Information Security Education & Awareness

Ministry of Electronics and Information Technology
Government of India

सी डैक
CDAC

INFORMATION SECURITY AWARENESS

HANDBOOK

For Virus Alerts, Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Acknowledgement

HRD Division

Ministry of Electronics & Information Technology

Government of India

InfoSec HANDBOOK

CREDITS

Honorary Professor. N Balakrishnan
(IISc, Bangalore)
Prof. Sukumar Nandi
(IIT, Guwahati)
Prof. V Kamakoti (IIT, Madras)
Prof. M S Gaur (SVNIT, Jaipur)

Design & Technical Team
Ch A S Murty
I L Narasimha Rao
K Indra Veni
K Indra Keerthi
P S S Bharadwaj

Action Group Members
HoD (HRD), MeitY
Shri.Sitaram Chamarthy (TCS)
Prof. M S Gaur (MNIT, Jaipur)
Prof. Dr.Dhiren R Patel
(NIT Surat)
Representative of Chairman
(CBSE)
CEO, DSCI (NASSCOM)
Representative of Prasar Bharati,
Member of I & B
Shri U Rama Mohan Rao
(SP, Cyber Crimes, CID,
Hyderabad, Andhra Pradesh)
Shri S K Vyas, MeitY

Compiled by
G V Raghunathan
Ch A S Murty

From C-DAC
E Magesh, Director

Acknowledgement
HRD Division
Ministry of Electronics &
Information Technology

For Virus Alerts, Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

About C-DAC

C-DAC established its Hyderabad Centre in the year 1999 to work in Research, Development and Training activities embracing the latest Hardware & Software Technologies. The centre is a knowledge centre with the components of Knowledge Creation, Knowledge Dissemination and Knowledge Application to grow in the areas of Research & Development, Training and Business respectively. The R & D areas of the centre are e-Security, Embedded Systems, Ubiquitous Computing, e-Learning and ICT for Rural Development. The centre has developed over a period of time a number of products and solutions and has established a number of labs in cutting edge technologies. In line with these R&D strengths, the centre also offers Post Graduate level diploma courses. Centre is also actively involved in organizing faculty training programs. The centre regularly conducts skill based training and information security awareness programmes. Vikaspedia portal is hosted and maintained to facilitate rural development through provision of relevant information, products and services in local languages.

About ISEA

Looking at the growing importance for the Information Security, Ministry of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched by the Govt. of India. One of the activities under this programme is to spread Information Security Awareness among children, teachers, home users, IT and non-IT professionals throughout the country. C-DAC Hyderabad has been assigned the responsibility of executing this project by Ministry of Electronics & Information Technology, Government of India. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events, etc.,

Comments & Feedback mail us to
pmu-isea@cdac.in

Introduction

Information Security Awareness

Information security needs have to be addressed at all levels, from the individual user to an organization and beyond that to the government and the nation. Information Security is becoming synonymous with National Security as Computer Networking, which is vulnerable to Cyber attacks, forms the backbone of critical infrastructure of the country's banking, power, communication network etc.. It is, therefore, important to have secured Computer Systems and Networks. Also, increased focus on outsourcing of IT and other services from developed countries is bringing the issue of data security to the fore. Furthermore, owing to the massive Internet boom, a lot of home users with little or no prior knowledge of the threats and their countermeasures are exposed to the Internet. This, the attacker, can exploit to expand their base of malicious activity and use innocent people for their schemes. Consequently, we aim to spread the education to school children, teachers, parents and senior citizens and equip them with the knowledge needed to mitigate the threat.

Looking at the growing importance for the Information Security, Ministry of Electronics & Information Technology, Government of India has formulated and initiated the Information Security Education and Awareness (ISEA) programme. One of the activities under this programme is to widely generate information security awareness to children, home users and non-IT professionals in a planned manner.

Importance of Cyber Security

Cyber security is important for the users because they have to protect themselves against identity theft. Organizations including government also need this security to protect their trade secrets, financial information, and some sensitive or critical data. Since all sensitive information that is mostly stored on a computer that is connected to the Internet, there is a need for information assurance and security. So in order to have Cyber Security, everyone should follow the Cyber Security standards that enable us to protect various Malware threats.

A poor cyber security practice arises because of some of the following reasons. Poor administrative practices of application, poor software coding which may be vulnerable and improper usage of Cyber Security practices.

Vision

Generate information security awareness among Indian citizens
to enable them to participate safely in Information Society

Chapters

Chapters

Understanding about "the Internet"

The Internet stands for Interconnection of Computer Networks. It is a massive, heterogeneous combination of millions of computers, network devices and smart phone devices, all connected by wires and wireless signals. There are different definitions for Internet but the meaning is the same as shown below

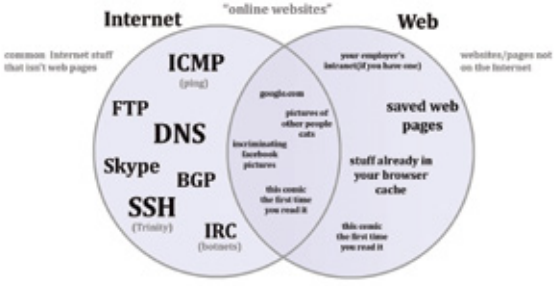
- The series of interconnected network allowing communication of data surrounded by millions of computers worldwide.
- A global communication network that allows computers worldwide to connect and exchange information.
- A worldwide system of computer network, a network of networks in which users at any one computer can get information from any other computer

The word "Internet" exactly means "network of networks". The Internet consists of thousands of smaller regional networks spread throughout the world. The Internet is referred as a physical part of the global network. It is a giant collection of cables and computers. Although it started in the 1960's as a military experiment in communication, the Internet evolved into a public free broadcast forum in the 70's and 80's. No single authority owns or controls the Internet. No one "owns" the Internet, though there are companies that help out to manage different parts of the networks that tie everything together, there is no single governing body that controls what happens on the Internet.World Wide Web (WWW)

How is the 'Internet' Different from the 'Web'?

In 1989, a large subset of the Internet was launched as the World Wide Web (www). The 'Web' is a massive collection of HTML pages that transmits through the Internet's hardware. You will hear the expressions 'Web 1.0', 'Web 2.0', and 'the Invisible Web' to describe these billions of web pages. The World Wide Web is some part of Internet as Internet is having a variety of data other than web pages.

The web is one of software application or services that run on the Internet. It is a collection of documents and resources in the form of web pages. It provides easy access to a huge range of information that is stored on computers around the world. The expressions 'Web' and 'Internet' are used interchangeably by the layperson. This is technically incorrect, as the Web is contained by the Internet.



What is 'Web 1.0', 'Web 2.0', and 'the Invisible Web'?

- **Web 1.0:** When the World Wide Web was launched in 1989 by Tim Berners-Lee, it was comprised of just text and simple graphics as a collection of electronic brochures. The Web was organized as a simple broadcast-receive format. We call this simple static format as 'Web 1.0'. Today, millions of web pages are still quite static, and the term Web 1.0 still applies.
- **Web 2.0:** In the late 1990's, the Web started to go beyond static content, and began offering interactive services. Instead of just web pages as brochures, the Web began to offer online software where people could perform tasks and receive consumer-type services. Online banking, video gaming, dating services, stocks tracking, financial planning, graphics editing, home videos, webmail services like Gmail, yahoo mail etc... all of these became regular online Web offerings around 2000. These online services are now referred to as 'Web 2.0'. Names like Facebook, Flickr, , eBay, and Gmail helped to make Web 2.0 a part of our daily lives.

The Invisible Web is a third part of World Wide Web.

Technically a subset of Web 2.0, the Invisible Web describes those billions of web pages that are purposely hidden from regular search engines. These invisible web pages are private-confidential pages (e.g. personal email, personal banking statements), and web pages generated by specialized databases (e.g. job postings in Cleveland or Seville). Invisible Web pages are either hidden completely from your casual eyes, or require special search engines to locate. Read more about Invisible Web here.

What is a web site?

Web site contains one to millions of inter connected pages, has hyperlinks to connect and help to find your way around the web site. You can find different kinds of information on the web- like games, health matters, holiday destination, train timetables, weather forecast and many more. There are millions of web sites available on the Internet, and you can find anything that interests you.

A Web Address

Each Web site has its own unique address, which is called a Uniform Resource Locator or URL. To visit a site, you need to type its address in the address bar of your web browser.

Usage of Internet

The Internet is used mainly for communication, to gather information, education, entertainment, current affairs, online learning, commerce, publishing, etc. In the usage of Internet, publishing is not just used for organization or businesses, anyone can create their own web sites and publish their information or files on the Worldwide Web.

Through the Internet, thousands of people around the world are able to access information from their homes, schools, Internet cafes and workplaces.

The Internet is a global collection of computer network, that help in exchanging data using a common software standard. Internet users can share information in a variety of forms.

- The user can connect easily through ordinary personal computers and share the knowledge, thoughts by making the use of an Internet.
- We can send electronic mail (e-Mail) to family members and friends with accounts on the Internet, which is similar to sending letters by post. The
- E-mail can be sent within minutes no matter where they are without postal stamps etc.
- We can post information that can be accessed by others and can update it frequently.
- We can access multimedia information that includes video, audio, and images.
- We can learn through Web-Based Training and Distance Learning on the Internet.

Access to Internet

The Internet is a time-efficient tool for teachers that enlarge the possibilities for curriculum growth. Learning depends on the ability to find relevant and reliable information quickly and easily, and to select, understand and assess that information. Searching for information on the Internet can help to develop these skills. Classroom exercises and take-home assessment tasks, where students are required to compare website content, are ideal for alerting students to the requirements of writing for different audiences, the purpose of particular content, identifying and judging accuracy and reliability. Since many sites adopt particular views about issues, the Internet is a useful tool for developing the skills of distinguishing fact from opinion and exploring subjectivity and objectivity.

The Internet is a great tool for developing the communication and collaboration skills of students and children. Above all, the Internet is an effective means of building language skills. Through e-Mail, chat rooms and discussion groups, students learn the basic principles of communication in the written form. This gives teachers the opportunity to incorporate Internet-based activities into normal literacy programs and bring variety to their teaching strategies.

Collaborative projects can be intended to improve students' literacy skills, generally through e-Mail messaging with their peers from other schools or even other countries. Collaborative projects are also useful for engaging students and providing significant learning experiences. In this way, the Internet becomes an effective means of advancing intercultural understanding. Moderated chat rooms and group projects can also provide students with opportunities for collaborative learning.

The Internet is a very large store room of learning material. As a result, it significantly expands the resources available to students beyond the standard print materials found in school libraries. Students can access the latest reports on government and non-government websites, including research results, scientific and artistic resources in museums and art galleries, and other organizations with information applicable to student learning. At secondary schooling levels, the Internet can be used for undertaking reasonably tricky research projects.

As Internet is a powerful resource for learning, and is an efficient means of communication, it is very useful in education and provides a number of learning benefits. It includes the development of independent learning and research skills, by improving access to specific subject learning across a wide range of learning areas, as well as in integrated or cross-curricular studies and communication and collaboration, such as the ability to use learning technologies to access resources, create resources and communicate with others.

Features of Internet

- ***Geographic sharing***
  The geographic sharing of the Internet continues to spread, around the world and even beyond. A main feature of the Internet is that once you have connected to any part of it, you can communicate with all of it.
- ***Architecture***
  The architecture of Internet is most ever communication network designed. The failure of individual computers or networks will not affect its overall reliability. The information will not change or destroy over time or while transferring in between sites.
- ***Universal Access***
  It is easy to access and make the information like text, audio, video and also accessible to a worldwide people at a very low price. Access to Internet is same to everyone no matter where they are.One can connect to any computer in the world, and you can go to many excited places without leaving your chairs.

Benefits of Internet

There are many advantages of Internet:

- *The Internet is data and information loaded, including a range of medium.*
- *The Search engines that are available online are, fast and powerful.*
- *The Internet is easy to use.*
- *Students can become researchers because of easier access to data.*
- *Students are motivated to share their work online with the world.*
- *The Internet appeals to different learning styles.*
- *Unlike paper the web can present dynamic data sources which change over time.*
- *The characters in an e-Mail don't get transposed or mixed up when they are sent over long distances.dent can access libraries around the world.*

Privacy Issues

Many children are skilled navigators of the Internet. They are comfortable using computers and are fascinated by the information and images that can be explored at the click of a mouse. Recent figures show that 90% of school-age children have access to computers either at home or at school. The ability to interact and communicate with others is one of the biggest attractions of the Internet for children. We are watching about spending time with people in chat rooms and instant messaging through mobiles, playing games, entering contests and filling forms in popular online activities. Unfortunately, most parents don't really understand how such activities can put their children's privacy at risk or even threaten their safety. Surprisingly in India, most parents never know about some of the activities that their child is participating on the Internet.

In today's Internet communications scenario, the personal data is valuable and protecting the same has become a skill that the children need to understand and learn.

The privacy of children can be compromised in certain online activities:

- ✓ *Filling forms for various surveys, contests, download games on commercial or free web sites.*
- ✓ *Giving details about personal information when registering for e-mail access, chat access.W*
- ✓ *Providing information when registering for downloads free games.*
- ✓ *Providing information when registering for social networking web sites.*

- **Privacy**
  Some websites prompt students to complete a form revealing their name, e-Mail address, age and gender, and sometimes even their telephone number and postal address, in order to access information. Some requests are legitimate: much depends on the nature of the website requesting the information. Providing personal information online can result in a student being targeted for spam (unsolicited e-Mail), advertising materials and/or viruses. Privacy issues also apply to students developing personal websites and publishing online. Personal details, including photographs of themselves or other students, may lead to the information being captured and reused by others for illicit purposes.

- **Exposing your Computer to Unwanted Software**
  Usually, many peer-to-peer file sharing programs do not employ good security or access control. If users are not familiar with the programs or if there is improper configuration of the settings, it will be dangerous for all the contents stored in user's hard disk to be exposed to other users.

- **Contracting Computer Viruses**
  Besides, the computers of P2P software users can easily contract computer viruses especially when the file downloaded is from an unknown source. Moreover, these P2P programs may also contain viruses and worms, which prevent users' computers from functioning properly.

- **Infringing Copyright**
  Many copyright laws infringing copies of entertainment files e.g. MP3 Music files, VCD video files etc. and software are often shared by P2P software. The act of unauthorized uploading of a copyright works for others to download may attract civil or even criminal sanctions. Unauthorized downloading of copyright works entails civil liability.

- **Slowing down your School Internet Speed**
  Last but not least, if you host a large amount of files for other people to download through P2P software via the School campus network, the network traffic thus created can slow down the entire campus network

Never participate in peer-to-peer (P2P) networks if you are not well-known to P2P networks

There are plenty of risks in sharing your files over peer-to-peer networks

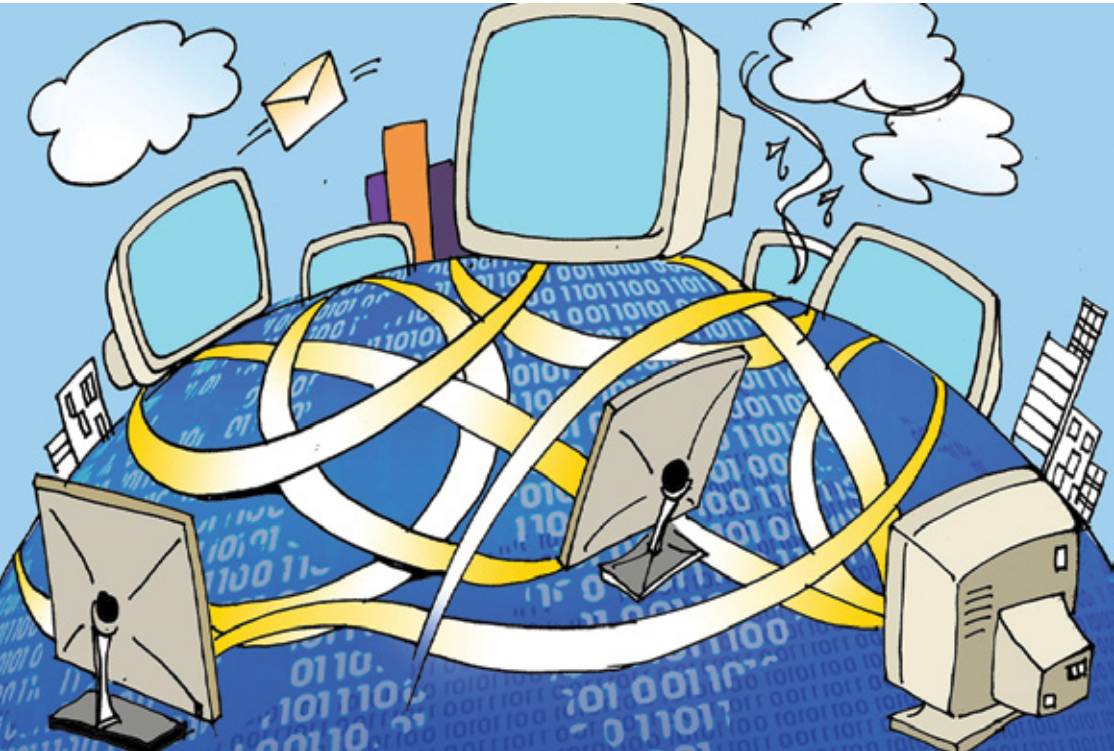
- **Peer To Peer (P2P) Networking**
  A peer to peer (or P2P) computer network uses diverse connectivity between participants in a network and the cumulative bandwidth of network participants rather than conventional centralized resources

(client-server architecture) where a relatively low number of servers provide the core services. Sharing content such as audio, video, data or any form of digital data by connecting the nodes via largely ad hoc networks.

Risks in Peer to peer networking due to their unstructured networks and sharing with unknown computers or persons may rise to affect or infect your computers with viruses, spam.

Tips for P2P Networks

- *Use filtering software you trust to filter the data communication from your system.*
- *Use file sharing program controls and adjust the P2P program to run whenever required. Disable automatic starting.*
- *Always update Operating System, Antivirus and Anti Spyware packages.*
- *Do not use an administrative account. It may expose the whole system to other users in P2P networks. Create separate account for normal operations.*
- *Treat all download files with suspicion.*
- *Take back up of important files. This will help you in recovering the files.*
- *Delete any pirated software, files, etc. Alternatively, never download them at all.*



Computer Ethics

Ethics are a set of moral principles that governs an individual or a group on what is acceptable behaviour while using a computer. Computer ethics are set of moral principles that govern the usage of computers. One of the common ethic missed by many among computer ethics is violation of copyright issues.

Duplicating the copyrighted content without the author's approval, accessing personal information of others are some of the examples that violate ethical principles.

What is the UnEethical behaviour of students/teachers?

Digital plagiarism:

Plagiarism is one of the major forms of academic dishonesty which has always existed in education, including higher education. For example, assignments submitted by students may turn out to be copied from fellow students or could be taken over, in part or in whole, from existing published works. The use of computers and Internet added to the means that students have at their disposal to commit plagiarism. However, they make it much easier to do and much harder to detect.

Breaking copyright and software theft:

Throughout the society, it is well known that the illegal copying of copyrighted media (texts, music works, movies and software programs) is widespread. Moreover, many people who engage in such activity do not consider themselves to be doing something that is immoral. This is certainly true for college students. And this attitude of students

seems to match developments in the current information age, in which the Internet increasingly functions as the most important information medium that people use.

Improper use of computer resources:
Students and staff may have authorized access to computer resources, but then go on to use these resources improperly. They may have a school/library Internet account, or they may use computer system or computer network or computer software that is owned by the school, or they may use computerized services offered by the school, and do so in a way that does not meet the school's standards for proper use of that particular resource.
For example, students may use their student account to run their own Internet business, may open up a popular website or service that generates much traffic, downloads MP3 files, staff members may use the school's server or computer systems to download or view or store content that is either illegal or against the school policies (e.g., racist or fascist materials or pornography) or members of the academic community may spread computer viruses or worms.

Securing information privacy and confidentiality:

- **Personal information on public computers:**
  While using publicly accessible computers, students or staff may unknowingly leave personal information on the public computers, such as cached web pages (accessed web pages that are left in temporary storage on the disk drive and may remain there even after a browser is closed) and cookies (small files that are put on a hard disk by a web site to identify users and their preferences), that are then available for inspection by others.

- **File sharing:**
  The computers that are used by Student or faculty may contain software that allow files from computer accessible to other users on the campus network and outside without knowledge of the owner, or they may allow files to be stored on a central server that are then accessible to others without their permission. This could allow strangers to read these files that may contain personal information.

Ensure that you have policies regarding the use of e-mail and the Internet

- **School web pages and bulletin boards:**
  Web pages maintained by the school, by faculty or by students may contain personal information that may access the privacy of others. Likewise, postings and re-postings (forwarded messages) on bulletin boards or in other electronic forums may contain personal information of third parties for which no authorization has been given.

The ten rules of computer ethics:

- One shall not use a computer to harm other people.
- One shall not interfere with other's computer work.
- One shall not snoop around in other 's computer files.
- One shall not use a computer to steal.
- One shall not use a computer to bear false witness.
- One shall not copy or use proprietary software for which one have not paid.
- One shall not use other's computer resources without authorization or proper compensation.
- One shall not appropriate other's intellectual output.
- One shall think about the social consequences of the program written or of the system designed by one.
- One shall always use a computer in ways that insure consideration and respect for one's fellow humans.

Ethical rules for the computer users

Some of the rules that the individuals should follow while using a computer are listed below:

- Do not use computers to harm other users.
- Do not use computers to steal other's information.
- Do not access files without the permission of the owner.
- Do not copy copyrighted software without the author’s permission.
- Always respect copyright laws and policies.
- Respect the privacy of others, just as you expect the same from others.
- Do not use other user's computer resources without their permission.
- Use Internet ethically.
- Complain about illegal communication and activities, if found, to Internet service Providers and local law enforcement authorities.
- Users are responsible for safeguarding their User Id and Passwords. They should not write them on paper or anywhere else for remembrance.
- Users should not intentionally use the computers to retrieve or modify the information of others, which may include password information, files, etc.

Ethics are a set of moral principles that govern an individual or a group on what is acceptable behaviour while using a computer.

Computer ethics is a set of moral principles that govern the usage of computers. One of the common issues of computer ethics is violation of copyright issues.

Internet Ethics

Internet ethics means an acceptable behaviour for using internet. We should be honest, respect the rights and property of others on the internet.

Acceptance

World Wide Web is not a waste wild web. It's place where values are considered in a broadest sense. We must take care while shaping content and services and we should recognize that internet is not apart from universal society but it is a primary component of it.

Sensitivity to National and Local cultures

It belongs to all and there is no barrier of national and local cultures. It cannot be subject to one set of values like local TV channel, a local newspaper and we have to accommodate multiplicity of usage.

While using e-Mail and chatting

Internet must be used for communication with family and friends. We should not use

the internet chatting for communicating with strangers and should not forward the e-mails from strangers. And we must teach children on risks involved by chatting or forwarding e-mails to strangers.

Pretending someone else

We must not use the internet to pretend as someone else and fool others. We must teach children that fooling others and hiding your own identity is a crime.

Avoid Bad language

We must not use rude or bad language while using e-Mail, chatting, blogging and social networking, we need to respect their views and should not criticize anyone on the internet and the same should be taught to children.

Hide personal information

We should teach children not to give personal details like home address, phone numbers, interests, passwords to anyone. No photographs should be sent to strangers and they taught to hide personal details from strangers because it might be misused and shared with others without their knowledge.

While Downloading

Internet is used to learn about music, video and games by listening to it, and learning how to play games. We must not use it for downloading them or share the copyrighted material. The same should be taught to children, and they must be aware about the importance of copyrights and issues of copyright.

Supervision

You should know what children are doing on the internet and the sites they visit on the internet and should check with whom they are communicating. Look-over their shoulder and restrict them browsing inappropriate sites. Parental involvement while a child is using the internet and helps the child to follow computer ethics.

Encourage children to use Internet

We must encourage children, students and others to gain the knowledge from the internet and use it wisely. Internet is a great tool where one can gather information which can be used for learning.

Access to Internet

The internet is a time-efficient tool for everyone that enlarges the possibilities for curriculum growth. Learning depends on the ability to find relevant and reliable information quickly and easily, and to select, understand and assess that information. Searching for information on the internet can help to develop these skills. Classroom exercises and take-home assessment tasks, where students are required to compare website content, are ideal for alerting students to the requirements of writing for different audiences, the purpose of particular content, identifying and judging accuracy and reliability. Since many sites adopt particular views about issues, the internet is a useful tool for developing the skills of distinguishing fact from opinion and exploring subjectivity and objectivity.

Cyber Ethics

Cyber ethics is a code of behaviour for moral, legal and social issues on the Internet or cyber technology. Cyber ethics also includes obeying laws that apply to online behaviour. By practising cyber ethics, one can have a safer and enjoyable Internet experience. Cyber bullying is the use of information technology to repeatedly harm or harass other people in a deliberate manner. With the increase in use of these technologies, cyber bullying has become increasingly common, especially among teenagers.

Cyber technology refers to a wide range of computing and communications devices from individual computers, to connected devices and communications technologies. Cyber ethics suggest the study of ethical issues limited to computing machines, or to computing professionals. It is more accurate than Internet ethics, which is limited only to ethical issues affecting computer networks.

Cyber Safety

Cyber safety addresses the ability to act in a safe and responsible manner on the Internet and other connected environments. These behaviours protect personal information and reputation and include safe practices to minimize danger from behavioural-based, rather than hardware/software-based, problems.

Cyber Security

Cyber safety focuses on acting safely and responsibly, whereas cyber security covers physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technology.

Safety measures for Ethics

There are four effective approaches who want to ensure they are doing the right thing online:

- Have a basic understanding of the technology
- Participate with your child online.
- Determine what standards have been established for in-school computer use.
- Create a set of rules; along with your child, relating to both ethics and safety.

As per the importance of information technology, and given the possibilities of unethical use of this technology by students and faculty, schools/colleges should ensure that they have policies regarding the use and management of information technology by students and staff.

Several ethical codes dealing with technology use exist and many schools have adopted "Acceptable Use Policies" that include rules for the proper use of information technologies. Teachers, students, and parents need to know and understand these ethical codes.

For children, the major issues surrounding technology ethics can be categorized into three areas: privacy, property, and appropriate use. School related cases can be found in each of these areas.

Teachers need to develop learning objectives and activities that specifically address technology ethics. Proper use needs to be taught at the same time that other computer skills are taught. Students understanding of ethical concepts need to be assessed. Technology use privileges, especially those involving on-line use, should not be given to students until the assessments show that a student knows and can apply ethical standards and school policies.

In schools, one should have an Acceptable User Policy. An "Acceptable Use Policy" that describes the use of the Internet and other information technologies and networks in a school. The rules in these policies often apply to both staff and students. Everyone in the school, as well as parents, needs to know and understand these policies.

An Acceptable User Policy may contain

- *Not using the service as part of violating any law*
- *Not attempting to break the security of any computer network or user*
- *Not posting commercial messages to school groups without prior permission*
- *Not attempting to send junk e-mail or spam to anyone who doesn't want to receive it*
- *Not attempting to mail bomb a site with mass amounts of e-mail in order to flood their server*
- *Do not use computer technology to cause interference in other users' work.*
- *Do not use computer technology to steal information*

Cyber Bullying

Cyberbullying is when the Internet and related technologies are used to bully other people, in a planned, repeated, and hostile manner. This could be done via:

- Text messages or images,
- personal remarks posted online,
- hate speeches,
- making others to dislike and gang up on the target by making them the subject of ridicule in forums, and
- Posting false statements in order to humiliate or disturb another person.

Cyberbullies may also disclose victims' personal data (e.g. real name, address, or workplace/schools) on websites. Cases of piggy-backing on victim's identity are now common. This could be used to publish objectionable material in their name that defames or ridicules a subject.

Under the Indian law, cyberbullying is covered by section 66A of the Information Technology Act. This section is titled "Punishment for sending offensive messages through communication service, etc." This section provides for imprisonment up to 3 years and fine. Section 66A penalizes the following being sent through email, sms etc:

- Information that is grossly offensive or has menacing character; or
- False information sent for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will.

This section also penalizes the sending of emails (this would include attachments in text, image, audio, video as well as any additional electronic record transmitted with the message.) for the following purposes:

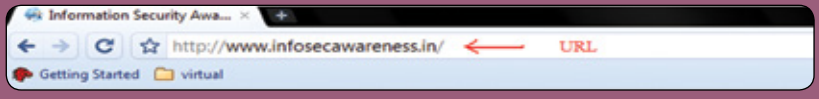
- Causing annoyance, or
- Causing inconvenience, or
- To deceive or to mislead about the origin of the messages.

Browser Security

What is Web Browser ?

Web browser is used to access the information and resources on the World Wide Web. It is a software application used to trace and display the web pages .The main purpose of a web browser is to bring the information resources to the user. An information resource is identified by a Uniform Resource Identifier/Locator (URI/URL) and may be a web page, image, video or other piece of content. Web browsers are used not only on the personal computers, laptops but are also used on mobile phones to access the information.

Uniform Resource Locator (URL)



The URL looks like http://www.infosecawareness.in

Each URL is divided into different sections as shown below :

http:// In short, http means the hypertext transfer protocol and the file is a web page and every time you don't needed to type the http, it is automatically inserted by the browser.

www– notation used for World Wide Web

infosecawareness – web site name
Other domain names are .com (commercial organization), .net (network domain) etc.

(The organization address and location of the organization address are known as the domain name).

co.in –suffix or global domain name shows the type of organization address and the origin of the country like the suffix co.in indicates a company in India.
Generally a web browser connects to the web server and retrieves the information. Each web server contains the IP address, and once you are connected to the web server by using http, it reads the hyper text mark-up language (HTML) which is a language used to create document on World Wide Web and the same document is displayed in the web browser.
In short, a browser is an application that provides a way to look at and interact with all the information on the World Wide Web.

Types of Web Browsers

There are different types of web browsers available with different features.

Some of the popular Web Browsers are :

- **Internet Explorer:**
  It is known as Microsoft Internet Explorer in short IE. It comes pre-installed on all Windows computers. It is one of the most popular web browsers and latest edition of IE 11 is available on the Internet. It can be installed with the following: windows operating system like Windows 7, Windows 8, Windows Vista and Windows Server's.

- **Mozilla Firefox:**
  It is a free, open source web browser developed by Mozilla Corporation. It has been said as being stable and safer, less prone to security breaches, viruses, and malware than Microsoft Internet Explorer. The browser can be used in different operating systems like Windows, Linux and Apple MAC operating system etc.

- **Google Chrome:**
  It is a web browser designed for windows operating system. This browser works on windows vista, windows 7 and windows 8. The chrome can be downloaded and installed for OS X or Linux operating system

- **Safari:**
  It is web browser developed by Apple Corporation. It is a default web browser of MAC OS X. This browser also works on all windows flavours. Apple maintains a plug-in blacklist that it can remotely update to prevent potentially dangerous or vulnerable plug-ins from running.

Always use the latest updated browsers

Why to secure your Web Browser ?

Today, web browsers such as Internet Explorer, Mozilla Firefox, Google Chrome and Apple Safari are installed on almost all computers. And it is easy to notice the increasing threat coming from online criminals that try to take advantage of web browsers and their vulnerabilities. Because web browsers are used so frequently, it is very important to configure them securely. Often, the web browser that comes with an operating system in a default settings not set up in a secure configuration.

Securing browser is the first step that need to be taken in order to assure secure online protection. There is an increase in number of threats taking advantage of vulnerabilities present in the web browsers through use of malicious websites. This problem is made worse by a number of factors, including the following:

- Many computer users are not aware of the click on the web links.
- Software and third party software packages installed combined increases the number of vulnerabilities
- Many websites require that users enable features or install more software, third-party software which doesn't get security updates putting the computer at additional risk.
- Many users do not know how to configure their web browsers securely.

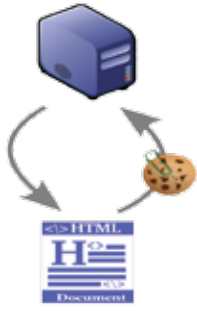
Web Browser Risks and Case Studies

Browsers are used to access various web pages to have a complete online experience. The browsers are enabled by default with some of the features to improve our online sessions, but at the same time these options create a big security risk for our operating systems and databases. The online criminals use available vulnerabilities in our browser and in its additional features to control operating systems, retrieve private data, damage important system files or install data stealing software.

Some of the features are important for browser's functionality and the user should understand their importance and should enable or disable for securing the browser.

Browser Cookies:

A cookie is used to identify a website user. A cookie is a small piece of text sent to a browser by a website accessed through the browser. It contains information about that visit like remembering the website visited preferred language and other settings. The browser stores this data and uses it in accessing the features of the website or the next time the same site is visited to make the access more personalized. If a website uses cookies for authentication, then an attacker may be able to obtain unauthorized access to that site by obtaining the cookie.



- ***Case 1:***
  Shania visited a movie website and indicated that she is interested in comedies. The cookies sent by the website remembered her choice and when she visited the same website next time, she sees comedies are displayed on the website.

- ***Case 2:***
  When users log in to a Web site, they enter their username and password into a login page and, if they are authenticated, a cookie is saved that allows the Web site to know the users are already logged in as they navigate around the site. This permits them access to any functionality that may be available only to logged-in users, probably the primary use of cookies at this time.

- ***Case 3:***
  Online shopping carts also use cookies. As you browse for DVDs on that movie shopping site, for instance, you may notice that you can add them to your shopping cart without logging in. Your shopping cart doesn't "forget" the DVDs, even as you hop around from page to page on the shopping site, because they're preserved through browser cookies. Cookies can be used in online advertising as well, to remember your interests and show you related ads as you surf the web.

Pop-ups:

Pop upsare a small window pane that opens automatically on your browser. Generally, they show advertising, which can be from legitimate company, but also may be scams or dangerous software. It works when certain websites are opened. Pop-up ads can be part of a phishing scam designed to trap you into revealing your personal or financial information as you visit web sites. Pop-ups mislead you to click the buttons on the pop-up window. But sometimes advertisers create a pop-up window that look similar to a close or cancel option so whenever user choose such options the button performs an unexpected action like opening another pop-up window, performing unauthorized commands on your system.

Not all pop-ups are bad some web sites use pop-up windows for particular tasks. You might have to view the window in order to complete that task.

- ***Case 4:***
  Sarah was listening music online from XYZ@music.com, after some couple of hours later I came across a Pop-up which tells to download the latest songs with only one click. I filled the form displayed in my browser download section. After a month I saw my credit card bill information which is showing some unauthorized charges. I was very upset and surprised, called repeatedly to that particular website where I have downloaded the songs but it was of no use.

Scripts:

Scripts are used to create websites more interactive. It is most commonly used as part of web browsers, whose implementations allow client-side scripts to interact with the user, control the browser, communicate asynchronously, and alter the document content that is displayed. There are specifications in the JavaScript standard that limit certain features such as accessing local files.

The same script can be used for inclusion of malicious code which takes control of the web browser there in by allowing to access the files of the system. It may cause damage to the system by accessing the vulnerabilities in the browser.

- ***Case 5:***
  Chintu used to visit at Internet for regular updates for his school work and playing games and listening music. When playing the games I found some news popping about Lady Gaga found dead. When I click on the BBC site a survey dialog is pop out and prompt user to complete a survey form. In the respective survey form it was written "If you are true fan on Lady Gaga" Click for Like Button. As soon as survey completed I returned back to my account homepage and posted the same link for the news to be known for my family and friends.

Plug-ins:

Plug ins is the in-built applications for use in the web browser and Netscape web browser had developed the NPAPI standard for developing plug-ins. Later this standard is used by many web browsers. Plug-ins are same to ActiveX controls but cannot be executed outside of a web browser. Adobe Flash is an example of an application that is available as a plug-in inside the web browser.

- ***Case 6:***
  For example, users may download and install a plug-in like Adobe Flash Player to view a web page which contains a video or an interactive game. But the plugin may be installed with a key logger which captures all the key strokes of the user typing in the browser and send it to the attacker.

Browser Extensions let you add new features to your browser exactly like extending your browser for customising your browser with the features that are mainly important to you. In the other words you can say adding new superpowers to the browser. For example, you may install a currency converter extension that shows up as a new key next to your browser's address bar. Click the button and it converts all the prices on your present web page into any currency that you give.

Adding more code to the browser also added to security concerns, as it gave attackers more chances to exploit the browser. Because the code was sometimes hidden, extensions were notorious for causing browser crashes as well.

How to secure your Web Browser ?

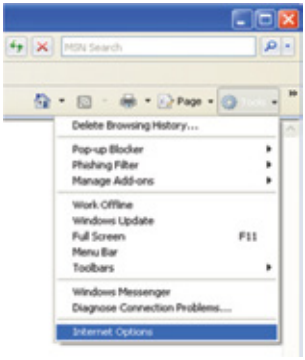
By default web browser comes with an operating system and it is setup with default configuration which doesn't have all secure features enabled in it. Not securing web browser leads to problems caused by anything like spyware, malware, viruses, worms etc being installed in to a computer and this may cause intruders to take control over your computer.

There is a raise of threat from software attacks which may take advantage of vulnerable web browsers. Some software of a web browser like java script, Active X etc may also be the cause for the vulnerabilities in the computer system. So it is important to enable security features in your web browser to minimize the risk to the computer.

Security zone

Security zone in an Internet web browser lets you to secure the browser and offer to trust the people, companies on the Internet. This helps to decide and adds which

sites to be allowed to run the application, scripts, add-ons, install plug-in on your computer .Security zone also contains other features like adding address of web sites under restricted sites this feature is available in Internet explorer and block the untrusted sites or attack sites this feature is available in Firefox, these vary with different web browser.



Trusted site

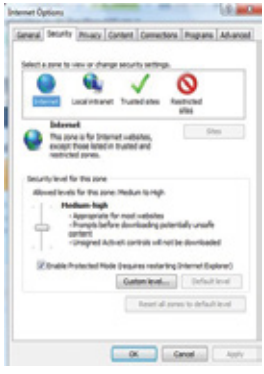
Internet is a network of people, with all kinds of stuff for different kinds of people through various websites. Generally you don't trust everyone around you so why to trust all the web sites? Also why should you allow everyone to come into your computer without your authorization? Using the feature of trusted sites in your web browser will help you to decide whom to trust.

Windows® Internet Explorer

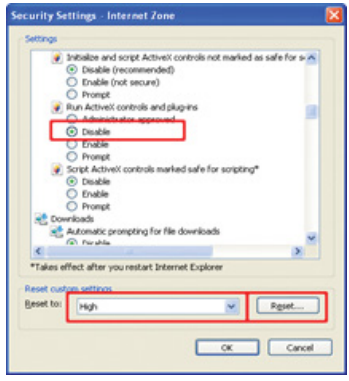
Internet Explorer

The following are the some of the features and their settings of Internet explorer

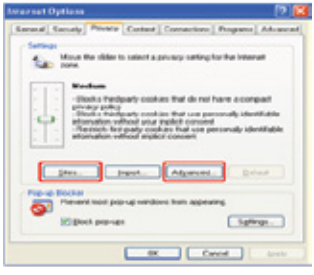
- In order to change settings for Internet Explorer, select Tools.
- From the tools menu of Internet explorer select the Internet options and then click on the security tab, check the current security settings and change the settings of security zone as necessary.
- To change the security setting under security level move the slider up to increase the security level and down to, medium, and low levels.
- For more settings and controls click on the custom level and then select the options you want
- From the tools menu option if required there is an option for: Delete browsing history which deletes all the cookies, temp files, history, active x filtering and more as shown in the figure
- To add or remove trusted or restricted web sites ,click on the sites option and then click on the add or remove button and enter your list of sites for the selected zone



- The Privacy button contains settings for cookies. Cookies are text files placed on your computer browser by various sites that you visit either directly or indirectly through third party web sites.
- From the Advanced button and select override automatic cookie handling. Then select Prompt for both first and third-party cookies. This will prompt you each time a site tries to place a cookie on your machine.
- From the menu select tools and choose the smart screen filter and click on the turn on smart screen filter and enable the smart screen filter which is recommended, this option is used to "Avoid phishing scams and malware"



- From the tools menu select the option in private filtering settings, this option is used for "Browse privately" which doesn't store any browsing history
- In the tools menu there is an option called tracking protection which protect your information like if some websites try to track your visits to those websites or any of your personal information such information would be stopped. This feature works based on the add-ons we install.
- Enable the protected mode by this option all the web sites are opened in protected mode.
- Select the advanced tab and select the options as you want like enable " Use SSL 3.0, Use TLS 1.0 "

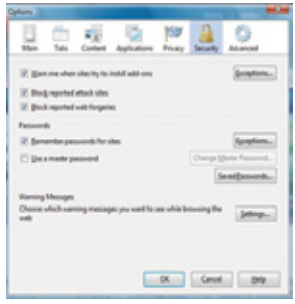


Mozilla Firefox

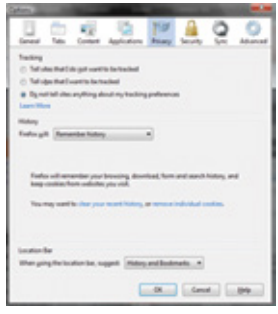
The following are the features and their setting of Mozilla Firefox web browser.

- Security settings in a Firefox control the level of examination you'd like Firefox to give a site and enter exceptions—sites that don't need the third degree. Customize settings for passwords, cookies, loading images and installing add-ons for a fully

empowered Web experience as shown below



- From the tools menu of the Firefox browser select the options and then click on the security tab
- Under security tab enable the options like warn me when sites try to install the add-ons in and to add or remove the sites click on the exception tab and add or remove the sites you want
- Enable the option tell me if the site I'm visiting is a suspected attack site
- Enable the option tell me if the site I am using is a suspected forgery Firefox gets a fresh update of web forgery sites 48 times in a day, so if you try to visit a fraudulent site that's pretending to be a site you trust a browser prompts you message and will stop you



- Disable the option remember passwords for sites Firefox integrated the feature into your surfing experience. Choose to "remember" site passwords without intrusive pop-ups.
- Select the advanced tab and enable the encryption tab in order to have a secure data transfer and use SSL 3.0
- The other feature is automated updates this lets us to find the security issues and fix updates and make the safe surfing and receive automatic notification or wait until you are ready
- One more feature is tracking which is under options privacy it stops the activities you do from the browser and we can choose the option do not tell sites anything about my tracking preferences which will not track and don't share the information to other websites.

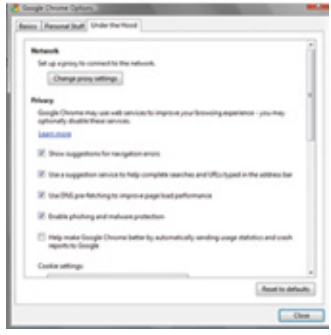
Google Chrome

From the setting menu select the Incognito window a new window appears and pages you view from this window won't appear in your web browser history or search history and they won't leave any traces like cookies after you close the incognito window any files you download or bookmarks will be preserved.

Chrome there is a new feature that it has an own Task Manager that shows you how much memory and CPU usage each tab and plug-in is using.

The safe browsing feature in the Google Chrome displays the warning if the web address listed in the certificate doesn't match the address of the website .The following are the steps for a safe browsing setting in Google Chrome.

From the settings tab select the options and click on the under the hood



- Enable the option use a suggestion service to help complete searches and URLS typed in the address bar.
- Enable DNS pre-fetching to improve page load performance
- Enable the phishing and malware protection
- Under cookies select the "Restrict how third party cookies can be used" only first-party cookie information is sent to the website.
- Under minor tweaks enable the enable the never save passwords
- Under computer wide SSL settings enable the option use SSL 2.0

Apple safari:

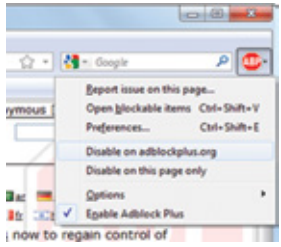
The following are the features of Apple safari secure web browser

- **Phishing Protection**
  Safari protects you from fraudulent Internet sites. When you visit a suspicious site, Safari warns you about its suspect nature and prevents the page from loading.
- **Malware Protection**
  Safari recognizes websites that harbour malware before you visit them. If Safari identifies a dangerous page, it warns you about the suspect nature of the site.
- **Antivirus Integration**
  Thanks to support for Windows Attachment Monitor, Safari notifies your antivirus software whenever you download a file, image, application, or other item. This allows the antivirus software to scan each download for viruses and malware.
- **Secure Encryption**
  To prevent eavesdropping, forgery, and digital tampering, Safari uses encryption technology to secure your web communications. Safari supports the very latest security standards, including SSL versions 2 and 3, Transport Layer Security (TLS), 40- and 128-bit SSL encryption, and signed Java applications.
- **Automatic Updates**
  Get quick, easy access to the latest security updates. Safari takes advantage of Apple Software Update, which checks for the latest versions of Safari when you're on the Internet.
- **Pop-Up Blocking**
  By default, Safari intelligently blocks all unprompted pop-up and pop-under windows, so you can avoid distracting advertisements while you browse.

- **Cookie Blocking**
  Some companies track the cookies generated by the websites you visit, so they can gather and sell information about your web activity. Safari is the first browser that blocks these tracking cookies by default, better protecting your privacy. Safari accepts cookies only from your current domain.

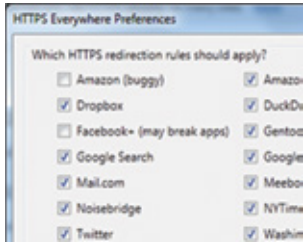
Security Extensions in Browsers

AdBlock Plus (Firefox/Chrome)



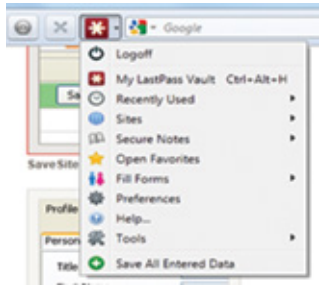
21 AdBlock, as its name would imply, blocks certain scripts serving advertisements on a website. As we've mentioned before, you can tweak ABP for added security benefit by using a "malicious ad" blocklist. You can, of course, whitelist sites you want to support (ahem), but ABP also provides the more obvious aesthetic benefit of a web less cluttered with ads.

HTTPS Everywhere (Firefox)



HTTPS Everywhere from the Electronic Freedom Foundation will help you to secure the connection between your browser and the servers it is connecting to. It helps to encrypt your connection when possible, even when the default setting on the web site does not offer the added security. A good example is Twitter. The username and password input boxes are encrypted, but after that all text coming to or from the server is sent in the clear. (Very recently, Facebook added an option to always turn on HTTPS. Here's how to do that.) HTTPS Everywhere even helps to protect against hacking tools such as Firesheep.

LastPass (All Platforms)



LastPass secures another vector that hackers can use to try to gain access to your personal information - your password. When you use the LastPass browser plugin, it stores your password, encrypted, for you and also allows you to easily generate a complicated and hard-to-crack password that is unique to a site. LastPass has plug-in available for every browser under the sun. If you're just getting started with LastPass, here's our introduction to LastPass, our intermediate guide, and a guide to auditing and updating your passwords with Last Pass.

NoScript (Firefox)

NoScript is a Firefox-only plugin that does one thing and does one thing well—it

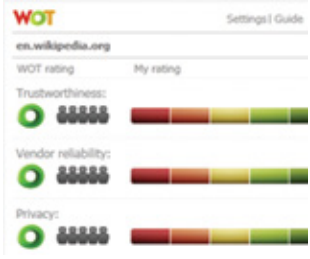
blocks scripts such as JavaScript, Flash, Quicktime, and more from loading in your browser window. (Chrome users may want to check out the similar Chrome extension, NotScripts.) The reason it works so well for security purposes is that malicious web sites can use these scripts as attack vectors in order to cause a browser crash and to gain access to your computer. By blocking these scripts you can make yourself significantly safer on the web.

Keep in mind that for most of us, blocking all scripts would result in a fairly broken internet, given that many websites, such as Google, Gmail, Twitter, Life hacker and others rely on JavaScript to load their pages. No Script allows you to block 3rd-party scripts or even just from unsafe domains. You can manage these settings in detail, giving you the maximum security with minimum inconvenience.

Web of Trust (All Browsers)

Web of Trust is another plug-in that does something different than the above. Instead of halting any attack vectors, it lets you know when the website you are visiting is trustworthy or not. That way if you happen across a website that you think is trustworthy and even look it, you get a warning that you should not submit your personal information to the site.

They rely on user-ratings to rate their site and in my experience it has been very accurate and useful.



Note: Add the above extension only through the browsers extensions

Tips

- *Always use the secured web browser to avoid the risks .Using secure browser we can gain access the information and resources that are available on the Internet and can have safe browsing over Internet.*
- *To avoid your PC being compromised and becoming a weapon to attack other machines, web browser and the Internet users are advised to: ensure that your operating system and key system components such as the web browser is fully patched and up to date.*
- *Install a personal firewall along with anti-virus software with the latest virus signatures that can detect malware such as key loggers.*
- *Regularly change your passwords with the combinations of letters, numbers and special case characters in critical web applications if a one-time password system is not supported.*
- *Turn off all JavaScript or ActiveX support in your web browser before you visit any unknown websites.*
- *Most vendors give you the option to download their browsers directly from their websites. Make sure to verify the authenticity of the site before downloading any files.*
- *To additional minimize risk; follow the latest good security practices, like using a personal firewall, Updating to the latest browser with security patches installed and keeping anti-virus software up to date with regular scanning the entire system.*

Filtering Services

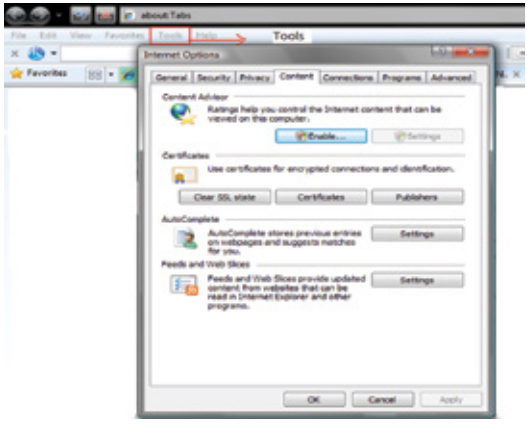
The content filtering over the Internet sometimes called parental controls, these are used to block any access to offensive websites. It is not guaranteed but it can be very helpful.

What is content filtering?
People find some inappropriate content like images of sex, violence or strong language on the Internet.

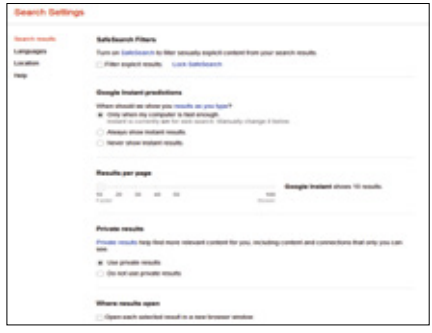
As Internet is a free zone anyone can post anything and there is no effective restriction on the Internet itself. As a result, many people use content filtering software and set browser settings to block offensive websites.

In Internet Explorer, there is an option to restrict the web sites and access only those web sites set by a user.

- In Internet Explorer web browser select tools → Internet options→Selectcontent → Click enable



- In Google search engine there is option for a safe search filtering Click on search settings →search settings → SafeSearch Filters and select desired options



- In Yahoo search engine there is option for a safe search filtering Click on Advanced → Select desired option

- Remember none of these filtering features are 100 % accurate- and some unsuitable content may still slip through.
- It is important to teach your children to surf the web safely and take time to explore the Internet with them.

Parental Control Bars

Parental Control Bar is a simple, powerful tool to help shield your children from explicit websites. Simply activate Child-Mode while your children surf the Internet, and the toolbar will block access to adult-oriented websites. Ensure that your child is safe while using the Internet. Parental controls will provide you with the advantage of being able to do the following

- Enforce time limits to child Internet activity set by parent.
- Block access to materials (pictures) identified as inappropriate for kids.
- Monitor your child's activity on the Internet by storing names of sites and/or snapshots of material seen by your child on the computer for you to view later.
- Set different restrictions for each family member.
- Limit results of an Internet search to content appropriate for kids.

Parental control Bars in Web Browsers

- **Internet Explorer**

  The Parental Control Bar in Windows vista OS supports for Internet Explored by default. For information on setting up parental controls in Windows Vista. Open Parental Controls by clicking the start button, clicking Control Panel, under User accounts, clicking Setup Parental Controls. If you are prompted for an administrator password or confirmation, type the password or provide confirmation. Then click the standard user account for which to set Parental Controls Under Parental Controls, Click On.

  Once you've turned on Parental Controls for your child's standard user account, you can adjust the individual settings that you want to control. You can control the following areas like web restrictions, time limits , games, can block specific programs.

  Third party parental control bar tools can be downloaded from the following links. Go to following website and download
  http://www.ieaddons.com/en/details/Security/ParentalControl_Bar/

- **Firefox Browser in Windows**

  There are many Firefox addons or extensions, which we can download from
  https://addons.mozilla.org/en-US/firefox/search?q=parental+control&cat=all
  Some of the products/addons for Firefox

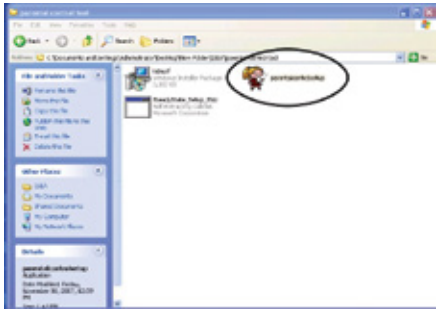
- **Glubble for Families**
  Glubble allows you to create a private family page where you can monitor and support your children's online activities. Glubble provides games, chat, safe surfing, and a Family Photo Timeline service for uploading, storing, and sharing your photos online. Glubble integrates Ask for Kids, a safe search engine for children.
  https://addons.mozilla.org/firefox/addon/5881

- **ProCon filters**
  Web page content by using a list of inappropriate words and replacing them with asterisks (***). Note that the bad word filter does not block websites containing the words; you must add the website to a Blacklist. ProCon can also block all traffic, making sure that only desired websites (set in the Whitelist) can be accessed. You can manage "white" and "black" lists of sites and pages. ProCon also has password protection in order to keep others from changing the settings

- **ProCon Latte**
  In addition to Firefox extensions, there are many third-party software packagesthat can filter content through your operating system or at the point where your network connects to the Internet.
  Available: https://addons.mozilla.org/firefox/addon/1803

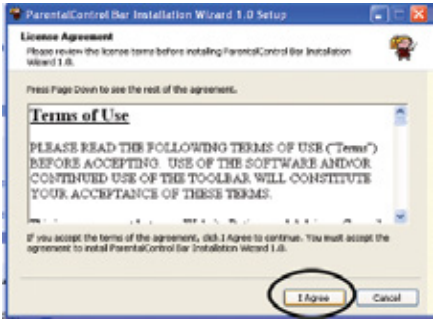
Procedure for installing Parental control toolbar.

- Double "click parental control setup downloaded" from the website.

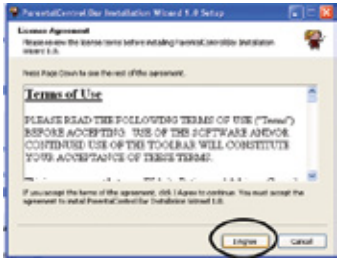


- After double clicking, it will ask to close any other browser windows. Click 'OK' button.

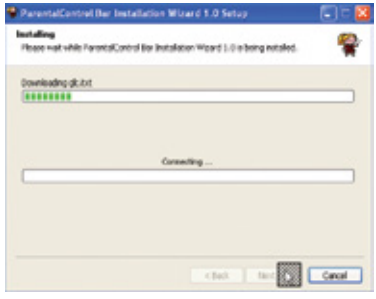
- Click 'I agree' button to agree the license agreement.



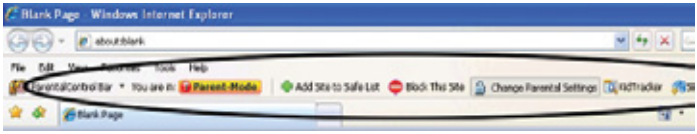
- The wizard asks for the parental control password which will be used to manage parental control settings



- Type the password and enter a question which will be used as a hint when you forget the password typed earlier. Be sure that your child doesn't know the answer for the question.
- Type the e-Mail address, to which the parental password will be sent and click 'Next'.



- Next the installation starts by taking appropriate files from the website and completes with in a few minutes.
- The parental control bar will be added to the Internet Explorer browser as shown above



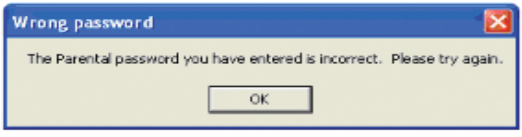
- Below shows the 'parent' button showing that the browser is acting in 'parent' mode.

- Type the website that you want to block for children and click the button 'Block this site'.

- To block this site parental control bar asks password

- After entering the password and clicking OK. A window opens telling that the site is blocked.

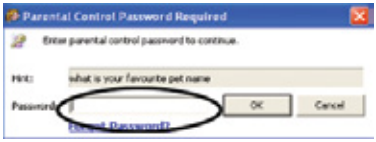
- Whenever child wants to browse the website, the browser should be in child mode. So click 'parent mode' button, so that the browser is changed to child mode. Then the parent control toolbar appears as shown below telling that child safe mode is now active.
- Click 'ok'.
- When the child wants to browse the blocked site, it asks for the password to open the site which is shown as below.
- Now if the child wants to view the website without entering password, an error occurs like this

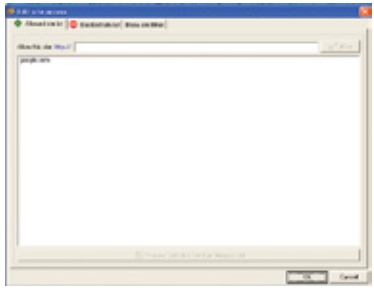


Changing the parental control settings in the parental control toolbar

- To change settings for allowing and blocking websites, click the 'change parental settings'.

- After clicking change parental settings, a window opens and asks for the 'parent control password'.
- Type the password and click 'ok'. After that a window opens

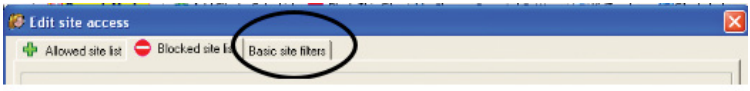




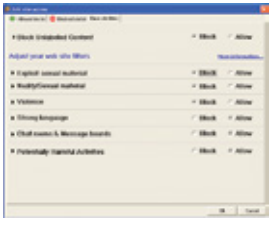
- You can add sites in the allowed list by clicking the 'allowed site list' tab

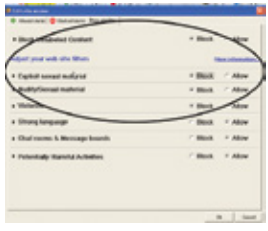
- Type the website that you want to allow and click 'allow' button as shown below.
- You can also add sites in the blocked list by clicking 'blocked site list'.
- Type the website that you want to block and click 'block' button as shown in the below figure.

- You can also filter some type of contents by clicking 'basic site filters' tab.



- The following window appears after click the 'Basic site filters' tab.
- By default, the following types of sites are filtered.
- You can also block other types of sites by checking the 'block' button.





Spam filter

Along with the content filter and website filter nowadays all the e-Mail services providers are built with spam filter.

Click on the spam filter option and add e-Mail ID which you feel not a trusted ID or e-Mail ID of an unknown user.

What is K9 Web Protection ?

K9 Web Protection is a parental control and web filtering software. When you have it turned on, it prevents the computer user from viewing Web sites that contain unwanted content. It can block more than 60 different categories of content, including pornography, hate/racism/violence, gambling and malware/spyware.

Download Link

http://www1.k9webprotection.com/get-k9-web-protection-free

My kids wouldn't go looking for those kinds of sites. Why do I need K9 Web Protection ?

Even when they don't intend to, most children run into pornography, gambling and even predators on the Internet. Consider these statistics:

70 percent of all 15-17 year-olds who have ever gone online have accidentally stumbled across pornography online, 23 percent "very" or "somewhat" often. One in five children ages 10-17 have received a sexual solicitation over the Internet. 43 percent of children said they do not have rules about Internet use in their homes.

17 percent of parents believe their children are posting online profiles, as compared to 45 percent of children who report doing this. We don't want to sound alarmist, but the kinds of material available today on the Internet are nothing like the Playboy magazine of your childhood. The pornography is far more explicit and much of it promotes pedophilia or a connection between violence and sex.

Addictive gambling among teenagers is a growing problem, and many of them are learning to gamble online. Web filtering software can keep them from getting started. Social networking sites, such as Facebook or MySpace, can also pose a real danger for children. On these sites, teenagers and even pre-teens post personal information and photographs. These sites are a gold mine for predators.

What kind of computer do I need ?

K9 Web protection runs on all recent versions of Windows or Mac computers. K9 works no matter what Internet Service Provider delivers your Internet connection, and no matter which browser you use and supports all types of windows versions.

Can my kids turn it off ?

When you install the software on your computer, you will be asked to create a password. Only someone with the correct password can turn K9 off.

What kind of computer do I need ?

A "Block" Web page is displayed that tells you that this site is not permitted by your filtering software. If you want, you can also set K9 up so that Zander, the K9 Watch Dog, will bark. (This feature is nifty for parents. If you hear Zander barking, you can be pretty sure your kid has just clicked on a site that's a no-no.)

How does K9 Work ?

We maintain a database of Web sites that contain pornography, hate speech, violence, gambling and more than 55 other categories. When a computer user tries to go to a site that's in a category you want blocked, the "prohibited" screen appears, and Zander the K9 Watch Dog barks. (You can turn off the bark.) If a user tries to go to a Web site that the database hasn't seen before, it scans the content of the site for inappropriate material, and then either permits or prohibits the site (we call this process DRTR -- Dynamic Real-Time Rating). This happens so quickly that the user doesn't realize its happening. New prohibited Web sites are added to the database.

What's the difference between K9 and other filtering software ?

One difference between K9 and many other filtering solutions is that K9 is Internet-provider-independent and browser-independent. It will run on any Windows or Mac computer, no matter what Internet Service Provider delivers your Internet connection. It also works with any Internet browser.

Another difference is that K9 uses a commercial-grade filtering solution – it's a combination of a central database and dynamic page-rating technology that has been tested against the biggest players in the business, and come up on top. We see anywhere from 250 to 500 million rating requests every day. That's a lot of Internet visibility. The result is that you get the benefits of a serious solution in an easy-to-use package. Another difference is that K9 doesn't have to be "trained." You don't have to teach it which kinds of Web sites you want to block. It starts working as soon as you install it.

Reference:

http://www1.k9webprotection.com/

Internet Communication Media

The mass media are diversified media technologies that are intended to reach a large audience by mass communication. The technology through which this communication takes place varies. Broadcast media such as radio, recorded music, film and television transmit their information electronically. Print media use a physical object such as a newspaper, book, pamphlet or comics, to distribute their information. Outdoor media are a form of mass media that comprises billboards, signs, or placards placed inside and outside of commercial buildings, sports stadiums, shops, and buses. The Internet media Communication which is largest mass media by Internet technologies for various communications in both Internet and mobile networks.

An Internet media type is a standard identifier used on the Internet to indicate the type of data that a file contains. Common uses include the following:

- e-mail clients use them to identify attachment files,
- Web Browsers use them to determine how to display or output files that are not in HTML format,
- Search Engines use them to classify data files on the web E-Mail Security

E-Mail Security

e-Mail is a short form of electronic mail. It is one of the widely used services on the Internet. e-Mail is used for transmission of messages in a text format over the Internet. The message can be sent by using the receiver e-Mail address and vice versa. e-Mail can be sent to any number of users at a time it takes only few minutes to reach the destination. E-Mail consists of two components; the message header contains control information, an originator's e-Mail address and one or more recipient addresses and message body, which is the e-mail content.

Some e-Mail systems are confined to a single computer system or to a small network, and they are connected to the other e-Mail systems through the gateway, which enables the users to connect to anywhere in the world. Though different electronic mail systems have different formats, there are some emerging standards like MAPI, X.400 that enables the users to send messages in between different electronic mail systems.

MAPI is a Mail Application Programming Interface, system built in Windows, which allow different mail applications working together for distributing mails. Until MAPI is enabled on both the application's the users can share mails with each other.

X.400 is the universal protocol that provides a standard format for all e-Mail messages. X.500 is an extension to X.400 standard, which provides standard addressing formats for sending e-Mails so that all e-Mail systems are linked to one another.

How an e-Mail works?

There are 3 main types of email servers:

POP3: Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline. Note, that when you use POP3 to connect to your email account, messages are downloaded locally and removed from the servers. This means that if you access your account from multiple locations, that may not be the best option for you. On the other hand, if you use POP3, your messages are stored on your local computer, which reduces the space your email account uses on your web server.

By default, the POP3 protocol works on two ports:

- Port 110 - this is the default POP3 non-encrypted port
- Port 995 - this is the port you need to use if you want to connect using POP3 securely

IMAP:

The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers.

While the POP3 protocol assumes that your email is being accessed only from one application, IMAP allows simultaneous access by multiple clients. This is why IMAP is more suitable for you if you're going to access your email from different locations or if your messages are managed by multiple users.

By default, the IMAP protocol works on two ports:

- Port 143 - this is the default IMAP non-encrypted port
- Port 993 - this is the port you need to use if you want to connect using IMAP secure.

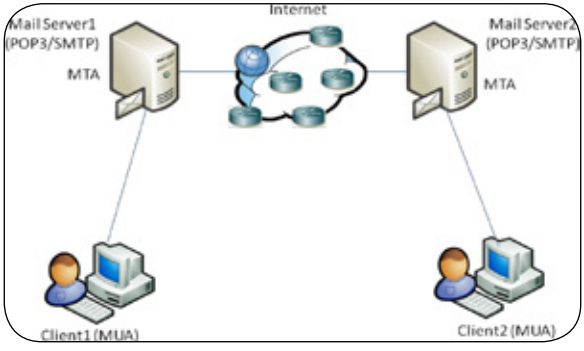
SMTP:

Simple Mail Transfer Protocol (SMTP) is the standard protocol for sending emails across the Internet.

By default, the SMTP protocol works on three ports:

- Port 25 - this is the default SMTP non-encrypted port
- Port 2525 - this port is opened on all Site Ground servers in case port 25 is filtered (by your ISP for example) and you want to send non-encrypted emails with SMTP
- Port 465 - this is the port used, if you want to send messages using SMTP securely

The working of e-Mail is as shown in the figure below. Each mail server consists of two different servers running on a single machine. One is POP3 (Post Office Protocol) or IMAP (Internet Mail Access Protocol) server which holds the incoming mails and the other SMTP (Simple Message Transfer Protocol) server which holds the outgoing mails. SMTP works on the port number 25 and POP works on the port number 110 and IMAP works on the port number 143.



In the figure shown above,

- Client 1 has an account in the mail server 1 and Client 2 has an account in mail server
- When Client 1 sends a mail to Client 2, first the mail goes to the SMTP server of mail server 1. Here the SMTP server divides the receiver address into two parts username and domain name.
- For example, if SMTP server rec
- eives user1@example.com as the receiver's address. It will separate into user1, which is a mail account in destination mail server and example.com which is the domain name of destination mail server. Now with the help of the domain name it will request particular IP address of the recipient's mail server, and then it will send the message to mail server 2 by connecting to its SMTP server.
- The SMTP server of Mail Server 2 stores the message in Client2 mailbox with the help of POP3 in mail server 2. When the client 2 opens his mailbox, he can view the mail sent by client 1.

Possible threats through e-Mail and guidelines for handling e-Mails safely

e-Mails are just like postcards from which the information can be viewed by any-one. When a mail is transferred from one mail server to another mail server there are various stops at which there is a possibility of unauthorized users trying to view the information or modify it.

Since a backup is maintained for an e-Mail server all the messages will be stored in the form of clear text though it has been deleted from your mailbox. Hence there is a chance of viewing the information by the people who are maintaining backups. So it is not advisable to send personal information through e-Mails.
Say you have won a lottery of million dollars, Getting or receiving such kind of mails is a great thing, and really it's the happiest thing. However these mails may not be true.

Tips

- ✓ *Always scan the attachments before you open them.*
- ✓ *Always check and confirm from where the e-mail has been received, generally service people will never ask or provide your password to change.*
- ✓ *It is always recommended to ignore or delete spam e-mails.*
- ✓ *Always ignore free gifts offered from unknown users.*

By responding to such a kind of mails many people lost huge amount of money. So ignore such kind of e-Mails, do not participate in it and consider it as a scam.
Sometimes e-Mails offering free gifts and asking personal information are received from unknown addresses. This is one way to trap your personal information.

- One way of stealing the password is standing behind an individual and looking over their password while they are typing it or searching for the papers where they have written the password.
- Another way of stealing the password is by guessing. Hackers try all possible combinations with the help of personal information of an individual.
- When there are large numbers of combinations of passwords the hackers use fast processors and some software tools to crack the password. This method of cracking password is known as “Brute force attack”.
- Hackers also try all the possible words in a dictionary to crack the password with the help of some software tools. This is called a “dictionary attack”.
- Generally spammers or hackers try to steal e-Mail address and send malicious software or code through attachments, fake e-Mails, and spam and also try to collect your personal information.

Attachments

Sometimes attachments come with e-mails and may contain executable code like macros, .EXE files and ZIPPED files. Sometimes attachments come with double extensions like “attachment.exe.doc”.By opening or executing such attachments malicious code may download into your system and can infect your system.

Fake e-Mails

Some times e-Mails are received with fake e-mail address like services@facebook.com by an attachment named, “Facebook_Password_4cf91.zip and includes the file Facebook_Password_4cf91exe" that, the e-mail claims, contains the user's new Facebook password. When a user downloads the file, it could cause a mess on their computer and which can be infected with malicious software.

Spam e-Mails

Spam messages may trouble you by filling your inbox or your e-mail database. Spam involves identical messages sent to various recipients by e-Mail. Sometimes spam e-mails come with advertisements and may contain a virus. By opening such e-Mails, your system can be infected and your e-Mail ID is listed in spammers list.

e-Mails offering free gifts

Sometimes e-Mails are targeted at you by; unknown users by offering gifts, lottery, prizes, which might be free of cost, and this may ask your personal information for

accepting the free gift or may ask money to claim lottery and prizes it is one way to trap your personal information.

Hoaxes

Hoax is an attempt to make the person believe something which is false as true. It is also defined as an attempt to deliberately spread fear, doubt among the users.

How to prevent?

Using filtering software's

Use e-Mail filtering software to avoid Spam so that only messages from authorized users are received. Most e-Mail providers offer filtering services.

Ignore e-mails from strangers

Avoid opening attachments coming from strangers, since they may contain a virus along with the received message.

Be careful while downloading attachments from e-Mails into your hard disk. Scan the attachment with updated antivirus software before saving it.

Guidelines for using e-mail safely

- Since the e-Mail messages are transferred in clear text, it is advisable to use some encryption software like PGP (pretty good privacy) to encrypt e-Mail messages before sending, so that it can be decrypted only by the specified recipient only.
- Use E-Mail filtering software to avoid Spam so that only messages from authorized users are received. Most e-Mail providers offer filtering services.
- Do not open attachments coming from strangers, since they may contain a virus along with the received message.
- Be careful while downloading attachments from e-Mails into your hard disk. Scan the attachment with updated antivirus software before saving it.
- Do not send messages with attachments that contain executable code like Word documents with macros, .EXE files and ZIPPED files. We can use Rich Text Format instead of the standard .DOC format. RTF will keep your formatting, but will not include any macros. This may prevent you from sending virus to others if you are already infected by it.
- Avoid sending personal information through e-Mails.
- Avoid filling forms that come via e-Mail asking for your personal information. And do not click on links that come via e-Mail.
- Do not click on the e-Mails that you receive from un trusted users as clicking itself may execute some malicious code and spread into your system.

Avoid filling forms through e-mails links which ask for personal information

Do not follow the web links that come through e-mails

Be suspicious of any e-mail with urgent requests for personal financial information

Instant Messaging

Nowadays Instant messaging (IM) is growing due to evolving technologies and Internet speeds in India and in changed in the form of real time text based to real time of audio, video communication between two or more people connected over the network. Instant message became most popular with this you can interact with people in a real time and you can keep the list of family and friends on your contact list and can communicate until the person is online .There are many instant service providers like AOL, Yahoo messenger, Google Talk and many more.

Limit interactions to users in a chat room

Risks involved in IM

Hackers constantly access instant messages and try to deliver malicious codes through the instant message and the code may contain a virus, Trojan, and spyware and if you click on the file the code will enter your system and within seconds it infects the system.

Spim

Spim is a short form of spam over instant messaging, it uses IM platforms to send spam messages over IM. Like e-mail spam messages, a spim message also contains advertisements. It generally contains web links, by clicking on those links malicious code enters into your PC.

Generally, it happens in real time and we need to stop the work and deal with spim as the IM window pop-ups, in the e-mail we have time to delete and we can delete all spam at a time, or we can scan before opening any attachments. This cannot be done in IM.

Tip: Avoid opening attachments and links in IM

Skype Video Communication

New technologies empower everybody and help them reach audiences all over the world. Their words, pictures and sounds can be transmitted around the globe in a matter of seconds. Many users use Skype, WhatsApp, Facebook, Google Mail, Blogger, WordPress and Dropbox to communicate, store data, collaborate and promote their work through Internet media communication.

But there are risks associated with using these tools and we all need to be prepared for the worst-case scenario. Let's have a look at the popular services for us, their risks and possible, more secure alternatives.

Risks through Skype: Skype was always assumed to be safe because of its end-to-end encryption. In the same time, through revelations have revealed that the NSA has been listening to Skype since 2011 and it's unclear to what extent other agencies are able to intercept the service. Also according to Eric King, head of research at Privacy International, Skype "can no longer be trusted to protect user privacy"

Possible solutions: Use Skype as if it were a public forum. Everything you say or write may be used against you.

Alternatives: Jitsi (encrypted text, voice and video messaging), Linphone (encrypted voice and video chat), Mumble (encrypted voice chat).

WhatsApp

WhatsApp is one of the most popular messaging apps in the word. It lets you send messages without having to pay for sms services although the person you are sending to also has to be using the app. It's an easy way to stay in touch with the newsroom and colleagues while in the field, especially as you can exchange images, video and audio.

Risks with whatsapp: Currently, WhatsApp claims messages are encrypted but because the company won't say what method they use, it's difficult to know how secure the service is. There are reports that WhatsApp messages sent over wifi and other public channels can be decrypted. There are apps out there which try to make WhatsApp more secure.

Possible solutions: Resort to more secure apps

Alternatives: Pidgin (off-the-record messaging), TorChat (anonymous P2P chat), ChatSecure (formerly Gibberbot) and Xabber for Android.

Facebook

The most of Internet users use this global social network to share their work, crowd source information, stay in touch with colleagues and newsmakers, follow companies and news on their beats, subscribe to important people and participate in groups.

Facebook is a huge data collector. The list of your friends may influence the decision

of local authorities to grant you a visa to work in a certain region, and the open groups you are a member of let strangers know about your interests even if your profile is closed to external visitors. Also, Facebook is constantly experimenting with new tracking methods.

Possible solutions: Be very careful publishing information on Facebook. Once it's online, you lose control of it. Go to the privacy settings in the upper right corner of your Facebook page and make sure you have all the precautionary measures taken. Always try to log out of your Facebook page while surfing other websites in your computer.

Twitter

Twitter is good for following breaking news and breaking news yourself. You can also use it to collaborate with others, find communities, and follow trends and topics.

Everything you do on Twitter is visible. If you have geotagging enabled, it can be easy to locate you. The service is also a haven for malware attacks.

Possible solutions: Be careful what you post and whom you follow. Don't create open lists unless you are absolutely sure you won't get into trouble by doing this. Disable geotagging

For more about Internet media communications refer browsers and search engines sections

References:
http://www.dolsenz.com
http://www.akademie.dw.de
http://en.wikipedia.org/wiki/Mass_media

BEWARE OF JOB OFFERS THROUGH E-MAILS

- ✓ They may conduct spoofed interviews before sending job offer
- ✓ They may ask to deposit money for third party consultancy

- ✓ Never transfer/deposit money without proper verification
- ✓ Consult the offered company

Online Games

An online game is a game played over a computer network via the Internet. Online games range from normal text based to graphical based games. Simultaneously Players can play the same game. The main advantage of online games is the ability to connect to multiple games even though single player is online. Based on technology the games are also become more complex the technology related games like flash games and java games became more popular.

There are free online games and commercial games, most of the popular games are enclosed with end user license agreements and limited to access by the creators of games and the breaking of the agreement range from warning to termination.

Online gambling is now also very popular. People play casino-like games, lotteries, and bet sporting events like any form of gambling, the risks include addiction and the potential rapid loss of any funds invested in the game

There are massively multi-player online games like real time strategy games, role playing game, first person shooter games and many more as new technologies and high-speed internet connections have helped online gaming. Because gamers invest large amounts of time and money in today's sophisticated games, others see an opportunity for mischief or illicit profit. The technological and social risks of online games should be understood by anyone who enjoys them. These include the following:

- *risks from social interactions with strangers who may trick you into revealing personal or financial information*
- *risks from computer intruders exploiting security vulnerabilities*
- *risks from online and real-world predators*
- *risks from viruses, Trojan horses, computer worms, and spyware*

Online Gaming Risks

There are a lot of choices exist in today's online gaming environment. Massive Multiplayer Online Role Playing Games has emerged as popular genre of games. Most allow players to create online identities as game characters who participate in virtual adventures, which sometimes cross into the real world. For example, gamers sell virtual game items for real-world money in markets such as Flipkart, Amazon etc. In some games, there is a user-created, virtual world where people use real money to create or purchase personal property in their online world. This has created an opportunity for a new type of criminal activity called "virtual crime."

In general, online gaming may involve both social risks and technological risks. Thus, many online gaming risks are similar to those computer users may have already encountered, but they may not have realized that the games pose another opportunity for the compromise of their privacy or computer security.

Be careful about copyright issues when you download software, games, books etc.

Technology Risks	Social Risks
Malicious Software • Viruses may arrive as attachments through shared email IDs as messages or via instant messaging programs • Malicious programs may be hidden in game files you download or software you install. • Malicious individuals mWay also take advantage of the social networks associated with online games that rely on chat, email, or even voice communication • They then use this software for a variety of illicit purposes. **Insecure or Compromised Gamer Servers** • **Gamer concerns:** If the software on the game server has been compromised, computers that connect to it can be compromised also. • By exploiting vulnerabilities, malicious users might be able to control your computer remotely and use it to attack other computers or install programs such as Trojan horses, adware, or spyware, or gain access to personal information on your computer. **Insecure Game Coding** • Some game protocols – the methods for communicating game information between machines – are not implemented as securely as other protocols. Game code may not be as well scrutinized as more popular commercial software.	**Social Engineering** Malicious individuals may try to trick you into installing software on your computer that they can use to control your computer, monitor your online activities, or launch attacks against other computers. They may, for instance, direct you to phony web sites offering bogus patches or game downloads that, in reality, are malicious software **Identity Theft** If a malicious individual can gather information about you from the profiles you create in games and other sources, they may be able to use it to establish accounts in your name, resell it, or use it to access your existing financial accounts. **Cyber Prostitution** In the game "The Sims Online," an MMO, a "cyber-brothel" was developed by a 17-year old boy using the game alias "Evangeline."4 Customers paid sim-money ("Simoleans") for cybersex by the minute. **Virtual Mugging** The term "virtual mugging" was coined when some players of Lineage II used software applications that run over the web, called bots, to defeat other player's characters and take their items. **Virtual Sweatshop** The virtual economies of some online games and the exchange of virtual items and currency for real money has spawned the virtual sweatshop, in which workers in the third-world countries are economically exploited by people seeking to find new ways to profit from the new online economies

Things to be noted while downloading the games

- Study the rating of an online game, frequently they will let you know if it is suitable for your age.
- Read the terms and conditions of the sites that you use and check if there are special safety features for children.
- It is important and make sure that game vendor is reputable and download the game from trusted web sites.
- Sometimes free download games conceal malicious software , this includes plug-ins required to run a games, administrative mode to open a game which is not advisable , by doing this you open yourself to the risk that an attacker could gain complete control of your computer, it is always safe to play in a user mode rather than the administrative mode.
- When playing an online game it is best to play it at the game site , this may reduce the risk and end up with a malicious web site.

Guidelines for Online Games

- Create a family e-Mail address for signing up for online games. Screenshots: If anything bad happens while playing online games, take a screen shot using the "print screen" button on the keyboard of those displayed things on the screen and report it to the concerned web site ad use the screen shot as evidence.
- Use antivirus and antispyware programs.
- Be cautious about opening files attached to e-Mail messages or instant messages.
- Verify the authenticity and security of downloaded files and new software.
- Configure your web browsers securely. Use a firewall.
- Set up your user profile to include appropriate language and game content for someone your age.
- Set time limits for children.
- Never download software and games from unknown websites.
- Beware of clicking links, images and pop ups in the web sites as they may contain a virus and harm the computer.
- Never give personal information over the Internet while downloading games.
- Some free games may contain a virus, so be cautious and refer while downloading them.
- Create and use strong passwords.
- Patch and update your application software

References

http://www.media-awareness.ca/english/teachers/wa_teachers/safe_passage_teachers/risks_gambling.cfm
http://www.mediafamily.org/facts/facts_gameaddiction.shtml
https://www.us-cert.gov
http://www.netsmartz.org/

About Social Networks

A social network is a social structure made of nodes (which are generally individuals or organizations) that are tied by one or more specific types of interdependency, such as values, visions, ideas, financial exchange, friendship, dislike, conflict or trade. Social networks are fun to use, helpful for job hunting, and great for keeping in touch with friends, business contacts and relatives.

Social networking is the grouping of individuals into specific groups, like small communities who share interests and/or activities, or who are interested in exploring the interests and activities of others. Although social networking is possible in person, especially in the workplace, schools, colleges and universities, it is most popular online. This is because unlike most high schools, colleges, or workplaces, the Internet is filled with millions of individuals who are looking to meet other people, to share first-hand information and experiences about interests like cooking, golfing, gardening, developing friendships professional alliances, finding employment, business-to-business marketing and even groups sharing information about baking

cookies to the Thrive Movement. The topics and interests are as varied and rich as the story of our universe.

The other side of Social Network is security and privacy issues and is entirely treated as two different issues. As security issue, the third person gains unauthorized access to the information of protected resources and the privacy issues is someone can gain access to confidential information by simply watching you what you type your password. But both types of breaches are often intertwined on social networks, especially since anyone who breaches network and opens the door to easy access to private information belonging to any user. The reason behind Social network security and privacy lapses exist because of the amounts of information the sites process each and every day that end up making it much easier to exploit a single flaw in the system. Features that invite user participation - messages, invitations, photos, open platform applications, etc. – are often the avenues used to gain access to private information.

The popularity of social networking sites has increased at astonishing levels. There is no arguing the usefulness of sites such as Face book, Twitter and LinkedIn. They can be used for professional networking and job searches, as a means to increase sales revenue, as a tool to keep the public informed of safety and other issues or as a way to reconnect with friends from way-back-when.

Take advantage of the privacy settings available in social networking sites

Uses of Social Networking

- Meeting the people online across the world
- Making friendship with the people who are far away
- Profile building
- Self representation
- Exchanging / Sharing the information related to studies or education, current affairs, sports, business, transport, movies, latest news updates, event announcements, exchanging the thoughts etc
- Share the data files, videos, music, photos

Social Networking Risks and Challenges

Social networking has become most popular activity in today's Internet world, with billions of people across the world are using this media to meet old friends, making new friends, to collect and share information, social networking while being a popular media has several disadvantages associated with it. These sites can be trapped by or hackers leading to loss of confidentiality and identity theft, of the users. Social Networking sites are becoming very popular especially among the growing kids. These sites expose the kids to various risks like online bullying, disclosure of personal information, cyber-stalking, access to inappropriate content, online grooming, child abuse, etc. In addition there are many more risks like fake profiles with false information, malicious application, spam, and fake links which leads to phishing attacks etc.,

- **Illegal content:**

  In General, anybody who access social networking or media sites may not deliberately seek out inappropriate content and may inadvertently access content while undertaking online access or searches or they may seek it out or be referred content by others. The content that includes sexually explicit, illegal images of sexual abuse, violence, criminal activity or accidents, from video clips, promotes extreme political views, potentially used in the radicalization of vulnerable members of the community, basis of race, religion, sexual preference or other social/cultural factors. They may also exposes to online advertising which promotes adult content.

  The illegal content on the sites, images of child abuse and unlawful hate speech. Age-inappropriate content on the sites, such as pornography or sexual content, violence, or other content with adult themes which may be inappropriate for young people and they might discover content through their smart phones that may be blocked by home and school internet filters

- **Spam**

  As we all know that spam is usually unwanted e-mail advertising about a product sent to list of e-mails or group of e-mail addresses. Similarly spammers are sending the unwanted mails or messages to the billions of users of social networking sites which are free; and are easily accessible by spammers to gather the personal information of the unsuspecting users.

  Social spam is unwanted spam content appearing on social networks and any website with user-generated content (comments, chat, etc.). It can be manifested in many ways, including bulk messages, insults, hate speech, malicious links, fraudulent reviews, fake friends, and personally identifiable information. Bulk messages in social networking sites are a set of comments repeated multiple times with the same or very similar text. These messages, also called as spam-bombs, can come in the form of one spammer sending out duplicate messages to a group of people in a short period of time, or many active spam accounts simultaneously posting duplicate messages.

- **Abusive, vulgar, or irreverent language:**

  User-submitted comments that contain swear words or slurs are classified as profanity or abusive or vulgar or irrelevant language. Common techniques include "cloaking" works by using symbols and numbers in place of letters. These bad words are still recognizable by the human eye, though are often missed by website monitors due to the misspelling.

- **Insults:**

  User-submitted insults are comments that contain mildly or strongly insulting language against a specific person or persons. These comments range from mild name-calling to severe bullying. Online bullies often use insults in their interactions, referred to as cyber bullying. Hiding behind a screen name allows users to say mean, insulting comments with anonymity; these bullies rarely have to take responsibility for their comments and actions.

Always check the authenticity of the person before you accept a request

- **Threats:**
  User-submitted threats of violence are comments that contain mild or strong threats of physical violence against a person or group. It may also quickly turn into a stream of racism and provoke to insulting comments, and threats against others. This is a more serious example of social spam.

- **Hate speech:**
  User-submitted hate speech is a comment that contains strongly offensive content directed against people of a specific race, gender, sexual orientation, etc.

- **Fake Friends:**
  Fake friends occur when several fake accounts connect or become "friends". These users or spam boats often try to gain credibility by following verified accounts, such as those for popular celebrities and public figures. If that account owner follows the spammer back, it legitimizes the spam account, enabling it to do more damage.

- **Malicious links:**
  User-submitted comments can include malicious links that will inappropriately harm, mislead, or otherwise damage a user or computer. These links are most commonly found on video entertainment sites, such as Youtube. What happens when you click on malicious links can range from downloading malware to your device, to directing you to sites designed to steal your personal information, to drawing unaware users into participating in concealed advertising campaigns.
  Malware can be very dangerous to the user, and can manifest in several forms: virus, worm, spyware, Trojan Horse, or adware. Malicious application might come through different application while using or installing software's. Similarly, the clicking on the social networking application starts the application installation process or link to view the video, etc. In order to fulfill its intended operation the application requests for some elevated privileges from the user like access to my basic information, update on my wall, post on my wall, etc

- **Fraudulent Reviews:**
  Reviews of a product or service or Movie or story from users that never actually used it. These are often solicited by the proprietor of the product or service, who contracts out positive reviews, "reviews-for-hire". Some companies are attempting to tackle this problem by warning users that not all reviews are genuine

- **Personally identifiable information:**
  User-submitted comments that inappropriately display full names, physical

addresses, email addresses, phone numbers, or credit card numbers are considered leaks of personally identifiable information.

- **Phishing:**
  As we all know the phishing attack is creation of fake site just similar to original site. Similarly these days even social networking phishing has come in different flavors just like phishing attacks on banks and popular trading websites. Social networking phishing has come up with fake mails and messages like offering some specialized themes, updating the profile, updating the security application/ features etc. In order to see the updates the user needs to follow a link and log in, through which the credentials are taken by the attacker. The linked page is a fake copy of the original login page, focused on stealing user account credentials

Think twice before posting pictures of you, or your family members, or your friends on the Internet

Remember, hackers are not only a threat to your computer but also they can harm other computers by using your computer

Avoid file transfers during chatting as that may control your system

Social Networking Statistics during 2014

49% of children 8-17 have an online profile
22% of 16+ have an online profile
On average adults have profiles on 1.6 sites
63% of 8 to 17-year-olds with a profile use Bebo
37% of 8 to 17-year-olds with profile use MySpace
18% of 8 to 17-year-olds with a profile use Facebook
59% of 8 to 17-year-olds use social networks to make new friends
16% of parents do not know if their child's profile is visible to all
33% of parents say they set no rules for their children's use of social networks
43% of children say their parents set no rules for use of social networks

- **Click jacking:**
  Generally, click jacking is a malicious technique of tricking Web users like phishing into revealing confidential information or taking control of their computer while clicking on seemingly innocuous Web pages. Vulnerability across a variety of browsers and platforms, a click jacking takes the form of embedded code or script that can run without the user's knowledge. The same is followed in the social networking domain. The objective behind such an attack is that users can be tricked into clicking in the links, icons, buttons etc, which could trigger running of processes at the background wi thout the knowledge of the user

- **Conduct:**
  This relates to how people behave online, this may include bullying or victimization (behaviors such as spreading rumors, excluding peers from one's social group, and withdrawing friendship or acceptance) and potentially risky behaviors (which may include for example, divulging personal information, posting sexually provocative photographs, lying about real age or arranging to meet face-to-face with people only ever previously met online) Networking sites are third party application program interface (API) which allows for easy theft of private information and it gave developers access to more information like addresses, pictures than needed to test the applications.

Guidelines for Social networking:

- Don't give or post any personal information like your name, address of the school / home, phone numbers, age, sex, credit card details
- The information which was posted by you in online can be seen by everyone who is online because internet is the world's biggest information exchange tool. Many people who are having access to the site which you are using can access your profile and get all the information what you have posted. The persons who is having access to your profile may include good persons like your friends, parents, teachers and bad persons like strangers
- Be aware that the information you give in the sites could also put you at risk of victimization
- Never give out your password to anyone other than your parent or guardian
- Change your password frequently, and avoid clicking links that purport to send you back to the social network site. Instead, type the site's address directly into your browser (or follow a bookmark you've previously saved) to get back to your account
- When you are choosing a Social Networking site, privacy issues should be considered
- While accepting the friends on Social Networking sites, be selective. Only add

people as friends to your site if you know them in real life

- Never meet in person with anyone whom you met on Social Networking site because some of the people may not be who they say they are
- Take your parents' permission if you want to meet the person whom you met in the networking site
- Most of the Social Networking web sites enabling users to set privacy controls for who has the ability to view the information. So try to use such facilities
- Do not post anything which harm to your family credibility
- Never post photographs, videos and any other sensitive information to unknown persons in Social network sites
- If you think that your social networking account details have been compromised or stolen, report your suspicions to the networking site support team immediately.
- Never respond to harassing or rude comments which are posted on your profile.
- Delete any unwanted messages or friends who continuously leave inappropriate comments and immediately report those comments to the networking site
- Do not post your friends information in networking sites, which may possibly put them at risk. Protect your friends by not posting the group photos, school names, locations, ages, sex…etc
- Avoid posting the plans and activities which you are going to do in networking sites
- Check the privacy settings of the Social Networking sites and set the settings in such a way that the people can only be added as your friend if you approve them also set the settings in such a way that the people can only view your profile if you have approved them as a friend

File sharing, Downloading & Uploading

Safe Downloading and uploading

About Downloading

Downloading is the transmission of a file from one computer system to another, usually smaller computer system. From the Internet user's point-of-view, to download a file is to request it from another computer (or from a Web page on another computer) and to receive it. The term download is used to describe the process of copying a file from an online service that is via an Internet to one owns a computer.

About uploading

The opposite of download is uploading this means copying a file from your computer to another computer over the network. Uploading means to transmit data. Whatever is transferred can be uploaded. In short “Uploading means sending a file to a computer that is set up to receive it”. You can upload any kind of files like documents, music, videos, images and software and many more. Uploading files or file sharing in P2P network is always between peer computers where as uploading server-client technology, the uploading would be done from no. of clients to a particular machine, which is a server.

Downloading also refers to copying a file from network server to a computer on the network. To download means to receive data i.e. whatever offered for downloading can be downloaded. You can download any kind of files from Internet like documents, music, videos, images and software and many more.

P2P (peer to peer) file sharing allows users to access media files such as books, music, movies, and games using a P2P software program that searches for other connected computers on a P2P network to locate the desired content. The nodes (peers) of such networks are end-user computer systems that are interconnected via the Internet.

P2P is differs with server- client technology as files would be downloaded from one computer which is server.

Downloading from the Internet and sharing files are common, every day practices and can come with a set of risks you should be aware of.

What are the risks of file sharing or insecure downloads?

When you try to share a file or download a file from the Internet, it includes installing a program, opening pictures, links from different websites or from e-mails, downloading music files and many more files on to a computer .These files could be the same what they say are, but they can also be involved with something like malicious software that can harm your computer, which includes viruses, worms and many destructive programs.

You could unknowingly give others access to your computer while file sharing, who could potentially copy private files. This can happen when you're asked to disable or alter your firewall settings in order to use Peer-to-Peer (P2P) to upload to a file sharing program, which could leave your computer vulnerable.

Downloading viruses, Trojans and other malware to your computer without your knowledge, may destroy data or give someone access to all the information on your computer or destroy all the confidential information on your PC as they're often disguised as popular movie or song downloads.

The spyware often changes your computer's behavior like PC becomes slow, and even causes a computer crash. The Spyware can be used to track the browsing history, steal the passwords and allow an attacker to grab complete information of your system.

Downloading unwanted pornography labeled as something else and also exposing yourself to legal issues such as copyright infringement if you download movies, TV shows, music or software that are copyright protected, even if you didn't realize it.

Check the validity of the certificate and issuer of the certificate for a site before any downloads

When you download chat software, check for default settings and adjust them if they are too permissive

Tips for Safety downloads

- *While downloading any file close all the applications that are running on your computer, let only one set-up file run at a time of downloading.*
- *Close all the important applications in order to be safe if something goes wrong while downloading.*
- *Set firewalls, set antivirus to actively scan all the files you download.*
- *Scan all the files after you download whether from websites or links received from e-mails.*
- *Always use updated antivirus, spam filter and spyware to help detect and remove virus, spyware from the application you want to download.*
- *Never download any files like music, video, games and many more from untrusted sites and don't go by the recommendations given by your friends or made by any random website's comments.*
- *Check that the URLs are same and always download games, music or videos from the secure websites like which use HTTPS websites instead of HTTP. In the web address, it replaces "http" to https". The https refers to the hypertext transfer protocol secure.*
- *Download anything only from thrust worthy websites. Don't click links to download anything you see on unauthorized sites.*
- *If any dirty words appear on the website just close the window no matter how important it is, because spyware may be installed on your PC from such websites.*
- *Check the size of the file before you download, sometimes it shows a very small size but after you click it increases the size of the file.*
- *Never believe anything which says click on this link and your computer settings will be changed and your PC can be turned into XBOX and can play unlimited games on your computer.*

- *Don't accept anything that offers you free download because that may contain malicious software.*
- *Don't click the link or file and let it start download automatically, download the file and save where you want save and then run on the application.*
- *Set secure browser settings before you download anything.*
- *Read carefully before you click on install or run application. That means read terms and conditions.*
- *do not download anything until you know complete information of the website and know whether it is an original site of an original company.*
- *Never download from the links that offer free antivirus or anti spyware software, always download from trusted sites, if you are not sure about the site you are downloading, enter the site into favorite search engine to see anyone posted or reported that it contains unwanted technologies.*
- *Never download from the links that offer free antivirus or anti spyware software, always download from trusted sites, if you are not sure about the site you are downloading, enter the site into favourite search engine to see anyone posted or reported that it contains unwanted technologies.*

References:

www.getcybersafe.gc.ca/cnt/rsks/nln-ctvts/dlng-shrng-eng.aspx
www.referenceforbusiness.com

Be aware of copyright issues

Instant Messaging

Instant messaging has existed in some form or another for decades in Internet History. It is a process by which users on a computer network can quickly communicate with one another using short text-based sentences rather than using email. Each user has a piece of software that communicates with a common server that connects the chat sessions. Over the past few years, two distinct settings for the use of instant messaging have evolved.

The first is the corporate or institutional environment composed of many potential users but who are all under the same organizational umbrella. The second setting is individual users 'after work' or at home who do not have a mission-oriented commonality between them, but are more likely family and friends.

Features of Instant Messengers

- **Presence and Status Broadcasting -** Messengers attempt to maintain a social environment and always stay 'connected'.
- **Interoperability –** Many other manufacturers can interoperate with the example messenger.
- **Contact Lists -** Maintains lists of all desired contacts.
- **Client-Server Design –** Requires use of third party servers to provide chat functionality to messenger clients.
- **Logs Messages –** Messages and other events are recorded

Viber:
Developed by Viber Media, it is a proprietary cross-platform instant messaging voice over Internet protocol application for smart phones. In addition to text messaging, users can exchange images, videos and audio messages

LINE:
LINE is a Japanese proprietary application for instant messaging on smart phones and personal computers that allows users to make free voice calls and send free messages. Stickers and emoticons used in the app are popular among teenagers

KakaoTalk:
KakaoTalk is a multi-platform texting app created by South Korean team that allows iPhone, Android and BlackBerry users to send and receive messages for free. It has achieved 100 million subscribers since its release on March 18, 2010

WeChat:
WeChat, the mobile messaging application released by China's Internet giant Tencent, has 450 million monthly active users

WhatsApp:
WhatsApp Messenger is a cross-platform mobile messaging app that allows users to exchange messages without having to pay for them.

Kik:
Kik Messenger is an instant messaging application for mobile devices. Kik Messenger was released on October 19, 2010, by Kik Interactive, started by a group of students from the University of Waterloo, Ontario, Canada

Hike:
Hike is a communication app that offers both instant messaging and SMS under one roof, according to NDTV.com, an Indian TV network. It has been developed by Bharti Softbank, which is jointly held by India's Bharti Telecom and Japan's Softbank telecom provider. The app is the brainchild of Kavin Bharti Mittal

Risks in Mobile Instant Messaging

- **Virus and Worms**
  In 2014, 38% of Viruses in top 50 viruses and worms are targeted towards peer-to-peer or IM applications in Internet Communications. Most viruses are sent through file transfers, Public Instant Messaging (IM) clients also have publicized vulnerabilities, where flaws such as buffer overflows and boundary condition errors have been exploited to spread viruses, worms or denial-of-service attacks.

Be Polite and kind during your chat sessions

- **Spim**
  IMlogic says that 5% to 7% of IM traffic today is spim (instant messaging spam). Spim can be more disruptive than e-mail spam, as it is more intrusive (the pop-up spim interrupts the user) and generally of a more sexually offensive nature (leading to human resources and legal risk

Watch out for SPIM. (Spam Instant Messages)

- **Identity theft/authentication spoofing**
  Public IM systems let individuals create anonymous identities, which do not map to any identity and also IDs can be created even if the IDs and domains are not owned by that individual ("icici" or "john chambers," for example). Spoofing creates risk, as these IDs can be used maliciously, outside the control of the IT security department.

- **Firewall tunnelling**
  IM clients find ways to tunnel through firewalls, creating risk. Most IM services come through well-publicized ports (5190 for AOL Instant Messenger, 1863 for MSN and 5050 for Yahoo), but IM clients also can exploit any open port on the firewall, including those used by other applications (such as Port 80 for Web and HTTP traffic). Some clients also can connect via peer-to-peer connections or establish connections on randomly negotiated ports.

- **Data security leaks**
  Unmonitored content leaving the corporation without the knowledge of the information security department introduces legal and competitive risk (such as a CFO sending a confidential spreadsheet via IM without an audit trail). File transfer over IM is a powerful way to send information beyond the tracing capabilities of the IT department. The lack of content filtering and archiving makes it difficult for IT to discover potential breaches of policy or to hold individuals accountable.

- **Avoid Exposing Private Information:**
  Developers have warned that many of the instant messaging applications make it easy for private information to be exposed and used for fraudulent purposes. Researchers at the University of California studied more than 120,000 free applications that are available for use on Android devices.

  Many of the applications have parts of the code that are public, which means they could be modified easily for fraudulent purposes. The use of malicious code allows hackers and other individuals having malicious intent to send messages on behalf of someone, to get access to personal information and to replace the actual application with code designed for alternative purposes.

  Despite the emphasis on Android apps, researchers believe that similar security concerns are valid for iPhone instant messaging options.

- **What we need to do?**
  Instant messaging applications add a lot of convenience, but few people take the time to think about security concerns. Every day, hackers are trying to gain access to our conversations. The good news is, there are certain things that can be done to make instant messaging safer.

- **Encryption:**
  Several other instant messaging apps for smart phones were examined concerning the manner in which personal information is transferred and stored. WhatsApp, a market leader in the instant messaging niche, has been accused of transmitting address books and personal information unencrypted to the app server. Many bits of private information, including ID, are readily available for third parties to see and to utilize.

  An even more troublesome trend has emerged recently. Certain applications were developed for the purpose of getting access to the instant messaging conversations of other people and for access to personal information. WhatsApp Sniffer is

one such development. Such applications reveal once again how many security gaps instant messaging applications leave.

- **Facebook Chat? Think Again:**
  Various surveys were carried out and the conclusion is that Facebook Chat applications for mobile devices are one of the least safe options on the market. Encryption is not used to protect log in, which means that the password of an individual can easily be seen. The instant messaging conversations themselves are protected minimally. Yahoo! Messenger and the now defunct Windows Live Messenger are two other applications that fail protecting member conversations adequately.

- **Using Instant Messaging Apps Safely:**
  What does it take? The first and most obvious thing you can do to increase instant messaging safety and privacy is the selection of the right application. No two instant messaging apps are alike. Some developers put more emphasis on the protection of sensitive data. Data encryption is the first and the most basic way of data protection. Make sure that the apps you choose transfer all information in an encrypted form to the server. Some Internet apps such as Skype, Google Talk, AOL, Instant Messenger, similar major developments brag higher than usual security. Make sure you do your research before downloading your app of choice to keep your information secure.

  So always use secured chat / IM applications

Secure Instant Messaging

Secure instant messaging is a form of instant messaging wherein at the very least the users are exchanging chat messages the contents of which they have caused to be encrypted with keys they generate and control.

Recent news events have revealed that the NSA is not only collecting emails and im messages but also tracking relationships between senders and receivers of those chats and emails in a process known as 'meta data' collection.

'Meta data' refers to the data concerned about the chat or email as opposed to contents of messages. It may be used to collect valuable information. The wireless network that you use to do instant messaging is just as important.
Open networks like the ones available in cafés, at airports and bus stations are very easy to break through. When doing instant messaging, rely on a closed, password-protected Internet network. Instant messaging can be used to communicate with friends, business partners and acquaintances. Still, it is important to keep security

concerns in mind. Though convenient, instant messaging can compromise personal information if the wrong app is chosen. Choose applications carefully and be smart in terms of what you share.

Almost by definition alone a secure messenger cannot be a social messenger. Therefore to be considered secure a messenger must behave differently than one used for more social purposes. Traits of a secure instant messenger include the ability to:

- Provide a 'stealth' online presence
- Send messages in cipher text not clear text form.
- Not log or store any information regarding any message or its contents.
- Not log or store any information regarding any session or event.
- Operate as a decentralized computing model not relying on third party servers for message security and handling.

Secure instant messengers aren't needed for every chat session but when there is a requirement for private, secure and untraceable messaging there is no other means to effect those requirements.

Popular Secure Instant Messaging Solutions in Mobiles/Tablets

Telegram:

Telegram is a cloud-based mobile and desktop messaging app with a focus on security and speed

Adium:

Adium is a free instant messaging application for Mac OS X that can connect to AIM, MSN, XMPP (Jabber), Yahoo, and more.

Bitbee:

BitlBee is a cross-platform IRC instant messaging gateway, licensed under the terms of the GNU General Public License

Jitsi:

JITSI (formerly SIP Communicator) is a free and open source multiplatform voice (VoIP), videoconferencing and instant messaging application for Windows.

Blogging

A web blog is a web site that consists of a series of entries arranged in reverse chronological order, often updated on frequently with new information about particular topics. The information can be written by the site owner, gathered from other Web sites or other sources, or contributed by users. A web blog may consist of the recorded ideas of an individual (a sort of diary).

Types of blogs

There are many different types of blogs, and they span over 100 languages. You can browse our tags to get a sense of the topics covered by, or take a look at these examples of popular blog categories

- **Personal:**
  This is the broadest category and includes blogs about personal topics like politics, music, family, travel, health, you name it.
- **Business:**
  Professionals ranging from realtors to lawyers and stock brokers are using to share their expertise, and companies have discovered the power of blogs to personally engage with their customers.
- **Schools:**
  It is a great way for teachers and students to collaborate on classroom projects.
- **Non-profits:**
  Foundations, charities, and human rights groups find our blogs to be great tools to raise awareness and money for their causes.
- **Politics:**
  Political parties, government agencies, and activists using our blogs to connect with their constituencies.
- **Private:**
  Some people make their blogs private to share photos and information within families, companies, or schools.

- **Sports:**
  We've got teams, athletes, and fans using blogs to express and share their passion for various sports
- **Media type Blogs:**
  Media may be using for sharing the videos called vlogs, for sharing the links called linklogs and for sharing the photos called photoblog
- **By the device**
  (mobile phone, PDA, wearable wireless webcam) are used to write the blogs through the mobile device like mobile phones or PDA called moblog
- **Genre blogs**
  (causes, education, political, travel) are focused on a particular subject like education, fashion, music, travel, political, personal (home) blogs …etc.

Risks involved in blogging

While blogging provides a humanizing effect on news and journaling, it also opens a window into personal lives. The details shared in blogs were once only available to a select group of friends, and while blogging has become common place, it has risks that should not be ignored

If you give your personal information like your name, location address, phone numbers, credit card details in the blogging sites, your information may be stolen by others (identity theft) because everyone who is having login account in the site which you are using can access to your profile. The profile which you are creating will be visible to everyone on the blog site. The persons like strangers can access your profile and can view all your details

For example, if you give your credit card number in the site, they may use that number for their own business or shopping purpose and the bill will be sent to you. Another example is if your children give their school name or location addresses in the site, the strangers who access that data may take advantage of it and may kidnap your children.

Limit your data that you put online

Never reveal password on questionnaires, or forums, or blogs or social networking sites

Spammers collect e-mail addresses from websites and blogs. So, minimize posting your e-mail address.

Cyber stalking

Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group. Cyber stalking is a new phenomenon that allows anonymous online stalkers to prowl for victims. Online bloggers traditionally provide personal details about their lives. As a result, many women that blog are becoming victims. Most people are concerned about children on the Internet and set up rigorous posting guidelines for children, adolescents, and teenagers, but few adults heed the warnings and often do not consider that they too can be targeted.

Females, in particular, should be cautious when circumnavigating the blogosphere. If you are a blogger or contemplating an online journal, consider these tips to protecting your identity.

Do not have an online profile:

Most blogging services allow bloggers to create an online profile. While it might be fun to post information about likes and dislikes, it is best to refrain from posting any personal details. Often, personal details inadvertently provide insight into physical location or habits. The aggregate information in a personal profile can also assist someone interested in pursuing an individual.

Tips to avoid risks by blogging

- *Never give away your personal information into the blogging sites*
- *Put reliable information as it reaches entire world and assume what you publish on the web is permanent.*
- *Avoid competition with other bloggers.*
- *State the terms of use, copy right in blog properly to viewers to protect your blogs.*
- *Guide them with other positive examples such as the children are posting their related information.*
- *Post anonymously: Manage your blog anonymously or adopt an alias for all online posting. This will help protect you in the event that you draw unwanted attention*
- *Avoid personal or identifying details: Avoid any personal or identifying details when posting in your blog. Do not post in advance about locations that you will be or about areas that you live near*
- *No photos: Refrain from posting a picture. Photos can invite trouble or unwanted attention.*
- *Avoid inappropriate dialogue: Be careful not to engage in dialogue that could be interpreted in a way that it was not intended. Sometimes humorous threads can get out of hand. If the dialogue degrades to an area that makes you uncomfortable,*

disengage from the dialogue and refrain from further posting. Also when making decisions about individuals online, consider their past posting behaviour and attempt to consider their true intentions

- *Always remember that just because you do not have a dialogue with someone does not mean that they are not reading everything that you write. Many people merely lurk on line and don't engage in comment posting, but do read what is written. Your audience could be much larger than you realize*
- *Timeless: Internet content is timeless, and keep in mind that even if you remove content, it might be archived or syndicated. If you do not want something read, do not post it to the Internet. High Schools, Colleges and Employers all search the Internet to discern an individual's history. Sordid details about a late night will not help land a coveted job*
- *The internet is a haven for all types of predators. Always remember that just because someone says something is true, does not mean that it is. Predators adopt personas of who they think you want them to be. Just as we provide guidelines to young children, adults should be wary and take precautions when posting online as well*
- *While blogging can be a great outlet and channel, and in some way immortalizing thoughts, it is important that safety is considered and that good blogging practices are followed at all times.*

Guidance for Parents on Blogging

- Establish Rules for online use with children.
- Monitor what your children plan to post before they post it.
- Evaluate Blogging Service and their features like a password protected secured blogs etc.
- Review your children blogs regularly
- Guide them with other positive example such as reference to the students who are posting their related information.

References:

http://www.feedforall.com
http://en.wikipedia.org/wiki/Blog
http://www.problogger.net

Cyberbullying

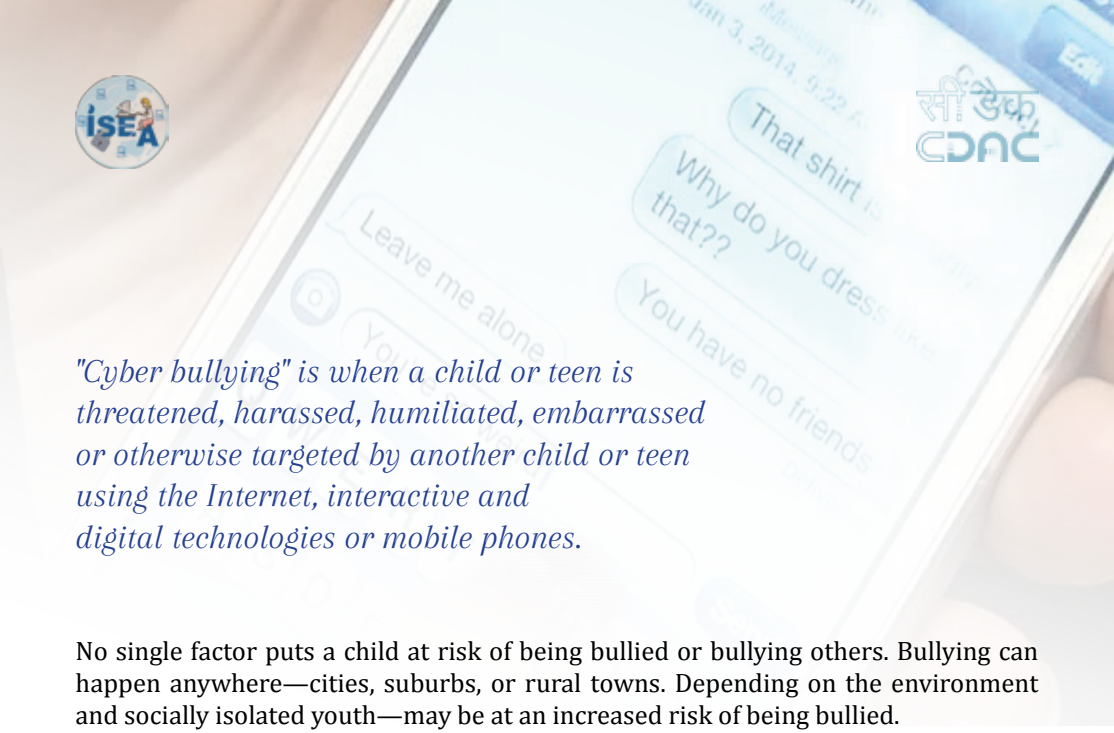
What is Cyber Bullying ?

Cyberbullying is bullying which happens among kids that take place using electronic technology. It can be carried out through electronic technology includes devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, e-mail, chat rooms, discussion groups and websites in Internet. Cyber bullying can include teasing and being made fun of, spreading rumors online, sending unwanted messages and defamation.

Examples of Cyberbullying include mean text messages or emails, rumors sent by email or posted on social networking sites, and sending embarrassing pictures, videos, websites, or fake profiles

Cyber Bullying: Risk Factors

Bullying can happen anywhere, but depending on the environment, some groups may be at an increased risk. Learn what factors increase the risk of children being bullied or children more likely to bully others and what warning signs can indicate that bullying may be happening. You can also find out how bullying can negatively impact kids.



"Cyber bullying" is when a child or teen is threatened, harassed, humiliated, embarrassed or otherwise targeted by another child or teen using the Internet, interactive and digital technologies or mobile phones.

No single factor puts a child at risk of being bullied or bullying others. Bullying can happen anywhere—cities, suburbs, or rural towns. Depending on the environment and socially isolated youth—may be at an increased risk of being bullied.

In order to prevent cyberbullying it is important to recognize the risk factors and which members of our youth are more likely to be targeted for cyberbullying than others. By recognizing these risk factors we can better prepare and educate youth about the dangers of cyberbullying and how to protect one self.

Social Networking

Cyberbullying has increased with the rising popularity of social media, online chat rooms, blogs and personal websites. Social networking cannot be totally blamed for the actions of cyberbullies. While social networking sites may provide a medium with which cyberbullies attack others, the site itself did not create the bully nor did it encourage the behaviour. A bully is still a bully whether they exist in the online realm or in the physical world. That being said, youth who participate in social networking sites or post personal information on websites or blogs are more likely to be cyberbullied. One way to prevent cyberbullying is to adjust your account settings to private to avoid unwanted visitors seeking private information.

Gender

According to the Cyberbullying Research, girls are more likely than boys to experience cyberbullying. Girls are also more likely to engage in cyberbullying behaviour such as posting unwanted photos of others online and using social networking sites to embarrass others. Girls are not the only ones guilty of cyberbullying though. According to their research more boys than girls admitted to sending emails to ridicule or anger others.

In gaming

Sexual harassment as a form of cyberbullying is common in video game culture. A recent study says that this harassment is due in part to the portrayal of women in video games. This harassment generally involves slurs directed towards women, sex role stereotyping, and overaggressive language.

Children at Risk of Being Bullied

Generally, children who are bullied have one or more of the following risk factors:

- Are perceived as different from their peers, such as being overweight or underweight, wearing glasses or different clothing, being new to a school, or being unable to afford or cope up with peer children
- Are perceived as weak or unable to defend themselves
- Are depressed, anxious, or have low self esteem
- Are less popular than others and have few friends
- Do not get along well with others, seen as annoying or provoking, or antagonize others for attention.

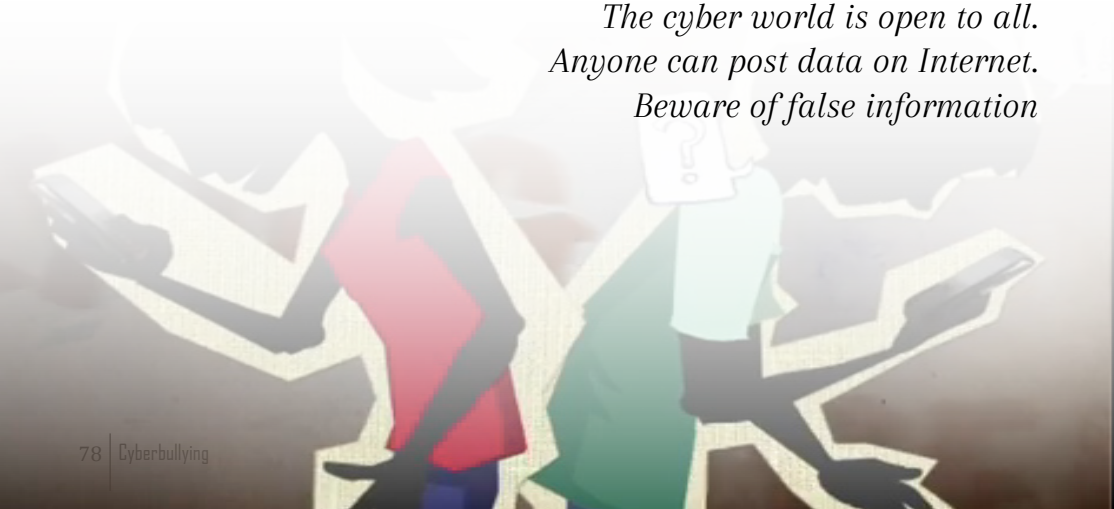
However, even if a child has these risk factors, it doesn't mean that they will be bullied.

Children More Likely to Bully Others

There are two types of kids who are more likely to bully others:

- Some are well-connected to their peers, have social power, are overly concerned about their popularity, and like to dominate or be in charge of others.
- Others are more isolated from their peers and may be depressed or anxious, have low self esteem, be less involved in school, be easily pressured by peers, or not identify with the emotions or feelings of others.

The cyber world is open to all.
Anyone can post data on Internet.
Beware of false information



Children who have these factors are also more likely to bully others;

- Are aggressive or easily frustrated
- Have less parental involvement or having issues at home
- Think badly of others
- Have difficulty following rules
- View violence in a positive way
- Have friends who bully others

Remember, those who bully others do not need to be stronger or bigger than those they bully. The power imbalance can come from a number of sources—popularity, strength, cognitive ability—and children who bully may have more than one of these characteristics.

Cyberbullying Effects

- Emotional distress: anger, frustration, embarrassment, sadness, fear, depression
- Interference with school work or job performance
- Quit job, drop out or switch schools
- Delinquency and violence
- Substance abuse
- Possession of weapons on school grounds
- Suicide

Cyber bullying can be done in the following ways:

- **Forwarding a private IM communication to others**
  A kid/teen may create a screen name that is very similar to another kid's name. The name may have an additional "i" or one less "e". They may use this name to say inappropriate things to other users while posing as the other person. Children may forward the above private communication so others to spread their private communication.
- **Impersonating to spread rumours**
  Forwarding gossip mails or spoofed mails to spread rumours or hurt another kid or teen. They may post a provocative message in a hate group's chat room posing as the victim, inviting an attack against the victim, often giving the name, address and telephone number of the victim to make the hate group's job easier.
- **Posting embarrassing photos or video**
  A picture or video of someone in a locker room, bathroom or dressing room may be taken and posted online or sent to others on cell phones.
- **By using web sites or blogs**
  Children used to tease each other in the playground; now they do it on Web sites. Kids sometimes create Web sites or blogs which may insult or endanger another

child. They create pages specifically designed to insult another kid or group of people.

- **Humiliating text sent over cell phones**
  Text wars or text attacks are when kids gang up on the victim, sending thousands of text-messages related to hatred messages to the victim's cell phone or other mobile phones.
- **Sending threatening e-mails and pictures through e-mail or mobile to hurt another**
  Children may send hateful or threatening messages to other kids, without realizing that while not said in real life, unkind or threatening messages are hurtful and very serious.
- **Insulting other user in Interactive online games**
  Kids/Teens verbally abuse the other kids/teens, using threats and foul language while playing online games or interactive games.
- **Stealing Passwords**
  A kid may steal another child's password and begin to chat with other people, pretending to be the other kid or by changing actual user profile.

How to prevent Cyber Bullying

When adults respond quickly and consistently to bullying behavior they send the message that it is not acceptable. Research shows this can stop bullying behavior over time. There are simple steps adults can take to stop bullying on the spot and keep kids safe.

Do:

- Intervene immediately. It is ok to get another adult to help.
- Separate the kids involved.
- Make sure everyone is safe.
- Meet any immediate medical or mental health needs.
- Stay calm. Reassure the kids involved, including bystanders.
- Model respectful behavior when you intervene.
- Avoid these common mistakes:
- Don't ignore it. Don't think kids can work it out without adult help.
- Don't immediately try to sort out the facts.
- Don't force other kids to say publicly what they saw.
- Don't question the children involved in front of other kids.
- Don't talk to the kids involved together, only separately.
- Don't make the kids involved apologize or patch up relations on the spot.

Tips and guidelines

- Use Parental Control Bars, Desktop Firewalls, Browser Filters to avoid or prevent-

ing children from cyber bullying others or accessing inappropriate content.

- Make sure your child's school has Internet Safety education programming.
- You may request school authorities to teach or guide students about how to prevent and respond to online peer harassment, interact wisely through social networking sites and responsible online users.
- Form the rules of computer Labs, Internet labs.
- Specify clear rules, Guidelines and policies regarding the use of the Internet, Computers and Other Devices such as USB, CDROM at School for Cyber Bullying.
- Teach Students the impact of Cyber Bullying.
- Teach students that all types of bullying are unacceptable and such behaviour is subject to discipline.
- Mentoring the students and establishment of peer Monitoring.
- Teachers need to mentor or establishment mentorship with senior students to guide information security awareness and monitoring through peer students
- **Implement Blocking/Filtering Software at Lab PCs in School.**
  Use Desktop Firewalls, Browser Filters to avoid or preventing children from cyber bullying other or accessing inappropriate content. In addition use monitoring with software tools for students online activity.
- **Educate your students.**
  Educate students by conducting various workshops from an internal or external expert to discuss related issues in cyber bullying, good online behaviour and other information security issues. Moreover keep related posters in school.

References:

http://www.stopbullying.gov
http://www.ohio.edu
http://en.wikipedia.org/wiki/Cyberbullying
http://stopcyberbullying.org

Online Predators

Online predators are internet users who exploit children and teens for sexual and violent purposes. This may include child grooming, engage in sexual activities, unwanted exposure of materials and pictures, online harassment, threats to cause fear or embarrassment . It is online harassment.

Communication tools used by online predators

Online predators use communication tools like social networking, email, chat rooms, instant messaging and also use grooming process for personal meetings.

- By using social networking web sites
  Social networking web sites are popular for expressing user's views, to post and share photos, and videos over websites. Online predators take advantage of these web sites and pretend to be a child and make online friendship and try to collect your personal details and gradually introduce sexual communications and engage you in sexual activities.

- **By using e-mail address**
  An online predator collect the email addresses of children and starts sending them photographs, links related to porn sites and try to abuse the children and insist child to involve in sexual communication by threats and makes children feel uncomfortable.
- **Through Chat rooms**

Online predators join into chat rooms and start chatting with children and try to pretend as a child to collect the personal information, build trust and try to be a good friend by asking about child's interests, hobbies, personal photographs, ask for private chats, offers gifts. Sometimes the predators will be very kind and affectionate toward a child and gradually introduce the sexual content in their conversation and ask a child to maintain secrecy by not informing parents. If a child doesn't agree they may threaten and abuse them into submission.

- **By Grooming Process**
  An online predator builds a false trust, relationships and breaks child's resistance and tries for iface to face meeting.

- *Always take security measures like privacy settings and set the limited view of your profile.*
- *Ignore or delete the mails from unknown users.*
- *It is suggested to hide personal information like interests, hobbies and family details to online friends.*
- *Do not get lead by any strangers into changing your habits and thoughts. Take your parents if you want to meet your online friend.*
- *Don't be scared of threats inform your parents and report to police.*

> *Online Predators make threats when you no longer want to chat with them and start forcing you for in person meeting by issuing threats to harm your family members and friends.*

How to prevent online predators?
If someone offers you gifts or without any reason wants to meet you and try to be very affectionate – these may be signs of an online predator

Recognize the techniques tried to mislead you.
If someone offers gifts and if some stranger for no reason asks you to meet personally and triesto be very affectionate, be aware that these are the tactics of online predators , they are trying t o mislead you.

Use nick names
Make sure to choose the user names without using your real names.

Don't fill your personal details in your online profile.
Don't post your personal details in social networking where everyone can see your details.

Set rules for online chatting
Set rules like time limit and use Internet under guidance of parents and make sure the computer is placed in the common room.

Avoid chats like gender, problems at home and schools
Always avoid the topics related to your gender, age, location, and don't share problems at home and school.

If you are threatened

- **Don't fear**
  Be cool, stop chatting and get out of the chat room or log off.

- **Don't be scared to say no**
  If you are not willing to do things asked by predator don't be scared to say no.

- **Inform to parents**
  If some one threatens you, immediately inform your parents.

- **Take a screen shot of your conversation as evidence and tell you will report to police.**
  If someone uses bad language or threatens, take a screen shot of your conversation and tell them that you would report to police.

- **Don't log off**
  If someone tries to abuse you don't logoff immediately, inform parents and inform the law enforcement.

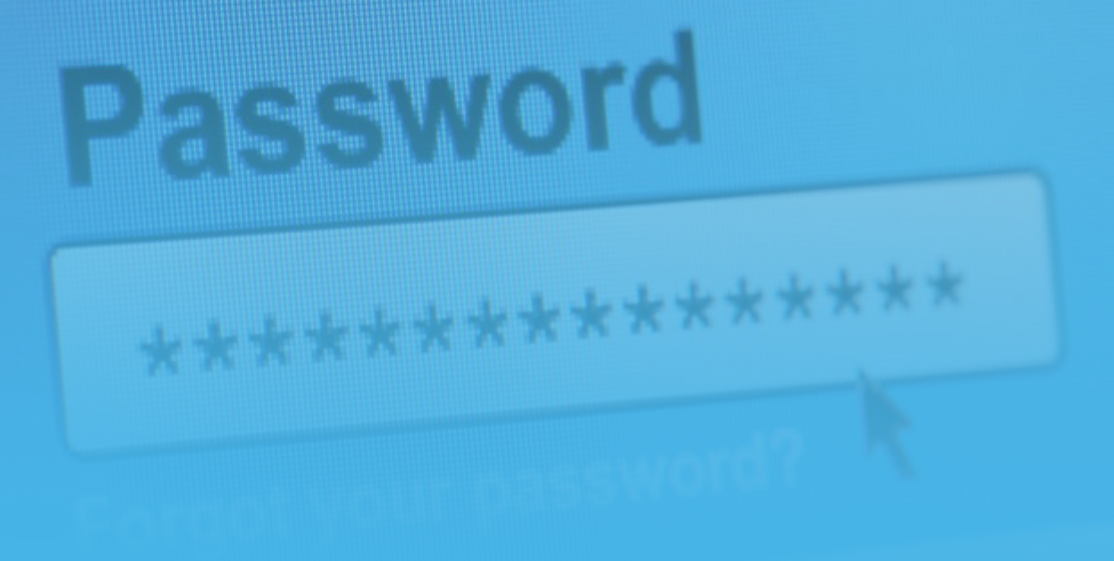
- **Contact cyber police**
  If something goes to the extreme like threatening to harm family members, immediately contact cyber police.

Are You getting offers from Lottery E-mails/Calls/SMS

like

They may be spooffed offers

Never respond



About Passwords

Password is a key or a Secret word or a string of characters which is used to protect your assets or information from others in the cyber world. It is used for authentication, to prove our identity or to gain access to our own resources. It should be kept secret to prevent access by unauthorized users.

In social networking sites like Facebook, Orkut, and LinkedIn each of which is studded with answers to commonly used security questions such as favourite place, school, college, etc..

Importance of Passwords

- Password represents the identity of an individual for a system.
- A password helps individuals in protecting personal information from being viewed by unauthorized users. Hence it is important to secure passwords.
- Password acts like a barrier between the users and his personal information

Possible Vulnerabilities with Passwords are

- Passwords could be shared with other persons and might be misused.
- Passwords can be forgotten
- Stolen password can be used by an unauthorized user who may collect your personal information
- Easy Passwords such as with name, date of birth, mobile numbers could be guessed by anybody and misuse them
- If you use same password for all accounts, It would be 90% of easy chances to the hackers to crack all account passwords

Various Techniques used by hackers/crackers to retrieve your passwords

Shoulder Surfing

One way of stealing the password is standing behind an individual and look over their shoulder to read their password while they are typing it. Shoulder Surfing is a direct observation technique, such as looking over someone's shoulder to get passwords, PINs, other sensitive personal information and even overhearing your conversation when you give your credit-card number over the phone.

Shoulder surfing is easily done in crowded places. It's comparatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM, or use a calling card at a public pay phone. It can also be done long distance with the help of binoculars or other vision-enhancing devices.

Your confidential information will be at risk if your passwords are observed by Shoulder Surfers. They can use your password information for logging into your account and they may do harm to your information.

Tip : *Explain to your children to be aware of Shoulder Surfers at public places like Internet*

Centers or schools while they are entering their passwords into the login accounts. Ask them to not to reveal their passwords in front of others or not to type their usernames and passwords before unauthorized persons. Ask them to cover the keyboard with paper or hand or something else to prevent then from being viewed by unauthorized users. Writing your passwords on papers or storing it on hard disk

Writing your passwords on papers or storing it on hard disk

Strangers search for papers or the disk for passwords where they have been written.

Tip : *Tell your children not to write the passwords on any paper or on any disk drive to store it. Explain to them that memorizing is the best way to store them.*

Brute force attacks

Another way of stealing the password is through guesses. Hackers try all the possible combinations with the help of personal information of an individual. They will try with the person's name, pet name (nickname), numbers (date of birth, phone numbers), school name… etc.. When there are large numbers of combinations of passwords the hackers use fast processors and some software tools to crack the password. This method of cracking password is known as "Brute force attack".

Tip: *Explain to your children not to use a password that represents their personal information like nicknames, phone numbers, date of birth, etc..*

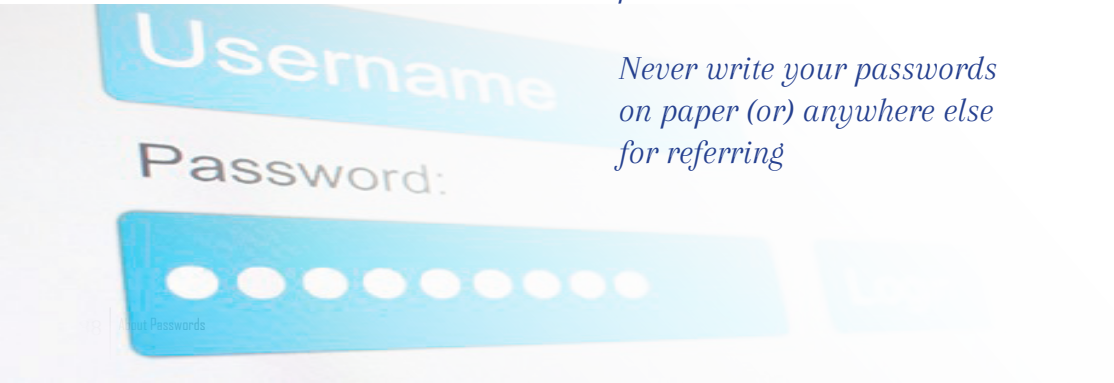
Dictionary attacks

Hackers also try with all possible dictionary words to crack your password with the help of some software tools. This is called a "Dictionary attack".

Tip: *Teach your children not to use dictionary words (like animal, plants, birds or meanings) while creating the passwords for login accounts.*

You are responsible for safeguarding your ID and password.

Never write your passwords on paper (or) anywhere else for referring



Sending your password information through network

The Hackers/Crackers even get the password information by sniffing the network traffic which is travelling on the network or even can get the password information by listening to your phone call conversation with others.

Tip: *Teach your children not to give their passwords to their friends or to anyone through online chatting, e-mails or even through phone conversations.*

Sharing your passwords with strangers

Sharing the passwords with unknown persons (strangers) may also lead to loss of your personal information. They can use your login information and can get access to your information. The operating system does not know who is logging into the system, it will just allow any person who enters the credential information into the login page. Strangers, after getting access to your information, can do anything with it. They can copy, modify or delete it.

Tip: *Explain to your children not to share their passwords with unknown persons (strangers).*

Strong and easiest to remember Password

A strong Password should have combinations of Alphabets, Numbers and Characters such as c.!@*^&)(~@. Remembering these passwords are very difficult. So can be made as shown below,

Using weak Passwords or blank passwords

Weak and blank passwords are one of the easiest ways for attackers to crack your system.

Tip: *Explain to your children that their information can be easily stolen or accessed by strangers if they use weak passwords. Ask them to "Use Strong Passwords".*

Things to be remembered while creating Strong Passwords

- Use at least 8 characters or more to create a password. The more number of characters we use, the more secure is our password.
- Use various combinations of characters while creating a password. For example, create a password consisting of a combination of lowercase, uppercase, numbers and special characters etc..
- Avoid using the words from dictionary. They can be cracked easily.
- Create a password such that it can be remembered. This avoids the need to write passwords somewhere, which is not advisable.
- A password must be difficult to guess.
- Change the password frequently at least 2 weeks once

Guidelines for maintaining a good password

- Change the password once in two weeks or when you suspect someone knows the password.
- Do not use a password that was used earlier.
- Be careful while entering a password when someone is sitting beside you.
- Store the passwords on computer with the help of an encryption utility.
- Do not use the name of things located around you as passwords for your account.

Your brain is the best place to store your passwords

Beware of shoulder surfing

Make sure you donot use remenber password option in browser

Do not use your name, or family name, or birth place, etc. as passwords

Avoid using dictionary words as password

Mobile Phone Security

Mobile phones are becoming ever more popular and are rapidly becoming attractive targets for malicious attacks. Mobile phones face the same security challenges as traditional desktop computers, but their mobility means they are also exposed to a set of risks quite different to those of a computer in a fixed location. Mobile phones can be infected with worms, trojan horses or other virus families, which can compromise your security and privacy or even gain complete control over the device. This guide provides the necessary steps, do's, don'ts & tips to secure your mobile devices.

Steps to be followed before Mobile Phone usage :

- Read the manufacturer's manual carefully and follow the guidelines as specified to setup your mobile phone.
- Record the IMEI (International Mobile Equipment Identity) number for tracking your mobile in case you lose it.

Note: This is usually printed on the phone below the battery, or can be accessed by keying *#06# on most of the phones.

For more information refer to manufacturer manual

Mobile Phone Security Threats Categories :

- Mobile Device and Data Security Threats
  - Threats related to unauthorised or intentional physical access to mobile phone and Lost or Stolen mobile phones.
- Mobile Connectivity Security Threats
  - Threats related to mobile phone connectivity to unknown systems, phones and networks using technologies like Bluetooth, WiFi, USB etc.
- Mobile Application and Operating System Security Threats
  - Threats arising from vulnerabilities in Mobile Applications and Operating Systems.

Typical impact of attacks against Mobile Phones :

- Exposure or Loss of user's personal Information/Data, stored/transmitted through mobile phone.
- Monetary Loss due to malicious software unknowingly utilizing premium and highly priced SMS and Call Services.
- Privacy attacks which includes the tracing of mobile phone location along with private SMSs and calls without user's knowledge.
- Loosing control over mobile phone and unknowingly becoming zombie for targeted attacks.

Mitigation against Mobile Device and Data Security Attacks :

Mobile Device

Do's

Record IMEI number:

Record the unique 15 digit IMEI number. In case Mobile phone is stolen/lost, this IMEI number is required for registering complaint at Police station and may help in tracking your mobile phone through service provider.

Enable Device locking:

Use autolock to automatically lock the phone or keypad lock protected by passcode/ security patterns to restrict acess to your mobile phone.

Use a PIN to lock SIM card:

Use a PIN (Personal Identification Number) for SIM (Subscriber Identity Module) card to prevent people from making use of it when stolen. After turning on SIM security, each time phone starts it will prompt to enter SIM PIN.

Use password to protect information on the memory card.

Report lost or stolen devices
Report lost or stolen devices immediately to the nearest Police Station and concerned service provider. Use mobile tracking feature.
Use the feature of Mobile Tracking which could help if the mobile phone is lost/stolen. Every time a new SIM card is inserted in the mobile phone, it would automatically send messages to two preselected phone numbers of your choice, so that you can track your Mobile device.

Don'ts:
Never leave your mobile device unattended.
Turn off applications [camera, audio/video players] and connections [Bluetooth, infrared, Wi-Fi] when not in use. Keeping the connections on may pose security issues and also cause to drain out the battery.

Data Security:

Do's:

Backup data regularly
Backup data regularly and set up your phone such that it backs up your data when you sync it. You can also back up data on a separate memory card. This can be done by using the Vendor's document backup procedure.

Reset to factory settings:
Make sure to reset to factory settings when a phone is permanently given to another user to on sure that personal data in the phone is wiped out.

> *Activate your pin code request for your mobile phone access. Choose a pin which is not easily predictable but something which you can remember easily.*

Mitigation against Mobile Connectivity Security Attacks:

Bluetooth:

Bluetooth is a wireless technology that allows different devices to connect to one another and share data, such as ringtones or photos. Wireless signals transmitted with Bluetooth cover short distanes, typically 30 feet (10 meters).

Do's:

- Use Bluetooth in hidden mode so that even if the device is using Bluetooth it is not\visible to others.

- Change the name of the device to a different name to avoid recognition of your Mobile phone model.
- Note: The default name will be the mobile model number for Bluetooth devices.
- Put a password while pairing with other devices. The devices with the same password can connect to your computer
- Disable Bluetooth when it is not actively transmitting information.
- Use Bluetooth with temporary time limit after which it automatically disables so that the device is not available continuously for others.

Don'ts:

- Never switch on Bluetooth continuously.
- Never put Bluetooth in always discoverable mode.
- Note: Attackers can take advantage of its default always-on, always discoverable settings to launch attacks.

> *Be cautious while downloading the applications through bluetooth or as an MMS attachment.*

Mobile as USB:

The mobile phones can be used as USB memory devices when connected to a computer. A USB cable is provided with the mobile phone to connect to computer. Your mobile's phone memory and memory stick can be accessed as USB devices.

Your mobile's phone memory and memory stick can be accessed as USB devices.

Do's:

- When a mobile phone is connected to a personal computer, scan the external phone memory and memory card using an updated anti virus.
- Take regular backup of your phone and external memory card because if an event like a system crash or malware penetration occurs, at least your data is safe.
- Before transferring the data to Mobile from computer, the data should be scanned with latest Antivirus with all updates.

Don'ts:

- Never keep sensitive information like user names/passwords on mobile phones.
- Never forward the virus affected data to other Mobiles.

Wi-Fi

Wi-Fi is short for "Wireless Fidelity." Wi-Fi refers to wireless networking technology that allows computers and other devices to communicate over a wireless signal. Many mobile devices, video game systems, and other standalone devices also include Wi-Fi capability, enabling them to connect to wireless networks. These devices may be able to connect to the Internet using Wi-Fi.

Do's:

- Connect only to the trusted networks.
- Use Wi-Fi only when required. It is advisable to switch off the service when not in use.
- Beware while connecting to public networks, as they may not be secure.

Don'ts:

- Never connect to unknown networks or untrusted networks.

> *Read your mobile phone's operating instructions particularly security settings, pin code settings, Bluetooth settings, and infrared settings, etc. very carefully.*

Mitigation against Mobile Application and Operating System Attacks:

Application and Mobile Operating System:

- Update the mobile operating system regularly.
- Upgrade the operating system to its latest version.
- Always install applications from trusted sources.
- Consider installing security software from a reputable provider and update them regularly.
- It's always helpful to check the features before downloading an application. Some applications may use your personal data.
- If you're downloading an app from a third party, do a little research to make sure the app is reputable.

> Dial 112 your mobile will search for any existing network to establish the emergency number for you
>
> Interestingly this number can be dialed even if the keypad is locked

> Dial *#06# to record 15 digit IMEI number

Security Concerns

Exposure of critical information

Small amounts of WLAN signals can travel significant distance, and it's possible to peep into these signals using a wireless sniffer. A wireless intruder could expose critical information if sufficient security isn't implemented.

Lost or Stolen devices

Even if sufficient security is implemented in wireless Virtual Private Networks (VPNs), if a device is lost or stolen. the entire corporate intranet could be threatened if those devices aren't protected by a password and other user-level security measures.

Bluejacking

Bluejacking is sending nameless, unwanted messages to other users with Bluetooth enabled mobile phones or laptops. Bluejacking depends on the capability of Bluetooth phones to detect and contact another Bluetooth enabled device . The Bluejacker uses a feature originally proposed for exchanging contact details or electronic business cards. He or she adds a new entry in the phone's address book, types in a message, and chooses to send it via Bluetooth.The phone searches for other Bluetooth phones and, if it finds one, sends the message. Despite its name, Bluejacking is essentially harmless. The Bluejacker does not steal personal information or take control of your phone.

Bluejacking can be a problem if it is used to send obscene or threatening messages or images, or to send advertising. If you want to avoid such messages, you can turn off Bluetooth, or set it to "undiscoverable".

Bluesnarfing

Bluesnarfing is the theft of data from a Bluetooth phone. Like Bluejacking, Bluesnarfing depends on the ability of Bluetooth-enabled devices to detect and contact others nearby.

In theory, a Bluetooth user running the right software on a laptop can discover a near by phone, connect to it without your confirmation, and download your phonebook, pictures of contacts and calendar. Your mobile phone's serial number can also be downloaded and used to clone the phone.

You should turn off Bluetooth or set it to "undiscoverable". The undiscoverable setting allows you to continue using Bluetooth products like headsets, but means that your phone is not visible to others.

Mobile Viruses

Mobile Viruses can be major threat, particularly with devices that have significant computational capabilities. Mobile devices, in general are susceptible to Viruses in several ways. Viruses can take advantage of security holes in applications or in applications or in the underlying Operating System and cause damage. Applications downloaded to a mobile device can be as Virus-prone as desktop applications. In some mobile OS, malformed SMS messages can crash the device.

E-mail Viruses

E-mail Viruses affect PDAs in much the same way regular e-mail Viruses affect PCs. These Viruses are costly to enterprises and interrupt normal business too. PalmOS / LibertyCrack is an example of a PDA e-mail virus. It's a known Trojan horse that can delete all applications on a Palm PDA.

Malicious softwares like Worms, Spywares and Trojans

Worms may disturb the phone network by spreading from one mobile to other mobile through Bluetooth transfer, Infrared transfer or through MMS attachments. Spyware that has entered into the mobile phone through Bluetooth may transfer the personal information to the outside network. The Trojan which got installed along with the game application in the mobile may send SMS messages to expansible members and may increase the phone bill.

Guidelines for securing mobile devices

- Be careful while downloading applications through Bluetooth or as MMS attachments. They may contain some harmful software, which will affect the mobile phone.
- Keep the Bluetooth connection in an invisible mode, unless you need some user to access your mobile phone or laptops. If an unknown user tries to access the mobile phone or laptop through blue tooth, move away from the coverage area of blue tooth so that it automatically gets disconnected.
- Avoid downloading the content into mobile phone or laptop from an untrusted source.
- Delete the MMS message received from an unknown user without opening it.
- Read the mobile phone's operating instructions carefully mainly regarding the security settings, pin code settings, Bluetooth settings, infrared settings and procedure to download an application. This will help in making your mobile phone secure from malicious programs.
- Activate the pin code request for mobile phone access. Choose a pin, which is unpredictable and which is easy to remember for you.
- Use the call barring and restriction services provided by operators, to prevent the applications that are not used by you or by your family members.
- Don't make you mobile phone as a source for your personal data, which is dangerous if it falls in to the hands of strangers. It is advisable not to store important information like credit card and bank cards passwords, etc in a mobile phone.
- Note the IMEI code of your cell phone and keep it in a safe place. This helps the owner to prevent access to the stolen mobile. The operator can block a phone using the IMEI code.
- Regularly, backup important data in the mobile phone or laptop by following the instructions in the manual.
- Define your own trusted devices that can be connected to mobile phone or laptop through Bluetooth.
- Use free cleansing tools, which are available in the Internet to make your mobile work normally, when ever it is affected by malicious soft wares.

Location tracking services allow the whereabouts of registered cell phones to be known and monitored. While it can be done openly for legitimate purposes, it may also be used for malicious purposes.

Check the source of all your files and apps to make sure they’re safe before you download.

Secure Usage of Credit & Debit Card/ATM

Security Threats

Identity theft

The fraudulent acquisition and use of person's private identifying information, usually for financial gain. It can be divided into two broad categories :

- **Application fraud**
  Application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information.
- **Account takeover**
  Account takeover happens when a criminal tries to take over another person's account, first by gathering information about the intended victim, and then contacting their card issuer while impersonating the genuine cardholder, and asking for the mail to be redirected to a new address. The criminal then reports the card loss and asks for a replacement to be sent.

Credit card fraud

Credit card fraud is commited by making use of credit/debit card of others for obtaining goods or services. The threat emerge due to stealing of information like Credit card number, PIN number,password etc. Theft of cards and cloning of cards are also employed to commit such frauds.

Hackers use complex techniques like Phishing, Skimming etc. to gain credit card information from innnocent users.

- **Phishing**

  Phishing is a way of attempting to acquire information such as usernames, passwords, and creditcard details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

- **Skimming**

  Skimming is the theft of credit card / Debit card information. Thief can procure victim's credit card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victim's credit card numbers. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card and makes note of card details for further use.

- **Vishing**

  It is one of the method of social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and "phishing".

- **Social Engineering**

  Social engineering involves gaining trust – hence the fraudster poses as a member of staff or even security guard. The fraudster would then ask the customer to check the card for damages. The fraudster would have gained confidence from his prey using various tactics such as offering assistance to the customer who perhaps would have tried to use the ATM without success or perhaps the customer who is not familiar with use of ATM machine and requires assistance.

Be careful with credit card transaction for online shopping

Always be careful about fraudulent / phishing e-mails

Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction

Be aware of social engineering attacks on mobile and bluetooth devices

Steps to be followed before Credit card & Debit card/ATM card usage

- Whenever you receive the card from the bank make sure the mail is completely sealed and there is no damage.
- Whenever you receive the card from the bank immediately sign on the card.
- Try to cover the last three digit number on the card.
- Register your phone number to check the account transactions.
- Change the pin number immediately.

Secure usage of Credit/Debit cards at Shopping malls and Restaurants

- Always keep an eye how the vendor swipe your card.
- Always make sure that the transactions happen at your presence.
- Never sign a blank credit card receipt. Carefully draw a line through blank portions of the receipt
- Don't give away your personal information in the survey forms given in restaurants/shopping malls.

Secure usage of Credit / Debit card over Internet

- Always use secure websites for transaction and shopping.
- Please look for signs of security.

  Identify security clues such as a lock image at the bottom of your browser,
  A URL that begins with https:
  (These signs indicates that your purchases are secured with encryption to protect Your account information)
- Always shop with merchants you know and trusts.
- Always log off from any website after completing online transaction with your credit / debit card and delete the browser cookies
- Treat all e-mail messages with suspicion to avoid phishing scams. Do not respond to e-mail messages asking for personal information including financial information, as banks do not ask for such information.
- Never send payment information via e-mail. Information that travels over the Internet (such as e-mail) may not fully protected from being read by outside parties.
- Please be careful when providing personal information online.
- Please be wary of promotional scams. Identity thieves may use phony offers asking for your personal information.
- Please keep your passwords secret. Some online stores may require you to register with them via a username and password before buying. Online passwords should be kept secret from outside parties the same way you protect your ATM PIN.
- Always make sure to use the virtual keyboard for net banking.

Do's

- Before you use an ATM, please ensure that there are no strange objects in the insertion panel of the ATM.(to avoid skimming)
- Shield the ATM pin number during transaction. Don't carry the transaction receipts along.
- Please change your ATM PIN once in every 3 months. As advised by banks.
- Keep your credit card receipts to guard against transaction frauds, check your receipts against your monthly statement.
- Only carry around credit cards that you absolutely need.
- Shred anything that contain your credit card number written on it. (bills)
- Notify your credit card issuers in advance of your change of address, then you change home address.
- If you lose your credit card, please report the loss immediately.
- When you dispose a card at the time of renewal/upgradation, please make sure to cut it diagonally before disposal.

Don'ts

- Don't accept the card received directly from bank in case if it is damaged or seal is open.
- Don't write your PIN number on your credit card.
- Don't carry around extra credit cards that you rarely use.
- Don't disclose your Credit Card Number/ATM PIN to anyone.
- Don't hand over the card to anyone, even if he/she claims to represent the Bank.
- Don't get carried away by strangers who try to help you use the ATM machine.
- Don't use the ATM machines if the device is not in good conditions.
- Don't transfer or share your account details with unknown/non validated source.
- Don't access Net banking or make payment using your Credit/Debit card from shared or unprotected computers in public places.
- Don't open unexpected e-mail attachments from unexpected sources or instant message download links. Delete suspicious e-mail immediately.
- Don't give out your account number over the phone unless you initiate the call and you know the company is reputable. Never give your credit card info out when you receive a phone call. (This is called Vishing)
- Don't provide your credit card information on a website that is not a secure site.
- Don't share any confidential information such as password, customer id, Debit card number, Pin CVV2, DOB to any email requests, even if the request is from government authorities like Income Tax department, RBI or any card association company like VISA or Master card.
- Don't address or refer to your bank account problems or your account details and password on social networking site or blogs.
- Don't store critical information like your ATM PIN number on your mobile phone.

Be aware of Credit/Debit Card Frauds

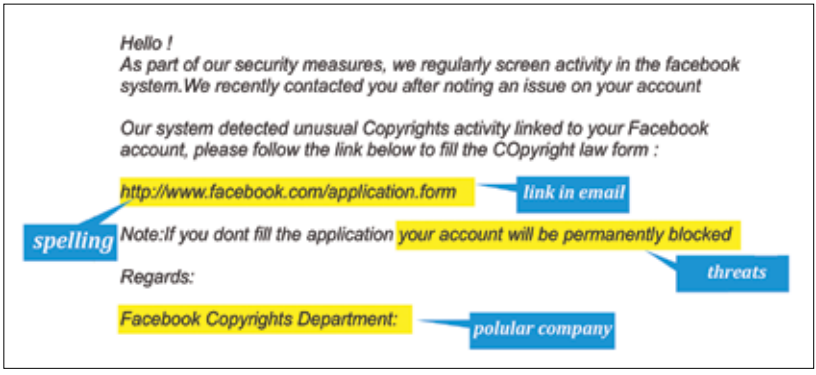
- Don't share bank account,Credit/Debit card details through E-mail or phone
- Don't hand over Debit/Credit Card to strangers
- They may misuse them

Phishing Attacks

Phishing is a way of attempting to acquire information such as usernames, passwords, PIN,bank account, credit card details by masquerading as a trustworthy entity details through electronic communication means like e-mail.

Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users.

How does a phishing email message look like? In detail



- Spelling and grammar.
- Links might also lead you to .exe files. These kinds of file are known to spread malicious software.

Threats

- Sometimes you may receive a threat mail saying that your webmail account would be closed if you do not respond to an e-mail message. The e-mail message shown above is an example of the same trick. Cybercriminals often use techniques to make one belive that security has been compromised.
- Spoofing popular websites or companies.
- Scam artists use graphics in email that look identical to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows.
- Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered.
- Cybercriminals might call you on the phone and offer to help solve your computer problems or sell you a software license.

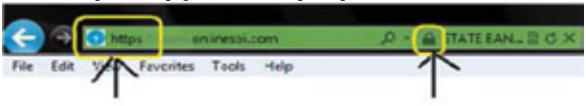
Know that phishing can also happen by phone. So, never give personal information by phone

Steps to remember :

Don't enter your information in the websites that start with numbers

So Always key in the URL in the address bar yourself don't copy and paste

Step3: Always perform online banking in secure channel i.e check for the Padlock and



Always check for the trusted website which has https and padlock

Step 4 : Always view any email request for financial or other personal information with suspicion, particularly any "urgent" requests. When in doubt, do not respond to questionable email or enter information on questionable websites. You may also contact the alleged sender to confirm the legitimacy of communications you've

An Example of Phishing site, the look and feel of the Punjab national bank is same.

Step 5 : Never respond to the emails that ask for your personal information like credit card /debit card/bank information.

Here are the few Phishing techniques

- Social networking sites are now a prime target of phishing, since the personal details in such sites can be used in identity theft.
- One of the latest phishing techniques is tabnabbing. It takes advantage of the multiple tabs that users use and silently redirects a user to the affected site.
- **Filter Evasion** - Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing e-mails.
- **Phone Phishing** - Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Visher sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.
- Another attack used successfully is to forward the client to a bank's legitimate website, then to place a popup window requesting credentials on top of the website in a way that it appears the bank is requesting this sensitive information

Never open/reply/forward suspicious e-mail.

How I can recognize a message of phishing?

- Normally phishing e-mails display grammatical errors or overlapped text.
- Test using false data before putting in actual information.

What should I do if I think I've responded to a phishing scam?

- Take these steps to minimize any damage if you suspect that you've responded to a phishing scam
- with personal or financial information or entered this information into a fake website.
- Change the passwords or PINs of all your online accounts that you think could be compromised.
- Place a fraud alert on your credit reports. Check with your bank or financial advisor if you're not sure how to do this.
- Contact the bank or the online merchant directly. Do not follow the link in the fraudulent e-mail.
- Routinely review your bank and credit card statements for unexplained charges or inquiries that you didn't initiate.

Be on alert for Phishing email scam

Never click links in e-mail which starts with IP address

Never send credit card number or other personal details through e-mail

Do's

- Be cautious about opening any attachments or downloading files you receive regardless of who sent them.
- Look for the sender email ID before you enter/give away any personal information.
- Use antivirus, antispyware and firewall software (update them regularly too).
- Always update your web browser and enable phishing filter.
- If you receive any suspicious e-mail do call a company to confirm if it is legitimate or not.
- Do use a separate email accounts for things like shopping online, personal etc.

Dont's

- Don't reply to an e-mail or pop-up message that asks for personal or financial information.
- Don't e-mail personal or financial information i.e credit card or other sensitive information via e-mail.
- Don't click on any email or social media messages you don't expect or need.
- Don't open e-mail that you have any suspicion may not be legitimate. If it is legitimate and the individual trying to contact you really needs to, they will try another means.
- Don't open attachments that you were not expecting, especially ZIP files and NEVER run .exe files.
- Don't use your company e-mail address for personal things.
- Don't open any spam e-mail.
- Don't open suspicious videos or images in social networking sites since social networking are prime target of phishing.
- Never respond to phone calls asking for bank details. It might be vishing (voice phishing).
- Beware of phishing phone calls.
- Don't respond if you receive any message(sms) asking you to confirm account information that has been "stolen" or "lost" or encouraging you to reveal personal information in order to receive a prize, it's most likely a form of phishing.

Wi-Fi Security

Internet users are widely using Wi-Fi devices to access Internet. Every year millions of Wi-Fi devices are sold in the market. Out of these most of the wireless devices are vulnerable in their default configuration mode. Since end users are not fully aware of security levels to be set on these devices, these get rendered vulnerable. By taking advantage of these unsecured Wi-Fi devices terrorists and hackers fulfill their needs.

Anyone with Wi-Fi connectivity in his computer, laptop or mobile can connect to unsecured Access Points(wireless routers). Anyone in the range of Access point can connect to an Access Point if it is unsecured. Once the connection is established the attacker can send mails, download classified/confidential stuff, initiate attack on other computers in the network, send malicious code to others, install a Trojan or botnet on the victims computer to get long term control on it through Internet, etc.

All these criminal acts will naturally be associated with the legal user of Access Point (wireless router). It is up to the legal user of the Access Point to defend himself to prove that he has not been involved in these acts. It now becomes the responsibility of the user to secure his/her own Access Point.

Never auto-connect to open Wi-Fi networks in public places

There are some real incidents that took place in the recent years.

- Terrorists and hackers used unsecured Access Points to perform illegal activities on the Internet.
- Hackers penetrated into open Wi-Fi network of luxury hotels owned by the Thompson Group in New York, Los Angeles and Washington DC and stole the private emails sent by the guests.The hackers then attempted to extort money from the hotel chain by threatening to publish the emails.(www.crpcc.in)
- Just 5 minutes before Delhi blasts on September 2008 terrorists used an unsecured Wi-Fi connection of a company at Chembur in Mumbai to send terror emails to authorities and news channels. These hackers do not leave a trail of footprints for the investigators to arrive at a logical conclusion. The audit trail ends at Wi-Fi Access Point of the legal user. So it is becomes imperative for the users to secure their own Access Points(wireless router). The following are the steps to secure an Access Point.

Types of attacks on wireless environment

- Denial of Service Attack

  Denial of Service Attack aims at preventing the users from accessing the network resources. In a Wireless network, denial of service attack can be applied in various ways.
- Man-In-Middle Attack in Wifi Devices

  Performing Man-In-Middle Attack in a wireless network is much easier, when compared to wired network. As the transmissons from an accesspoint is broadcasted, it is easy for an unauthorised user to collect the traffic sent by other wireless clients. And the process of collecting the packets in this manner is known as Eavesdropping. Also the third party user can manipulate the packets sent to the legitimate users which results in breaking the users privacy.

  So In order to avoid these kind of attacks, Strong encryption should be used for transmitting the data between wireless client and accesspoint.
- WarDriving

  It is a process of tracking Wi-Fi hotspots located at a particular place, while moving with a hand held device or a laptop in a vehicle. This helps the user in finding out the accesspoints that doesnot use encryption and takes control over it for performing the attacks on the network.

- *All Wi-Fi equipment support some form of encryption. So, enable them*
- *Enable MAC address filtering on Wi-Fi devices*
- *Avoid dynamic IP address for home Wi-Fi rather use static IP addresses*
- *Use encryption technology for sensitive data in wireless networks*

How the attack occurs in Wifi Environment ?

- At the physical layer of TCP/IP Model, denial of service attack can be implemented by introducing a device which will generate noise in the same frequency band in which wireless accesspoint is operating. This makes the users who are trying to connect to the accesspoint may not be able to connect to it.
- Also the other possibility of Denial of service Attack is spoofing the accesspoint. Normally wireless clients connect to the wired network with the help of an accespoint. For associating with the accesspoint they require SSID of it. When an unauthorised user places an accesspoint with the same SSID, then there is a chance of authorised user getting associated with the attackers accesspoint. If that happens, the attacker will try to collect sufficient number of packets from the wireless client and cracks the WEP key used by the legitimate accesspoint. Then the attacker gets associated with the legitimate accesspoint and generates large ping requests in the network or generate some abnormal traffic, which may finally result in Denial of Service Attack.

Tips for securing Wireless Communications

- **Always use strong password for encryption**
  A strong password should have atleast 15 characters, uppercase letters, lowercase letters, numbers and symbol. Also it is recommended to change the encryption key frequently so that it makes difficult for the cracker to break the encryption key. Do not use WEP for encryption, rather use WPA/WPA2.
- **Always use the maximum key size supported by access point for encryption**
  If the keysize is large enough, then it takes more time to crack the key by the hacker. Also it is recommneded to change the encryption key frequently so that it makes difficult for the cracker to break the encryption key.

- **Isolate the wireless network from wired network with a firewall and a antivirus gateway.**
  Do not connect the accesspoint directly to the wired network. As there is a chance of comprimised wireless client inturn effecting the systems in the wired network, a firewall and an antivirus gateway should be placed between the accespoint and the wired network.
- **Restrict access to the Access Point based on MAC address**
  In order to allow authorized users to connect to the Access Point, wireless clients should be provided access based on MAC address.
- **Shutdown the Access Point when not in use**
  Hackers try to brute force the password to break the keys, so it is good practice to turn off the Access points during extended periods of Non-use.
- **Change the default username and Password of the Access Point**
  Most of the users do not change the default passwords while configuring the Access Point.But it is recommended to keep a strong password, as this default password information can be known from product manufacturers.
- **Do not broadcast your network name**
  SSID information is used to identify a Access Point in the network and also the wireless clients connect to the network using this information. Hence, in order to allow authorized users to connect to the network, the information should not be provided in public.
- **Always maintain a updated firmware**
  Updating the firmware of accesspoint is recommended, as it will reduce the number of security loop holes in the accesspoint.
- **Use VPN or IPSEC for protecting communication**
  When the information flowing from wireless client to the wired network receiver is critical, then it is recommended to use VPN or IPSEC based communication so that the information is protected from sniffers in the network.
- **Do not make the SSID information public**
  SSID information is used to identify a accesspoint in the network and also the wireless clients connect to the network using this information. Hence, in order to allow authorised users to connect to the network, the information should not be provided in public.
- **Disable DHCP service**
  When the number of users accessing the Access Point is less, it is recommended to disable the DHCP service. As this may make the attackers easy to connect to the network once they get associated with the Access Point.

Security Tools for Windows Operating System

Malicious Software Removal Tool

The Microsoft Windows Malicious Software Removal Tool helps remove specific, prevalent malicious software from computers that are running Windows 7, Windows Vista, Windows Server 2003, Windows Server 2008, or Windows XP. When the detection and removal process is complete, the tool displays a report describing the outcome, including which, if any, malicious software was detected and removed.

The easiest way to download and run the tool is to turn on Automatic Updates; this guarantees that you receive the tool automatically every month. If you have Automatic Updates turned on, you have already been receiving new versions of this tool monthly. The tool runs in quiet mode unless it finds an infection. If you have not been notified of an infection, no malicious software has been found that needs your attention.

Note: If your computer is running Windows XP Service Pack 2 (SP2), Automatic Updates is turned on by default.

The Microsoft Malicious Software Removal Tool does not replace an antivirus product. The tool differs from an antivirus product in three key ways:

- It removes malicious software from an already-infected computer. Antivirus products block malicious software from running on a computer. It is significantly more desirable to block malicious software from running on a computer than to remove it after infection.
- It removes only specific prevalent malicious software. Specific prevalent malicious software is a small subset of all the malicious software that exists today.
- It focuses on the detection and removal of active malicious software. Active malicious software is malicious software that is currently running on the computer. The tool cannot remove malicious software that is not running. However, an antivirus product can perform this task.

Note: Visit for more information http://www.microsoft.com/security/default.aspx

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) lets users, administrators scan local and remote systems for missing security update as well as common security misconfigurations.

Download from https://www.microsoft.com/en-us/download/details.aspx?id=7558

Microsoft Security Compliance Manager Tool (SCM)

An end-to-end Solution Accelerator which will help you plan, deploy, operate, and manage your security baselines for Windows client and server operating systems, and Microsoft applications. This Solution Accelerator provides centralized security baseline management features, a baseline portfolio, customization capabilities, and security baseline export flexibility to accelerate your organization's ability to efficiently manage the security and compliance process for the most widely used Microsoft technologies

Download from https://www.microsoft.com/en-us/download/details.aspx?id=16776

UrlScan Security Tool

UrlScan screens all incoming requests to the server by filtering the requests based on rules that are set by the administrator. Filtering requests helps secure the server by ensuring that only valid requests are processed. The UrlScan security tool comprises two files ? UrlScan.dll and UrlScan.ini ? that are packaged together in UrlScan.exe. This latest update of UrlScan 2.5 gives administrators even greater control over UrlScan configuration and provides functionality that helps administrators further secure and lock down the server.

Download from http://www.iis.net/learn/extensions/working-with-urlscan/urlscan-3-reference

Microsoft Security Essentials

Microsoft Security Essentials is a free* download from Microsoft that is simple to install, easy to use, and always kept up-to-date so you can be assured your PC is protected by the latest technology.

Microsoft Security Essentials runs quietly and efficiently in the background so you're free to use your Windows-based PC the way you want—without interruptions or long computer wait times.
Before installing Microsoft Security Essentials, we recommend that you uninstall other antivirus software already running on your PC. Running more than one antivirus program at the same time can potentially cause conflicts that affect PC performance
Download from https://www.microsoft.com/en-us/download/details.aspx?id=5201

Note: The Microsoft Malicious Software Removal Tool does not remove spyware. To help detect and remove spyware, you can download Microsoft Security Essentials.

Secure It Pro 4.70.0117

Use Secure It Pro to lock your computer when you're not there. The program comes with a ton of features: Disabling the main Windows key functions, like Ctrl+Alt+Del, Alt+Tab, the Windows key, and the Ctrl+Esc key combination. Secure It Pro can also disable the Windows boot keys, detect for cold boots, allow other people to leave messages, log incorrect password attempts, or even hide itself every few seconds. The program also includes password reminder options, which can assist you if you ever forget your password, as well as several advanced configuration options as well as a locking screen saver.

http://www.cleansofts.com/get/945/17903/SecureIT_Pro_470.html

PC Locker Pro

PC Locker Pro is a Freeware that locks and protects your computer when you leave.

http://pc-locker-pro.en.softonic.com/

Steady state

It's simple to create, modify, and remove user profiles with Windows Steady State. There's no need to log in to the user account, edit the registry, or manipulate files or folders on the hard drive. You control all user restrictions directly from the main console. Rapidly assign high, medium, or low security defaults to each user profile. Then fine tune the profiles precisely, using the many available options in Windows Steady State.

http://www.microsoft.com/windows/products/winfamily/sharedaccess/default.mspx

MBSA

Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool designed for the IT professional that helps small and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. Built on the Windows Update Agent and Microsoft Update infrastructure, MBSA ensures consistency with other Microsoft management products including Microsoft Update (MU), Windows Server Update Services (WSUS), Systems Management Server (SMS) and Microsoft Operations Manager (MOM). Apparently MBSA on average scans over 3 million computers each week.

http://www.microsoft.com/technet/security/tools/mbsahome.mspx

Microsoft Office Visio 2007 Connector

Do you know the security status of your network? Get a visual. The Visio 2007 Connector for Microsoft Baseline Security Analyzer (MBSA) lets you view the results of an MBSA scan in a clear, comprehensive Microsoft Office Visio 2007 network diagram. You must have both Visio 2007 Professional and MBSA 2.1, a free security tool from Microsoft, for this connector to work properly.

Virus Protection and Cleaner Tools

Windows Based Tools

- **Avast Home Edition**
  - Standard Shield — Real-time protection
  - IM shield — Instant Messenger protection
  - P2P shield — P2P protection
  - Internet Mail — E-mail protection
  - Outlook/Exchange — Microsoft Outlook/Exchange protection
  - Web Shield — HTTP protection (local transparent proxy)
  - Script blocker — script checker (Pro version only)
  - Network Shield — basic protection against well-known network worms.
  - Acts as a lightweight Intrusion Detection System
  - Audible alarms — vocal warnings such as "Caution, a virus has been detected!"
  - Boot-time scan — through the program interface, a user can schedule a boot-time scan to remove viruses that load during Windows startup and are therefore difficult to remove.

Avast! Antivirus normally updates itself freely for the first 14 months of usage as long as the using computer is connected to the Internet. After each 14 month period, the user of the software must re-register to receive a new license key. Unless upgraded to the pay version, registration currently remains free.

http://www.avast.com/eng/download-avast-home.html

AVG free edition

According to Grisoft, over 60 million users have AVG Anti-Virus protection, including users of the Free Edition. The AVG Anti-Virus Free Edition is similar to the AVG Anti-Virus Professional Edition product, but does not have all the features. It lacks the fine-grained control over how scans are conducted. In addition, the free versions do not receive technical support from Grisoft, and English is the only available language. Grisoft announced that support for AVG Anti-Virus Free Edition version 7.1 ended on February 18, 2007. Users were required to upgrade to AVG Anti-Virus Free Edition version 7.5.

http://free.grisoft.com/doc/5390/us/frt/0

Avira Antivirus Personal Edition Classic

AntiVir Personal Edition Classic (Windows, Linux) is freeware. This application is for personal usage only. Like most antivirus software, it scans disk for viruses and also runs as a background process, checking each opened and closed file. It can detect and possibly remove root kits. It also performs Internet updates (daily by default) in which it opens a window, with an advertisement suggesting the user to purchase AntiVir Personal Edition Premium.

AntiVir Personal Edition Premium costs €20 yearly. It has several improvements over the free version, most notable:

- Detection of adware and spyware
- Exclusive download server
- E-Mail scanning

http://www.free-av.com/antivirus/allinonen.html

Bit defender 10 free edition

Bit Defender is an antivirus software suite developed by Bucharest-based software company SOFTWIN. It was launched in November 2001, and currently tenth version of it is available. Bit Defender placed SOFT Win's earlier AVX (Antivirus express) product range. The Bit Defender range includes antivirus products for home users, business, enterprise users and Internet service providers.

http://www.bitdefender.com/PRODUCT-14-en--BitDefender-Free-Edition.html

Mcafee Virus Scan Plus

- Virus protection guards your whole PC
- Spyware Protection blocks potentially unwanted programs
- Firewall helps keep hackers out

http://home.mcafee.com/store/package.aspx?pkgid=276&ctst=1

Comodo Antivirus

Comodo Antivirus 2.0 beta has been specifically engineered to deliver the highest protection against all known viruses, Trojans and Worms. Easy to install, configure and use Comodo antivirus boasts an industry leading feature list that's packed with the latest and most sophisticated technologies.

http://antivirus.comodo.com/download.html

Clamav (Open source)

Clam Antivirus (ClamAV), is a free open source antivirus software toolkit for Windows and Unix-like operating systems. One of its main uses is with mail exchange servers as a server-side e-Mail virus scanner. ClamAV is distributed under the terms of the GNU, General Public License (GPL). Both ClamAV and its updates are made available free of charge. http://www.clamwin.com/content/view/18/46/

Win pooch (Open source)

Win pooch is a free and open source program that detects and blocks spyware from computers running Microsoft Windows. It also detects Trojans and can associate with the Clam Win and Bit Defender antivirus software to provide real-time protection. As of version 0.6.0, kernel-mode hooking has been implemented through a kernel-mode driver, allowing Win pooch to monitor

the Windows kernel and system services. It was, however, notorious for causing Blue Screens of Death.
http://www.clamwin.com/content/view/18/46/

Malicious Software Removal Tool
The Microsoft Malicious Software Removal Tool is an anti-malware utility that checks computers running Windows 8, Windows 7, Windows Vista, Windows XP*, Windows Server 2012, Windows Server 2008, and Windows Server 2003 for infections by specific, prevalent malicious software—including Blaster, Sasser, and Mydoom—and helps remove malware and any other infections found. When the detection and malware removal process is complete, the tool displays a report describing the outcome, including which, if any, malware was detected and removed.
http://www.microsoft.com/security/pc-security/malware-removal.aspx

Microsoft Security Essentials
Microsoft Security Essentials (MSE) is antivirus software (AV) product that provides protection against different types of malware such as computer viruses, spyware, rootkits and Trojan horses. It runs on Windows XP, Windows Vista and Windows 7, but not on Windows 8, which has a built-in AV component. The license agreement allows home users and small businesses to install and use the product free of charge.
http://windows.microsoft.com/en-us/windows/security-essentials-download

Windows Defender
Windows Defender, formerly known as Microsoft AntiSpyWare, is a software product that helps combat malware. Windows Defender was initially an antispyware program; it is included with Windows Vista and Windows 7 and is available as a free download for Windows XP and Windows Server 2003. In Windows 8, however, it is upgraded to an antivirus program. It included a number of real-time security agents that monitored several common areas of Windows for changes which may be caused by spyware. It also included the ability to easily remove installed ActiveX software.
http://en.wikipedia.org/wiki/Windows_Defender

Microsoft Active Protection Service
Microsoft Active Protection Service (abbreviated MAPS and formerly known as Microsoft SpyNet) is the network of Windows Defender and Microsoft Security Essentials users that help determine which programs are classified as spyware. The signatures created for any submitted programs by the users of the product are available to all users, displayed as a bar graph that shows the percentage of people who have allowed, blocked, or removed an item. This method of spyware classification allows rare, unknown, or new spyware to be categorized as most people choose to send their data.
http://en.wikipedia.org/wiki/Microsoft_Active_Protection_Service

RUBotted
RUBotted monitors your computer for potential infection and suspicious activities associated with bots. Bots are malicious files that enable cybercriminals to secretly take control of your computer. Upon discovering a potential infection, RUBotted will identify and clean it with

HouseCall. Protect your system by continuously monitoring your computer for potential infection and suspicious activities with RUBotted.
http://free.antivirus.com/us/rubotted/

Microsoft Safety Scanner
Microsoft Safety Scanner is a free disposable virus scanner similar to Windows Malicious Software Removal Tool that can be used to scan a system for computer viruses and other forms of malware. Microsoft Safety Scanner is not meant to be used as a day-to-day tool, since it does not provide real-time protection against viruses cannot update its virus definitions and expires after ten days. On the other hand, it can be run on a computer which already has an antivirus product without any potential interference. Therefore, it can be used to scan a computer where there is a potential infection and the user wants a second check from another antivirus.
http://en.wikipedia.org/wiki/Microsoft_Safety_Scanner

Windows Live OneCare
Windows Live OneCare currently features an integrated anti-virus, firewall, backup and restores utility and a tune-up utility with the integrated functionality of Windows Defender for malware protection. The future addition of a registry cleaner was considered but not added because "there are not significant customer advantages to this functionality". Version 2 has features such as multi-PC and home network management, printer sharing support, start-time optimizer, proactive fixes and recommendations, monthly reports, centralized backup, and online photo backup.
Windows Live OneCare is built for ease-of-use and is designed for home users. OneCare also attempts a very minimal interface to lessen user confusion and resource use. It adds an icon to the notification area that tells the user at a glance the status of the system's health by using three alert colors: green (good), yellow (fair), and red (at risk).
http://en.wikipedia.org/wiki/Windows_Live_OneCare_Safety_Scanner

RootkitBuster
Trend Micro RootkitBuster is a free tool that scans hidden files, registry entries, processes, drivers, and the master boot record (MBR) to identify and remove rootkits. The latest version of Trend Micro RootkitBuster features an even more sensitive detection system. Trend Micro RootkitBuster can find rootkits by checking the following:

- Master Boot Record (MBR)
- Files
- Registry entries
- Kernel code patches
- Operating system service hooks
- File streams
- Drivers
- Ports
- Processes
- Services

By cleaning or removing hidden files, registry entries, and services, Trend Micro RootkitBuster can eliminate a wide and ever-growing number of rootkit variants.
http://free.antivirus.com/us/rootkit-buster/index.html

Browser Guard
Proactively protect your browser against new web threats. Browser Guard 2011 has zero-day vulnerability prevention and protects against malicious JavaScript using advanced heuristics and emulation technologies. Browser Guard is quickly and continuously updated to deliver the most secure and up-to-date technology. The latest version includes detection enhancement for Web Trojans, and for tracing infection chains.
http://free.antivirus.com/us/browser-guard/

Browser JS Gaurd
In the recent times, most of the systems connected to Internet are getting infected with malware and some of these systems are even becoming zombies for the attacker. When user knowingly or unknowingly visits a malware website, his system gets infected. Attackers do this by exploiting vulnerabilities in web browser and acquire control over the underlying Operating System. Once attacker compromises the user's web browser, he can instruct the browser to visit the attacker's website by using number of redirections. During the process, user's web browser downloads the malware without the intervention of the user. Once the malware is downloaded, it would be placed in the file system and responds as per the instructions of the attacker. These types of attacks mostly happen through JavaScript and malicious HTML tags. JSGuard detects and defends from such attacks made through the web browser. It blocks access to the harmful, inappropriate and dangerous websites that may contain malicious content.
https://addons.mozilla.org/en-US/firefoxladdon/browser-jsguard/
https://chrome.google.com/webstore/detail/browserjsguard/ncpkigeklafkopcelcegambndlhkcbhb

Malwarebytes Anti-Malware Free
Malwarebytes Anti-Malware Free is an excellent complement to any antivirus program. The software has a laser-like focus on eliminating tricky zero-day malware from your PC. We especially like the Chameleon feature, which disguises the software so malicious programs can't find it. We recommend Malwarebytes Anti Malware Free for every PC user.
http://www.tomsguide.com/us/malwarebytes-free,review-2204.html

Panda Internet Security 2015
Panda Internet Security 2015 is designed to ensure you can enjoy your online life with complete peace of mind. It provides maximum antivirus and online fraud protection for your PC, the firewall and Wi-Fi protection. Control and safeguard access to your data, documents or any sensitive information. Our internet security gives you a peace of mind. Panda Internet Security 2015 protects your family from inappropriate content (pornography, drugs, weapons, etc.). Parental control gives your kids the freedom to use the Internet, at the same time flagging any behavior you feel is inappropriate.
http://www.pandasecurity.com/india/homeusers/solutions/internet-security/

Kaspersky Virus Removal Tool
Kaspersky Virus Removal Tool is a standalone virus scanner, designed to remove all types of infections from your computer. It implies the same effective algorithms of detection used by Kaspersky products but it does not offer any real-time protection. Kaspersky Virus Removal Tool can be useful if you need to clean an infected machine but don't want to install a full-featured anti-virus solution.

ClamWin Portable

ClamWin Portable is very much like its big brother: It's free, open source, and does a great job of disinfecting machines. ClamWin has a very high detection rate, has frequently updated definitions, and has an easy to use graphical interface. The only caveat to using ClamWin is that it does not offer a real-time scanner - which is not an issue for a portable version. This is my go-to portable virus scanning software.

http://www.techrepublic.com/blog/five-apps/five-portable-antivirus-and-antimalware-tools-to-carry-with-you-at-all-times/

Sophos Anti Rootkit Portable

Sophos Anti Rootkit Portable is one of those tools you hope you never have to use; but you know, at some point, you will. Sophos is remarkably adept at locating root kits - especially for a portable app. Sophos: scans, detects and removes rootkits, is 100% free, supports Windows XP, Vista and 7, and works alongside your existing antivirus. I have found Sophos reliable enough to use even while the PC being scanned is in use.

http://www.techrepublic.com/blog/five-apps/five-portable-antivirus-and-antimalware-tools-to-carry-with-you-at-all-times/

Emsisoft Free Emergency Toolkit

Emsisoft Free Emergency Toolkit is a powerful malware removal tool that can scan for, and remove, over six million dangers to your PC. Emsisoft Free Emergency Toolkit has both a GUI and a command line version, so you can scan your machine even if there are problems with the GUI. With this toolkit, you not only get the malware scanner, you also get HiJackFree and BlitzBlank as well. Emsisoft offers the free download, or you can purchase a pre-compiled USB stick.

http://www.techrepublic.com/blog/five-apps/five-portable-antivirus-and-antimalware-tools-to-carry-with-you-at-all-times/

Vipre Rescue

Vipre Rescue is that tool you use when your machine is severely infected. Vipre is run in safe mode and does not depend upon a GUI tool for use. You double-click the executable and a command window opens with the scanner running (and running at blazing speeds). If you already use the full version of Vipre, you can still run this tool should your machine become so infected, Vipre will not run.

http://www.techrepublic.com/blog/five-apps/five-portable-antivirus-and-antimalware-tools-to-carry-with-you-at-all-times/

Spybot Search and Destroy Portable

Spybot Search and Destroy Portable is the portable version of the massively popular full Spybot Search and Destroy. This antimalware tool does a great job of finding and removing malicious software - all from your flash drive. Spybot has a unique feature that will help you backup your registry before you begin the scan. Should Spybot fubar your PCs registry, you have a backup to restore to - safe and sound.

http://www.techrepublic.com/blog/five-apps/five-portable-antivirus-and-antimalware-tools-to-carry-with-you-at-all-times/

Ad-Aware Free Antivirus+
Lavasoft's Ad-Aware is one of the most trusted spyware tools and has been a benchmark in the industry for years given it's incredibly smooth installation, non-intrusive notifications, and fantastic results. The free version of the software provides real-time anti-virus and malware protection in addition to the latest in sandbox emulation technology, thus providing overarching protection whether you're browsing the Web, downloading files, or merely checking your email.
http://www.digitaltrends.com/computing/best-free-antivirus-software/

PhrozenSoft VirusTotal Uploader
PhrozenSoft VirusTotal Uploader enables you to upload any file to the free VirusTotal service, where it will be scanned with more than 40 leading anti-virus products. The program adds an upload option to the Windows right-click menu and you can also drag'n drop files onto a desktop widget or the application interface. Once your files have been uploaded and scanned you will be notified and can review the scan results from the integrated report viewer. The program also includes a task manager that shows running processes, active connections, services and startup program and lets you quickly submit any suspicious items to VirusTotal for scanning. Other features include detailed logging uploads and results, customizable notification options and support for personal VirusTotal APIs.
http://www.spychecker.com/program/vtu.html

McAfee Stinger
McAfee Stinger is a portable anti-virus scanner to detect and remove specific viruses. It is not a substitute for full featured anti-virus protection, but rather a tool to assist administrators and users when dealing with an infected system. The program utilizes McAfee scan engine technology, including process scanning, digitally signed DAT files, and scan performance optimizations. Stinger detects more than 3000 viruses, Trojans and variants as well as malware that masquerade as a legitimate security application (Fake Alerts).
http://www.spychecker.com/program/stinger.html

Immunet
It delivers real-time protection to your PC. Stay protected against over 13 million viruses and thousands of new threats daily without ever downloading another virus detection file again. Immunet's low disk and memory use won't weigh down your PC unlike other solutions. It is a community-Based Protection allows you to give protection to your friends for FREE. Immunet Free is the first antivirus application created to protect your community and social network. Easily add people to the Immunet Community and view their protection status online.
Real-time Detection from the Immunet Cloud against viruses, spyware, bots, worms, Trojans, and keyloggers without downloading any virus signature files. Stay protected with Collective Immunity™ and intelligent virus detection technology that doesn't slow down your PC.
http://www.immunet.com/free/features/index.html

TDSSKiller
TDSSKiller is a standalone utility, specialized to find and remove Rootkits of the Rootkit.Win32.TDSS family, including SST, Pihar, ZeroAccess, Sinowal, Phanta, Stoned, RLoader,Cmoser and Cidox. Simply run the application, press the scan button and wait for the results.
http://www.spychecker.com/program/tdsskiller.html

Internet Security
360 Internet Security is a full-featured antivirus program that is powered by three scanning engines - 360 Heuristic Engine, 360 Cloud Engine and Bit-Defender. The program offers real-time protection, secure browsing, download protection, privacy protection, webcam protection, USB protection, as well as a secure Sandbox that enables you to isolate processes from your PC environment. Other features include automatic updated, scheduled and on-demand scanning, proactive defense, network protection, privacy cleaning (cache, cookies, history etc.) and self-protection to prevent malware from tampering with your anti-virus protection.
http://www.spychecker.com/program/360is.html

MCShield
MCShield is an anti-malware program, designed to prevent malware and virus infections from portable USB drives. It automatically scans each removable drive that is inserted and checks if it contains any potential threats. The program makes primarily use of a heuristic detection engine but also includes a signature database of known-bad items, which can be updated periodically with the built-in updater.
http://www.spychecker.com/program/mcshield.html

Roboscan Internet Security Free
Roboscan is an Internet Security suite that includes real-time antivirus scanning, malware protection and a personal firewall, as well as several other tools that can help you spot common system vulnerabilities and shred sensitive files. The antivirus protection uses VB100 certified dual engines (ESTsoft's Tera Engine and Bitdefender) and offers real-time protection, scheduled scans and automatic updates.
http://www.spychecker.com/program/roboscan.html

PC Tools AntiVirus Free Edition
PC Tools AntiVirus Free Edition is an anti-virus scanner that offers basic protection against viruses, worms and Trojans. It includes real-time scan of files as well as incoming and outgoing email messages and an optional browser toolbar (Browser Defender) that protects you from malicious websites. The free version has various advanced features disabled.
http://www.spychecker.com/program/pctoolsav.html

VirusTotal Uploader
VirusTotal Uploader enables you to upload a file to the popular VirusTotal service and scan it with 40 leading Anti-Virus products including Norton, McAfee, Avast, AVG and many others. You can then review a report that includes the scan results from each product. The VirusTotal Uploader integrates with the Windows Explorer Send To menu, allowing you to quickly upload files that you have already downloaded, or you can submit the download URL of a file and pass it on to the service without storing the file on your computer.
http://www.spychecker.com/program/virustotal.html

Sophos Anti-Rootkit
Sophos Anti-Rootkit finds and removes any rootkit that is hidden on your computer. It scans all running processes, as well as the registry and local hard drives for known rootkits, and automatically selects the files for removal without compromising system integrity. Also includes

command-line functionality.
http://www.spychecker.com/program/sophosantiroot.html

Sophos Conficker Removal Tool
Sophos Conficker Removal Tool is a free solution for eliminating Conficker infections enables the detection, isolation, and removal of the Conficker virus on your network.
http://www.spychecker.com/program/sophosconfrem.html

F-Secure BlackLight
F-Secure BlackLight scans your system for so-called rootkits that are hidden from the user and standard security software. If the scan finds any suspicious objects, you will have the option to remove them.
http://www.spychecker.com/program/fsblacklight.html

Amiti Antivirus
Amiti Antivirus is a free antivirus program that includes heuristic scanning and supports 4 different scan types, including one that can check for viruses that are currently running in memory. Amiti Antivirus can be used with Windows 8, 7, Vista, and XP.
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.htm

Baidu Antivirus 2015
Baidu Antivirus 2015 is lightweight and fights malware via its cloud-based virus database. Baidu Antivirus 2015 works in Windows 8, Windows 7, Windows Vista, and Windows XP. Install Baidu Antivirus 2015 alongside other antivirus software for increased protection. It automatically updates, scans USB devices and the Windows registry, has a built-in cloud file scanner to upload suspicious files to Baidu to be scanned, and includes several other useful tools like a traffic monitor and private browser tool.
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.htm

Comodo Antivirus
Comodo Antivirus from Comodo Security Solutions is another excellent program, easily one of the best free antivirus options out there. Comodo Antivirus protects you from several threat sources, just as most of the other free antivirus programs on this list do. Comodo Antivirus works on Windows 8, Windows 7 and Windows Vista.
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.htm

FortiClient
FortiClient is an antivirus, web filtering, firewall, parental control, optimization, (and then some) program that's powerful enough for a business to use. It's more accurately referred to as a "threat management" tool. FortiClient works on Windows 8, Windows 7, Windows Vista, and Windows XP.
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.htm

Kingsoft Antivirus 2012
Kingsoft Antivirus 2012 is a cloud-based antivirus program like Panda Cloud Antivirus and Immunet FREE Antivirus. Kingsoft Antivirus keeps an eye out for malware locally, when

downloading files, while chatting on IM, and more. Kingsoft Antivirus 2012 works on Windows 8, Windows 7, Windows Vista and Windows XP.
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.01.htm

Outpost Security Suite Free
Outpost Security Suite Free is a free antivirus program that supports web and email scanning as well as a firewall. The built-in firewall can control applications and network packets through a filter as well as local network policies. Also included in Outpost Security Suite Free is the ability to protect crucial system settings from being tampered with.
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.01.htm

Rising AntiVirus Free Edition
Rising Antivirus Free Edition is the free antivirus offering from China's largest antivirus maker, Rising Software. Rising Antivirus Free Edition works with Windows 7, Windows Vista, and Windows XP.
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.01.htm

UnThreat Free AntiVirus 2014
UnThreat Free AntiVirus 2014 offers standard malware protection, including threats via email. I found nothing too impressive about this program aside from its price... or lack thereof, I suppose. UnThreat Free AntiVirus 2014 works in Windows 8, Windows 7, Windows Vista, and Windows XP.
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.01.htm

Zillya! Antivirus
Zillya! Antivirus is another free antivirus program that works with Windows. It's nearly the same as most of the other programs from this list. It actively scans emails and USB devices, and you can choose a quick, full, or custom virus scan. There's an exclusions category so you can remove certain folders and/or files from being scanned.
Zillya! Antivirus has a few extra features like a built-in task manager and startup manager to disable startup items. Definition updates must be installed manually, and are usually very large in size, which is a big hassle when you compare this to other antivirus programs.
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.01.htm

ZoneAlarm Free Antivirus + Firewall 2015
Zone Alarm Free Antivirus + Firewall 2015 are just that - a combination free antivirus and firewall tool. Check Point Software, the makers of Zone Alarm Free Antivirus + Firewall 2015, has been in the firewall business for a long time. They make good software and this program is no exception. While I didn't notice anything spectacular about the antivirus portion of this program, having an antivirus and firewall tightly integrated has its benefits.
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.01.htm

EScan Antivirus
With new Advanced Virus Control technology and highly sophisticated Heuristics Algorithms, eScan effectively provides real time protection against malware that are continuously released by malware writers. It also detects and warns users about applications that behave in a

suspicious manner, thus providing protection from Zero-Day threats. The Two-Way Firewall feature of eScan filters as well as monitors all incoming and outgoing network traffic on the computer and protects it from all types of network-based attacks. EScan efficiently monitors and provides protection on real-time basis against viruses and other cyber threats with its advanced and innovative technologies. User can boot into a secure environment during system startup without using any optical media with the eScan Rescue Mode feature.
http://www.escanav.com/english/content/products/escan_soho/escan_universal_security_suite.asp

Symantec Endpoint Protection
Symantec Endpoint Protection, developed by Symantec Corporation, is an antivirus and personal firewall product leveled at centrally managed corporate environments security for servers and workstations.
http://en.wikipedia.org/wiki/Symantec_Endpoint_Protection

Linux BasedTools

Avast Home Edition
Avast! Linux Home Edition represents an antivirus solution for the increasingly popular Linux platform. This software is designed exclusively for home users and non-commercial use.

AVG Free Edition
AVG 7.5 Free for Linux provides comprehensive and reliable protection against viruses for Linux powered machines. It offers many features, such as scheduled and on-demand scanning of folders, files, and common archive types for possible virus infection. You can also perform a scheduled or on demand update of your AVG either from the Internet or from local updates Sources.

Clamtk
ClamTk is a GUI front-end for Clam Antivirus using gtk2-perl. It is designed to be an easy-to-use, lightweight, point-and-click desktop virus scanner for Linux.
http://sourceforge.net/projects/clamtk/

BitDefender
Bitdefender Antivirus Scanner for Unices has both a graphical user interface to access the scanner directly from the application menu lists, and a command line interface for more advanced users. Script and extension-based integration helps configuring your favorites file manager, email or news client to easily use Bitdefender Antivirus Scanner for Unices.
To minimize risk of further infection and to allow safe analysis, Bitdefender Antivirus Scanner for Unices can quarantine infected files into a protected directory. In addition to infected files, suspect files may also be moved to the quarantine area as they are identified by heuristic analysis as having known characteristics of malicious code but do not match a known virus signature.
http://www.bitdefender.com/business/antivirus-for-unices.html

Comodo Antivirus
Comodo Antivirus has been specifically engineered to deliver the highest protection against

all known viruses, Trojans and Worms. Easy to install, configure and use Comodo antivirus boasts an industry leading feature list that's packed with the latest and most sophisticated technologies.

https://www.comodo.com/home/download/download.php?prod=antivirus-for-linux

Bitdefender Antivirus Scanner

Bitdefender Antivirus Scanner for Unices has both a graphical user interface to access the scanner directly from the application menu lists, and a command line interface for more advanced users. Script and extension-based integration helps configuring your favorites file manager, email or news client to easily use Bitdefender Antivirus Scanner for Unices. To minimize risk of further infection and to allow safe analysis, Bitdefender Antivirus Scanner for Unices can quarantine infected files into a protected directory. In addition to infected files, suspect files may also be moved to the quarantine area as they are identified by heuristic analysis as having known characteristics of malicious code but do not match a known virus signature.

http://www.bitdefender.com/business/antivirus-for-unices.html

Panda Antivirus

Panda Antivirus for Linux is an antivirus for Linux servers and desktops. It is an antivirus designed to be managed from the command line or console. To do this, an executable called PAVCL will be used. The aim of Panda Antivirus is to scan and disinfect Windows and DOS workstations connected to a Linux server, as well as the Linux server itself. Panda Antivirus scans files using both string searches and heuristic methods. The target files are Word documents, Java Applets, ActiveX controls and compressed files (ZIP, RAR, etc.). At this time, it does not scan the boot sector or the partitions table.

http://pandacloudcleaner.pandasecurity.com/facebook/

F-PROT Antivirus

F-PROT for Linux Workstations features: Scans for over 2119958 known viruses and their variants. Ability to perform scheduled scans when used with the cron utility. Scans hard drives, CD-ROMS, diskettes, network drives, directories and specific files. Scans for images of boot sector viruses, macro viruses and Trojan Horses.

http://www.f-prot.com/products/home_use/linux/

PANDA Antivirus

Panda Internet Security 2015 is designed to ensure you can enjoy your online life with complete peace of mind. It provides maximum antivirus and online fraud protection for your PC, the firewall and Wi-Fi protection. Control and safeguard access to your data, documents or any sensitive information. Our internet security gives you a peace of mind. Panda Internet Security 2015 protects your family from inappropriate content (pornography, drugs, weapons, etc.). Parental control gives your kids the freedom to use the Internet, at the same time flagging any behavior you feel is inappropriate.

http://www.pandasecurity.com/india/homeusers/solutions/internet-security/

EScan Antivirus

EScan works as an on-demand software application that can be invoked as per your requirements.

It consists of Command Line and Graphical User Interface (GUI) Scanner. It facilitates selected Directory Scan, Local hard disk and Home Directory scanning as well as Memory Scan to ensure complete protection from cyber threats. eScan scans the data stream of a file to detect hidden malware, which consists of all types of files including zipped and archived file. Scheduled Scanning option along with Command line scanner helps to schedule automatic scans on your system at a preset time. eScan generates a comprehensive log of scanning activity with date and time of scanning, along with the path and name of objects scanned for further analysis.
http://www.escanav.com/english/content/products/escan_soho/escan_universal_security_suite.asp

F-Secure BlackLight
F-Secure BlackLight scans your system for so-called rootkits that are hidden from the user and standard security software. If the scan finds any suspicious objects, you will have the option to remove them.
http://www.spychecker.com/program/fsblacklight.html

Kaspersky Antivirus
Kaspersky Anti-Virus features include real-time protection, detection and removal of viruses, Trojan's, worms, spyware, adware, keyloggers malicious tools and auto-dialers, as well as detection and removal of rootkits. It also includes instantaneous automatic updates via the "Kaspersky Security Network" service.
http://en.wikipedia.org/wiki/Kaspersky_Anti-Virus

Mcafee Virus Scan Plus
- Virus protection guards your whole PC
- Spyware Protection blocks potentially unwanted programs
- Firewall helps keep hackers out

http://home.mcafee.com/store/package.aspx?pkgid=276&ctst=1

Symantec Endpoint Protection
Symantec Endpoint Protection, developed by Symantec Corporation, is an antivirus and personal firewall product leveled at centrally managed corporate environments security for servers and workstations.
http://en.wikipedia.org/wiki/Symantec_Endpoint_Protection

Always Use Updated Anti Virus

Use Latest Anti Spyware

Use Desktop Firewall Software

Information Security Awareness for Children

Information Security Awareness for Students

Information Security Awareness for Parents

Tips on Information Security

- Don't open e-mails received from unknown source
- Be safe by not giving personal info
- Update Software patches and Anti-Virus
- Backup critical data
- Change Passwords regularly
- Always use secured web sites (https://)
- Never tell your password to anyone!
- Don't follow links in spam messages or emails

For more details logon to: **www.infosecawareness.in**

Security Assessment Tools

Microsoft security assessment tool (Windows)
The Microsoft Security Assessment Tool (MSAT) is a risk-assessment application designed to provide information and recommendations about best practices for security within an information technology (IT) infrastructure.
http://www.microsoft.com/downloads/details.aspx?FamilyID=6d79df9c-c6d1-4e8f-8000-0be72b430212&displaylang=en

Nessus ($, Linux, Windows)
The Nessus vulnerability scanner is the world-leader in active scanners, featuring high speed discovery, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis of your security posture. Nessus scanners can be distributed throughout an entire enterprise, inside DMZs, and across physically separate networks.
http://www.nessus.org/download/

Retina (Windows)
Retina Network Security Scanner, the industry and government standard for multiplatform vulnerability management, identifies known and zero day vulnerabilities plus provides security risk assessment, enabling security best practices, policy enforcement, and regulatory audits.
http://www.eeye.com/html/products/retina/download/index.html

IBM Internet scanner

Internet Scanner can identify more than 1,300 types of networked devices on your network, including desktops, servers, routers/switches, firewalls, security devices and application routers. Once all of your networked devices are identified, Internet Scanner analyzes the configurations, patch levels, operating systems and installed applications to find vulnerabilities that could be exploited by hackers trying to gain unauthorized access.

https://www.iss.net/issEn/MYISS/login.jhtml?action=download

Patch link vulnerability assessment tool

Reduce corporate risk through the timely, proactive elimination of operating system and application vulnerabilities.

- Decrease IT costs and improve productivity with a highly automated, subscription-based patch management solution.
- Eliminate recurring risks through 'patch drift'
- Demonstrate compliance with security policies and government regulations through continuous patch monitoring and comprehensive reporting.

http://www.lumension.com/patch-management.jsp

Qualys guard (Linux & Windows)

Free Scan allows you to quickly and accurately scan your server for thousands of vulnerabilities that could be exploited by an attacker. If vulnerabilities exist on the IP address provided, Free Scan will find them and provide detailed information on each risk - including its severity, associated threat, and potential impact. It even provides links to give you more information about the vulnerability and how to correct it.

http://www.qualys.com/forms/trials/freescan/matrix/?lsid=6960

GFI LAN guard (Windows)

GFI LAN guard Network Security Scanner (N.S.S.) is an award-winning solution that allows you to scan, detect, assess and rectify any security vulnerabilities on your network. As an administrator, you often have to deal separately with problems related to vulnerability issues, patch management and network auditing, at times using multiple products. However, with GFI LAN guard N.S.S., these three pillars of vulnerability management are addressed in one package. Using a single console with extensive reporting functionality, GFI LAN guard N.S.S.'s integrated solution helps you address these issues faster and more effectively.

http://www.gfi.com/downloads/downloads.aspx?pid=lanss&lid=EN

Core Impact (Windows)

Core Impact is commercial penetration testing application developed by Core Security

Technologies which allows the user to probe for and exploit security vulnerabilities in a computer network. The interface is designed to be usable by individuals without specialized training in computer security, and includes functions for generating reports from the gathered information. It is used by over 600 companies and government entities.

http://www.coresecurity.com/?module=ContentMod&action=item&id=535

ISS Internet scanner (Windows)

Minimum purchase quantity, 10 IP's. ISS Internet Scanner is installed on one computer on the network, and scans computers and routers for security vulnerabilities in the operating system, key applications and configuration, using ISS's database of known vulnerabilities. The perpetual license requires annual support and maintenance. This version includes Site Protector Management for licenses up to 500 IP's.

https://www.securehq.com/group.wml&storeid=1&deptid=75&groupid=928&ds=wpshop_store&SessionID=20091285321932563

Nikto (Linux)

A more comprehensive web scanner Nikto is an open source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 3200 potentially dangerous files/CGIs, versions on over 625 servers, and version specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated (if desired). It uses Whisker/libwhisker for much of its underlying functionality. It is a great tool, but the value is limited by its infrequent updates. The newest and most critical vulnerabilities are often not detected.

http://linux.softpedia.com/get/System/Networking/Nikto-10271.shtml

X-scan (Windows)

X-Scan is a basic network vulnerability scanner utilizing a multi-threading scan approach. The scanner can be utilized both at the command line and has an easy to use GUI front-end. The following items can be scanned:

- Remote OS type and version detection,
- Standard port status and banner information,
- SNMP information,
- CGI vulnerability detection,
- IIS vulnerability detection,
- RPC vulnerability detection,
- SSL vulnerability detection,
- SQL-server,
- FTP-server,
- SMTP-server,
- POP3-server,

- NT-server weak user/password pairs authentication module,
- NT server NETBIOS information,
- Remote Register information, etc.

http://www.xfocus.org/programs/200507/18.html
http://www.vulnerabilityassessment.co.uk/xscan.htm

Sara (Linux, Windows, Open source)

In its simplest (and default) mode, it gathers as much information about remote hosts and networks as possible by examining such network services as finger, NFS, NIS, ftp and tftp, rexd, and other services. The information gathered includes the presence of various network information services as well as potential security flaws -- usually in the form of incorrectly setup or configured network services, well-known bugs in system or network utilities, or poor or ignorant policy decisions. It can then either report on this data or use a simple rule-based system to investigate any potential security problems. Users can then examine, query, and analyze the output with an HTML browser, such as Mosaic or Netscape. While the program is primarily geared towards analyzing the security implications of the results, a great deal of general network information can be gained when using the tool - network topology, network services running, types of hardware and software being used on the network, etc.

http://www-arc.com/sara/

SAINT ((Linux & Open source)

SAINT, or the Security Administrator's Integrated Network Tool, uncovers areas of weakness and recommends fixes. With SAINT® vulnerability assessment tool, you can:

- Detect and fix possible weaknesses in your network's security before they can be exploited by intruders.
- Anticipate and prevent common system vulnerabilities.
- Demonstrate compliance with current government regulations such as FISMA,SOX, GLBA, HIPAA, and COPPA and with industry regulations such as PCIDSS.
- The SAINT® scanning engine is the ideal cornerstone for your vulnerability assessmentprogram. SAINT features a graphical user interface that is intuitive and easy to use.

http://download.saintcorporation.com/downloads/freetrial/saint-install-6.7.2.gz

MBSA (Windows)

Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool designed for the IT professional that helps small and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. Built on the Windows Update Agent and Microsoft Update infrastructure, MBSA ensures consistency with other Microsoft management products

including Microsoft Update (MU), Windows Server Update Services (WSUS), Systems Management Server (SMS) and Microsoft Operations Manager (MOM). Apparently MBSA on average scans over 3 million computers each week.

Paros Proxy (Linux, Windows, Open source)

We wrote a program called "Paros" for people who need to evaluate the security of their web applications. It is free of charge and completely written in Java. Through Paros's proxy nature, all HTTP and HTTPS data between server and client, including cookies and form fields, can be intercepted and modified.

http://www.parosproxy.org/download.shtml

Web Scarab (Linux, Windows, Open source)

Web Scarab is a framework for analyzing applications that communicate using the HTTP and HTTPS protocols. It is written in Java, and is thus portable to many platforms. WebScarab has several modes of operation, implemented by a number of plug-ins.

In its most common usage, Web Scarab operates as an intercepting proxy, allowing the operator to review and modify requests created by the browser before they are sent to the server, and to review and modify responses returned from the server before they are received by the browser.

http://www.net-security.org/software.php?id=504

Web Inspect (Windows)

Web Inspect application security assessment tool ensures your organization's web security and the security of your most critical information by identifying known and unknown vulnerabilities within the Web application layer. Web Inspect also helps you ensure Web server security by including checks that validate that the Web server is configured properly. With Web Inspect, auditors, compliance officers, and security experts can perform security assessments on Web applications and Web services.

https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-201-200%5e9570_4000_100__

Whisker/Libwhisker (Linux, Windows, Open source)

Libwhisker is a Perl module geared towards HTTP testing. It provides functions for testing HTTP servers for many known security holes, particularly the presence of dangerous CGIs. Whisker is a scanner that used libwhisker but is now deprecated in favour of Nikto which also uses libwhisker.

http://www.wiretrip.net/rfp/

Burp suite (Linux, Windows, Open source)

Burp Suite is an integrated platform for attacking web applications. It contains the

entire Burp tools with numerous interfaces between them designed to facilitate and speed up the process of attacking an application. All tools share the same robust framework for handling HTTP requests, authentication, downstream proxies, logging, alerting and extensibility.

Burp Suite allows you to combine manual and automated techniques to enumerate, analyze, attack and exploit web applications. The various Burp tools work together effectively to share information and allow findings identified within one tool to form the basis of an attack using another.

http://portswigger.net/suite/download.html

Wikto (Windows, Open source)

Wikto is a tool that checks for flaws in web servers. It provides much the same functionality as Nikto but adds various interesting pieces of functionality, such as a Back-End miner and close Google integration. Wikto is written for the MS .NET environment and registration is required to download the binary and/or source code.

http://www.sensepost.com/research/wikto/

Acunetix Web Vulnerability Scanner (Windows)

Out of the 100,000 websites scanned by Acunetix WVS, 42% were found to be vulnerable to Cross Site Scripting. XSS is extremely dangerous and the number of the attacks is on the rise. Hackers are manipulating these vulnerabilities to steal organizations' sensitive data. Can you afford to be next? Cross Site Scripting allows an attacker to embed malicious JavaScript, VBScript, ActiveX, HTML, or Flash into a vulnerable dynamic page to fool the user, executing the script on his machine in order to gather data. Exploited Cross Site Scripting is commonly used to achieve the following malicious results:

- Identity theft
- Accessing sensitive or restricted information
- Gaining free access to otherwise paid for content
- Spying on user's web browsing habits
- Altering browser functionality
- Public defamation of an individual or corporation
- Web application defacement
- Denial of Service attacks

http://www.acunetix.com/cross-site-scripting/scanner.htm

Watchfire AppScan (Windows)

Watchfire® AppScan® automates web application security audits to help ensure the security and compliance of websites. Named the worldwide market-share leader according to Gartner and IDC, our AppScan product suite offers a solution for all types of web application security testing needs - outsourced, individual scans and

enterprise-wide analysis - and for all types of users - application developers, quality assurance teams,penetration testers, security auditors and senior management.
https://www.watchfire.com/securearea/appscan.aspx

N-Stealth (Windows)

N-Stealth is a comprehensive web server security-auditing tool that scans for over 30,000 vulnerabilities. It is ideal for system administrators, security consultant and IT professionals.
http://www.nstalker.com/products/free/

Metasploit

Metasploit is a fantastic, powerful open source framework that performs rigorous scans against a set of IP addresses.
Unlike many other frameworks, it can also be used for anti-forensics. Expert programmers can write a piece of code exploiting a particular vulnerability, and test it with Metasploit to see if it gets detected. This process can be reversed technically — when a virus attacks using some unknown vulnerability, Metasploit can be used to test the patch for it.
http://www.metasploit.com/

OpenVAS

The Nessus scanner is a famous commercial utility, from which OpenVAS branched out a few years back to remain open source. Though Metasploit and OpenVAS are very similar, there is still a distinct difference.
OpenVAS is split into two major components — a scanner and a manager. A scanner may reside on the target to be scanned and feed vulnerability findings to the manager. The manager collects inputs from multiple scanners and applies its own intelligence to create a report.
In the security world, OpenVAS is believed to be very stable and reliable for detecting the latest security loopholes, and for providing reports and inputs to fix them. A built-in Greenbone security assistant provides a GUI dashboard to list all vulnerabilities and the impacted machines on the network.
Creating detailed reports is one thing that makes OpenVAS a tool favoured by infrastructure security managers.
http://www.openvas.org/

Samurai framework

Once a baseline check is performed by Nikto, the next step is to take the “deep-dive” approach. Samurai is a framework — a bunch of powerful utilities, each one targeted for a specific set of vulnerabilities.
http://samurai.inguardians.com/

Safe3 scanner

While the first two tools are good for static websites, for portals needing user ID and password, we need something that can deal with HTTP sessions and cookies. Safe3 scanner is a fantastic open source project, which has gained momentum and fame because it can handle almost all types of authentication, including NTLM.

It contains a Web crawler (a spider like that of search engines) capable of ignoring duplicate page scans and yet detect client-side JavaScript vulnerabilities. Safe3 scans also detect the possibility of the latest AJAX-based attacks and even report vulnerable script libraries. It comes with a user-friendly GUI and is capable of creating nice management reports.

http://opensourceforu.com

Websecurity

Though very similar to Samurai, Websecurity also brings application-level assessment into play. In case of a large Web farm where code is maintained by a team of developers, following standards can sometimes yield insecure code like passwords mentioned in code, physical file paths in libraries, etc. Websecurity can traverse code and find such loopholes swiftly.

A nice feature is that it allows you to create screenshots of the problem areas automatically, which helps in preparing audit reports. It is one of the very few platform-independent tools and also supports mobile coding, which is helping it get more popular in the cyber-security assessment world.

http://opensourceforu.com

SQLmap

SQLmap is capable of not just exploiting SQL-injection faults, but can also take over the database server. Since it focuses on a specific task, it works at great speed to fingerprint databases, find out the underlying file system and OS, and eventually fetch data from the server. It supports almost all well-known database engines, and can also perform password-guessing attacks. This tool can be combined with the other four tools mentioned above to scan a website aggressively.

A vulnerability assessment tool should include network scanning as well as website vulnerability exploitation. Open source software is prone to attacks too; hence, network administrators must know about the reputed scanners and use them in their daily tasks to make their infrastructure secure and stable.

http://sqlmap.org

IPLocks

IPLocks Armour provides the industry's most robust solution for detecting and repairing database weaknesses. No other vendor can match the combination of

scalability, customizability, and cost-effectiveness of IPLocks. Companies around the world use IPLocks Armour to support critical initiatives such as:

- User Privilege Reporting
- Internal Security
- SOX Compliance
- PCI Compliance
- Risk Management

http://www.iplocks.com/products/iplocks_armour.html

App Detective

A network-based, vulnerability assessment scanner, App Detective Pro discovers database applications within your infrastructure and assesses their security strength. In contrast to piecemeal solutions, App Detective Pro modules allow enterprises to assess two primary application tiers - application / middleware, and back-end databases - through a single interface. Backed by a proven security methodology and extensive knowledge of application-level vulnerabilities, App Detective Pro locates, examines, reports, and fixes security holes and misconfigurations. As a result, enterprises can proactively harden their database applications while at the same time improving and simplifying routine audits.

https://www.appsecinc.com/downloads/appdetectivepro/

Watch fire

Watch fire® App Scan® automates web application security audits to help ensure the security and compliance of websites. Named the worldwide market-share leader according to Gartner and IDC, our App Scan product suite offers a solution for all types of web application security testing needs - outsourced, individual scans and enterprisewide analysis - and for all types of users - application developers, quality assurance teams, penetration testers, security auditors and senior management.

https://www.watchfire.com/securearea/appscan.aspx

N-stalker

N-Stalker Web Application Security Scanner 2006 is a web security assessment solution developed by N-Stalker. By incorporating the well-known N-Stealth HTTP Security Scanner and its 35,000 Web Attack Signature database, along with a patent-pending Component-oriented Web Application Security Assessment technology, N-Stalker is capable of sweeping your Web Application for a large number of vulnerabilities common to this environment, including Cross-site Scripting and SQL injection, Buffer Overflow and Parameter Tampering attacks and much more.

http://www.nstalker.com/products/free/download-free-edition

Sprajax (for AJAX)

Sprajax is an open source black box security scanner used to assess the security of

AJAX-enabled applications. By detecting the specific AJAX frameworks in use, Sprajax is able to better formulate test requests and identify potential vulnerabilities.
http://www.owasp.org/index.php/Category:OWASP_Sprajax_Project

Pixy (for PHP)

Pixy is an Open-Source Vulnerability Scanner that identifies SQL, XSS problems in PHPapplications.
http://pixybox.seclab.tuwien.ac.at/pixy/download.php

Prevx

However, in order to share files on your computer and sometimes in order for you to access files on other computers within a P2P network such as Bit Torrent, you must open a specific TCP port through the firewall for the P2P software to communicate. In effect, once you open the port you are no longer protected from malicious traffic coming through it.It may cause confusion for novice users in much the same way personal firewall software such as Zone Alarm does because simply allowing or banning actions wholesale would result in either allowing a large amount of suspicious activity to go undetected or banning a large amount of benign actions such as the user trying to install their own software, so Prevx asks the user how it should treat the activity.Any time that an application attempts to access system memory or critical files or alter the registry the Prevx Home software detects the activity and either blocks it completely or asks the user how to proceed. According to Prevx the software will detect and prevent buffer overflows and overruns, modification of critical files and directories, unauthorized changes to critical areas of the system registry and more.I removed my antivirus and firewall software for an entire week during my test and still ran into no viruses or other malicious code or spyware. A scan with Ad-Aware found a handful of tracking cookies, but nothing malicious.
http://info.prevx.com/downloadprevx2.asp

Honey trap

Honey trap is a network security tool written to observe attacks against network services. As a low-interactive honey pot, it collects information regarding known or unknown network-based attacks and thus can provide early-warning information.
http://honeytrap.mwcollect.org/download-Download%20Honeytrap

https://www.facebook.com/infosecawarenesss

Connect us with

Facebook

https://www.youtube.com/channel/UCWPBKQryyVvydUy4rYsbBfA

YouTube

Subscribe

https://twitter.com/CDAC_ISEA

Twitter

Follow

Always Use Updated Anti Virus

Use Latest Anti Spyware

Use Desktop Firewall Software

Information Security Awareness for Children

Information Security Awareness for Students

Information Security Awareness for Parents

Tips on Information Security

- Don't open e-mails received from unknown source
- Be safe by not giving personal info
- Update Software patches and Anti-Virus
- Backup critical data
- Change Passwords regularly
- Always use secured web sites (https://)
- Never tell your password to anyone!
- Don't follow links in spam messages or emails

For more details logon to: **www.infosecawareness.in**

Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

About ISEA

Looking at the growing importance for the Information Security, Ministry of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched by the Govt. of India. One of the activities under this programme is to spread Information Security Awareness among children, teachers, home users, IT and non-IT professionals throughout the country. C-DAC Hyderabad has been assigned the responsibility of executing this project by Ministry of Electronics & Information Technology, Government of India. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events etc.,

Disclaimer

The information in this book is for education purpose only.
C-DAC cannot held responsible for any of the inaccuracies. If any such inaccuracies please report to

isea@cdac.in

Toll Free No.
1800 425 6235

www.InfoSecAwareness.in

बेटी बचाओ बेटी पढ़ाओ

Supported by

certin

रा.इ.सू.प्रौ.सं NIELIT

Ministry of Electronics & Information Technology,
Government of India

सी डैक CDAC प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India
Plot No: 6&7, Hardware Park Sy. No.1/1, Srisailam Highway Raviryal (V & GP), Via Ragaanna guda
Maheshwaram (M), Ranga Reddy District, Hyderabad – 501510. Tel: 9248920201.