 : फायरवॉल सेटिंग कन्फिगर करना**

### एक्सप्लान्स (अपवाद)

इस विन्डो में सेटिंग्स बदलने के लिए हमें “चेन्ज सैटिंग्स” बटन को क्लिक करना होगा। जैसा कि तुम देख सकते हो, हमारे सामने पहले से तय प्रोग्राम्स और फीचर की एक लिस्ट है। ये वो प्रोग्राम और फीचर

है, जिन्हें, प्राइवेट या पब्लिक नेटवर्क्स पर कम्यूनिकेशन की अनुमति दी गई है। उदाहरण के लिए, कोर नेटवर्किंग फीचर को प्राइवेट और पब्लिक दोनों नेटवर्क पर कम्यूनिकेट करने की अनुमति दी गई है, जबकि फाइल एण्ड प्रिन्टर शेयरिंग केवल प्राइवेट नेटवर्क्स पर ही हो सकती है। यदि हम इन फीचर्स और प्रोग्राम्स की डिटेल्स देखना चाहते हैं तो हम लिस्ट में दिए आइटम को सलेक्ट करके ‘डिटेल्स’ बटन को क्लिक करेंगे।



### चित्र 38 : सेटिंग एक्सेप्शन्स

कोई ऐसा प्रोग्राम जो इस लिस्ट में नहीं है, उसे “एलाउ एनादर प्रोग्राम” बटन को क्लिक करके मैनुअली ऐड कर सकते हैं।



### चित्र 39 : लिस्ट में किसी नए प्रोग्राम को सलेक्ट करना

#### प्रोग्राम ऐड करना

इसके लिए हमें अपने प्रोग्राम के एक्जीक्यूटेबल को ब्राउज करने के बाद ऐड बटन को क्लिक करना होगा। हम उस लोकेशन टाइप्स को भी चून सकते हैं जिस पर यह प्रोग्राम चल सकेगा इसके लिए ‘नेटवर्क लोकेशन टाइप्स’ बटन को क्लिक कर।

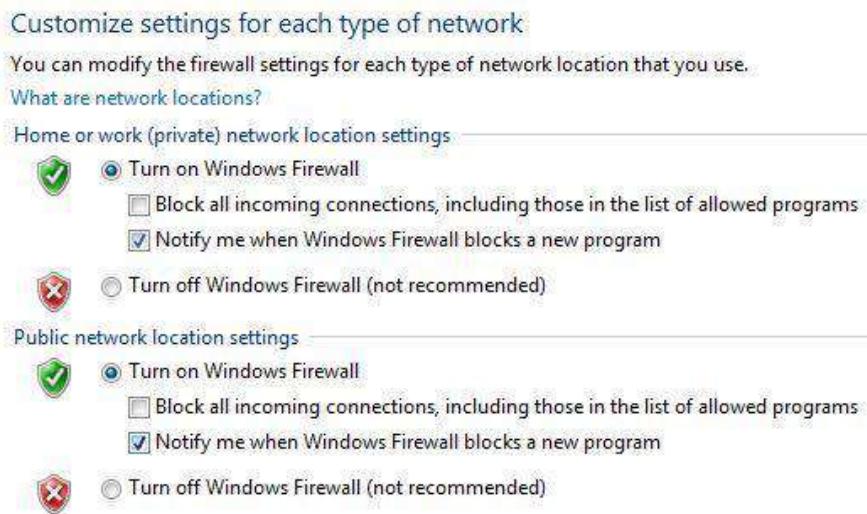


### चित्र 40 : प्रोग्राम ऐड करना

#### नेट वर्क लोकेशन्स

जब भी हम किसी प्रोग्राम को रन करेंगे, वह स्वतः ही विन्डोज फायरवॉल में प्रॉपर एक्सेप्शन्स कन्फिगर कर लेगा। उदाहरण के लिए, यदि हम मीडिया प्लेयर से स्ट्रीमिंग को इनेबल करें तो यह स्वतः ही फायरवॉल सेटिंग्स में “एलाउट स्ट्रीमिंग” से कन्फिगर कर लेगा। यदि हम सिस्टम प्रॉपरटीज विन्डो से रिमोट डेस्कटॉप फीचर को इनेबल करें तब भी ऐसा ही होगा। रिमोट डेस्कटॉप फीचर को इनेबल करके, दरअसल हम विन्डोज फायरवॉल में एक एक्सेप्शन क्रिएट करते हैं।

विन्डोज फायरवॉल को पूरी तरह “टर्न ऑफ” किया जा सकता है। ऐसा करने के लिए लेफ्ट साइड में मैन्यू से हम “टर्न विन्डो फायरवॉल ऑन और ऑफ” विकल्प का प्रयोग कर सकते हैं।



### चित्र 41 कस्टमाइज सेटिंग्स

#### फायरवॉल कस्टमाजेशन

ध्यान रखें कि हम प्रत्येक प्रकार के नेटवर्क लोकेशन (प्राइवेट अथवा पब्लिक) की सेटिंग्स बदल सकते हैं। यहाँ दिलचस्प बात यह है कि हम लिस्ट में एलाउड प्रोग्राम ही नहीं बल्कि सभी इनकमिंग कनेक्शन को

भी ब्लॉक कर सकते हैं। दरसअल विन्डोज फायरवाल विन्डोज द्वारा दी गई एक सुविधा है। जैसा कि आप जानते हैं, सुविधाओं को बन्द और चालू किया जा सकता है। यदि विन्डोज की फायरवॉल सर्विस को बन्द कर दें तो यह फायरवॉल काम नहीं करेगी।

Windows Event Log	This service ...	Started	Automatic
Windows Firewall	Windows Fi...	Started	Automatic
Windows Font Cache S...	Optimizes p...	Started	Automatic (D...
Windows Image Acquis...	Provides im...		Manual

चित्र 42 : विन्डोज सर्विसेज से फायरवॉल इनेबल करना

### फायरवाल सर्विस

अभी फायरवॉल सर्विस चल रही है। यदि हम इसे बन्द कर दें, तो हमें एक चेतावनी मिलेगी कि हम विन्डोज फायरवॉल ऑन करें।



चित्र 43 : फायरवॉल नोटिफिकेशन

### वार्णिंग:

याद रखें कि विन्डोज फायरवॉल से हम केवल फायरवॉल की बेसिक सैटिंग्स ही कन्फिगर कर सकते हैं और यह ज्यादातर सामान्य यूजर्स के लिए पर्याप्त ह। हम विन्डोज फायरवॉल में पोर्ट्स आधारित एक्सेसान्स को कन्फिगर नहीं कर सकते। इसके लिए, हमें विन्डोज फायरवॉल विथ एडवान्सड सिक्यूरिटी का यूज करना होगा।

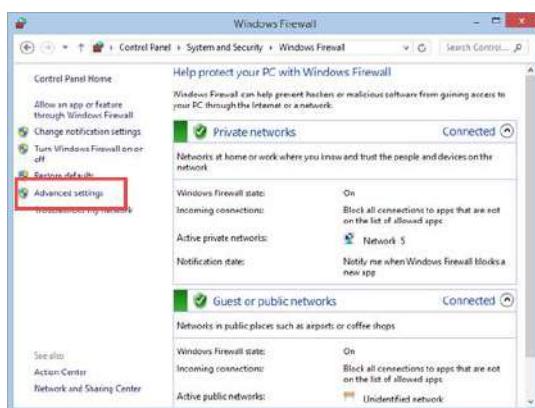
### 7.2.3 विन्डोज फायरवॉल विथ एडवान्सड सिक्यूरिटी को कैसे इनेबल और यूज करें?

विन्डोज फायरवॉल विथ एडवान्सड सिक्यूरिटी वह टूल है जो आपको विन्डोज फायरवॉल द्वारा प्रयुक्त रुल्स पर व्यापक कन्ट्रोल (कन्ट्रोल) की सुविधा देता है। विन्डोज फायरवॉल द्वारा प्रयुक्त रुल्स को व्यू कर सकते हैं, उनकी प्रॉपरटीज बदल सकते हैं, मौजूदा रुल्स को डिसेबल कर सकते हैं या नए रुल क्रिएट कर सकते ह। इस पाठ में हम, विन्डोज फायरवॉल विथ एडवान्सड सिक्यूरिटी कैसे खोले, इस पर चर्चा करेंगे।

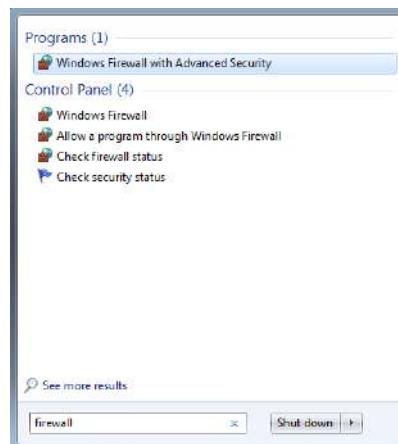
इसके अलावा, कैसे इसको समझें, इसके रूल्स क्या हैं और किस प्रकार के ट्रैफिक को यह फ़िल्टर करता है? इस पर भी बात करेंगे।

### 7.2.3.1 विन्डोज फायरवॉल विद एडवान्स्ड सिक्यूरिटी को कैसे एक्सेस करें?<sup>8</sup>

विन्डोज फायरवॉल विद एडवान्स्ड सिक्यूरिटी को एक्सेस करने के अनेक विकल्प हैं। इनमें से एक है आप “कन्ट्रोल पैनल ज्ञ सिस्टम एण्ड सिक्यूरिटी ज्ञ विन्डोज फायरवॉल” पर जाए और फिर “एडवान्स्ड सैटिंग्स” बटन पर क्लिक करें।



विन्डोज 7 में, फायरवॉल खोजन का एक और तरीका है। स्टार्ट मैन्यू के सर्चबॉक्स में फायरवॉल खोजें और ‘विन्डोज फायरवॉल विद एडवान्स सिक्यूरिटी’ रिजल्ट पर क्लिक करें।

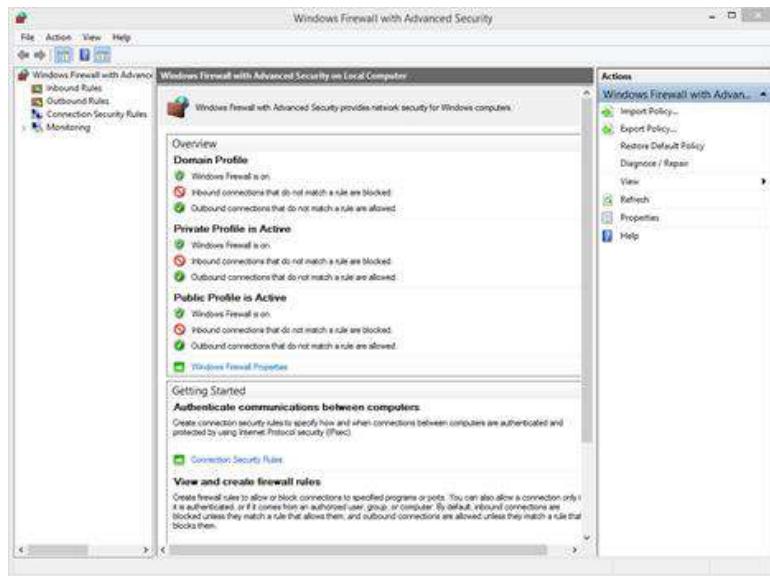


विन्डोज 8.1 में, सर्च रिजल्ट में विन्डोज फायरवॉल विद एंडवान्स सिक्यूरिटी नहीं मिलेगी। आपको इसे खोजने के लिए ऊपर बताए गए पहले मैथड को अपनाना होगा।

विन्डोज 7 और विन्डोज 8.1 में विन्डोज फायरवाल विद एडवांस सिक्यूरिटी एक जैसी नजर आती है और एक जैसे काम करती है।

<sup>8</sup> <http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advanced-security>

आगे पढ़ाई जारी रखने के लिए विन्डोज 8.1 में इस फायरवॉल के स्क्रीन शॉट्स का इस्तेमाल करेंगे।

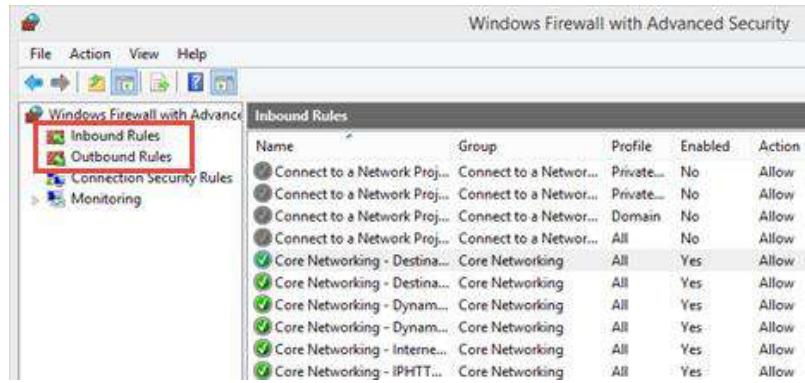


### 7.2.3.2. इनबाउन्ड और आउट बाउन्ड रुल क्या हैं?

सिक्युरिटी के लिए आप विन्डोज फायरवॉल का उपयोग करते हैं। फायरवॉल में इनबाउन्ड और आउटबाउन्ड रुल्स का एक स्टैन्डर्ड सैट है जिन्हें आपके नेटवर्क कनेक्शन की लोकेशन के आधार पर इनेबल किया जाता है। इन बाउन्ड रुल्स उस ट्रैफिक पर एप्लाई होते हैं जो नेटवर्क और इन्टरनेट से आपके कम्प्यूटर अथवा डिवाइस में आ रहा है। आउट बाउन्ड रुल्स उस ट्रैफिक पर लागू होता है जो आपके कम्प्यूटर अथवा डिवाइस से नेटवर्क या इन्टरनेट पर जा रहा है।

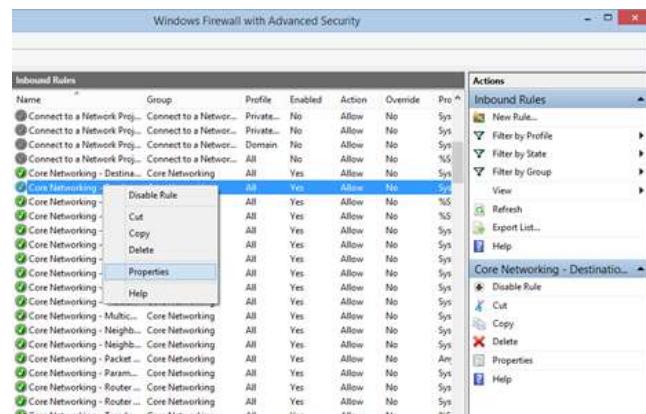
इन रुल्स को कम्प्यूटर्स, यूजर्स, प्रोग्राम्स, सर्विसेज, पोर्ट्स अथवा प्रोटोकोल स्पेसिफिक बनाने के लिए कन्फिगर किया जा सकता है। आप इन्हें नेटवर्क एडेप्टर (यानि वायरलैस, केबल, वर्चुअल प्राइवेट नेटवर्क) अथवा यूजर प्रोफाइल के प्रकार के अनुसार भी कन्फिगर कर सकते हैं।

विन्डोज फायरवॉल विद एडवान्स्ड सिक्युरिटी में आप सभी रुल्स को एक्सेस कर सकते हैं और इनकी प्रॉपर्टीज को एडिट कर सकते हैं। आपको बस लेफ्ट साइड पैनल में यथोचित सैक्षण को क्लिक या टैप करना है।

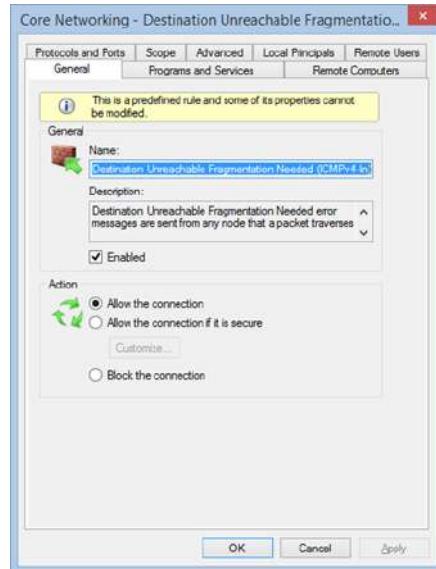


विन्डोज फायरवॉल के टूल्स इनेबल अथवा डिसेबल किए जा सकते हैं। जो रुल इनेबल या एकिटव हैं वे नेम कॉलम में ग्रीन (हरे) चेकबॉक्स से मार्क होते हैं। जो रुल डिसेबल हैं वे ग्रे चेकबॉक्स से मार्क होते हैं।

यदि आप किसी खास रुल अथवा इसकी प्रॉपर्टीज के बारे में जानना चाहते हैं तो आप इस रुल पर क्लिक करें और प्रॉपर्टीज सलेक्ट करें अथवा राइट साइड में प्राप्टीज पर प्रेस करें आपके सामने एक लिस्ट आ जाएगी, अपनी जरूरत के अनुसार इस लिस्ट में से सलेक्ट कर लें।



प्रॉपर्टीज विन्डो में सलेक्ट किए गए रुल के बारे में आपको यह रुल क्या करता है और इसे कब एप्लाई किया जाता है जैसी पूरी जानकारी मिल जाएगी। आप इसकी प्रॉपर्टीज को एडिट कर सकते हैं किसी पैरामीटर को बदल भी सकते हैं।



### 7.2.3.3 कनेक्शन सिक्यूरिटी रुल्स क्या हैं?

कनेक्शन सिक्यूरिटी रुल्स उस ट्रैफिक को सैक्योर बनाने के लिए यूज किए जाते हैं जो एक कम्प्यूटर से दूसरे कम्प्यूटर में आवाजाही के दौरान नेटवर्क से होकर गुजरता है। इसका एक उदाहरण वह रुल है जो यह बताता है कि किन्हीं दा कम्प्यूटर के बीच कनेक्शन एनक्रिप्टेड होना चाहिए।

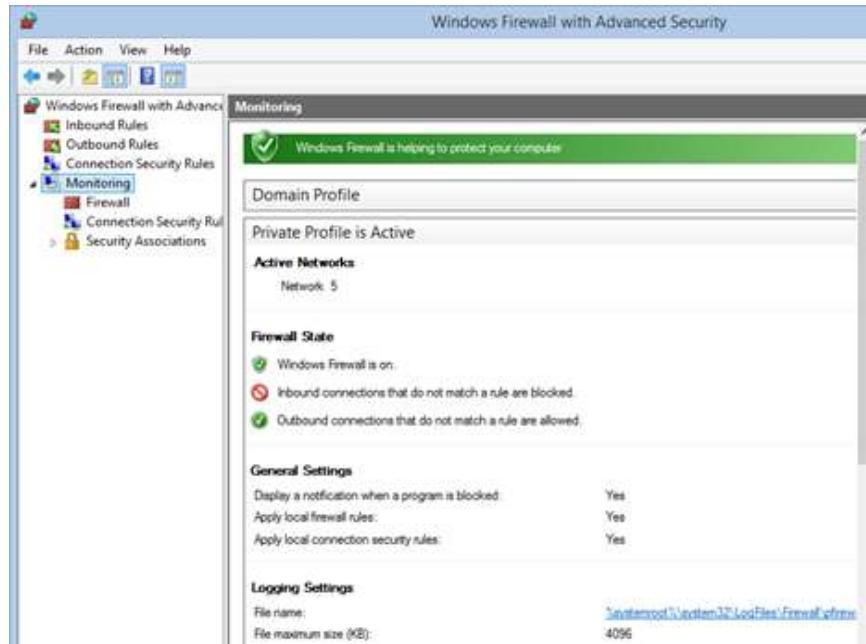
इन बाउन्ड और आउट बाउन्ड रुल्स केवल एक कम्प्यूटर पर सप्लाई किए गए हैं। लेकिन यहाँ ऐसा नहीं है कनेक्शन रुल्स में दोनों कम्प्यूटरों के लिए एक जैसे तयशुदा रुल्स होने ही चाहिए और साथ ही ये रुल्स इनेबल भी होने चाहिए।

यदि आप यह देखना चाहते हैं कि आपके कम्प्यूटर पर क्या ये रुल्स हैं, लेफ्ट साइड पर पैनल में “कनेक्शन सिक्यूरिटी रुल्स” को विलक अथवा टैप करें। विन्डोज कम्प्यूटर्स और डिवाइसेज पर बाइ डिफाल्ट ऐसे कोई रुल्स डिफाइन्ड नहीं हैं आमतौर पर कोरोबारी माहौल में इनका यूज होता है और नेटवर्क एडमिनिस्ट्रेटर ये रुल्स सेट करते हैं।



### 7.2.3.4 विन्डो फायरवॉल विद एडवान्स्ड सिक्यूरिटीज मॉनीटर का क्या कार्य है?

विन्डोज फायरवॉल विद एडवान्स्ड सिक्यूरिटी में कुछ मॉनिटरिंग फीचर शामिल हैं। मॉनिटरिंग सैक्षण में आप को निम्नलिखित जानकारी मिलती है : एकिटव फायरवॉल रूल्स (इन बाउन्ड और आउट बाउन्ड दोनों), कनेक्शन सिक्यूरिटी रूल्स जो एकिटव हैं और कोई अन्य सिक्यूरिटी एशोसिएशन जो एकिटव है।



यह ध्यान रखें कि मॉनिटरिंग सैक्षण केवल मौजूदा नेटवर्क लोकेशन के लिए एकिटव रूल्स शो करता है। यदि कोई रुल जो किसी अन्य नेटवर्क लोकेशन के लिए एकिटव किए गए हैं, वे इस सैक्षण में नजर नहीं आएंगे।

उपरोक्त खण्ड में हमने विन्डोज और मैक ऑपरेटिंग सिस्टम पर फायरवॉल सैट अप करने के तरीके पढ़े। लिनक्स के अनेक वैरिएन्ट हैं, इसलिए लिनक्स पर फायरवॉल कन्फिगर करन के तरीकों पर यहाँ चर्चा करना सम्भव नहीं होगा नीचे कुछ वीडियो दिए गए हैं जिनसे आप लिनक्स के अलग-अलग वैरिएन्ट्स में फायरवॉल सैटअप करने की प्रक्रिया समझ सकते हैं।

## लिनक्स के लिए वीडियो

<https://www.youtube.com/watch?v=hkzhtr fzpc>

<https://www.yautube.com/watch?v=ooa09cqi-48>

<https://www.youtabe.com/watch?v=vbzp2-Qvc40>

## अभ्यास

1. अपने सिस्टम में फायरवॉल सेटअप और कन्फिगर करें।
2. इन्टरनेट पर उपलब्ध फ्री और कामर्शियल फायरवॉल खोजें।

—□—

## अपनी जरूरत के अनुकूल सर्वश्रेष्ठ ब्राउजर का चयन करें

### 8.1 यूजर की आवश्यकता के अनुसार सर्वश्रेष्ठ ब्राउजर तलाशना<sup>9</sup>

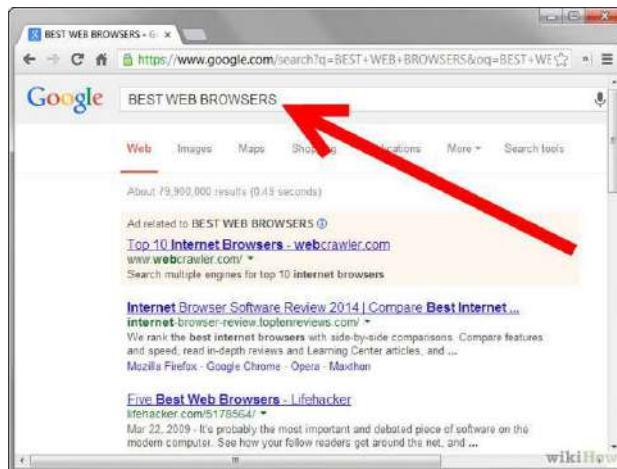
आजकल ज्यादातर कार्यों के लिए ब्राउजर इन्टरनेट की कुंजी (की) है। प्रत्येक प्लेटफार्म और आपरेटिंग सिस्टम के लिए बहुत से ब्राउजर उपलब्ध हैं। इसलिए चयन करना बड़ा मुश्किल हो जाता है। लेकिन हम यहाँ कुछ नुस्खे दे रहे हैं, इससे आप को ब्राउजर चुनने में मदद मिलेगी।

---

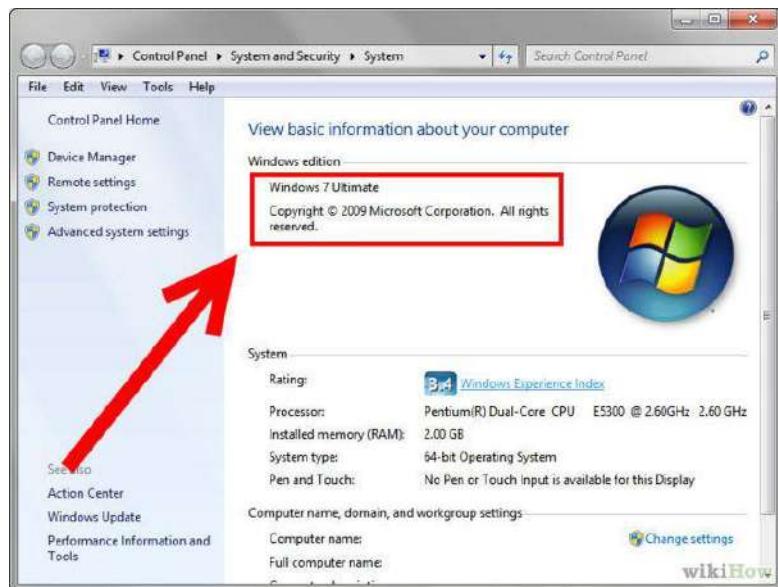
<sup>9</sup> <http://www.wikihow.com/Choose-an-Internet-Browser>



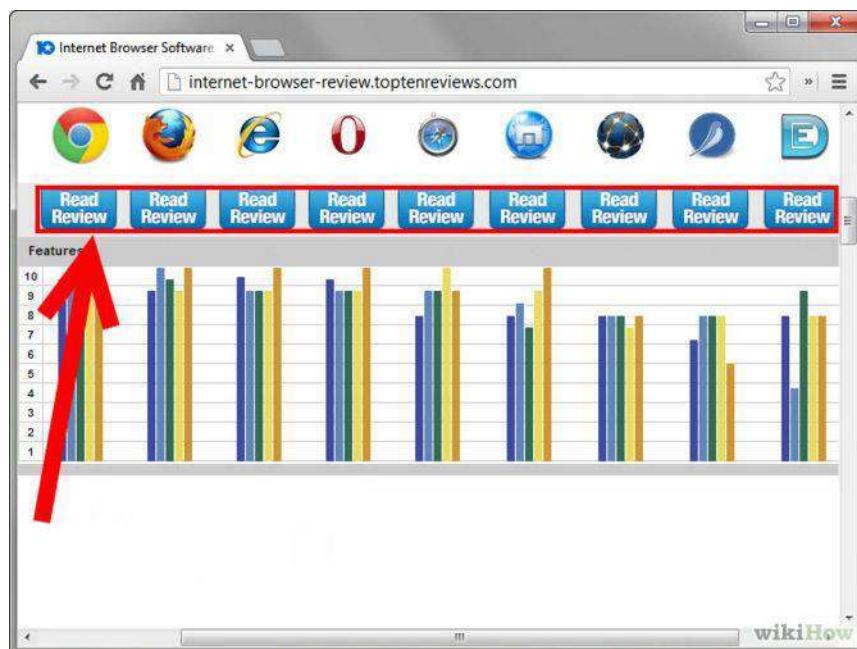
**स्टेप-1 :** यह देखें कि आपका कम्प्यूटर कितना पुराना है? क्या यह मोबाइल डिवाइस है। अपने सिस्टम की स्पेसिफिकेशन्स को जानें क्योंकि कुछ खास ब्राउजर ही इनके अनुकूल होंगे।



**स्टेप-2 :** अपने लिए आदर्श ब्राउजर की कल्पना करें, वह कैसा हो? हो सकता है कि आप चाहेंगे यह आसान हो, आपकी प्रत्यक्ष जरूरतों को हैण्डल करने में सक्षम हो। साथ ही आप चाहेंगे कि उसमें फीड रीडिंग, बुक मार्किंग (पसंदीदा) अथवा सर्च बॉक्स जैसे बुनियादी फोचर हों। कुछ ब्राउजरों में इसके अलावा और भी बहुत से फीचर होते हैं और यहाँ से कन्प्यूजन शुरू होता है।



**स्टेप-3 :** आप कौन सा ऑपरेटिंग सिस्टम यूज कर रहे हैं, यह आपको जरुर पता होना चाहिए। कुछ ब्राउजर ऐसे हैं जो किसी खास ऑपरेटिंग सिस्टम के लिए बने हैं या फिर कुछ ऐसे ब्राउजर भी हैं जो किसी खास ऑपरेटिंग सिस्टम के लिए नहीं हैं।



**स्टेप-4 :** रिसर्च ब्राउजर्स। टैब्ड ब्राउजर्स में सफारी (ओ एस एक्स, आई फोन पर चलता है, विन्डोज के लिए नया है), फायरफॉक्स (सर्वाधिक प्लग-इन वाला जनरल पर्पज), ऑपेरा टोरेन्ट को सपोर्ट करता है, ई-मेल्स हैण्डल करता है और मोबाइल उपकरणों पर चलता है) कॉन्करर (डुएल पर्पज फाइल मैनेजर),

सीमॉन्की (इसमें एचटीएमएल एडीटर और ईमेल क्लाइन्ट शामिल हैं) ऑफ बाई वन (टिनी) और फ्लॉक (सोशल नेटवर्किंग)

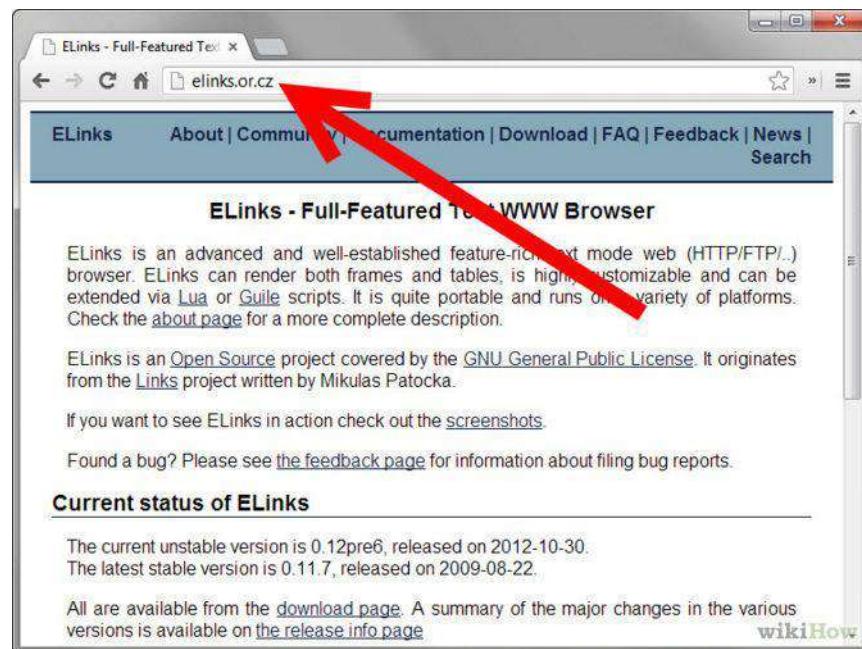
The screenshot shows a comparison chart titled "Internet Browser Software" from [toptenreviews.com](http://internet-browser-review.toptenreviews.com). The chart compares seven browsers: Chrome, Firefox, Internet Explorer, Opera, Safari, and two others whose names are partially visible. The columns represent different metrics: Speed (Initial Startup Time, Average Startup Time, Navigation Time), Features (Tabbed Browsing, Add-ons, Integrated Search Engine, Save Tabs, Customization Options, Bookmarks, RSS Feeds, Zoom, Find-On Page Function, Password Manager, Autofill, Automatic Updates), and Read Review (links to reviews for each browser). A large red arrow points to the "Features" column header.

	Initial Startup T.	Average Startup T.	Navigation T.	Read Review						
<b>Speed</b>										
Initial Startup T.	4	8.3	4.3	5.1	4.2	8	9			
Average Startup T.	4.3	8.3	4	4.4	3.7	5.9	4			
Navigation T.	4.4	5.7	4.5	4.6	3.8	3.2	11			
<b>features</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tabbed Browsing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Add-ons	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Integrated Search Engine	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Save Tabs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Customization Options	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Bookmarks	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
RSS Feeds	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Zoom	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Find-On Page Function	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Password Manager	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Autofill	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Automatic Updates	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

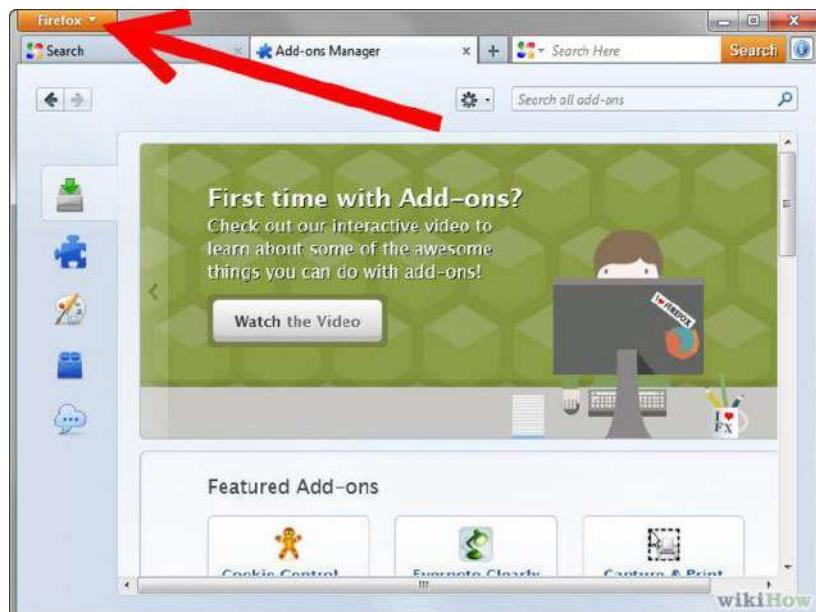
स्टेप-5 : अपने जो भी ब्राउजर तलाशे हैं उनके फीचर की तुलना अपने जरूरत वाले ब्राउजर से करें।

The screenshot shows the homepage of the Off By One Web Browser at [offbyone.com/offbyone/](http://offbyone.com/offbyone/). The page has a yellow header with the text "Yes, Another Free Web Browser". The main content area features a yellow sidebar with links like Home, Overview, FAQ, Help, Download, and Search. The main content area includes sections for "The Browser Has Landed" (describing the browser as the world's smallest and fastest), "New!" (mentioning a tabbed browsing interface), and "Also available as a component for Windows developers". A large red arrow points to the address bar at the top of the browser window.

स्टेप-6 : यदि आपके कम्प्यूटर की मेमोरी कम है, तो लोअर मेमोरी वाले ब्राउजरों पर विचार करें। ऑफ बाई वन, डिल्लो, स्किपस्टोन और नेटसर्फ इनमें से एक हो सकते हैं।



**स्टेप-7 :** यदि आप तेज से तेज (अधिकतम स्पीड/हाइपर ड्राइव) ब्राउजर की तलाश में हैं, तो टैक्स्ट बेस्ड-ब्राउजर ठीक रहेगा। इलिन्क्स ऐसा ही एक ब्राउजर है।



**स्टेप-8 :** पता लगाएं कि क्या आप अपनी जरूरत के अनुसार कोई फीचर प्लगइन अथवा एक्सटेंशन के रूप में इस ब्राउजर विशेषकर फायर फॉकस में जोड़ सकते हैं।



स्टेप-9 : अपना नया ब्राउजर डाउनलोड करें और इन्स्टॉल करें।

#### अभ्यास-

- विभिन्न प्रकार के ब्राउजरों की उनकी विशेषताओं के आधार पर तुलना करें।

—□—

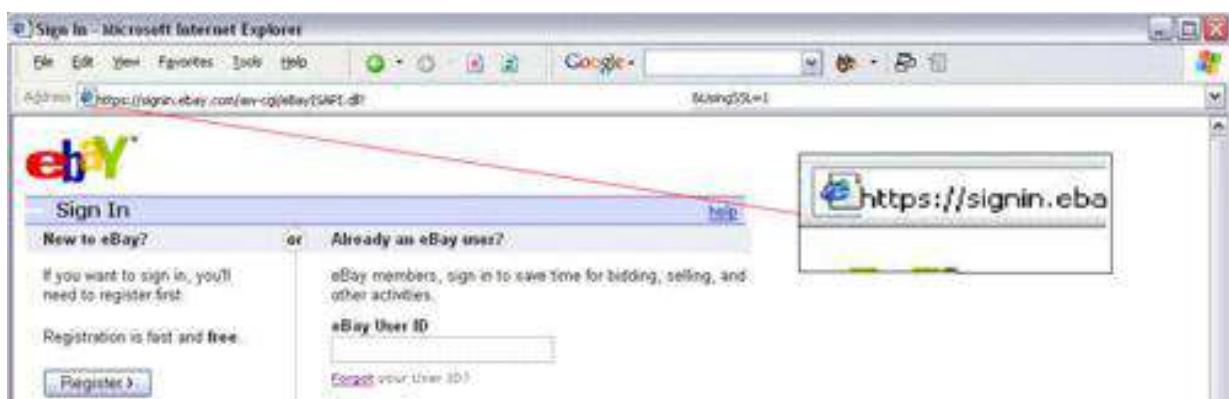
# सेफ इन्टरनेट ब्राउजिंग के दिशा-निर्देश

## 9.1 सुरक्षित ब्राउजिंग

इन्टरनेट यूजर्स के लिए इन्टरनेट सुरक्षा सबसे अधिक चिन्ता का विषय है। इन्टरनेट सफ करते समय यह जानना अहम है कि वह वेबसाइट सेक्योर है या नहीं<sup>10</sup>। वेबसाइट यदि सेक्योर है तो वेब ब्राउजर और वेबसाइट के बीच सुरक्षित कनेक्शन प्रदान करेगी ताकि पर्सनल इन्फॉर्मेशन, क्रेडिट कार्ड डिटेल्स, बैंकिंग इन्फॉर्मेशन आदि जैसे डाटा तक अनाधिकृत व्यक्तियों की पहुंच न हो। जब भी ब्राउजर कोई सेक्योर कनेक्शन खोलता है, यूआरएल में ऊजच की जगह ऊजचे दिखाई देगा। कोई वेबसाइट सेक्योर है या नहीं यह जानने के लिए ब्राउजर विन्डो के निचले दायें कोने पर पीले रंग के बंद ताले का निशान तलाशें।

### 9.1.1 कैसे जानें कि वेबसाइट सेक्योर है या नहीं?

कुछ वेबसाइटें आपके वेब ब्राउजर और वेबसाइट के बीच सेक्योर कनेक्शन का इस्तेमाल करती है। और आपके लिए यह बहुत महत्वपूर्ण है। उदाहरण के लिए, यदि आप किसी उत्पाद या सेवा के लिए ऑनलाइन पेमेन्ट करना चाहते हैं और आपको इसके लिए क्रेडिट कार्ड की जानकारी और व्यक्तिगत जनकारी एन्टर करनी है। यह जानने के लिए कि आपका ब्राउजर सेक्योर वेबसाइट दिखा रहा है, विन्डो के निचले दाहिने पार्ट पर नजर डालें। वहाँ आप किस जोन (आमतौर पर इन्टरनेट जोन, ग्लोब के आइकन के साथ) में है, यह बताने वाले एरिया के बांयी तरफ की विन्डो के फ्रेम में एक छोटा बॉक्स होगा। यदि आपको पीले रंग के बंद पैडलॉक का आइकन नजर आता है, तो जो वेबसाइट आप देख रहे हैं वह “सेक्योर वेबसाइट” है। यदि बॉक्स खाली है, तो इस वेबसाइट का आपके ब्राउजर के साथ सेक्योर कनेक्शन नहीं है।



<sup>10</sup> <http://ccm.net/faq/2-how-do-i-know-if-a-website-is-secure>

## **9.2 ऑनलाइन खरीददारी के सुझाव**

आपके लिए और बिजनेस के लिए ऑनलाइन खरीददारी किफायती और सहूलियत पूर्ण हो सकती है। लेकिन, खरीददारी से पहले और किसी ऑनलाइन नीलामी में बोली लगाने से पहले आपको अपने अधिकार और जोखिमों की जानकारी भी होनी चाहिए।

### **1. सुरक्षित तरीके से भुगतान करें : भुगतान तब करें जब :-**

- आप सुरक्षित (सेक्योर) वेबसाइट पर हों, और आप सुरक्षित भुगतान कर सकें।
- इससे आप धोखाधड़ी और अनाधिकृत क्रेडिट कार्ड लेन-देन से बच जाएंगे। सेक्योर वेबसाइट का एड्रेस हमेशा : ऐजजचर्ल्ड्स से शुरू होगा, न कि ऐजजचर्ल्ड्स से
- बंद पैडलॉक (ताले) का आइकन नजर आएगा (आमतौर पर आपके ब्राउजर विन्डो दाहिने कोने में नीचे की तरफ)।
- आपको ये दोनों चीजें नजर आएं तभी पेमेन्ट करें। यदि आपको पक्के तौर पता नहीं है कि यह बिजनेस एक प्रतिष्ठित कारोबारी का है तो अपना बैंक डिटेल, क्रेडिट कार्ड नम्बर तथा अन्य व्यक्तिगत जानकारी बिल्कुल न दें।

### **2. बिजनेस की जानकारी रखें:-**

केवल उसी वेबसाइट से खरीददारी करें जिस पर आपका भरोसा है। चैक करें कि कम्पनी का फिजिकल स्ट्रीट एड्रेस और लैण्डलाइन नम्बर हो। यदि कम्पनी किसी बाहरी देश से कारोबार कर रही तो आपको पैसा वापस लेने, उत्पाद की मरम्मत कराने में दिक्कत आ सकती है।

### **3. उत्पाद की जानकारी रखें : चैक करें कि:-**

- उत्पाद वैध है
- उत्पाद मेरे देश में काम करेगा
- वारण्टी या गारण्टी मेरे देश में वैध है
- उत्पाद की सर्विस या मरम्मत करने वाले आपके आस-पास अवस्थित हैं।

### **4. कॉन्ट्रैक्ट (शर्तें) जांच लें : शर्तें को पढ़ें और समझ लें:-**

- बिक्री की शर्तें।
- पैसा वापस करने की पॉलिसी
- डिलावरी विवरण
- रिटर्न और रिपेयर पॉलिसी, और इससे जुड़ी लागत यदि कोई हो।

### **5. खरीददारी की पूरी लागत:-**

अपनी खरीददारी की पूरी लागत की जानकारी रखें। अतिरिक्त लागत में निम्नलिखित शामिल हो सकता है:-

- मुद्रा परिवर्तन (करैसी कनवर्जन)
- टैक्स
- पोस्टेज और डिलीवरी शुल्क
- पैकेजिंग
- ये सब जोड़ने के बाद हो सकता है कि यही उत्पाद स्थानीय बाजार में सस्ता मिले।

## **6. प्रोजेक्ट और प्राइवेसी:-**

ऑनलाइन तभी खरीदें जब आप कम्पनी की प्राइवेसी पॉलिसी से सन्तुष्ट हों। बिक्री प्रक्रिया को पूरा करने के लिए आवश्यक होने पर ही इन्फॉर्मेशन दें, अन्यथा नहीं। याद रखें, यदि सौंदा इतना आकर्षक है कि उस पर संदेह होने लगे, तो आपका संदेह शायद सच हो।

## **7. रिकार्ड रखें:-**

हमेशा निम्नलिखित दस्तावेज के रिफरेंस नम्बर और प्रिंट आउट प्रतियां अवश्य रखें।

- आर्डर फार्म (आर्डर कन्फर्म करने से पहले और बाद के)
- रिसीप्ट (ई-मेल या पॉप-अपविन्डो से मिल सकती है। रिसीप्ट का मिलान निम्नलिखित दस्तावेजों से आवश्य करें और सुनिश्चित करें कि लिए गए सभी शुल्क सही हैं:
- क्रेडिट कार्ड स्टेटमेंट
- मर्चन्ट एकाउन्ट स्टेटमेंट (जैसे कि पे-पैल)
- बैंक स्टेमेंट

शुल्कों को एक मुद्रा से दूसरी मुद्रा में कन्वर्ट करके मिलान किया जा सकता है।

## **8. ऑनलाइन ऑक्सन साइट्स :**

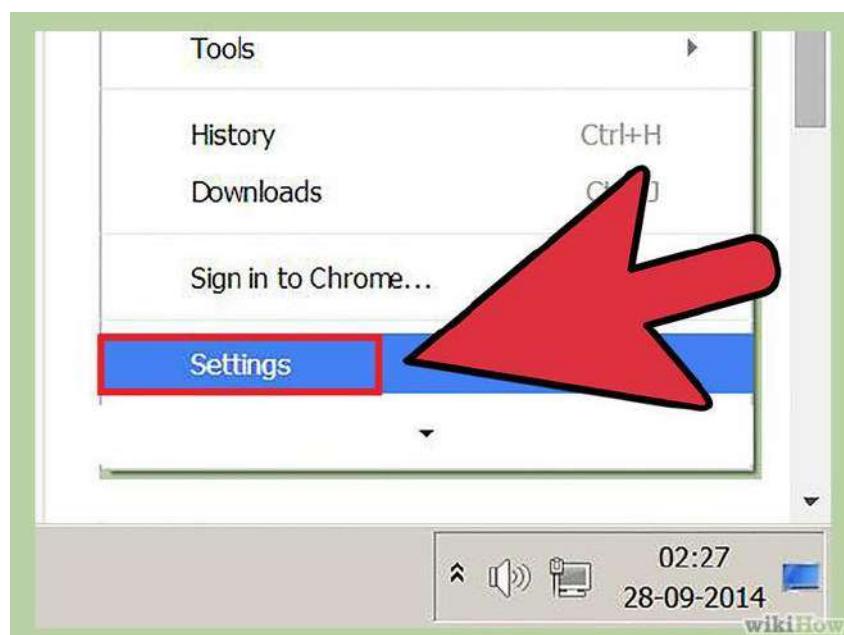
ज्यादतार ऑनलाइन ऑक्सन साइटें (जैसे कि ई.बे) खरीददार और विक्रेता के लिए विवाद समाधान प्रक्रिया का विवरण देती है। विवाद समाधान का यह पहला कदम होना चाहिए, यदि :

- आपको वह सामान नहीं मिला, जो आपने खरीदा था,
  - आपको अपने बेचे गए सामान का भुगतान नहीं हुआ,
  - आपको जो सामान मिला वह साइट पर दिए विवरण से बहुत कम मेल खाता है।
- ई-बे ने इस सुविधा का उदाहरण दिया है।

## 9.3 ब्राउजर का कैशे क्लीयर करना

जब भी आप कम्प्यूटर अथवा मोबाइल पर किसी वेबपेज पर जाते हैं, आपका इन्टरनेट ब्राउजर कैशे उस वेबपेज की कुछ जानकारी (स्नैप शॉट्स) स्टोर कर लेता है ताकि आगे कभी भी आप उस पेज पर जाएं या किसी ऐसी वेबसाइट को नेवीगेट करें या उसी इमेल वाले अनेक पेज हों तो आपका कैशे उसी पेज को तुरन्त डाउनलोड करेगा और साथ ही एक ही इमेल के अनेक बार डाउनलोड होने से रोकेगा<sup>11</sup>। कभी-कभार आपका कैशे आपको अपडेटेड कन्टेट नहीं दिखाता या स्टोर किए गए कन्टेट तथा लाइव कन्टेट में अन्तर होने पर फंक्शनल समस्या आ सकती है। इसी तरह की अनेक समस्याओं का समाधान है, कैशे को समय-समय पर क्लीअर करते रहना। इस अध्याय में स्क्रीन शॉट्स के जरिए यही समझाया जाएगा सभी ब्राउजरों के कैशे किस तरह क्लीअर करें।

### 9.3.1 वर्जन 10 से ऊपर के क्रोम ब्राउजर के कैशे क्लीअर करना



**स्टेप-1 :** क्रोम पर सैटिंग ओपन करें। दाहिनी ओर ब्राउजर के अपर राइट कॉर्नर में मैन्यू आइकन को विलक करें। मैन्यू के बॉटम में सैटिंग्स विलक करें।

<sup>11</sup> <http://www.wikihow.com/Clear-Your-Browser%27s-Cache>

**Users**

You are currently the only Google Chrome user.

Add new user... Delete this user Import b...

**Default browser**

The default browser is currently Google Chrome.

Show advanced settings...



wikiHow

स्टेप-2 : सेटिंग्स से, “शो एडवान्स्ड सैटिंग्स” पर विलक करें। यह सेटिंग सैक्षण के बिल्कुल बॉटम में मिलेगी।

**Privacy**

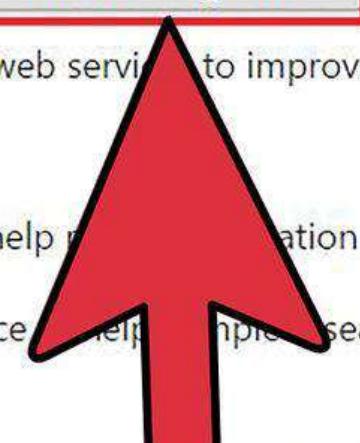
Content settings... Clear browsing data...

Google Chrome may use web services to improve your services. [Learn more](#)

Use a web service to help resolve application errors

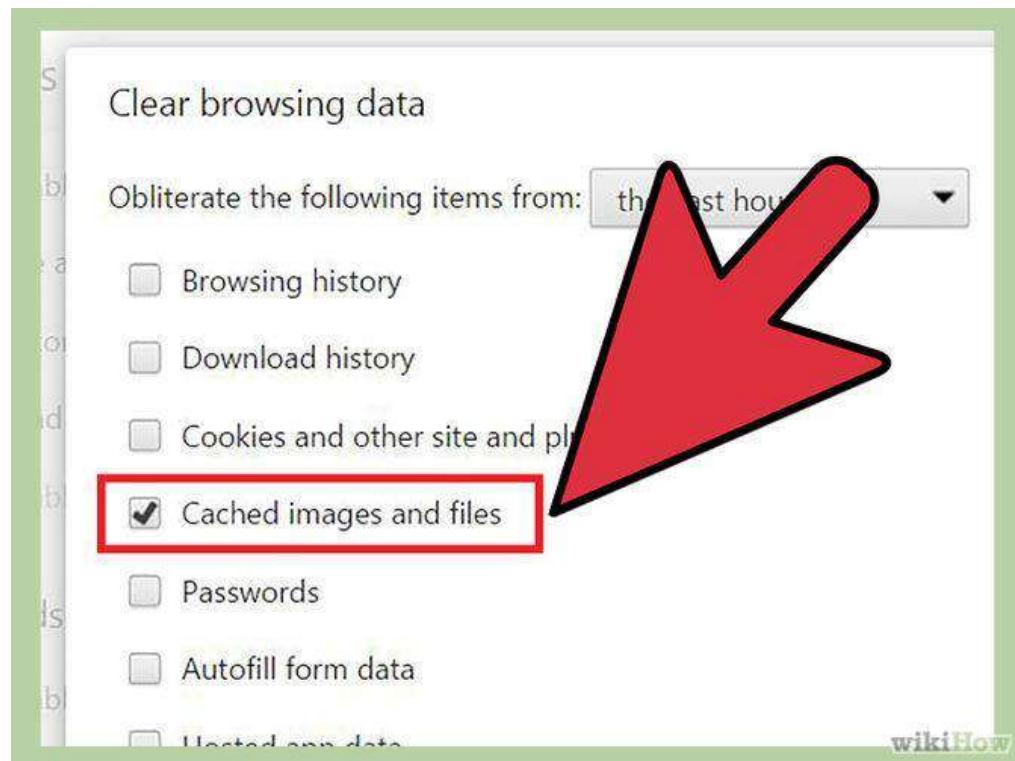
Use a prediction service to help complete search queries in the search box

Predict network actions to improve page load performance

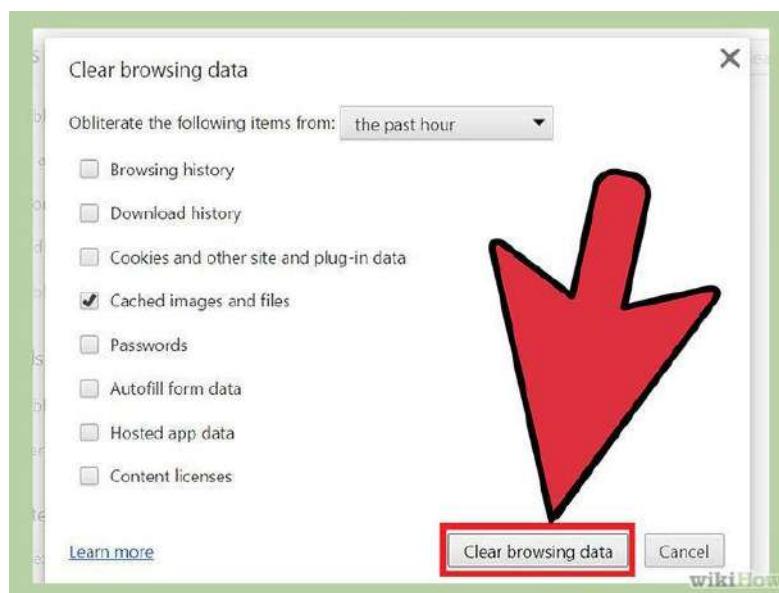


wikiHow

स्टेप-3 : प्राइवेसी सैक्षण में जाएं और ‘कलीअर ब्राउजिंग डाटा’ पर क्लिक करें।

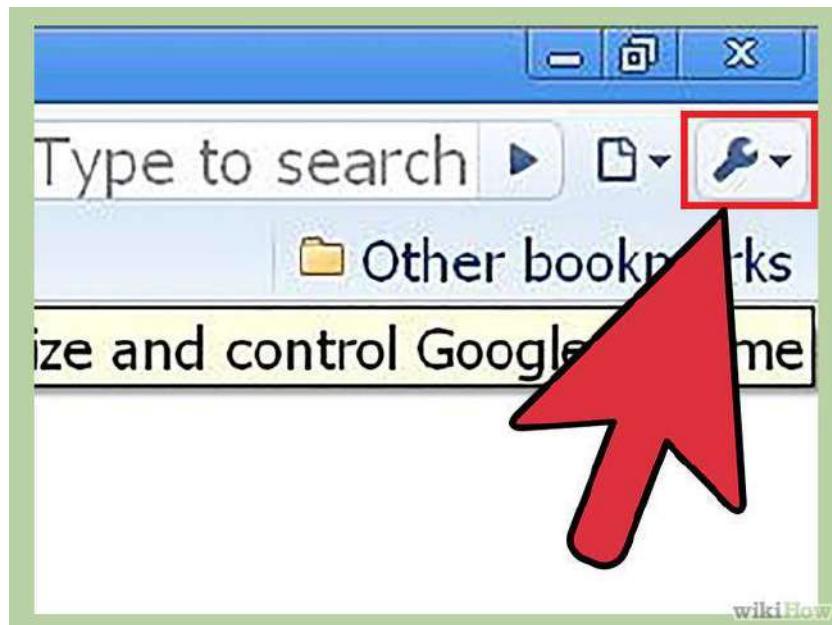


स्टेप-4 : “कैच्ड इमेजेज एण्ड फाइल्स” सलेक्ट करें। सभी अन्य आप्शन्स को अनचैक करें ताकि ब्राउजर की हिस्ट्री, कुकीज और वो अन्य चीजें जो आप रखना चाहते हैं, डिलीट न हों। “ऑब्लिट्रेट फौलोइंग आइटम्स फ्रॉम” को “दी बिगनिंग ऑफ टाइम” में चेन्ज करें।

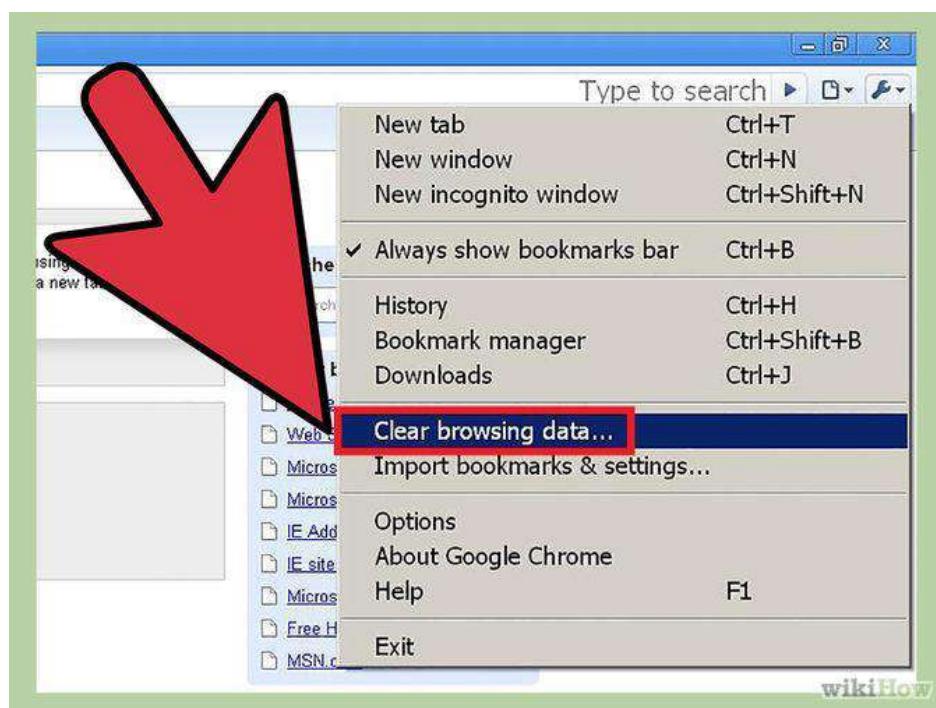


स्टेप-5 : “क्लीअर ब्राउजिंग डाटा” प्रेस करें। आपका काम हो गया है।

### 9.3.2 क्रोम ब्राउजर वर्जन 1 से 9 में कैसे क्लीअर करना



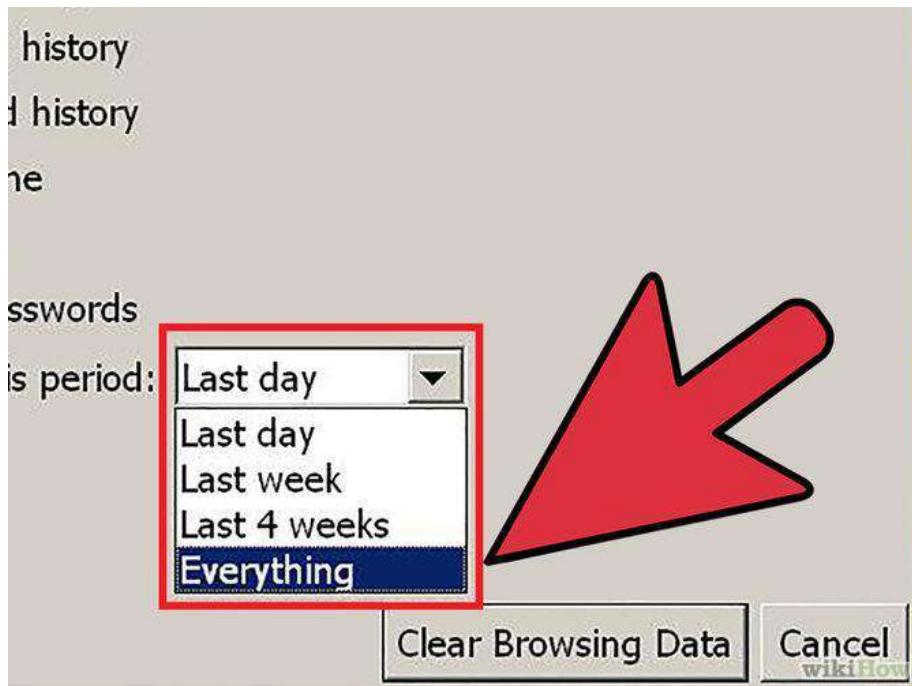
स्टेप-1 : ब्राउजर ओपन करने के बाद टूल मैन्यू (अपर राइट कॉर्नर में रेंच का निशान) सलेक्ट करें और ऑपशन्स (प्रीफरेंस ऑन मैक) सलेक्ट करें।



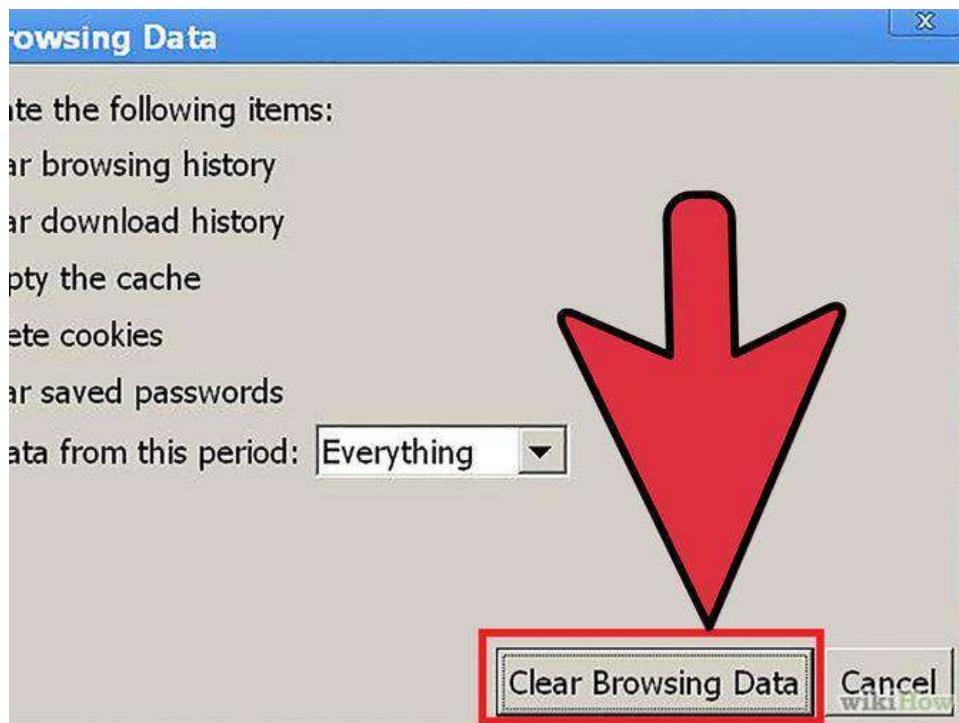
स्टेप-2 : हूड टेब के तहत, “क्लीअर ब्राउजिंग डाटा” बटन पर विलक करें



स्टेप-3 : “एम्पटी दी कैशे” चेक बॉक्स सलेक्ट करें



स्टेप- 4 : आप वह तारीख भी चुन सकते हैं जब से आप कैशे की इन्फॉर्मेशन डिलीट करना चाहते हैं। इसके ड्रापडाउन मैन्यू में “क्लीअर डाटा फॉर्म दिस पीरियड” पर जाएं और अपना समय चुनें।

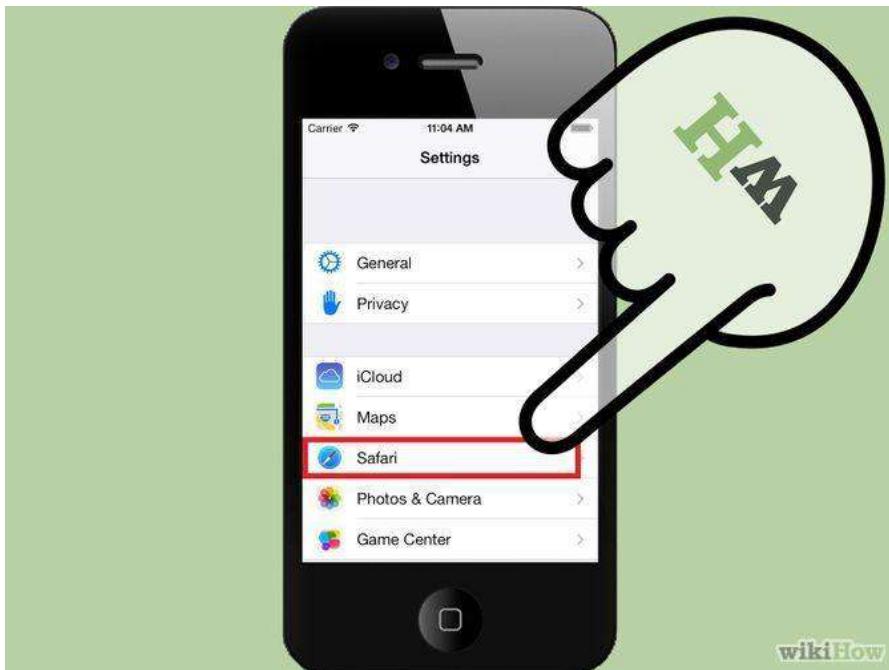


स्टेप-5 : “क्लीअर ब्राउजिंग डाटा” बटन क्लिक करें।

### 9.3.3 आई फोन और आइपैड के ब्राउजर “सफारी” का कैशे क्लीअर करना



**स्टेप-1** : होमपेज से सैटिंग्स पर विलक करें।

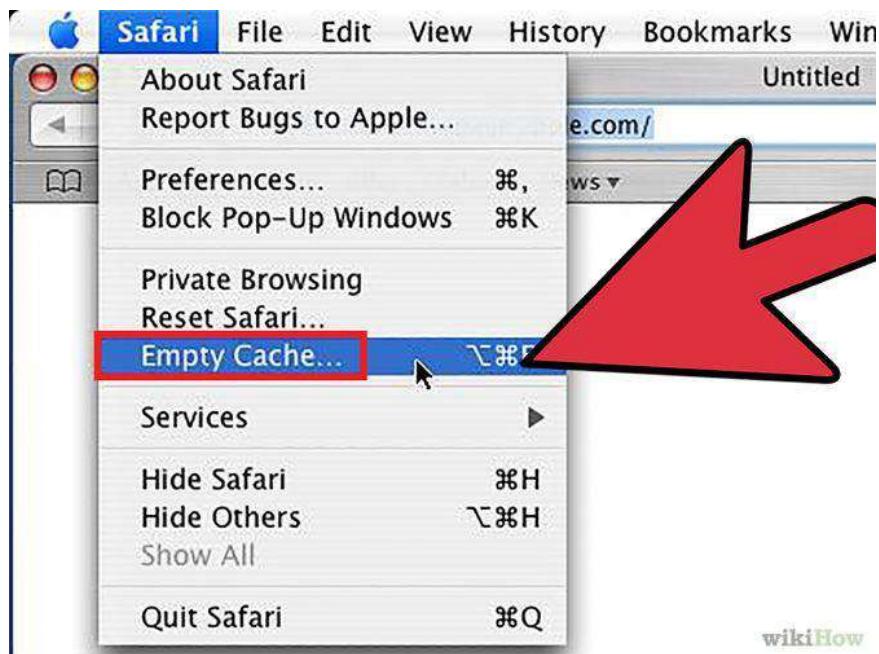


**स्टेप-2** : नीचे की ओर स्क्रोल करें और “सफारी” पर पहुंचें। उस पर विलक करें, ऑप्शन पेज आएगा।

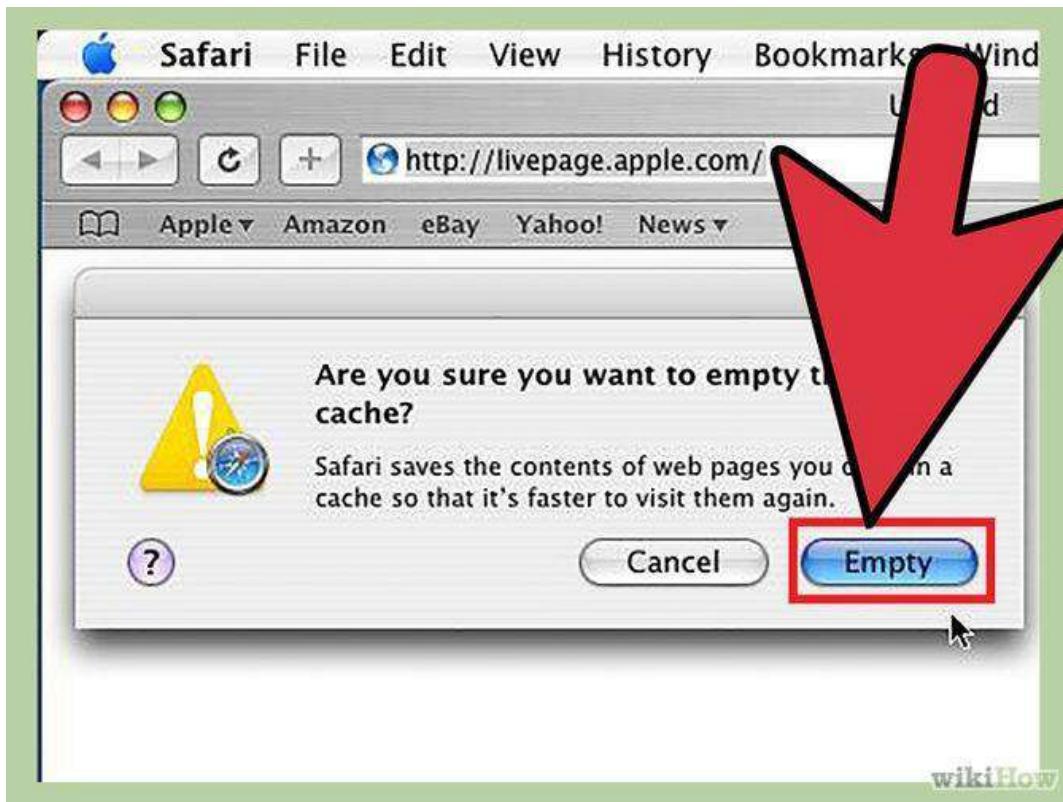


**स्टेप-3** “कलीअर कुकीज एण्ड डाटा” पर विलक करें। एक पॉप-अप बॉक्स दिखाई देगा। अपने विकल्प को कन्फर्म करने के लिए फिर से “कलीअर कुकीज एण्ड डाटा” पर विलक करें।

#### 9.3.4 मैक और एस एक्स के "सफारी" का कैसे क्लीअर करना

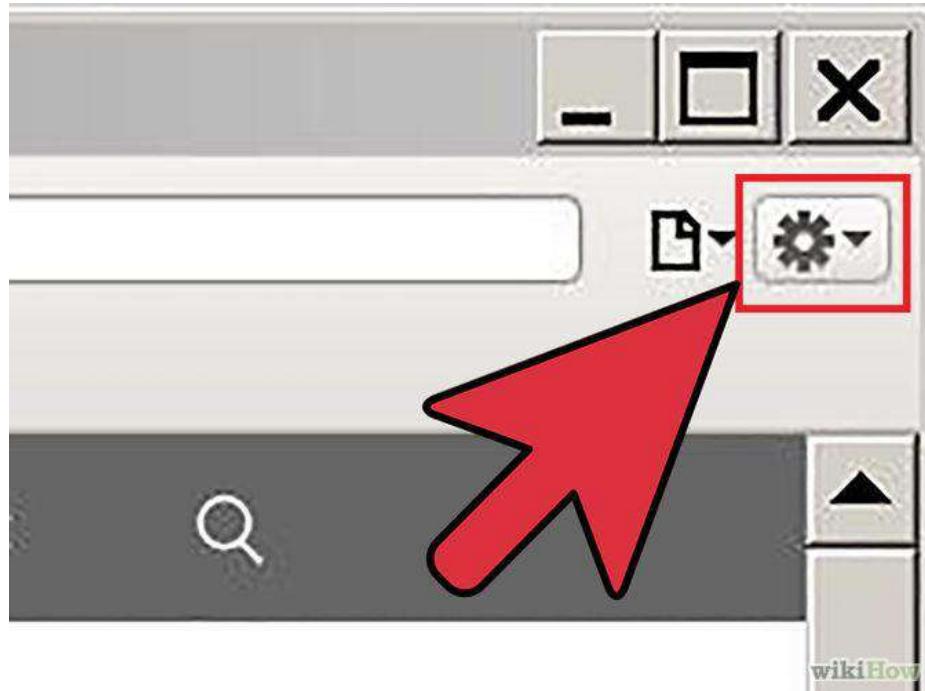


स्टेप-1 : ब्राउजर खुलने के बाद, सफारी मैन्यू पर विलक करें और एम्प्टी कैश सलेक्ट करें।

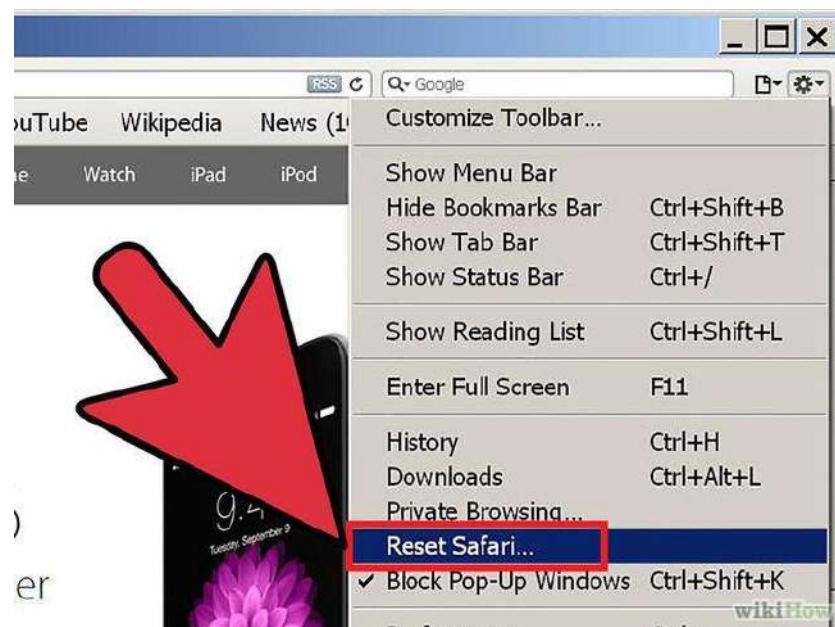


स्टेप-2 : “एम्पटी” विलक करें।

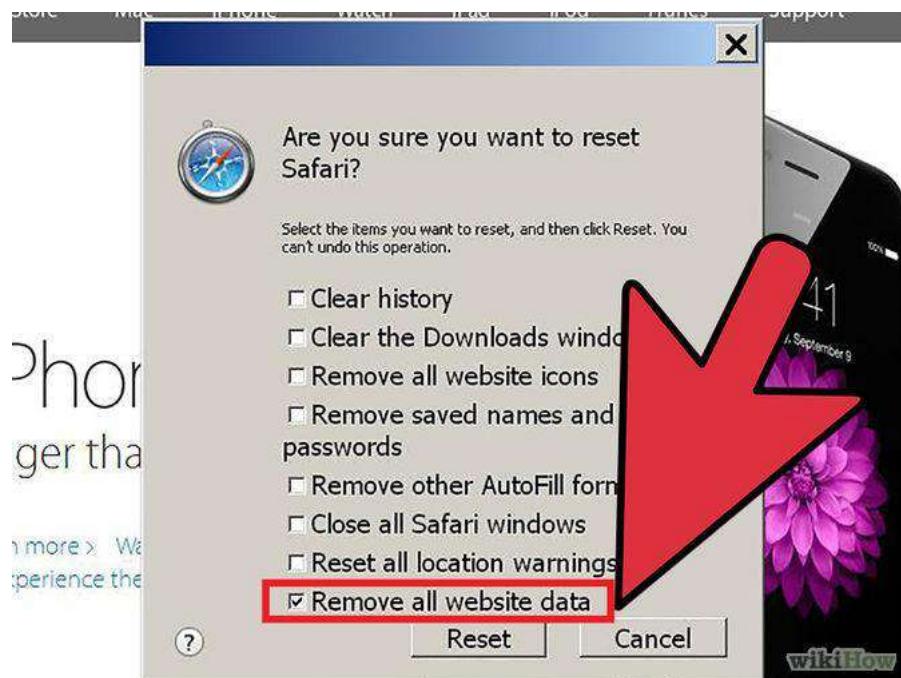
#### 9.3.5 विन्डोज के लिए “सफारी” का कैशे क्लीअर करना



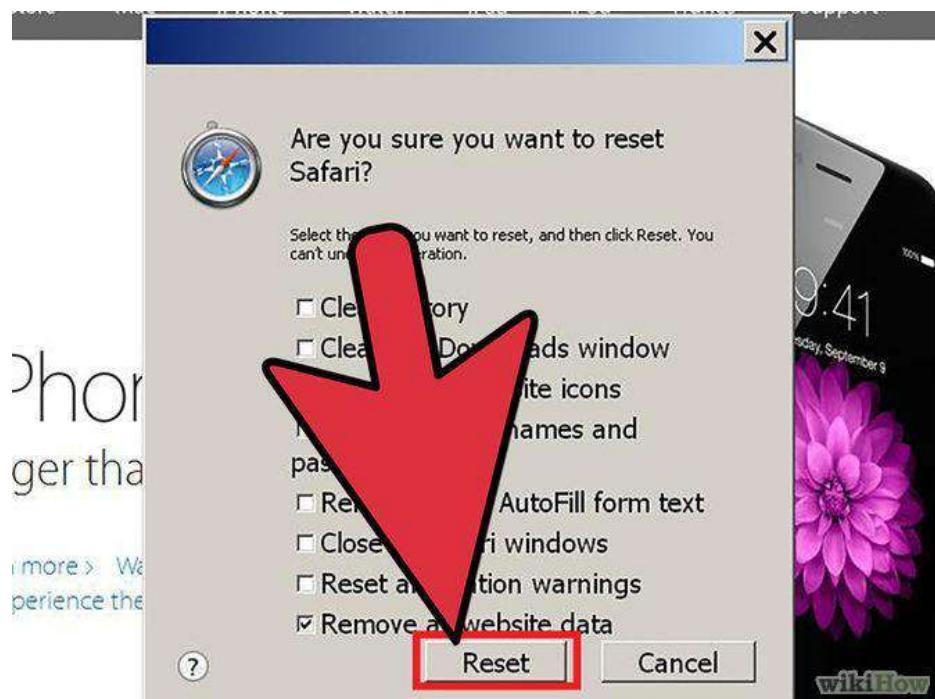
स्टेप-1 : ब्राजउर खुल जाने पर, दाहिनी ओर सबसे ऊपर गीयर आइकन को विलक करें।



स्टेप-2 : “री-सैट सफारी” सलेक्ट करें, इससे एक स्क्रीन खुलेगी।

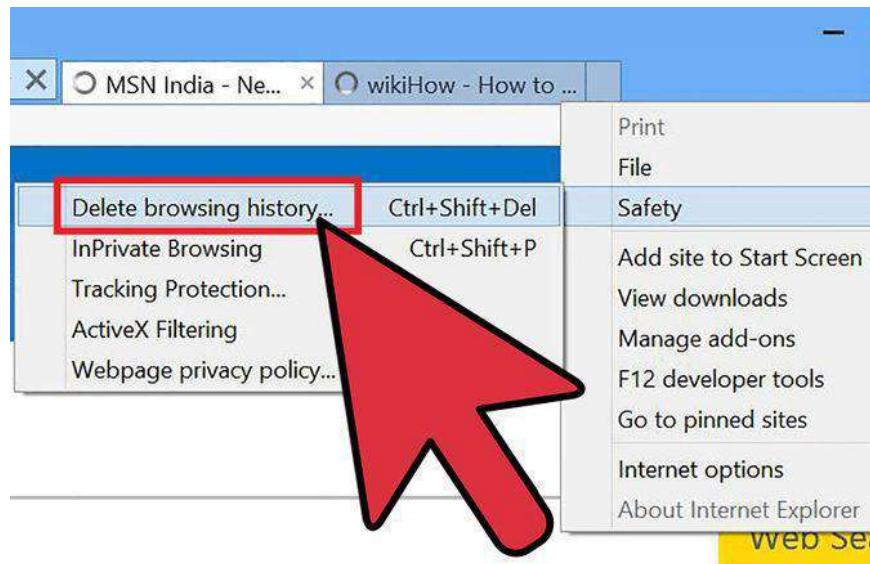


स्टेप-3 : इस प्रॉम्प्ट स्क्रीन के बिल्कुल बॉटम में “रिमूव ऑल वेबसाइट डाटा” सलेक्ट करें। यदि आप किसी अन्य कैटेगरीज को रीसैट करना चाहते हैं तो उन्हें विलक या अनचैक करें।



स्टेप-4 “री सैट” विलक करें।

#### 9.3.6 इन्टरनेट एक्सप्लोरर 9, 10 और 11 के लिए कैशे क्लीअर करना



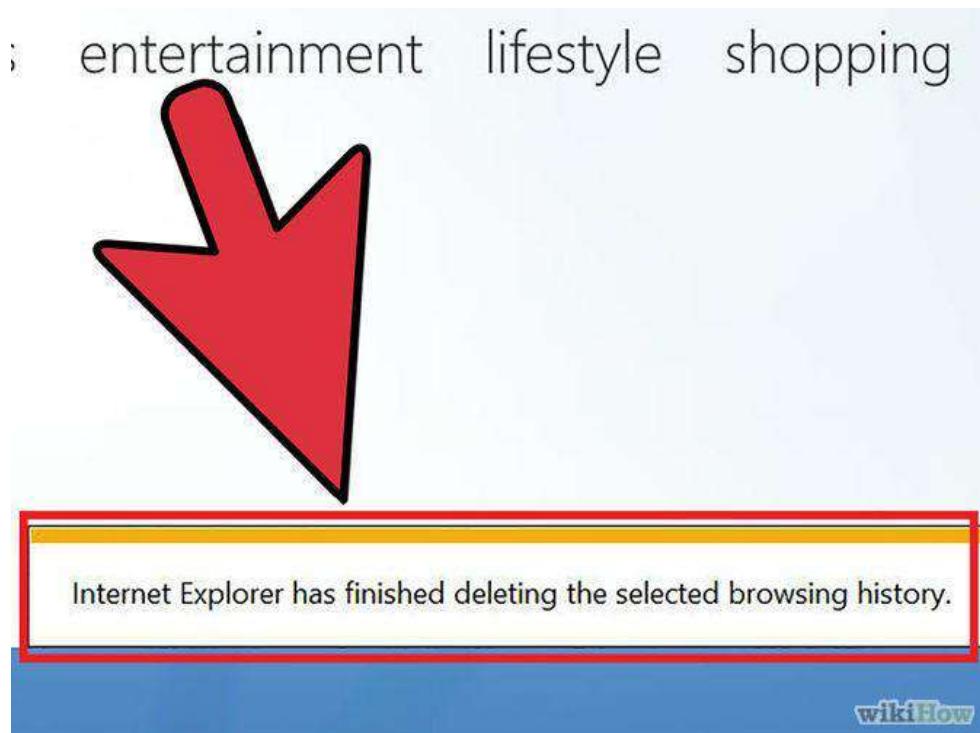
स्टेप-1 : ब्राजउर खुल जाने पर, सैटिंग्स मैन्यू को खोलने के लिए सबसे ऊपर दाहिनी ओर गीयर आइकन को विलक करें, इसके बाद सेफ्टी और डिलीट ब्राउजिंग हिस्ट्री को सलेक्ट करें।



**स्टेप-2 :** टैम्परेरी इन्टरनेट फाइल्स सलेक्ट करें। आपको अन्य सभी बॉक्स खासकर प्रीजर्व फेवरेट वेबसाइट डाटा को अनचेक करना होगा। यह ऑप्शन विन्डोज को आपके फेवरेट फोल्डर में मौजूद वेबसाइट्स से ऑबजेक्ट्स भी डिलीट करने की अनुमति देता है।



**स्टेप-3 :** विन्डो में नीचे की तरफ दिए गए डिलीट बटन को क्लिक करें। इस तरह आपके कैश से टैम्परेरी फाइल्स डिलीट हो जाएगी।

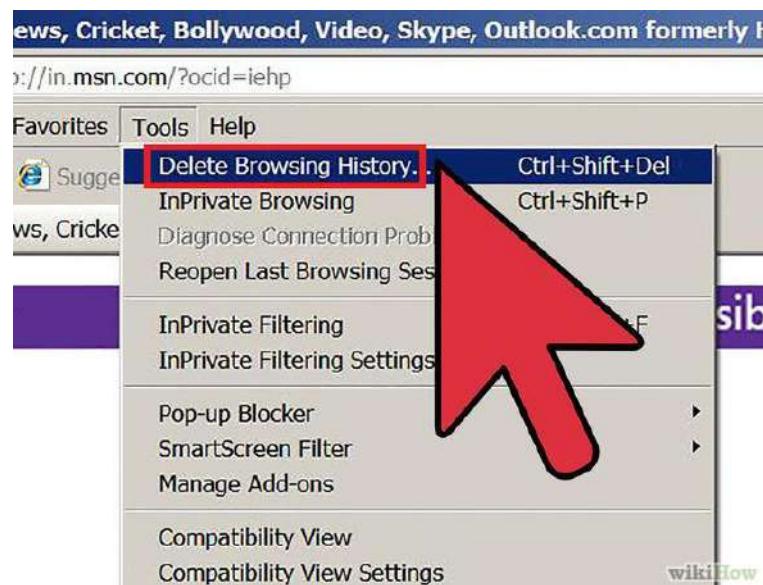


**स्टेप-4** : कम्प्यूटर कुछ क्षण के लिए ऑपरेशनल होगा और प्रोसेस पूरी हो जाएगी। अब आपने एक्सप्लोरर 9 के कैशे को क्लीअर कर दिया है।

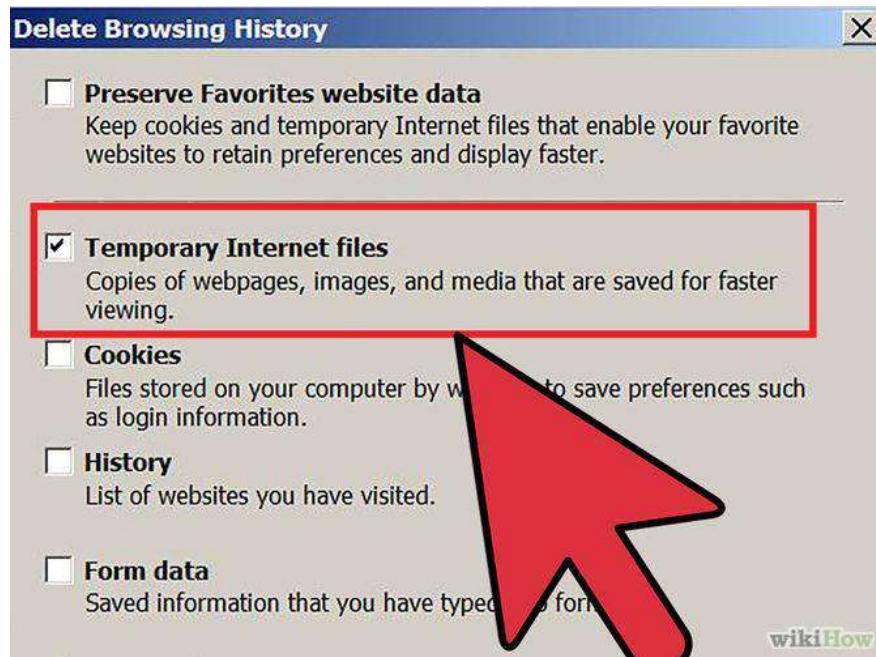
### 9.3.7 इन्टरनेट एक्सप्लोरर 8 के लिए कैशे क्लीअर करना



**स्टेप-1** : ब्राउजर ओपन करने के बाद, टूल्स मैन्यू को क्लिक करें



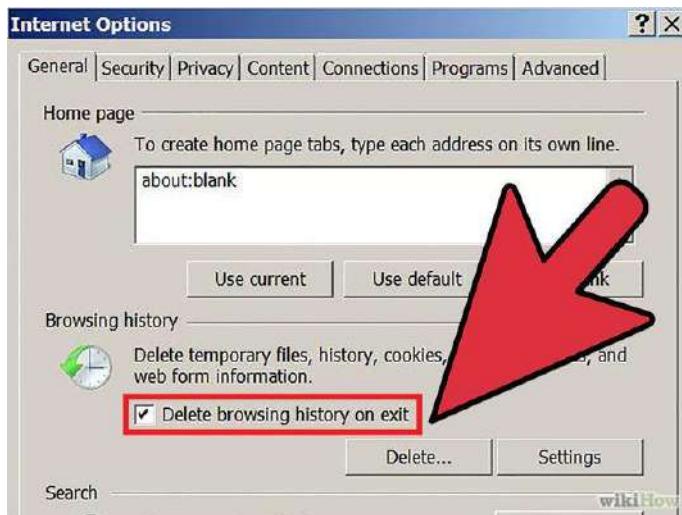
स्टेप-2 : डिलीट ब्राउजिंग हिस्ट्री पर क्लिक करें।



स्टेप-3 : टेम्परेरी इन्टरनेट फाइल्स सलेक्ट करें

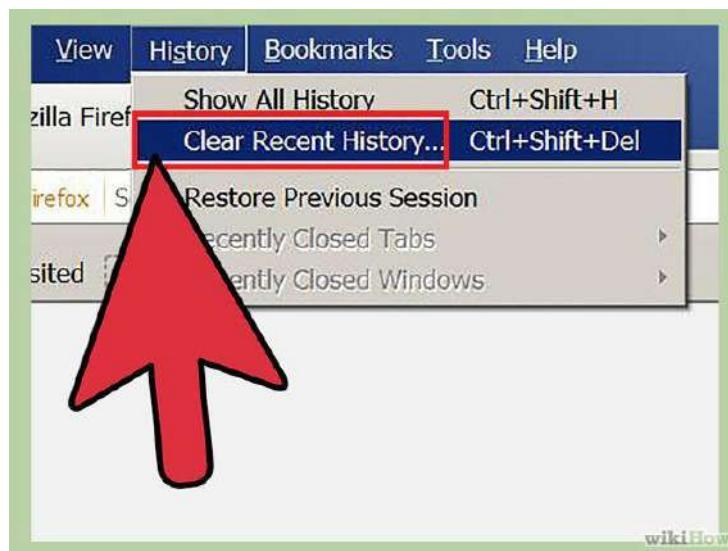


**स्टेप-4 :** विन्डो के नीचे की ओर एक डिलीट बटन किलक करें ताकि आपकी टेम्परेरी फाइल डिलीट हो जाएं (यानि आपका कैशे क्लीअर हो जाए)।

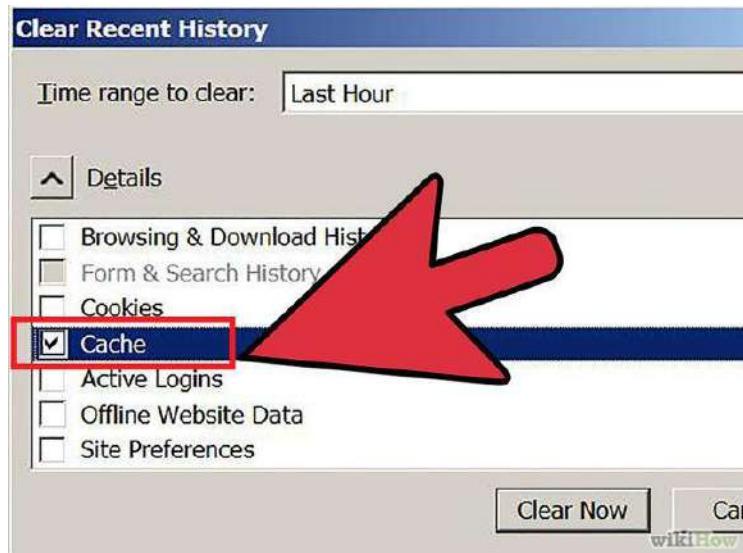


**स्टेप-5 :** जब भी आप इन्टरनेट एक्सप्लोरर क्लोज करें, आपकी टेम्परेरी फाइलें स्वतः डिलीट हो जाएं, तो इसके लिए अपने कैशे को सेट करें। “डिलीट ब्राउजिंग हिस्टी” को बंद करें, टूल्स मैन्यू से “इन्टरनेट ऑप्शन्स” सलेक्ट करें और “डिलीट ब्राउजिंग हिस्ट्री ऑन एक्जिट” चैक बॉक्स को टिक कर दें। नोट : आई ई 8 में एक फीचर है जो यदि आप “प्रीजर्व फेवरेट वेबसाइट डाटा” चैक बॉक्स को अनचैक नहीं करेंगे तो, कैशे को क्लीअर करने के बावजूद कुछ कुकीज को बनाए रखेगा। यदि पूरी तरह से कैशे क्लीअर करना चाहते हैं तो आपको इस चैक बॉक्स को अनचैक करना होगा।

### 9.3.8 फायरफॉक्स के लिए कैशे क्लीअर करना



**स्टेप-1** : फीसी पर, टॉप लेफ्ट कॉर्नर में “फायर फॉक्स” मेन्यू पर क्लिक करें। हिस्ट्री के बिल्कुल बाद बने इस चिन्ह सलेक्ट करें और “क्लीअर रीसेन्ट हिस्ट्री” पर क्लिक करें।



**स्टेप-2** : ध्यान रखें कि डिटेल्स को खोल लिया गया है, इसके लिस्ट से कैश सलेक्ट करें। शेष सभी को अनचैक कर दें।

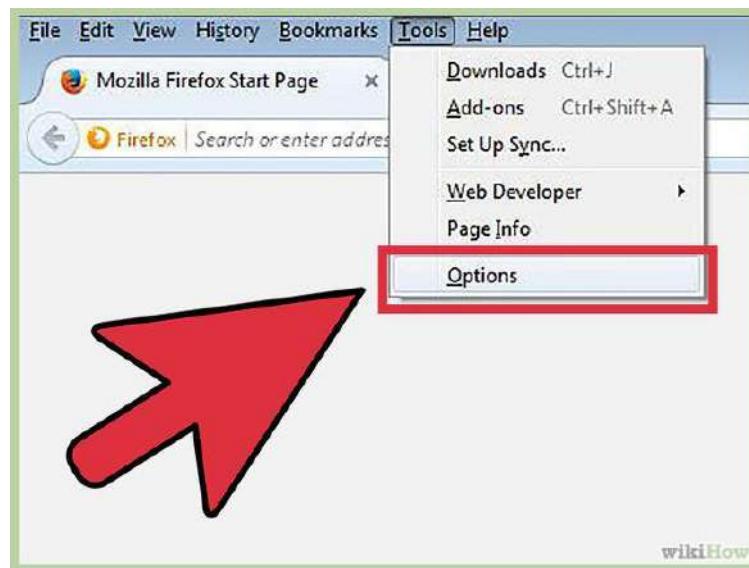


**स्टेप-3** : “टाइम रेन्ज टू क्लीअर” ड्रॉप डाउन में “एवरीथिंग” सलेक्ट करें।

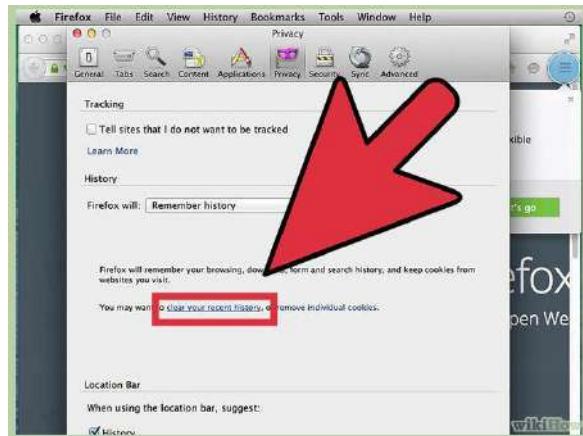


**स्टेप-4 :** “क्लीअर नाऊ” सलेक्ट करें। आपका कम्प्यूटर कुछ क्षण के लिए एविटव होगा और प्रक्रिया पूरी हो जाएगी। आपने फायर फॉक्स के कैशे क्लीअर कर दिया है।

### 9.3.9 फायरफॉक्स 33 के लिए कैशे क्लीअर करना।



**स्टेप-1 :** मेन्यू बटन (“हैम्बर्गर बटन”— तीन समानान्तर रेखाओं जैसा) क्लिक करें और ऑप्शन चूज करें।



**स्टेप-2 :** फायर फॉक्स फॉर मैक : फायर फॉक्स मेन्यू से प्रीफरेंस चूज करें और इसके बाद नीचे दिए गए अनुसार आगे बढ़ते रहें। ऑप्शन विन्डो खुलने के बाद, प्राइवेसी टैब विलक करें। हिस्ट्री एरिया में, “क्लीयर यौर रीसेन्ट हिस्ट्री” लिंक पर विलक करें।

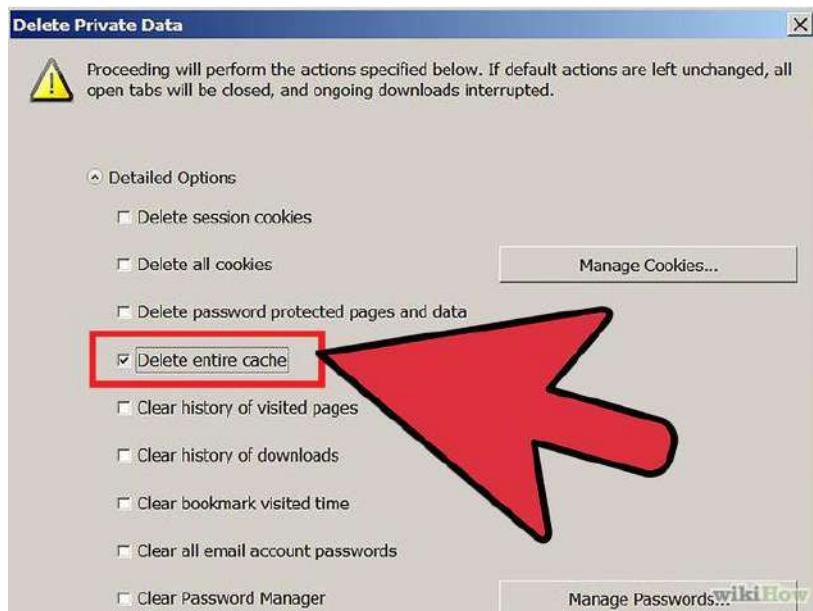


**स्टेप-3 :** यदि आप स्टोर किए गए अन्य डाटा क्लीअर करना चाहते हैं तो उनसे संबंधित बॉक्स को चेक कर दें। ये अगले स्टेप में कैश डाटा के साथ क्लीअर हो जाएंगे।

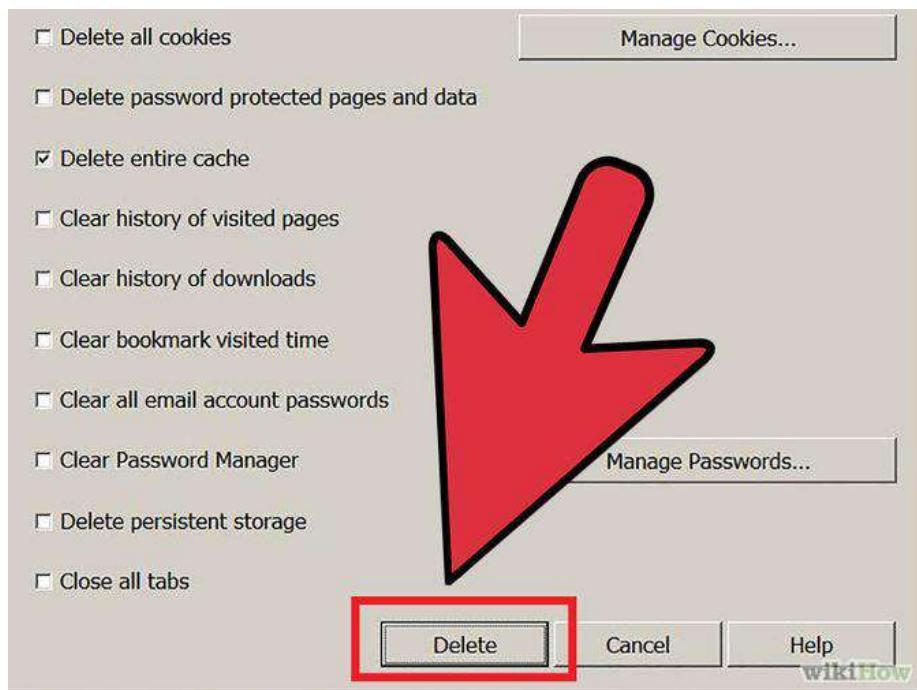
### 9.3.10 ऑपेरा के लिए कैश क्लीअर करना



**स्टेप-1 :** ब्राउजर खोलने के बाद “सेटिंग्स” मेन्यू किलक करें और “डिलीट प्राइवेट डाटा” किलक करें।

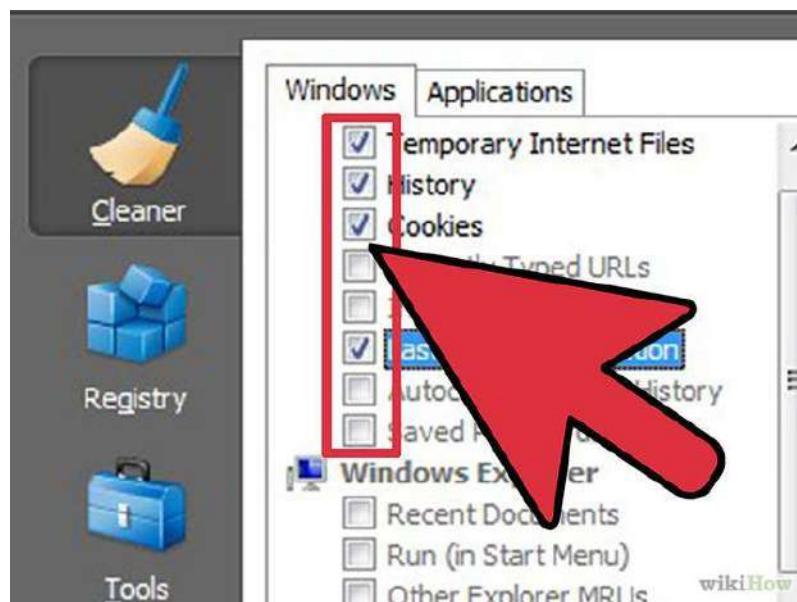


**स्टेप-2 :** ध्यान रखें कि “डिलीट एन्टायर कैशे” बॉक्स को चेक किया गया है और जिनकी जरूरत नहीं हैं, उन्हें अनचैक रखा गया है।



**स्टेप-3 :** “डिलीट” प्रेस करें।

### 9.3.11 क्लीनर के लिए कैशे क्लीअर करना



क्लीनर— यह एक कम्प्यूटर मैन्टेनेन्स टूल है जिससे आप ब्राउजर कैशे की कुकीज स्कैन और डिलीट कर सकते हैं। क्लीनर लॉच करें, क्लीनर टेब पर जाएं और अपने ब्राउजर की टेम्परेरी इन्टरनेट फाइल्स को चेक करना न भूलें।

#### अभ्यास:-

- क. अपने सिस्टम ब्राउजर पर कैशे क्लीअरिंग की प्रक्रिया निष्पादित करें।
- ख. अपने स्मार्टफोन के ब्राउजर पर कैशे क्लीअरिंग की प्रक्रिया निष्पादित करें।
- ग. अपने सिस्टम पर क्लीनर इन्स्टॉल करें और इसके द्वारा कैशे क्लीअर करें।
- घ. पता लगाए कि आपके द्वारा देखी जा रही वेबसाइट सेक्योर है या नहीं।
- ङ. क्या आप किसी ऐसे बैंक की साइट तलाश सकते हैं जो ऑफलाइन इस्तेमाल नहीं करती।
- च. क्या आप कोई ऐसी सोशल नेटवर्किंग साइट तलाश सकते हैं जो ऑफलाइन इस्तेमाल नहीं करती।
- छ. आनलॉइन शापिंग करने के लिए किन महत्वपूर्ण बातों को ध्यान में रखना चाहिए।

# वायरलैस सिक्यूरिटी

इस चैप्टर (अध्याय) में हम आपको अलग बेहतरीन तौर-तरीकों के बारे में बताएंगे। आप इन्हें वायरलैस लैन इस्तेमाल करते समय अपनाएं।

## 10.1 वायरलैस लैन क्या है?

आजकल कम्प्यूटर जैसे उपकरणों को वायरलैस लैन अथवा डब्ल्यू-लैन से कनेक्ट करके इन्टरनेट सेवा का लाभ लेना लोकप्रिय होता जा रहा है। वायर्ड लैन (लोकल एरिया नेटवर्क) की जगह अब वायरलैस लैन लेता जा रहा है। अलग-अलग उपकरणों को कनेक्ट करने की सहूलियत ने इसे किफायती बना दिया है और इसका रख-रखाव भी आसान है। विकीपीडिया के अनुसार, वायरलैस लैन के लोकप्रिय होने का एक कारण इसका इंस्टालेशन आसान होना है। साथ ही, बहुधा ये अपने कस्टमर को मुफ्त वायरलैस एक्सेस की पेशकश भी करते हैं।

डब्ल्यूलैन के लोकप्रिय होने के कुछ कारण इस प्रकार हैं:-

1. एक दूसरे के साथ कनेक्ट होने के लिए केबल आदि जैसे किसी अन्य माध्यम की आवश्यकता नहीं है। आप अपने ऑफिस परिसर घर या इसके पास निश्चिंत होकर घूम सकते हैं और कनेक्शन भी बरकरार रहेगा।
2. डब्ल्यूलैन किफायती होते हैं। कार्यालयों होटलों आदि में केबल बिछाने की जरूरत नहीं होती। इसलिए यह सस्ता है और सेवा गुणवत्ता भी वायर्ड लैन जैसी है।
3. वहाँ भी पहुँच सकता है, जहाँ केबल विछाना मुश्किल हो। डब्ल्यूलैन के सिग्नल, एयरपोर्ट जैसे बड़े प्रतिष्ठानों तक पहुँच सकते हैं। बस आपको, एक्सेस प्वाइन्ट (एपी) डिवाइस इन्स्टॉल करना होता है।
4. केबल वाले नेटवर्क की तुलना में व्यवधान कम है और यदि कोई व्यवधान आता है तो इसे दूर करना भी आसान होता है।
5. ज्यादा सैक्योर है क्योंकि ज्यादातर एपी बेर्स्ट एन्क्रिप्शन पद्धतियों से युक्त होते हैं जो इन्हें स्निफिंग और अन्य सायबर हमलों से सुरक्षित रखते हैं।



**चित्र 44 वायरलैस नेटवर्क**

## 10.2 डब्ल्यूलैन के साथ प्रमुख समस्याएं

डब्ल्यूलैन की अपनी विशेषताएं हैं, लेकिन वायर्ड लैन की तरह डब्ल्यूलैन भी सायबर हमलों का निशाना बन सकता है। वायर्ड लैन की तुलना में डब्ल्यू लैन को हैक करना ज्यादा आसान है। यदि इसे ठीक से कन्फिगर नहीं किया गया, तो प्रतिष्ठानों के आस-पास अपनी आसान पहुँच के कारण, इन्हें ज्यादा निशाना बनाया जाता है। इसे हैक करने के लिए केबल कनेक्शन की जरूरत नहीं है, इसलिए इसे कहीं से भी हैक किया जा सकता है। यदि ठीक से कन्फिगर नहीं किया गया तो इसकी सहूलियत वाली खूबी कम्पनी के लिए बड़ा जोखिम बन सकती है। जिन बड़े हमलों का यह शिकार बन सकता है, उनमें रिनफिंग, की क्रेकिंग, डिनायल ऑफ सर्विस (डीओएस), डिअथान्टिकेशन अटैक, वार ड्राइविंग आदि शामिल है। इस चैप्टर में हम इन सायबर अटैक पर चर्चा करने की बजाय उन तौर तरीकों पर चर्चा करेंगे, जो उपरोक्त अनेक हमलों को रोक सकते हैं। इनम से एक है, डब्ल्यू लैन कैसे इन्टर्टॉल और सुरक्षित तरीके से यूज करें।

### 10.2.1. सैक्योर डब्ल्यू लैन

वायरलैस सिक्यूरिटी मुख्यतया इन तीन फैक्टर्स पर निर्भर करती है:-

- एनक्रिप्शन का इस्तेमाल करके आपके वायरलैस को कितना सैक्योर बनाया गया है।
- संदेहजनक और असाधारण कार्यकलापों की निगरानी।
- यूजर जागरूकता और शिक्षा।

इसमें कारपोरेट और होम नेटवर्क के लिए विभिन्न तरीकों को शामिल किया गया है। यह यूजर्स को यह भी बताते हैं कि सेफ सर्फिंग कैस करें।

### 10.2.2 वाई-फाई एट होम

घर में वाई-फाई का उपयोग अब शान-शौकत को चीज नहीं बल्कि एक जरूरत बन गया है। लेकिन, जब सुरक्षा का प्रश्न उठता है, सबसे पहला विचार हमारे मन में यह आता है कि जिस चीज को आप देख नहीं सकते, महसूस नहीं कर सकते, उसे बचायेंगे कैसे। वायर्ड नेटवर्क्स की तुलना में वायरलैस नेटवर्क की घर में सुरक्षा एक बिल्कुल ही अलग मुद्दा है। ज्यादातर वायरलैस नेटवर्क डिवाइस वैन्डर और इन्टरनेट सर्विस प्रोवाइडर कोई स्वतः सुरक्षा सैटिंग्स उपलब्ध नहीं कराते हैं, वह कस्टमर पर ही सब कुछ छोड़ देते हैं। इसलिए आपको ही यह सुनिश्चित करना है कि आपके नेटवर्क का कोई गलत उपयोग न कर पाए। ऐसी कोई रामबाण दवा नहीं है जो आपके वायरलैस नेटवर्क के इनक्रास्ट्रक्चर को सुरक्षित बना सके। लेकिन, नीचे कुछ ऐसे सुरक्षा उपाय दिए गए हैं जिन्हें एक दूसरे से जोड़ कर आप अपने वायरलैस नेटवर्क को काफी कुछ सुरक्षित बना सकते हैं।

### 1. सबसे ज्यादा सैक्योर एनक्रिप्शन का उपयोग करने:-

सबसे पहला और सबसे अधिक जरूरी कदम है— इन्डस्ट्री स्टैन्डर्ड के एनक्रिप्शन यूज करें। पुरानी डब्ल्यू ईपी-वायर्ड इक्वीवैलेन्ट प्राइवेसी (आमतौर पर यही यूज होती है) का तोड़ निकाल लिया गया है। आप चाहे जितना जटिल पासवर्ड यूज करें इसे मिनटों में क्रैक और डिक्रिप्ट किया जा सकता है। डब्ल्यूईपी, चैनल एनक्रिप्ट करने के लिए 40 बिट अथवा 128 बिट्स आरसी 4 साइफर का इस्तेमाल किया जाता है।

इसके बजाय डब्ल्यूपीए2-वाई-फाई प्रोटोकोल एक्सेस-2 जैसे प्रोटोकाल का इस्तेमाल करें, जो 128 बिट्स ईएस साइफर्स का इस्तेमाल करता है, जिसे अपेक्षाकृत ज्यादा स्ट्रॉग एन्क्रिप्शन प्रोग्राम माना जाता है।

(यह डब्ल्यूईपी की क्रेकिंग, स्निकिंग, कैचरिंग/इवेसड्रॉपिंग (चोरी छुपे सुनना) जैसे हमलों से सुरक्षा प्रदान करता है।)

### 2. फायरवॉल का इस्तेमाल करें:-

सभी वायरलैस राउटर्स में इनबिल्ट फायरवॉल होती है। सभी सिक्योरिटी फीचर्स के साथ इसे इनेबल करें। अज्ञात सोर्स से प्राप्त पिंग रिकवरेस्ट को ब्लॉक करें और यदि जरूरी हो तो, वेबसाइट ब्राउजिंग पर रोक लगाएं। सुरक्षा हेतु और भी नीतियां तय करें और उन्हें लागू करें।

(फिंगर प्रिंटिंग, सिस्टम कम्प्रोमाइज जैसे हमलों को रोक सकता है।)

### 3. निगरानी सिस्टम बनाएं:-

एक कहावत है— प्रीवेन्शन इस बैटर दैन क्योर। यदि आपको किसी संदेहजनक एक्विटिटी का पता लगता है, इससे पहले कि यह आपके नेटवर्क में सेंध लगाए, इसे ब्लॉक कर दें या सुरक्षात्मक कदम उठाएं। संदेहजनक एक्टीविटीज की निगरानी के लिए डब्ल्यूआईपीएस/डब्ल्यूआईडीएस डिप्लॉय करें।

(यह स्वैनिंग और डीओएस जैसे हमलों से सुरक्षा देता है।)

#### **4. डिफाल्ट क्रेडेन्शियल यूज न करें:-**

हर एक वायरलैस राउटर में डिफॉल्ट यूजर नेम/पासवर्ड होता है। कई बार लोग इन्हें नहीं बदलते हैं और लम्बे समय तक इनका इस्तेमाल करते हैं। कम्प्यूटर और अन्य उपकरण वायरलैस राउटर से कनेक्ट होने के लिए यूजरनेम/पासवर्ड का उपयोग करते हैं। यदि कोई हैकर इसका पता लगा ले, तो वह आपको नेटवर्क से आसानी से कनेक्ट हो सकता है। अध्ययनों से पता चला है कि अधिकांश यूजर मैन्यूफैक्चर (बनाने वाली कम्पनी) द्वारा सेट यूजरनेम/पासवर्ड का कार्बिनेशन ही इसमेंाल करते रहते हैं। कुछ डिफॉल्ट यूजरनेम कार्बिनेशन इस प्रकार हैं:- एडमिन/एडमिन, एडमिन/पासवर्ड या एडमिन//”

(अनाधिकृत एक्सेस और वार ड्राइविंग को रोक सकता है।)

#### **5. ऑटो-कनेक्ट फीचर डिसेबल कर दें:-**

कुछ उपकरण अथवा कम्प्यूटर/लैपटॉप उपलब्ध नेटवर्क से स्वतः कनेक्ट हो जाते हैं यानि वे अपने इनबिल्ट टूल के जरिए आपके नेटवर्क को मैनेज करने लगते हैं। ऑटो-कनेक्ट फीचर को ऑन रखने वाले यूजर फिशिंग अटैक या मैलिसियस एपी अटैक का शिकार बन सकते हैं। अटैकर्स अपने एपी एलाइव और एविटव रखते हैं, ताकि ऐसे भोले-भाले यूजर्स को खोज सकें। वे ट्रैप में लेने के लिए “हॉट स्पॉट”, सेक्यार कनेक्ट, गवर्नमेंट नेटवर्क जैसे आकर्षक नामों का इस्तेमाल करते हैं। यूजर इन पर शक नहीं करता और मजे से वायरलैस नेटवर्क सर्फ करता रहता है। साथ ही, यदि आपने अपने राउटर का डिफॉल्ट पासवर्ड नहीं बदला है तो अटैकर इस फीचर को अपनी मशीन पर यूज करेगा और आपके डिफॉल्ट पासवर्ड का अनुमान लगाकर आसानी से आपके नेटवर्क पर कनेक्ट हो जाएगा।

(फिशिंग, स्निकिंग, रोग एपी अटैक को कम किया जा सकता है।)

#### **6. सेन्सिटिव वेबसाइट्स सर्फ करने के लिए पब्लिक वाई-फाई स्पॉट्स का उपयोग न करें:-**

एयरपोर्ट्स, कैफे रेलवे स्टेशन आदि पर उपलब्ध फ्री और ओपन वायरलैस नेटवर्क सुरक्षित नहीं हैं। ये आपके लैटटॉप और राउटर के बीच कनेक्शन को एन्क्रिप्ट नहीं करते हैं और चैनल सर्फ करना सुरक्षित नहीं बनाते हैं। अतः आपके लैपटॉप/स्मार्ट फोन से कोई भी इन्फार्मेशन जो बाई डिफाल्ट औजजचेरुळ्ळ पर नहीं जा रही है, स्निफ की जा सकती है, यहीं नहीं आपका सेशन भी हाइजैक किया जा सकता है, क्योंकि अनइनक्रिप्टेड चैनल आपकी वेबसाइट द्वारा यूज की गई एटिक्व सेशन आईडी को लीक कर सकता है। इस प्रकार के अटैक्स को दर्शाने के लिए, हाल ही में एक शोधकर्ता ने फायरशीप नाम का एक टूल :ीजजचरुळ्ळबवकवइनजसमतण्डजीनझण बवजीसवर्मोममचसद्व डेवलप किया है। अटैकर को बस इतना ही करना है कि वह इस टूल को फायरफॉक्स पर इन्स्टॉल करेगा और पब्लिक अनएनक्रिप्टेड वाई-फाई पर कम्प्यूनिकेशन स्निफ करना शुरू कर देगा। फेस बुक जैसी कुछ एप्लीकेशन्स लॉगिन पेज :ीजजचेद्व को एनक्रिप्ट करता है लेकिन

इनटरनल पेजों को अनएनक्रिप्टेड रीजजचद्व ही सर्व करता है इसलिए आप की सेशन आईडी लीक हो सकती है।

(सेशन हाईजैकिंग, स्निफिंग जसे अटैक कम किए जा सकते हैं।)

#### 7. डिफॉल्ट एसएसआईडी बदलें:-

हालांकि इससे आप हैकर्स को अपने नेटवर्क में सेंध लगाने से नहीं रोक पाएंगे। लेकिन डिफॉल्ट एसएसआईडी को यूज करना, इस बात का संकेत है कि यूजर लापरवाह है। इसलिए इसके बारे में और जानकारी हासिल की जा सकती है और यह पता लगाया जा सकता है कि क्या वह डिफॉल्ट पासवर्ड भी यूज कर रहा है?

(वार ड्राइविंग के अटैक को कम किया जा सकता है।)

#### 8. स्टैटिक आईपी एड्रेस देकर और एमएससी फिल्टरिंग का उपयोग करके एक्सेस सीमित करें:-

आटोमेटिक आईपी एसाइनिंग फीचर को बंद कर दें और आप जिस डिवाइस को कनेक्ट करना चाहते हैं, उसके लिए प्राइवेट स्टैटिक आईपी यूज करें। इससे आपको अवांछित डिवाइसेज के आपके नेटवर्क से कनेक्ट होने को रोकने में मदद मिलेगी। साथ ही एमएससी फिल्टरिंग को इनेबाल कर दें— राउटर उससे कनेक्ट प्रत्येक डिवाइस का एमएससी याद रखता है और इसे अपनी लिस्ट में सेव कर लेता है। आप एक्सेस रोकने के लिए इस सुविधा का इस्तेमाल कर सकते हैं और केवल भरोसेमंद डिवाइस ही कनेक्ट हो सकते हैं। लेकिन एमएससी स्नूफिंग की सम्भावना अभी भी मौजूद है यानि अभी भी आपको अपने वायरलैस नेटवर्क की सुरक्षा के लिए और उपाय करने हैं।

#### 9. जब यूज में न हो, राउटर ऑफ कर दें:-

यह अन्तिम उपाय जरूर है, पर यह भी पर्याप्त नहीं है। लेकिन, निश्चय ही, यह राउटर ऑफ रहने के दौरान आपके नेटवर्क को सभी तरह के हमलों से बचाएगा।

##### 1.7.2.3 कारपोरेट / एन्टरप्राइज नेटवर्क में वाई-फाई:-

इन प्रतिष्ठानों के कार्यकलापों और इन्फॉर्मेशन की अहमियत को देखते हुए, यह अत्यन्त महत्वपूर्ण है कि कारपोरेट / एन्टरप्राइजेज के नेटवर्क में सुरक्षा के और ज्यादा उपाय किए जाएं।

#### निम्नलिखित पर ध्यान देना बेहतर होगा:-

- पूरे आर्गेनेलशन के लिए वायरलेस नेटवर्क के मामले में एक व्यापक सुरक्षा नीति और प्रोसीजर तय करें।
- एसएसआईडी को संगठन, एपी वेन्डर या किसी अन्य संबंधित इन्फार्मेशन, जिसे आसानी से गैस (अनुमान) किया जा सकता हो या वर्तमान संगठन से एसोसिएट किया जा सकता हो, से सहयोगित (एसोशिएट) न करें।

- रेडियस अथॉन्टिकेशन (प्रमाणीकरण) के साथ डब्ल्यूएपी2 एन्टरप्राइज एनक्रिप्शन इनेबल करें और साथ ही ईएपी—ओटीएलएस, टीएलएस आदि जैसे ईएपी प्रोटोकोल यूज करें।
- सर्वर से क्लाइन्ट और क्लाइन्ट से सर्वर के अथॉन्टिकेशन के लिए सीए हस्ताक्षरित प्रमाणपत्र और पीके आई इन्फ्रास्ट्रक्चर का क्रियान्वयन अनिवार्य बनाएं।
- एमएसी एड्रेस जैसे यूनिक आइडेन्टिफायर के आधार पर क्लाइन्ट फ़िल्टरिंग।
- अलग से गेस्ट नेटवर्क स्थापित करें जिसका कारपोरेट नेटवर्क के साथ कोई इन्टरफ़ेस/कनेक्शन न हो।
- एपी के पावर आउटपुट को कम करके वाई—फाई नेट वर्क का दायरा (रेडियस) कम करें।
- पूरी तरह से सत्यापन के बाद ही कर्मचारी और गेस्ट मशीनों को आईपी एड्रेस एलॉट करें।
- की और पासवर्ड समय—समय पर बदलते रहें।
- पब्लिक वाई—फाई नेटवर्क से कारपोरेट इन्फॉर्मेशन एक्सेस करते समय वीपीएन का इस्तेमाल करें।
- डिकैफिएण्ट आइडीस्कैन जैसी क्लाइन्ट साइड यूटिलिटिज एआरपी टेबल में बदलाव का पता लगाने में मदद और होल 196 तथा डीओएस जैसे हमलों से बचाने के लिए जन—सामान्य की आईडी के तौर पर काम कर सकती है।
- वायरलेस आईडी इम्प्लीमेंट करें। वायरलैस आईडी एक नई अवधारणा है। वायरलेस आईडी की प्रमुख विशेषताएं इस प्रकार हैं:—
  - रोग (फ्रॉड) एपी की रोकथाम
  - डीओएस अटैक का पता लगाना और रोकना।
  - अटैकर की प्रत्यक्ष लोकेशन खोजने में मददगार।
  - वायरलेस नेटवर्क के बारे में संगठन की सूचना सुरक्षा लागू करने में सहायक।
  - किस्मेट और नेटस्लम्बर जैसे स्कैनिंग टूल्स के यूज पर नजर रखना।

## अभ्यास

1. पब्लिक प्लेस पर वाई—फाई नेटवर्क के इस्तेमाल में कौन सी सावधानियां बरतें।
2. होम नेटवर्क को कैसे सुरक्षित बनाएं?
3. एन्टरप्राइज नेटवर्क को कैसे सुरक्षित बनाएं।

4. इन्टर नेट पर निम्नलिखित शब्दों के बारे में ओर जानकारी हासिल करें।

- आईडीएस
- डीओएस
- किस्मेट
- नेट स्लम्बर

-□-

## ईमेल और सोशल मीडिया सिक्यूरिटी

### 11.1 सोशल नेटवर्किंग साइट्स पर सेफ बाउजिंग के दिशा निर्देश<sup>12</sup>:-

इन्टरनेट के उद्भव के साथ ही ऑन-लाइन समुदाय भी अस्तित्व में आ गया है। पहले बुलेटिन बोर्ड, ईमेल लिस्ट ने दुनियाँ के लोगों को आपस में सम्पर्क करने, बातचीत करने और किसी खास विषय पर जानकारी साझा करने के अवसर प्रदान किए। आज, सोशल नेटवर्किंग साइट्स का इतना अधिक विस्तार हो गया है कि ये लोगों को मैसेज, पिक्चर, फाइल्स, यहाँ तक कि आप क्या कर रहे हैं, कहाँ हैं, इसकी भी मिनट-दर-मिनट जानकारी उपलब्ध कराने की सहायता प्रदान कर रही है। ये फंक्शन कोई नए या अद्भुत नहीं हैं— इनमें से कोई भी एक्शन, बिना किसी सोशल नेटवर्किंग साइट में शामिल हुए बिना भी इन्टरनेट के जरिए निष्पादित किए जा सकते हैं।

हालांकि, ये नेटवर्क काफी उपयोगी हो सकते हैं, और ऑफलाइन तथा ऑफलाइन दोनों ही रूप में सोशल-सम्पर्क को बढ़ावा देते हैं लेकिन, इनका इस्तेमाल करके, कहीं हम सूचनाएं ऐसे लोगों को तो उपलब्ध नहीं करा रहे हैं, जो इनका दुरुपयोग कर सकते हैं, इस पर भी ध्यान देना जरूरी है। आप इसके, कुछ इस तरह समझिये, सोशल नेटवर्किंग साइट एक विशाल आयोजन की तरह है। इस आयोजन में आप कुछ लोगों को जानते हैं और कुछ ऐसे भी हैं, जिन्हें आप बिलकुल नहीं जानते। अब कल्पना कीजिए कि इस विशाल आयोजन में आप क्या साच रहे हैं, इसका हर पल का ब्यौरा, अपना सारा व्यक्तिगत विवरण एक बिलबोर्ड पर लिख कर अपनी पीठ पर लटकाए धूम रहे हैं, और हर कोई इसे पढ़ेगा तथा आपको पता भी नहीं चलेगा। क्या आप ऐसा होने देना चाहेंगे? ध्यान रखिए! सोशल नेटवर्किंग साइट के मालिक बड़े कारोबारी घराने होते हैं और ये घराने लोगों के बारे में डाटा (जानकारी) जुटा कर और इन डाटा को अन्य विज्ञापनदाताओं को बेच कर पैसा बनाते हैं। जब आप किसी सोशल नेटवर्किंग साइट में प्रवेश करते हैं तो समझ जाइए कि आप इन्टरनेट की आजादी को पीछे छोड़कर एक ऐसे नेटवर्क में प्रवेश कर रहे हैं, जिसका नियंत्रण उस साइट के मालिक के हाथ में है। प्राइवेसी सैटिंग्स आप के डाटा को केवल उस सोशल नेटवर्क के अन्य सदस्यों से बचाती हैं, लेकिन साइट के मालिक से नहीं। दरअसल, आप अपना सारा डाटा उस मालिक को सौंप रहे हैं और उस पर भरोसा कर रहे हैं।

यदि आपका कार्य संवेदनशील सूचना और विषयों से जुड़ा है तथा आप सोशल नेटवर्किंग साइट्स का इस्तेमाल करना पसंद करते हैं, तो आपको अपने कार्यों की प्राइवेसी और सुरक्षा के मुद्दों के बारे में बहुत सजग रहना होगा। मानव अधिकारों के समर्थक खासतौर पर सोशल नेटवर्किंग साइट्स के खतरों का

<sup>12</sup> <https://securityinabox.org/en/guide/social-networking>

निशाना बन सकते हैं और उन्हें अपने बारे में तथा जिनके साथ मिलकर वे काम करते हैं, उनके बारे में सूचनाएं साझा करने में बहुत ज्यादा सजग रहना चाहिए।

किसी खास नेटवर्किंग साइट का इस्तेमाल करने से पहले यह जानना बहुत जरूरी है कि ये साइट्स किस प्रकार आपको असुरक्षित बनाती हैं। और इसी को ध्यान में रखकर स्वयं को और जिन लोगों के साथ आप काम करते हो, उनको सुरक्षित बनाने के लिए कदम उठाएं। यहां दिए गए कुछ दिशा-निर्देश सोशल नेटवर्किंग साइट्स यूज करने के सुरक्षा-दुष्परिणामों को समझने में आपकी सहायता करेंगे।

### 11.1.1 सोशल नेटवर्किंग साइट्स सुरक्षित रूप से यूज करने के सामान्य सुझावः—

सोशल मीडिया हमारे जीवन का एक प्रत्यक्ष अंग बन चुका है। हम अपने अपडेट अपने दोस्तों, परिजनों और सोशल मीडिया का इस्तेमाल करने वालों के साथ साझा करते हैं। लेकिन हैकर्स महत्वपूर्ण डाटा चुराने और आपका एकाउन्ट हैक करने के लिए इस इन्फॉर्मेशन का इस्तेमाल कर सकते हैं। सोशल मीडिया इस्तेमाल करने के बारे में कुछ सामान्य सुझाव नीचे दिए गए हैं:-

#### झ विचार करें:-

- मेरी ऑनलाइन जानकारी कौन एक्सेस कर सकता है?
- सोशल नेटवर्क साइट्स पर मेरी इन्फॉर्मेशन किसके नियंत्रण में है?
- मेरे बारे में मेरे कॉन्टेक्ट्स कौन सी सूचनाएं अन्य लोगों को दे रहे हैं?
- यदि मैं अपने कॉन्टेक्ट्स की इन्फॉर्मेशन अन्य लोगों से शेयर करूं, तो क्या वे बुरा मानेंगे?
- मैं जिनसे कनेक्टेड हूँ क्या सब भरोसे लायक हैं?

झ सोशल नेटवर्क्स एक्सेस करने के लिए हमेशा सेक्योर पासवर्ड का इस्तेमाल करें। यदि कोई अन्य व्यक्ति आपके एकाउन्ट को एक्सेस कर लेगा तो यह आपकी ही नहीं बल्कि आपके कॉन्टेक्ट्स की भी सोशल नेटवर्क के जरिए इन्फॉर्मेशन एक्सेस कर लेगा। समय-समय पर पासवर्ड बदलना, अपनी आदत बना लें।

झ सोशल नेटवर्किंग साइट्स की डिफॉल्ट प्राइवेसी सैटिंग्स तथा उन्हें बदलने की प्रक्रिया अवश्य समझ लें। झ अलग-अलग अभियानों और एकिटविटीज के लिए, हो सके तो अलग-अलग एकाउन्ट/आइडेन्टिटी अथवा अलग-अलग छद्म नाम का उपयोग करें। नेटवर्क का सुरक्षित रूप से इस्तेमाल करना है तो आप में इस नेटवर्क के सदस्यों की विश्वसनीयता को परखने की क्षमता होनी चाहिए। अलग-अलग एकाउन्ट के जरिए सदस्यों की विश्वसनीयता का पता लगाना अच्छा तरीका है।

- पब्लिक इन्टरनेट पर अपना सोशल नेटवर्क एक्सेस करते समय सजग रहें। पब्लिक मशीन (सायबर कैफे आदि) में इन्टरनेट इस्तेमाल करने के बाद अपना पासवर्ड और ब्राउजिंग हिस्ट्री डिलीट कर दें।
- अपने यूजरनेम, पासवर्ड और पोस्ट की गई अपनी इन्फॉर्मेशन की सुरक्षा के लिए ऑजजचरूङ्घ सोशल नेटवर्किंग साइट्स ही एक्सेस करें। ऑजजचरूङ्घ की बजाय ऑजजचरूङ्घ का इस्तेमाल करके आप अपने ब्राउजर से नेटवर्किंग साइट को जाने वाले ट्रैफिक के एनक्रिप्शन द्वारा सुरक्षा की एक और परत जोड़ रहे हैं।
- भले ही आप अपने नेटवर्क में शामिल लोगों पर भरोसा करते हों, अपने स्टेट्स अपडेट में ज्यादा जानकारी देने से बचें। कोई भी आपकी इन्फॉर्मेशन कॉपी कर सकता है।
- ज्यादातर सोशल नेटवर्क्स आपको अपनी इन्फॉर्मेशन दूसरे सोशल नेटवर्क्स से जोड़ने से नहीं रोकते। उदाहरण के लिए, आप अपने टिवटर एकाउन्ट पर कोई अपडेट पोस्ट कर सकते हैं और इसे ऑटोमेटिकली फेसबुक एकाउन्ट पर पोस्ट करवा सकते हैं। अपने सोशल नेटवर्क्स एकाउन्ट इन्टीग्रेट करते समय सावधान रहें। हो सकता है कि एक साइट पर आप एनोनिमस हों और दूसरे पर नहीं।
- सोशल नेटवर्किंग साइट पर आपका कन्टेन्ट कितना सुरक्षित है, इस बारे में सावधान रहें। अपने कन्टेन्ट अथवा इन्फॉर्मेशन के लिए प्राइमरी होस्ट के रूप में किसी एक सोशल नेटवर्किंग साइट पर ही निर्भर न रहें।
- यदि सरकार को अचानक यह पता लगे कि उस वेबसाइट के कन्टेन्ट आपत्तिजनक हैं तो वह अपने राज्य की सीमा में उस साइट की पहुंच ब्लॉक कर सकती है। सोशल नेटवर्किंग साइट का एडमिनिस्ट्रेटर भी उस देश में सेंशरशिप झेलने के बजाय आपत्तिजनक विषय वस्तु (कन्टेन्ट) को हटाने का निर्णय ले सकता है।

### **11.1.2 व्यक्तिगत विवरण पोस्ट करना:-**

सोशल नेटवर्किंग साइट्स आपसे आपके बारे में काफी—कुछ डाटा लेना चाहती है ताकि अन्य यूजरों को आपको खोजकर आपसे जुड़ने में आसानी हो। और यूजर्स के लिए आइडैन्टिटी चोरी का यही सबसे बड़ा कारण बन सकता है। और यह खतरा धीरे—धीरे आम होता जा रहा है। इसके अलावा, जितना ज्यादा आप अपने बारे में खुलासा करेंगे, उतना ही अर्थारिटीज को आपको पहचानना और आपकी निगरानी करना आसान हो जाएगा। कुछ अन्य देशों में बसे प्रवासी एकिटविस्ट की ऑनलाइन गतिविधियों के चलते मूल देश में रहने वाले उनके परिवार के सदस्यों को अर्थारिटीज ने टारगेट किया है।

#### **स्वयं से पूछें:-**

क्या निम्नलिखित सूचना ऑनलाइन पोस्ट करना जरूरी है?

- जन्मतिथि
- सम्पर्क के लिए फोन नम्बर
- पता
- परिवार के सदस्यों का व्यौरा
- यौनाकर्षण
- शिक्षा और रोजगार का विवरण

### **11.1.3 फ्रेन्ड्स, फॉलोअर्स एण्ड कॉन्टेक्ट्सः—**

किसी भी सोशल नेटवर्किंग साइट पर अपनी पर्सनल डिटेल फिल करने के बाद, सबसे पहले आप अन्य लोगों से सम्पर्क स्थापित करते हैं। निश्चय ही ये वो लोग होते हैं, जिन्हें आप जानते हैं और भरोसा करते हैं, लेकिन आप उस ऑनलॉइन कम्यूनिटी के सम्पर्क में भी आते हैं, जिनकी सोच आप जैसी है, पर आप उनसे कभी मिले नहीं। अब सबसे महत्वपूर्ण यह है कि इस ऑनलाइन कम्यूनिटी के साथ कौन सी इन्फॉर्मेशन साझा करने जा रहे हैं। जब आप फेसबुक जैसे सोशल नेटवर्क, जहाँ आपके बारे में काफी कुछ इन्फॉर्मेशन मौजूद है, का इस्तेमाल करते हैं, तो ध्यान रखें कि आप उन्हीं लोगों से सम्पर्क करें, जिन्हें आप जानते हैं, और जिन पर आपका भरोसा है कि आपके द्वारा पोस्ट की गई इन्फॉर्मेशन का वे दुरुपयोग नहीं करेंगे।

### **11.1.4 स्टेट्स अपडेट्सः—**

ट्रिवटर और फेसबुक तथा ऐसे ही नेटवर्क्स पर, स्टेट्स अपडेट में प्रश्न के उत्तर के रूप में होते हैं, जैसे— मैं फिलहाल क्या कर रहा हूँ? क्या चल रहा है? अपडेट के बारे में सबसे महत्वपूर्ण बात यह समझनी है कि इन अपडेट्स को वास्तव में कौन देख सकता है। ज्यादातर स्पेशल नेटवर्किंग एप्लीकेशन्स में स्टेट्स अपडेट की डिफॉल्ट सैटिंग्स के अनुसार इन्टरनेट पर इन्हें कोई भी देख सकता है। यदि आप चाहते हैं कि केवल आपके कान्टेक्ट्स ही इन्हें देख पाएं तो आपको सोशल नेटवर्किंग एप्लीकेशन को बताना होगा कि अपडेट्स को अन्य लोगों से छिपा कर रखें। ट्रिवटर में ऐसा करने के लिए, “प्रोटेक्ट योर ट्रीट्स” पर जाएं। फेसबुक में, सैटिंग्स में बदलाव करें और अपने अपडेट्स शेयर करने के लिए “फ्रेन्ड्स ऑनली” विकल्प चुनें। ये सैटिंग्स अपनाने के बाद भी इस सम्भावना पर ध्यान दें कि आपकी इन्फॉर्मेशन फॉलोअर्स और फ्रेन्ड्स द्वारा शेयर करना या रीपोस्ट करना कितना आसान है। अपने नेटवर्क फ्रेन्ड्स के साथ एक साझा एप्रोच पर सहमति बनाए कि आपके सोशल नेटवर्किंग एकाउन्ट में कौन सी इन्फॉर्मेशन दी जाएगी।

आप इस पर भी विचार करें कि आप अपने फ्रैन्ड्स के बारे में जो जानकारी खुलासा कर रहे हैं, वह उन्हें पसन्द न आए। इसलिए इस बारे में संवेदी बनें। तभी दूसरों को भी अपने बारे में संवेदी बना सकेंगे।

ऐसे कई दृष्टांत हैं जिनमें स्टेट्स अपडेट में दो गई जानकारी का उन लोगों के खिलाफ इस्तेमाल हुआ है। अमरीका में कई अध्यापकों को बर्खास्त कर दिया गया था और इसका कारण था— वे अपने छात्रों के बारे में क्या महसूस करते हैं? इस प्रश्न का उनके अपडेट्स में जवाब। अन्य कई लोगों की नौकरी जाने का कारण था अपन नियोक्ता (एप्लॉयर) के बारे में अपडेट्स में पोस्ट करना। ऐसी ही कुछ अन्य बातें हैं जिनके बारे में सावधान रहने की आवश्यकता है।

#### **11.1.5 ऑनलाइन कन्टेन्ट शेयर करना:—**

किसी वेबसाइट की लिंक शेयर करके अपने मित्र का ध्यान आकर्षित करना आसान है। लेकिन कई और लोगों का ध्यान भी इस ओर आकर्षित होगा और उनकी क्या प्रतिक्रिया होगी? उदाहरण के लिए यदि आप किसी ऐसी साइट को शेयर (या लाइक) करते हैं जो सरकार के किसी नजरिये का विरोध करती है, तो हो सकता है कि सरकार के एजेंट आप पर नजर रखने लगें और आप पर सीधे कार्रवाई भी करें। यदि आप चाहते हैं कि आपके कान्टेक्ट्स (और निश्चय ही आपके द्वारा इस्तेमाल की जा रही सोशल नेटवर्किंग साइट का एडमिनिस्ट्रेटर भी) ही आपके द्वारा शेयर की गई या लाइक की गई विषय वस्तु को देखें, तो अपनी प्राइवेसी सेटिंग्स को जरूर चैक कर लें।

#### **11.1.6 अपनी लोकेशन की जानकारी देना:—**

यदि आपकी लोकेशन का डाटा उपलब्ध है तो अधिकांश सोशल नेटवर्किंग साइट्स इसे डिस्प्ले करेंगी। आमतौर पर जब सोशल नेटवर्क पर सम्पर्क के लिए जीपीएस—संचालित फोन का इस्तेमाल करते हैं तो यह फंक्शन काम करने लगता है। लेकिन यह भी मानकर मत चलिए कि यदि फोन के जरिए कनेक्ट नहीं हो रहे हैं तो ऐसा नहीं होगा। आपका कम्प्यूटर जिस नेटवर्क से कनेक्ट है वह भी आपकी लोकेशन बता सकता है। इस बारे में सुरक्षित रहना है, तो अपनी सैटिंग डबल चेक करें। फोटो और वीडियो शेयरिंग साइट्स पर तो विशेष रूप से सावधान रहें। ऐसा न मान लें कि वे आपके लोकेशन शेयर नहीं कर रहे हैं। आश्वस्त होने के लिए सैटिंग्स डबल चैक करें।

#### **11.1.7 वीडियो और फोटो शेयर करना:—**

फोटो और वीडियो से किसी भी व्यक्ति की पहचान का खुलासा आसानी से किया जा सकता है। इसलिए जब भी आप किसी व्यक्ति की फोटो या वीडियो पोस्ट करना चाहें, पहले उसकी सहमति अवश्य ले

लें। जब भी आप किसी अन्य व्यक्ति की फोटो या वीडियो पोस्ट करते हैं तो ध्यान रखें कि आप उसकी प्राइवेसी (निजता) को दांव पर लगा रहे हैं। किसी की भी फोटो या वीडियो उसकी सहमति के बिना कभी भी पोस्ट न करें।

फोटो और वीडियोज अनजाने में और भी बहुत सी जानकारी प्रकट कर सकते हैं। ऐसे बहुत से कैमरे हैं जिनमें गुप्त डाटा (मेटाडाटा टैग्स) इम्बेड (अन्तःस्थापित) होते हैं जो स्वयंमेव फोटो की तारीख, समय और स्थान तथा कैमरे के प्रकार का खुलासा कर देते हैं। जब आप इन फोटो अथवा वीडियो को उनकी साइट पर अपलोड करते हैं, तो ये साइट्स इस सूचना को भी पब्लिश कर देती हैं।

### 11.1.8 इन्स्टैन्ट चैट

अनेक सोशल नेटवर्किंग साइट्स में ऐसे दूल उपलब्ध हैं, जो आपको अपने मित्रों से रीयल टाइम (उसी समय) चैट की सुविधा देते हैं। ये इन्स्टैन्ट मैसेजिंग की तरह काम करते हैं और इन्टरनेट पर ये इन्स्टैन्ट चैट, बातचीत के सबसे ज्यादा असुरक्षित तरीके हैं। क्योंकि ये दूल आप किससे बात कर रहे हैं, क्या बात कर रहे हैं, इन सब का खुलासा कर सकते हैं।

### 11.1.9 ग्रुप, इवेन्ट और कम्यूनिटी ज्वाइन करना और बनाना:—

यदि आप किसी ग्रुप अथवा कम्यूनिटी को ज्वाइन करते हैं, तो आप लोगों को क्या इन्फॉर्मेशन दे रहे हैं? यह इन्फॉर्मेशन आपके बारे में क्या बताती है? इसके विपरीत, आपके द्वारा बनाए गए ग्रुप या कम्यूनिटी में शामिल होने वाले लोग दुनिया को क्या संदेश दे रहे हैं? आप किस प्रकार लोगों को जोखिम में डाल रहे हैं?

जब आप किसी ऑनलाइन ग्रुप या कम्यूनिटी में शामिल होते हैं तो इससे दूसरों को आपके बारे में कुछ जानकारी अवश्य मिलती है। कुल मिलाकर, लोग यह अनुमान लगाएंगे कि वह ग्रुप जो कह रहा है या कर रहा है, आप उसका समर्थन करने या उनसे सहमत हैं। उदाहरण के लिए, यदि आप किसी खास राजनीतिक दल के साथ जुड़े नजर आते हैं तो यह आपके लिए असरक्षित हो सकता है। साथ ही, यदि आप किसी ग्रुप में शामिल होते हैं, जिसके अधिकांश सदस्यों को आप नहीं जानते, तो आपकी यह हरकत आपकी प्राइवेसी अथवा आपके एकाउन्ट की सिक्यूरिटी सेटिंग्स के लिए खतरा बन सकती है। इसलिए, किसी भी ग्रुप को ज्वाइन करने से पहले यह जरूर सोचें कि आप अपने बारे में कौन सी इन्फॉर्मेशन देने जा रहे हैं। कहीं आप अपनी फोटो या सही नाम का इस्तेमाल तो नहीं कर रहें ताकि अनजान लोग आपको पहचान सकें?

इसके विपरीत, यदि आप कोई ग्रुप बनाते हैं और लोग इसमें शामिल होने लगते हैं। तो ये लोग ऐसा करके दुनियां को क्या बता रहे हैं? उदाहरण के लिए, हो सकता है कि यह गे और लेस्बियन सपोर्ट ग्रुप हो, जो आपने ऐसे लोगों की मदद के लिए बनाया है, लेकिन इस ग्रुप में शामिल होने वाले लोग अपने आपको खुले तौर पर गे (समलैंगिक) अथवा गे-फ्रेन्डली घोषित कर रहे हैं, जो वास्तविक दुनियां में उनके लिए खतरा बन सकता है।

## 11.2 ई मेल सिक्यूरिटी टिप्स<sup>13</sup>:-

1. ऐसे किसी भी ईमेल अटैचमेंट, जिसकी आपको उम्मीद नहीं थी या जो किसी ऐसे अनजान सोर्स से आई है, मत खोलिए। यदि आप ऐसी ई मेल को खोलें, तो यह सुनिश्चित कर लें कि आपका एन्टी-वायरस साफ्टवेयर अपडेट है और साथ ई मेल प्रोग्राम अथवा आपके ब्राउजर से प्राप्त चेतावनी को अनदेखा न करें।
2. आप एनोनिमिटी सॉफ्टवेयर का इस्तेमाल कर सकते हैं। यह सॉफ्टवेयर आपकी पसंदीदा ई मेल सर्विस को ऐसे लोगों की नजरों से छापा कर रखता है, जो आपके इन्टरनेट कनेक्शन की निगरानी कर रहे हैं। ऐसा ही एक फ्री और अच्छा सॉफ्टवेयर टॉर (टॉर ब्राउजर के बारे में और ज्यादा जानकारी गूगल से प्राप्त करें) है। यदि आप अपने ई-मेल के माध्यम से अपनी पहचान के बारे में जानकारी नहीं देना चाहते तो अपने व्यक्तिगत और पेशेवर जीवन से संबंधित “पूरे नाम” को अपना यूजरनेम न बनाएं।
3. आप अपनी ई-मेल पर नजर रखें और अपना ईमेल एड्रेस सोच समझ कर ही दें। इस तरह आप स्पैम (अवांछित और जंक ईमेल) से बच सकते हैं। यदि आप को कोई स्पैम मेल मिलती है तो न तो इसे खोलें और न ही इसका जवाब दें। ऐसा न करने पर स्पैमर्स यह समझ जाएंगे कि यह ई मेल अस्तित्व में है, तथा वे और ज्यादा स्पैम आपको भेजने लगेंगे। आप स्पैम फिल्टर का भी यूज कर सकते हैं, लेकिन आपको इसकी निगरानी करनी होगी, क्योंकि यह फिल्टर गलती से सही मेल को भी स्पैम मान सकता है।
4. आपको भी ऐसे प्रयास करने होंगे कि आपका ई मेल पाने वाला आपकी ईमेल को कहीं स्पैम न समझ ले। स्पैम फिल्टर्स मेल की सबजेक्ट हैंडिंग के कुछ शब्दों के आधार पर मैसेज ब्लॉक करते हैं। इसलिए ब्लॉक होने वाली मेल की सबजेक्ट लाइन्स को समझने के लिए अपने स्पैम फोल्डर को स्कैन करते रहें।
5. ई मेल स्कैम्स के प्रति सजग रहें। ऐसी बहुत से स्कैम ईमेल हैं जो ऐसी प्रतीत होती है कि किसी बैंक, ई बैंक पैल अथवा किसी अन्य ऑनलाइन शॉप से भेजी गई हैं। यदि आपको कोई ऐसी ईमेल मिलती

<sup>13</sup> <https://survival.tacticaltech.org/internet/email/tips>

है जो यह बता रही है कि आपका खाता बन्द किया जा रहा है या आप तत्काल अपनी एकाउन्ट इन्फॉर्मेशन को अपडेट करें, तो सावधान हो जाएं, ऐसी मेल आमतौर पर स्पैम होती हैं। इसके अलावा, आपको भी शायद ऐसी ई मेल प्राप्त हुई होंगी, जिसमें किसी ने अपनी आपदा का हवाला देत हुए, आपको तत्काल पैसे से मदद करने का अनुरोध किया होगा। सम्भव है कि इस पर्सनल ईमेल को किसी स्कैमर ने हैक कर लिया है।

6. आप किसी सेक्यूरिटी वेबमेल एकाउन्ट को एक्सेस कर रहे हैं और अचानक आपका ब्राउजर आपको इनवैलिड (अमान्य) सिक्यूरिटी सर्टिफिकेट की चेतावनी दने लगे तो सजग हो जाइये। इसका मतलब यह भी हो सकता है कि कोई व्यक्ति आपके मैसेज को इन्टरसेप्ट (बीच में पकड़ने) करने के लिए आपके कम्प्यूटर और सर्वर के बीच छेड़–छाड़ कर रहा है।

#### अभ्यास:-

1. एनोनिमस एकाउन्ट क्या है? ऐसे कुछ ब्राउजर्स का पता लगाएं जो एनोनिमिटी को सपोर्ट करते हैं।
2. उपरोक्त अध्याय को समझने के बाद क्या आप उपरोक्त सुरक्षा उपाय अपना रहे हैं? खामियों का पता लगाएं?
3. उपरोक्त सिफारिशों के आधार पर, अपने स्पेशल मीडिया एकाउन्ट की सैटिंग्स समायोजित (एडजस्ट) करें?

—□—

# स्मार्टफोन सिक्यूरिटी

## 12.1. परिचयः—

प्रौद्योगिकी में प्रगति से तात्पर्य है कि मोबाइल फोन भी डेस्कटॉप अथवा लैपटॉप कम्प्यूटर जैसी सेवाएं और फीचर उपलब्ध करा सकते हैं<sup>14</sup>। ये स्मार्टफोन संचार और मीडिया के प्रचार-प्रसार के कई नए तरीके पेश करते हैं। ये नए फंक्शन उपलब्ध कराने के लिए, स्मार्टफोन केवल मोबाइल नेटवर्क का ही इस्तेमाल नहीं करते, बल्कि वाई-फाई कनेक्शन के जरिए (इन्टरनेट कैफे में किसी लैपटॉप की तरह) अथवा मोबाइल नेटवर्क ऑपरेटर के माध्यम से डाटा कनेक्शन के जरिए इन्टरनेट से कनेक्ट होते हैं।

आप स्मार्टफोन से कॉल तो कर ही सकते हैं, परन्तु ये फोन दरअसल अब एक छोटे कम्प्यूटरिंग डिवाइस की तरह भी काम करने लगे हैं। यहां कहने का तात्पर्य यह है कि इस टूलकिट में उपलब्ध कराई गई प्रौद्योगिकी आपको स्मार्टफोन के साथ-साथ कम्प्यूटर की सुविधा भी प्रदान करती है।

स्मार्टफोन में अनक प्रकार के फंक्शन हैं जैसे कि वेब ब्राउजिंग, ईमेल, वॉइस एण्ड इन्स्टैन्ट मैसेजिंग ओवर इन्टरनेट, आडियो, वीडियो और फोटो कैचर करना, स्टोर करना और ट्रान्समिट करना, सोशल नेटवर्किंग, मल्टी यूजर गेम, बैंकिंग तथा कई अन्य कार्य आदि। लेकिन इनमें से अनेक टूल्स और फीचर्स ने सुरक्षा से जुड़े नए मुद्दों को जन्म दिया है अथवा मौजूदा जोखिम को और बढ़ा दिया है। उदाहरण के लिए, कुछ स्मार्ट फोन में बिल्ट इन जीपीएस फंक्शन है, यानि ये फोन बाई डिफाल्ट आपके मोबाइल नेटवर्क ऑपरेटर को आपकी सटीक लोकेशन उपलब्ध करा देंग। इसके अलावा आप जो अन्य एप्लीकेशन अपने फोन पर यूज करेंगे (जैसे कि सोशल नेटवर्किंग, मैपिंग, ब्राउजिंग और अन्य एप्लीकेशन आदि) के लिए भी आपकी लोकेशन डिस्प्ले करेंगे। जैसा कि ऊपर बताया गया है, ये मोबाइल फोन आपकी लोकेशन मोबाइल नेटवर्क ऑपरेटर को बता देते हैं। लेकिन, जीपीएस फंक्शन की यह अतिरिक्त सुविधा, आपके लोकेशन की सटीकता को ही नहीं बढ़ाती बल्कि उन स्थानों की संख्या भी बढ़ा देती है, जहां-जहां आपकी लोकेशन डिस्प्ले हो सकती है।

मोबाइल फोन को ज्यादा से ज्यादा सुरक्षित रूप से यूज करने के हमारे दिशा-निर्देशों में हमने इन फोन से जुड़े जोखिमों पर चर्चा की थी। ये जोखिम स्मार्टफोन पर भी लागू होते हैं, इसलिए इन पर फिर एक नजर डाल लें। उस दिशा-निर्देश में इवेस-ड्रॉपिंग, इन्टरसेप्शन ऑफ एसएमएस अथवा फोन कॉल्स, सिम कार्ड से जुड़े मुद्दों तथा सर्वश्रेष्ठ तौर-तरीकों को भी कवर किया गया है। इस अध्याय में हम स्मार्ट फोन से उत्पन्न सुरक्षा-संबंधी नई चुनौतियों पर चर्चा करेंगे।

<sup>14</sup> <https://securityinabox.org/en/guide/smartphones>

## **12.2 स्मार्ट फोन सिक्यूरिटी गाइड लाइन्सः—**

### **12.2.1 पर्स, वॉलेट्स, स्मार्टफोन्सः—**

अपने पर्स अथवा वॉलेट्स को सुरक्षित रखने की अहमियत के बारे में हम सभी को एक सहज समझ होती है। क्योंकि इनमें रखी गई इन्फॉर्मेशन इतनी महत्वपूर्ण होती है कि यदि हम इन्हें गुम कर दें तो हमारी प्राईवेसी दांव पर लग जाएगी। इसी तरह लोग उनके स्मार्टफोन में स्टोर पर्सनल इन्फॉर्मेशन के प्रति भी इतने सजग नहीं होते। फोन खो जाने पर परेशान तो होते हैं लेकिन इसके जोखिम को नहीं समझते। यदि आप भी यह मानते हैं कि स्मार्टफोन एक कम्प्यूटर की तरह है जो हमेशा नेटवर्क से कनेक्ट रहता है और हमेशा आपके साथ रहता है, चाहे कहीं भी आप जाएं। यदि आपका वॉलेट या पर्स आपकी पैसिव इन्फॉर्मेशन (निष्क्रिय जानकारी) रखता है तो आपका स्मार्टफोन एक्टिव इन्फॉर्मेशन (सक्रिय जानकारी) रखने वाले वॉलेट या पर्स की तरह है। इस अन्तर के महत्व को समझना होगा।

#### **एक आसान सी कवायद से उसे समझिएः—**

अपना पर्स खाली कीजिए और चैक कीजिए की उसमें क्या-क्या है? पियजनों की तस्वीरें (पांच चित्र), पहचान पत्र (ड्राइविंग लाइसेंस, मेम्बरशिप कार्ड, स्पेशल सिक्यूरिटी कार्ड) इन्श्योरेंश और हैत्थ इन्फॉर्मेशन (दो कार्ड) मनी (5 नोट), क्रेडिट-डेबिट कार्ड (3 कार्ड)।

अब अपने स्मार्टफोन में रखी जानकारी चैक करें— स्मार्टफोन का विशेष रूप से इस्तेमाल करने वाला उपरोक्त सभी मदों के अलावा कुछ और कीमती जानकारी इसमें पाएगा।

- प्रियजनों की तस्वीरें (100 से भी अधिक)
- ईमेल एप्लीकेशन और उनके पासवर्ड
- ई मेल (500 से भी ज्यादा)
- वीडियो (50 से भी ज्यादा)
- सोशल नेटवर्किंग एप्लीकेशन और उनके पासवर्ड
- बैंकिंग एप्स (बैंक एकाउन्ट तक एक्सेस के साथ)
- संवेदी डाक्यूमेंट्स
- लाइव कनेक्शन टू सेन्सिटिव इन्फॉर्मेशन।

आप जितना ज्यादा स्मार्टफोन यूज करेंगे उतना ही ज्यादा आपको इससे जुड़े जोखिमों के प्रति सजग रहना पड़ेगा। स्मार्ट फोन आपके पर्सनल डाटा के पॉवरफल एम्लीफायर और डिस्ट्रीब्यूटर होते हैं। ये बाई

डिफॉल्ट अधिक से अधिक केनविटविटी और सोशनल नेटवर्किंग सर्विसेज से लिंक करने के लिए डिजाइन किए गए हैं। ऐसा इसलिए है, क्योंकि आपका पर्सनल डाटा एक कीमती इन्फॉर्मेशन है जिसे जुटाया जा सकता है, खोजा जा सकता है और बेचा जा सकता है।

यदि आपने अपने महत्वपूर्ण डाटा (जैसे कि आपके कान्टेक्ट्स) का बैकअप सुरक्षित नहीं रखा और आपका फोन खो गया तो आपके लिए यह अत्यन्त खतरनाक हो सकता है। अपने डाटा का बैकअप रखने के अलावा आपको इन्हें रिस्टोर करना भी आना चाहिए। आपको कौन से कदम उठाने हैं इसकी हार्डकॉफी रख लें, ताकि इमर्जेंसी में तत्काल ये कदम उठा सकें।

इस अध्याय की शुरुआत हम स्मार्टफोन के कुछ बेसिक्स, विभिन्न प्लेटफॉर्म्स की जानकारी तथा सूचना और कम्यूनिकेशन को सेक्योर बनाने के कुछ बेसिक सेटअप से करेंगे। अध्याय के शेष भाग में हम स्मार्टफोन के सामान्य इस्तेमाल से जुड़ी विशेष सावधानियों पर चर्चा करेंगे।

## 12.2.2 प्लेटफॉर्म, सेटअप और इन्स्टॉलेशन

### 12.2.2.1 प्लेटफॉर्म और ऑपरेटिंग सिस्टम:-

आजकल सबसे ज्यादा प्रचलित स्मार्टफोन आई-फोन और गूगल के एन्ड्रॉयड फोन हैं और इनके बाद नम्बर आता है ब्लैकबैरी और विन्डोज फोन का। एन्ड्रॉयड और अन्य ऑपरेटिंग सिस्टम में एक प्रमुख अन्तर यह है कि एन्ड्रॉयड आमतौर पर एक ओपन सोर्स (एफओएसएस) सिस्टम है जो ऑपरेटिंग सिस्टम को व्यक्तिगत रूप से ऑडिट करने की सुविधा देता है ताकि यह सत्यापित किया जा सके कि यूजर की इन्फॉर्मेशन और कम्यूनिकेशन भलीभांति सुरक्षित हैं। यह इस प्लेटफॉर्म के लिए सिक्यूरिटी एप्लीकेशन डेवलप करने की सुविधा भी देता है। सुरक्षा के प्रति जागरूक बहुत से प्रोग्रामर यूजर की सेफ्टी और सिक्यूरिटी को ध्यान में रखते हुए एन्ड्रॉयड एप्लीकेशन विकसित करते हैं।

चाहे आप कोई सा भी स्मार्टफोन यूज करते हों, ऐसे बहुत से सुरक्षा से जुड़े मुद्दे हैं, जिन्हें आपको इन्टरनेट से कनेक्ट होने वाले फोन, जिनमें जीपीएस अथवा वायरलेस क्षमता है, यूज करते समय ध्यान में रखना होगा। इस चैप्टर में हम एन्ड्रॉयड प्लेटफॉर्म डिवाइसेस पर विशेष चर्चा करेंगे क्योंकि इस प्लेटफॉर्म पर डाटा और कम्यूनिकेशन सेक्योर करना अपेक्षाकृत आसान है। लेकिन, एन्ड्रॉयड के अलावा अन्य ऑपरेटिंग सिस्टम वाले डिवाइसेज के लिए बेसिक सेटअप गाइड और कुछ एप्लीकेशन्स पर भी चर्चा की गई है। ब्लैकबैरी फोन को ‘सेक्योर’ मैसेजिंग और ई मेल डिवाइस के रूप में प्रस्तुत किया गया है। क्योंकि इसमें मैसेज और ईमेल ब्लैकबैरी सर्वर के माध्यम से चैनल किया जाता है जो सम्भावित इवेसड्रॉपर्स (कनसुइयों यानि चोरी-छुपे किसी की बात सुनने वाले) की पहुंच से बाहर होते हैं। दुर्भाग्य से, अनेक सरकारें, सम्भावित आतंकवाद और संगठित अपराधों का हवाला देकर, इन कम्यूनिकेशन्स तक पहुंच की

मांग कर रही है। भारत, संयुक्त अरब अमीरात, सऊदी अरब, इन्डोनेशिया और लेबनान की सरकारें इसके उदाहरण हैं, जिन्होंने ब्लैकबेरी के इस्तेमाल की जांच-पड़ताल की है और उनके देशों में यूजर डाटा तक एक्सेस की मांग कर रही हैं।

#### 12.2.2.2 फीचर फोन्स

मोबाइल फोन की एक और कैटेगरी है जिन्हें बहुधा फीचर फोन कहा जाता है। हाल ही में इन फीचर फोन में कुछ स्मार्टफोन के फंक्शन भी जोड़ दिए गए हैं। लेकिन सामान्यतया, फीचर फोनों के ऑपरेटिंग सिस्टम्स कम एक्सेसिबल होते हैं इसलिए इनमें सिक्यूरिटी एप्लीकेशन्स और सुधारों की कम गुंजाइश होती है। हम फीचर फोन्स को केन्द्र में रखकर यह चर्चा नहीं कर रहे हैं, हालांकि यहां विचार-विमर्श में शामिल कुछ उपाय फीचर फोन्स पर भी लागू होते हैं।

#### 12.2.2.3 ब्रान्डेड और लॉकड स्मार्टफोन

स्मार्टफोन आमतौर पर ब्रान्डेड या लॉकड होते हैं। स्मार्टफोन लॉकिंग से तात्पर्य यह है कि यह डिवाइस केवल उस एक कैरियर से ही संचालित होगा, उसकी सिमकार्ड ही इस डिवाइस में काम करेगी। मोबाइल नेटवर्क ऑपरेटर आमतौर पर अपने फर्मवेयर अथवा सॉफ्टवेयर इन्स्टॉल करके फोन को ब्रान्ड करते हैं। वे कुछ फंक्शन डिसेबल भी कर सकते हैं या कुछ नए फंक्शन जोड़ भी सकते हैं। कम्पनियों के लिए ब्रान्डिंग एक जरिया है इसके द्वारा वे आपके स्मार्टफोन को चैनलाइज करके राजस्व कमाते हैं और बहुधा फोन इस्तेमाल करने के आपके तौर-तरीकों के बारे में डाटा जुटाकर अथवा आपके स्मार्टफोन की रिमोट एक्सेसिंग के द्वारा अपना राजस्व बढ़ाते हैं।

इन कारणों के चलते, हमारा सुझाव है कि आप अनब्रांडेड फोन खरीदें। लॉकड फोन के जोखिम बहुत ज्यादा है क्योंकि आपके डाटा एक कैरियर के जरिए रुट होते हैं जो आपकी डाटा स्ट्रीम को सेन्ट्रलाइज करता है और अलग-अलग कैरियर पर डाटा प्रसारित करने से रोकने के लिए आपको सिम नहीं बदलने देता है। यदि आपका फोन लॉकड है तो इसे अनलॉक करने के लिए उसकी मदद लें, जिस पर आपको भरोसा हो।

#### 12.2.2.4 सामान्य सेटअप

स्मार्टफोन में बहुत सी सैटिंग्स होती हैं जो डिवाइस की सिक्योरिटी को नियंत्रित करती हैं। आपको ध्यान देना है कि आपका स्मार्टफोन किस तरह सेटअप किया गया है। नीचे दिए गए सुलभ मार्गदर्शन में हम आपको स्मार्टफोन सेटिंग्स की कुछ खास सुरक्षा सेटिंग्स के बारे में बताएंगे जो उस फोन में उपलब्ध हैं।

लेकिन बाई डिफॉल्ट एकिटव नहीं हैं। साथ ही वो सैटिंग्स भी बताएंगे जो बाई डिफॉल्ट एकिटव हैं और आपके फोन के लिए जोखिम हैं।

#### 12.2.2.5 इन्स्टॉलिंग एण्ड अपडेटिंग एप्लीकेशन्स

हम अपने स्मार्टफोन पर नए सॉफ्टवेयर इन्स्टॉल करने के लिए आईफोन एप स्टोर या गूगल प्ले स्टोर का इस्तेमाल करते हैं। हम अपने लॉग-इन क्रेडेन्शियरम का उपयोग करके अपेक्षित एप्लीकेशन डाउनलोड करके इसे इन्स्टॉल कर लेते हैं। आप लॉग-इन करके एप ऑनलाइन स्टोर के अपने उपयोग को लॉगड-इन यूजर एकाउन्डट से जोड़ देते हैं। इस प्रकार एप्लीकेशन स्टोर के मालिक इस यूजर की ब्राउजिंग हिस्ट्री और एप्लीकेशन पसंद का रिकार्ड रखते हैं।

ऑफिसियल ऑनलाइन स्टोर पर उपलब्ध एप्लीकेशन यद्यपि स्टोर ओनर (गूगल या एपल) द्वारा सत्यापित है, लेकिन वास्तविकता में ये एप्लीकेशन इन्स्टॉल हो जाने के बाद क्या करगे, इसकी सुरक्षा की कोई गारंटी नहीं होती। उदाहरण के लिए, कुछ एप्लीकेशन इन्स्टॉल होने के बाद आपकी एड्रेस बुक को कॉपी करके अन्य को भेज सकते हैं। एन्ड्रॉयड फोन पर प्रत्येक एप्लीकेशन को इन्स्टॉलेशन प्रक्रिया के दौरान यह बताना होता है कि जब इस एप्लीकेशन का इस्तेमाल होगा तो यह क्या-क्या करेगा। आपको ध्यान से देखना होगा कि यह क्या अनुमति मांग रहा है और क्या ये अनुमतियां इस एप्लीकेशन के सही कार्य करने के लिए आवश्यक हैं? उदाहरण के लिए यदि कोई “न्यूजरीडर” एप्लीकेशन आपसे आपके कॉन्टेक्ट को मोबाइल डाटा कनेक्शन पर किसी अन्य पार्टी को भेजने का अधिकार मांग रही है तो आपको समुचित एक्सेस और अधिकार वाली किसी अन्य वैकल्पिक एप्लीकेशन को खोजना चाहिए। हो सकता है कि कुछ यूजर्स इन वैकल्पिक साइट्स पर विचार करें ताकि गूगल के साथ ऑनलाइन कान्टेक्ट को कम कर सकें। इसके लिए एक वैकल्पिक स्टोर एफ-ड्रॉइड (फ्री डॉइड) है, जो केवल क्रॉस एप्लीकेशन्स उपलब्ध कराता है। लेकिन यह ध्यान रखें कि किसी भी एप्स को डाउनलोड करने के पहले आपको उस साइट पर भरोसा होना जरूरी है। अनुभवी यूजर्स को हमारा सुझाव है कि आप गूगल प्ले स्टोर का प्रयोग करें। यदि आप एप्स हासिल करने के लिए ऑनलाइन नहीं होना चाहते (अथवा ऐसा नहीं कर पाते), आप किसी और के फोन पर ब्ल्यू टूथ के द्वारा ज्वा फाइल्स (एन्ड्रॉयड एप्लीकेशन पैकेज का लघुनाम) भेज कर इसे ट्रान्सफर कर सकते हैं। एक और तरीका है, आप अपने डिवाइस के माइक्रो कार्ड पर ज्वा फाइल्स डाउनलोड कर सकते हैं अथवा यूएसबी केबल का उपयोग करके पीसी से अपने फोन पर ले सकते हैं। जब आपको फाइल मिल जाए, आप फाइल नेम पर लॉग टैप करें और आपको इसे इन्स्टॉल करने का संकेत मिल जाएगा। (नोट : ब्ल्यू टूथ इस्तेमाल करते समय विशेष रूप से सावधान रहें।)

### **12.2.3 स्मार्टफोन से सिक्यूरिटी कम्यूनिकेट (वॉयस या मैसेज द्वारा) करना:-**

अपने फोन से कॉल करने या कॉल रिसीव करने के लिए आपका फोन सबसे नजदीकी टॉवर को अपनी मौजूदगी का संकेत देने के उद्देश्य से अर्लट सिग्नल भेजता है। इन अलर्ट्स और कम्यूनिकेशन के फलस्वरूप, उस निश्चित समय पर आपकी लोकेशन की जानकारी नेटवर्क सर्विस प्रोवाइडर को प्राप्त होती है।

**गुमनाम बने रहना (एनोनिमिटी):** यदि आप फोन पर कोई गोपनीय वार्तालाप कर रहे हैं या गोपनीय एसएमएस भेज रहे हैं तो सभी मोबाइल फोनों के उपरोक्त ट्रैकिंग फीचर के प्रति सजग रहें। निम्नलिखित उपायों पर ध्यान दें:-

- हर बार अलग-अलग लोकेशन से फोन करें, और ऐसी लोकेशन चुनें जो आपसे जुड़ी न हो।
- बैटरी डिस्कनेक्ट करके फोन ऑफ रखें, चुनी गई लोकेशन पर जाएं, फोन स्विच ऑन करें, वार्तालाप करें, फोन स्विच ऑफ करें, बैटरी डिस्कनेक्ट करें। जब भी आप को फोन करना हो, और आप ऐसा करेंगे तो नेटवर्क आपके मूमेंट को ट्रैक नहीं कर पाएगा।
- अपना फोन और सिमकार्ड बदलते रहें। दोस्तों अथवा सैकेन्ड हैण्ड मार्केट के जरिए इन्हें रोटेट करते रहें।
- यदि आपके क्षेत्र में सम्भव हो तो अन-रजिस्टर्ड प्री-पेड सिमकार्ड का उपयोग करें। फोन अथवा सिमकार्ड के भुगतान के लिए क्रेडिट कार्ड के उपयोग से बचें। क्योंकि क्रेडिट कार्ड इन आइटम्स और आपके बीच कनेक्शन की एक कड़ी (लिंक) बन सकता है।

### **इवेसड्रॉपिंग:-**

आपकी जानकारी के बिना आपके फोन को इसके माइक्रोफोन की रेन्ज में कोई भी आवाज रिकार्ड करने और ट्रान्समिट करने के लिए सेट किया जा सकता है। कुछ फोन्स को रिमोटली स्विच ऑन किया जा सकता है और इस तरह उन्हें एविटब किया जा सकता है जबकि फोन स्विच ऑफ ही नजर आएंगे।

- जिन लोगों पर आप भरोसा नहीं करते उन्हें अपना फोन बिल्कुल न दें, सामान्यतया स्पाइवेयर फोन हासिल करके ही इन्स्टॉल किए जाते हैं।
- यदि आप किसी प्राइवेट मीटिंग या महत्वपूर्ण मीटिंग में हैं, अपना फोन स्विचऑफ रखें और बैटरी निकाल दें। यदि फोन किसी पूरी तरह सुरक्षित स्थान पर रख सकते हैं तो फोन मीटिंग में न ले जाएं।
- यह भी सुनिश्चित करें कि आप जिससे वार्तालाप कर रहे हैं वह भी यही सुरक्षा उपाय अपनाएं।

- इसके अलावा, यह न भूलें कि सार्वजनिक स्थलों या गैर-भरोसेमंद जगहों पर फोन का इस्तेमाल करके आप सुरक्षा को दांव पर लगा रहे हैं, कोई भी आपकी बात सुन सकता है, या आपका फोन चोरी हो सकता है।
- **कॉल इन्टरसेप्ट करना:**— मोबाइल फोन नेटवर्क से लेकर गुजरने वाले वायঁस कम्यूनिकेशन्स (और टेक्स्ट मैसेज) का एनक्रिप्शन अपेक्षाकृत कमज़ोर होता है। ऐसी बहुत सी सस्ती तकनीक है। जिनके द्वारा आपके लिखित वार्तालाप को इन्टरसेप्ट (बीच में पकड़ना) किया जा सकता है या आपकी कॉल सुनी जा सकती है। फिलहाल फोन कॉल को इतना मजबूती से एनक्रिप्ट करना कि मोबाइल फोन प्रोवाइडर भी चोरी छुपे आपका वार्तालाप न सुन सके, काफी महंगा और जटिल है। लेकिन उम्मीद है कि जल्दी ही ये टूल्स सस्ते हो जाएंगे। एनक्रिप्शन का इस्तेमाल करने के लिए, सबसे पहले आपको अपने फोन और साथ ही जिससे आप वार्तालाप करेंगे उसके फोन पर एनक्रिप्शन एप्लीकेशन इन्स्टॉल करना होगा। उसके बाद ही आप एनक्रिप्टेड कॉल और/अथवा मैसेज भेजने और प्राप्त करने के लिए इस एप्लीकेशन का प्रयोग कर पाएंगे। फिलहाल, इन तथा-कथित स्मार्टफोन्स के कुछ ही मॉडल एनक्रिप्शन सॉफ्टवेयर को स्पोर्ट करते हैं।

चूंकि वार्तालाप के दारान कई बार सिग्नल उस मोबाइल नेटवर्क में भी जाते हैं, जहां एनक्रिप्शन की सुविधा नहीं है इसलिए स्काइप और फोनों के बीच भी वार्तालाप एनक्रिप्टेड नहीं होते। अपने स्मार्टफोन के मोबाइल डाटा के जरिये या वाई-फाई के जरिए इन्टरनेट का इस्तेमाल करके वीओआईपी (वॉयस ओवर इन्टरनेट प्रोटोकॉल) के द्वारा और कम्यूनिकेशन के इस चैनल को सुरक्षित बनाने के तरीके अपना कर लोगों से कम्यूनिकेट करना ज्यादा सेफ है। कुछ स्मार्टफोन टूल्स वीओआईपी से परे, मोबाइल फोन काल्स को भी थोड़ी सुरक्षा प्रदान करते हैं (नीचे बताया गया रेडफान)। हम कुछ टूल्स और उनके फायदे तथा नुकसान पर आगे चर्चा करने जा रहे हैं:—

### **स्काइप**

सबसे ज्यादा लोकप्रिय वीओआईपी एप्लीकेशन स्काइप सभी स्मार्टफोन प्लेटफार्म के लिए उपलब्ध है और यदि आपकी वायरलेस कनेक्टिविटी भरोसेमंद है तो काम भी ठीक से करता है। लेकिन मोबाइल डाटा पर इसकी पर्फॉर्मेंस कोई खास नहीं है।

स्काइप ओपन-सोर्स वाला सॉफ्टवेयर नहीं है इसलिए इसके सिक्योरिटी स्तर को सत्यापित करना मुश्किल है। इसके अलावा स्काइप का स्वामित्व माइक्रोसॉफ्ट के पास है, और जिसके वाणिज्यिक हित, आप कब और कहाँ से स्काइप का यूज करते हैं, इससे जुड़े हैं। स्काइप आपके वार्तालाप का पिछला विवरण कानून लागू करने वाली एजेंसियों के साथ भी साझा कर सकता है।

## अन्य वीओआईपी टूल्स

वीओआईपी आमतौर पर फ्री (अथवा मोबाइल फोन कॉल की तुलना में काफी सस्ता) है और कोई डाटा सबूत नहीं छोड़ता है। दरअसल, वीओआईपी कॉल वार्तालाप का सबसे ज्यादा सुरक्षित तरीका है।

### रेडफोन

एक फ्री और ओपन सोर्स वाला सॉफ्टवेयर एप्लीकेशन है जो इस एप्लीकेशन पर चलने वाले दो डिवाइसेज के बीच भेजे गए वॉयस-डाटा को एनक्रिप्ट करता है। इसे इन्स्टॉल करना और यूज करना बहुत आसान है क्योंकि यह स्वयं को आपके नॉर्मल डायलिंग और कॉन्टेक्ट स्क्रीम से जोड़ लेता है। लेकिन आप उसी व्यक्ति से बात कर सकते हैं जिसने अपने फोन में इस एप्लीकेशन को इन्स्टॉल कर रखा है। इस्तेमाल को आसान बनाने के लिए, रेडफोन आपके कॉन्टेक्ट्स को आपकी पहचान बताने के लिए आपके मोबाइल नम्बर का उपयोग करता है। दुर्भाग्य से, यदि आपके पास फंक्शनिंग मोबाइल सर्विस प्लान नहीं हैं तो रेडफोन का इस्तेमाल करना मुश्किल होगा, भले ही आपका डिवाइस इन्टरनेट से कनेक्ट होने के लिए वाई-फाई का इस्तेमाल करने में सक्षम क्यों न हो। रेडफोन एक सेन्ट्रल सर्वर का इस्तेमाल करता है, इसके चलते सर्विस एडमिनिस्ट्रेटर आपकी एनक्रिप्टेड वीओआईपी कॉल से जुड़े मेटा-डाटा देख सकता है।

### सीशिपसिम्प्ल:-

यह एन्ड्रॉयड फोन के लिए एक सशक्त वीओआईपी क्लाइन्ट है। यह भलीभांति अनुरक्षित है और विभिन्न वीओआईपी सेवाओं के लिए इसमें बहुत से आसान सेट-अप विजार्ड हैं।

ओपन सेक्योर टेलीफोन नेटवर्क (ओएसटीएन) और गार्जियन प्रोजेक्ट वेजमसण्व द्वारा उपलब्ध कराया गया सर्वर वॉयस कम्यूनिकेशन के लिए सबसे ज्यादा सुरक्षित जरिया है। सबसे ज्यादा महत्वपूर्ण है आपके वीओआईपी के लिए सर्वर ऑपरेट करने वाले निकाय को जानना और उस पर भरोसा करना।

सीशिपसिम्प्ल यूज करते समय, आप कभी भी, सीधे अपेन कॉन्टेक्ट से वार्तालाप नहीं करते, बल्कि आपका सारा डाटा ऑस्टल सर्वर से होकर रुट होता है। इससे आपके डाटा को ट्रेस करना और आप किससे बात कर रहे हैं, यह जानना मुश्किल हो जाता है। इसके अलावा, ऑस्टल आपके डाटा नहीं रखता है, यह केवल लॉगइन के लिए आपका एकाउन्ट डाटा रखता है। आपके डाटा को सुरक्षित रूप से एनक्रिप्ट किया जाता है और चूंकि ट्रैफिक वेजमसण्व सर्वर के जरिए प्रौक्षसी द्वारा रुट किया जाता है, इसलिए आपका मेटा-डाटा जिसे छुपना बड़ा मुश्किल होता है, भी धुंधला (ब्लर) कर दिया जाता है। यदि आप वेजमसण्व से सीशिपसिम्प्ल डाउनलोड करते हैं, तो यह ऑस्टल के साथ उपयोग के लिए पहले से ही स्वतः कन्फिगर होता है, इसके चलते इसे इन्स्टॉल करना और यूज करना आसान हो जाता है। सीशिपसिम्प्ल और वेजमसण्व के लिए टूल्सगाइड पर आगे चर्चा करेंगे। इस बीच, आप उपरोक्त लिंक पर जाकर और ज्यादा जानकारी हासिल कर सकते हैं।

### **12.2.3.2 सुरक्षित रूप से संदेश भेजना**

एसएमएस भेजते समय, इन्स्टॉट मैसेजिंग का यूज करते समय या अपने स्मार्टफोन पर चैटिंग के दौरान सावधानी बरतें।

#### **एसएमएस**

एसएमएस कम्प्यूनिकेशन बार्झिफॉल्ट इनसेक्योर होता है। मोबाइल टेलीकम्प्यूनिकेशन नेटवर्क की सुविधा से युक्त कोई भी व्यक्ति इन संदेशों को आसानी से इन्टरसेप्ट कर सकता है और ऐसा रोज हो रहा है। आपातकालीन स्थिति में अनसेक्योर एसएमएस भेजने पर निर्भर न रहें। एसएमएस संदेशों को प्रमाणित करने का कोई तरीका भी नहीं है, इसलिए यह जानना असम्भव होता है कि डिलीवरी के दौरान मैसेज की विषयवस्तु बदल तो नहीं दी गई या मैसेज भेजने वाला वही व्यक्ति है जो वह होने का दावा करता है।

#### **एसएमएस सेक्योर करना**

एन्ड्रॉयड फोन पर सेक्यूर एसएमएस भेजने और प्राप्त करने के लिए टैक्स्टसैक्योर एक एफओएसएस टूल है। यह एनक्रिप्टेड और नॉन-एनक्रिप्टेड दोनों संदेशों के लिए काम करता है, इसलिए आप इसे अपने डिफॉल्ट एसएमएस एप्लीकेशन के रूप में इस्तेमाल कर सकते हैं। एनक्रिप्टेड संदेशों के आदान-प्रदान के लिए, संदेश भेजने और प्राप्त करने वाले दोनों के फोन पर यह टूल इन्स्टॉल होना चाहिए, इसलिए आप जिनसे वार्तालाप करते हैं, उनसे कहें कि इस टूल का नियमित रूप से इस्तेमाल करें। किसी अन्य टैक्स्टसैक्योर यूजर से प्राप्त एनक्रिप्टेड मैसेज को दूसरे छोर पर इन्स्टॉल टैक्स्टसैक्योर स्वतः डिटेक्ट कर लेता है। आप टैक्स्टसैक्योर के जरिए एक से अधिक लोगों को एनक्रिप्टेड मैसेज भेज सकते हैं। संदेश ऑटोमेटिकली हस्ताक्षरित होते हैं, इसलिए संदेश की विषय-वस्तु से छेड़-छाड़ करना असम्भव होता है। टैक्स्टसैक्योर की सुलभ गाइड में हम इस टूल की विशेषताओं और इस्तेमाल के तरीके पर विस्तार से चर्चा करेंगे।

#### **सैक्योर चैट:-**

आपके फोन पर इन्स्टॉन्ट चैटिंग और मैसेजिंग जानकारी का भण्डार पैदा कर सकती है और इस जानकारी के इन्टरसेप्ट होने का जोखिम बना रहता है। आपका अहित करने के इच्छुक लोग बाद में इसका इस्तेमाल कर सकते हैं। इसलिए अपने फोन पर चैटिंग या इन्स्टॉन्ट मैसेजिंग के दौरान आपको सजग रहने की जरूरत है आपको संदेश लिखते समय यह ध्यान रखना है कि आप क्या जानकारी चैटिंग या मैसेजिंग के जरिए दे रहे हैं।

सुरक्षित चैट और मैसेजिंग के भी तरीके हैं। सबसे बढ़िया तरीका है, एन्ड्रॉयड एन्क्रिप्शन। इससे आप यह सुनिश्चित कर पाएंगे कि दूसरे छोर पर वही व्यक्ति है, जिससे आप सम्पर्क रखना चाहते हैं। हमारा सुझाव है कि एन्ड्रॉयड फोन के लिए आप चैटसैक्योर एप्लीकेशन का इस्तेमाल करें। चैटसैक्योर आपकी चैट

के लिए आसान और स्ट्रांग एन्क्रिप्शन उपलब्ध करता है और वह भी ऑफ-दी-रिकॉर्ड प्रोटोकोल के साथ। यह एन्क्रिप्शन प्रमाणिकता (आप यह सत्यापित कर सकते हैं कि आप सही व्यक्ति से बात कर रहे हैं) और प्रत्येक चैट सेशन (सत्र) की अलग-अलग सुरक्षा दोनों ही मुहैया कराता है ताकि यदि एक सत्र की सुरक्षा में सेंध लग भी जाए, तो भी अन्य पिछले और भावी चैट सेशन सुरक्षित रहें।

चैटसैक्योर को ऑरबोट के साथ मिलकर काम करने के लिए डिजाइन किया गया है, ताकि आपके चैट-मैसेजेज को टोर एनोनिमाइजिंग नेटवर्क से लेकर गुजारा जा सके। इस फीचर के चलते आपकी चैट को ट्रैस करना, यहाँ तक कि चैट हुई भी थी, का पता लगाना मुश्किल होता है। आइफोन के लिए भी, चैटसैक्योर यही फीचर उपलब्ध कराता है। हालांकि इसे टोर नेटवर्क के साथ यूज करना आसान नहीं है।

आप कोई भी एप्लीकेशन यूज करें, पर यह अवश्य ध्यान रखें कि आप किस एकाउन्ट से चैट कर रहे हैं। उदाहरण के लिए, जब आप गूगल टॉक यूज करते हैं, आपके क्रेडेन्शियल और चैटिंग सेशन का टाइम गूगल की जानकारी में रहता है। साथ ही जिससे आप चैट कर रहे हैं उससे यह करार करें कि दोनों ही चैट हिस्ट्री सेव नहीं करेंगे।

### 12.2.3.3 स्मार्टफोन पर इन्फॉर्मेशन स्टोर करना:-

स्मार्टफोनों में डाटा स्टोरेज की अच्छी-खासी क्षमता होती है। आपके फोन में स्टोर डाटा को कोई तीसरा पक्ष रिमोट ऑपरेशन से या प्रत्यक्ष तौर पर आपका फोन हासिल करके, एक्सेस कर सकता है। आप विशिष्ट टूल्स का इस्तेमाल करके अपने फोन में रखी महत्वपूर्ण जानकारी को एन्क्रिप्ट कर सकते हैं।

#### डेट एन्क्रिप्शन टूल्स

एन्ड्रॉयड प्राइवेसी गार्ड (एपीजी) फाइल्स और ई-मेल के लिए ओपन जीपीजी एनक्रिप्शन की सुविधा देता है। आप अपने फोन पर फाइलें और डॉक्यूमेंट्स सुरक्षित रखने के लिए इसका उपयोग कर सकते हैं।

#### पासवर्ड सुरक्षित रूप से रिकॉर्ड करना

आप कीपपास का इस्तेमाल करके अपनी जरूरत के सभी पासवर्ड एक सैक्योर और एनक्रिप्टेड फाइल में रख सकते हैं। आपको केवल एक मास्टर पासवर्ड याद रखना होता है, जिसके जरिए आप अन्य सभी पासवर्ड एक्सेस कर सकते हैं। कीपपास के द्वारा आप अपने हर एक एकाउन्ट के लिए बहुत मजबूत पासवर्ड इस्तेमाल कर सकते हैं क्योंकि कीपपास आपके लिए वह पासवर्ड याद रखेगा। यही नहीं कीपपास में पासवर्ड जनरेटर भी होता है जो आपके लिए पासवर्ड बनाएगा। आप कीपपास पासवर्ड डाटाबेस को अपने फोन और कम्प्यूटर के बीच सिंक्रोनाइज कर सकते हैं। हमारा सुझाव है कि आप केवल उन्हीं पासवर्ड को सिंक्रोनाइज करें जिन्हें आप दरअसल अपने फोन पर यूज करेंगे। आप अपने कम्प्यूटर पर एक छोटा पासवर्ड डाटा बेस बना सकते हैं और सारे पासवर्डों के साथ पूरे डाटाबेस जिसे आप अपने स्मार्ट फोन में

यूज करते हैं, को कॉपी करने के बजाय, इस छोटे डाटाबेस को सिंक्रोनाइज करें। साथ ही, चूंकि आपके सारे पासवर्ड मास्टर पासवर्ड के द्वारा संरक्षित हैं, इसलिए बेहतर होगा कि अपने **कीपपास** डाटाबेस के लिए अत्यन्त मजबूत पासवर्ड का इस्तेमाल करें।

#### 12.2.3.4 स्मार्ट फोन से ईमेल भेजना

इस खण्ड में हम स्मार्टफोन पर ईमेल के यूज पर संक्षिप्त में चर्चा करेंगे। सबसे पहले आप यह सोचें कि क्या स्मार्टफोन पर ईमेल पर एक्सेस करना जरुरी है। कम्प्यूटर और इसके कन्ट्रोल को सैक्योर बनाना स्मार्टफोन की तुलना में ज्यादा आसान है। स्मार्टफोन की ओरी होना, इस पर नजर रखना और इसमें सैध लगाना ज्यादा आसान है।

यदि स्मार्टफोन पर ईमेल एक्सेस करना अत्यन्त आवश्यक है तो जोखिम कम करने के लिए आप निम्नलिखित कदम उठा सकते हैं:-

- अपने स्मार्टफोन को ईमेल चैक करने और भेजने का मुख्य जरिया न बनाएं। ईमेल सर्वर से अपने स्मार्टफोन पर ईमेल न तो डाउनलोड करें और न ही स्टोर करें। केवल ईमेल की कॉपी यूज करने के लिए अपनी ईमेल एप्लीकेशन सेट-अप करें।
- यदि आप अपने कुछ कॉन्टेक्ट के साथ ईमेल एनक्रिप्शन का इस्तेमाल करते हैं, तो इसे अपने स्मार्टफोन पर भी इंस्टॉल कर लें। इसका एक अतिरिक्त फायदा यह होगा कि यदि किसी गलत हाथ में आपका फोन पड़ जाता है तब भी आपकी एनक्रिप्टेड मेल गोपनीय बनी रहेगी।

अपनी प्राइवेट एनक्रिप्शन “की” मोबाइल फोन पर स्टोर करना जोखिम भरा हो सकता है। लेकिन इससे आप मोबाइल पर सुरक्षित तरीके से एनक्रिप्टेड ईमेल भेज सकते हैं और स्टोर कर सकते हैं, तो यह फायदा उक्त जोखिम से ज्यादा बेहतर है। एपीजी का इस्तेमाल करके मोबाइल ऑनली एनक्रिप्शन की-पेयरक्रिएट करें, जो केवल आपके स्मार्टफोन पर काम करेगा और आपको कम्प्यूटर से मोबाइल पर अपनी प्राइवेट एनक्रिप्शन की कॉपी करके सेव करने की आवश्यकता नहीं होगी। ध्यान रखें कि, आप अपने कॉन्टेक्ट से आग्रह करें कि वे भी आपकी मोबाइल-ऑनली एनक्रिप्शन “की” का इस्तेमाल करके ईमेल्स एनक्रिप्ट करें।

#### 12.2.3.5 स्मार्टफोन से मीडिया कैचर करना

अपने स्मार्टफोन से महत्वपूर्ण अवसरों के पिक्चर्स, वीडियो और ऑडियो कैचर करना और इन्हें शेयर करना एक सशक्त जरिया हो सकता है। लेकिन, इन पिक्चरों की प्राइवेसी और सुरक्षा सुनिश्चित करना भी उतना ही महत्वपूर्ण है। उदाहरण के लिए यदि आप किसी महत्वपूर्ण अवसर की वीडियो अथवा ऑडियो रिकॉर्ड करते हैं और आपका फोन गलत लोगों के हाथ आ जाए तो यह आपके लिए या उन लोगों के लिए जो इस वीडियो में नजर आ रहे हैं, खतरनाक भी हो सकता है। इस स्थिति में निम्नलिखित सुझाव सहायक हो सकते हैं:-

- मीडिया फाइल्स सेक्योरली अपलोड करने के लिए अपने फोन में मैक्रोनिज्म इन्स्टॉल करें ताकि ऑनलाइन लोकेशन को गुप्त रखा जा सके या रिकॉर्डिंग के बाद फोन से तत्काल हटाया जा सके।
- वीडियो या फोटो में दिखाई देने वाले लोगों के चेहरे धूमिल करने या ऑडियो अथवा वीडियो की आवाज विकृत करने के लिए टूल्स का उपयोग करें और अपने मोबाइल फोन पर धूमिल या विकृत (डिस्टॉर्टेड) कॉपी ही सेव करें।
- मीडिया फाइल के अन्दर समय और स्थान के बारे में उपलब्ध मेटा सूचना गोपनीय रखें या हटा दें।

गार्डियन प्रोजेक्ट ने ऑब्स्क्योराकैम नाम से एक एफओएसएस ऐप बनाया है जो फोटो में चेहरों को पहचान कर धूमिल (ब्लर) कर देता है। निश्चय ही, यह आप पर निर्भर करेगा कि आप ब्लरिंग मोड चुन कर कौन से चेहरों को ब्लर करना चाहते हैं। ऑब्स्क्योराकैम ओरिजिनल फोटो को डिलीट भी करता है और यदि आपने सर्वर सेट-अप किया है तो यह कैचर्ड मीडिया को आसानी से अपलोड करने की सुविधा भी देता है।

#### **12.2.3.6 स्मार्टफोन से सुरक्षित तरीके से इन्टरनेट एक्सेस करना**

अपने इन्टरनेट कम्प्यूनिकेशन को किस प्रकार प्राइवेट बनाएं, इससे संबंधित गाइड और इन्टरनेट पर किस प्रकार गुमनाम बने रहे और सेन्शाराशेप को किस तरह बाइपास करें, इससे संबंधित गाइड में जैसी कि हमने चर्चा की है, इन्टरनेट पर कन्ट्रोल एक्सेस करने, अथवा फोटो या वीडियो ऑनलाइन अपलोड करने से आप अपने बारे में तथा अपनी लोकेशन के बारे में एवं आप अपने एक्शन के बारे में कई निशान (ट्रेसेज) छोड़ जाते हैं। ये आपको जोखिम में डाल सकता है। कम्प्यूनिकिशन के लिए मोबाइल फोन का इस्तेमाल इस जोखिम को और बढ़ा देता है।

वाई-फाई या मोबाइल डाटा के जरिए मोबाइल फोन आपको इन्टरनेट एक्सेस पर कन्ट्रोल की सुविधा देते हैं: जैसे कि एक्सेस प्वाइंट (यानि इन्टरनेट कैफे आदि) द्वारा प्रदत्त वायरलेस कनेक्शन द्वारा या मोबाइल डाटा कनेक्शन— अर्थात् मोबाइल नेटवर्क प्रोवाइडर द्वारा प्रदत्त जीपीआरएस, ईडीजीई या यूएमटीएस इत्यादि द्वारा।

यदि आप वाई-फाई कनेक्शन यूज करते हैं तो मोबाइल फोन सर्विस प्रोवाइडर के पास आपके डाटा के ट्रेस रहने की सम्भावना खत्म हो जाती है (इसके लिए आपको अपने मोबाइल फोन सब्सक्रिप्शन से फोन कनेक्ट नहीं करना है।) लेकिन, कई बार मोबाइल डाटा कनेक्शन का इस्तेमाल करना मजबूरी हो जाता है। दुर्भाग्यवश, मोबाइल डाटा कनेक्शन प्रोटोकोल (जैसे कि ईडीजीई या यूएमटीएस) ओपन स्टैन्डर्ड नहीं हैं। व्यक्तिगत डेवलपर और सिक्यूरिटी इंजीनियर यह जानने के लिए, कि मोबाइल डाटा कैरियर इन प्रोटोकोल को किस तरह लागू कर रहे हैं, इन प्रोटोकोल की जांच नहीं कर पाते।

कुछ देशों में, मोबाइल एक्सेस प्रोवाइडर के लिए अलग कानून है और इन्टरनेट सर्विस प्रोवाइडर के लिए अलग कानून हैं। इसके चलते सरकारें और कैरियर्स अपेक्षाकृत ज्यादा प्रत्यक्ष निगरानी रख सकते हैं।

अपने डिजिटल कम्यूनिकेशन के लिए आप चाहे जो भी जरिया चुनें, एनोनिमाइजिंग तथा एनक्रिप्शन टूल्स का उपयोग करके आप डाटा खुलासे के जोखिम को कम कर सकते हैं। स्मार्टफोन को अज्ञात (एनोनिमिटी) रखना, अज्ञात रह कर कन्ट्रोल ऑनलाइन एक्सेस करने के लिए, आप ऑरबोट नाम का एन्ड्रॉयड एप उपयोग कर सकते हैं। ऑरबोट आपके इन्टरनेट कनेक्शन को टोर के एनोनिमिटी नेटवर्क से चैनलाइज करता है।

एक और ऐप, **ऑरबेब**, एक वेब ब्राउजर है जिसमें प्रोक्सीज का यूज और लोकल ब्राउजिंग हिस्ट्री न रखने जैसे फीचर हैं, जो प्राइवेसी बढ़ा देते हैं। और वेब और ऑरबेट दोनों मिलकर फिल्टर्स और फायर वॉल्स को दरकिनार कर एनोनिमस ब्राउजिंग की सुविधा देते हैं।

### प्रौक्सीज

फायरफॉक्स के मोबाइल वर्जन—फायरफॉक्स मोबाइल को प्रौक्सी एड—ऑन से सज्जित किया जा सकता है, जो आपके ट्रैफिक को प्रॉक्सी सर्वर को भेजता है। वहां से आपका ट्रैफिक उस साइट को भेजा जाता है, जिस पर आप जाना चाहते हैं। ये सेन्शरशिप जैसे मामलों में सहायक हैं लेकिन यदि आपके कलाइन्ट से प्रौक्सी का कनेक्शन एनक्रिप्टेड नहीं है तो आपकी रिक्वेस्ट यानि साइट का खुलासा हो सकता है। हमारा सुझाव है कि गार्डियन पोस्ट के प्रॉक्सी मोबाइल एड ऑन का उपयोग करें, ये फायरफॉक्स के साथ प्रॉक्सी कनेक्शन को आसान बना देते हैं। फायरफॉक्स मोबाइल कम्यूनिकेशन को ऑरबोट को चैनलाइज करने और टार नेटवर्क का इस्तेमाल करने का यही एकमात्र तरीका है।

### 12.2.3.7 आधुनिक स्मार्टफोन सुरक्षा

अपने स्मार्टफोन पर पूरी एक्सेस प्राप्त करें। स्मार्टफोन निर्माता, इन स्मार्ट फोनों में ऑपरेटिंग सिस्टम, मैन्यूफैक्चरर्स (फर्मवेयर) या मोबाइल आपरेटर के प्रोग्राम इन्स्टॉल करके बाजार में उतारते हैं, लेकिन स्मार्टफोनों की क्षमता इनसे कहीं अधिक होती है। यूजर स्मार्टफोन के फक्शन्स को नियंत्रित या बदल न पाएं इसके लिए कुछ फंक्शन्स को “लॉक—इन” कर दिया जाता है, और यूजर उन तक नहीं पहुंच पाता। ज्यादातर मामलों में यह फंक्शन, यूजर्स के स्मार्टफोन में किसी काम के नहीं होते। लेकिन कुछ एप्लीकेशन और फंक्शन स्मार्टफोन पर डाटा और कम्यूनिकेशन सिक्योरिटी बढ़ाते हैं। साथ ही कुछ फंक्शन ऐसे भी हैं जिन्हें सिक्यूरिटी जोखिम कम करने के लिए हटाया जा सकता है।

इस वजह से और कुछ अन्य कारणों से कुछ स्मार्टफोन यूजर स्मार्टफोन चलाने वाले विभिन्न प्रोग्राम और सॉफ्टवेयर में फेर—बदल करना पसंद करते हैं ताकि वे बेहतर फंक्शन्स इन्स्टॉल कर सकें और कुछ अन्य को हटा सकें अथवा कम कर सकें। मोबाइल कैरियर्स अथवा स्मार्टफोन के आपरेटिंग सिस्टम निर्माता द्वारा

थोपी गई लिमिटेस से पार पाने की प्रक्रिया को रुटिंग (एन्ड्रॉयड उपकरणों के मामले में) अथवा जेल ब्रेकिंग (आईफोन अथवा आईपैड जैसे उपकरणों के आईओएस के मामलों में) कहते हैं। यदि आप रुटिंग या जेलब्रेकिंग की प्रक्रिया सफलतापूर्वक सम्पन्न कर लेते हैं तो आप अतिरिक्त एप्लीकेशन इन्स्टॉल कर पाएंगे। इनका उपयोग कर पाएंगे, “लॉक-डाउन” कन्फिगरेशन्स को बदल पाएंगे और स्मार्ट-फोन की मैमोरी तथा डाटा स्टोरेज पर आपका नियंत्रण हो जाएगा।

### चेतावनी:-

रुटिंग और जेल ब्रेकिंग प्रक्रिया रिवर्सिबल नहीं है और इसके लिए साप्टवेयर इन्स्टॉलेशन तथा कन्फिगरेशन का अनुभव होना जरूरी है। निम्नलिखित का ध्यान रखें:-

- सम्भव है कि आपका फोन रथायी रूप से काम करना बंद कर दे या इसकी ब्रिकिंग (स्मार्टफोन का डैड हो जाना) हो जाए।
- मैन्यूफैक्चरर या मोबाइल कैरियर द्वारा गारंटी बेकार हो जाए।
- कुछ जगहों में, यह प्रक्रिया गैर-कानूनी है। लेकिन यदि आप सजग हैं, तो अपने स्मार्टफोन को और ज्यादा सेक्यूर बनाने और इस पर अपना कन्ट्रोल रखने के लिए, रुटिंग सबसे सीधा रास्ता है।

### वैकल्पिक फर्मवेयर:-

फर्मवेयर उन प्रोग्राम्स को कहते हैं जो किसी खास डिवाइस से घनिष्ठता से जुड़े होते हैं। ये डिवाइस के ऑपरेटिंग सिस्टम के साथ ताल-मेल से काम करते हैं और आपके स्मार्टफोन के हार्डवेयर जैसे कि स्पीकर, माइक्रोफोन, कैमरा, टचस्क्रीन मैमोरी, की, एन्टीना आदि के बुनियादी कार्य भी ये ही संचालित करते हैं।

यदि आपके पास एन्ड्रॉयड डिवाइस है, तो शायद आप अपने फोन पर नियंत्रण बढ़ाने के लिए फर्मवेयर का कोई विकल्प इन्स्टॉल करना चाहेंगे। ध्यान रखें कि वैकल्पिक फर्मवेयर इन्स्टॉल करने के लिए आपको अपना फोन रुट करना होगा।

एन्ड्रॉयड फोन के लिए सायनोजेन मोड एक वैकल्पिक फर्मवेयर है जो आपको अपने फोन के सिस्टम लेवल से एप्लीकेशन्स (जिन्हें फोन निर्माता या मोबाइल नेटवर्क ऑपरेटर ने इन्स्टाल किया है) अनइन्स्टॉल करने की सुविधा देता है। ऐसा करके आप, आपकी जानकारी के बिना आपके सर्विस प्रोवोइडर को डाटा भेजना आदि पर रोक लगा कर, अपने डिवाइस की निगरानी के अनेक जरियों को कम कर सकते हैं।

इसके अलावा, सायनोजेन मोड के साथ बाई-डिफाल्ट एक ओपन वीपीएन एप्लीकेशन भी मिलता है, जिसे इन्स्टॉल करना थोड़ा जटिल है। वीपीएन (वर्चुअल प्राइवेट नेटवर्क) इन्टरनेट कम्यूनिकेशन को गोपनीय तरीके से प्रॉक्सी करने का एक तरीका है। (नीचे देखें) सायनोजेनमोड गुप्त मोड में ब्राउजिंग की सुविधा भी देता है, इससे आपके कम्यूनिकेशन का पिछला विवरण आपके स्मार्टफोन में रिकॉर्ड नहीं होता है।

## **पूरे डाटा स्टोरेज का एनक्रिप्शन:-**

आप फोन रुट हो जाने पर इसके सम्पूर्ण डाटा स्टोरेज का एनक्रिप्शन करने या फोन पर रखी जानकारी को संरक्षित बनाने के लिए अलग से वॉल्यूम बनाने पर भी विचार कर सकते हैं।

ल्यूक्स मैनेजर यूजर फ्रैन्डली इन्टरफ़ेस के साथ वॉल्यूम्स के आसानी से सशक्त एनक्रिप्शन की सुविधा देता है। हमारा सुझाव है कि अपने एन्ड्रॉयड फोन पर महत्वपूर्ण डाटा स्टोर करने से पहले आप यह टूल इन्स्टॉल कर लें और अपने सम्पूर्ण डाटा को स्टोर करने के लिए ल्यूक्स मैनेजर द्वारा उपलब्ध कराए गए इस एनक्रिप्टेड वॉल्यूम का इस्तेमाल करें।

## **वर्चुअल प्राइवेट नेटवर्क (वीपीएन) सिक्यूरिटी:**

वीपीएन आपके डिवाइस और वीपीएन सर्वर के बीच इन्टरनेट से होकर गुजरने वाली एक एनक्रिप्टेड टनल (सुरंग) उपलब्ध कराता है। इसे टनल इसलिए कहा जाता है क्योंकि यह सभी सर्विसेज, प्रोटोकोल और विषय-वस्तु को हाइड (छुपा देना) कर देता है, जबकि एचटीटीपीएस जैसे अन्य एनक्रिप्टेड ट्रैफ़िक में ऐसा नहीं होता है। वीपीएन कनेक्शन एक ही बार सेट-अप करना पड़ता है, और यह तभी टर्मिनेट होगा जब आप चाहेंगे।

ध्यान रखें, कि आपका सारा ट्रैफ़िक प्रॉक्सी अथवा वीपीएन सर्वर से होकर गुजरता है। आपके कार्यकलापों पर नजर रखने के लिए किसी बीच के व्यक्ति को केवल आपकी प्रॉक्सी एक्सेस करनी होगी। इसलिए जरूरी है कि प्रॉक्सी सर्विस और वीपीएन सर्वर का सावधानी से चयन करें। यह भी सुझाव है कि अलग-अलग प्रॉक्सी और/अथवा वीपीएन का इस्तेमाल करें क्योंकि अलग-अलग डाटा स्ट्रीम के लिए अलग-अलग उक्त सेवाओं का उपयोग करने से जोखिमयुक्त सर्विसेज से होने वाला नुकसान कम हो जाता है।

## **अभ्यास**

1. इन्टरनेट पर जेल ब्रेकिंग के बारे में और जानकारी जुटाएं।
2. अपनी चैट एप्लीकेशन में “ऑफ-द-रिकार्ड” ऑप्शन वाले फीचर का पता लगाएं और यूज करें और देखें की इससे क्या फर्क पड़ता है।
3. अपने मित्र को कॉल करने के लिए स्काइप डाउनलोड करें और यूज करें।
4. इन्टरनेट पर ऑब्स्क्योराकैम के बारे में और जानकारी हासिल करें।

## **अनुशंसित वीडियो**

<https://www.youtube.com/watch?v=kcobm4pbtvk>

[https://www.youtube.com/watch?v=v8bcy\\_rcqkok.](https://www.youtube.com/watch?v=v8bcy_rcqkok)