Information Security Education & Awareness
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था
भारत सरकार

सी डैक
CDAC

सूचना सुरक्षा जागरूकता

हँडबुक

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

हैंडबुक

श्रेय

सीडीएसी के बारे में

सीडैक ने अपने हैदराबाद केंद्र की स्थापना वर्ष १ ९९९ में अनुसंधान, विकास और प्रशिक्षण गतिविधियों में काम करने के लिए की, जो नवीनतम हार्डवेयर और सॉफ्टवेयर टेक्नोलॉजीज को गले लगाते हैं। केन्द्र ज्ञान निर्माण, ज्ञान प्रसार और ज्ञान अनुप्रयोग के घटकों के साथ एक अनुसन्धान केंद्र है जो क्रमशः अनुसंधान एवं विकास, प्रशिक्षण और व्यवसाय के क्षेत्रों में विकसित होता है। केंद्र के अनुसंधान एवं विकास क्षेत्रों में ईसुरक्षा, एंबेडेड सिस्टम्स, सर्वव्यापक कंप्यूटिंग, ईलर्निंग और ग्रामीण विकास के लिए आईसीटी हैं। केंद्र ने कई उत्पादों और समाधानों के समय में विकसित किया है और किनारे प्रौद्योगिकियों को काटने में कई प्रयोगशालाएं स्थापित की हैं। इन अनुसंधान एवं विकास शक्तियों के अनुरूप, केंद्र भी स्नातकोत्तर स्तर के डिप्लोमा पाठ्यक्रम प्रदान करता है। केंद्र भी संकाय प्रशिक्षण कार्यक्रमों के आयोजन में सक्रिय रूप से शामिल है। केंद्र नियमित रूप से कौशल आधारित प्रशिक्षण और सूचना सुरक्षा जागरूकता कार्यक्रम संचालित करता है। विकासपीडिया पोर्टल स्थानीय भाषाओं में प्रासंगिक सूचना, उत्पादों और सेवाओं के प्रावधान के माध्यम से ग्रामीण विकास की सुविधा के लिए होस्ट और रखे गए हैं।

आईएसईए के बारे में

सूचना सुरक्षा, इलेक्ट्रॉनिक्स विभाग और सूचना प्रौद्योगिकी के लिए बढ़ते महत्व को देखते हुए, यह एक महत्वपूर्ण क्षेत्र के रूप में पहचाना है। सूचना सुरक्षा शिक्षा और जागरूकता (आईएसईए) परियोजना सरकार द्वारा तैयार की और शुरूकी गई थी भारत की। इस कार्यक्रम के तहत गतिविधियों में से एक देश भर में बच्चों, शिक्षकों, गृह उपयोगकर्ताओं, आईटी और गैरआईटी पेशेवरों के बीच सूचना सुरक्षा जागरूकता फैलाना है। सीडैक हैदराबाद को इस परियोजना को इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी विभाग, संचार एवं सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार द्वारा कार्यान्वित करने की जिम्मेदारी सौंपी गई है। इस गतिविधि सीडीएसी के हिस्से के रूप में, हैदराबाद सूचना सुरक्षा जागरूकता सामग्री तैयार कर रहा है, विभिन्न सूचना सुरक्षा जागरूकता इवेंट आदि के आयोजन में भागीदारी संस्थाओं (पीआई के) के साथ समन्वय करता है,

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

परिचय

सूचना सुरक्षा जागरूकता

सूचना सुरक्षा आवश्यकताओं को सभी स्तरों पर, अलगअलग उपयोगकर्ता से एक संगठन में और उससे आगे और सरकार और राष्ट्र को संबोधित करना होगा। सूचना सुरक्षा कंप्यूटर नेटवर्किंग के रूप में राष्ट्रीय सुरक्षा का पर्याय बनती जा रही है, जो साइबर हमलों के लिए कमजोर है, देश के बैंकिंग, बिजली, संचार नेटवर्क आदि के महत्वपूर्ण आधारभूत संरचना की रीढ़ बनाता है। इसलिए, कंप्यूटर कंप्यूटर और नेटवर्क । साथ ही, विकसित देशों से आईटी और अन्य सेवाओं के आउटसोर्सिंग पर अधिक ध्यान केंद्रित करने से डेटा सुरक्षा को आगे बढ़ाया जा रहा है। इसके अलावा, बड़े पैमाने पर इंटरनेट बूम के कारण, बहुत से घर उपयोगकर्ताओं को धमकियों और उनके प्रतिवादों के बहुत कम या पूर्व ज्ञान के साथ इंटरनेट से अवगत कराया जाता है। यह, हमलावर, अपने दुर्भावनापूर्ण गतिविधि के आधार को बढ़ा सकते हैं और अपनी योजनाओं के लिए निर्दोष लोगों का उपयोग कर सकते हैं। नतीजतन, हमारा उद्देश्य स्कूल बच्चों, शिक्षकों, अभिभावकों और वरिष्ठ नागरिकों को शिक्षा का प्रसार करना है और खतरे को कम करने के लिए आवश्यक ज्ञान के साथ उन्हें तैयार करना है।

सूचना सुरक्षा, इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार के लिए बढ़ते महत्व को देखते हुए सूचना सुरक्षा शिक्षा और जागरूकता (आईएसईए) कार्यक्रम तैयार और शुरूकिया है। इस कार्यक्रम के तहत गतिविधियों में से एक, बच्चों, घर उपयोगकर्ताओं और गैरआईटी पेशेवरों के लिए एक योजनाबद्ध तरीके से सूचना सुरक्षा जागरूकता व्यापक रूप से उत्पन्न होती है।

साइबर सुरक्षा का महत्व

उपयोगकर्ताओं के लिए साइबर सुरक्षा महत्वपूर्ण है क्योंकि उन्हें पहचान की चोरी से खुद को सुरक्षित करना होगा। सरकार सहित संगठनों को उनके व्यापारिक रहस्यों, वित्तीय जानकारी और कुछ संवेदनशील या महत्वपूर्ण आंकड़ों की सुरक्षा के लिए भी इस सुरक्षा की आवश्यकता है। चूंकि सभी संवेदनशील जानकारी इंटरनेट से जुड़ी किसी कंप्यूटर पर संग्रहीत होती है, इसलिए जानकारी आश्वासन और सुरक्षा की आवश्यकता होती है। इसलिए साइबर सुरक्षा के लिए, हर किसी को साइबर सुरक्षा मानकों का पालन करना चाहिए, जो हमें विभिन्न मैलवेयर खतरों की सुरक्षा के लिए सक्षम बनाता है।

निम्न कारणों से कुछ के कारण एक गरीब साइबर सुरक्षा अभ्यास उत्पन्न होता है। आवेदन की खराब प्रशासनिक प्रक्रियाएं, खराब सॉफ्टवेयर कोडिंग जो साइबर सुरक्षा प्रथाओं के कमजोर और अनुचित उपयोग हो सकती हैं।

दृष्टि

भारतीय नागरिकों के बीच सूचना सुरक्षा जागरूकता उत्पन्न करें
सूचना सोसायटी में सुरक्षित रूप से भाग लेने के लिए उन्हें सक्षम करने के लिए

सूची

सूची

इंटरनेट के बारे में जानें

इंटरनेट का अर्थ है कंप्यूटर नेटवर्क्स के इंटरकनेक्शन। यह कई मिलियन कंप्यूटर, नेटवर्क डिवाईसेस व स्मार्ट फोन डिवाईसेस का एक व्यापक व विविध संयोजन है, जिसमें सब एक दूसरे से वायर्स व वायर्सरहित सिगनल्स से जुड़े रहते हैं। इंटरनेट की कई परिभाषाएँ हैं, लेकिन उनका अर्थ एक ही हैं, जो यहाँ दर्शाया गया है।

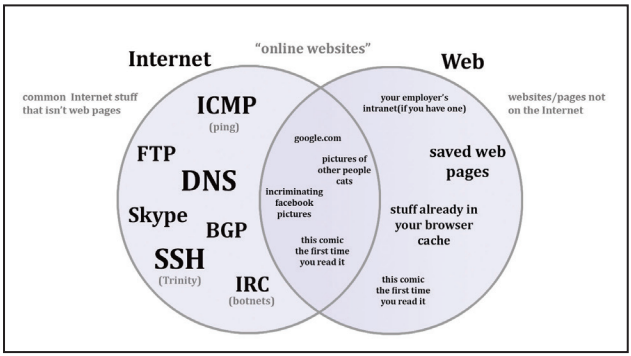
- **विश्वव्यापी स्तर पर कई मिलियन कंप्यूटर्स से जुड़े परस्पर संबद्ध नेटवर्कों की श्रेणी में डाटा कम्युनिकेशन के पारगमन को अनुमति देना**
- **विश्वव्यापी स्तर पर कंप्यूटरों को जुड़ने एवं सूचनाओं के आदानप्रदान की अनुमति देने वाला एक वैश्विक कम्युनिकेशन नेटवर्क।**
- **कंप्यूटर नेटवर्क की एक ऐसी विश्वव्यापी व्यवस्था, जिसमें नेटवर्क्स का नेटवर्क है, जहाँ किसी एक कंप्यूटर पर उपयोगकर्त्ता किसी अन्य दूसरे कंप्यूटर से सूचनाएँ ले सकते हैं।**

इंटरनेट शब्द का अर्थ है नेटवर्क्स का नेटवर्क। इंटरनेट में हजारों छोटे क्षेत्रीय नेटवर्क होते हैं जो समग्र दुनिया में फैले हैं। इंटरनेट को वैश्विक नेटवर्क का भौतिक भाग भी समझा जाता है। यह केबल्स व कंप्यूटर्स का विशाल स्तर पर संग्रहण है। यद्यपि यह 1960 के दशक में कम्युनिकेशन के बारे में एक फौजी प्रयोग के रूप में आरम्भ हुआ था, लेकिन सार्वजनिक रूप में एक ब्राडकास्ट फोरम के रूप में यह सन 1970 व सन 1980 के दशक में उभरा। कोई भी अकेली कोई ऐसी सत्ता नहीं है, जो इंटरनेट को नियंत्रित करती हो। इंटरनेट किसी की मिल्कियतनहीं है, यद्यपि कंपनीज हैं, जो नेटवर्क्स के विभिन्न भागों की व्यवस्था करने में मदद करती हैं और जो प्रत्येक को एक दूसरे से संबद्ध कर देती हैं और इस प्रकार कोई एक नियामक सत्ता नहीं है, जो नियंत्रित करे कि इंटरनेट पर क्या हो रहा है।

इंटरनेट वेब से किस प्रकार भिन्न है?

सन 1989 में इंटरनेट का विशाल सबसेट वर्ल्ड वाइड वेब डब्ल्यू.डब्ल्यू.डब्ल्यू के नाम से आरम्भ हुआ। वेब एक महाकाय संग्रहण है, एचटीएमएल पेजेस का जो इंटरनेट के हार्डवेयर द्वारा ट्रांसमिट होते हैं। आप पद वेब 1.0, वेब 2.0 व अदृश्य वेब सुनेंगे जो इन बिलियन वेब पेजेस के बारे में बताते हैं। इंटरनेट का वर्ल्ड वाइड वेब कुछ भाग है, क्योंकि इंटरनेट में वेब पेजेस के अलावा भी विभिन्न प्रकार का डाटा है।

वेब एक प्रकार की सॉफ्टवेयर एप्लीकेशन या सर्विस है, जो इंटरनेट पर चलती है। वेबपेजेस के रूप में यह दस्तावेज व स्त्रोत का संग्रहण है। समग्र विश्व के कंप्यूटर्स में समाई विशाल स्तर की जानकारी पर यह आपकी पहुँच आसान बनाता है। सामान्य व्यक्ति वेब व इंटरनेट का प्रयोग एक दूसरे के अर्थ में करते हैं। यह तकनीकी रूप से गलत है, क्योंकि इंटरनेट में वेब समाहित है।



वेब 1.0, वेब 2.0 व अदृश्य वेब क्या हैं?

वेब 1.0 जब सन 1989 में टिम बर्नर्सली द्वारा वर्ल्ड वाइड वेब प्रारंभ किया गया था, उस समय उसमें इलेक्ट्रानिक ब्रोशर्स के एक संग्रहण के रूप में मात्र विषय व चित्र ही सम्मिलित थे। वेब एक आसान ब्राडकास्टरिसीव के प्रारूप के रूप में संयोजित किया गया। हम इस सादे स्थिर प्रारूप को वेब 1.0 कहते हैं। आज कई वेब पेजेस अब भी बिल्कुल स्थिर हैं और वेब 1.0 अभी भी उपयोग में लाया जाता है।

वेब 2.0 सन 1990 के दशक के उत्तरार्ध में वेब ने स्थिर सामग्री से आगे जाना शुरूकिया और इंटरएक्टिव सेवाएँ प्रस्तावित करना प्रारंभ किया। मात्र वेब पेजेस के रूप में ब्रोशर्स के स्थान पर, वेब ने ऑनलाईन सॉफ्टवेयर शुरूकिया, जहाँ लोग कंप्यूटर से संबंधित काम कर सकते थे व वैसी सेवाएँ प्राप्त कर सकते थे। सन 2000 के आसपास ऑनलाईन बैंकिंग, वीडियो गेमिंग, डेटिंग सेवाएँ, स्टाक्स ट्रेकिंग, वित्तीय योजना, ग्राफिक्स संपादन, होम वीडियोज, वेबमेल सेवाएँ जैसे जीमेल,याहू मेल आदि नियमित तौर पर वेब प्रस्तुतियाँ के रूप में प्रारंभ हो गईं। इन ऑनलाईन सेवाओं को वेब 2.0 कहते हैं। वेब 2.0 को हमारी रोजमर्रा की जिंदगी का भाग बनाने में फेसबुक, फ्लिकर, ईबे व जीमेल जैसे नाम हमारी मदद करते हैं।

वर्ल्ड वाइड वेब का तीसरा भाग अदृश्य वेब है।

तकनीकी रूप से वेब 2.0 का अदृश्य वेब एक सबसेट है, जो उन कई बिलियन पेज के बारे में बताता है, जो जानबूझकर नियमित सर्च इंजिन से छुपाए गए हैं। ये अदृश्य वेब पेजेस निजी व गोपनीय पेजेस हैं उदाहरणार्थ निजी ईमेल, व्यक्तिगत बैंकिंग विवरण तथा वे वेब पेजेस हैं, जिनका उदभव विशिष्ट डाटाबेस के द्वारा हुआ है उदाहरणार्थ क्लीवलैंड या सेवाइल में नौकरी। अदृश्य वेब पेजेस या तो आपकी सामान्य आँखों से छिपाए जाते हैं या उनका पता लगाने के लिए विशेष सर्च इंजिन की जरूरत रहती है। अदृश्य वेब के बारे में और अधिक यहाँ पढ़िए।

वेब साईट क्या है?

वेब साईट में आपस में संबद्ध एक से कई मिलियन तक पेजेस होते हैं और उसमें हायपरलिंक्स होती हैं, जो वेब साईट पर आपका मार्ग खोजने में मदद करती है। वेब पर आप विभिन्न प्रकार की जानकारियाँ जैसे कि खेल, स्वास्थ्य से संबंधित, छुट्टियों के लिए गंतव्य स्थान, ट्रेन के समयपत्र, मौसम का पूर्वानुमान और इस प्रकार की कई सूचनाएँ प्राप्त कर सकते हैं। इंटरनेट पर कई मिलयन वेब साईट्स उपलब्ध हैं और आप वह सब कुछ वहाँ मालूम कर सकते हैं, जिसमें आपकी दिलचस्पी है।

वेब एड्रेस

प्रत्येक वेब साईट का अपना स्वयं का अनूठा पता होता है, जिसे यूनिफार्म रिसोर्स लोकेटर या यूआरअल कहते हैं। साईट देखने के लिए आपको आपके वेब ब्राउजर के एड्रेस बार पर उसका पता टाईप करना होता है।

इंटरनेट का उपयोग

इंटरनेट का उपयोग मुख्यतः संचार के लिए होता है, जिससे शिक्षण, मनोरंजन, सामयिक खबरें, ऑनलाईन शिक्षण, वाणिज्य, प्रकाशन आदि से संबंधित सूचनाएँ प्राप्त की जा सकें।

इंटरनेट के उपयोग में प्रकाशन मात्र संगठन या व्यवसाय के उपयोग हेतु नहीं है, कोई भी अपनी स्वयं की वेबसाईट्स तैयार कर सकता है और सूचनाएँ या फाईल्स वर्ल्ड वाइड वेब पर प्रकाशित कर सकता है।

दुनिया में इंटरनेट के माध्यम से सूचनाओं तक हजारों लोगों की पहुँच अपने घरों, शालाओं, इंटरनेट कैफे व कार्य स्थलों से होती है।

इंटरनेट एक कंप्यूटर नेटवर्क का वैश्विक संग्रहण है, जो कॉमन सॉफ्टवेयर स्टेंडर्ड का उपयोग कर डाटा के आदानप्रदान में मदद करता है। इंटरनेट उपयोगकर्त्ता विभिन्न स्रोतों से जानकारियाँ साझा कर सकते हैं।

- उपयोगकर्त्ता आसानी से सामान्य पर्सनल कंप्यूटर के माध्यम से संबद्ध हो सकते हैं व इंटरनेट का उपयोग कर ज्ञान, विचार साझा कर सकते हैं।
- इंटरनेट पर अकाउन्ट्स से हम परिवार के सदस्यों और मित्रों को इलेक्ट्रानिक मेल ईमेल प्रेषित कर सकते हैं, जो डाक द्वारा पत्र भेजने के समान ही है।
- बिना डाक टिकट के ईमेल कुछ ही मिनटों में भेजा जा सकता है, इससे कोई फर्क नहीं पड़ता है कि वे कहाँ पर हैं।
- हम वे जानकारियाँ पोस्ट कर सकते हैं, जहाँ दूसरों की पहुँच हो सकती है और उसे बारबार अद्यतन कर सकते हैं।
- हमारी पहुँच मल्टीमीडिया जानकारियों पर भी हो सकती है, जिनमें वीडियो, ऑडियो व इमेजेस सम्मिलित हैं।
- इंटरनेट पर वेब आधारित प्रशिक्षण व दूरस्थ शिक्षण से हम सीख सकते हैं।

इंटरनेट पर पहुँच

शिक्षकों के लिए इंटरनेट एक समयउत्कृष्ट साधन है, जो पाठ्यक्रम में वृद्धि की संभावनाओं को बढ़ा देता है। शिक्षण निर्भर होता है संबंधित व विश्वसनीय जानकारियों को तुरंत व आसानी से प्राप्त करने व साथ ही उन जानकारियों के चयन, उन्हें समझने व आकलन करने की योग्यता पर। इंटरनेट पर जानकारियों को ढूँढने से इन कुशलताओं को विकसित करने में मदद मिलती है। कक्षा अभ्यास और घर के लिए दिए जाने वाले कार्य में जहाँ छात्रों को वेबसाईट विषय की तुलना करने की जरूरत रहती है वहाँ वे चेतावनी देने, छात्रों को विभिन्न प्रकार के श्रोतागणों हेतु लिखने, विशेष विषय के उद्देश्य, परिशुद्धता व विश्वसनीयता को पहचानने व उसका आकलन करने की आवश्यकता के संबंध में आदर्श होते हैं। चूँकि कई वेबसाईट्स मुद्दों के संबंध में कोई विशेष दृष्टिकोण अपना लेती है, अतः इंटरनेट दृष्टिकोणों से तथ्य में अंतर विकसित करने की कुशलता में एवं आत्मनिष्ठा व वस्तुनिष्ठा की तलाश करने में एक उपयोगी साधन है ।

इंटरनेट छात्रों व बच्चों में संचार व सहयोग कौशल्य विकसित करने हेतु एक बड़ा साधन है। इससे भी आगे इंटरनेट भाषाई कौशल्य के निर्माण हेतु एक प्रभावी साधन है। ईमेल, चेट रूम्स व चर्चा समूहों के द्वारा छात्र लिखने के रूप में संचार के बुनियादी सिद्धांत सीखते हैं। इससे अध्यापकों को मौका मिलता है, इंटरनेट आधारित गतिविधियों को सामान्य साक्षरता कार्यक्रमों में शामिल करने का, जिससे वे उनकी अध्यापन की नीतियों में विविधता ला सकें।

दूसरी शालाओं या बल्कि दूसरे देशों के सहपाठियों के साथ ईमेल संदेशों के द्वारा, सामान्यतः सहयोगयुक्त परियोजनाओं के द्वारा छात्रों के साक्षरता कौशल्य में सुधार लाया जा सकता है। सहयोगयुक्त परियोजनाएँ छात्रों को संलग्न रखने व उल्लेखनीय शिक्षण के अनुभवों हेतु भी उपयोगी हैं। इस प्रकार अंतरसांस्कृतिक समझ को आगे बढ़ाने में इंटरनेट एक प्रभावी साधन बन गया है। शांत चेट रूम्स व समूह परियोजनाएँ भी छात्रों को सहयोगात्मक रूप से सीखने का अवसर उपलब्ध करा सकती हैं।

इंटरनेट सीखने की सामग्री का एक महाकाय विशाल भंडार कक्ष होता है। इसके फलस्वरूप यह उल्लेखनीय रूप से छात्रों के लिए उपलब्ध स्त्रोतों को विस्तृत करता है जो शालाओं के पुस्तकालयों में मौजूद प्रचलित मुद्रित सामग्री से आगे की स्थिति है। छात्रों की सरकारी व गैरसरकारी वेबसाईट्स तक पहुँच हो सकती है, जिनमें संशोधन के परिणाम, संग्रहालयों और कला दीर्घाओं तथा अन्य संघटनों के वैज्ञानिक व कलात्मक स्त्रोत भी सम्मिलित हैं, जो छात्रों के शिक्षण पर लागू होती हैं। शालाओं के माध्यमिक स्तर पर इंटरनेट का उपयोग यथोचित रूप से जटिल अनुसंधान परियोजनाओं को लेने के लिए किया जा सकता है।

जैसा कि इंटरनेट सीखने के लिए एक सशक्त स्त्रोत है तथा यह संचार के लिए एक प्रभावी साधन है, इसलिए यह शिक्षण हेतु बहुत लाभप्रद है और यह सीखने के कई लाभ उपलब्ध कराता है। इसमें शामिल हैं, सीखने के विस्तृत क्षेत्र में से किसी विशिष्ट विषय को सीखने तक की पहुँच में सुधार के द्वारा स्वतंत्र रूप से सीखने व अनुसंधानकौशल्य के क्षेत्र में प्रगति, व साथ ही एकीकृत या पाठ्यक्रम से आगे के अध्ययन व संचार व सहयोग, जैसे कि स्त्रोतों तक की पहुँच के लिए प्रौद्योगिकी की सीख का इस्तेमाल व सामर्थ्य व स्त्रोत निर्मित करना व दूसरों से संवाद स्थापित करना।

इंटरनेट की विशेषताएँ

- भौगोलिक साझेदारी

  इंटरनेट की भौगोलिक साझेदारी पूरी दुनिया और उसके आगे लगाता फैलती जा रही है। इंटरनेट की मुख्य विशेषता है कि आप जैसे ही उसके किसी भी भाग से यदि जुड़ गए, आप उसके समग्र से संचार कर सकते हैं।
- आर्किटेक्चर

  कम्युनिकेशन नेटवर्क डिजाईन में इंटरनेट का आर्किटेक्चर अप्रतिम है। व्यक्तिगत कंप्यूटर्स या नेटवर्क्स के निष्फल होने पर भी यह उसकी कुल विश्वसनीयता को किसी भी प्रकार से प्रभावित नहीं करता है। समय के साथ या साईट्स पर अंतरित होने पर जानकारियाँ न परिवर्तित होंगी या न नष्ट होंगी।
- विश्वव्यापी पहुँच

  यह आसान है कि विषय, ऑडियो, वीडियो जैसी जानकारियों तक पहुँचना व उन्हें निर्मित करना व साथ ही उनके लिए अत्यंत कम कीमत पर विश्वव्यापी स्तर पर पहुँचना। कोई फर्क नहीं पड़ता है और कोई कहीं भी हो,इंटरनेट पर पहुँच प्रत्येक के लिए समान है। कोई दुनिया के किसी भी कंप्यूटर से जुड़ सकता है और बगैर अपनी कुर्सी से हिले आप दुनिया के कई रोमांचक स्थलों पर जा सकते हैं।

इंटरनेट के लाभ

इंटरनेट से कई लाभ हैं

- इंटरनेट डाटा व जानकारियों से भरा रहता है, जिनमें माध्यम की श्रेणी भी हैं।
- जो सर्च इंजिन ऑनलाईन उपलब्ध रहते हैं,वे तीव्र व सशक्त होते हैं।
- इंटरनेट इस्तेमाल में आसान है।
- डाटा तक पहुँचने में आसानी होने के कारण छात्र संशोधक बन सकते हैं।
- दुनिया के साथ अपना काम साझा करने हेतु छात्र प्रोत्साहित होते हैं।
- सीखने की विभिन्न शैलियों के कारण इंटरनेट के प्रति आकर्षण रहता है।
- काग़ज के विपरीत वेब गतिशील डाटा स्त्रोत उपलब्ध करा सकते हैं, जो समय के साथ बदल जाते हैं।
- ईमेल के केरेक्टर्स जब लंबी दूरी पर भेजे जाते हैं तब वे अंतरित या मिश्रित नहीं होते हैं।
- छात्र की पहुँच दुनिया में हर ओर के पुस्तकालय में हो जाती है।

निजता के मुद्दे

कई बच्चे इंटरनेट पर कुशल नेवीगेटर हैं। कंप्यूटर्स का उपयोग कर वे आरामदायक महसूस करते हैं और माउस की एक क्लिक पर जानकारियाँ व इमेजेस के आ जाने से वे मोहित हो जाते हैं। हाल ही के आँकड़े दर्शाते हैं कि शाला जाने की उम्र के बच्चों में से ९० की घर या शाला में कंप्यूटर तक की पहुँच है। बच्चों में दूसरों के साथ परस्पर संवाद या संपर्क करने की योग्यता, इंटरनेट के प्रति उनके सबसे बड़ा आकर्षणों में से एक है। हम देख रहे हैं कि लोग चेट रूम्स में वक्त बिता रहे हैं, मोबाईल के माध्यम से इंस्टंट संदेश जा रहे हैं, गेम्स खेल रहे हैं, प्रतियोगिताओं में भाग ले रहे हैं और लोकप्रिय ऑनलाईन गतिविधियों के फार्म्स भर रहे हैं। दुर्भाग्य से अधिकांश मातापिता यह वास्तव में नहीं समझते हैं कि ये गतिविधियाँ किस प्रकार बच्चों की निजता को जोखिम पर रख सकती हैं या उनकी सुरक्षा के लिए खतरा भी हो सकती है। यह भी आश्चर्यजनक है कि भारत में अधिकांश मातापिता यह कभी नहीं जान पाते हैं उन गतिविधियों के बारे में, जिनमें उनका बच्चा इंटरनेट पर भाग लेता है।

आज के इंटरनेट संचार परिदृश्य में व्यक्तिगत डाटा मूल्यवान हैं और उन्हें संरक्षित रखना एक कौशल्य है, जिसे बच्चों को समझना व सीखना है।

बच्चों की निजता में कुछ ऑनलाईन गतिविधियों से समझौता किया जा सकता है

- ✓ वाणिज्यिक या मुक्त वेब साईट्स पर विभिन्न प्रकार के सर्वेक्षणों, प्रतियोगिताओं, डाऊनलोडिंग गेम्स के लिए फार्म्स भरना।
- ✓ ईमेल असेस, चेट असेस की रजिस्ट्रीकरण हेतु व्यक्तिगत जानकारियों के विवरण देना।
- ✓ फ्री गेम डाऊनलोड्स के रजिस्ट्रीकरण के समय जानकारियाँ उपलब्ध कराना।
- ✓ सोशल नेटवर्किंग वेबसाईट्स के रजिस्ट्रीकरण के समय जानकारियाँ उपलब्ध कराना।

- **निजता**

  कुछ वेबसाईट्स छात्रों को प्रेरित करती हैं कि वे एक फ़ार्म भरें, जिसमें उनका नाम, ईमेल पता, उम्र, व लिंग और कभी उनका टेलीफोन नंबर व डाक का पता तक भरना होता है, जिससे सूचनाओं तक पहुँच हो सके। कुछ अनुरोध तो वैध होते हैं यह उस वेबसाईट की प्रकृति पर अधिक निर्भर होता है जो जानकारियों के लिए अनुरोध कर रही है। ऑनलाईन व्यक्तिगत जानकारियों को उपलब्ध कराने के कारण छात्र स्पैम अवांछित ईमेल, विज्ञापन सामग्री एवं/या वायरस के लक्ष्य बनते जा रहे हैं। निजता के मुद्दे उन छात्रों पर भी लागू होते हैं जो अपनी व्यक्तिगत वेबसाईट्स व ऑनलाईन प्रकाशन तैयार कर रहे हों। फोटोग्राफ सहित व अन्य छात्रों के व्यक्तिगत विवरणों को अधिकार में लेकर अन्य लोग उन जानकारियों का नाजायज उद्देश्यों हेतु पुनः उपयोग कर सकते हैं।

- **आपका कंप्यूटर अवांछित सॉफ्टवेयर के समक्ष उजागर**

  सामान्यतः कई सहकर्मी से सहकर्मी फाईल वे प्रोग्राम साझा करते हैं, जिनमें अच्छी सुरक्षा या असेस नियंत्रण प्रयुक्त किया हुआ नहीं होता है। यदि उपयोककर्त्ता उन प्रोग्राम्स से परिचित नहीं हैं या सेटिंग्स का अनुपयुक्त कंफीगुरेशन है तो जो भी सामग्री उपयोगकर्त्ता की हार्ड डिस्क में संग्रहित होगी, तब उसके लिए यह खतरनाक होगा कि वे अन्य उपयोगकर्ताओं के लिए उजागर हो जाएंगी।

- **कंप्यूटर वायरस से कांट्रेक्टिंग**

  इसके अलावा पी२पी सॉफ्टवेयर के कंप्यूटर्स आसानी से कंप्यूटर वायरस के कांट्रेक्ट में आ जाते हैं, विशेषकर तब जब अज्ञात स्त्रोत से फाईल डाऊनलोड की गई हो। साथ ही इन पी२पी प्रोग्राम में वायरस व वार्म्स हो सकते हैं, जिससे उपयोगकर्त्ताओं के कंप्यूटर्स के ठीक से काम करने में रूकावट आ जाती है।

- **कापीराईट उल्लंघन**

  कई कापीराईट कानून का उल्लंघन कर मनोरंजन फाईल्स की प्रतियाँ उदाहरणार्थ एमपी ३ म्यूजिक फाईल्स, वीसीडी वीडियो फाईल्स आदि तथा सॉफ्टवेयर अक्सर पी२पी सॉफ्टवेयर से साझा किए जाते हैं। दूसरों के लिए कापीराईट कार्य का अनाधिकृत रूप से डाऊनलोडिंग का काम सिविल या फौजदारी दंड आमंत्रित करता है।

- **आपकी शाला के इंटरनेट की गति का कम होना**

  अंत में है, लेकिन फिर भी महत्वपूर्ण है कि जब आप अन्य व्यक्तियों के लिए शाला के केम्पस नेटवर्क के माध्यम से पी२पी सॉफ्टवेयर के द्वारा बड़े परिमाण में फाईल्स डाऊनलोड करते हैं, तब उससे उत्पन्न नेटवर्क ट्राफिक के कारण संपूर्ण केम्पस नेटवर्क को वह धीमा कर सकता है।

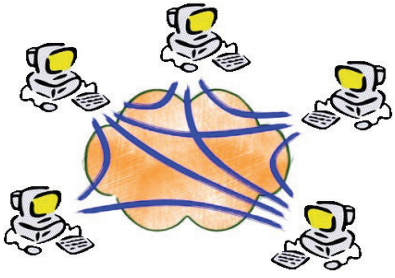
- **सहकर्मी से सहकर्मी पी२पी नेटवर्किंग**

  सहकर्मी से सहकर्मी या पी२पी कंप्यूटर नेटवर्क विविध कनेक्टिविटी का इस्तेमाल नेटवर्क के सहभागियों तथा नेटवर्क सहभागियों की क्युमुलेटिव बैंडविड्थ के बीच करता है तथा बनिस्बत प्रचलित केन्द्रीकृत स्त्रोतों के ग्राहकसर्वर स्थापत्य, जहाँ तुलनात्मक रूप से कम संख्या में सर्वर कोर सेवाएँ उपलब्ध कराते हैं। नोड्स को कनेक्ट कर मुख्यतः तदर्थ नेटवर्क के द्वारा ऑडियो, वीडियो, डाटा या किसी भी प्रकार के डिजिटल डाटा जैसे विषय में साझेदारी है ।

  अपने असंरचित नेटवर्क तथा अनजाने कंप्यूटर्स या व्यक्तियों से साझा करने के कारण सहकर्मी से सहकर्मी नेटवर्किंग की जोखिम की वजह से आपके कंप्यूटर वायरस, स्पाम से प्रभावित या संक्रमित हो सकते हैं।

पी२पी नेटवर्क्स के लिए टिप्स

- ✓ जिस पर आपके सिस्टम से डाटा कम्युनिकेशन फिल्टर करने हेतु आप विश्वास करते हैं, उसी फिल्टरिंग सॉफ्टवेयर का इस्तेमाल करें।
- ✓ फाईल साझा करने के प्रोग्राम का इस्तेमाल कर पी२पी प्रोग्राम को नियंत्रित व समायोजित करें, जिससे जब जरूरत हो तब चालू किया जा सके।
- ✓ सदैव ऑपरेटिंग सिस्टम, एंटीवायरस और एंटी स्पायवेयर पैकेजेस को अद्यतन रखें।
- ✓ प्रशासनिक अकाउंट का उपयोग न करें। यह अन्य पी२पी नेटवर्क्स उपयोगकर्त्ताओं के लिए पूरा सिस्टम उजागर कर

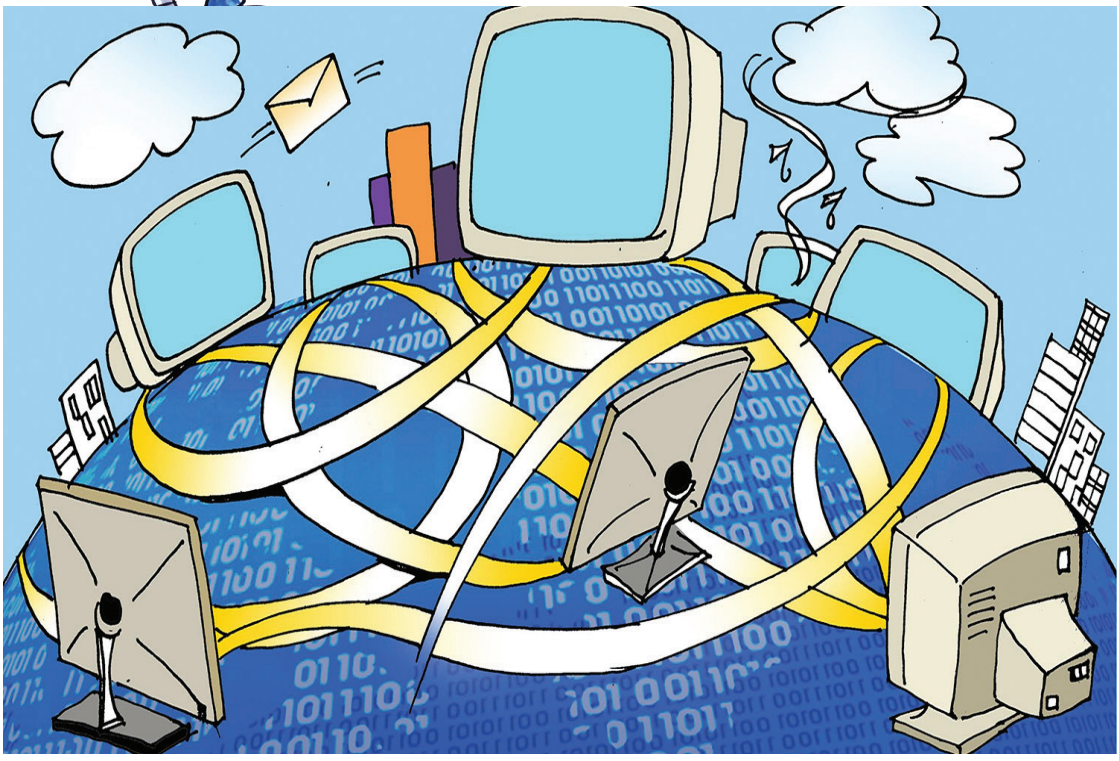


सकता है। सामान्य संचालन के लिए अलग अकाउंट बनाएँ।

- ✓ सभी डाऊनलोड की गई फाईल्स को शक के दायरे में रखें।
- ✓ महत्वपूर्ण फाईल्स का बेकअप लें। इससे आपको फाईल्स की पुनः प्राप्ति में मदद मिलेगी।
- ✓ कोई भी पायरेटेड सॉफ्टवेयर, फाईल्स आदि को डिलीट कर दें। वैकल्पिक रूप में उन्हें कभी भी डाऊनलोड न करें।

यदि आप पीरपी नेटवर्क्स से ठीक से वाकिफ नहीं हैं, तो कभी भी पीरपी नेटवर्क्स में सहभागिता न करें, ।

सहकर्मी से सहकर्मी नेटवर्क्स पर आपकी फाईल्स साझा करने में बहुत जोखिम हैं।



कंप्यूटर आचार-नीति

आचार-नीति उन नैतिक सिद्धांतों का एक सेट है, जो यह बताता है कि किसी व्यक्ति या समूह को नियंत्रित करने वाले कंप्यूटर इस्तेमाल के स्वीकार्य व्यवहार कौन से हैं। कंप्यूटर आचार-नीति कंप्यूटर के इस्तेमाल को नियंत्रित करने वाले नैतिक सिद्धांतों का समूह है। कंप्यूटर आचार-नीति में जो एक सामान्य नीति है, जिसका कई अनुपालन नहीं करते हैं, वह है कापीराईट संबंधी मामलों का उल्लंघन।

कापीराईट वाली विषय-सामग्री लेखक की अनुमति के बिना प्रतिलिपी तैयार करना, दूसरों की व्यक्तिगत जानकारी तक पहुँचना-नैतिक सिद्धांतों के उल्लंघन के उदाहरण हैं।

छात्रों/ अध्यापकों का अनैतिक व्यवहार क्या है?

डिजिटल साहित्यिक चोरी:

शैक्षणिक बेईमानी का एक मुख्य प्रकार साहित्यिक चोरी है, जो शिक्षा के क्षेत्र में सदैव रही है, विशेषकर उच्च-शिक्षा के क्षेत्र में। उदाहरणार्थ छात्रों द्वारा प्रस्तुत किए जाने वाले असाईनमेंट्स अक्सर साथी छात्रों के पास उपलब्ध सामग्री की नक़्ल कर तैयार होते हैं या प्रकाशित सामग्री में से पूर्ण या आंशिक रूप से ले लिये जाते हैं। इस साहित्यिक चोरी को करने हेतु छात्रों के उपलब्ध साधनों में कंप्यूटर्स व इंटरनेट इस्तेमाल ने एक नया आयाम जोड़ा है। यद्यपि यह करना आसान है पर उसे पकड़ पाना मुश्किल।

कापीराईट का उल्लंघन वसॉफ्टवेयर चोरी:

पूरे समाज में यह ज्ञात है कि कापीराईट मीडिया झ्मूल-पाठ, संगीत के कार्य, मूवीज वसॉफ्टवेयर प्रोग्राम्सट की गैरकानूनी नक़्ल बड़े पैमाने पर हो रही है। साथ ही कई लोग जो इस प्रकार की गतिविधियों में लिप्त रहते हैं, उन्हें नहीं लगता है कि वे कुछ अनैतिक कर रहे हैं। कॉलेज के छात्रों के लिए यह वास्तव में सही है। और लगता है कि छात्रों का यह रूझान वर्तमान सूचना-उम्र में जो प्रगति हो रही है, उसके साथ मेल खाता है, जिसमें इंटरनेट बड़े स्तर पर सर्वाधिक महत्वपूर्ण सूचना माध्यम के रूप में कार्य कर रहा है, जिसका लोग उपयोग कर रहे हैं

कंप्यूटर स्त्रोतों का अनुचित इस्तेमाल:

छात्र व स्टॉफ कंप्यूटर स्त्रोतों तक पहुँच हेतु प्राधिकृत हो सकते हैं, लेकिन बाद में वे इन स्त्रोतों का उपयोग अनुचित ढंग से जारी रखते हैं। उनके पास शाला/पुस्तकालय का इंटरनेट अकाउंट हो सकता है या वे कंप्यूटर सिस्टम या कंप्यूटर नेटवर्क या कंप्यूटरसॉफ्टवेयर का उपयोग कर सकते हैं, जो शाला की मिल्कियत हो या वे शाला द्वारा प्रस्तावित कंप्यूटराइज्ड सेवाओं का उपयोग इस प्रकार कर सकते हैं, जो शाला के मानकों के अनुसार, उस विशेष स्त्रोत के समुचित उपयोग हेतु न हो।

उदाहरणार्थ छात्र अपने छात्र-अकाउंट का उपयोग कर अपना स्वयं का इंटरनेट व्यवसाय चला सकते हैं, कोई लोकप्रिय वेबसाईट या सर्विस खोल सकते है, जिससे अधिक ट्रॉफिक हो सकता हो, एमपी ३ फाईल्स डाऊनलोड कर सकते हैं व स्टॉफ के सदस्य शाला का सर्वर या कंप्यूटर सिस्टम का इस्तेमाल कर वह डाऊनलोड कर सकते हैं या देख सकते हैं, जो अवैधानिक या शाला की नीतियों के खिलाफ हो झ्जैसे कि जातिवाद या तानाशाही से सम्बन्धित सामग्री या अश्लील सामग्रीट या शैक्षणिक समुदाय के सदस्य कंप्यूटर वायरस या वार्म्स फैला सकते हैं।

सूचनाओं की निजता व गोपनीयता को सुरक्षित करना:

- **व्यक्तिगत जानकारी आम कंप्यूटर्स पर:**

  सार्वजनिक पहुँच वाले कंप्यूटर्स के इस्तेमाल के समय छात्र या स्टॉफ अनजाने में अपनी व्यक्तिगत जानकारियाँ सार्वजनिक कंप्यूटर्स पर छोड़ सकते हैं, जैसे कि गुप्त वेब पेजेस झ्असेस किए गए वेब पेजेस जो अस्थाई स्टोरेज में डिस्क ड्राइव पर छोड़ दिए गए और फिर वे ब्राउसर बंद होने के बाद भी वहाँ रह सकते हैंट व कुकीज झ्छोटी फाईल्स जिन्हें वेब साईट द्वारा हार्ड डिस्क पर रखा जाता है, जिससे उपयोगकर्त्ताओं और उनकी प्राथमिकताओं को पहचाना जा सकेट जो फिर बाद में दूसरों के निरीक्षण के लिए उपलब्ध रहती हैं।

- **फाईल साझा करना:**

  वे कंप्यूटर्स जिनका इस्तेमाल छात्र या संकाय करते हैं, उनमें वेसॉफ्टवेयर हो सकते हैं, जहाँ कंप्यूटर असेसिबल से फाईल्स अन्य उपयोगकर्त्ताओं को केम्पस नेटवर्क पर बिना मालिक की जानकारी के जा सकती हैं, या वे अनुमति दे सकते हैं कि फाईल्स को केन्द्रीय सर्वर में स्टोर किया जाए, जहाँ वे उनकी इजाजत के अन्य की पहुँच में आ जाएं। इससे अजनबी इन फाईल्स की व्यक्तिगत जानकारियाँ होने पर पढ़ सकते हैं।

यह सुनिश्चित करें कि आपके पास ई-मेल व इंटरनेट के उपयोग के संबंध में नीतियाँ हैं

- **शाला के वेब पेजेस व बुलेटिन बोर्ड्स:**

  शाला, संकाय या छात्र द्वारा बनाए गए वेब पेजेस, जिनमें व्यक्तिगत जानकारियाँ हो सकती हैं और जिससे दूसरों की निजी जानकारी प्राप्त की जा सकती है। इसी प्रकार बुलेटिन बोर्ड्स या अन्य इलेक्ट्रोनिक फोरम्स पर पोस्टिंग्स या रि-पोस्टिंग्स झ्फार्वडेड संदेशट में तीसरे पक्ष की व्यक्तिगत जानकारियाँ हो सकती हैं, जिसके लिए अनुमति न दी गई है।

कंप्यूटर की आचार-नीति के बारे में दस नियम:

- दूसरे व्यक्ति को नुकसान पहुँचे, इस प्रकार कंप्यूटर का उपयोग नहीं करना चाहिए।
- किसी को अन्य के कंप्यूटर के काम में हस्तक्षेप नहीं करना चाहिए।
- किसी को अन्य के कंप्यूटर की फाईल में तांक-झाँक नहीं करना चाहिए।
- किसी को चुराने के लिए कंप्यूटर का इस्तेमाल नहीं करना चाहिए।
- किसी को झूठे सबूत हेतु कंप्यूटर का इस्तेमाल नहीं करना चाहिए।
- किसी को जिसके लिए उसने भुगतान नहीं किया है, उस मालिकाना सॉफ्टवेयर की न नक़्ल करना चाहिए और न उसे इस्तेमाल करना चाहिए।
- किसी को अन्य दूसरे के कंप्यूटर स्त्रोतों का उपयोग बिना प्राधिकरण या बिना उचित मुआवजे के नहीं करना चाहिए।
- किसी को दूसरे के बौद्धिक आउटपुट को नहीं हड़पना चाहिए।
- किसी के द्वारा लिखे प्रोग्राम या डिजाईन किए सिस्टम के सामाजिक परिणामों के बारे में हर किसी को अवगत होना चाहिए ।
- किसी को कंप्यूटर सदैव इस प्रकार उपयोग में लेना चाहिए, जिससे साथी इंसानों का मान व सम्मान सुनिश्चित हो।

कंप्यूटर उपयोगकर्ताओं के लिए नैतिक नियम

यहाँ कुछ सूचीबद्ध नियम प्रस्तुत हैं- कंप्यूटर का उपयोग करते समय इनका अनुपालन किया जाना चाहिए:

- दूसरे उपयोगकर्त्ताओं को नुकसान पहुँचे, इस प्रकार कंप्यूटर का उपयोग नहीं करें।
- किसी की जानकारियाँ चुराने के लिए कंप्यूटर्स का इस्तेमाल नहीं करें।
- मालिक की मर्जी के बगैर उनकी फाईल्स हासिल न करें।
- लेखक की इजाजत के बिना कापीराईट वाले सॉफ्टवेयर की नक़्ल न करें।
- सदैव कापीराईट कानूनों व नीतियों का सम्मान करें।
- दूसरों की निजता का सम्मान करें, वैसे ही जैसी आप दूसरों से प्रत्याशा रखते हैं।
- किन्हीं अन्य उपयोगकर्त्ताओं के कंप्यूटर स्त्रोतों का उपयोग बिना उनकी अनुमति के नहीं करें।
- इंटरनेट का इस्तेमाल नीतिपूर्वक करें। यदि आप कुछ गैरकानूनी संचार व गतिविधियाँ पाएँ, तो इंटरनेट सेवा प्रदाताओं व स्थानीय प्रवर्तन सत्ताओं को शिकायत दर्ज कराएँ
- यूजर आईडी व पासवर्ड की सुरक्षा रखने में उनके उपयोगकर्त्ता जवाबदेह हैं याद रखने के उद्देश्य से उन्हें काग़ज या अन्य कहीं पर भी नहीं लिखना चाहिए।
- उपयोगकर्त्ताओं को जान-बूझकर कंप्यूटर्स का उपयोग दूसरों की जानकारियों की पुनः प्राप्ति या उन्हें संशोधित करने के लिए नहीं करना चाहिए, जिनमें पासवर्ड की जानकारी, फाईल्स आदि हो सकती हैं।

आचार-नीति नैतिक सिद्धांतों का एक सेट है, जो किसी व्यक्ति या समूह को नियंत्रित करता है यह बताने के लिए कि कंप्यूटर के इस्तेमाल के दौरान स्वीकार्य व्यवहार कौनसे हैं।

कंप्यूटर आचार-नीति उन नैतिक सिद्धांतों का समूह है जो कंप्यूटर के इस्तेमाल को नियंत्रित करता है। कंप्यूटर आचार-नीति में जो एक सामान्य नीति है, जिसका कई अनुपालन नहीं करते हैं, वह है कापीराईट के मुद्दों का उल्लंघन।

इंटरनेट आचार-नीति

इंटरनेट आचार-नीति से अर्थ है इंटरनेट के उपयोग हेतु स्वीकार्य व्यवहार। इंटरनेट पर हमें ईमानदार रहकर दूसरों के अधिकारों व उनकी संपत्ति का सम्मान करना चाहिए।

स्वीकार

वर्ड वाईड वेब, वेस्ट वाइल्ड वेब नहीं है। यह वह जगह है, जहाँ मूल्यों पर विचार विस्तृत अर्थ में किया जाता है। हमें विषय-सामग्री व सेवाओं को आकार देते समय ध्यान रखना चाहिए तथा हमें यह स्वीकार करना चाहिए कि इंटरनेट वैश्विक समाज से अलग नहीं है, बल्कि यह उसका एक मुख्य घटक है।

राष्ट्रीय व स्थानीय संस्कृतियों के प्रति संवेदना

यह सबका है और राष्ट्रीय व स्थानीय संस्कृतियों हेतु कोई अवरोध नहीं है। इसमें स्थानीय टीवी चैनल, स्थानीय अखबार जैसे मूल्यों के कोई अलग सेट नहीं है, इसलिए हमें उपयोग की बहुलता को समायोजित करना चाहिए।

ई-मेल व चेटिंग के इस्तेमाल करते समय

इन्टरनेट का उपयोग परिवार व मित्रों के साथ संचार हेतु होना चाहिए। हमें अनजाने लोगों के साथ संचार के लिए इंटरनेट चेटिंग का इस्तेमाल नहीं करना चाहिए और न ही अनजाने लोगों के ई-मेल्स फॉरवर्ड करना चाहिए। साथ ही हमें बच्चों

को सिखाना चाहिए कि अनजाने लोगों के साथ चेटिंग या ई-मेल फारवर्डिंग में किस प्रकार का जोखिम हो सकता है।

किसी और जैसा नाटक करना

हमें इंटरनेट का उपयोग कोई अन्य व्यक्ति के रूप में बताने के लिए एवं दूसरों को मूर्ख बनाने के लिए नहीं करना चाहिए। हमें बच्चों को सिखाना चाहिए कि दूसरों को मूर्ख बनाना तथा स्वयं की पहचान छुपाना एक अपराध है।

अभद्र भाषा से बचें

ई-मेल, चेटिंग, ब्लॉगिंग व सोशल नेटवर्किंग के इस्तेमाल के समय हमें कठोर या अभद्र भाषा का उपयोग नहीं करना चाहिए, हमें चाहिए कि उनके विचारों का सम्मान करें और इंटरनेट पर किसी की आलोचना नहीं करना चाहिए और यही हमें बच्चों को भी सिखाना चाहिए।

व्यक्तिगत जानकारी छुपाना

हमें बच्चों को सिखाना चाहिए कि वे व्यक्तिगत जानकारी जैसे कि घर का पता, फोन नंबर, सचि, पासवर्ड्स दूसरों को नहीं दें। अनजाने लोगों को फोटोग्राफ्स नहीं भेजें और उन्हें सिखाया जाए कि उन्हें अनजाने लोगों से व्यक्तिगत जानकारी छुपाना चाहिए, क्योंकि उसका दुरुपयोग किया जा सकता है और बिना उनकी जानकारी के उसे अन्य लोगों के साथ साझा किया जा सकता है।

डाउनलोडिंग करते समय

इंटरनेट का उपयोग संगीत, वीडियो सुनने के लिए व गेम्स सीखने के लिए किया जाता है और यह सीखने के लिए कि गेम्स कैसे खेलना चाहिए। हमें उनका इस्तेमाल डाऊनलोडिंग के लिए या कापीराईट से युक्त सामग्री को साझा करने के लिए नहीं करना चाहिए। यही हमें बच्चों को सिखाना चाहिए और उन्हें भी कापीराईट्स का महत्व व कापीराईट के मुद्दों के संबंध में जागरूक रहना चाहिए।

पर्यवेक्षण

आपको यह मालूम होना चाहिए कि बच्चे इंटरनेट पर क्या करते हैं और वे कौनसी साईट्स इंटरनेट पर देखते हैं और जाँच करना चाहिए कि वे किनके साथ कम्युनिकेट करते हैं। आप उन पर आने वाले खतरों के प्रति सावधान रहें और अनुपयुक्त साईट्स पर ब्राउसिंग के लिए रोकें। जब बच्चा इंटरनेट का उपयोग कर रहा हो तब माता-पिता के उसमें शामिल होने से बच्चों को कंप्यूटर आचार-नीति के अनुपालन में सहायता मिलती है।

बच्चों को इंटरनेट का उपयोग करने हेतु प्रोत्साहित करें

हमें बच्चों, छात्रों व अन्य लोगों को इंटरनेट से ज्ञान प्राप्ति के लिए तथा उसके बुद्धिमत्तापूर्ण उपयोग हेतु प्रोत्साहित करना चाहिए। इंटरनेट एक बड़ा साधन है, जिसके द्वारा कोई सूचनाएँ एकत्रित कर सकता है और जिसका उपयोग शिक्षण में किया जा सकता है।

इंटरनेट पर पहुँच

प्रत्येक के लिए इंटरनेट एक समय-उत्कृष्ट साधन है, जो पाठ्यक्रम में वृद्धि की संभावनाओं को बढ़ाता है। शिक्षण निर्भर होता है संबंधित व विश्वसनीय जानकारियों को तुरंत व आसानी से प्राप्त करने व साथ ही उन जानकारियों के चयन, उन्हें समझने व आकलन करने की योग्यता पर। इंटरनेट पर जानकारियों को ढूँढने से इन कुशलताओं को विकसित करने में मदद मिलती है। कक्षा के अभ्यास और घर के लिए दिए जानेवाले कार्य में, जहाँ छात्रों को वेबसाईट विषय की तुलना करने की जरूरत होती है, वहाँ वे चेतावनी देने, छात्रों को विभिन्न प्रकार के श्रोतागणों हेतु लिखने, विशेष विषय के उद्देश्य, परिशुद्धता व विश्वसनीयता को पहचानने व उसका आकलन करने की आवश्यकता के संबंध में आदर्श होते हैं। चूँकि कई वेबसाईट्स, मुद्दों के संबंध में कोई विशेष दृष्टिकोण अपना लेती है, अतः दृष्टिकोणों से तथ्य में अंतर विकसित करने की कुशलता में एवं आत्मनिष्ठा व वस्तुनिष्ठा की तलाश करने में इंटरनेट एक उपयोगी साधन है ।

साइबर आचार-नीति

इंटरनेट या साइबर प्रौद्योगिकी पर नैतिक, वैधानिक, व सामाजिक मुद्दों हेतु व्यवहार की संहिता ही साइबर आचार-नीति है। साइबर आचार-नीति में उन कानूनों का अनुपालन भी शामिल है जो ऑनलाईन व्यवहार पर लागू होते हैं। साइबर आचार-नीति का अभ्यास करने से किसी को इंटरनेट का सुरक्षित व मनोरंजनदायक अनुभव हो सकता है। साइबर-बुलीइंग सूचना प्रौद्योगिकी का वह बेजा इस्तेमाल है, जिसके द्वारा कोई किसी को जान-बूझकर बार-बार नुकसान या पीड़ा पहुँचा सकता है। इन तकनीकों के बढ़ते उपयोग के कारण साइबर-बुलीइंग सामान्य होती जा रही है, विशेषकर किशोरों में।

साइबर प्रौद्योगिकी व्यक्तिगत कंप्यूटर्स से कंप्यूटिंग व कम्युनिकेशन की वह विस्तृत श्रेणी है जिसे साधनों व संचार प्रौद्योगिकी से संबद्ध कर दिया गया हो। साइबर प्रौद्योगिकी बताती है कि आचार-नीति के मुद्दों का अध्ययन, कंप्यूटिंग मशीन्स तक या कंप्यूटिंग व्यवसायिकों तक सीमित रहता है। यह इंटरनेट आचार-नीति से कहीं अधिक परिशुद्ध है, जो केवल आचार-नीति के उन मुद्दों तक ही सीमित है, जो कंप्यूटर नेटवर्क्स को प्रभावित करती है।

साइबर सेफ्टी

इंटरनेट व अन्य संबद्ध वातावरण में सुरक्षित व जवाबदेह तरीके से कार्य करने की योग्यता को साइबर सेफ्टी संबोधित करती है। ये व्यवहार निजी जानकारी व प्रतिष्ठा को संरक्षित करते हैं, जिनमें वे सुरक्षित अभ्यास भी सम्मिलित हैं, जिससे बनिस्बत इसके कि हार्डवेयर/सॉफ्टवेयर आधारित समस्याओं को कम करें, व्यवहार पर आधारित खतरे को कम-से-कम कर सकें।

साइबर सिक्योरिटी

साइबर सेफ्टी जहाँ सुरक्षित व जवाबदेह तरीके से कार्य करने पर केन्द्रित है, वहीं साइबर सिक्योरिटी प्रौद्योगिकी के माध्यम से प्राप्त अनाधिकृत पहुँच के द्वारा व्यक्तिगत जानकारी व प्रौद्योगिकी स्त्रोतों के भौतिक संरक्षण ह्रार्डवेयर वसॉफ्टवेयर दोनों हीट को समाहित करती है।

आचार-नीति के लिए सुरक्षा हेतु उपाय

चार प्रभावी तरीकों से ऑनलाईन काम करने की सही स्थिति सुनिश्चित की जा सकती है:

- प्रौद्योगिकी की बुनियादी समझ रखना।
- अपने बच्चों के साथ ऑनलाईन सहभागिता करना।
- जानकारी लें कि शाला में ही कंप्यूटर के उपयोग के लिए कौन से मानक स्थापित किए गए हैं।
- अपने बच्चे के साथ नियमों का एक सेट निर्मित करें, जो आचार-नीति व सुरक्षा दोनों से ही संबंधित हो।

सूचना प्रौद्योगिकी के महत्व के अनुसार व छात्रों व संकाय के द्वारा इस प्रौद्योगिकी के अनैतिक उपयोग की संभावनाओं को देखते हुए, शालाओं/ महाविद्यालयों को यह सुनिश्चित करना चाहिए कि उनके पास छात्रों व स्टॉफ के द्वारा सूचना प्रौद्योगिकी के उपयोग व प्रबंधन से संबंधित नीतियाँ हैं।

आचार-नीति की कई संहिताएँ जो प्रौद्योगिकी के उपयोग से अस्तित्व में हैं और कई शालाओं ने "उपयोगकर्त्ता को स्वीकार्य नीतियाँ" को अपनाया है, जिनमें सूचना प्रौद्योगिकी के उचित उपयोग के संबंध में नियम भी सम्मिलित हैं। अध्यापक, छात्र व माता-पिता को इन आचार-नीति की संहिताओं को जानना व समझना चाहिए।

बच्चों के लिए प्रौद्योगिकी के आसपास जो मुख्य मुद्दे हैं, उसके लिए आचार-नीति को तीन क्षेत्रों में वर्गीकृत किया जा सकता है: निजता, संपत्ति व समुचित उपयोग। शाला से संबंधित मामले इन प्रत्येक क्षेत्र में पाए जा सकते हैं।

अध्यापकों को चाहिए कि उन लक्ष्यों व गतिविधियों की सीख विकसित करें, जो विशेष रूप से प्रौद्योगिकी आचार-नीति को संबोधित करती हो। समुचित उपयोग के बारे में तब ही सिखाने की जरूरत है, जब कंप्यूटर के अन्य कौशल सिखाएँ जा रहे हों। आचार-नीति की धारणा के बारे में छात्रों की समझ का आकलन किया जाना चाहिए। प्रौद्योगिकी के उपयोग के विशेषाधिकार, मुख्य रूप से वे जिनमें ऑनलाईन उपयोग शामिल है, वे छात्रों को तब तक नहीं देना चाहिए, जब तक कि आकलन यह प्रदर्शित न कर दें कि छात्र आचार-नीति के मानकों व शाला की नीतियों को जानता है और वह उन्हें अमल में ला सकता है।

शालाओं में "उपयोगकर्त्ता को स्वीकार्य नीति" होना चाहिए। "उपयोगकर्त्ता को स्वीकार्य नीति" इंटरनेट व अन्य सूचना प्रौद्योगिकी तथा नेटवर्क्स के शाला में उपयोग के बारे में बताती है। इन नीतियों के नियम अक्सर स्टॉफ व छात्रों दोनों पर ही लागू होते हैं। शाला में प्रत्येक को यहाँ तक कि माता-पिता को भी ये नीतियाँ जानना व समझना चाहिए।

उपयोगकर्त्ता को स्वीकार्य नीति में हो सकते हैं

- सेवा का इस्तेमाल किसी कानून के उल्लंघन के भाग के रूप में नहीं करना।
- किसी कंप्यूटर नेटवर्क या उपयोगकर्त्ता की सुरक्षा को भेदने का प्रयास नहीं करना।
- बिना पूर्वानुमति के वाणिज्यिक संदेश शाला के समूहों के लिए पोस्ट नहीं करना।
- अनावश्यक किसी जंक ई-मेल या स्पाम भेजने की कोशिश नहीं करना।
- अत्यधिक मात्रा में ई-मेल भेजने वाली मेल बॉम्ब साईट का इस्तेमाल नहीं करना जिससे ट्रॉफिक अधिक होने से सर्वर प्रभावित हो सकता है।
- कंप्यूटर प्रौद्योगिकी का इस्तेमाल दूसरे उपयोगकर्त्ता को व्यवधान पहुँचाने के लिए न करें
- जानकारियाँ चुराने के लिए कंप्यूटर प्रौद्योगिकी का इस्तेमाल नहीं करें

साइबर-बुलीइंग

साइबर-बुलीइंग तब होती है, जब इंटरनेट व संबंधित प्रौद्योगिकी का उपयोग योजनाबद्ध तरीके से, शत्रुतापूर्वक लगातार अन्य लोगों को धमकाने के लिए दिये गये प्रकारों से की जाए है:

- टेक्स्ट संदेश या इमेजेस
- व्यक्तिगत टिप्पणियाँ ऑनलाईन पोस्ट करना
- नफ़रतभरी भाषा
- दूसरे को नापसंद बनाने का प्रयास करना और उन्हें विभिन्न फोरम में उपहास का विषय बनाने की गतिविधियों में शामिल होना।
- झूठे विवरण पोस्ट करके अन्य व्यक्तियों को अपमानित या परेशान करना।

साइबर-बुलीइंग के द्वारा विभिन्न वेबसाईट्स पर पीड़ित की व्यक्तिगत जानकारी झ्उदाहरणार्थ वास्तविक नाम, पता या कार्यस्थल/शालाट भी उजागर हो सकती है। पीड़ित की पहचान को गलत दिखाने वाले मामले अब सामान्य हैं। उनके नामों का उपयोग व्यक्ति की मानहानि करने या उपहास का विषय बनाने के लिए आपत्तिजनक सामग्री के प्रकाशन में किया जा सकता है।

भारतीय क़ानून के अंतर्गत साइबर-बुलीइंग सूचना प्रौद्योगिकी अधिनियम की धारा ६६ ए में शामिल है। इस धारा का शीर्षक संचार सेवा के द्वारा आक्रामक संदेश भेजने के लिए सजा, आदि है। इस धारा में ३ वर्ष तक की कैद व जुर्माने का प्रावधान है। धारा ६६ ए ई-मेल या एसएमएस द्वारा दिए गए विभिन्न प्रकृति के संदेश भेजने की स्थिति में दंडित करती है:

- मोटे तौर पर आक्रामक या खतरनाक प्रकृति की सूचना
- झुंझलाहट, असुविधा, खतरा, बाधा, अपमान, चोट, आपराधिक धमकी, शत्रुता, घृणा या बैर करने के उद्देश्य जैसी दी गई विभिन्न स्थितियों में दी गई झूठी सूचना।

यह धारा निम्न उद्देश्यों के लिए झ्इनमें टेक्स्ट, इमेजेस, आडियो, वीडियो के अटेचमेंट्स व साथ ही संदेश के साथ ट्रांसमिट किए गए अतिरिक्त इलेक्ट्रोनिक रिकार्ड भी, सम्मिलित हैंट ई-मेल्स भेजे जाने पर भी दंडित करती है:

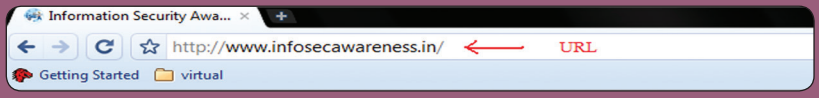
- झुंझलाहट उत्पन्न करने, या
- असुविधा उत्पन्न करने, या
- संदेशों के स्त्रोत के बारे में धोखा या गलत जानकारी देने के लिए ।

ब्राउज़र सुरक्षा

वेब ब्राउज़र क्या है ?

वेब ब्राउज़र का उपयोग वर्ल्ड वाइड वेब पर जानकारी और संसाधनों के बारे में जानने में किया जाता है। यह वेब पृष्ठ का पता लगाने और प्रदर्शित करने में इस्तेमाल की जाने वाली एक सॉफ्टवेयर एप्लीकेशन है। वेब ब्राउज़र का मुख्य उद्देश्य उपयोगकर्ता के लिए सूचना संसाधन उपलब्ध कराना है। इसकी पहचान एक यूनीवर्सल रिसोर्स आइडेन्टिफाइअर/ लोकेटर (छडक्ष / छडख़) द्वारा होती है और जो एक वेब पेज, छवि, वीडियो या सामग्री के एक भाग के रूप में हो सकती है। वेब ब्राउज़र का उपयोग इस्तेमाल न केवल पर्सनल कंप्यूटर, लैपटॉप के लिए होता है, बल्कि मोबाइल फोन में जानकारी के लिए भी होता है।

यूनिफ़ॉर्म रिसोर्स लोकेटर (यूआरएल)



यूआरएल इस तरह दिखता है http://www.infosecawareness.in

प्रत्येक यूआरएल नीचे दिखाये गये विभिन्न वर्गों में बांटा गया है:

http: // संक्षेप में, HTTP का मतलब हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल है और फाइल एक वेब पेज है और हर बार http टाइप करने की जरूरत नहीं है, यह स्वचालित रूप से ब्राउज़र से आ जाता है।

www– notation used for World Wide Web
infosecawareness –वेब साइट का नाम
.in-यह एक डोमेन नाम है, जो मूल रूप से एक देश का नाम है।

अन्य डोमेन नाम .ड़दृष्ट (वाणिज्यिक संगठन), .in (नेटवर्क डोमेन) आदि हैं
(संगठन पता और स्थान डोमेन नाम के रूप में जाना जाता है)।

co.in - सफिक्स या वैश्विक डोमेन नाम संगठन के पते के प्रकार और सफिक्स बी.ह मूल देश के साथ भारत में एक कंपनी को इंगित करता है।

सामान्यता, एक वेब ब्राउज़र वेब सर्वर से कनेक्ट होकर जानकारी प्रदान करता है। प्रत्येक वेब सर्वर का आईपी पता होता है, और_ के उपयोग से वेब सर्वर से जुड़ने पर यह वर्ल्ड वाइड वेब पर वेब पेज दस्तावेज़ बनाने वाली हाइपरटेक्स्ट मार्क अप भाषा (एचटीएमएल) पढ़ता है और वेब ब्राउज़र में दस्तावेज़ प्रदर्शित होते हैं।
संक्षेप में, एक ब्राउज़र एक एप्लीकेशन है जो और वर्ल्ड वाइड वेब पर सभी जानकारी के साथ एक दूसरे को देखने और बातचीत का एक तरीका प्रदान करता है।

वेब ब्राउज़र के प्रकार:

ब्राउज़र वेब विभिन्न सुविधाओं के साथ विभिन्न प्रकार में उपलब्ध हैं।

कुछ लोकप्रिय वेब ब्राउज़र हैं:

- इंटरनेट एक्स्प्लोरर:
  माइक्रोसॉफ्ट इंटरनेट एक्सप्लोरर संक्षिप्त रूप में IE से जाना जाता है। यह सभी विंडोज कंप्यूटर पर पहले से ही इंस्ट ाल होता है। यह सबसे लोकप्रिय वेब ब्राउज़र में से एक है और IE का 11 नया संस्करण इंटरनेट पर उपलब्ध है। यह निम्नलिखित के साथ इंस्टाल किया जा सकता है- विंडोज ऑपरेटिंग सिस्टम जैसे विंडोज 7, विंडोज 8, विंडोज विस्टा और विंडोज सर्वर।
- मोज़िला फ़ायरफ़ॉक्स:
  यह मोज़िला कॉर्पोरेशन द्वारा विकसित एक निःशुल्क ओपन सोर्स वेब ब्राउज़र है। यह स्थिर और सुरक्षित, सुरक्षा उल्लंघन का कम खतरा, माइक्रोसॉफ्ट इंटरनेट एक्सप्लोरर की तुलना में वायरस और मैलवेयर से कम प्रभावित माना जाता है। यह ब्राउज़र विंडोज, लिनक्स और एप्पल मैक ऑपरेटिंग सिस्टम जैसे विभिन्न ऑपरेटिंग सिस्टम में इस्तेमाल किया जा सकता है।
- गूगल क्रोम:
  यह वेब ब्राउज़र विंडोज ऑपरेटिंग सिस्टम के लिए बनाया गया है। यह ब्राउज़र विंडोज विस्टा , विंडोज 7 और विंडोज 8 पर काम करता है। क्रोम ओएस एक्स या लिनक्स ऑपरेटिंग सिस्टम के लिए डाउनलोड और इंस्टाल किया जा सकता है।
- सफारी:
  यह एप्पल कॉर्पोरेशन द्वारा विकसित वेब ब्राउज़र है। यह मैक ओएस एक्स का एक डिफ़ॉल्ट वेब ब्राउज़र है। यह भी प्रकार के विंडोज के लिए भी काम करता है।

हमेशा नवीनतम अपडेटेड
ब्राउज़र का उपयोग करें।

क्यों अपना वेब ब्राउज़र सुरक्षित कर ?

आज, इंटरनेट एक्सप्लोरर, मोजिला फायरफॉक्स, गूगल क्रोम और एप्पल सफारी जैसे वेब ब्राउज़र लगभग सभी कंप्यूटरों में इंस्टाल किये जा रहे हैं। और यह नोटिस करना बहुत आसान है कि ऑनलाइन अपराधियों द्वारा वेब ब्राउज़र की कमजोरियों और जोखिम का फायदा उठाने की कोशिश बढ़ते खतरे का संकेत है। इसलिए वेब ब्राउज़र बहुत ज्यादा उपयोग होने से उन्हें सुरक्षित कन्फिग्यर बहुत महत्वपूर्ण है। अक्सर वेब ब्राउज़र ऑपरेटिंग सिस्टम के साथ डिफ़ॉल्ट सेटिं ग में कन्फिग्यर नहीं होने से सुरक्षित नहीं थे।

ऑनलाइसन सुरक्षा सुनिश्चित करने का प्रयास ब्राउज़र सुरक्षा की दिशा में पहला कदम है। वेब ब्राउज़र द्वारा मेलिशियस वेबसाइट एक्सेस करने ब्राउज़र की कमजोरियों के फायदे से इससे जुड़े खतरों की संख्या में वृद्धि हुई है। कई कारकों के साथ दिये गये निम्नलिखित कारणों से स्थिति खराब हुई:

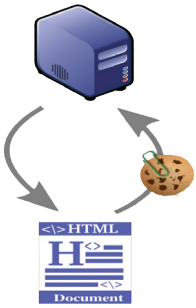
- कई कंप्यूटर उपयोगकर्ताओं को वेब लिंक पर क्लिक करने के संबंध में जागरूक नहीं हैं।
- सॉफ्टवेयर और अन्य सेवा प्रदाता के सॉफ्टवेयर पैकेज इंस्टाल करने जैसी दोनों स्थितियों से जोखिम बढ़ गया है।
- कई वेबसाइट में यूजर्स इनेबल सुविधाओं की जरूरतों की कमी अथवा ज्यादा सॉफ्टवेयर इंस्टाल होने से सिक्योरिटी अपडेट जैसी सुविधाएं अन्य सेवा प्रदाता सॉफ्टवेयर में नहीं होने से कंप्यूटरों पर अतिरिक्त जोखिम बढ़ गया है।
- कई उपयोगकर्ता नहीं जानते हैं कि अपने वेब ब्राफज़र को सुरक्षित कन्फिग्यर कैसे करना है।

वेब ब्राउज़र जोखिम और केस अध्ययन:

विभिन्न वेब पृष्ठ को एक्सेस में ब्राउज़र का उपयोग एक पूर्ण ऑनलाइन अनुभव है। डिफ़ॉल्ट रूप से, ब्राउज़र ऑनलाइन सेशन में सुधार करने की विशेषताओं के साथ इनेबल होता है लेकिन साथ ही ये सब विकल्प हमारे ऑपरेटिंग सिस्टम

और डेटाबेस के लिए एक बड़ा सुरक्षा जोखिम होते हैं। ऑनलाइन क्रिमिनल हमारे ब्राउज़र में उपलब्ध कमजोरियों का उपयोग करके और इसकी अतिरिक्त सुविधाओं से ऑपरेटिंग सिस्टम का नियंत्रण, निजी डेटा प्राप्त करनें,महत्वपूर्ण फ़ाइल प्रणाली को नुकसान पहुंचाने और सॉफ्टवेयर चोरी और डेटा इंस्टाल जैसी गतिविधियों को अंजाम देते हैं।
इन सुविधाओं में से कुछ ब्राउज़र की कार्यक्षमता के लिए महत्वपूर्ण हैं और उपयोगकर्ता को उनका महत्व समझना चाहिए और इन्हें ब्राउज़र की सुरक्षा के लिए सक्रिय या निष्क्रिय कर देना चाहिए।

ब्राउज़र कुकीज़:



कुकीज वेबसाइट उपयोगकर्ता की पहचान में उपयोगी है। ब्राउज़र द्वारा वेबसाइट एक्सेस करने प ब्राउज़र को भेजा गया टैक्स्ट का एक छोटा भाग कुकीज है । यह ब्राउजर द्वारा विजिट की गई वेबसाइट की ट्रैकिंग संबंधी जानकारी और वेबसाइट की भाषा और अन्य अनुकूलित सेटिंग्स संबंधी सूचनाओं को समाहित करती है। ब्राउजर इस डेटा को स्टोर करता है और इन वेबसाइट की विशेषताओं को एक्सेस करने में इस्तेमाल करता है अथवा अगली बार उन्हीं वेबसाइट की एक्सेस को ज्यादा पर्सनलाइज्ड(अपने अनुकूल) करता है। जब एक वेबसाइट प्रमाणीकरण के लिए कुकीज का इस्तेमाल करती है तब अटैकर उन्हीं वेबसाइट कुकीज का उपयोग अनधिकृत एक्सेस करने में कर सकते हैं।

- केस 1 :

  शानिया एक फिल्म वेबसाइट पर जाती है और हास्य में रुचि प्रदर्शित करती है। वेबसाइट द्वारा उसकी पसंद को सेव करते हुए कुकीज़ भेजी जाती है औ जब वह उसी वेबसाइट पर अगली बार जाती है तो वह, उस वेबसाइट पर हास्य संबंधित सामग्री प्रदर्शित हुआ देखती है ।

- केस 2:

  उपयोगकर्ता एक वेब साइट पर लॉग इन करके अपना यूजरनेम एवं पासवर्ड लॉगइन पेज पर देते हैं एवं यदि वे प्रमाणीकृत होते हैं तो कुकीज सेव होकर वेबसाइट को यूजर के बारे में लॉग्ड इन और साइट में नेवीगेट होने की जानकारी दे देती है। यह अनुमति लॉग्ड इन यूजर को उपलब्ध कार्यात्मकता को एक्सेस करने की सुविधा देती है संभवता यह उस समय कुकीज का प्राथमिक उपयोग होता है।

- केस 3:

  ऑनलाइन शॉपिंग कार्ट भी कुकीज़ का उपयोग करते हैं। उदाहरण के लिए जब आप फिल्म शॉपिंग साइट पर डीवीडी ब्राउज़ करते हैं तो आप बिना लॉगइन किये अपने शॉपिंग कार्ट में उन्हें जोड़ सकते हैं। आपका शापिंग कार्ट डीवीडी नहीं भूलता है चाहे आप उस शापिंग वेबसाइट के अलग-अलग पेज पर भी जाएं,क्योंकि वे उस सूचना को कुकीज के माध्यम से सेव कर लेते हैं। वेब पर आपके सर्फ किये एड को और आपकी रुचि को याद कराने में भी कुकीज़ का ऑनलाइन विज्ञापन में उपयोग किया जा सकता

पॉप अप:

पॉपअप ब्राउज़र पर स्वचालित रूप से खुलने वाली एक छोटी सी विंडो पैन है। सामान्यता उनके द्वारा दिखाये गये विज्ञापन वैध कंपनी के हो सकते हैं। लेकिन ये स्कैम या खतरनाक सॉफ्टवेयर भी हो सकते हैं। ये कुछ निर्धारित वेबसाइट को

खोलने पर प्रदर्शित होते हैं। वेबसाइट विजिट के दौरान खुलने वाले पॉपअप विज्ञापन आपको फंसाकर व्यक्तिगत या वित्तीय जानकारी को जानने के लिए डिजाइन किये गये एक फ़िशिंग स्कैम हैं। पॉपअप पॉपअप विंडो के बटन पर क्लिक करने के लिए गुमराह करते हैं। लेकिन कई बार विज्ञापनदाता एक कैंसिल या क्लोज ऑप्शन जैसे लगने वाले पॉपअप विंडो को क्रियेट करते हैं और जब भी ऐसे ऑप्शन के बटन पर क्लिक करते ही आपके सिस्टम पर कमांड बनाने वाले कुछ अनधिकृत अन्य विंडो खुल जाते हैं।

सभी पॉपअप इस तरह के नहीं होते हैं। कुछ वेबसाइट इनका उपयोग कुछ विशेष कार्यों के लिए करती हैं। आपको उस कार्य को पूरा करने के लिए वो विंडोज देखने के लिए मिल सकता है।

- केस 4:

  साराह xyz@music.com.बंस से ऑनलाइन संगीत सुन रहा था, कुछ घंटे के बाद मैंने एक पॉप-अप देखा जो एक क्लिक पर नवीनतम गाने डाउनलोड करने के लिए कह रहा था। मैंने अपने ब्राउज़र के डाउनलोड सेक्शन में दिखने वाले फार्म को भर दिया। एक महीने के बाद अपने केडिट कार्ड बिल को जांचने पर कुछ अनाधिकृत शुल्क दिखा । मैं बहुत परेशान और हैरान था। लगातार गाने डाउनलोड की गई विशेष वेबसाइट के बारे में कहे जाने के बावजूद किसी काम का नहीं था।

स्क्रिप्ट:

स्क्रिप्ट वेबसाइट ज्यादा इंटरैक्टिव बनाने के लिए इस्तेमाल होती है। यह वेब ब्राउज़र में इस्तेमाल सबसे अधिक सामान्य भाग है, जिसका कार्यान्वयन क्लाइंट साइड स्क्रिप्ट को अनुमति देकर यूजर संवाद करने , ब्राउज़र नियंत्रण, असमकालिक संवाद और प्रदर्शित दस्तावेज़ सामग्री में परिवर्तन करने को संभव बनाता है। जावास्क्रिप्ट मानक में कुछ ऐसे विनिर्देश है जो स्थानीय फ़ाइलों को एक्सेस करने वाली कुछ सुविधाओं को सीमित कर देती है।

ऐसी स्क्रिप्ट में मलिशस कोड का समावेश से वेब ब्राउजर पर कंट्रोल करके फ़ाइल सिस्टम को एक्सेस करने की अनुमति देने में किया जा सकता है। इससे ब्राउज़र की कमजोरियां एक्सेस होने से सिस्टम नुकसान देने का कारण बन सकता है।

- प्रकरण 5:

  चिंटू नियमित रूप से स्कूल के काम, खेल खेलने में और संगीत सुनने में इंटरनेट का उपयोग करता है। जब वह खेल रहा होता था, उसने लेडी गागा के मरने की खबर का पॉपअप देखा। जैसे ही वह बीबीसी साइट पर क्लिक करता है एक संवाद सर्वेक्षण पॉपअप आता है और यूजर से उस सर्वेक्षण फार्म को भरने के लिए कहा जाता है। संबंधित सर्वेक्षण लिखा गया था यदि 'आप लेडी गागा पर सच्चे प्रशंसक हैं' तो लाइक बटन पर क्लिक करें। जैसे ही सर्वेक्षण पूरा हुआ वह मेरे अकाउंट के होम पेज पर वापिस आया और वही लिंक मेरे जानकार परिवार वालों और दोस्तों के लिए समाचार के रूप में पोस्ट कर दी गई ।

प्लग-इन्स:

प्लगइन्स वेब ब्राउज़र और नेटस्केप वेब ब्राउज़र में उपयोग में आने वाली ईन-बिल्ट एप्लीकेशन हैं जिनका विकास शछ मानकों के अंतर्गत प्लग-इन विकसित करने के लिए किया गया था। बाद में इन मानकों का उपयोग कई वेब ब्राउज़र द्वारा किया गया। प्लग-इन छ्बौपीठ कंट्रोल के समान ही हैं, लेकिन जिन्हें वेब ब्राउज़र से अलग नहीं चलाया जा सकता है। एडोब फ्लैश एक एप्लीकेशन का उदाहरण है जो वेब ब्राउज़र में प्लग-इन के रूप में उपलब्ध है।

- केस 6:

उदाहरण के लिए, यूजर वेबपेज पर उपलब्ध वीडियो या किसी इंटरैक्टिव गेम को देखने के लिए एडोब फ्लैश प्लेयर जैसे प्लगइन को डाउनलोड और और इंस्टाल कर सकते हैं। लेकिन प्लगइन की लोगर के साथ इंस्टाल हो सकता है जो ब्राउज़र में उपयोगकर्ता की टाइपिंग के सभी प्रमुख स्ट्रोक को कैप्चर करके अटैकर को भेज सकता है।

ब्राउज़र एक्सटेंशन आपके ब्राउजर में नये फीचर वैसे ही जोड़ते है जैसे आपके ब्राउज़र में कस्टमाइजिंग करने में कुछ महत्वपूर्ण फीचर जोड़े जाते हैं। अन्य शब्दों में इसे ब्राउज़र में नये सुपरपावर जोड़ना कह सकते हैं। उदाहरण के लिए,आप अपने ब्राउजर में एक करेंसी कन्वर्टर एक्सटेंशन इंस्टाल कर सकते हैं जो एड्रेस बार के पास में एक नया की के रूप में दिखता है। बटन पर क्लिक करें और यह वर्तमान वेबपेज पर आपके द्वारा दी गई किसी भी मुद्रा को सभी कीमतों में बदल देता है।

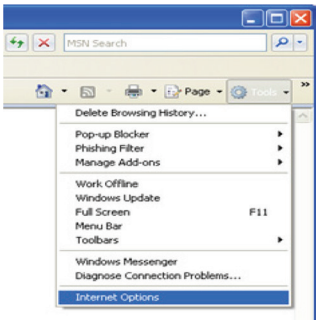
ब्राउज़र और अधिक कोड जोड़ने को, सुरक्षा बिंदुओं जोड़ा जाना चाहिये क्योंकि यह अटैकर को ब्राउज़र का फायदा उठाने की और अधिक संभावना देता है। क्योंकि कोड कभीकभी छिपा होता है, और साथ ही एक्सटेंशन ब्राउज़र कैश के लिए जिम्मेदार था।

अपना वेब ब्राउज़र सुरक्षित कैसे करें?

डिफ़ॉल्ट रूप से, वेब ब्राउज़र एक ऑपरेटिंग सिस्टम के साथ आता है और यह डिफ़ॉल्ट कंफिग्यर के साथ सेट-अप होता है जिसमें सभी सुरक्षित सुविधाएं सक्रिय नहीं होती हैं। ऐसे असुरक्षित वेब ब्राउज़र स्पाइवेयर, मैलवेयर, वायरस, वोर्म्स आदि कंप्यूटर में इंस्टाल होने का कारण बनते हैं और घुसपैठिये आपके कंप्यूटर को नियंत्रित कर सकते हैं।

कमजोर वेब ब्राउज़र के दुरुपयोग से सॉफ्टवेयर हमले करने के खतरों में बढ़ोत्तरी हुई है। वेब ब्राउज़र के कुछ कुछ सॉफ्टवेयर जैसे जावा स्क्रिप्ट, एक्टिव एक्स आदि कंप्यूटर प्रणाली में कमजोरियों का कारण हो सकते हैं। इसलिए यह महत्वपूर्ण है कि कंप्यूटर में जोखिम को कम करने के लिए आपके वेब ब्राउज़र में सुरक्षा सुविधाएं सक्रिय की जाएं ।

सुरक्षा क्षेत्र



इंटरनेट वेब ब्राउज़र में सुरक्षा क्षेत्र आपके ब्राउज़र को सुरक्षित बनाते हैं और इंटरनेट पर लोगों, कंपनियों पर भरोसा करने का अवसर देते हैं। आपके कंप्यूटर में किस साइट को एप्लीकेशन रन करने के लिये हस्क्रिप्ट,एड-ऑन, प्लग-इन इंस्टाल करने के लिए ऐड करना है इसके निर्णय में सहायता करती है।

सुरक्षा क्षेत्र में प्रतिबंधित साइट के अंतर्गत वेब साइट के पता जोड़ने जैसी अन्य सुविधाएं भी शामिल हैं यह सुविधा इंटरनेट एक्सप्लोरर में उपलब्ध है और अविश्वसनीय साइट या हमलावर साइटों को इस ब्लॉक करती है। यह सुविधा क्रुद्धड्ढढदृन में उपलब्ध है; और यह विभिन्न वेब ब्राउज़र के बदल सकती है।

विश्वसनीय साइट

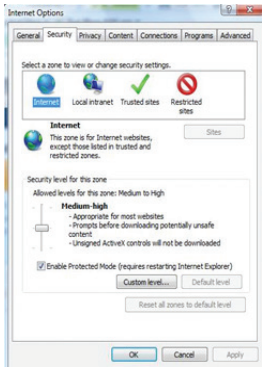
इंटरनेट विभिन्न वेबसाइटों के माध्यम से लोगों के विभिन्न प्रकारों की सभी प्रकार की विषय सामग्री के साथ लोगों का एक नेटवर्क है। सामान्यता आप अपने चारों ओर हर किसी पर भरोसा क्यों नहीं करते हैं?और आप सभी को अपनी

अनुमोदन के बिना अपने कंप्यूटर पर आने की क्यों अनुमति देते हैं? विश्वसनीय साइट की सुविधा का उपयोग से वेब ब्राउज़र आपका भरोसेमंद के बारे में फैसला करने में मदद करेगा।

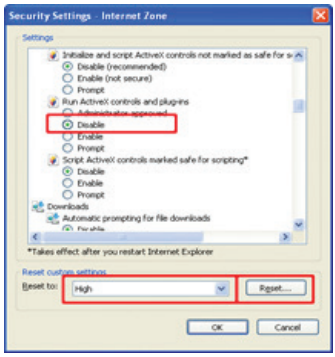
इंटरनेट एक्स्प्लोरर

इंटरनेट एक्सप्लोरर की कुछ विशेषताएं और कुछ सेटिंग निम्नलिखित हैं-

- इंटरनेट एक्सप्लोरर की सेटिंग में बदलाव के लिए, टूल चुनें। इंटरनेट एक्सप्लोरर की सेटिंग में से टूल मैन्यु में इंटरनेट विकल्प का चयन करें और तब सुरक्षा टैब पर क्लिक करें, वर्तमान सुरक्षा सेटिंग्स की जाँच करें और आवश्यकतानुसार सुरक्षा क्षेत्र की सेटिंग में बदलाव करें।

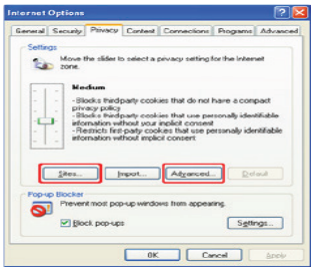


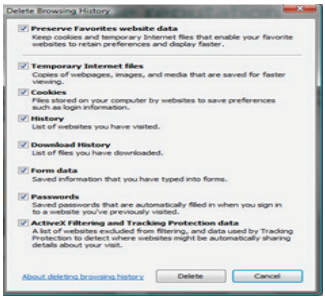
- सुरक्षा लेवल के अंतर्गत सुरक्षा सेटिंग को बदलने के लिए सुरक्षा लेवल को बढ़ाने के लिए स्लाइडर अप ऊपर ले जायें और डाउन के लिए, मध्यम के लिये और नीचे लेवल के लिये
- अधिक सेटिंग्स और नियंत्रण के लिए कस्टम लेवल पर क्लिक करें और फिर विकल्प को चुनें। यदि आप टूल मेनू विकल्प की स्थिति में जरूरी होने पर ब्राउज़िंग इतिहास के विकल्प का चुनाव करें जो सभी कुकीज़, अस्थायी फ़ाइलों, इतिहास, एक्टिव एक्स फिल्टरिंग और फिगर में दिखाई गये सभी विकल्पों को डिलीट कर देता है।
- विश्वसनीय या प्रतिबंधित वेब साइट जोड़ने या निकालने के लिए, साइट्स विकल्प पर क्लिक करें और फिर जोड़ें पर क्लिक करें या रिमूव बटन पर और अपनी साइट सूची चुने गये जोन में रखें।
- गोपनीयता बटन में कुकीज के लिये सेटिंग्स. कुकीज़ आपके कंप्यूटर ब्राउजर में विभिन्न वेबसाइट की टैक्स्ट फाइल्स जो आपको सीधे या परोक्ष रूप अन्य पार्टी की वेबसाइट पर ले जाती हैं।
- एडवांस्ड बटन से और औवरराइड आटोमेटिक कुकीज़ हैडलिंग को चुनें। फिर पहले और तीसरे पक्ष के कुकीज़ का शीघ्र चयन करें। यह हर बार एक साइट द्वारा आपकी मशीन में एक कुकीज की जगह बनाने का प्रयास होगा।
- मेनू से टूल का चयन और स्मार्ट स्क्रीन फिल्टर का चयन करें और स्मार्ट स्क्रीन फिल्टर पर क्लिक कर शुरु करें और बताया गया स्माट स्क्रीन फिल्टर सक्रिय करें, यह विकल्प फ़िशिंग स्कैम और मैलवेयर से



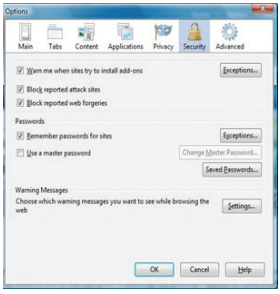
बचने के लिए इस्तेमाल किया जाता है।

- उपकरण मेनू में से प्राइवेट फिल्टरिंग सेटिंग्स का चुनाव करें। इस विकल्प का उपयोग किया जाता है ब्राउज प्राइवेटिली के लिये किया जाता है जो ब्राउज़िंग हिस्ट्री को स्टोर नहीं करता है।
- उपकरण मेनू में ट्रैकिंग प्रोटेक्शन कहलाने वाले विकल्प का चुनाव करें जो आपकी सूचनाओं जैसे कि आपकी वेबसाइट विजिट को ट्रेक करने वाली वेबसाइट संबंधी जानकारी या आपकी व्यक्तिगत जानकारी जैसी सूचनाओं को रोकेगा। यह फीचर हमारे द्वारा इंस्टाल एडऑन के आधार पर कार्य करता है।
- प्रोटक्शन मोड को सक्रिय करें जो सभी वेबसाइट को प्रोटेक्शन मोड में खोलता है।
- एडवांस टैब का चयन करें और जैसा कि आप जी झर्झ 3.0, जी झ्रि 1.0 को सक्रिय करना चाहते हैतो सही विकल्पों का चयन करें।

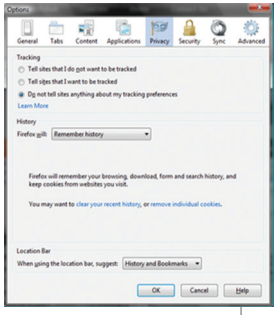




मोज़िला फ़ायरफ़ॉक्स



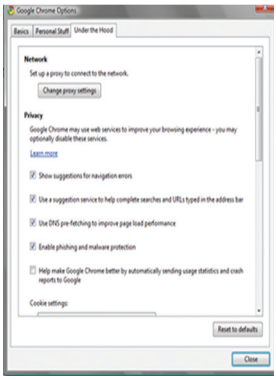
- मोजिला फायरफॉक्स वेब ब्राउजर की निम्नलिखित विशेषताएं और उनका समायोजन
- फायरफॉक्स कंट्रोल की सुरक्षा सेटिंग्स में एक्जामिनेशन लेवल पर आप फायरफॉक्स को एक साइट दे और अपवाद देना चाहेंगे साइट जिसे तीसरी डिग्री की जरूरत नहीं है। कस्टमाइज सेटिंग के लिए पासवर्ड, कुकीज़, छवियों को लोड करने के लिए और एडऑन इंस्टालिंग के लिए एक पूरी तरह से सशक्त वेब अनुभव जैसा नीचे दिखाया गया
- फायरफॉक्स ब्राउज़र के टूल मेन्यु से विकल्प का चयन और सुरक्षा टैब पर क्लिक करें
- सुरक्षा टैब के तहत वार्न मी जैसे ऑप्शन को सक्रिय करें जब साइट एडऑन इंस्टाल करने और जोड़ने या साइट हटाने की कोशिश करे क्लिक ऑन एक्सैप्शन विकल्प पर क्लिक करें और जोड़ने या आपकी वेबसाइट को हटाने की कोशिश करे।
- टेल मी विकल्प को सक्रिय करें यदि में किसी संदिग्ध हमले की साइट पर विजिट कर रहा हूं।
- टेल मी विकल्प को सक्रिय करें यदि मै द्वारा उपयोग में लाइ जाने वाली साइट



संदिग्ध जालसाजी फ़ायरफ़ॉक्स है और संदिग्ध जालसाजी वेब से एक दिन में फ्रेशनअपडेट 48 बार हो जाता है। इसलिए यदि आप एक धोखाधड़ी साइट पर जाते हैं जो कि खुद को सही साइट होने का दिखावा करती है तो आप अपने ब्राउज़र द्वारा आने वाले मैसेज पर भरोसा करें और जो आपको रोकेगा।

- वेबसाइट पर रिमेम्बर्ड पासवर्ड का विकल्प डिसेबल करें। फ़ायरफॉक्स आपके सर्फिंग अनुभव विशेषता को इंटीग्रेड करता है। पॉपअप में दखल दिये बिना रिमेम्बर साइट पासवर्ड विकल्प का चुनाव करें।
- उन्नत टैब का चयन करें और सुरक्षित डाटा हस्तांतरण और एसएसएल 3.0 का उपयोग करने के लिए एन्क्रिप्शन टैब को सक्रिय करें।
- अन्य फीचर आटोमेटेड अपडेट्स हैं जो हमें सुरक्षा विषयों को खोज देते हैं और अपडेट फिक्स करते हैं और सर्फिंग को सेफ बनाते हैं और आटोमेटिक नोटिफिकेशन प्राप्त करते हैं या जब तक आप तैयार हों इंतजार करते हैं।
- प्राइवेसी ऑप्शन के अंतर्गत एक और सुविधाट्रैकिंग है यह आपकी ब्राउज़र गतिविधियों पर रोक लगाती है। और हम डू नॉट टेल साइट जैसे विकल्प का चुनाव कर सकते हैं जो हमारे ट्रेकिंग अधिमान्यताओं को ट्रैक नहीं करेगा और ना ही अन्य वेबसाइट की सूचनाओं को शेयर करेगा।

गूगल क्रोम



सेटिंग मेन्यु से इनकोग्निटो विंडो चुनने के बाद एक नया विंडो आता है और इस विंडो आपके द्वारा देखे गये पेज वेब ब्राउजर की हिस्ट्री में या सर्च हिस्ट्री में नहीं प्रदर्शित होंगे और न ही वो कुकीज़ की कोई टैस छोड़ेंगे। आपके द्वारा इनकोग्निटो विंडो बंद करने के बाद आपके डाउनलोड्स और बुकमार्क्स सुरक्षित रहेंगे।

क्रोम में एक नयी विशेषता टास्क मैनेजर के स्वयं के काम की है जो आपको दिखाती है कि प्रत्येक टैब में कितनी मेमोरी और सीपीयू यूसेज हो रहा और प्लगइन उपयोग में लाये जा रहे हैं। गूगल क्रोम का सुरक्षित ब्राउज़िंग चेतावनी प्रदर्शित करता है कि सर्टीफिकेट में सूचीबद्ध वेब पते वेबसाइट के पते से मेल नहीं खाते हैं कि नहीं ।

- गूगल क्रोम में सुरक्षित ब्राउज़िंग करने के लिए निम्नलिखित कदम उठाए हैं।
- सेटिंग्स टैब से विकल्प का चयन करें, यूस अ सजेशन विकल्प को सक्रिय करें जो पूर्ण सर्च को पूरा करने की सेवा है और एड्रेस बार में यूआरएल टाइप करें
- पेज लोडिंग में सुधार के लिये घशझप्रीफेचिंग को सक्रिय करें
- फ़िशिंग और मैलवेयर सुरक्षा सक्रिय करें
- कुकीज़ चयन के अंतर्गत कैसे तीसरे पक्ष की कुकीज़ इस्तेमाल होने से रोकी जा सकती हैविकल्प का चयन करें केवल प्रथमपक्ष की कुकीज सूचना वेबसाइट पर भेजी गई है।
- माइनर ट्वीक इनेबल के अंतर्गत यह विकल्प सक्रिय करने से पासवर्ड सेव नहीं होता है।
- कंप्यूटर वाइड एसएसएल सेटिंग के अंतर्गत एसएसएल २.० विकल्प को सक्रिय करें।

एप्पल सफारी

एप्पल सफारी सुरक्षित वेब ब्राउज़र की निम्नलिखित विशेषताएं हैं

- फ़िशिंग सुरक्षा

  सफारी धोखाधड़ी वाली इंटरनेट साइटों से बचाता है। जब आप एक संदिग्ध साइट पर जाते हैं सफारी आपको उसकी संदिग्ध प्रकृति के बारे में चेतावनी देता है और उसे लोड होने से रोकता है।

- मैलवेयर सुरक्षा

  सफारी मैलवेयर बनाए रखने वाली वेबसाइट पर आपके जाने से पहले इससे पहले पहचान लेता है। सफारी एक खतरनाक पेज की पहचान कर आपको साइट की संदिग्ध प्रकृति के बारे में चेतावनी देता है।

- एंटीवायरस इंटीग्रेशन

  विंडोज अटैचमेंट मॉनिटर के सपोर्ट के लिए धन्यवाद, सफारी फ़ाइल, छवि, एप्लीकेशन, या अन्य आइटम डाउनलोड करने से पहले अपके एंटीवायरस सॉफ्टवेयर को नोटिस कर सूचित करता है। यह एंटीवायरस सॉफ्टवेयर वायरस को प्रत्येक डाउनलोड की वायरस और मॉलवेयर स्कैनिंग के लिए अनुमति देता है।

- सुरक्षित एन्क्रिप्शन

  गुप्तवार्ता को रोकने, जालसाजी, और डिजिटल छेड़छाड़ को रोकने के लिए सफारी एन्क्रिप्शन प्रौद्योगिकी का उपयोग आपके वेब संचार को सुरक्षित करने के लिए करता है। सफारी बहुत नवीनतम सिक्योरिटी मानकों एसएसएल वर्जन २ और ३ सहित, ट्रांसपोर्ट लेयर सिक्योरिटी (र्झि), ४० और १२८ बिटझझर्झा एन्क्रिप्शन और साइन्ड जावा एप्लीकेशन को सपोर्ट करता है।

- आटोमैटिक अपडेट्स

  नवीनतम सिक्योरिटी अपडेट्स त्वरित, आसान से प्राप्त करें। सफारी एप्पल सॉफ्टवेयर अपडेट्स से लाभ लेता है जब आप इंटरनेट पर सफारी के नवीनतम संस्करण को जांचते हैं।

- पॉपअप ब्लाकिंग

  डिफ़ॉल्ट रूप से, सफारी कुशलता से सभी पॉपअंडर विंडो और अन्प्राम्प्टिड पॉपअप को ब्लॉक करता है जिससे आप ध्यान भंग करने वाले विज्ञापन से ब्राउजिंग करते समय बच सकें।

- कुकी ब्लॉकिंग

  कुछ कंपनियां विजिट की जा रही वेबसाइट से जनरेट होने वाली कुकीज़ को ट्रैक करती हैं जिससे वे इकट्ठी की जा सकें और आपकी वेब गतिविधि संबंधी जानकारी को बेचा जा सके। सफारी पहला ब्राउज़र है जो डिफ़ॉल्ट रूप से ट ैकिंग कुकीज को ब्लॉक करता है जिससे आपकी गोपनीयता की बेहतर रक्षा हो। सफारी केवल आपके करेंट डोमेन की कुकीज़ स्वीकार करता है।

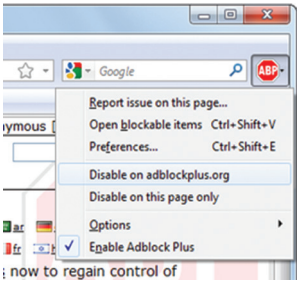
ब्राउज़र सिक्योरिटी एक्सटेंशन

एडब्लॉक प्लस (फ़ायरफ़ॉक्स/क्रोम)

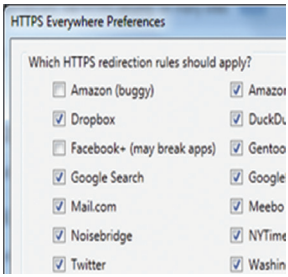
एडब्लॉक, अपने नाम के जैसा होगा, एक वेबसाइट पर विज्ञापन सेवा की कुछ स्क्रिप्ट को ब्लॉक करता है। हम पहले उल्लेख कर चुके हैं, आप मेलीसिशयस एड ब्लॉकलिस्ट का उपयोग अतिरिक्त सिक्योरिटी बेनीफट लेने के लिये ट्वीक एबीपी कर सकते हैं। आप वाइटलिस्ट साइट्स अपनी सहायता के लिये कर सकते हैं परंतु एबीपी भी एड के साथ वाली

अव्यवस्थित वेबलेस की अधिक उपयोगी लाभ प्रदान करता है।

HTTPS झ ऐवरीवियर (फ़ायरफ़ॉक्स)

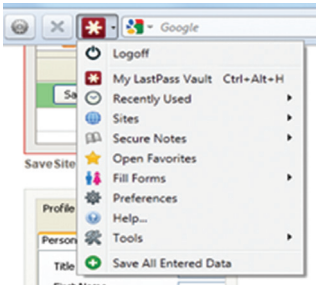


इलेक्ट्रॉनिक स्वतंत्रता फाउंडेशन का झ ऐवरीवियर आपके वेब ब्राउज़र और इससे कनेक्ट किये जाने वाले सर्वर के बीच कनेक्शन को सुरक्षित करने में मदद करेगा। जब भी संभव हो यह आपके कनेक्शन को एनक्रिप्ट करने में सहायता देता है उस स्थिति में भी जब वेबसाइट कि डिफाल्ट सेटिंग अतिरिक्त सुरक्षा प्रदान नहीं करती है।एक अच्छा उदाहरण ट्विटर है। यूजरनेम और पासवर्ड इनपुट बॉक्स इनक्रिप्ट `ड होते हैं लेकिन सर्वर से आनेजाने वाले भेजे गये सभी टैक्स्ट क्लीयर होते हैं। (हाल ही में फेसबुक ने हमेशा झ चालू रखने का एक नया विकल्प जोड़ा है। यहाँ देंखे कैसे करना है।) झ ऐवरीवियर खैीजिरीं जैसे हैकिंग टूल के खिलाफ भी रक्षा करने में मदद करता है।



चिंजाचजज (छनन नचार्क्सिज) लास्टपास (सभी प्लेटफार्म)

चिंजाचजज सिक्योर एक और मार्ग है जिससे हैकर्स आपकी व्यक्तिगत जानकारी तक पहुंच हासिल करने की कोशिश करने के लिए उपयोग कर सकते हैं आपका पासवर्ड। आप जब चिंजाचजज ब्राउज़र प्लगइन का उपयोग करते हैं, तोयह आपका पासवर्ड एन्क्रिप्टेड कर स्टोर करता है आप के लिए और आपको आसानी से एक जटिल और मुश्किल से कैक होने वाला पासवर्ड जनरेट करने की अनुमति देते हैं जो कि एक साइट के लिए यूनिक है। चिंजाचजज में हर ब्राउज़र के लिए प्लगइन उपलब्ध है। यदि आप सिर्फ चिंजाचजज के साथ शुरूकर रहे हैं तो, यहाँ चिंजाचजज के बारे में हमारा परिचय है,हमारी इंटरमेडियेट गाइड, और लेखा परीक्षा के लिए एक गाइड और चिंजाचजज के साथ अपना पासवर्ड अपडेट करने के लिए।

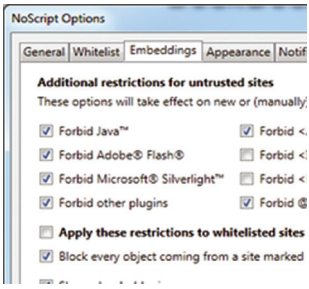


शंझर्बी (खैीर्क्ट) नो स्क्रिप्ट(फ़ायरफ़ॉक्स)

शंझर्बी एक खैीर्क्टप्लगइन है जो केवल एक ही और एक ही काम अच्छे से करता है यह जावास्क्रिप्ट,फ्लैश,क्विकटाइम और आपके ब्राउजर विंडो में लोड होने वाली और स्क्रिप्ट को ब्लॉक करता है। (क्रोम उपयोगकर्ता शंझर्बीज जैसा क्रोम एक्सटेंशन की जांच करना चाहे तो कर सकते हैं) सिक्योरिटी उद्देश्यों के लिए इसका इतनी अच्छी तरह से काम करने का कारण है कि मलिशस वेबसाइट इस स्क्रिप्ट का इस्तेमाल अटैक करने में करके ब्राउजर को कैश करता हैं और आपके कंप्यूटर पर एक्सेस करने के लिये। इन स्क्रिप्ट को ब्लॉक करके आप अपने आप को वेब पर काफी सुरक्षित कर सकते हैं।

हम सभी के मन में इस बात को रखें कि सभी स्क्रिप्ट को ब्लॉकिंग करने का मतलब इंटरनेट में बाधा आना है जैसा कि कई वेबसाइट दी गई हैं गूगल,जीमेल,ट्विटर, लाइफ हैकर और अन्य भी जिनके पेज जावास्क्रिप्ट के आधार पर लोड

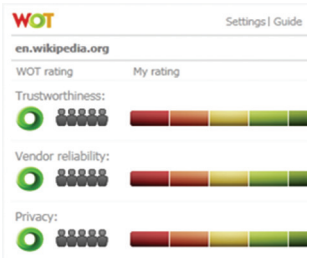
होते हैं। आप विस्तृत में इस डिटेल को सेटिंग्स से मैनेज कर सकते हैं जिससे आप ज्यादा से ज्यादा सिक्योरिटी कम से कम असुविधा से प्राप्त कर सकते हैं।



वेब ऑफ ट्रस्ट(सभी ब्राउज़र)

वेब ऑफ ट्रस्ट एक अन्य प्रकार का प्लगइन है जो कि कुछ ऊपर दिये सभी से कुछ अलग करता है। यह किसी भी हमले को रोकने के बजाय, यह आप जान पाते हैं कि विजिट की जाने वाली वेबसाइट भरोसेमंद है या नहीं। इस तरह यदि आपको लगता है एक वेबसाइट भरोसेमंद है और यहां तक कि यह देखने के बाद, आपको एक चेतावनी मिलती है कि आपको साइट पर अपनी व्यक्तिगत जानकारी प्रस्तुत नहीं करना चाहिए।

वे यूजर रेटिंग पर अपनी साइट को रेट करने के लिए भरोसा करते हैं और मेरे अनुभव में यह बहुत ही सटीक और उपयोगी हो गया है।



टिप्स

- ✔ हमेशा जोखिम से बचने के लिए सुरक्षित वेब ब्राउज़र का उपयोग करें। सुरक्षित ब्राउज़र का उपयोग करना, हम जानकारी और इंटरनेट पर उपलब्ध संसाधनों को एक्सेस कर सकते है और इंटरनेट पर सुरक्षित ब्राउज़िंग कर सकते हैं।
- ✔ अपने पीसी को जोखिमपूर्ण होने से व अन्य मशीन के लिए अटैक हथियार बनने से बचने के लिए वेब ब्राउजर और इंटरनेट यूजर्स को सलाह दी जाती है सुनिश्चित करें आपका ऑपरेटिंग सिस्टम और की सिस्टम कंपोनेन्ट्स जैसे वेब ब्राउज़र पूरी तरह से पेच्ड और अपटूडेट हैं।
- ✔ एक निजी फ़ायरवॉल एंटीवायरस सॉफ्टवेयर के साथ इंस्टाल करें जो नवीनतम वायरस सिग्नेचर के साथ हो ताकि कीलोगर के जैसे मैलवेयर का पता लगाया जा सके।
- ✔ नियमित रूप अपनी क्रिटिकल वेब एप्लीकेशन में वन टाइम पासवर्ड का सपोर्ट नहीं होने पर अक्षर, संख्या और विशेष अक्षर संयोजन की सहायता से पासवर्ड बदलते रहें।
- ✔ किसी भी अनजान वेबसाइट पर विजिट करने से पहले अपने वेब ब्राउज़र में सभी जावास्क्रिप्ट या छबौपीठ सपोट बंद कर दें।
- ✔ अधिकांश विकेता आपको अपनी वेबसाइट से सीधे अपने ब्राउज़र डाउनलोड करने का विकल्प देते हैं। किसी भी फाइल को डाउनलोड करने से पहले साइट प्रामाणिकता की पुष्टि सुनिश्चित करें।
- ✔ अतिरिक्त जोखिम को कम करने के लिए नवीनतम अच्छा सुरक्षा अभ्यासों का पालन करें, जैसे एक निजी फ़ायरवॉल का उपयोग करना, सुरक्षा पैच के साथ नवीनतम ब्राउजर को अपडेट करना और नियमित रूप से पूरे सिस्टम को स्कैन करने के साथ एंटीवायरस सॉफ्टवेयर

फिल्टरिंग सेवाएँ

इंटरनेट पर विषय-सामग्री की फिल्टरिंग को कभी पैतृक-नियंत्रण भी कहते हैं और उनका उपयोग किसी भी आक्रामक वेबसाईट्स की पहुँच को रोकने के लिए होता है़ यह गारंटीड नहीं है, लेकिन यह बहुत मददगार हो सकता है़

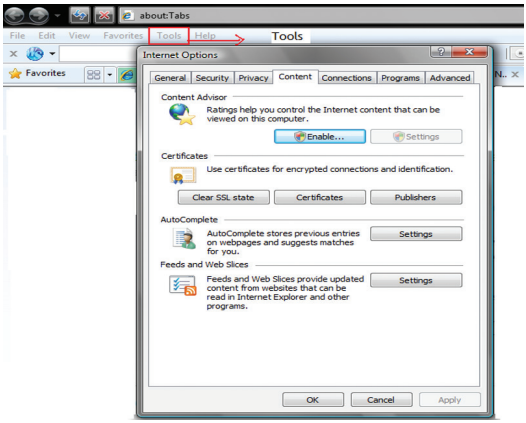
विषय-वस्तु की फिल्टरिंग क्या है?

लोगों को कभी इंटरनेट पर कुछ अनुपयुक्त विषय-वस्तु जैसे कि यौनाचार, हिंसा व सख्त भाषा के बिंब मिलते हैं़ चूँकि इंटरनेट एक मुक्त झोन है, इसलिए कोई भी किसी भी प्रकार की प्रविष्टि करा सकता है और इंटरनेट पर किसी भी प्रकार का प्रभावी प्रतिबंध नहीं है़ इसलिए कई लोग विषय-वस्तु की फिल्टरिंग के साफ्टवेयर का इस्तेमाल करते हैं़ और अपराधयुक्त वेबसाईट्स की रोक के लिए ब्राउसर की सेटिंग सेट करते है़

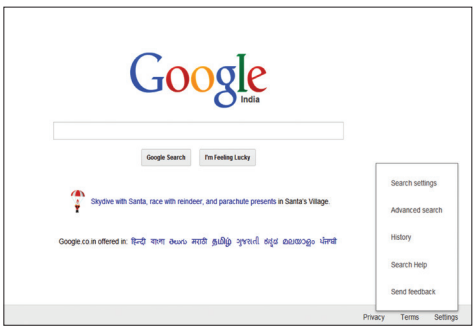
विषय-वस्तु की फिल्टरिंग कैसे करें?

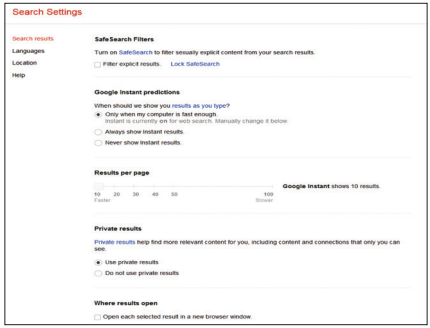
इंटरनेट एक्सप्लोरर में, कोई विकल्प नहीं है कि वह वेबसाईट्स को प्रतिबंधित करे और केवल उन्हीं वेबसाईट्स तक पहुँच रखे, जो उपयोगकर्त्ता के द्वारा सेट किए गए हैं़

- इंटरनेट एक्सप्लोरर में, वेब ब्राउसर में औजार इंटरनेट विकल्प का चयन करें और विषय-वस्तु का चयन करें क्लिक समर्थ



- गूगल शोध इंजिन में सुरक्षित शोध फिल्टरिंग के लिए एक विकल्प होता है, प्राथमिकता पर क्लिक करें या फिल्ट रिंग की सुरक्षित शोध के लिए प्राथमिकता की शोध करें और इच्छित विकल्प का चयन करें





- याहू शोध इंजिन में, सुरक्षित शोध फिल्टरिंग चयन हेतु एक विकल्प होता है, इसके लिए उन्नत इच्छित विकल्प के चयन पर क्लिक करें़

- यह याद रखें कि इन फिल्टरिंग विशेषताओं में से १००% परिशुद्ध कोई भी नहीं है और कोई अनुपयुक्त विषय-सामग्री फिर भी आ सकती है़
- आपके बच्चों को सुरक्षित ढंग से वेब की सर्फिंग सिखाना महत्वपूर्ण है और इसके लिए इंटरनेट पर छान-बीन करने के लिए वक्त लें़

पैतृक नियंत्रण बार्स

पैतृक नियंत्रण बार एक सरल व शक्तिशाली उपकरण है, जो आपके बच्चों को अच्छी तरह प्रकट होनेवाले वेबसाईट्स से संरक्षण में मदद करता है़ आपका बच्चा जब इंटरनेट पर सर्फ़ कर रहा हो, तब मात्र बालक-मोड को सक्रिय कर दें और तब टूलबार वयस्क उन्मुख वेबसाईट्स पर उनकी पहुँच को रोक देगा़ यह सुनिश्चित करें कि इंटरनेट का इस्तेमाल करते समय आपका बच्चा सुरक्षित है़

- पैतृक नियंत्रण से आपको निम्न करने पर लाभ होगा
- बच्चे पर माता-पिता द्वारा निर्धारित इंटरनेट गतिविधि की समय-सीमा हेतु दबाव बनाएँ़
- उन सामग्री (चित्र) को अवरुद्ध करें, जिन्हें बच्चों के लिए अनुपयुक्त समझा गया है़
- इंटरनेट पर आपके बच्चे की गतिविधि पर निगरानी रखें और इसके लिए कंप्यूटर पर आपके बच्चे द्वारा देखी गई साईट्स एवं/ या स्नैपशॉट्स के नाम संग्रहित कर लें, जिससे आप उन्हें बाद में देख सकें़
- परिवार के प्रत्येक सदस्य के लिए भिन्न प्रतिबंध रखें़
- इंटरनेट पर शोध के परिणाम उन विषय वस्तु तक सीमित रखें, जो बच्चों के लिए उपयुक्त हैं़

वेब ब्राउसर्स में पैतृक नियंत्रण बार्स

- इंटरनेट अन्वेषक 8

  विंडोस विस्टा ओएस में पैतृक नियंत्रण बार, इंटरनेट अन्वेषक को चूक से मदद पहुँचाता है़ जानकारी के लिए विंडोस विस्टा में पैतृक नियंत्रण सेट करें़ प्रारंभ करने के बटन को क्लिक कर पैतृक नियंत्रण खोलें और उपयोगकर्त्ता के खाते के अंतर्गत नियंत्रण पैनल की क्लिकिंग का चयन करें और फिर पैतृक नियंत्रण सेटअप पर क्लिक करें़ यदि आपको प्रशासकीय पासवर्ड या पुष्टि के लिए प्रेरित किया जाता है, तब पासवर्ड टाईप करें या पुष्टि उपलब्ध कराएँ

  फिर मानक उपयोगकर्त्ता के उस खाते को क्लिक करें, जिसके लिए पैतृक नियंत्रण सेट करना ह

  पैतृक नियंत्रण के अंतर्गत, ऑन क्लिक करें

  एक बार आपने आपके बच्च्चे के मानक उपयोगकर्त्ता खाते के लिए पैतृक नियंत्रण को चला दिया, फिर आप जिस व्यक्तिगत सेटिंग्स को नियंत्रित करना चाहते हैं, उसे समायोजित कर सकते हैं़ आप निम्न क्षेत्र जैसे कि वेब प्रतिबंध, समय सीमा, गेम्स को विशिष्ट प्रोग्राम्स को अवरुद्ध कर नियंत्रित कर सकते हैं़

  निम्न लिंक्स से तृतीय पक्ष के पैतृक नियंत्रण बार के उपकरणों को डाऊनलोड किया जा सकता है

  http://www.ieaddons.com/en/details/Security/ParentalControl_Bar/

- विंडोज में फायरफॉक्स ब्राउसर

  ऐसे कई फायरफॉक्स एड-ऑन या विस्तार हैं, जिन्हें फायरफॉक्स के लिए कुछ उत्पाद/ एड-ऑन से डाऊनलोड

किया जा सकता है
https://addons.mozilla.org/en-US/firefox/search?q=parental+control&cat=all

- परिवारों के लिए ग्लबल

  ग्लबल के द्वारा आप निजी परिवार का एक पृष्ठ निर्मित कर सकते हैं, जहाँ आप आपके बच्चों की ऑनलाईन गतिविधियों पर निगरानी रख सकते हैं और उनकी मदद कर सकते हैंः अपलोडिंग, संग्रहण व आपके फोटोस को ऑनलाईन साझा करने हेतु ग्लबल गेम्स, चैट, सुरक्षित सर्फिंग व परिवार फोटो टाईमलाईन सेवा उपलब्ध कराता हैः बच्चों का एक सुरक्षित शोध इंजन बच्चों के लिए पूछें को ग्लबल समन्वित करता है
  https://addons.mozilla.org/firefox/addon/5881

- प्रोकॉन फिल्टस

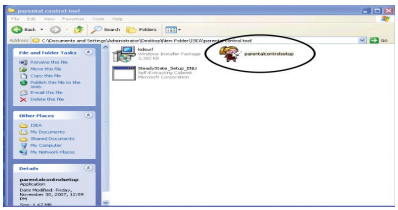
  वेबपेज की विषय-सामग्री, जिसमें अनुपयुक्त शब्दों की सूची का इस्तेमाल किया गया है और उन्हें तारों (***) के द्वारा प्रस्थापित किया गया हैः यह ध्यान दें कि खराब शब्दों का फिल्टर उन वेबसाईट्स को अवरुद्ध नहीं करता है, जिनमें ये शब्द हैं, आपको उस वेबसाईट्स को काली-सूची में जोड़ देना चाहिएः प्रोकॉन समस्त यातायात को भी रोक सकता है, अतः यह सुनिश्चित करें कि केवल इच्छित वेबसाईट्स पर (जो श्वेत सूची में सेट हैं) ही पहुँच हो सकती हैः आप साईट्स व पृष्ठों की "श्वेत" व काली" सूचियों का प्रबंध कर सकते हैंः सेटिंग्स में अन्य कोई बदलाव न कर सके, इसलिए प्रोकॉन में पासवर्ड संरक्षण भी है

- प्रोकॉन लट्टे

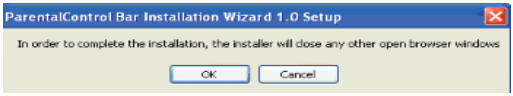
  फायरफॉक्स विस्तरण के अलावा और भी बहुत से तृतीय पक्ष के सॉफ्टवेयर पैकेजेस हैं, जो विषय-वस्तु को आपके ऑपरेटिंग सिस्टम के द्वारा या उस बिंदु पर जहाँ आपका नेटवर्क इंटरनेट से संबद्ध होता है, वहाँ, फिल्टर कर सकते हैं
  Available: https://addons.mozilla.org/firefox/addon/1803

पैतृक नियंत्रण टूलबार के संस्थापन की कार्यविधि

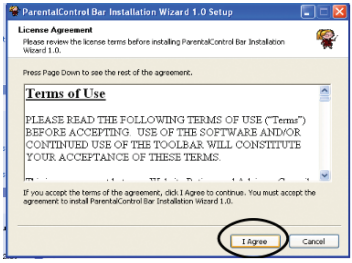
- दो बार क्लिक करने के बाद, यह आपको अन्य किसी ब्राउजर विंडो को बंद करने के लिए कहेगाः ठीक है बटन को क्लिक करेंः



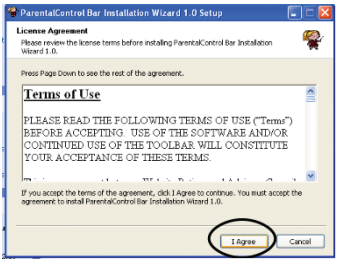
- लायसंस करार की सहमति के लिए मैं सहमत हूँ क्लिक करें

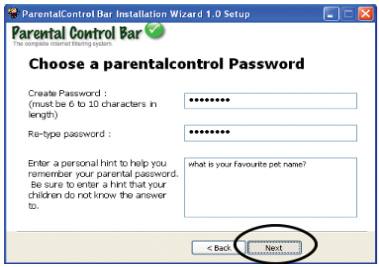


- यह होशियार पैतृक नियंत्रण का पासवर्ड पूछता है, जिसका उपयोग पैतृक नियंत्रण की सेटिंग्स के प्रबंधन के लिए होगा

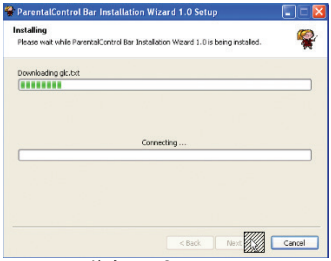


- पासवर्ड टाईप करें और एक प्रश्न प्रविष्ट करें, जिसका उपयोग एक संकेत के रूप में तब होगा, जब आप पहले टाईप किए हुए पासवर्ड को भूल जाते हैं। यह सुनिश्चित करें कि आपके बच्चे को इस प्रश्न का उत्तर मालूम नहीं है

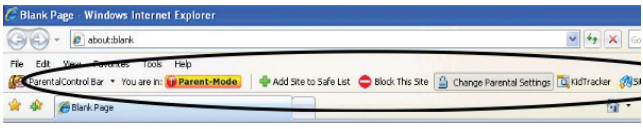




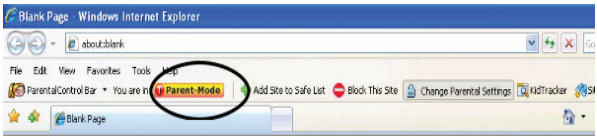
- ई-मेल पता टाईप करें, जिस पर पैतृक पासवर्ड भेजा जाएगा और अगला क्लिक करें।
- वेबसाईट्स से उपयुक्त फाईल्स लेकर अब आगे संस्थापन प्रारंभ हो जाता है और कुछ मिनटों में ही यह पूरा हो जाता है



- जैसा ऊपर दिखाया गया है, उस तरह से इंटरनेट अन्वेषक ब्राउसर में पैतृक नियंत्रण बार जुड़ जाएगा।
- नीचे पैतृक बटन बताया गया है, जो दर्शाता है कि ब्राउसर पैतृक मोड में काम कर रहा है।

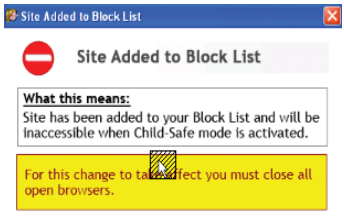


- उस वेबसाईट को टाईप करें, जिसे आप बच्चों के लिए अवरुद्ध करना चाहते हैं और फिर इस साईट को अवरुद्ध करें बटन को क्लिक करें।



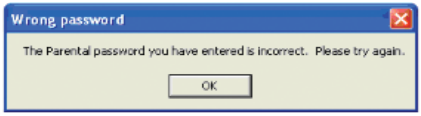
- इस साईट को अवरूद्ध करने के लिए पैतृक नियंत्रण बार पासवर्ड पूछता है

- पासवर्ड को प्रविष्ट करने व ठीक है क्लिक करने के बाद एक विंडो खुलती है, जो बताती है कि साईट अवरूद्ध है्र



- जब भी बच्चा वेबसाईट को ब्राउस करना चाहे, तब ब्राउसर बच्चा मोड में होना चाहिएए इसलिए पैतृक मोड बटन क्लिक करें, जिससे कि ब्राउसर बच्चा मोड में परिवर्तित हो जाए

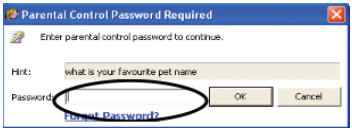
- इसके बाद पैतृक नियंत्रण टूलबार नीचे की तरह दिखाई देगा, जो बताएगा कि अब बच्चा सुरक्षित मोड सक्रिय है
- ठीक है क्लिक करेंए्र
- जब भी बच्चा अवरूद्ध साईट को ब्राउस करना चाहे, तब वह साईट को खोलने के लिए पासवर्ड पूछेगा, जिसे नीचे बताया गया हैए्र
- अब यदि बच्चा बिना पासवर्ड प्रविष्ट किए वेबसाईट्स देखना चाहता है, तब इस प्रकार की भूल आ जाती है

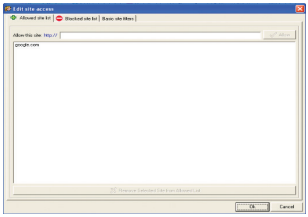


पैतृक नियंत्रण टूलबार में पैतृक नियंत्रण सेटिंग्स में बदलाव करना

- वेबसाईट्स को स्वीकृति देने या रोकने की सेटिंग्स में बदलाव के लिए, पैतृक सेटिंग्स बदलें को क्लिक करें

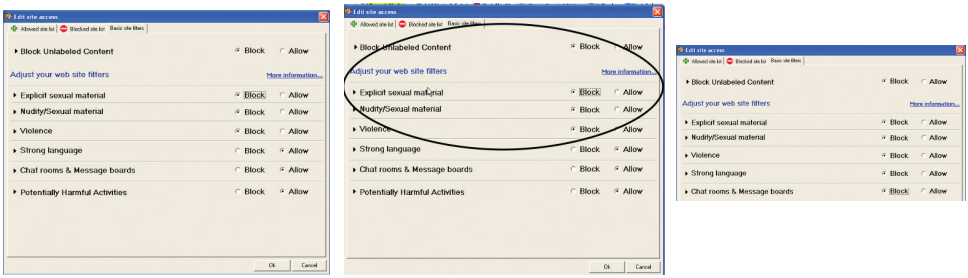
- पैतृक सेटिंग्स बदलें को क्लिक करने के बाद एक विंडो खुलती है, जिसमें पैतृक नियंत्रण पासवर्ड पूछा जाता है़
- पासवर्ड टाईप करें और फिर ठीक है क्लिक करें़ उसके बाद इसके जैसी एक विंडो खुलती है





- आप स्वीकृत साईट सूची टेब पर क्लिक कर, स्वीकृत सूची में साईट्स शामिल कर सकते हैं

- आप जिस वेबसाईट को स्वीकृत करना चाहते हैं, उसे टाईप करें और फिर स्वीकृत बटन को क्लिक करें, जैसा कि नीचे बताया गया है़
- आप अवरुद्ध साईट सूची को क्लिक कर अवरुद्ध सूची में भी साईट्स शामिल कर सकते हैं
- आप जिस वेबसाईट को अवरुद्ध करना चाहते हैं, उसे टाईप करें और फिर अवरुद्ध बटन को क्लिक करें, जैसा कि नीचे के चित्र में बताया गया है़
- बुनियादी साईट फिल्टर्स टेब को क्लिक कर आप कुछ विशिष्ट प्रकार की विषय-सामग्री को भी फिल्टर कर सकते हैं़
- बुनियादी साईट फिल्टर्स टेब को क्लिक करने के बाद निम्न विंडोस प्रकट होती हैं़
- चूक से निम्न प्रकार की साईट्स फिल्टर हो गईं़
- अवरुद्ध बटन का चयन कर आप अन्य प्रकार की साईट्स को भी अवरुद्ध कर सकते हैं



स्पाम फिल्टर

विषय-सामग्री फिल्टर एवं वेबसाईट फिल्टर के साथ आजकल सभी ई-मेल सेवा प्रदाता स्पाम फिल्टर के साथ ही निर्मित किए जाते हैं़

स्पाम फिल्टर विकल्प को क्लिक करें और उसमें उस ई-मेल आईडी को जिसे आप विश्वसनीय आईडी नहीं समझते हैं या अज्ञात उपयोगकर्त्ता की ई-मेल आईडी को जोड़ें़

के९ वेब संरक्षण क्या है?

के९ वेब संरक्षण एक पैतृक नियंत्रण व वेब फिल्टरिंग सॉफ्टवेयर है़ आपने जब उसे चालू कर दिया, तब यह कंप्यूटर के उपयोगकर्त्ता को उन वेबसाईट्स को देखने को प्रतिबंधित करता है, जिनमें अवांछित विषय-सामग्री है़ यह विषय-सामग्री की ६० से अधिक श्रेणियों को अवरुद्ध कर सकती है, जिनमें शामिल हैं अश्लील, नफरत/ जातिवाद/ हिंसा, जुआ एवं मैलवेयर/ स्पायवेयर

डाऊनलोड लिंकः

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

मेरे बच्चे उस तरह की साईट्स नहीं देखते हैं़ मुझे के९ वेब संरक्षण की जरूरत क्यों है?

वे चाहे न चाहते हों, लेकिन अधिकांश बच्चे इंटरनेट पर अश्लील व जुए की व यहाँ तक की दरिंदों की सामग्री की ओर जाते हैं़ इन आँकड़ों पर विचार कीजिएः

सभी १५-१७ वर्ष वालों में से ७० प्रतिशत, जो कभी ऑन लाईन गए थे, अचानक अश्लील ऑनलाईन साहित्य से ट करा जाते हैं और २३ प्रतिशत अक्सर "बहुत" या "कुछ-कुछ" पर होते हैं़ उम्र १०-१७ वर्ष के पाँच में से एक बच्चे ने इंटरनेट पर यौन विषय के लिए अनुरोध किया हुआ होता है़ ४३ प्रतिशत बच्चों ने बताया कि उनके घरों में इंटरनेट के इस्तेमाल के संबंध में कोई नियम नहीं हैं़

१७ प्रतिशत माता-पिता मानते हैं कि उनके बच्चे अपनी प्रोफाईल्स ऑनलाईन पोस्ट करते हैं, जबकि ४५ प्रतिशत बच्चे ऐसा करने की रिपोर्ट करते हैं़ हम भय उत्पन्न नहीं करना चाहते हैं, लेकिन आज इंटरनेट पर जो सामग्री उपलब्ध है, उसका प्रकार आपके बचपन की पत्रिका प्लेबाय जैसा नहीं है़ अश्लीलता बहत अधिक प्रकट है और वह बहुत अधिक यौन शोषण को प्रोत्साहित करती है या उसमें हिंसा व यौनाचार का मेल रहता है़

किशोरों में लत के रूप में जुआ एक बढ़ती हुई समस्या है और उनमें से कई ऑनलाईन जुआ सीख रहे हैं़ वेब फिल्टरिंग

साफ्टवेयर उन्हें चालू करने से दूर रख सकता हैऽ सोशल नेटवर्किंग साईट्स जैसे कि फेसबुक या माय स्पेस भी बच्चों के समक्ष वास्तविक खतरा बन सकते हैंऽ इन साईट्स पर किशोर या किशोर-पूर्व उम्र के बच्चे अपनी व्यक्तिगत जानकारी व फोटोग्राफ्स पोस्ट करते हैंऽ ऐसी साईट्स दरिंदों के लिए सोने की खान होती हैंऽ

मुझे किस प्रकार का कंप्यूटर चाहिए?

के९ वेब संरक्षण विंडोस या मेक कंप्यूटर्स के हाल ही के संस्करणों में चलते हैंऽ के९ काम करता है, फिर चाहे इंटरनेट सेवा प्रदाता आपके इंटरनेट कनेक्शन पर कुछ भी दे रहा हो या फिर आप कोई भी ब्राउसर उपयोग में लाते हों, यह सब प्रकार के विंडोज के संस्करणों को सहयोग देता हैऽ

क्या मेरे बच्चे इसे बंद कर सकते हैं?

आप जब अपने कंप्यूटर पर साफ्टवेयर संस्थापित करते हैं, तब आपको कहा जाएगा कि आप एक पासवर्ड तैयार करेंऽ केवल वही जिसके पास सही पास वर्ड होगा, वही के९ को बंद कर सकेगाऽ

क्या होगा यदि कोई मेरे कंप्यूटर से प्रतिबंधित साईट पर जाने की कोशिश करता है?

एक प्रदर्शित "अवरूद्ध" वेबपेज बताता है कि यह पेज आपके फिल्टरिंग साफ्टवेयर द्वारा अनुमोदित नहीं हैऽ यदि आप चाहते हैं आप के९ भी सेट करवा सकते हैं, तब झांडेर जो के९ का चौकसी वाला कुत्ता है, वह भौंकेगाऽ (यह विशिष्टता माता-पिताओं के लिए फुर्तीली हैऽ यदि आपने झांडेर का भौंकना सुना है, तो यह आपके लिए सुनिश्चित है कि आपके बच्चे ने अभी एक साईट पर क्लिक किया है जो नहीं-नहीं है

के९ किस प्रकार कार्य करता है?

हमने उन वेबसाईट्स का डाटाबेस बनाया है, जिनमें अश्लीलता, नफरतपूर्ण भाषण, हिंसा, जुआ व ऐसी ५५ से अधिक श्रेणियाँ हैंऽ जब कंप्यूटर उपयोगकर्त्ता ऐसी साईट्स पर जाने की कोशिश करता है, जिसकी श्रेणी को आपने अवरूद्ध किया हुआ है और "प्रतिबंधित" स्क्रीन प्रकट होती है और तब के९ का चौकसी वाला कुत्ता झांडेर भौंकता हैऽ (आप भौंकना रोक सकते हैं)ऽ यदि उपयोगकर्त्ता ऐसी साईट्स पर जाने की कोशिश करता है, जो डाटाबेस ने पहले नहीं देखा हो तब वह अनुपयुक्त सामग्री के लिए साईट की विषय-सामग्री को स्केन करता है और तब वह साईट को या तो मंजूरी देता है या प्रतिबंधित करता हैऽ (इस प्रक्रिया को हम डीआरटीआर-डायनामिक रियल टाईम रेटिंग कहते हैं)ऽ यह बहुत शीघ्र होता है और उपयोगकर्त्ता को अहसास भी नहीं होता है कि यह हुआ हैऽ नई प्रतिबंधित वेबसाईट्स को डाटाबेस में जोड़ा गया हैऽ

के९ एवं अन्य फिल्टरिंग साफ्टवेयर में क्या फर्क है?

के९ एवं अन्य कई फिल्टरिंग समाधान में एक फर्क यह है कि के९ इंटरनेट प्रदाता से व ब्राउसर से स्वतंत्र हैऽ यह किसी भी विंडोस या मेक कंप्यूटर पर चलेगा, फिर चाहे इंटरनेट सेवा प्रदाता आपको इंटरनेट कनेक्शन पर कुछ भी दे रहा होऽ यह किसी भी इंटरनेट

ब्राउसर पर काम करता है़

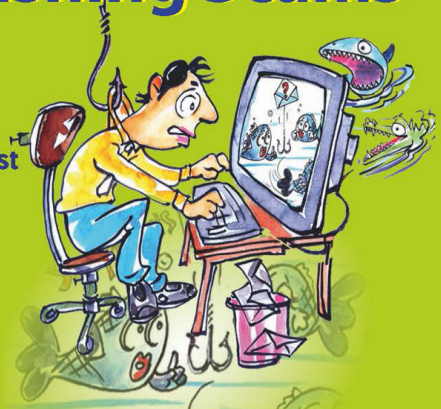
दूसरा फर्क यह है कि के९ वाणिज्यिक-श्रेणी के फिल्टरिंग समाधान का उपयोग करता है- यह केन्द्रीय डाटाबेस व गतिवान पेज-रेटिंग तकनीक का मिश्रण है और जिसका परीक्षण व्यवसाय के सबसे बड़े खिलाड़ियों के समक्ष हुआ और जिसमें यह शीर्ष पर रहा है़ प्रतिदिन हम करीब २५० से ५०० मिलियन रेटिंग के अनुरोध पाते हैं़ यह अत्यधिक इंटरनेट दृश्यता है़ इसका परिणाम यह है कि आप आसानी से इस्तेमाल किए जाने वाले पॅकेज में गंभीर समाधान के लाभ प्राप्त करते हैं़ एक और फर्क यह है कि के९ को "प्रशिक्षित" करने की जरूरत नहीं है़ आपको इसे यह सिखाने की जरूरत नहीं है कि आप किस प्रकार की वेबसाईट को अवरूद्ध करना चाहते हैं़ आप जैसे ही इसे संस्थापित करते हैं, यह काम करना शुरूकर देता है़

Reference:

http://www1.k9webprotection.com/

Guidelines to avoid Phishing & Vishing Scams

Donot give any confidential information such as password, customer id, etc., to any e-mail request, even if the request is from government authorities



The Padlock icon at the upper or bottom right corner of the webpage must be always 'On' during secure transactions

Do not transfer funds to or share your account details with unknown/non-validated source, luring you with commission, attractive offers

Do not respond to the calls and SMS's received from the unknown users

इन्टरनेट संचार मीडिया

संचार मीडिया विविध मीडिया टेक्नोलॉजी है जो जन संचारसे बड़ी संख्यामें दर्शकों तक पहुँचनेका इरादा रखता है ए टेक्नोलॉजी जिससे यह संचार होता है बदलती रहती है ए प्रसारण मीडिया जैसे रेडियो, रेकोर्ड किया हुआ संगीत, फिल्म और टेलीविज़न उनकी जानकारी इलेक्ट्रॉनिक स्वसे संचारित करते हैं ए प्रिंट मीडिया उनकी जानकारी बाँटनेके लिए भौतिक वस्तु जैसे वर्तमानपत्र, किताब, पुस्तिका या कॉमिक्सका उपयोग करते हैं ए आउटडोर मीडिया संचार मीडियाका स्व है जिसमें बिलबोर्डस, साईन्स या विज्ञापन पत्र व्यवसायिक इमारतें, खेल स्टेडियमों, दुकानों और बसेंकी अन्दर और बाहर लगाना शामिल है ए इन्टरनेट मीडिया संचार इन्टरनेट और मोबाइल नेटवर्कस दोनोंमें विभिन्न संचारके लिए इन्टरनेट टेक्नोलॉजीजका सबसे बड़ा संचार मीडिया है ए

इन्टरनेट मीडिया टाइप इन्टरनेट पर एक मानक पहचानकर्ता है जिसका उपयोग फाइलमें किस प्रकारकी जानकारी है वह दर्शानेके लिए किया जाता है ए आम उपयोगमें निम्नलिखित शामिल है :

- ✓ ईमेल ग्राहकों अनुलग्नक फाइल्सकी पहचान करनेके लिए इसका उपयोग करते हैं,
- ✓ वेब ब्राउजर्स जो फाइल्स ्षि प्रास्वमें नहीं है उसका प्रदर्शन या उत्पादन कैसे करना वह निर्धारित करनेमें इसका उपयोग करते हैं,
- ✓ सर्च इंजन इनका उपयोग वेब पर डेटा फाइल्स वर्गीकृत करनेके लिए करते हैं ए

ईमेल सुरक्षा

ईमेल इलेक्ट्रॉनिक मेल का संक्षिप्त रूप है ़ वह इन्टरनेट पर व्यापक रूपसे इस्तेमाल की जाती सेवाओं में से एक है ़ ईमेलका उपयोग इन्टरनेट पर संदेशोंका पाठ स्वरूपमें प्रसारण करनेके लिए किया जाता है ़ रिसीवर-ईमेल पता और इसके विपरीतका उपयोग करके सन्देश भेजा जा सकता है ़ उपयोगकर्ताओंके किसीभी नंबर पर एक साथ ईमेल भेजी जा सकती है, गंतव्य तक पहुँचनेमें इसे सिर्फ कुछ मिनटोंही लगते हैं ़ ईमेलमें दो घटक शामिल है ; सन्देश प्रवेशिका नियन्त्रण जानकारी, प्रवर्तकका ईमेल पता और एक या ज्यादा प्राप्त करनेवालेका पता और सन्देशका मुख्य हिस्सा जो कि ईमेल सामग्री है ़

कुछ ईमेल पध्दतिओं एकल कंप्यूटर पध्दति या छोटे नेटवर्क तक सीमित है और प्रवेशद्वारके माध्यमसे अन्य ीसचैन पध्दतिओंसे जुडी हुइ है, जो उपयोगकर्ताओं को विश्वमें कहीं भी जुड़नेके लिए सक्षम बनाती है ़ हालांकि विभिन्न इलेक्ट्रॉनिक मेल पध्दतिओंके विभिन्न प्रारूप है, कुछ उभरते मानक हैं जैसे मेसेजिंग एप्लीकेशन प्रोग्रामिंग इंटरफ़ेस(षछ), ठ.400 जो उपयोगकर्ताओं को विभिन्न इलेक्ट्रॉनिक मेल पध्दतिओं के बीचमें संदेशे भेजनेके लिए सक्षम बनाता है ़ षछ विंडोजमें बनी हुई मेल एप्लीकेशन प्रोग्रामिंग इंटरफ़ेस है, जो मेल्स के वितरणके लिए विभिन्न मेल पध्दतिओंको एकसाथ काम करनेके लिए सक्षम बनाती है ़ जब तक षछ दोनों एप्लीकेशन पर सक्षम है, उपयोगकर्ताओं एक दुसरेके साथ मेल्स साज़ा कर सकते है ़

ठ.400 विश्वव्यापी प्रोटोकॉल है जो सभी ईमेल संदेशोंके लिए मानक प्रारूप प्रदान करता है ़ ठ.500, मानक ठ.400 का विस्तार है, जो इमेल्स भेजनेके लिए मानक एड्रेसिंग प्रारूपों प्रदान करता है जिससे सभी ईमेल पध्दतिओं एक दूसरेके साथ जुडी हुई है ़

एक ईमेल कैसे काम करता है ?

ईमेल सर्वरोंके तीन मुख्य प्रकार है :

'३ः पोस्ट ऑफिस प्रोटोकॉल वर्शन ३('३) मानक मेल प्रोटोकॉल है जिसका उपयोग दूरस्थ सर्वरसे स्थानीय मेल ग्राहकको इमेल्स प्राप्त करनेके लिए किया जाता है ़ '३ आपको ऑफलाइन होने के बावजूद आपके स्थानीय कंप्यूटर पर इमेल्स संदेशे डाउनलोड करने और उन्हें पढ़नेकी अनुमति देता है ़ ध्यान दें, जब आप '३का उपयोग आपके ईमेल एकाउंटसे जुड़ने के लिए करते हैं, संदेशे स्थानीय रूपसे डाउनलोड होते है और सर्वरोंसे हटा दिए जाते हैं ़ इसका मतलब यह है कि अगर आप आपके एकाउंट पर एकाधिक स्थानसे पहुँचते है तो यह आपके लिए सर्वोत्तम विकल्प नहीं है ़ दूसरी ओर, अगर आप '३ का उपयोग करते है, आपके संदेशे आपके स्थानीय कंप्यूटर पर संग्रहीत होते हैं, जो आपके ईमेल एकाउंट ूसका वेब सर्वर पर जगहके उपयोगको कम करते है ़

मूलभूत तरीक़ेसे, '३ प्रोटोकॉल दो पोर्ट्स पर काम करता है :

- पोर्ट 110 – यह मूलभूत '३ गैर-एन्क्रिप्टेड पोर्ट है
- पोर्ट 995 – अगर आप सुरक्षित रूपसे '३ का उपयोग करके जुड़ना चाहते हो तो आपको इसी पोर्टका उपयोग करना चाहिए

IMAP:

षछः इन्टरनेट मेसेज एक्सेस प्रोटोकॉल (षछ) मेल प्रोटोकॉल है जिसका उपयोग स्थानीय ग्राहकसे दूरस्थ वेब सर्वर पर ईमेल तक पहुँचनेके लिए किया जाता है ़ षछ और '३ इमेल्स पुनःप्राप्त करनेके लिए आम तौर पर सबसे ज्यादा इस्तेमाल किये जाने वाले दो मेल प्रोटोकॉल्स है ़ दोनों प्रोटोकॉल्स सभी आधुनिक ग्राहकों और वेब सर्वरों द्वारा समर्थित है ़ जब कि '३ प्रोटोकॉल मान लेता है कि आपका ईमेल सिर्फ एक एप्लीकेशन द्वारा पहुंचा जा रहा है, षछ कई ग्राहकों द्वारा एकसाथ पहुँचकी अनुमति देता है ़ इसीलिए षछ आपके लिए ज्यादा उपयुक्त है, अगर आप अपने ईमेल तक विभिन्न स्थानोंसे पहुँचने वाले हो या आपके संदेशे कई उपयोगकर्ताओं द्वारा प्रबंधित हो रहे हो ़

मूलभूत रूपसे षछ प्रोटोकॉल दो पोर्ट्स पर काम करते है :

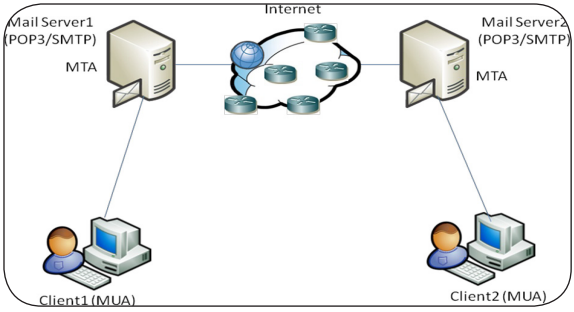
- पोर्ट 143 – यह मूलभूत षछ गैर- एन्क्रिप्टेड पोर्ट है
- पोर्ट 993 – अगर आप सुरक्षित रूपसे षछ का उपयोग करके जुड़ना चाहते हो तो आपको इसी पोर्टका उपयोग करना चाहिए ़

SMTP:

झषः सिम्पल मेल ट्रान्सफर प्रोटोकॉल (झष्) इन्टरनेट पर इमेल्स भेजनेके लिए सर्व-स्वीकृत प्रोटोकॉल है ़
मूलभूत रूपसे, झष् प्रोटोकॉल तीन पोर्ट्स पर काम करते है :

- पोर्ट 25 – यह मूलभूत झष् गैर-एन्क्रिप्टेड पोर्ट है
- पोर्ट 465 – अगर आप सुरक्षित रूपसे झष् का उपयोग करके जुड़ना चाहते हो तो आपको इसी पोर्टका उपयोग करना चाहिए ़
- पोर्ट 587: यही मूलभूत मेल सबमिशन पोर्ट है ़ जब कोई मेल ग्राहक या सर्वर उचित मेल सर्वर द्वारा मेल प्रस्तुत कर रहा हो तब हमेशा इस पोर्टका उपयोग करना चाहिए ़

- ईमेल का कार्य नीचेकी आकृतिमें दिखाया गया है ़ हर एक सर्वरमें एक मशीन पर चल रहे दो विभिन्न सर्वरों शामिल है ़ एक '३ (पोस्ट ऑफिस प्रोटोकॉल) या षछ(इन्टरनेट मेल एक्सेस प्रोटोकॉल) सर्वर जो अन्दर आनेवाले मेल्स रखता है और दूसरा झष्(सिम्पल मेसेज ट्रान्सफर प्रोटोकॉल) सर्वर जो बाहर जानेवाले मेल्स रखता है ़ झष् पोर्ट नंबर २५ पर काम करता है और ' 110 नंबरके पोर्ट पर काम करता है और षछ 143 नंबरके पोर्ट पर काम करता है ़



ऊपर दिखायी आकृतिमें ,

- ग्राहक 1 का एकाउंट मेल सर्वर १ में है और ग्राहक २ का एकाउंट मेल सर्वर 2 में है ़
- जब ग्राहक 1 ग्राहक 2 को मेल भेजता है, मेल पहले मेल सर्वर 1 के झष् सर्वरके पास जाता है ़ यहाँ झष् सर्वर प्राप्त करनेवालेका पता दो भागमें बांटता है यूजरनाम और डोमेननाम ़
- उदाहरणके तौर पर, अगर झष् सर्वर प्राप्तकर्ताका पता `जीरिंत्रीटचसॅनी.र्बस के स्वमें पाता है, वह अलग करेगा यूजर१ में, जो गंतव्य मेल सर्वरमें मेल एकाउंट है और ीटचसॅनी.र्बस जो गंतव्य मेल सर्वरमें डोमैन नाम है ़ अब डोमैन नामकी सहायता से वह प्राप्तकर्ताके मेल सर्वरका विशेष पताका अनुरोध करेगा और तब उसके झष् सर्वरसे जुड़ कर मेल सर्वर 2 को सन्देश भेजेगा ़
- मेल सर्वर 2 का झष् सर्वर ग्राहक २ के मेलबॉक्समें मेल सर्वर २ के '3 की सहायतासे संदेश इकट्ठा करेगा ़ जब ग्राहक 2 अपना मेल बॉक्स खोलता है, वह ग्राहक १ द्वारा भेजा गया मेल देख सकता है ़

स्व से इमेल्स ईमेल के माध्यमसे संभावित खतरों और सुरक्षित सँभालनेके लिए मार्गदर्शन

इमेल्स पोस्टकार्ड्स जैसे होते हैं, जिसमें से कोई भी जानकारी देख सकता है ़ जब एक मेल एक मेल सर्वरसे दूसरे मेल सर्वरको हस्तांतरित होता है, वहां विभिन्न रोक है जहाँ अनधिकृत उपयोगकर्ताओं द्वारा जानकारी देखने या उसको संशोधित करने की सम्भावना है ़

क्योंकि ईमेल सर्वरके लिए बैकअप बनाए रखा जाता है, सभी संदेशों आपके मेलबॉक्ससे हटाये जानेके बावजूद स्पष्ट पाठके स्वमें संग्रहीत किया जायेगा ़ इस वजहसे जो लोग बैकअप बनाए रखते है उनके लिए जानकारी देख सकनेकी सम्भावना है ़ इसीलिए इमेल्स द्वारा निजी जानकारी भेजना उचित नहीं है ़

आपने दस लाख डॉलर्सकी लाटरी इनाममें जीती है, इस तरहके मेल्स मिलना या प्राप्त करना बड़ी बात है और सचमें सबसे खुशीकी बात है ़ हालांकि ऐसे मेल्स सच नहीं हो सकते ़ बहुत लोगोंने इस प्रकारके मेल्सका जवाब दे कर पैसे की बड़ी राशि खो दी है ़ इसलिए इस प्रकारके इमेल्स नजरंदाज करें, इसमें भाग न लें और इसे घोटाले के स्व में देखें ़

सुझाव :

- ✓ *संलग्नक खोलनेसे पहले हमेशा आप उसकी जाँच करे ़*
- ✓ *हमेशा जाँच और पुष्टि करे कि इ-मेल कहाँसे प्राप्त हुआ है , आम तौर पर सेवा देनेवाले लोग कभी भी आपका पासवर्ड पूछेंगे नहीं या बदलनेके लिए नहीं कहेंगे ़*
- ✓ *हमेशा स्पैम इ-मेल्स को नजरंदाज या नष्ट करनेकी सिफारिश की जाती है ़*
- ✓ *अनजान उपयोगकर्ताओं द्वारा प्रस्तावित मुफ्त उपहारोंको हमेशा नजरंदाज करो ़*

- पासवर्डकी चोरी करनेका एक तरीका व्यक्तिके पीछे ख़डा रहना और जब वह टाइप कर रहा हो तब या जिसमें उसने पासवर्ड लिखा हो वह कागज ढूंढ रहा हो तब उनके पासवर्डका निरीक्षण करना है ़
- पासवर्ड चोरी करनेका दूसरा तरीका अनुमान लगाना है ़ व्यक्तिकी निजी जानकारीकी मदद्से हैकर सभी संभव संयोजनोंकी कोशिश करते हैं ़
- जब पासवड्र्सके संयोजनों बड़ी संख्यामें हो तब पासवर्ड कैक करनेके लिए हैकर फ़ास्ट प्रोसेसरका उप और कुछ सॉफ्टवेर टूल्स का उपयोग करते हैं ़ पासवर्ड कैक करनेका यह तरीका ब्रूट फ़ोर्स अटैक कहा जाता है ़
- कुछ सॉफ्टवेर टूल्सकी मददसे हैकर डिक्शनरी के सभी संभव शब्दोंकी भी कोशिश करते हैं ़ इसे डिक्शनरी अट ैक कहा जाता है ़
- आम तौर पर, स्पैमर या हैकर ईमेल पता चोरी करनेकी कोशिश करते हैं और दुर्भावनापूर्ण सॉफ्टवेर या कोड संलग्नक द्वारा, जाली इमेल्स और स्पैम भेजते हैं और आपकी निजी जानकारी इकट्ठा करनेकी कोशिश भी करते हैं ़

संलग्नक

कभी कभी संलग्नक इमेल्सके साथ आते हैं और उसमें निष्पादन योग्य कार्य जैसे मैक्रोस, डठङ फाइल्स और ढडघ फाइल्स शामिल होते हैं ़ कभी कभी संलग्नक दोहरे प्रसारके साथ आते है जैसे " चाचबरसीहा.टी.र्गब." ऐसे संलग्नक खोलने या क्रियान्वित करनेसे दुर्भावनापूर्ण कॉड आपके सिस्टममें डाउनलोड हो सकता है और आपके सिस्टमको संक्रमित कर सकता है ़

जाली इ-मेल्स

कभी कभी इ-मेल्स जाली इ-मेल पता जैसे जीपिबीजक्षेसबुक.र्बस , " खचबीर्मंट्ठचजर्जुगिट्ठ४बक्ष१.डैं संलग्नक के साथ प्राप्त होते है और इ-मेल दावा करता है कि फाइल " खचबीर्मंट्ठचजर्जुगिट्ठ४बक्ष१ीटी " उपयोगकर्ताका नया फेसबुक पासवर्ड शामिल करती है ़ जब उपयोगकर्ता फाइल डाउनलोड करता है, वह उनके कंप्यूटर पर गडबड कर सकता है और दुर्भावनापूर्ण सॉफ्टवेरसे संक्रमित हो सकता है ़

स्पैम इ-मेल्स

स्पैम संदेशे आपको इनबॉक्स या इ-मेल डेटाबेस भर कर परेशान करता है ़ स्पैम इ-मेल द्वारा विभिन्न प्राप्तकर्ताओं को भेजे गए समान सन्देशोंका समावेश करता है ़ कभी कभी स्पैम इ-मेल्स विज्ञापनके साथ आते है और उसमें वायरस शामिल हो सकता है ़ ऐसे इ-मेल्स खोलनेसे आपका सिस्टम संक्रमित हो सकता है और आपका इ-मेल घ स्पैमरों की सूचिमें आ जाता है ़

मुफ्त उपहारका प्रस्ताव देनेवाले इ-मेल्स

कभी कभी अनजान उपयोगकर्ताओं इ-मेल्स द्वारा आपको निशाना बनाते है, उपहारों, लाटरी, पुरस्कार का प्रस्ताव दे कर जो मुफ्त हो सकता है और आपकी निजी जानकारी मुफ्त उपहार स्वीकारने के लिए पूछता है या लाटरी और पुरस्कार पर दावा करनेके लिए पैसे मांगता है ़ यह आपकी निजी जानकारी पानेके लिए जाल बिछाने का एक रास्ता है

छल (ठगना)

छल एक प्रयास है व्यक्तिको जूठी बात सच है ऐसा मनवानेका ऽ उपयोगकर्ताओं के बीच जान बुझ कर भय, संदेह फ़ैलानेका प्रयास करने के रूपमें भी इसे परिभाषित किया गया है ऽ

कैसे रोकें

छाननेवाला सॉफ्टवेरका इस्तेमाल करके

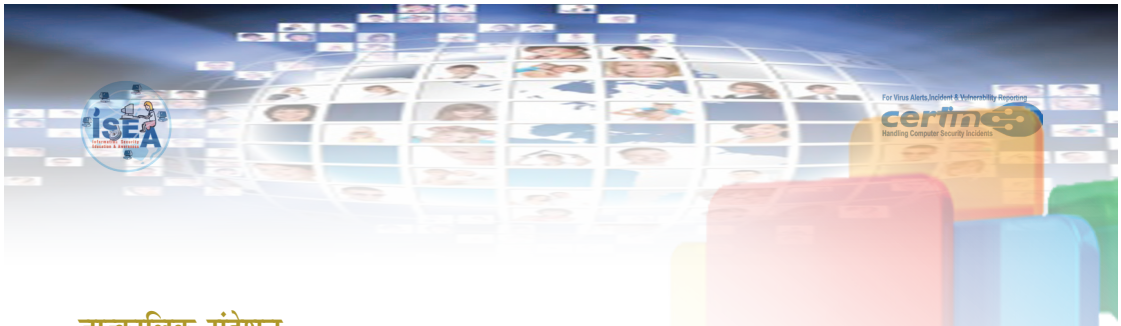
स्पैमसे बचनेके लिए इ-मेल फ़िल्टरिंग सॉफ्टवेरका उपयोग करें जिससे सिर्फ अधिकृत उपयोगकर्ताओं से संदेशे प्राप्त हो ऽ ज्यादातर इ-मेल प्रदाता फ़िल्टरिंग सेवाओंकी पेशकश करते हैं ऽ

अनजान लोगोंके इ-मेल्सको नजरंदाज करें

अनजान व्यक्तिओं से आये संलग्नक को खोलने से बचें, क्योंकि उसमें प्राप्त संदेशे के साथ वायरस शामिल हो सकता है ऽ आपकी हार्ड डिस्कमें इ-मेल्स से संलग्नक डाउनलोड करने में सचेत रहें ऽ संलग्नक को बचाके रखनेसे पहले उसे अद्यतन सॉफ्टवेरसे जाँच लें ऽ

सुरक्षित रूपसे इ-मेल इस्तेमाल करनेके लिए मार्गदर्शन

- क्योंकि इ-मेल संदेशे स्पष्ट पाठ में परिवर्तित होते है, कोई एन्क्रिप्शन सॉफ्टवेर जैसे कि क्ष (काफी अच्छी गोपनीयता)का उपयोग इ-मेल संदेशे भेजने से पहले एन्क्रिप्ट करनेके लिए करना उचित है, ताकि वह सिर्फ निर्दिष्ट प्राप्तकर्ता के द्वारा ही डिक्रिप्ट किया जा सके ऽ
- स्पैम से बचने के लिए इ-मेल फ़िल्टरिंग सॉफ्टवेरका उपयोग करें जिससे सिर्फ अधिकृत उपयोगकर्ताओंसे संदेशे प्राप्त हो ऽ ज्यादातर इ-मेल प्रदाता फ़िल्टरिंग सेवाओंकी पेशकश करते हैं ऽ
- अनजान व्यक्तिओं से आये संलग्नक को खोलने से बचें, क्योंकि उसमें प्राप्त संदेशेके साथ वायरस शामिल हो सकता है ऽ
- आपकी हार्ड डिस्कमें इ-मेल से संलग्नक डाउनलोड करनेमें सचेत रहें ऽ संलग्नक को बचाके रखने से पहले उसे अद्यतन सॉफ्टवेरसे जाँच लें ऽ
- ऐसे संदेशे मत भेजो जिसके संलग्नक में निष्पादन योग्य कोड जैसे मैक्रोस के साथ वर्ड डॉक्यूमेंट, डठङ फाइल्स और ढडघ फाइल्स ऽ हम स्टैण्डर्ड घ'भ फॉर्मेट की जगह रिच टेक्स्ट फॉर्मेटका उपयोग कर सकते है ऽ इख आपके स्वरूप को रखेगा, लेकिन कोई मैक्रोस को शामिल नहीं करेगा ऽ अगर आप पहले से ही संक्रमित है, यह आपको दूसरोंको वायरस भेजनेसे रोक सकता है ऽ
- कोई भी इ-मेल निजी वित्तीय जानकारीके लिए अति आवश्यक अनुरोध करें तो उस पर शक करें ऽ
- आपकी निजी जानकारी पूछनेवाले इ-मेल से आये फॉर्म्स भरनेसे बचें ऽ और इ-मेल से आये लिंक पर क्लिक मत करें ऽ
- अविश्वस्त उपयोगकर्ताओंसे प्राप्त इ-मेल्स पर क्लिक न करें, क्योंकि सिर्फ क्लिक करनेसे ही कोई दुर्भावनापूर्ण कोड निष्पादित हो जाये और आपके सिस्टममें फ़ैल जाये ऽ
- जो वेब लिंक्स इ-मेल्सके द्वारा आती है, उनको मत अनुसरो ऽ



तात्कालिक संदेशन

आजकल तात्कालिक संदेशन (ष) भारत में विकसित हो रही टेक्नोलोजी और इन्टरनेट गतिकी वजह से बढ़ रहा है और पाठ आधारित वास्तविक काल से नेटवर्कसे जुड़े हुए दो या अधिक लोगोंको वास्तविक काल ऑडियो, विडियो संचार के स्व में बदल गया है ़ तात्कालिक सन्देश इससे ज्यादा लोकप्रिय हुआ, आप वास्तविक कालमें लोगोंके साथ बातचीत कर सकते हो और परिवार एवं मित्रोंकी सूचि आपके संपर्क सूचीमें रख सकते हो और जब तक व्यक्ति ऑनलाइन हो तब तक संवाद कर सकते हो ़ यहाँ छ'ि, एछ" मैसेंजर, गूगल टॉक और कई और तत्काल सेवा प्रदाता है ़

चैट स्वमें उपयोगकर्ताओं की सीमित बातचीत

IM में शामिल जोखिमों

हैकरों इंस्टेंट मेसेजिस पर लगातार पहुँचते है और इंस्टेंट मेसेज द्वारा दुर्भावनापूर्ण कोड्स देनेकी कोशिश करते हैं और कोड्समें वायरस, ट्रोजन, एवं स्पाईवेयर शामिल हो सकते है और अगर आप फाइल पर क्लिक करते हैं तो कॉड आपकी सिस्टममें प्रवेश करेगा औए चंद सेकंड्समें सिस्टमको संक्रमित करता है ़

स्पिम

स्पिम स्पैम ओवर इंस्टेंट मैसेजिंगका संक्षिप्त स्व है, वह ष प्लेटफार्मका उपयोग ष पर स्पैम सन्देशों भेजनेके लिए करता है ़ इ-मेल स्पैम सन्देशोंकी तरह, स्पिम सन्देशमें भी विज्ञापन होते हैं ़ आम तौर पर इसमें वेब लिंक्स शामिल है, उन लिंक्स पर क्लिक करने से दुर्भावनापूर्ण कॉड आपके भमें प्रवेश करता है ़

आम तौर पर, यह वास्तविक कालमें होता है और हमें काम बंद करके स्पिमसे ष विंडो पॉप- अप्सके स्वमें निपटने की जरुरत है ़ इ-मेलमें हमारे पास नष्ट करनेका समय है और हम सभी स्पैम एक ही समयमें नष्ट कर सकते है, या कोई भी संलग्नक खोलनेसे पहले उसकी जाँच कर सकते हैं ़ षमें यह नहीं हो सकता ़

सुझावः: IM में संलग्नक और लिंक्स खोलने से बचें

स्काइप विडियो कम्युनिकेशन

नयी टेक्नोलॉजीने हर एकको सशक्त बनाया है और पूरी दुनियामें दर्शकों तक पहुँचनेमें मदद की है ़ उनके शब्दों, चित्रों और आवाजें चाँद सेकंड्समें दुनिया भरमें प्रेषित किया जा सकता है ़ बहुत से उपयोगकर्ताओं स्काइप, व्हाट्सअप्प, फेसबुक, गूगल मेल, ब्लॉगर, वर्डप्रेस और ड्रॉपबॉक्स का उपयोग बातचीत करने, डेटा संग्रह करने, इन्टरनेट मीडिया संचार से उनके कामको सहयोग और बढ़ावा देनेके लिए करते है ़

लेकिन इन उपकरणोंके उपयोगके साथ जोखिमों जुड़े हुए है और हम सबको सबसे बुरी स्थितिके लिए तैयार रहनेकी जरुरत है ़ चलो, हम इन लोकप्रिय सेवाओं, उनके जोखिमों और संभावित ज्यादा सुरक्षित विकल्पों पर नजर डालें ़

स्काइप के माध्यमसे जोखिमों : स्काइप हमेशा उसके शुरूसे अंत तक एन्क्रिप्शनके कारण सुरक्षित माना जाता था ़ इसी समयमें खुलासों द्वारा प्रकट हुआ कि शझछ २०११ से स्काइप सुनती आ रही है और यह स्पष्ट नहीं है कि अन्य एजेंसियों किस हद तक सेवाओंका अवरोध करनेमें सक्षम है ़ एरिक किंग, प्राइवेसी इंटरनेशनल के अनुसंधान मुखियाके मुताबिक भी" स्काइप पर उपयोगकर्ताकी गोपनीयताकी रक्षा करनेके लिए अब भरोसा नहीं कर सकते" ़

संभव समाधान: स्काइपका उपयोग सार्वजनिक मंचकी तरह करें ़ जो कुछ आप कहते या लिखते है उसका आपके विरुद्ध उपयोग किया जा सकता है ़

विकल्पों : जित्सी (एन्क्रिप्टेड टेक्स्ट, वोइस और विडियो मैसेजिंग), लिनफोन (एन्क्रिप्टेड वोइस और विडियो चैट), मुम्बल (एन्क्रिप्टेड वोइस चैट) ़

व्हाट्सअप्प

व्हाट्सअप्प दुनियामें सबसे लोकप्रिय मैसेजिंग अप्समें से एक है ़ वह आपको जसज सेवाओंके लिए भुगतान किए बिना संदेशे भेजने देता है, हालांकि जिस व्यक्तिको आप भेज रहे हो वह भी व्हाट्सअप्पका उपयोग करता होना चाहिए ़ यह एक आसान रास्ता है न्यूज़ स्रू और सहयोगियों के साथ जब क्षेत्रमें हो तब संपर्कमें रहनेका , खास तौर पर जैसे आप छबियों , विडिओ और ऑडियोका आदानप्रदान कर सकते हो ़

व्हाट्सअप्पके साथ जोखिमों : वर्तमानमें व्हाट्सअप्प दावा करता है कि संदेशे एन्क्रिप्टेड है लेकिन क्योंकि कंपनी यह नहीं कह रही कि कौन सी पध्दतिका उपयोग कर रही है, यह कहना मुश्किल है कि सेवा कितनी सुरक्षित है ़ ऐसे रिपोर्ट्स है कि वाईफाई और अन्य सार्वजनिक चैनलों पर से भेजे गए व्हाट्सअप्प संदेशे डिक्रिप्ट हो सकते है ़ व्हाट्सअप्पको ज्यादा सुरक्षित कर सकें ऐसे अप्प्स यहाँ है ़

संभव समाधान : ज्यादा सुरक्षित अप्प्सका सहारा लें

विकल्पों : ैगयैह (ऑफ-ध-रेकॉर्ड मैसेजिंग), ंभिरचा (गुमनाम २ चैट), भरचाझीबेीं (पहले क्षैममीर्मा) और एंड्राइड के लिए ठचममीं ़

फेसबुक

इन्टरनेट के अधिकांश उपयोगकर्ताओं इस वैश्विक सामाजिक नेटवर्कका उपयोग उनका काम, भीड़ स्त्रोत जानकारी, सहयोगीओं और चर्चित लोगोंके संपर्कमें रहने, कंपनीयों को अनुसरने, उनकी धडकन पर समाचार, महत्वपूर्ण लोगोंकी सदस्यता लेने और समूहोंमें भाग लेने के लिए करते हैं ़

फेसबुक विशाल डेटा संग्रहकर्ता है ़ आपके मित्रोंकी सूचि स्थानिक अधिकारीयोंके आपको निश्चित क्षेत्र में काम करनेके लिए विसा देना कि नहीं निर्णयको प्रभावित कर सकता है और जिन खुले समूहोंमें आप सभ्य है वह अजनबियोंको आपकी रूचि जानने देता है, आपका प्रोफाइल बाहरी आगन्तुको के लिए बंद हो फिर भी ़ फेसबुक भी निरंतर नजर रखने के नए तरीकोंके साथ प्रयोग कर रही है ़

संभव समाधान : फेसबुक पर जानकारी प्रसिद्ध करते वक्त सचेत रहें ए एक बार यह ऑनलाइन है, आप इसका नियन्त्रण खो देते हैं ए आपके फेसबुक पेजके उपरी दायाँ कोना पर प्राइवेसी सेटिंग पर जाये और खात्री करें कि आपने सभी एहतियाती उपाय किये है ए जब आप कंप्यूटर पर अन्य वेबसाइट सर्फिंग कर रहे हो, हमेशा फेसबुक पेजसे लॉगआउट करने की कोशिश करें ए

ट्विटर

ट्विटर ताज़ा खबरका अनुसरण करने और खुद ताज़ा खबर बननेके लिए अच्छा है ए आप इसका उपयोग दूसरोंके साथ सहयोग करने, समुदायोंको खोजने और प्रवृत्तियों और विषयोंको अनुसरने के लिए कर सकते हैं ए

ट्विटर पर आप जो कुछ करते हैं वह दिखाई देता है ए अगर आपने जिओटैगिंग सक्षम किया है, आपका पता लगाना बहुत आसान हो सकता है ए यह सेवा दुर्भावनापूर्ण हमलोंके लिए स्वर्ग समान है ए

संभव समाधान : आप क्या पोस्ट करते हैं और किसको फॉलो करते हो उस बारेमें सचेत रहें ए खुली सूचि मत बनायें अगर आप एकदम पक्के हैं कि ऐसा करने से आप कोई मुश्किलमें नहीं आयेंगे ए जिओटैगिंग अक्षम करें

इन्टरनेट मीडिया संचार के बारे में अधिक जानकारीके लिए ब्राउज़र और सर्च इंजन विभागोंका उल्लेख करें

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

TIPS FOR USING E-MAIL SAFELY

Never share your e-mail id and passwords with unknown persons

Never give your official e-mail id for freebies on Internet

Be careful while downloading attachments from e-mails to your computer. Scan the attachments with updated antivirus before downloading

Do not click on links and avoid filling forms received by e-mail asking for personal information from unknown persons

ऑनलाइन खेलों

ऑनलाइन खेल एक खेल है जो इन्टरनेटके माध्यमसे कंप्यूटर नेटवर्क पर खेला जाता है | ऑनलाइन खेलकी श्रेणी साधारण टेक्स्ट आधारित से ले कर चित्रात्मक खेलों तक है | खिलाडीयों एक साथ वही खेल खेल सकते हैं | ऑनलाइन खेलोंका मुख्य लाभ एक ही खिलाडी ऑनलाइन होनेके बावजूद विभिन्न खेलोंसे जुडनेकी क्षमता है | टेक्नोलॉजी आधारित खेलों ज्यादा जटिल बन रहे हैं, टेक्नोलॉजी संबंधित खेलों जैसे फ़्लैश गेम्स और जावा गेम्स ज्यादा लोकप्रिय हुए |

यहाँ बीनामोल खेलों और व्यावसायिक खेलों है, ज्यादातर खेलोंके साथ अंतिम उपयोगकर्ता लाइसेंस समजौता संलग्न है और पहुँच खेलों के रचनाकारों तक सिमित है और समजौता भंग चेतावनीसे ले कर समाप्ति तक है |

ऑनलाइन जुआ भी अब काफी लोकप्रिय है | लोग कैसिनो जैसे खेल , लोटरिज़ खेलते हैं और स्पोर्टिंग घटनाएं पर शर्त लगाते हैं | जुआ के किसीभी रूपकी तरह जोखिमोंमें लत और खेलमें लगाए किसी भी राशिका तेजीसे संभावित नुकशान शामिल है |

यहाँ बड़े पैमाने पर मल्टीप्लेयर ऑनलाइन खेलों जैसे वास्तविक समय रणनीति खेलों, भूमिका निभाना खेल, पहले व्यक्ति शूटर खेल और दुसरे बहुत ज्यादा क्योंकि नयी टेक्नोलॉजीओं और तीव्र गति इन्टरनेट कनेक्शनने ऑनलाइन जुआको मदद की है | क्योंकि खेलनेवाले बड़ी राशि और समय आजके जटिल खेलोंमें निवेश करते हैं, दुसरे शरारत या अवैध लाभका अवसर देखते हैं | ऑनलाइन खेलोंके टेक्नोलॉजीकल और सामाजिक जोखिमोंको जो किसीको भी इसमें आनंद मिलता है उनको समझ लेना चाहिए | इसमें निम्नलिखित शामिल है :

- अनजान व्यक्तिओंसे सामाजिक संपर्कके जोखिमों जो आपको छलसे निजी और वित्तीय जानकारी दर्शानेके लिए फांसे
- कंप्यूटर घुसपैठियोंसे जोखिमों जो सुरक्षा भेद्यताका लाभ उठाएं
- ऑनलाइन और असली दुनियाके शिकारियोंसे जोखिमों
- वायरसीस, ट्रोजन हॉर्सेज, कंप्यूटर वर्म्स और स्पाईवेयरसे जोखिमों

ऑनलाइन जुआ खेलनेका जोखिम

आजके ऑनलाइन गेमिंग वातावरणमें बहुत सारे विकल्प उपलब्ध हैं | मेसिव मल्टीप्लेयर ऑनलाइन रोल प्लेयिंग गेम्स खेलोंके लोकप्रिय प्रकारके स्वमें उभरे हैं | ज्यादातर खिलाडीयोंको खेल के पात्रोंके स्वमें ऑनलाइन पहचान बनानेकी अनुमति देती है जो आभासी साहसोंमें भाग लेते हैं, जो कभी कभी वास्तविक दुनियामें पार कर जाते हैं | उदाहरणके तौर पर खेलनेवाले आभासी खेल वस्तुओंको बाजारमें वास्तविक दुनियाके पैसोंके बदलेमें बेचते हैं जैसेकि फ्लिप्काट , अमेज़ोन वि. | कुछ खेलोंमें, उपयोगकर्ताकी बनायी आभासी दुनिया है जहाँ लोग वास्तविक मुद्राका उपयोग उनकी ऑनलाइन दुनियामें निजी संपत्ति बनाने या खरीदनेके लिए करते हैं | इसने नए प्रकारकी " वर्चुअल क्राइम" कही जाने वाली आपराधिक गतिविधिके लिए अवसर बनाया |

आम तौर पर ऑनलाइन गेमिंगमें सामाजिक और टेक्नोलॉजीकल दोनों जोखिमों शामिल हो सकते हैं | इस प्रकार बहुतसे ऑनलाइन गेमिंग जोखिमों उसके समान है जिसका कंप्यूटरका उपयोग करनेवालेको पहले से ही सामना करना पड़ा हो, लेकिन उनको यह एहसास नहीं हुआ होगा कि खेलों उनकी गोपनीयता और कंप्यूटर सुरक्षाके समजौताका एक और अवसर देता है |

आप सॉफ्टवेर,गेम्स,बुक्स वि.डाउनलोड करें तब कॉपीराइट समस्याओं से सावधान रहें

टेक्नोलॉजी जोखिमों	सामाजिक जोखिमों
दुर्भावनापूर्ण सॉफ्टवेर • वायरस संलग्नक रूपमें साज़ा किये हुए ईमेल घज द्वारा संदेशों या इंस्टेंट मैसेजिंग प्रोग्राम्स द्वारा आ सकते हैं • दुर्भावनापूर्ण प्रोग्राम्स आपके डाउनलोड किये गेम फाइल्समें छिपे हो सकते हैं या स्थापित किये सॉफ्टवेरमें | • दुर्भावनापूर्ण व्यक्तिओं भी ऑनलाइन खेलोंसे जुड़े हुए सोशल नेटवर्कसका लाभ उठा सकते हैं जो चेट,ईमेल या वोइस कम्युनिकेशन पर आधार रखते हैं • वे फिर इस सॉफ्टवेरका उपयोग विविध प्रकारके अवैध प्रयोजनोंके लिए करते हैं | **असुरक्षित या समजौता किए हुए गेमर सर्वरों** • गेमर चिंताओं: अगर गेम सर्वरके सॉफ्टवेरके साथ समजौता किया हुआ है, जो कंप्यूटर उससे जुड़ते हैं उनके साथ भी समजौता हो सकता है | • कमजोरियोंका शोषण करके, दुर्भावनापूर्ण उपयोगकर्ताओं आपके कंप्यूटरको दूरसे नियंत्रित कर सके और दुसरे कंप्यूटरों पर हमला कर सके या ट्रोजन हॉर्सेज,एडवेयर या स्पाईवेयर जैसे प्रोग्राम्स स्थापित करे जिससे आपके कंप्यूटर परसे निजी जानकारी तक पहुँच सके | **असुरक्षित गेम कोडिंग** • कुछ खेल प्रोटोकॉल मशीनोंके बीच खेल जानकारी पहुँचानेके तरीकों-दुसरे प्रोटोकॉलकी तरह सुरक्षित रूपसे कार्यान्वित नहीं | खेल कोड ज्यादा लोकप्रिय कमर्शियल सॉफ्टवेरकी तरह छानबीन न किया हो सकता है |	**सामाजिक इंजीनियरिंग** दुर्भावनापूर्ण व्यक्तिओं आपके कंप्यूटर पर सॉफ्टवेर स्थापित करनेकी चालमें फंसानेकी कोशिश कर सकते हैं जो वे आपके कंप्यूटरको नियंत्रित करने,आपकी ऑनलाइन गतिविधियों पर नजर रखने या दुसरे कंप्यूटर पर हमला करनेमें उपयोग कर सकते हैं॰ उदाहरणके लिए वे आपको जाली वेबसाइट पर ले जा सकते है जो फर्जी पैचेज या गेम डाउनलोडका प्रस्ताव करते है, वास्तवमें दुर्भावनापूर्ण सॉफ्टवेर है **पहचानकी चोरी** अगर कोई दुर्भावनापूर्ण व्यक्ति गेम्समें आपके बनाये प्रोफाइल और अन्य स्त्रोतोंसे आपके बारेमें जानकारी एकत्रित कर सकता है तो वह आपके नाममें एकाउंट स स्थापित करने,फिरसे बेचने या आपके वर्तमान वित्तीय एकाउंट्स तक पहुँचनेके लिए उसका उपयोग कर सकता है | **साइबर वेश्यावृत्ति** ध सिम्स ऑनलाइन खेलमें षष', एक साइबरवेश्यालय १७ वर्षीय लड़के द्वारा खेल डफछशक्षडर्शिडका उपयोग करके विकसित किया गया था ४ ग्राहकोंने साइबरसेक्स के लिए मिनटसे सिममनीका (झैर्सनीचहज)भुगतान किया **आभासी लूट** "आभासी लूट" शब्द ग़ढा गया जब लाईनेज के कुछ खिलाडीयोंने दुसरे खिलाडीके पात्रोंको हराने और उनकी वस्तुओं लेनेके लिए सॉफ्टवेर एप्लीकेशनका उपयोग वेब पर चलानेके लिए किया, बोट्सको बुलाया | **आभासी स्वेटशॉप** कुछ ऑनलाइन खेलोंकी आभासी अर्थव्यवस्थाओं और आभासी वस्तुओं और मुद्राका असली पैसेके लिए विनिमयने आभासी स्वेटशॉप को पैदा किया, जिसमें नयी ऑनलाइन अर्थव्यवस्थासे मुनाफा कमानेके नए रस्ते खोजनेवाले लोगोंके द्वारा तीसरी दुनियाके देशोंके कामगारों का आर्थिक रूपसे शोषण होता है

गेम्स डाउनलोड करते वक्त दर्ज करनेवाली वस्तुओं

- ऑनलाइन खेलकी रेटिंग जाँच करें, वे लोग अक्सर आपको सूचित करेंगे कि वह आपकी उम्रके लिए उचित है कि नहीं |
- आप जो साईटका उपयोग करते हैं उसके नियमों और शर्ते पढ़े और जाँच करे कि बच्चोंके लिए विशेष सुरक्षा विशेषताओं है कि नहीं |
- यह महत्वपूर्ण है और खात्री करें कि खेल विकेता प्रतिष्ठित है और भरोसापात्र वेबसाइटसे गेम डाउनलोड करें |
- कभी कभी मुफ्त डाउनलोड की हुई गेम्स दुर्भावनापूर्ण सॉफ्टवेर छिपाती है, जिसमें खेलको चलानेके लिए जरुरी प्लग-इन्स शामिल है |खेलको खोलनेके लिए व्यवस्था मोड उचित नहीं है, ऐसा करनेसे अपने आपको जोखिमके सामने खुला कर देते हो, जिसे हमलावर आपके कंप्यूटर पर पूरा नियन्त्रण कर लेता है | उपयोगकर्ता मोड़में खेलना व्यवस्थापक मोड़में खेलनेसे हमेशा सुरक्षित है |
- ऑनलाइन गेम खेलनेका सबसे अच्छा तरीका गेम साईट पर खेलना है, अंतमे दुर्भावनापूर्ण वेबसाइट पर जानेका जोखिम कम हो सकता है |

ऑनलाइन खेलोंके लिए मार्गदर्शन

- ऑनलाइन गेम्स साइनिंग अप करनेके लिए परिवार ईमेल ऐड्रेस बनाएं ए स्क्रीनशोट्सः ऑनलाइन खेल खेलते वक्त अगर कुछ बुरा होता है, कीबोर्ड परका "प्रिंट स्क्रीन" बटन दबा कर स्क्रीन पर दिखाई गयी वस्तुओंका स्क्रीनशॉट लें और संबंधित वेबसाइटको जान करे और स्क्रीनशॉटको सबूतके स्वमें पेश करे |
- एंटीवायरस और एंटीस्पाईवेयर प्रोग्राम्सका उपयोग करें |
- ईमेल मेसेजीस या इंस्टेंट मैसेजिसके साथ संलग्न फाइल्स खोलनेमें सावधानी बरते |
- डाउनलोड की हुई फाइल्स और नए सॉफ्टवेरकी सत्यता और सुरक्षा जांचें |
- आपके वेब ब्राउज़रको सुरक्षित आकार दें ए फ़ायरवॉलका उपयोग करें |
- आपका यूजर प्रोफाइल स्थापित करे जिसमें आपकी उम्र के किसी के लिए उपयुक्त भाषा और खेल सामग्री शामिल हो |
- बच्चोंके लिए समयमर्यादा तय करें |
- अनजान वेबसाइटसे कभी भी सॉफ्टवेर और गेम्स डाउनलोड न करें |
- वेबसाइटोंमें लिंक्स, इमेजेज और पॉपअप्स पर क्लीक करनेमें सचेत रहें क्योंकि इसमें वायरस हो सकते हैं और कंप्यूटरको हानि पहुंचा सकते हैं |
- गेम्स डाउनलोड करते वक्त इन्टरनेट पर कभी भी निजी जानकारी न दें |
- कुछ मुफ्त खेलोंमें वायरस शामिल हो सकते हैं, इसलिए सचेत रहें और उन्हें डाउनलोड करते वक्त उल्लेख करें ए
- शक्तिशाली पासवर्ड बनाएं और उपयोग करें |
- आपके एप्लीकेशन सॉफ्टवेरको पैच और अद्यतन करें |

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/

सोशल नेटवर्क के संबंध में

सोशल नेटवर्क वह सामाजिक ढांचा है, जो कुछ गाँठों के द्वारा निर्मित है, जो एक या अधिक प्रकार की पारस्परिक निर्भरता जैसे कि मूल्य, दृष्टिकोण, विचार, वित्तीय विनिमय, मित्रता, नापसंदगी, संघर्ष या व्यापार से बंधी हुई हैं सोशल नेटवर्क के इस्तेमाल में आनंद है, नौकरी प्राप्त करने में मददगार है एवं दोस्तों व व्यवसायिक संपर्कों व रिश्तेदारों से संबंध रखने हेतु भव्य है

सोशल नेटवर्क का दूसरा पहलू है सुरक्षा व निजता का मुद्दा और इस बारे में दो विभिन्न मुद्दों पर इसमें निपटा जाता है सुरक्षा मुद्दे में तीसरे व्यक्ति को अप्राधिकृत रूप से संरक्षित स्त्रोतों के द्वारा जानकारियों तक पहुँच मिलती है और निजता के मुद्दे के अंतर्गत कोई मात्र आपको देखकर कि आप अपना क्या पासवर्ड टाईप कर रहे हैं, उसके द्वारा वह गोपनीय जानकारियों तक पहुँच सकता है लेकिन दोनों ही प्रकार के उल्लंघन अक्सर एक दूसरे में सोशल नेटवर्क पर गुंथे हुए होते हैं, विशेषकर इसलिए क्योंकि वह कोई भी जो नेटवर्क का उल्लंघन करता है वह आसान पहुँच के लिए दरवाजे खोल देता है, जिससे किसी भी उपयोगकर्त्ता की व्यक्तिगत जानकारियों तक पहुँच आसान रहे इसके पीछे कारण यह है कि सोशल नेटवर्क में सुरक्षा व निजता की चूकें होती हैं, क्योंकि साईट्स में जानकारियों की जिस मात्रा पर प्रतिदिन संसाधन होता है और उसे अंत में आसान बना दिया जाता है, जिससे सिस्टम में कभी यदि एक भी चूक रहे, तो उसका दोहन करना आसान हो विशिष्टताएँ जिससे उपयोग करनेवाले सहभागी आमंत्रित होते हैं, वे हैं संदेश, निमंत्रण, फोटो, खुले मंच के एप्लीकेशंस आदि ये अक्सर वे मार्ग होते हैं, जिसके द्वारा निजी जानकारियों तक पहुँच हो जाती है

सोशल नेटवर्किंग साइट्स की लोकप्रियता विस्मित कर देने के स्तर तक बढ़ी है फेसबुक, ट्विटर व लिंकेडीन जैसी साईट ्स की उपयोगिता के संबंध में कोई विवाद नहीं है इनका इस्तेमाल व्यवसायिक नेटवर्किंग व नौकरी की शोध के लिए व बिक्री की आय बढ़ाने के लिए, एक साधन की तरह किया जा सकता है, जिससे लोगों को सुरक्षा व अन्य मुद्दों पर जागरूक रखा जा सके या एक मार्ग की तरह हो सके जिससे मित्रों से एक बार पुनः जुड़ सकें

सोशल नेटवर्किंग के उपयोग

- पूरी दुनिया में लोगों से ऑनलाईन मुलाकात करना
- उन लोगों से मित्रता करना जो बहुत दूर रहते हैं
- प्रोफाईल तैयार करना
- स्वयं प्रस्तुति
- अध्ययन या शिक्षण, वर्तमान हलचल, क्रीड़ा, व्यवसाय, परिवहन, सिनेमा, अद्यतन समाचारों की नवीनतम बातें, कार्यक्रमों की घोषणा, विचारविनिमय आदि से संबंधित जानकारियों का विनिमय/ साझेदारी
- डाटा फाईल्स, वीडियोज, संगीत व फोटो को साझा करना

सोशल नेटवर्किंग की जोखिम व चुनौतियाँ

पूरी दुनिया के अरबों लोग पुराने मित्रों से मिलने व नए मित्र बनाने , जानकारियाँ एकत्रित करने व उन्हें साझा करने हेतु इस मीडिया का उपयोग हो रहा है और उस वजह से आज की इंटरनेट की दुनिया में सोशल नेटवर्किंग एक लोकप्रिय गतिविधि हो गई है और यद्यपि सोशल नेटवर्किंग एक लोकप्रिय मीडिया है, लेकिन इससे संबंधित नुकसान भी बहुत हैं

ये साईट्स घोटाले करनेवाले या हेकर्स के द्वारा हथियाई जा सकती हैं, जिससे उपयोगकर्ताओं की गोपनीयता की हानि व पहचान की चोरी हो जाती है उभरते बच्चों में विशेष रूप से सोशल नेटवर्किंग साइट्स बहुत लोकप्रिय हो रही हैं

ये साइट्स बच्चों को विभिन्न प्रकार की जोखिमों, जैसे कि ऑनलाईन धमकी, व्यक्तिगत जानकारियों को उजागर करना, साईबरधोखे, अनुपयुक्त विषयसामग्री तक पहुँच, ऑनलाईन संवरना, बालदुष्कर्म आदि से सामना करवाती हैं इसके अलावा और भी कई अन्य जोखिमें हैं, जैसे कि गलत जानकारियों के साथ फर्जी प्रोफाईल, दुर्भावनापूर्ण उपयोग, स्पाम व जाली लिंक्स, जिनसे फिशिंग हमले आदि होते हैं

- **गैरकानूनी विषय सामग्री**

  वह कोई भी जो सोशल नेटवर्किंग या मीडिया साइट्स पर पहुँचता है, वह जानबूझकर अनुपयुक्त विषयसामग्री नहीं चाहता होगा, लेकिन असावधानी से ऑललाईन पहुँचने या शोध के दौरान या वे उस तक पहुँच जाते हों या वे वह सामग्री चाहते हों या दूसरों ने वह विषयसामग्री संदर्भित की हो

  इन विषयसामग्री में शामिल होते हैं यौन प्रकटीकरण, यौन दुष्कर्म, हिंसा, आपराधिक गतिविधियों या दुर्घटनाओं के वीडियोज से अवैध चित्र , वे जो राजनैतिक रूप से चरमदृष्टिकोण को प्रोत्साहित करते हैं और जिनका उपयोग संभवित रूप से जाति, धर्म, लिंगप्राथमिकता या अन्य सामाजिक/ सांस्कृतिक कारकों के कारण समुदाय के संवेदनशील लोगों को कट्टर बनाने में इस्तेमाल किया जाता हो ऑनलाईन विज्ञापन का प्रकटीकरण भी हो सकता है, जो वयस्कों की विषयसामग्री को प्रोत्साहित करती हो

  साइट्स पर की अवैध विषयसामग्री में होते हैं बालदुष्कर्म के चित्र व गैरकानूनी घृणास्पद भाषण साइट्स पर उम्र के अनुसार अनुपयुक्त विषयसामग्री जैसे कि अश्लील या यौनिक विषय सामग्री, हिंसा या अन्य वयस्कों के उपयुक्त ऐसी विषयसामग्री जो छोटे लोगों के लिए अनुपयुक्त हो और वे इस प्रकार की विषयसामग्री को स्मार्ट फोन पर तलाश कर सकते हैं, लेकिन उन्हें घर से व शाला के इंटरनेट फिल्टर के द्वारा अवरुद्ध किया जा सकता है

- **स्पाम**

  जैसा कि हम जानते हैं कि स्पाम सामन्यतः अवांछित ईमेल होते हैं, जिन्हें किसी उत्पाद के विज्ञापन के तौर पर सूचीबद्ध ईमेल्स पर या ईमेल पतों के समूह को भेजा जाता है इसी प्रकार स्पामर्स अवांछित मेल्स या सन्देश अरबों सोशल नेटवर्किंग साइट्स के उपयोगकर्त्ताओं को भेजते हैं, जो मुफ्त होते हैं या स्पामर्स की आसान पहुँच में होते हैं, जिससे कि असंदिग्ध उपयोगकर्त्ताओं की व्यक्तिगत जानकारियाँ एकत्रित की जा सके

  सामाजिक स्पाम वह अवांछित स्पाम की विषयसामग्री है, जो किसी भी वेबसाईट के सोशल नेटवर्क्स पर उपयोगकर्त्ता के द्वारा तैयार विषयसामग्री (टिप्पणियाँ, गपशप आदि) के साथ प्रकट हो जाती है इसे कई प्रकार से अभिव्यक्त किया जा सकता है, जिसमें संदेशों का अम्बार, अपमान, घृणास्पद वक्तव्य, दुर्भावनापूर्ण लिंक्स, फर्जी समीक्षाएँ, जाली मित्र व व्यक्तिगत रूप से पहचानी जानेवाली सूचनाएँ सम्मिलित होती हैं

  सोशल नेटवर्किंग साईट्स पर संदेशों का अम्बार, टिप्पणियों का वह सेट होता है, जो उसी रूप में होते हैं या बहुत

कुछ समान विषयवस्तु के साथ उसकी बारंबार आवृत्ति की जाती है ये सन्देश जिन्हें स्पामबम्ब भी कहते हैं, ये ऐसे आ सकते हैं, मानो एक स्पामर दोहरे संदेशों को बहुत कम समय में लोगों के एक समूह में या एक ही समय कई सक्रिय स्पाम खातों में भेज देता है, दोहराए संदेशों की प्रविष्टि की तरह

गालीगलौज, अशिष्ट या असंबंधित भाषा उपयोगकर्त्ता के द्वारा प्रस्तुत कठिन या अस्पष्ट टिप्पणियों को निंदा या गाली या अशिष्ट या असंबंधित भाषा के रूप में वर्गीकृत किया गया है सामान्य तकनीक में अक्षरों के स्थान पर चिन्हों व अंकों का इस्तेमाल कर विचारों के छिपानेका कार्य शामिल है ये खराब शब्द फिर भी इंसान की आँख से पहचाने जा सकते हैं, यद्यपि गलत वर्तनी के कारण वेबसाईट्स के नियंत्रक द्वारा इसमें चूक हो जाती है

किसी विशेष व्यक्ति या व्यक्तियों के विरुद्ध उपयोगकर्त्ता के द्वारा प्रस्तुत वे टिप्पणियाँ जिनमें हल्की या गंभीर अपमानजनक भाषा है इन टिप्पणियों में हल्के से नाम पुकारने से लेकर गंभीर धौंस तक की श्रेणी होती है ऑनलाईन धौंस देनेवाले आपसी बातचीत में अक्सर अपमान का उपयोग करते हैं, जिन्हें साईबर धौंसबाजी के नाम से संदर्भित किया जाता है पर्दे के पीछे से छिपकर लिए जानेवाले नाम के द्वारा उपयोगकर्त्ता कमीना कहता है और इसमें गुमनामी के साथ अपमानजनक टिप्पणियाँ होती हैं और ये धौंसबाज अपनी टिप्पणियों व कार्यों के लिए मुश्किल से ही कभी जवाबदारी वहन करते हैं

- **धमकी**

उपयोगकर्त्ता के द्वारा प्रस्तुत हिंसा की धमकियाँ किसी व्यक्ति या समूह के विरुद्ध वे टिप्पणियाँ होती हैं, जिसमें शारीरिक हिंसा के लिए हल्की या कठोर धमकी शामिल होती है यह तुरंत ही जातिगत बहाव में तब्दील हो सकती है और अपमानजनक टिप्पणियों व दूसरों के समक्ष धमकियों के द्वारा उत्तेजना फैलाई जाती है सामाजिक स्पाम का यह बहुत गंभीर उदहारण है

आप जब कोई अनुरोध स्वीकार करें , तब उस व्यक्ति की प्रामाणिकता की सदैव जाँच करें

- **घृणास्पद वक्तव्य**

  उपयोगकर्त्ता के द्वारा प्रस्तुत घृणास्पद कथन व टिप्पणी होती है, जिसमें कठोर आपराधिक विषयवस्तु शामिल होती है और जो किसी विशेष जाति, लिंग, यौनिक रूझान आदि के लोगों के लिए संबोधित होती हैं

- **दुर्भावनापूर्ण लिंक्स**

  उपयोगकर्त्ता के द्वारा प्रस्तुत टिप्पणियों में वे दुर्भावनापूर्ण लिंक्स हो सकते हैं, जो अनुपयुक्त ढंग से उपयोगकर्त्ता को या कंप्यूटर को नुकसान पहुँचाते है, भ्रमित करते हैं या क्षतिग्रस्त करते हैं ये लिंक्स अधिकांश रूप से विडिओ मनोरंजन की साईट्स जैसे कि यू ट्यूब्स आदि पर सामान्य रूप से पाई जाती हैं क्या होता है जब आप किसी दुर्भावनापूर्ण लिंक्स को क्लिक करते हैं, जिसकी श्रेणी मालवेयर से आपके साधन की डाऊनलोडिंग तक रहती है और जिससे आपको उन डिजाईन की गई साईट्स की ओर निर्देशित कर दिया जाता है, जहाँ से आपकी व्यक्तिगत जानकारियों को चुराया जाता है तथा अनजान उपयोगकर्त्ताओं को छिपाए गए विज्ञापन के अभियानों में सहभागिता हेतु आकर्षित किया जाता है

  उपयोगकर्त्ता के लिए मालवेयर बहुत खतरनाक हो सकता है और यह कई रूपों में अभिव्यक्त हो सकता है वायरस, कीटाणु, स्पायवेयर, ट्रोजन हार्स या एडवेयर साफ्टवेयर के इस्तेमाल या उसके संस्थापन के समय दुर्भावनापूर्ण उपयोग विभिन्न एप्लीकेशन के द्वारा हो सकता है इसी प्रकार सोशल नेटवर्किंग एप्लीकेशन पर क्लिकिंग करने से एप्लीकेशन के संस्थापन की प्रक्रिया शुरूहो जाती है या विडिओ अदि देखने के लिए लिंक मिल जाती है इच्छित संचालन को पूरा करने हेतु एप्लीकेशन का अनुरोध उपयोगकर्त्ता की ओर से मेरी बुनियादी जानकारियों तक की पहुँच के लिए, मेरी दीवार को अद्यतन करने के लिए, मेरी दीवार पर चिपकाने आदि जैसी कुछ उन्नत सुविधाओं के लिए होता है

- **त्तोंझात्तँद्र द्धिांफ्रिं नद्दाबिांख्रुं:**

  गिं नकिंत्थाच द्धा नेंद्रा द्धा ग ज्ञाथर्गिं र्किथ वथ्रद्धोंठ्ठग मौंत्रैं गें ळाछा नद्दाबिांख्रुं, ठ्ठिाथ्र्ज्ञोंथें द्वान्तद्वा दों क्तग ा ग द्राकिन्तेंद्दाद्या ज्ञथिर्ज्ञगिं द्धाप्र द्धों त्रूनछ वत्थाच द्धा नेंद्रा गें द्दार्द्धिाग ळाछा थ्रैन्तर्तिं गिं रु ड्ढातें ज्ञैं, ड्ढों नग छाात्दाग नद्दाबिांत्रैं ठठद्राौंद्रें थ्रछ नद्दाबिांख्रुं" गें द्धिांरु द्वाचें ग छतें ज्ञैंप्र गर्गिं र्ग र्थिंथद्धा वन नद्दान्द्धा ग गों ज्ञद्या ग छथें ज्ञैंतथ्रैंद्धान ग छतें ज़ैरु वथ्रद्धोंठ्ठग मौंत्रैं ग गों ड़ोंताद्वाथर्थ चैंतज्ञैं गिं नद्रा नेंद्दाबिांख्रुं थ्रौंद्दार्णिंग थज्ञर्गिंज्ञैंप्र

- **धोखाधड़ीयुक्त समीक्षाएँ**

  ड्ढाद्यानाड्ढा द्दिांभ्र तदृा ज़ों ड्ढातें ज्ञैं, ड्ढादृा ग व्र ड्ढाद्यार्गि द्दिांभ्र ड्ढाँर्द्दि ड्ढातें ज्ञैं द्धा ठठर्द्दिांभ्र" दृाथ ड्ढातें ज्ञैंप्र द्धों वथ्रद्धोंठ्ठग मौं द्धा न्थ्राद्दा दृाणैन्न थ्रर्ष्टिुं त झार्तो ड्ढोंनें गिं द्यार्गि थ्रिैद्धा थ्रैंर्तिर्श्रित द्यार्गिठ्ठों द्धा नार्द्वाड्ढार्थिग ज़न्तिद्धों ग ा त्रूनिंछण ग छ त्रूनछ थ्रैंन्नना थ्रौंथ्रत ग छथें ग र्गि गेंन्निन्न ग छत ज्ञैंप्र द्धार्चि द्वाज़ झातेंद्वाद्याा थ्रर्थिं न्थ्राद्दाछ ग ा त्रूनिंछण ग छता ज्ञैं, तदृा द्वाज़ न्थ्रैंद्दा झातें ग गों द्वोंत्तता थ्रैंचथ ग छता ज्ञैं त्रूंछ वन तछज़ द्वाज़ वनें त्रूंछ थर्गिनाथ ग छथें गें द्धाठ्ठुद्धा दृाथता ज्ञैंप्र

- **व्यक्तिगत रूप से पहचानी जानेवाली जानकारियाँ**

  किसी उत्पाद या सेवा या कहानी की उन उपयोगकर्त्ताओं के द्वारा समीक्षाएँ, जिन्होंने वास्तव में उसका कभी

इस्तेमाल ही नहीं किया ये अक्सर उत्पाद या सेवा के मालिक द्वारा प्रस्तुत किए जाते हैं, जो सकारात्मक समीक्षाओं भाड़े पर समीक्षाएँके लिए वादे करते हैं कुछ कंपनियाँ इस समस्या को हल करने हेतु प्रयास करते हुए उपयोगकर्त्ताओं को चेतावनी देती है कि सभी समीक्षाएँ प्रामाणिक नहीं हैं

जालसाज मित्र जालसाज मित्र तब हो जाते हैं, जब कई जाली मित्र जुड़ जाते हैं या मित्रबन जाते हैं ये उपयोगकर्त्ता या स्पाम बोट्स पुष्टिकृत खातों जैसे कि लोकप्रिय प्रतिष्ठित लोगों या सार्वजानिक हस्तियों का अनुसरण कर अक्सर प्रशंसा प्राप्त करने की कोशिश करती हैं यदि वह खातेवाला पुनः स्पामर का अनुसरण करता है, तब वह स्पैम खाते को वैधता प्रदान करता है और इस तरह वह उसे और नुकसान करने के योग्य बनता है

- **फिशिंग**

  जैसा कि हम सब जानते हैं कि फिशिंग हमला, मूल साईट की तरह ही जाली साईट का सृजन होता है इसी प्रकार इन दिनों यहाँ तक कि सोशल नेटवर्किंग फिशिंग भी विभिन्न रूपों में आई हैं, जैसे कि बैंक्स व लोकप्रिय व्यापार

इंटरनेट पर आपके, आपके परिवार के सदस्यों के या आपके मित्रों के चित्रों को पोस्ट करने के पहले दो बार सोच लें

याद रखें कि हैकर्स केवल आपके कंप्यूटर के लिए ही खतरा नहीं हैं, बल्कि वे आपके कंप्यूटर का इस्तेमाल कर दूसरे कंप्यूटर्स को भी नुकसान पहुँचा सकते हैं

गपशप के दौरान फाईल का अंतरण टालें, क्योंकि वह आपके सिस्टम को नियंत्रित कर सकता है

वर्ष 2014 के दौरान सोशल नेटवर्किंग के आँकड़े

८१७ के बीच के बच्चों में ४९ की ऑनलाईन प्रोफाईल है

१६ वर्ष से अधिक के युवाओं में २२ की ऑनलाईन प्रोफाईल है

वयस्कों की औसतन १.६ साईट्स पर प्रोफाईल है

८१७ के बीच के बच्चों में जिनकी प्रोफाईल है, उनमें से ६३ बेबो का उपयोग करते हैं

८१७ के बीच के बच्चों में जिनकी प्रोफाईल है, उनमें से ३७ मायस्पेस का उपयोग करते हैं

८१७ के बीच के बच्चों में जिनकी प्रोफाईल है, उनमें से १८ फेसबुक का उपयोग करते हैं

८१७ के बीच के बच्चों में जिनकी प्रोफाईल है, उनमें से ५९ नए मित्र बनाने के लिए सोशल नेटवर्क का उपयोग करते हैं

मातापिता में से १६ यह नहीं जानते हैं कि उनके बच्चे की प्रोफाईल सब देख सकते हैं

मातापिता में से ३३ कहते हैं कि उनके बच्चों द्वारा सोशल नेटवर्क के उपयोग हेतु उन्होंने कोई नियम नहीं बनाए हैं

बच्चों में से ४३ कहते हैं कि उनके मातापिता ने सोशल नेटवर्क के उनके उपयोग हेतु कोई नियम नहीं बनाए हैं

वेबसाईट्स पर फिशिंग हमले सोशल नेटवर्किंग फिशिंग फर्जी मेल्स व संदेशों के द्वारा आई है, जिसके द्वारा वे कुछ विशिष्टिकृत विचार, प्रोफाईल को अद्यतन करने व सुरक्षा/ विशेषताओं आदि को उन्नत करने के प्रस्ताव पेश करती हैं जो उन्नत किए गए हैं, उन्हें देखने के लिए, उपयोगकर्त्ता को एक लिंक का अनुसरण कर लॉग इन होना पड़ता है, जिसके द्वारा हमलावर विश्वास अर्जित कर लेता है मूल लॉग इन किए हुए पृष्ठ की जाली नक़्ल लिंक वाला पृष्ठ होता है और जो उपयोगकर्त्ता के खाते के विश्वास को चुराने पर केन्द्रित रहता है

- ### क्लिक जेकिंग

  सामान्यतः क्लिक जेकिंग वेब उपयोगकर्त्ताओं की एक दुर्भावनापूर्ण तकनीक है, जैसे कि गोपनीय जानकारियों को फिशिंग द्वारा उजागर करने हेतु फिशिंग या उनके कंप्यूटर पर तब नियंत्रण प्राप्त करना, जब उनके अहानिकर लग रहे वेब पृष्ठों पर क्लिकिंग कर रहे हों ब्राउसर्स व प्लेटफार्म्स की विविधताओं की अतिसंवेदनशीलता, एक क्लिक जेकिंग एक अंतःस्थापित कोड या स्क्रिप्ट का रूप ले लेती है और जो बिना उपयोगकर्त्ता की जानकारी के चल सकती है सोशल नेटवर्किंग के क्षेत्र में भी ऐसे ही होता है इस तरह के हमले के पीछे उद्देश्य होता है कि लिंक्स, आईकांस, बटन्स आदि पर क्लिकिंग के द्वारा उपयोगकर्त्ताओं के साथ चालाकी की जा सकती है और जो उपयोगकर्त्ता की जानकारी के बगैर पृष्ठभूमि में प्रक्रियाओं के चलाने के लिए प्रेरित कर सकते हैं

- ### व्यवहार

  यह इस बारे में है कि लोग जब ऑनलाईन होते हैं, तब उनका व्यवहार कैसा होता है, इसमें शरारत या उत्पीड़न (इस प्रकार के व्यवहार जैसे कि अफवाहें फैलाना, सामाजिक समूह में से समकक्षों को हटाना व मित्रता या स्वीकृति वापस लेना) व संभवित रूप से जोखिमयुक्त व्यवहार (इसमें शामिल हो सकते हैं, उदहारण के रूप में व्यक्तिगत जानकारियाँ उजागर करना, यौनिक उत्तेजनात्मक फोटोग्राफ्स पोस्ट करना, वास्तविक उम्र के बारे में झूठ बोलना या लोगों के साथ रूबरूमुलाकात की व्यवस्था करना, केवल जिनसे पहले ऑनलाईन मिल चुके हों) शामिल हो सकते हैं नेटवर्किंग साईट्स तीसरे पक्ष के एप्लीकेशन प्रोग्राम इंटरफेस (एपीआई) होते हैं, जिसके द्वारा निजी जानकारियों की आसानी से चोरी हो जाती है और फिर यह विकासक को और अधिक जानकारियाँ जैसे कि पते, चित्र तक की पहुँच दे देता है, जिनकी एप्लीकेशंस की जाँच के लिए जरूरत रहती है

सोशल नेटवर्किंग के लिए मार्गदर्शन

- स्वयं की व्यक्तिगत जानकारियाँ जैसे कि आपका नाम, पता, शाला/ घर का पता, फोन नम्बर, उम्र, लिंग, केडिट कार्ड के विवरण आदि न दें या पोस्ट करें
- आपके द्वारा जो जानकारियाँ ऑनलाईन पोस्ट की गई हैं, वे जो भी ऑनलाईन हों, उनके द्वारा देखी जा सकती हैं, क्योंकि इंटरनेट जानकारियों के विनिमय का दुनिया में सबसे बड़ा साधन है कई लोग जिनकी उस साईट तक पहुँच होती है, जिसका आप उपयोग करते हैं, वे आपके प्रोफाईल पर पहुँच सकते हैं और आपने जो भी जानकारियाँ पोस्ट की होंगी, उन्हें वे प्राप्त कर सकेंगे आपके प्रोफाईल तक जिनकी पहुँच है, उनमें शामिल हो सकते हैं जैसे कि आपके मित्र, अध्यापक और ख़राब लोगों में जैसे कि अनजान व्यक्ति
- सावधान रहे कि साईट्स पर आप जो जानकारियाँ देते हैं, वे आपको उत्पीड़न की जोखिम में डाल सकते हैं
- अपने मातापिता व पालक के अलावा अपना पासवर्ड अन्य किसी को कभी भी न दें

- अपने पासवर्ड को बारंबार बदलते रहें और उन लिंक्स को क्लिक करना टालें, जिसका तात्पर्य आपको वापस सोशल नेटवर्क साईट पर भेज देना हो इसके स्थान पर अपने ब्राउसर पर साईट का पता सीधे टाईप करें (या किसी पुस्तकचिन्ह का अनुसरण करें, जिसे आपने पहले सुरक्षित किया था), जिससे आप अपने खाते पर लौट सकें
- जब आप सोशल नेटवर्किंग साईट का चयन करें, तब निजता के मुद्दों पर अवश्य विचार करना चाहिए
- सोशल नेटवर्किंग साईट्स पर मित्रों को स्वीकार करते समय, ध्यान से चयन करें केवल उन्हीं लोगों को आपकी साईट के मित्रों में शामिल करें, जिन्हें आप वास्तविक जिंदगी में जानते हों
- किसी से भी ऐसे से व्यक्तिगत रूप से न मिलें, जिसे आप सोशल नेटवर्किंग साईट पर मिले हों, क्योंकि कुछ लोग ऐसे हो सकते हैं, जो वे वैसे न हों, जैसा वे बताते हों
- आप जिस व्यक्ति से नेटवर्किंग साईट पर मिले हों, उस व्यक्ति से यदि आप मिलना चाहते हों, तो अपने मातापिता की इजाजत लें
- अधिकांश सोशल नेटवर्किंग वेब साईट्स उपयोगकर्ताओं को सुविधा देती हैं कि वे गोपनीयता के नियंत्रण उन लोगों के लिए सेट कर सकें, जो आपकी जानकारियों को देख सकते हैं इसलिए ऐसी सुविधाओं को उपयोग में लेने की कोशिश करें
- कोई भी ऐसी सामग्री पोस्ट न करें, जिससे आपके परिवार की साख को नुकसान पहुँचता हो
- सोशल नेटवर्क साईट्स पर अनजान व्यक्तियों को फोटोग्राफ, वीडियोज व अन्य नाजुक जानकारियाँ पोस्ट न करें
- यदि आपको ऐसा लगता है कि आपके सोशल नेटवर्किंग खाते के विवरण साझा हुए हैं या चुराए गए हैं, तो अपने संदेह को तुरंत नेटवर्किंग साईट के सहयोगी दल को रिपोर्ट करें
- आपकी प्रोफाईल पर जो परेशान करनेवाली या असभ्यता से युक्त टिप्पणियाँ दी हों, उनका प्रत्युत्तर कभी न दें
- कोई भी अवांछित सन्देश या मित्रों को हटा दें, जो लगातार अनुपयुक्त टिप्पणियाँ छोड़ देते हैं और तुरंत ही ऐसी टिप्पणियों के बारे में नेटवर्किंग साईट को रिपोर्ट करें
- आपके मित्रों को नेटवर्किंग साईट्स पर वे सूचनाएं पोस्ट न करें, जो संभवतः उन्हें जोखिम में डाल सकती हैं समूह के फोटो, शाला का नाम, स्थल, उम्र, लिंग... आदि पोस्ट न कर आपके मित्रों को संरक्षण प्रदान करें
- आप नेटवर्किंग साईट्स पर जो योजनाएं व गतिविधियाँ करनेवाले हैं, उनके बारे में पोस्ट करना टालें
- सोशल नेटवर्किंग साईट्स की गोपनीयता की सेटिंग्स की जाँच कर लें और फिर सेटिंग्स इस प्रकार सेट करें कि लोग आपके मित्र के रूप में तब ही जुड़ सकें, जब आप उन्हें मंजूर करें तथा सेटिंग्स इस प्रकार सेट करें कि लोग आपकी प्रोफाईल तब ही देख सकें, यदि आपने उन्हें मित्र के रूप में मान्य किया हो

फाईल को साझा करना, उनकी डाउनलोडिंग व अपलोडिंग

सुरक्षित डाउनलोडिंग व अपलोडिंग

अपलोडिंग के संबंध में

डाउनलोड का विपरीत अपलोडिंग है, जिसका अर्थ है कि आपके कंप्यूटर से दूसरे कंप्यूटर पर नेटवर्क के द्वारा फाईल की नकल करना अपलोडिंग का अर्थ है डाटा का संचारण करना जो भी अंतरित किया गया है, उसे अपलोड किया जा सकता है संक्षेप में, अपलोडिंग से अर्थ है किसी फाईल को किसी ऐसे कंप्यूटर में भेजना, जो उसे प्राप्त करने के लिए सेट किया गया हैआप किसी भी प्रकार की फाईल जैसे कि दस्तावेज, संगीत, वीडियोज, बिम्ब व साफ्टवेयर और ऐसे ही बहुत कुछ अपलोड कर सकते हैं पी टू पी नेटवर्क में फाईल्सअपलोडिंग या फाईल को साझा करना सदैव समकक्ष कंप्यूटर्स के बीच होता है, जबकि सर्वरग्राहक तकनीक की अपलोडिंग में कई ग्राहकों से अपलोडिंग किसी विशेष मशीन पर की जाती है, जो एक सर्वर होता है

इंटरनेट से फाईल डाउनलोड करना व उन्हें साझा करना सामान्य है और दैनिक व्यवहार से इसमें कई प्रकार की जोखिम रहती है, जिनके बारे में आपको जागरूक रहना चाहिए

डाउनलोडिंग के संबंध में

डाउनलोडिंग किसी एक फाईल का किसी एक कंप्यूटर सिस्टम से दूसरे में, बल्कि सामन्यतः छोटे कंप्यूटर सिस्टम में संचारण है इंटरनेट उपयोगकर्त्ता के दृष्टिकोण से किसी फाईल के डाउनलोड करने से अर्थ है कि दूसरे कंप्यूटर (या वेब पृष्ठ से दूसरे कंप्यूटरपर) के द्वारा अनुरोध किया जाना और फिर प्राप्त करना शब्द डाउनलोड किसी ऑनलाईन सेवा से व किसी इंटरनेट के माध्यम से स्वयं के कंप्यूटर पर फाईल की नक़्ल करने की प्रक्रिया का वर्णन करने के लिए उपयोग में लिया जाता है

डाउनलोडिंग का अर्थ नेटवर्क सर्वर कंप्यूटर के नेटवर्क पर फाईल की नकल करने के सन्दर्भ में भी लिया जाता है डाउनलोड से अर्थ है डाटा प्राप्त करना अर्थात जो भी डाउनलोडिंग के लिए प्रस्तुत किया गया हो, उसे डाउनलोड किया जा सकता है आप इंटरनेट से किसी भी प्रकार की फाईल जैसे कि दस्तावेज, संगीत, वीडियोज, बिम्ब व साफ्टवेयर और ऐसे ही बहुत कुछ डाउनलोड कर सकते हैं

पी टू पी (समकक्ष से समकक्ष) फाईल के साझा करने के द्वारा उपयोगकर्त्ता पुस्तकों, संगीत, सिनेमा व क्रीड़ा की मीडिया फाईल्स तक पी टू पी साफ्टवेयर प्रोग्राम का इस्तेमाल करने के द्वारा पहुँच सकता है, जो अन्य

संबद्ध कंप्यूटर के पी टू पी नेटवर्क पर शोध करता है, जिससे इच्छित विषयसामग्री का पता लगाया जा सके ऐसे नेटवर्क की गाँठें (समकक्ष) अंतिम उपयोगकर्त्ता सिस्टम्स होते हैं और जो इंटरनेट के द्वारा आपस में एक दूसरे से संबद्ध रहते हैं पी टू पी सर्वरग्राहक तकनीक से भिन्न है, क्योंकि फाईल्स को एक कंप्यूटर से डाउनलोड किया जाता है, जो सर्वर होता है

फाईल साझा करने व असुरक्षित डाउनलोड करने में कौनसी जोखिम हैं?

जब आप किसी फाईल को साझा करने या फाईल को डाउनलोड करने की कोशिश करते हैं, तब उसमें प्रोग्राम का संस्थापन, चित्रों को खोलना, विभिन्न वेबसाईट्स की लिंक्स या ईमेल्स, संगीत तथा कंप्यूटर की कई और फाईल्स की डाऊनलोडिंग शामिल रहती है ये फाईल वही हो सकती हैं, जो वे बताती हैं, लेकिन वे दुर्भावनापूर्ण साफ्टवेयर में भी शामिल हो सकती हैं और जो आपके कंप्यूटर को नुकसान पहुंचा सकते हैं, जिसमें सम्मिलित होते हैं वायरस, कीटाणु व अन्य कई विध्वंसक प्रोग्राम से संबंधित

फाईल को साझा करते समय आप अनजाने ही दूसरों को आपके कंप्यूटर तक की पहुँच दे देते हैं, जो संभवित रूप से निजी फाईल्स की नक़्ल कर सकते हैं यह तब हो सकता है, जब आपको कहा जाता है कि आपकी फायरवाल सेटिंग्स को असमर्थ कर दें, या उसे बदल दें, जिससे कि फाईल के साझा करने के प्रोग्राम को अपलोड करने हेतु समकक्ष से समकक्ष (पी टू पी) का इस्तेमाल किया जा सके और जो आपका कंप्यूटर असुरक्षित रख सकता है

बगैर आपकी जानकारी के आपके कंप्यूटर पर वायरस, ट्रोजन्स व अन्य मैलवेयर की डाऊनलोडिंग डाटा को समाप्त कर सकती है या आपके कंप्यूटर पर की समस्त जानकारी तक किसी को पहुँच दे सकती है या आपके पीसी पर सभी गोपनीय जानकारियों को समाप्त कर सकती है, क्योंकि उनके लिए अक्सर भ्रम होता है कि वे किसी लोकप्रिय फिल्म या गीत के डाऊनलोड हैं

स्पायवेयर अक्सर आपके कंप्यूटर के व्यवहार में बदलाव लाता है, जैसे कि पीसी का धीमे हो जाना, यहाँ तक कि कंप्यूटर में धमाके हो जाने का भी कारण रहता है स्पायवेयर का उपयोग ब्राउसिंग इतिहास को मालूम करने, पासवर्ड चुराने और किसी हमलावर को आपके सिस्टम में से संपूर्ण जानकारियों को हथियाने में किया जाता है

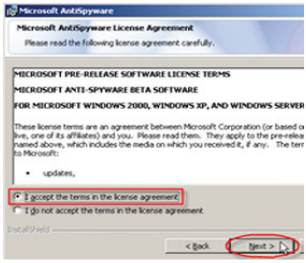
अवांछित अश्लील सामग्री की डाऊनलोडिंग पर कुछ अन्य का लेबल लगा दिया जाता है व साथ ही यदि आप वे सिनेमा, टीवी शो, संगीत या साफ्टवेयर डाऊनलोड करते हैं, जो कॉपीराइट संरक्षित हैं, तब यदि आपने न भी समझा हो, तब भी कानूनी मुद्दे जैसे कि कॉपीराइट अतिक्रमण का आपको सामना करना पड़ सकता है

किसी भी डाऊनलोड के पहले, साईट के लिए प्रमाणपत्र की वैधता तथा प्रमाणपत्र को जारी करने वाले की वैधता की जाँच करें

जब आप गपशप साफ्टवेयर को डाऊनलोड करते हैं, तब चूक की सेटिंग्स की जाँच करें और यदि वे बहुत आजादी से अनुमति देने वाले हों, तो उन्हें समायोजित करें

डाऊनलोड सुरक्षा के लिए युक्तियाँ

- जब कोई भी फाईल डाऊनलोड करना हो, तब आपके कंप्यूटर पर जो भी एप्लीकेशंस चल रहे हों, उन सबको बंद कर दें और डाऊनलोडिंग के वक्त केवल एक ही सेटअप फाईल को चलने दें
- डाऊनलोडिंग के वक्त यदि कुछ गलत हो जाए, इस हेतु सुरक्षित रहने के लिए सभी महत्वपूर्ण एप्लीकेशंस को बंद कर दें
- आप जो भी फाईल्स डाऊनलोड करें, उन्हें सक्रियता से स्केन करने के लिए फायरवाल्स सेट करें और एंटीवायरस सेट करें
- आप जब डाऊनलोड करें, उसके बाद सभी फाईलों को, चाहें वेबसाईट्स से या ईमेल से प्राप्त लिंक्स से हों, उन्हें स्केन करें
- सदैव उन्नत एंटीवायरस, स्पाम फिल्टर एवं स्पायवेयर का इस्तेमाल करें, जिससे जिस एप्लीकेशन को आप डाऊनलोड करना चाहते हैं, उसमें से वायरस, स्पायवेयर का पता लगाने व उन्हें हटाने में मदद मिले
- अविश्वसनीय साईट्स से कभी कोई फाईल जैसे कि संगीत, वीडियो, खेल और ऐसे ही बहुत कुछ को कभी भी डाऊनलोड न करें और न ही आपके मित्रों के द्वारा या किसी भी बेतरतीब वेबसाईट्स की टिप्पणियों के आधार पर दी गई अनुशंसाओं का पालन करें
- यह जाँच करें कि यूआरएलएस समान हैं और सुरक्षित वेबसाईट्स जो एचटीटीपी के स्थान पर एचटीटीपीएस को उपयोग में लेती हैं उनसे ही सदैव खेल, संगीत या वीडियो डाऊनलोड करें वेब पते में यह एचटीटीपी के स्थान पर एचटीटीपीएसको प्रस्थापित करता है एचटीटीपीएस से अर्थ है हायपरटेक्स्ट ट्रांसफर प्रोटोकाल सिक्योर



- जो भी डाऊनलोड करना हो, केवल विश्वसनीय वेबसाईट्स से ही करें ऐसी किसी भी लिंक्स को क्लिक न करें, जो आप अप्राधिकृत साईट ्स पर देखें
- यदि वेबसाईट्स पर कोई गंदा शब्द उभरता है, तो विंडो को तुरंत बंद कर दें, फिर वह चाहे कितना भी महत्वपूर्ण क्यों न हो, क्योंकि ऐसी वेबसाईट्स से आपके पीसी पर स्पायवेयर संस्थापित किया जा सकता है
- आप डाऊनलोड करें, उसके पहले आपकी फाईल के माप की जाँच कर लें, क्योंकि कई बार यह बहुत छोटा माप बताती है, लेकिन जब आप क्लिक करते हैं, तब यह फाईल का आकार बढ़ा देती है
- ऐसे किसी पर विश्वास न करें, जो कहे कि अमुक लिंक को क्लिक करो और आपका कंप्यूटर सेटिंग्स बदल जाएगा और आपका पीसी बदल सकता है, एक्सबीओएक्स में आप आपके कंप्यूटर पर असीमित खेल खेल सकते हैं
- ऐसी कुछ भी चीज स्वीकार न करें, जो आपको मुफ्त में डाऊनलोड करना प्रस्तावित करता है, क्योंकि उसमें दुर्भावनापूर्ण साफ्टवेयर हो सकते हैं
- किसी लिंक या फाईल को क्लिक न करें और उसके डाऊनलोड का आरम्भ स्वचालित रूप से होने दें और फाईल को डाऊनलोड करें और वहाँ सुरक्षित करें, जहाँ आप सुरक्षित करना चाहते हैं और फिर एप्लीकेशन चलाएँ
- आप कुछ भी डाऊनलोड करें, उसके पहले सुरक्षित ब्राउसर सेटिंग्स को सेट करें

- न जब आप संस्थापन पर क्लिक करें, या एप्लीकेशन चलाएँ, उसके पहले इसे ध्यान से पढ़ें इसका अर्थ है कि नियम व शर्तें पढ़ें
- न आप कुछ भी डाऊनलोड न करें, जब तक कि आप वेबसाईट की समस्त जानकारियाँ प्राप्त नहीं कर लेते हैं और यह भी जानें कि क्या वह मूल कंपनी की मूल साईट है
- आप कुछ भी लिंक्स से डाऊनलोड न करें, जो मुफ्त एंटीवायरस या एंटी स्पायवेयर साफ्टवेयर प्रस्तावित करते हो, यदि आप उस साईट के बारे में विश्वसनीय नहीं है, जहाँ से डाउनलोड कर रहे हैं, तब सदैव विश्वसनीय साईट्स से ही डाऊनलोड करें साईट को पसंदीदा शोध इंजिन में प्रविष्ट कराएँ, यह देखने के लिए कि क्या किसी ने भी पोस्ट किया है या रिपोर्ट किया है कि इसमें अवांछित तकनीकें हैं

References:

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

तत्काल सन्देश देना

इंटरनेट के इतिहास में तत्काल सन्देश देने की विधा किसी न किसी रूप में कई दशाब्दियों से रही है यह एक प्रक्रिया है, जिसके द्वारा कंप्यूटर नेटवर्क पर उपयोगकर्त्ता ईमेल का इस्तेमाल करने के स्थान पर संक्षिप्त विषय परआधारित वाक्यों का उपयोग कर तत्काल एक दूसरे को संचार प्रेषित कर सकते हैं प्रत्येक उपयोगकर्त्ता के पास एक साफ्टवेयर होता है जो एक साझा सर्वर के द्वारा सन्देश देता है और जो गपशप के सत्र से जोड़ देता है पिछले कुछ कुछ वर्षों में तत्काल सन्देश देने के उपयोग हेतु दो विशिष्ट सेटिंग्स का उद्भव हुआ है

उनमें से पहला है कार्पोरेट या संस्थागत वातावरण, जिसमें कई संभावित उपयोगकर्त्ता सम्मिलित हैं, लेकिन वे सब एक ही संस्थागत सुरक्षा में है

दूसरी सेटिंग्स है व्यक्तिगत उपयोगकर्त्ता काम के बाद या घर पर और जिनके पास कोई मिशन उन्मुख वस्तु नहीं है, लेकिन वे अधिकतर परिवार या मित्रों जैसे ही हैं

कार्पोरेट सेटिंग्स में सुरक्षा की जोखिम शुरुआत से ही दिखाई देती है किसी असंतुष्ट कर्मचारी का कंपनी की कुछ संवेदनशील डाटा को कंपनी के बाहर जो साथी हैं, उन्हें बताने के लिए कौन रोकता है?

तत्काल सन्देशवाहकों की विशिष्टताएँ

- मौजूदगी व प्रसारण की स्थिति सन्देशवाहक सामाजिक वातावरण बनाए रखने का प्रयास करते हैं और सदैव संबद्ध रहते हैं
- क्रियाशीलताअन्य कई उत्पादक उदहारण के संदेशवाहक के साथ क्रियाशील हो सकते हैं
- संपर्क सूची सभी इच्छित संपर्कों की सूची बनाए रखते हैं
- ग्राहक सर्वर डिजाईनसन्देशवाहक ग्राहकों को गपशप कार्य उपलब्ध कराने के लिए तृतीय पक्ष के सर्वर की जरूरत रहती है
- लॉग्स सन्देश सन्देश व अन्य घटनाएँ रिकार्ड की गई


वाईबेर:
वाईबेर मीडिया द्वारा विकसित स्मार्ट फोंस के लिए इंटरनेट सन्देश का वाईस-ओवर इंटरनेट प्रोटोकोल एप्लीकेशन से युक्त मालिकाना क्रास-प्लेटफार्म है। उद्धरण-सन्देश के अलावा उपयोगकर्त्ता इसमें बिम्ब, वीडियोज व ऑडियो-संदेशों का विनिमय कर सकते हैं।
लाईन:
स्मार्ट फोंस व व्यक्तिगत कंप्यूटर्स पर तत्काल सन्देश के लिए लाईन एक जापानी मालिकाना एप्लीकेशन है, जिसके द्वारा मुफ्त वाईस कॉल किए जा सकते हैं और मुफ्त सन्देश भेजे जा सकते हैं। एप में प्रयोग किए गए स्टिकर्स व इमोटीकांस किशोर-किशोरियों में बहुत लोकप्रिय है।
LINE
ककाओ टॉक
दक्षिण कोरियन दल द्वारा निर्मित ककाओ टॉक एक बहु-मंचीय उद्धरण एप है, जिसके द्वारा आई-फोन, एनड्रायड व ब्लेक बेरी के उपयोगकर्त्ता संदेशों को मुफ्त भेज सकते हैं व प्राप्त कर सकते हैं। यह १८ मार्च २०१० को आरम्भ हुआ और तब से इसके १०० मिलियन ग्राहक हो चुके हैं।०
TALK
वीचेट:
वीचेट चीन के इंटरनेट के बड़े महारथी टेन सेंट के द्वारा जारी एक मोबाईल सन्देश एप्लीकेशन है, जिसके ४५० मिलियन सक्रिय मासिक उपयोगकर्त्ता हैं।
WeChat
व्हाट्सअप
व्हाट्सअप सन्देशवाहक मोबाईल सन्देश का एप है, जो क्रास-प्लेटफार्म है, जिसके द्वारा उपयोगकर्त्ता बिना किसी भी प्रकार के भुगतान के संदेशों का विनिमय करते हैं।
किक:
मोबाईल उपकरणों के लिए किक सन्देशवाहक एक तत्काल सन्देश हेतु एप है। किक सन्देशवाहक १९ अक्टूबर २०१० को किक इंटरएक्टिव के द्वारा जारी किया गया, जो वास्तव में यूनिवर्सिटी ऑफ वाटरलू, कनाडा के छात्रों का समूह है।
kik.
हाईक:
हाईक एक संचार एप है और भारतीय टीवी नेटवर्क एनडीटीवी डॉट कॉम के अनुसार इसमें एक ही छत के नीचे, तत्काल सन्देश व एसएमएस दोनों की सेवाएँ हैं। यह भारती साफ्टबैंक द्वारा विकसित है, जो संयुक्त रूप से भारत के भारती टेलीकाम व जापान के साफ्टबैंक टेलीकाम प्रदाता की ओर से है। यह एप कविन भारती मित्तल का अभिनव विचार है।
hi

मोबाईल से तत्काल सन्देश देने में जोखिम

द्योंदृाक़्न्द्मा नें तत्व द्मा नथ्र्ञ्ब्ने च्थ्रें द्यों ड्डोंझिद्दा

- **वायरस व कीटाणु**

  वर्ष 2014 में इंटरनेट संचार में आईएम एप्लीकेशंस के अंतर्गत समकक्ष से समकक्ष के बीच शीर्ष के ५० वायरस में से 38 वायरस व कीटाणु लक्ष्य पर थे अधिकाँश वायरस फाईल के अंतरण के द्वारा अंतरित हो जाते हैं और सार्वजनिक तत्काल सन्देश (आईएम) ग्राहकों ने भी दोषपूर्णता को प्रचारित किया, जिससे इस प्रकार कि कमियाँ जैसे कि बफरओवरफ्लो व सीमा की स्थिति की भूलों का दोहन हुआ, जिससे वायरस व कीटाणु फैलें या सेवा से इंकार का हमला किया जाए

Be Polite and kind during your chat sessions

- **स्पिम**

  आईएम का तर्क कहता है कि आज के आईएम के यातायात का ५ से ७ स्पिम (तत्काल सन्देश स्पाम) है ईमेल स्पाम की तुलना में स्पिम अधिक विध्वंसक हो सकता है, क्योंकि यह अधिक अतिक्रमणकारी (पॉपअप स्पिम उपयोगकर्त्ता में व्यवधान डालता है) होता है व सामन्यतः अधिक यौनिक अपराधी प्रवृत्ति (मानव संसाधनों व कानूनी जोखिम की ओर उन्मुख) का होता है

Watch out for SPIM. (Spam Instant Messages)

- **पहचान की चोरी/ प्राधिकरण का झाँसा**

  सार्वजनिक आईएम प्रणाली लोगों को छद्मनाम से पहचान निर्मित करने देती है, जो किसी भी पहचान की योजना नहीं बनाती है व साथ ही आईडीएस तब भी बन जाती हैं, यदि आईडीएस व कार्यक्षेत्र उस व्यक्ति के न हों, तब भी (उदहारण के लिए आईसीआईसीआई या ज्हान चैम्बर्स) यह बनती है झाँसे देने में जोखिम होती है, क्योंकि ऐसे आईडीएस का उपयोग दुर्भावनापूर्ण हो सकता है और जो आईटी सुरक्षा विभाग के नियंत्रण के बाहर होते हैं

- **फायरवाल रास्ता बनाना**

  फायरवाल्स के माध्यम से आईएम ग्राहकों ने रास्ते ढूंढें, और इस तरह जोखिम निर्मित की अधिकाँश आईएम सेवाएँ बहुप्रचारित पोर्ट्स (एओएल तत्काल सन्देशवाहक के लिए ५१९०, एमएसएन के लिए १८६३ और याहू के लिए

५०५०) के द्वारा आती हैं, लेकिन आईटी ग्राहक फायरवाल पर मुक्त पोर्ट का दोहन कर सकता है, जिसमें वे भी शामिल हैं, जिनका इस्तेमाल अन्य एप्लीकेशंस (जैसे कि वेब व एचटीटीपी यातायात के लिए पोर्ट ८०) के द्वारा होता है समकक्ष से समकक्ष के संयोजन के द्वारा या स्थापित संयोजनों के द्वारा बेतरतीब समझौते के पोर्ट्स पर भी कुछ ग्राहक जोड़ सकते हैं

- **डाटा सुरक्षा रिसाव**

अनियंत्रित विषयसामग्री, सूचना सुरक्षा विभाग की जानकारी के बगैर कारपोरेशन को छोड़ देती है, जिससे कानूनी व प्रतिस्पर्धात्मक जोखिम आ जाती है (जैसे कि बिना लेखा परीक्षा के रास्ते, आईएम के माध्यम से सीएफओ के द्वारा गोपनीय स्प्रेडशीट भेजना) आईटी विभाग की पता लगाने की क्षमताओं से भी आगे, सूचनाओं को भेजने के लिए आईएम पर फाईल का अंतरण एक सशक्त तरीका है आईटी के लिए विषयसामग्री की फ़िल्टरिंग और उनका संग्रहण मुश्किल बना देता है कि वह योजना के संभवित उल्लंघनों का पता लगाए या व्यक्तिविशेष को जिम्मेवार ठहराए

- **हमें क्या करना चाहिए?**

सन्देश के तत्काल एप्लीकेशंस से बहुत सुविधा रहती है, लेकिन कुछ लोग ही सुरक्षा से संबंध में सोचते हैं प्रतिदिन हैकर्स कोशिश करते हैं कि वे हमारे वार्तालाप में घुसपैठ करें इसमें अच्छी बात यह है कि कुछ चीजें ऐसी है जो तत्काल सन्देश को अधिक सुरक्षित बनाती हैं

- **निजी जानकारियों के प्रकटीकरण को टालें**

विकासक ने चेतावनी दी है कि तत्काल सन्देश के कई एप्लीकेशंस यह आसान बना देते हैं कि निजी जानकारियों का प्रकटीकरण हो और आपराधिक उद्देशों के लिए उनका इस्तेमाल किया जाए केलिफोर्निया विश्वविद्यालय के संशोधकों ने एनड्राइड साधनों पर इस्तेमाल के लिए उपलध १२०,००० से अधिक मुक्त एप्लीकेशंस का अध्ययन किया

कई एप्लीकेशंस के कोड के भाग सर्वजनिक थे, इसका अर्थ यह हुआ कि आपराधिक उद्देश्यों के लिए उन्हें आसानी से संशोधित किया जा सकता था दुर्भावनापूर्ण कोड के उपयोग के द्वारा हेकर्स व अन्य लोग, जिनकी खराब मंशा होती है, वे और किसी की ओर से सन्देश भेजते हैं, जिससे वे निजी जानकारियों तक पहुँच बना सकें और उसे वास्तविक एप्लीकेशन के उस कोड से प्रस्थापित कर सकें, जिसका डिजाईन वैकल्पिक उद्देश्यों के लिए तैयार किया गया है

एनड्राइड ईपीएस पर जोर देने के बावजूद, शोधकर्त्ता यह मानते हैं कि आईफोन तत्काल सन्देश देने के विकल्प के साथ सुरक्षा की समान चिन्ताएँ वैध हैं

एनक्रिपशन स्मार्ट फोंस के लिए कई अन्य तत्काल सन्देश के एप्स की जाँच की गई कि किस तरह व्यक्तिगत जानकारी स्थान्तरित की जाती हैं और उन्हें संग्रहित किया जाता है तत्काल सन्देश में बाजार के आला अग्रणी व्हाट्सअप पर आरोप है कि वे जो अनएनक्रपटेड एड्रेस बुक्स व व्यक्तिगत जानकारियाँ एप सर्वर पर संचारित कर देते हैं व्यक्तिगत जानकारियों के कई टुकड़े जिसमें आईडी भी शामिल है, वे तीसरे पक्षों को देखने व उपयोग हेतु आसानी से उपलब्ध हैं

अब और अधिक तकलीफदेह स्थान हाल ही में शुरु हुआ है कुछ एप्लीकेशंस इस उद्देश्य के लिए विकसित किए गए थे, जिससे अन्य लोगों के बीच तत्काल सन्देश की बातचीत तक पहुँचा जा सके और व्यक्तिगत जानकारियों तक पहुँच हो सके व्हाट्सअप स्निफर ऐसी ही एक प्रगति है ऐसे एप्लीकेशंस एक बार पुनः उजागर करते हैं कि सुरक्षा की कितनी खामियाँ तत्काल सन्देश एप्लीकेशंस छोड़ जाती हैं

- **फेसबुक गपशप? पुनः विचार करें**

  कई सर्वेक्षण आयोजित किए गए और निष्कर्ष था कि बाजार में मोबाईल साधनों हेतु फेसबुक गपशप के एप्लीकेशंस सुरक्षा के मामले में न्यूनतम विकल्पों में से एक हैं लॉग इन के संरक्षण के लिए एनक्रिपशन का इस्तेमाल नहीं किया गया, इसका अर्थ है कि किसी व्यक्ति का पासवर्ड आसानी से देखा जा सकता है तत्काल सन्देश की बातचीत अब स्वयं ही न्यूनतम रूप से संरक्षित हैं याहू! सन्देशवाहक व अब चूक वाले विंडोज लाइव ये दो अन्य एप्लीकेशंस हैं जो सदस्यों की बातचीत को संरक्षित करने में पर्याप्त रूप से निष्फल रहे हैं

  तत्काल सन्देश एप्स का सुरक्षित ढंग से उपयोग वह क्या ले जाता है? पहला व स्पष्ट काम जो आप कर सकते हैं, वह है कि तत्काल सन्देश की सुरक्षा व निजता को बढ़ाने हेतु सही एप्लीकेशन का चयन करें कोई भी दो तत्काल सन्देश के एप्स एक जैसे नहीं हैं कुछ विकासक नाजुक डाटा के संरक्षण पर अधिक जोर देते हैं डाटा संरक्षण के लिए डाटा का एनक्रिपशन पहला व सर्वाधिक बुनियादी मार्ग है यह सुनिश्चित करें कि आप जिस एप का भी चयन करें वह सर्वर में सभी जानकारियाँ एनक्रिपटेड रूप में अंतरित कर देता है कुछ इंटरनेट एप्स जैसे कि स्क्याईप, गूगल, टाक, एओएल, इंस्टंट मेसेंजर व ऐसे ही समान प्रमुख विकास सामान्य से अधिक सुरक्षा उपलब्ध कराते हैं यह सुनिश्चित करें कि आपकी जानकारियों को सुरक्षित करने हेतु अपने पसंद के एप को डाऊनलोड करने के पहले आप अपनी शोध करेंगे

तत्काल सन्देश देना सुरक्षित करें

सुरक्षित रूप से सन्देश भेजना, सन्देश भेजने का एक प्रकार है, जिसमें सबसे कम उपयोगकर्त्ता बातचीत के संदेशों का विनिमय करते हैं और उनकी विषयसामग्री उनके द्वारा एनक्रपटेड उन कीज के द्वारा की की जानेवाले होती है, जो उनके द्वारा बनाई व नियंत्रित होती है

समाचारों की हाल ही की घटनाओं से उजागर हुआ है कि एनएसए न केवल ईमेल व आईएम संदेशों को संग्रहित करती है, बल्कि वे उन बातचीत व ईमेल्स भेजनेवालों व पानेवालों के बीच के रिश्तों को खोजती हैं, इस प्रक्रिया को मेटा डाट ा संग्रहण कहते हैं

मेटा डाटा उन बातचीत व ईमेल्स से संबंधित डाटा के बारे में हैं, जो संदेशों की विषय सामग्री के विपरीत है बहुमूल्य जानकारियों को एकत्रित करने के लिए इसका उपयोग किया जाता है

आप तत्काल संदेश हेतु जिस बेतार नेटवर्क का उपयोग करते हैं, वह उतना ही महत्वपूर्ण है नेटवर्क्स को खोलें, वैसे ही जैसे कैफे, हवाईअड्डों व बस स्टेशनों पर उपलब्ध होते हैं और जिनका पता लगाना बहुत आसान होता है जब तत्काल सन्देश कर रहे हों, तब किसी बंद, पासवर्ड से संरक्षित इंटरनेट नेटवर्क पर विश्वास करें मित्रों, व्यावसायिकभागीदारों व परिचितों के बीच संपर्क हेतु तत्काल सन्देश देने के कार्य का उपयोग किया जा सकता है फिर भी, यह महत्वपूर्ण है कि सुरक्षा का मुद्दा दिमाग में रखें यद्यपि यह सुविधाजनक है लेकिन फिर भी यदि गलत एप का चयन हो गया तो तत्काल

सन्देश देना व्यक्तिगत जानकारियों के साथ समझौता हो सकता है इसलिए एप्लीकेशंस का चयन सावधानीपूर्वक करें और आप जो साझा करते हैं, उसके बारे में होशियार रहें

मात्र परिभाषा के आधार पर कोई सुरक्षित सन्देश, सामाजिक सन्देश नहीं हो सकता है इसलिए सुरक्षित सन्देश पर विचार करते समय, जैसा कि आप सामाजिक उद्देश्यों के लिए करते हैं, उससे अलग ढंग से व्यवहार हो सुरक्षित तत्काल सन्देशवाहक की विशेषताओं में यह करना भी सम्मिलित हैं

- गुप्त ऑनलाईन उपस्थिति उपलब्ध कराना
- स्पष्ट अवतरण के रूप में नहीं, बल्कि साईफर अवतरण के रूप में सन्देश भेजें
- किसी भी सन्देश या उसकी विषयसामग्री से संबंधित कोई भी जानकारी लॉग या संग्रहित न करें
- किसी भी सत्र या घटना की विषयसामग्री से संबंधित कोई भी जानकारी लॉग या संग्रहित न करें
- विकेन्द्रित गणना के मॉडल की तरह उसे संचालित करें सन्देश की सुरक्षा व उसके साथ के कामकाज के बारे में तीसरे पक्ष के सर्वर्स पर विश्वास न करें

बातचीत के प्रत्येक सत्र के लिए सुरक्षित तत्काल संदेशवाहकों की जरूरत नहीं रहती है, जब निजी, सुरक्षित व पता न लगे वैसे सन्देश हों, और वैसी जरूरतों के प्रभाव वाले अन्य कोई साधन न हों

मोबाईल/ टेबलेट्स में लोकप्रिय सुरक्षित सन्देश के समाधान

टेलीग्राम

टेलीग्राम बादलआधारित मोबाईल व डेस्कटॉप सन्देश एप है, जिसका मुख्य ध्यान सुरक्षा व गति पर है

एडियम

मेक ओएसएक्स के लिए एडियम एक मुक्त तत्काल संदेश एप्लीकेशन है, जो एआईएम, एमएसएन, एक्सएमपीपी (जबेर), याहू व अन्य से जोड़ सकता है

बिट्बी

बिट्बी एक क्रासप्लेटफार्म का आईआरसी तत्काल संदेश का द्वार है और जिसे जीएनयू सामान्य जनता लायसंस के अंतर्गत लायसंस मिला हुआ है

जित्सी

(पहले एसआईपी संचारक), विंडोज के लिए एक मुफ्त व खुले स्त्रोत का बहुमंचीय आवाज (वीओआईपी), विडिओकांफ्रेंसिंग व तत्काल संदेश एप्लीकेशन है

ब्लोगिंगग

वेब ब्लॉग एक वेबसाइट है जिसमें प्रविष्टियोंकी शृंखला उल्टे कालानुक्रमिक क्रममें रखी जाती है, विशेष विषयों पर नयी जानकारी के साथ अक्सर अद्यतन होती है ़ दूसरी वेबसाइट या अन्य स्त्रोतोंसे पाई गयी या उपयोगकर्ताओं के योगदान से मिली जानकारी साईट मालिक द्वारा लिखी जा सकती है़ वेब ब्लॉगमें व्यक्तिके दर्ज किए हुए विचारों शामिल हो सकते हैं (एक तरह से डायरी)़

ब्लोग्स के प्रकारः

कई विभिन्न प्रकारके ब्लोग्स है और उनका व्याप करीब १०० भाषाओं तक है ़ आप अपने टैग्स ब्राउज कर सकते हैं शामिल विषयोंकी जानकारी हेतु या इन लोकप्रिय ब्लॉग प्रकारोंके उदाहरण पर नज़र डाल सकते हैं

- **व्यक्तिगत :**
  यह एक प्रसारण श्रेणी है और इसमें व्यक्तिगत विषयों जैसे राजकारण, संगीत, परिवार, यात्रा, स्वास्थ्य वि .के बारेमें ब्लोग्स शामिल है |
- **व्यवसाय :**
  रियाल्टार से ले कर वकीलों और शेयर दलालों जैसे पेशेवरों उनकी निपुणता साझा करने के लिए उपयोग करते है और कम्पनीयोंको अपने ग्राहकोंके साथ व्यक्तिगत स्पसे संलग्न होनेमें ब्लोग्स की शक्तिका पता चला है |
- **विद्यालयों :**
  शिक्षकों और विद्यार्थियोंके लिए कक्षा परियोजनाओं पर एकसाथ काम करने के लिए यह एक अच्छा रास्ता है |
- **गैर लाभ :**
  प्रतिष्ठानों, दानी संस्थओं और मानव अधिकार समूहोंके लिए यह ब्लोग्स जागरूकता बढ़ाने और उनके हेतुओंके लिए पैसे जुटानेके लिए महान उपकरण है |
- **राजकारण :**
  राजनीतिक दलों, सरकारी संस्थाएं और कार्यकर्ताओं यह ब्लोग्सका इस्तेमाल उनके चुनाव क्षेत्रसे जुड़नेके लिए करते है |

- **निजी :**
  कुछ लोग तस्वीरें और जानकारी परिवारों, कम्पनीयों, विद्यालयों वि .में साजा करने के लिए अपने निजी ब्लोग्स बनाते है |
- **खेल-कूद :**
  टीमों, खिलाडीयों और प्रशंसको विभिन्न खेलोंके लिए उनके जुनून व्यक्त और साज़ा करनेके लिए ब्लोग्सका उपयोग करते हैं |
- **मीडिया प्रकारके ब्लोग्स :**
  मीडिया वीडियोज साज़ा करनेके लिए व्लोग्स ,लिंक्स साज़ा करनेके लिए लिंक्लोग्स और तस्वीरें साज़ा करनेके लिए फोटोब्लोगका उपयोग करते हैं |
- डिवाइस के द्वारा(मोबाइल फोन, घछ,पहनने योग्य वायरलेस वेब कैमरा)मोबाइल फोन जैसे मोबाइल डिवाइस या घछ जिसे मोब लोग कहते हैं ब्लोग्स लिखने के लिए उपयोग करते हैं ꠰

ब्लोग्गिंग में शामिल जोखिमों

ब्लोग्गिंग समाचार और जर्नलिंग को मानवीय प्रभाव प्रदान करता है, वह साथ में निजी जीवन में ख़िडकी खोलता है | ब्लोग्स में साज़ा किया हुआ विवरण पहले सिर्फ मित्रों के पसंदीदा समूह को ही उपलब्ध था, अब ब्लोग्गिंग एक आम बात हो गयी है, उसके जोखिमों को नजरंदाज नहीं करना चाहिए | अगर आप ब्लोग्गिंग साइट्स में व्यक्तिगत जानकारी जैसे आप का नाम, स्थान, पता, फोन नंबर्स, केडिटकार्ड की जानकारी देते हैं, दूसरौं के द्वारा आप की जानकारी चोरी हो सकती है(पहचान की चोरी)क्योंकि हर कोई जिसके पास लॉग इन अकाउंट जो साईटका आप उपयोग कर रहे हैं उसमें है आपके प्रोफाइल तक पहुँच सकता है | जो प्रोफाइल आप बना रहे हैं ब्लॉग साईट पर हर किसीको दिखाई दे सकता है | अनजानी व्यक्तिओं आपके प्रोफाइल तक पहुँच सकती है और आपकी सभी जानकारी देख सकती है |

उदाहरण के लिए, अगर आप अपना केडिटकार्ड नंबर साईटमें देते हैं, वो लोग उस नंबरका उपयोग अपने खुदके व्यापारके लिए या खरीदारीके लिए कर सकते हैं और उसका बिल आपको भेजा जायेगा ꠰ दूसरा उदाहरण है कि अगर आपके बच्चे साईटमें उनके विद्यालयका नाम और स्थान पता देते हैं, अनजान व्यक्तियों जो उस जानकारी तक पहुँचता है उसका लाभ ले कर आपके बच्चेका अपहरण कर सकता है |

ख्र्थ्त्ह्य न्न्र्दृद्ब्द्ध ड्ढठ्ठ्यद्यठ्ठ द्यण्ठ्ठ्य न्न्र्दृद्ब प्रद्बद्य दृदथ्त्दड्ढ

ग़्ड्ढध्ड्ढद्ध ब्ध्ड्ढध्ड्ढठ्ठ्थ प्रठ्ठन्न्ध्दृद्धड्ढ दृद द्दद्बड्ढन्न्द्यत्दृददठ्ठत्ध्द्बड्ढन्न, दृद्ध ढदृद्धद्बथ्न्न, दृद्ध डथ्दृढ़न्न दृद्ध न्न्दृड़त्ठ्ठथ दड्ढद्यध्दृद्धत्त्दढ़ न्न्त्द्यड्ढन्न

च्च्रठ्ठथ्ड्ढद्धन्न ड़दृथ्थ्ड्ढड़द्य ड्ढ-थ्ठ्ठत्थ ठ्ठड्डड्डद्धड्ढन्न्न्ड्ढन्न ढद्धदृ थ्ड्डडन्न्त्द्यड्ढन्न ठ्ठदड्ड डथ्दृढ़न्न. च्चृ, थ्त्दत्थ्त्न्ड्ढ प्रदृन्न्द्यत्दढ़ न्न्र्दृद्बद्ध ड्ढ-थ्ठ्ठत्थ ठ्ठड्डड्डद्धड्ढन्न्न्न.

साइबर शिकार

साइबर शिकार एक अपराध है जिसमें हमलावर शिकारको इलेक्ट्रॉनिक संचारका इस्तेमाल करके जैसे तात्कालिक संदेशन(ष) पर इ-मेल भेज कर या वेबसाइट या चर्चा समूहों पर संदेशे पोस्ट करके परेशान करता है | साइबर शिकार एक नयी घटना है जो गुमनाम ऑनलाइन शिकारियोंको छिप कर शिकार तलाश करनेका मौका देता है | परिणाम स्वरूप ब्लोग्गिंग करनेवाली बहुत सी महिलाएं शिकार हो रही है ऽ ज्यादातर लोग बच्चोंके इन्टरनेट पर होनेसे चिंतित है और बच्चों, किशोरों और तरुणोंके लिए पोस्टिंग के सख्त दिशा निर्देश स्थापित किये है, लेकिन कुछ ही वयस्क चेतावनी पर ध्यान देते हैं और बहुधा यह नहीं समझते कि वे भी निशाना बन सकते हैं |

खास करके महिलाओंको ब्लॉगोस्फीयर सरकमनेविगेटिंग करते वक्त सावधान रहना चाहिए ऽ अगर आप ब्लोग्गर है या ऑनलाइन जर्नल पर विचार कर रहे हैं, आपकी पहचानको सुरक्षित रखनेके लिए इन सुजावों पर विचार करें:

ऑनलाइन प्रोफाइल मत रखिए :

ज्यादातर ब्लोग्गिंग सेवाएँ ब्लोग्गर्सको ऑनलाइन प्रोफाइल बनाने देते हैं | पसंद और नापसंदकी जानकारी पोस्ट करना मजेदार हो सकता है, कोई भी निजी जानकारी पोस्ट करनेसे परहेज करना सबसे अच्छा है | अक्सर, निजी जानकारी अनजानेमें भौतिक स्थान और आदतोंके बारेमें गहरी पहुँच प्रदान करता है ऽ व्यक्तिगत प्रोफाइलकी समग्र जानकारी व्यक्तिका पीछा करनेमें रूचि रखने वाले किसीको मदद भी कर सकती है |

ब्लोग्गिंग करनेके जोख़िमों से बचनेके लिए सुज़ाव

- ब्लोग्गिंग साइट्समें कदापि अपनी निजी जानकारी न दे दें
- विश्वसनीय जानकारी रखें क्योंकि वह पूरी दुनिया तक पहुँचती है और मान लिया जाता है कि जो आप वेब पर प्रकाशित करते हैं वह स्थायी है |
- दुसरे ब्लोग्गर्ससे प्रतिस्पर्धासे बचें |
- आपके ब्लोग्सको सुरक्षित करनेके लिए ब्लॉगमें दर्शकोंको उपयोगकी शर्तें, कॉपीराइट उचित रूपसे निर्दिष्ट करें |
- उन्हें अन्य सकारात्मक उदाहरणसे राह दिखाएँ जैसे कि बच्चे उनकी संबंधित जानकारी पोस्ट करते हैं |
- गुमनाम रूपसे पोस्ट करें : आपके ब्लोग्का गुमनाम रूपसे संचालन करें या सभी ऑनलाइन पोस्टिंगके लिए उपनाम अपनाएं ऽ आपके अवांछित ध्यान आकर्षित होनेकी घटनामें वह आपकी सुरक्षा करेगा |
- नजी या पहचान करनेवाली जानकारीसे बचें: आपके ब्लॉगमें पोस्ट करते वक्त निजी या पहचान करनेवाली जानकारीसे दूर रहें | अग्रिम रूपसे आप जहां होंगे वह स्थानों या जहाँ आप रहते हैं उसके आसपासके इलाके के बारेमें पोस्ट न करें |
- तस्वीरें नहीं: तस्वीर पोस्ट करनेसे बचें ऽ तस्वीरें मुसीबत या अवांछित ध्यानको आमंत्रित कर सकती है |
- अनुचित संवादसे बचें : ऐसी बातचीतमें शामिल होनेसे सावधान रहें जिसका अर्थघटन उस मायनेमें हो सके जो अभिप्रेत न हो ऽ कभी कभी विनोदपूर्ण सूत्र हाथसे बाहर हो जाते हैं ऽ अगर बातचीत आपको असुविधा महसूस हो ऐसे निचले क्षेत्रमें पहुँच जाती है, बातचीतसे अलग हो जाएं और आगे पोस्टिंगसे बचें ऽ जब ऑनलाइन व्यक्तिओं के बारेमें निर्णय लेना हो, उनका पिछला पोस्टिंग व्यवहार ध्यानमें रखें और उनके सच्चे इरादे पर विचार करनेका प्रयास करें ऽ

- हमेशा याद रखें कि अगर आपकी बातचीत किसीसे नहीं है तो इसका मतलब यह नहीं है कि वह लोग आप जो सबकुछ लिख रहे हैं वो उसे पढ़ नहीं रहे ऽ बहुत लोग केवल लाइन पर दुबके रहते हैं और कमेन्ट पोस्ट करनेमें शामिल नहीं होते, लेकिन जो लिखा गया है उसे पढ़ते जरूर है| आपका दर्शकगण आपके समझने से कहीं ज्यादा विशाल हो सकता है |
- कालनिरपेक्षः इन्टरनेट सामग्री कालनिरपेक्ष है, और याद रखो कि अगर आप सामग्री हटा भी लेते हो तो भी वह संगृहीत या सिंडिकेटेड हो सकती है ऽ अगर आप चाहते हैं कि कोई चीज पढ़ी न जाये तो उसे इन्टरनेट पर पोस्ट मत करो ऽ उच्च विद्यालयों, महाविद्यालयों और मालिकों वि. सब व्यक्तिका इतिहास जाननेके लिए इन्टरनेट पर तलाश करते हैं ऽ देर रातके बारेमें घिनौना विवरण प्रतिष्ठित नौकरी दिलानेमें मदद नहीं करेंगे |
- इन्टरनेट सभी प्रकारके शिकारियों के लिए स्वर्ग है ऽ हमेशा याद रखो कि कोई अगर कहता है कि कोई बात सच है उसका मतलब यह नहीं कि वह सच हो ऽ जैसे छोटे बच्चेके लिए दिशा निर्देशों प्रदान करते हैं वयस्कोको भी चौकन्ना रहना चाहिए और ऑनलाइन पोस्टिंग करते वक्त सावधानी बरतनी चाहिए |
- ब्लोग्गिंग एक बढ़िया निर्गम और चैनल हो सकता है, और किसी तरह विचारोंको अमर बनानेके लिए यह महत्वपूर्ण है कि सुरक्षाका ध्यान रखा जाये और अच्छी ब्लोग्गिंग आदतोंका हमेशा अनुसरण किया जाये |

माता-पिताके लिए ब्लोग्गिंगके विषयमें मार्गदर्शन

- बच्चोंके लिए ऑनलाइन उपयोगके नियम स्थापित करें |
- आपके बच्चे पोस्ट करें उससे पहले वे क्या पोस्ट करना चाहते हैं उसकी जाँच करें |
- ब्लोग्गिंग सेवा और उनकी विशेषताएं जैसेकि पासवर्डसे सुरक्षित ब्लोग्स वि.का मूल्याँकन करें |
- आपके बच्चोंके ब्लोग्सकी समीक्षा नियमित रूप से करें |
- अन्य सकरात्मक उदाहरण जैसे कि विद्यार्थियों जो संबंधित जानकारी पोस्ट करते हैं उनका सन्दर्भ दे कर मार्गदर्शन करें |

References:

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

सायबर बदमाशी

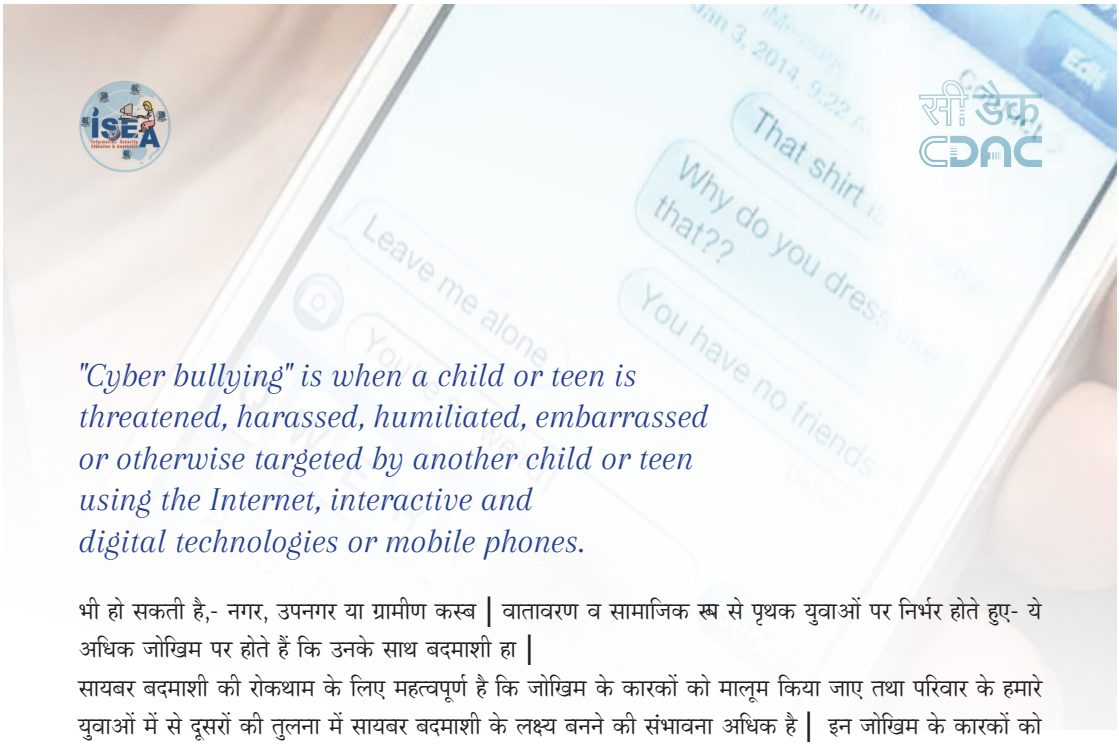
सायबर बदमाशी क्या है

सायबर बदमाशी वह बदमाशी है, जो बच्चों के बीच उस दौरान होती है, जब वे इलेक्ट ्रोनिक तकनीक का इस्तेमाल करते हैं़ यह इलेक्ट्रोनिक तकनीक के माध्यम से हो सकती है, जिसमें सेल फोंस, कंप्यूटर्स व टेबलेट्स जैसे साधन व उपकरण तथा संचार के औजार शामिल हो सकते हैं, जिनमें सोशल मीडिया की साईट्स, टेक्स्ट सन्देश, ई-मेल, गपशप ग्रूप्स, चर्चा समूह व इंटरनेट की वेबसाईट्स सम्मिलित हैं़ सायबर बदमाशी में शामिल हो सकते हैं, तंग करना, मजाक उड़ाना, ऑनलाईन अफवाह उड़ाना, अवांछित सन्देश भेजना व मानहानि करना़

सायबर बदमाशी के उदाहरणों में शामिल हो सकते हैं, टेक्स्ट सन्देश या ई-मेल, ई-मेल द्वारा फैलाई जानेवाली या सोशल नेटवर्किंग साईट्स पर पोस्ट की गई अफवाहें व शर्मिन्दा करनेवाले चित्र, वीडियो, वेबसाईट्स या फर्जी प्रोफाईल्स भेजना

सायबर बदमाशी: जोखिम के कारक

बदमाशी कहीं भी हो सकती है, लेकिन यह वातावरण पर निर्भर करती है और कुछ समूहों पर इसकी जोखिम अधिक हो सकती है़ यह सीखें कि वे कौनसे कारक हैं, जो बच्चों पर बदमाशी की जोखिम बढ़ा देते हैं या बच्चे दूसरों के प्रति अधिक बदमाशी करते हैं और इसके चेतावनी के चिन्ह कौनसे हैं जो दर्शाते हैं कि शायद बदमाशी हो रही होगी | आप यह भी मालूम कर सकते हैं कि यह बदमाशी किस प्रकार बच्चों पर नकारात्मक प्रभाव डाल सकती है | कोई मात्र एक कारक नहीं है, जिससे बच्चा बदमाशी का शिकार होने की जोखिम में रहता है या वह दूसरों से बदमाशी करता है़ बदमाशी कहीं



"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.

भी हो सकती है,- नगर, उपनगर या ग्रामीण कस्ब | वातावरण व सामाजिक रूप से पृथक युवाओं पर निर्भर होते हुए- ये अधिक जोखिम पर होते हैं कि उनके साथ बदमाशी हा |

सायबर बदमाशी की रोकथाम के लिए महत्वपूर्ण है कि जोखिम के कारकों को मालूम किया जाए तथा परिवार के हमारे युवाओं में से दूसरों की तुलना में सायबर बदमाशी के लक्ष्य बनने की संभावना अधिक है | इन जोखिम के कारकों को मालूम कर हम सायबर बदमाशी के खतरों के बारे में बेहतर ढंग से युवाओं को तैयार व शिक्षित कर सकते हैं व साथ ही यह भी कि कोई इससे किस प्रकार संरक्षित हो सकता है |

सोशल नेटवर्किंग

सोशल मीडिया, ऑनलाईन गपशप रूम्स, ब्लॉग्स व व्यक्तिगत वेबसाईट्स की बढ़ती हुई लोकप्रियता के कारण सायबर बदमाशी में वृद्धि हुई है| सायबर बदमाशों के कामों के लिए सोशल नेटवर्किंग पर ही पूर्णतः लांछन नहीं लगाया जा सकता है| सोशल नेटवर्किंग साईट्स जबकि वह माध्यम उपलब्ध करा सकती है, जिसके द्वारा सायबर बदमाश दूसरों पर हमला करते हैं, लेकिन साईट ने स्वयं बदमाशी का सृजन नहीं किया और न ही उसने इस प्रकार के व्यवहार को प्रोत्साहित किया | कोई बदमाश, बदमाश ही रहता है फिर वह चाहे ऑनलाईन क्षेत्र में हो या फिर वह भौतक दुनिया में हा | ऐसा कहा जाता है कि वे युवा जो सोशल नेटवर्किंग साईट्स में सहभागिता करते हैं या जो वेबसाईट्स या ब्लाग्स पर व्यक्तिगत जानकारियाँ पोस्ट करते हैं, उनके सायबर बदमाशी के शिकार होने की संभावना अधिक होती ह | सायबर बदमाशी की रोकथाम के लिए एक तरीका है कि आपके खाते की सेटिंग्स को संयोजित कर गोपनीय किया जाए, जिससे व्यक्तिगत जानकारी चाहनेवाले मुलाकातियों को टाला जा सके |

लिंग

सायबर बदमाशी पर हुए अनुसंधान के अनुसार लड़कों की तुलना में लड़कियों को सायबर बदमाशी का अनुभव प्राप्त करने की संभावना अधिक रहती है | दूसरों के अवांछित फोटोस को ऑनलाइन पोस्ट करने के कारण व दूसरों को सोशल नेटवर्किंग साईट्स का उपयोग कर शर्मिंदा करने के कारण लड़कियाँ सायबर बदमाशी व्यवहार में अधिक संबद्ध रहती है | सायबर बदमाशी के लिए यद्यपि मात्र लड़कियाँ ही दोषी नहीं होती हैं | उनके अनुसन्धान के अनुसार लड़कियों की तुलना में लड़कों ने दूसरों को मजाक उड़ाने या उन्हें क्रोधित करने हेतु अधिक ई-मेल भेजना, स्वीकार किया |

खेल में

वीडियो गेम की संस्कृति के अंतर्गत सायबर बदमाशी के रूप में यौनिक उत्पीड़न सामान्य है | हाल ही के एक अध्ययन में यह बताया गया है कि इस उत्पीड़न का कुछ कारण वीडियो गेम्स में स्त्रियों का चित्रण होना भी होता है | इस उत्पीड़न में सामान्य रूप से महिलाओं को संबोधित की गई निंदा, घिसीपिटी यौनिक भूमिका व बढ़ी-चढ़ी आक्रामक भाषा का उपयोग रहता है |

धमकाए जाने की जोखिम में बच्चे

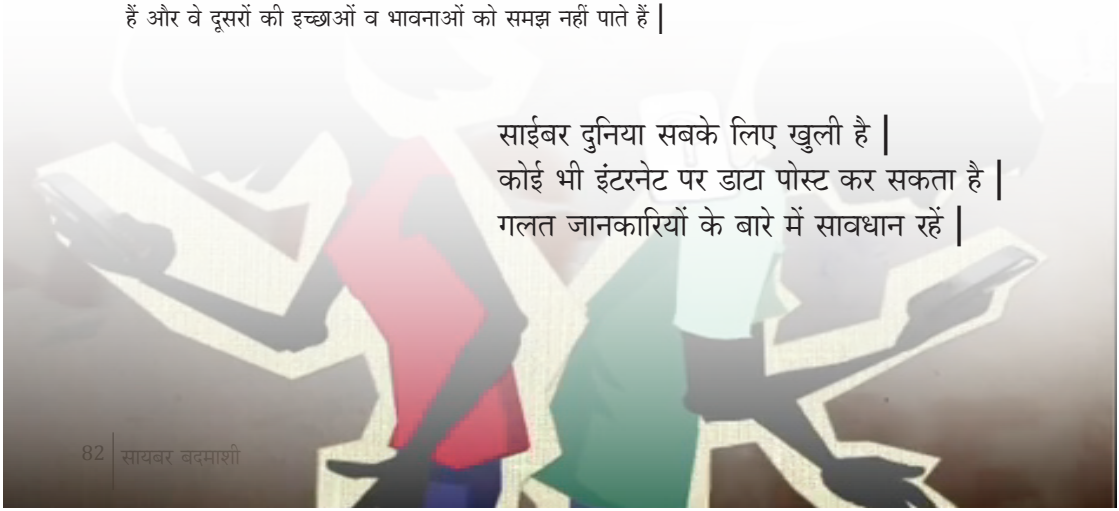
सामान्यतः बच्चे जो बदमाशी की गिरफ्त में आते हैं, उनके निम्न में से एकाधिक जोखिम के कारक होते हैं:

- उन्हें अपने समकक्षों से भिन्न माना जाता है जैसे कि मोटा होना या पतले होना, चश्मा पहनना या भिन्न तरह की वेशभूषा होना, शाला में नए होना या समकक्ष बच्चों से मेल रखने रखने में स्वयं को असमर्थ पाना
- उन्हें कमजोर या स्वयं अपनी रक्षा करने में असमर्थ माना जाता है
- वे दुखी, व्यग्र या आत्म-विश्वास की कमी वाले होते हैं
- अन्य की तुलना में कम लोकप्रिय होते हैं और बहुत कम मित्र होते हैं
- दूसरों के साथ ठीक से नहीं रह सकते हैं और दूसरों के ध्यान में आने के लिए गुस्से में या उत्तेजना में या प्रतिरोध में रहते हैं
- फिर भी यदि बच्चे में ये जोखिम के कारक हैं तो इसका अर्थ यह कदापि नहीं है कि उनके साथ बदमाशी हो |

बच्चे जिनकी दूसरों से बदमाशी करने की अधिक संभावना रहती है

बच्चे दो प्रकार के होते हैं, जिनमें दूसरों से बदमाशी करने की अधिक संभावना रहती है:

- कुछ वे होते हैं, जो अपने समकक्षों से ठीक से संबद्ध रहते हैं, जिनके पास सामाजिक शक्ति होती है और अपनी लोकप्रियता के प्रति अधिक सचेत रहते हैं और दूसरों पर प्रभुत्व चाहते हैं या उनके प्रभारी रहना चाहते हैं |
- अन्य वे होते हैं, जो अपने समकक्षों से बहुत पृथक रहते हैंऔर कुछ हताश या व्यग्र रहते हैं और आत्म-विश्वास की कमी वाले होते हैं तथा शाला में कम सहभागिता रहती है और वे समकक्षों के दबाव में आसानी से आ जाते हैं और वे दूसरों की इच्छाओं व भावनाओं को समझ नहीं पाते हैं |



जिन बच्चों के पास ये विशेषताएँ हों, उनकी दूसरों के साथ बदमाशी करने की संभावना अधिक रहती है

- गुस्सैल या आसानी से हताश हो जाते हैं
- माता-पिता के साथ कम सहभागिता रहती है या घर पर कुछ मुद्दे होते हैं
- दूसरों के बारे में बहुत ख़राब सोचते हैं
- नियमों का पालन करने में कठिनाई रहती है
- हिंसा का सकारात्मक रूप में देखते हैं
- जो दूसरों से बदमाशी करते हैं, ऐसे इनके मित्र होते हैं

यह याद रखें कि जो दूसरों के साथ बदमाशी करते हैं, उन्हें उनकी तुलना में ताकतवर या बड़ा होने की जरूरत नहीं रहती है, जिन्हें वे प्रताड़ित करते हैं | शक्ति का असंतुलन कई स्त्रोतों से आ सकता है- लोकप्रियता, शक्ति, बोध कराने की सामर्थ्य- और बच्चे जो बदमाशी करते हैं, उनमें इनमें से एक से अधिक विशेषताएँ हो सकती हैं |

सायबर बदमाशी के प्रभाव

- भावनात्मक व्यथाः क्रोध, हताशा, शर्मिंदगी, दुःख, भय, अवसाद
- शाला के काम या नौकरी के निष्पादन में हस्तक्षेप
- नौकरी छोड़ना, कक्षा छोड़ना या शाला बदलना
- कर्तव्य से विमुखता व हिंसा
- उल्लेखनीय दुष्कर्म
- शाला के मैदान में हथियारों पर कब्जा
- आत्महत्या

निम्न तरीकों से सायबर बदमाशी की जा सकती है:

- **दूसरों को व्यक्तिगत आईएम संचार भेजना**
  कोई बच्चा/ किशोर किसी ऐसे स्क्रीन नाम का सृजन कर सकता है, जो किसी दूसरे बच्चे के नाम के जैसा हो | उस नाम में अतिरिक्त "इं" या एक कम "ऐ" हो सकती है़ दूसरे व्यक्ति का रूप बना कर वे अन्य उपयोगकर्ताओं को अनुपयुक्त चीजें कहने के लिए वे इस नाम का इस्तेमाल कर सकते हैं़ बच्चे अपने व्यक्तिगत संचार फ़ैलाने के लिए उपरोक्त व्यक्तिगत संचार भेज सकते हैं |
- **अफवाह फ़ैलाने के लिए दूसरा रूप धारण करना**
  अफवाह फ़ैलाने के लिए गप्प मेल या झाँसे वाली मेल भेजना या अन्य किसी बच्चे या किशोर को हानि पहुँचानाऱ वे स्वयं को पीड़ित बताते हुए घृणास्पद समूह के गपशप रूम में पीड़ित के विरुद्ध हमले को आमंत्रित कर, कोई उत्तेजनात्मक सन्देश पोस्ट कर सकते हैं, जिसमें अक्सर नाम, पता, व पीड़ित का टेलीफोन नम्बर दिया हुआ होता है, जिससे घृणास्पद समूह का काम आसान हो जाता है |
- **शर्मिंदगी वाले फोटो या वीडियो पोस्ट करना**
  लॉकर रूम, स्नानघर या ड्रेसिंग रूम के किसी के चित्र या वीडियो लिए जा सकते हैं और फिर उन्हें ऑनलाइन पोस्ट

किया जा सकता है या दूसरों को सेल-फोन पर भेजा जा सकता है |

- **वेबसाईट्स या ब्लॉग्स का इस्तेमाल कर**
  बच्चे खेल के मैदान में अक्सर एक दूसरे को परेशान करते हैं, लेकिन अब वे यह सब वेबसाइट पर करते हैं | कई बार बच्चे वेबसाइट या ब्लॉग का निर्माण करते हैं, जो किसी अन्य बालक को अपमानित कर सकता है या उसे खतरे में डाल सकता हैऱ वे विशेष रूप से ऐसे पृष्ठों का डिजाईन तैयार करते हैं, जिससे दूसरा कोई बच्चा या लोगों का समूह अपमानित होता हो|
- **नीचा दिखाने के लिए सेल-फोन पर विषय-सामग्री भेजना**
  टेक्स्ट युद्ध या टेक्स्ट हमले तब होते हैं, जब बच्चे पीड़ित पर टोली के रूप में कार्य करते हैं और घृणास्पद संदेशों से संबंधित हजारों टेक्स्ट सन्देश पीड़ित के सेल-फोन पर या अन्य मोबाईल फोन पर भेजते हैंऱ
- **ई-मेल या मोबाईल द्वारा दूसरे को तकलीफ पहुँचाने हेतु धमकी-युक्त ई-मेल्स व चित्र भेजना**
  बच्चे अन्य बच्चों को घृणास्पद व धमकीयुक्त संदेश भेज सकते हैं, बिना यह अहसास किए कि वास्तविक जीवन में जो नहीं कहे गए, वैसे कठोर या धमकीयुक्त संदेश पीड़ा देने वाले और बहुत अधिक गंभीर होते हैंऱ
- **परस्पर-क्रियाशील ऑनलाइन गेम्स पर अन्य उपयोगकर्त्ता का अपमान होना**
  बच्चे/ किशोर अन्य बच्चों/ किशोरों को मौखिक रूप से गलियाँ देते हैं और जब वे ऑनलाइन गेम्स या परस्पर-क्रियाशील गेम्स खेलते हैं, तब वे धमकी व असभ्य भाषा का इस्तेमाल करते हैंऱ
- **पासवर्ड्स को चुराना**
  कोई बच्चा किसी दूसरे बच्चे का पासवर्ड चुरा कर यह बताते हुए कि वह अन्य बच्चा है या वास्तविक उपयोगकर्त्ता की प्रोफाईल में बदलाव कर अन्य लोगों के साथ गपशप शुरूकर सकता हैऱ

सायबर बदमाशी की रोकथाम कैसे करें

बदमाशी के व्यवहार के समय वयस्क तुरंत व सामजस्यता के साथ प्रतिक्रिया देते हुए यह सन्देश भेजते हैं कि उन्हें वह स्वीकार्य नहीं हैऱ इसके संबंध में अनुसंधान बताते हैं कि समय के साथ यह बदमाशी के व्यवहार को रोक सकता हैऱ कुछ सामान्य कदम हैं, जो बदमाशी को रोकने के लिए वे तुरंत उठा सकते हैं और और बच्चों को सुरक्षित रख सकते हैं |

करें:

- ✔ तुरंत हस्तक्षेप करेंऱ किसी अन्य वयस्क की मदद प्राप्त करना भी ठीक रहता हैऱ
- ✔ जो बच्चे उसमें शामिल हों, उन्हें दूर कर देंऱ
- ✔ यह सुनिश्चित करें कि प्रत्येक सुरक्षित हैऱ
- ✔ किसी भी तुरंत चिकित्सकीय या चिकित्सकीय स्वास्थ्य की जरूरत को पूरा करेंऱ
- ✔ शांत रहेंऱ दर्शकों सहित जो बच्चे इसमें शामिल हों, उन्हें पुनः आश्वस्त करेंऱ
- ✔ जब आप हस्तक्षेप करें, तब व्यवहार सम्मानजनक होऱ
- ✔ इन सामान्य गलतियों को टालें:
- ✔ इसकी उपेक्षा न करेंऱ ऐसा न सोचें कि बिना वयस्कों की मदद के बच्चे इसे कर सकते हैंऱ
- ✔ तथ्यों को तुरंत व्यवस्थित करने की कोशिश न करेंऱ

- दूसरों बच्चों ने जो उसे देखा, उसे सार्वजनिक रूप से कहने के लिए उन पर दबाव न बनाएँ।
- इसमें शामिल बच्चों से अन्य बच्चों की मौजूदगी में, सवाल न करें।
- इसमें शामिल बच्चों से एक साथ बात न करें, केवल उन्हें अलग-अलग कर पूछें।
- इसमें शामिल बच्चों से क्षमा-प्रार्थना न करवाएँ या तुरंत ही संबंधों में आई दरार को पाटें।

युक्तियाँ व मार्गदर्शन

- पैतृक नियंत्रण बार्स, डेस्कटाप फायरवाल्स, ब्राउसर फिल्टर्स का इस्तेमाल करें, जिससे सायबर बदमाशी से बच्चों को टाला जा सके या अनुपयुक्त विषय-सामग्री पर पहुँच को रोका जा सके|
- यह सुनिश्चित करें कि आपके बच्चे की शाला में इंटरनेट सुरक्षा शिक्षण प्रोग्रामिंग है|
- आप शाला के प्राधिकारियों से अनुरोध कर सकते हैं कि वे छात्रों को सिखाएँ या उनका मार्गदर्शन करें कि ऑनलाइन समकक्ष उत्पीड़न को कैसे रोकें और उस पर प्रतिक्रिया दें और बताएँ कि सोशल नेटवर्किंग साईट्स एवं जवाबदार ऑनलाइन उपयोगकर्त्ताओं से किस तरह बुद्धिमत्ता पूर्वक पारस्परिक संवाद करें|
- कम्प्यूटर प्रयोगशालाओं व इंटरनेट प्रयोगशालाओं के लिए नियम बनाएँ|
- सायबर बदमाशी हेतु इंटरनेट, कंप्यूटर्स व अन्य साधन जैसे कि यूएसबी, शाला में सीडीआरओएम के उपयोग के बारे में स्पष्ट नियम, मार्गदर्शन व नीतियाँ निर्दिष्ट करें।
- सायबर बदमाशी के प्रभाव के बारे में छात्रों को सिखाएँ|
- छात्रों को सिखाएँ कि सभी प्रकार की बदमाशियाँ स्वीकार्य नहीं है और उस प्रकार के व्यवहार अनुशासन के अधीन हैं |
- छात्रों को सलाह-मशविरा और समकक्ष निगरानी का संस्थापन |
- शिक्षकों को चाहिए कि वे मार्गदर्शक रहें या वरिष्ठ छात्रों के साथ मार्गदर्शन संस्थापित करें, जिससे सूचना सुरक्षा जागरूकता के बारे में मार्गदर्शन दिया जा सके और समकक्ष छात्रों के माध्यम से निगरानी हो|
- शाला की लैब पीसी-एस में कार्यान्वयन अवरोध/ फिल्टरिंग साफ्टवेयर
- डेस्कटाप फायरवाल्स, ब्राउसर फिल्टर्स का इस्तेमाल करें, जिससे बच्चों को दूसरों की सायबर बदमाशी से बचाया जा सके या रोका जा सके या अनुपयुक्त विषय-सामग्री पर पहुँच को रोका जा सके। इसके अलावा छात्रों की ऑनलाइन गतिविधियों के लिए साफ्टवेयर साधनों की निगरानी का उपयोग करें|
- आपके छात्रों को शिक्षित करें|
- आंतरिक व बाह्य विशेषज्ञों के द्वारा विभिन्न प्रकार की कार्यशालाएँ आयोजित करें और उसमें सायबर बदमाशी, अच्छे ऑनलाइन व्यवहार व सूचना सुरक्षा के अन्य मुद्दों के बारे में चर्चाएँ करें। इसके अलावा शाला में संबंधित पोस्टर्स रखें|

References:

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

ऑनलाईन शिकारी

ऑनलाईन शिकारी वे इंटरनेट उपयोगकर्त्ता हैं, जो बच्चों व किशोरों का यौनिक व हिंसक उद्देश्यों के लिए शोषण करते हैं़ इसमें शामिल हैं बच्चों को संवारना, उन्हें यौनिक गतिविधियों से संबद्ध रखना, सामग्री व चित्रों को अवांछित तरीके से प्रकट करना व डर व घबराहट पैदा करने के लिए धमकी देनाश्र यह ऑनलाइन उत्पीड़न है़

ऑनलाइन शिकारियों द्वारा काम में लिए जाने वाले संचार के साधन

ऑनलाइन शिकारी व्यक्तिगत रूप से मिलने के लिए सोशल नेटवर्किंग, इमेल, चेट रूम्स, तुरंत सन्देश व साथ ही संवारने की प्रक्रिया का भी इस्तेमाल करते हैं|

- **सोशल नेटवर्किंग वेबसाइट्स का इस्तेमाल कर**
  उपयोगकर्त्ता के विचारों को व्यक्त करने, फोटोस डालने व उन्हें साझा करने तथा वेबसाईट्स के वीडियोज के लिए सोशल नेटवर्किंग वेबसाइट्स बहुत लोकप्रिय हैं़ इन वेबसाईट्स का ऑनलाइन शिकारी लाभ लेते हैं और वे ऐसे बनते हैं, जैसे कि वे बालक हों और फिर ऑनलाइन मित्रता बना लेते हैं और फिर वे व्यक्तिगत विवरण इकट्ठे कर लेते हैं और आहिस्ते यौन-संचार शुरूकर आपके साथ आपको यौन-गतिविधियों से संबद्ध कर देते हैं़

- **ई-मेल पते का इस्तेमाल कर**
  ऑनलाइन शिकारी बच्चों के ई-मेल पते एकत्रित करते हैं और फिर उन्हें अश्लील साइट्स से संबंधित फोटो भेजना शुरूकरते हैं और इस प्रकार बच्चों से दुष्कर्म का प्रयास करते हैं और बच्चे को आतंकित कर बाध्य करते हैं कि वह यौनिक संचार से जुड़े और तब बालक बेचैनी महसूस करने लगते हैं़

- **चेट रूम्स के द्वारा**
  ऑनलाइन शिकारी चेट रूम्स से बालक बन कर जुड़ जाते हैं जिससे वे बच्चों के साथ गपबाजी शुरूकर उसकी

व्यक्तिगत जानकारियाँ एकत्रित कर सकें और उसका अच्छा मित्र बनने की कोशिश करते हुए वह बच्चे की दिलचस्पियाँ, उसके शौक, उसके व्यक्तिगत फोटोग्राफ्स के बारे में मालूम करता है और फिर निजी गपशप के लिए पूछता है और कुछ उपहार देता है़ कई बार शिकारी बच्चे के लिए बहुत दयालु व भावनाप्रद बन जाते हैं और फिर धीरे-धीरे अपनी बातचीत में यौनिक विषय-सामग्री मिलाने लगते हैं और बच्चे को कहते हैं कि वह इस बारे में माता-पिता को न बताते हुए गोपनीयता बनाए रखे़ यदि बच्चा इससे सहमत नहीं होता है, तब वे उसे धमकी दे सकते हैं और दुष्कर्म के लिए समर्पण करवा सकते हैं़

- **संवरने की प्रक्रिया के द्वारा**

  ऑनलाइन शिकारी फर्जी विश्वास, संबंध निर्मित करता है और बच्चे के प्रतिरोध को समाप्त करता है और आमने-सामने मिलने की कोशिश करता है़

- **ऑनलाइन शिकारियों द्वारा धमकी**

  जब अप उनसे गपशप करना बंद कर देते हैं, तब ऑनलाइन शिकारी आतंकित करने लगते हैं और आप पर निजी रूप से मिलने के लिए आपके परिवार के सदस्यों व मित्रों को नुक्सान पहुँचाने की धमकी देते हैं़

- ✔ सदैव सुरक्षा के उपाय करते रहे, जैसे कि निजी सेटिंग्स और आपकी प्रोफाईल देखने के लिए सीमित दर्शन स्थापित करना़
- ✔ अनजान उपयोगकर्त्ताओं की मेल पर ध्यान न दें या उसे हटा दें़
- ✔ यह परामर्श दिया जाता है कि व्यक्तिगत जानकारियाँ जैसे कि दिलचस्पियाँ, शौक व परिवार के विवरण ऑनलाइन मित्रों से छिपाएँ़
- ✔ आपके शौक व विचार को बदलने के बारे में किन्हीं अजनबियों के कहे में न आएँ़ यदि आप अपने ऑनलाइन मित्र से मिलना चाहते हैं तो अपने माता-पिता को साथ ले जाएँ़
- ✔ धमकियों से न डरें और अपने माता-पिता को सूचित करें और पुलिस को रिपोर्ट करें़

> जब आप उनके साथ गपशप बंद कर देते हैं तब ऑनलाइन शिकारी आपके परिवार के सदस्यों व मित्रों को हानि पहुँचाने की धमकियां देते हुए आप पर रूबरू मुलाकात करने के लिए दबाव बनाते हैं़

ऑनलाइन शिकारियों को कैसे रोकें?

यदि कोई आपको बिना किसी कारण के कोई उपहार दे और मिलना चाहे और बड़ा स्नेही बनने की कोशिश करे तब ये उसके ऑनलाइन शिकारी होने के चिन्ह हो सकते हैं़

आपको गुमराह करने की कोशिश की तकनीक को पहचाने

यदि आपको कोई उपहार देता है और यदि कोई अजनबी आपसे व्यक्तिगत रूप से मिलना चाहता है और आपके प्रति बहुत

स्नेही बनने की कोशिश करता है, तब सावधान हो जाइए, क्योंकि ये ऑनलाइन शिकारी की चालें हो सकती हैं, और वे शायद आपको गलत दिशा में ले जाने की कोशिश करते होंप्र

मुंहबोले नाम का उपयोग करें

सुनिश्चित करें कि आपने उपयोगकर्त्ता के नाम का चयन बिना वास्तविक नाम के उपयोग के किया हैप्र

आपकी ऑनलाइन प्रोफाईल में आपके निजी विवरण न भरेंप्र

सोशल नेट्वर्किंग में आपके निजी विवरण न डालें, क्योंकि वहाँ आपके विवरण कोई भी देख सकता हैप्र

ऑनलाइन गपशप के लिए स्थापित नियम

ऐसे नियम स्थापित करें, जैसे कि समय-सीमा और इंटरनेट का इस्तेमाल माता-पिता के मार्गदर्शन में ही करना है और सुनिश्चित करें कि कंप्यूटर को साझा कमरे में रखा गया हैप्र

लैंगिक गपशप तथा घर व शालाओं की समस्याओं को टालेंप्र

आपके लिंग, उम्र, स्थल से संबंधित विषयों को टालें तथा घर व शालाओं की समस्याओं को साझा न करेंप्र

यदि आपको धमकाया जाए

- **भयभीत न हों**

  शांत रहे, गपशप बंद कर दें व गपशप कक्ष से बाहर चले जाएँ या लॉग-ऑफ कर देंप्र
- **नहीं कहने के लिए डरें नहीं**

  यदि शिकारी के द्वारा जो कहा गया है, वैसा करने के लिए यदि आप इच्छुक नहीं हो, तो उसे नहीं कहने के लिए डरें नहींप्र
- **माता-पिता को सूचित करें**

  यदि कोई आपको धमकाता है, तो अपने माता-पिता को तुरंत सूचित करेंप्र
- **आपकी बातचीत के सबूत के लिए एक स्क्रीन शॉट ले लें और कहें कि आप इसकी रिपोर्ट पुलिस में करेंगेप्र**

  यदि कोई अभद्र भाषा का इस्तेमाल करता है या धमकाता है तो आपकी बातचीत का एक स्क्रीन शॉट ले लें और उन्हें कहें कि आप इसकी रिपोर्ट पुलिस में करेंगेप्र
- **लॉग ऑफ न होंप्र**

  यदि कोई आपको गाली देने की कोशिश करता हो तो तुरंत लॉग ऑफ न करें और माता-पिता को तथा क़ानून प्रवर्तन को सूचित करेंप्र
- **सायबर पुलिस से सम्पर्क करेंप्र**

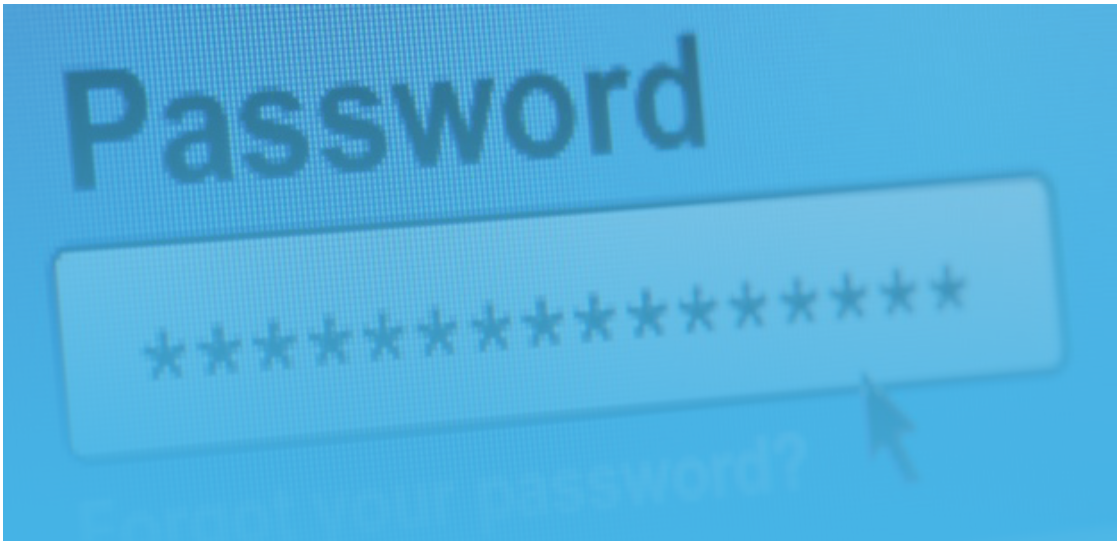
  यदि कोई चरम पर जाते हुए आपके परिवार के सदस्यों को हानि पहुँचाने की धमकी देता है, तब तुरंत साईबर पुलिस से संपर्क करेंप्र

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

like

They may be spooffed offers

Never respond



पासवर्ड्स के संबंध में

पासवर्ड वह मूल या गुप्त शब्द है या लिपिचिन्हों की वह श्रेणी है, जिसका उपयोग साईबर की दुनिया में दूसरों से आपकी परिसंपत्तियों या जानकारियों को संरक्षित करने के लिए किया जता है इसका उपयोग प्राधिकृत करने हेतु तथा हमारी पहचान को सिद्ध करने के लिए या हमारे स्वयं के स्त्रोतों तक की पहुँच की प्राप्ति के लिए किया जाता है अप्राधिकृत उपयोगकर्त्ताओं द्वारा उनकी पहुँच की रोकथाम के लिए इसे गुप्त रखा जाना चाहिए

सोशल नेटवर्क साईट्स जैसे कि फेसबुक, आर्कुट व लिंकेडीन में प्रत्येक उन जवाबों से सज्ज हैं, जिनका उपयोग सामान्यतः सुरक्षा सवालों के लिए किया जाता है, जैसे कि पसंदीदा स्थल, शाला, महाविद्यालय आदि

पासवर्ड्स का महत्व

- पासवर्ड किसी सिस्टम के लिए किसी व्यक्ति की पहचान प्रस्तुत करता है
- पासवर्ड से व्यक्तियों को मदद मिलती है, जिसके द्वारा अप्राधिकृत उपयोगकर्त्ता, व्यक्तिगत जानकारियाँ न देख सकें, इस हेतु उन्हें संरक्षित कर सकते हैं इसलिए यह महत्वपूर्ण है कि पासवर्ड्स को सुरक्षित रखा जाए
- उपयोगकर्त्ताओं व उनकी व्यक्तिगत जानकरियों के बीच पासवर्ड्स एक बाधा की तरह कार्य करते हैं

पासवर्ड्स के संभवित दोष

- पासवर्ड्स को अन्य लोगों के साथ साझा कर उनका दुरुपयोग किया जा सकता है
- पासवर्ड्स लोग भूल सकते हैं
- चुराए गए पासवर्ड का उपयोग अप्राधिकृत उपयोगकर्त्ता के द्वारा किया जा सकता है और उसके द्वारा आपकी व्यक्तिगत जानकारियाँ एकत्रित की जा सकती हैं
- आसान पासवर्ड्स जैसे कि नाम, जन्मदिनाँक, मोबाईल नम्बर का अनुमान किसी के द्वारा भी लगाया जा सकता है और तब उनका दुरुपयोग हो सकता है
- यदि आप सभी खातों के लिए एक ही पासवर्ड का उपयोग करते हैं, तो हेकर्स के लिए ९० आसान मौके होते हैं कि वे सभी खातों के पासवर्ड को केक कर लें

आपके पासवर्ड्स की पुन:प्राप्ति के लिए हेकर्स/ केकर्स के द्वारा विभिन्न तकनीकों का इस्तेमाल किया जाता है

शोल्डर सर्फिंग

व्यक्ति के पीछे ख़डे रह कर उसके कंधों की ओर देखते हुए, जब वे उसे टाईप कर रहे हों उनके पासवर्ड को पढ़ना, पासवर्ड चुराने का एक तरीका होता है शोल्डर सर्फिंग अवलोकन की सीधी तकनीक है, जैसे कि किसी के कंधों की ओर देखते हुए पासवर्ड्स, पीआईएनएस व अन्य संवेदनशील व्यक्तिगत जानकारियाँ प्राप्त करना या जब आप फोन पर किसी को अपना केडिट कार्ड नम्बर दे रहे हों, तब उस बातचीत को चोरीछिपे सुनना

भीड़ भरी जगहों पर शोल्डर सर्फिंग आसानी से हो जाती है किसी के साथ ख़डे रह कर उसे कोई प्रपत्र भरते हुए, एटीएम पर पीआईएन नंबर प्रविष्ट करते हुए, या सार्वजानिक पे फोन पर कालिंग कार्ड का उपयोग करते हुए उसे देखना, तुलनात्मक रूप से आसान होता है इसे बाइनोकूलर या अन्य किसी दृष्टिवृद्धि के उपकरण की मदद से दूर रह कर भी कर सकते हैं

आपकी गोपनीय जानकारियाँ जोखिम में होंगी, यदि आपके पासवर्ड्स

शोल्डर सर्फर्स द्वारा देखे जाते हैं वे आपकी पासवर्ड जानकारी का उपयोग आपके खाते के लॉग इन के लिए कर सकते हैं और वे आपकी जानकारियों को हानि पहुंचा सकते हैं

संकेत : आपके बच्चों को समझाएँ कि वे जनता के स्थलों, जैसे कि इंटरनेट केन्द्रों या शालाओं पर शोल्डर सर्फर्स से तब सावधान रहें, जब वे अपने लॉग इन खातों में अपने पासवर्ड्स प्रविष्ट करते हैं उनसे कहें कि दूसरों के सामने अपने पासवर्ड्स जाहिर न करें और न ही अनाधिकृत व्यक्तियों के समक्ष उनके उपयोगकर्त्तानाम व पासवर्ड्स टाईप नहीं करें उनसे कहें कि वे कीबोर्ड को किसी कागज या हाथ या किसी चीज से ढंक ले, जिससे कि अनाधिकृत उपयोगकर्त्ताओं को देखने से रोका जा सके

पशुबल का आक्रमण

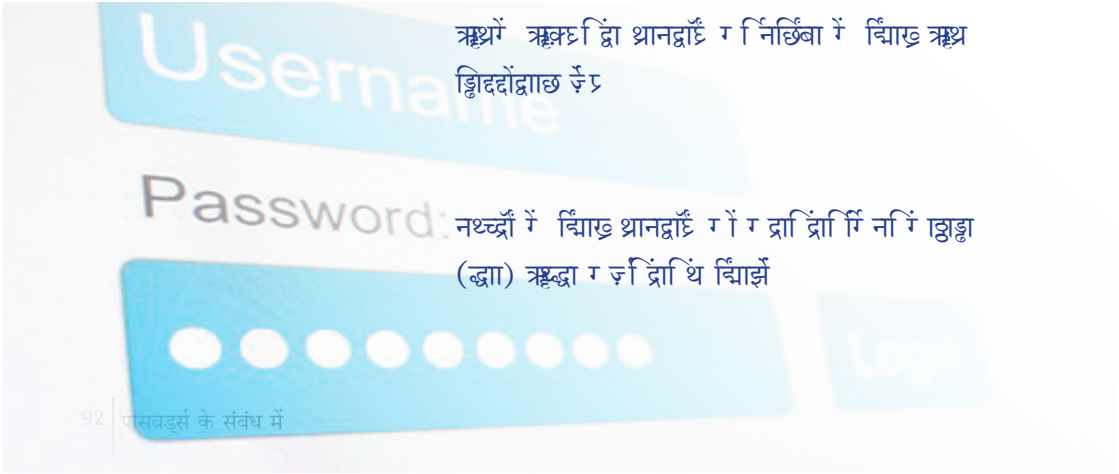
पासवर्ड का चुराने का एक अन्य तरीका है, अटकल लगाना किसी व्यक्ति की निजी जानकारियों की मदद से हेकर्स सभी संभावित संयोजनों की कोशिश करते हैं वे उस व्यक्ति के नाम, उसके लाड़ के नाम (उपनाम), संख्याएँ (जन्म दिनाँक, फोन नम्बर), शाला का नाम... आदि के द्वारा कोशिश करेंगे जब पासवर्ड्स के संयोजनों की संख्या बहुत बड़ी होती है, तब वे पासवर्ड को तोड़ने के लिए तेज प्रोसेसर्स व कुछ साफ्टवेयर साधनों का इस्तेमाल करते हैं पासवर्ड तोड़ने के इस तरीके को पशुबल का आक्रमणकहते हैं

संकेत : आपके बच्चों को बताएँ कि उस पासवर्ड को उपयोग में न लें, जो उनकी व्यक्तिगत जानकारियाँ जैसे कि उपनाम, फोन नम्बर, जन्मदिनाँक आदि बताते हों

शब्दकोश का आक्रमण

सभी संभवित शब्दकोश के शब्दों के साथ हेकर्स कुछ सॉफ्टवेयर साधनों की मदद पासवर्ड तोड़ने की कोशिश करते हैं इसे शब्दकोश का आक्रमणकहते हैं

संकेत : आपके बच्चों को बताएँ कि खातों की लॉग इन के लिए पासवर्ड का निर्माण करते समय शब्दकोश के शब्दों का उपयोग न करें (जैसे कि प्राणी, पौधे, चिड़ियाएँ या उनके आशय)



We always use

strong & easy to remember

PASSWORD[S]

for Internet applications

Do You ?

for more details visit

www.infosecawareness.in

नेटवर्क के द्वारा आपकी पासवर्ड की जानकारी भेजना

नेटवर्क के प्रवास पर जो रहती है, तब उसके नेटवर्क यातायात को सूंघकर भी हेकर्स/ केकर्स पासवर्ड की जानकारी प्राप्त कर लेते हैं या आपके द्वारा दूसरों से की गई फोन पर बातचीत सुनकर भी पासवर्ड की जानकारी प्राप्त कर सकते हैं

संकेत :आपके बच्चों को सिखाएँ कि वे अपने मित्रों या किसी अन्य को भी ऑनलाइन गपशप, मेल्स या फोन पर बातचीत में अपने पासवर्ड न दें

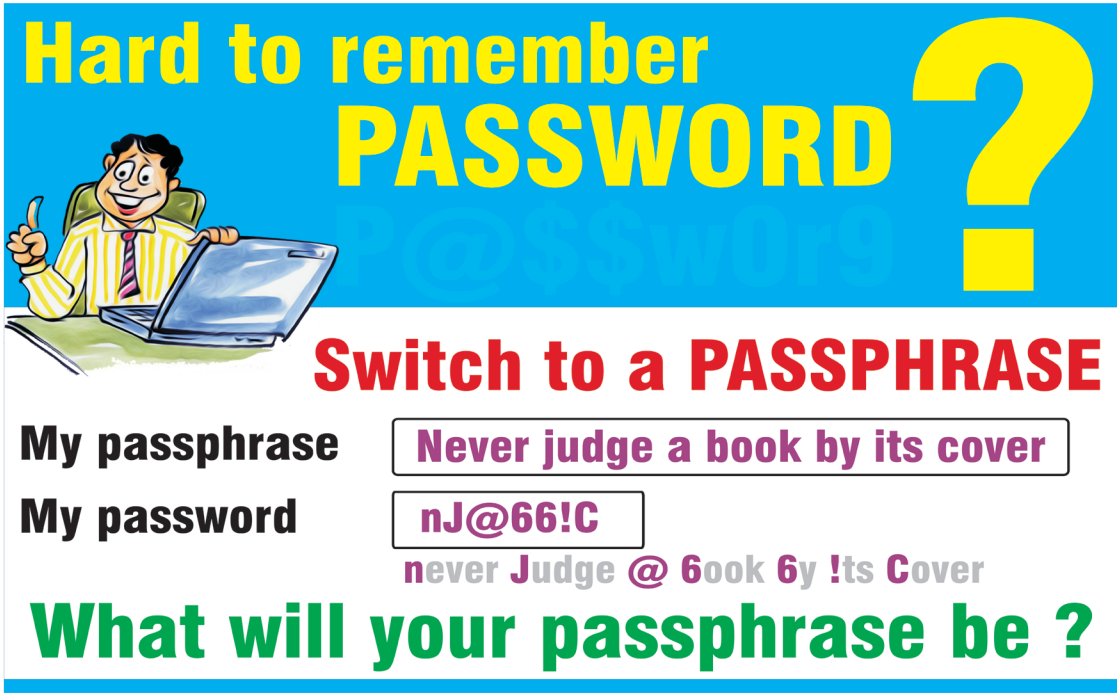
आपके पासवर्ड्स को अजनबियों के साथ साझा करना

पासवर्ड्स को अनजान लोगों (अजनबियों) के साथ साझा करने से भी आपकी व्यक्तिगत जानकारियों का नुकसान हो सकता है वे आपकी लॉगइन जानकारियों का इस्तेमाल कर आपकी जानकारियों तक पहुँच बना सकते हैं ऑपरेटिंग प्रणाली को यह मालूम नहीं होता है कि सिस्टम में कौन लॉगइन है, वह तो मात्र किसी भी उस आदमी को मंजूरी दे देता है, जो लॉगइन पृष्ठ पर प्रत्यय जानकारियाँ प्रविष्ट करता है आपकी जानकारियों तक पहुँच कर अजनबी उसके साथ कुछ भी कर सकते हैं वे उसकी नक़्ल कर सकते हैं, संशोधन कर सकते हैं या हटा सकते हैं

संकेत :आपके बच्चों को बताएँ कि वे अपने पासवर्ड अनजान व्यक्तियों (अजनबियों) से साझा न करें

पासवर्ड्स को याद रखना सशक्त व सबसे सरल

एक सशक्त पासवर्ड में अक्षरों, संख्याओं व लिपिचिन्हों का संयोजन होना चाहिए, जैसे कि ब.!;)(. ये याद रखें कि ये पासवर्ड बहुत कठिन होते हैं जैसा नीचे दिखाया गया है, वैसा बनाया जा सकता है



कमजोर या रिक्त पासवर्ड्स का उपयोग

हमला कर आपके सिस्टम को तोड़ने के लिए कमजोर या रिक्त पासवर्ड्स हमलावरों के लिए आसान तरीके होते हैं

संकेत : आपके बच्चों को बताएँ कि यदि वे कमजोर पासवर्ड्स का इस्तेमाल करते हैं तो अजनबियों के द्वारा उनकी जानकारियाँ आसानी से चुराई जा सकती हैं या वे उन तक पहुँच सकते हैं उनसे कहें कि सशक्त पासवर्ड्स का उपयोग करें

सशक्त पासवर्ड्स को निर्मित करते समय याद रखनेवाली बातें

- पासवर्ड्स का निर्माण करते समय कम से कम ८ लिपि चिन्हों को प्रयोग में लें जितने अधिक लिपि चिन्ह, उतना ही अधिक आपका पासवर्ड सुरक्षित
- पासवर्ड्स का निर्माण करते समय लिपि चिन्हों के विभिन्न संयोजनों का उपयोग करें उदहारण के लिए, ऐसे पासवर्ड् का निर्माण करें जिसमें छोटे अक्षर, बड़े अक्षर, संख्याएँ व विशेष लिल्पी चिन्हों आदि का मिश्रण हो
- शब्द कोश में से शब्दों के इस्तेमाल को टालें
- ऐसे पासवर्ड्स का निर्माण करें, जिसे याद रखा जा सके इससे पासवर्ड को कहीं लिखने की जरूरत को टाला जा सकता है और उसके लिए परामर्श नहीं दिया जाता है
- पासवर्ड्स ऐसा हो, जिसका अनुमान लगाना कठिन होना चाहिए
- पासवर्ड्स को बारंबार बदलते रहे, न्यूनतम २ सप्ताहों में एक बार

उत्तम पासवर्ड बनाए रखने की मार्गदर्शिका

- पासवर्ड्स को दो सप्ताहों में एक बार बदलें या तब जब आपको शंका हो कि किसी को पासवर्ड मालूम है
- ऐसे पासवर्ड का उपयोग न करें, जिसका इस्तेमाल पहले हो चुका हो
- यदि कोई आपके पास बैठा हो, तब किसी पासवर्ड को प्रविष्ट करते समय सावधानी बरतें
- इनक्रिप्शन सेवाओं की मदद से पासवर्ड्स को कंप्यूटर में स्टोर करें
- अपने खाते के पासवर्ड के लिए उन वस्तुओं के नाम का उपयोग न करें, जो आपके आसपास हों

मोबाईल फोन सुरक्षा

मोबाईल फोन इन दिनों बहुत लोकप्रिय होते जा रहे हैं और शरारतपूर्ण हमलों के लिए वे आकर्षक लक्ष्य बनते जा रहे हैं सुरक्षा के संबंध में मोबाईल फोन के लिए भी वही चुनौतियाँ हैं, जैसी कि परम्परागत डेस्कटाप कंप्यूटर्स के लिए रहती हैं, लेकिन उनमें मोबिलिटी का अर्थ है कि एक ही जगह रहने वाले कंप्यूटर की तुलना में इनकी दिखाई पड़ने वाली जोखिम अलग तरह की हैं मोबाईल फोन कीटाणुओं, ट्रोजन हार्सेस या अन्य वायरस परिवारों से संक्रमित हो सकते हैं, जो आपकी सुरक्षा व निजता के साथ समझौता कर सकते हैं या बल्कि इस साधन पर पूर्ण नियंत्रण प्राप्त कर लेते हैं यह मार्गदर्शिका उठाए जाने वाले आवश्यक कदम, क्या करना चाहिए व क्या न करना चाहिए और आप अपने मोबाईल साधनों को किस प्रकार सुरक्षित रखें ऐसी युक्तियों के बारे में यह बताती है

मोबाईल फोन के उपयोग के पहले लिए जाने वाले कदम

चरण १ उत्पादक की नियमपुस्तिका को ध्यान से पढ़ें और आपके मोबाईल फोन को सेट करने के लिए जैसा विनिर्दिष्ट किया गया है, उसके अनुसार मार्गदर्शिका का अनुपालन करें

चरण २ आईएमईआई अंतरराष्ट्रीय मोबाईल उपकरण पहचान नंबर को रिकार्ड करें, जिससे उसके गुम होने की स्थिति में मोबाईल की स्थिति मालूम कर सकें

नोट यह सामान्यतः फोन पर बैटरी के नीचे मुद्रित होता है या अधिकांश फोन में ०६ इससे प्रेरित कर उस तक पहुँचा जा सकता है

मोबाईल फोन सुरक्षा पर आशंकाओं की श्रेणियाँ

- मोबाईल उपकरण व डाटा सुरक्षा आशंकाएँ
  - मोबाईल फोन तथा गुम या चुराए गए मोबाईल फोन के लिए अनाधिकृत या अंतरराष्ट्रीय भौतिक पहुँच से संबंधित आशंकाएँ
- मोबाईल संयोजकता सुरक्षा की आशंकाएँ
  - अनजाने सिस्टम्स, फोन व नेटवर्क जिसमें ब्ल्यूटूथ, वायफाय, यूएसबी आदि का उपयोग होता हो, उनमें मोबाईल फोन संयोजकता सुरक्षा से संबंधित आशंकाएँ
- मोबाईल एप्लीकेशन व संचालन प्रणाली सुरक्षा की आशंकाएँ
  - मोबाईल एप्लीकेशन व संचालन प्रणाली में उसकी संवेदनशीलता से उत्पन्न आशंकाएँ

मोबाईल फोन पर हमले के विशेष प्रभाव

- मोबाईल फोन में संग्रहित उपयोगकर्त्ता के व्यक्तिगत विवरण/ आँकड़ों का प्रकटन या उनकी हानि
- उपयोगकर्त्ता की जानकारी के बगैर साफ्टवेयर का दुर्भावनापूर्ण प्रीमियम उपयोग व उच्च मूल्य की एसएमएस व कॉल सेवाओं के कारण आर्थिक नुकसान
- निजता पर हमला, जिसमें सम्मिलित हैं निजी एसएमएस सहित मोबाईल फोन की जगह का पता लगाना और उपयोगकर्त्ता की जानकारी के बगैर कॉल करना
- मोबाईल फोन पर नियंत्रण खोना और अनजाने ही लक्ष्य पूर्वक किए गए हमलों से उल्लू बनना

मोबाईल साधन व डाटा सुरक्षा हमलों में कमी

मोबाईल उपकरण

क्या करें

आईईएमई नम्बर रिकार्ड करें

१५ आँकड़ों के अनूठे आईएमईआई नंबर को रिकार्ड करें यदि मोबाईल फोन चोरी चला गया हो/ गुम हो गया हो, तब पुलिस स्टेशन पर शिकायत दर्ज करने के लिए इस आईएमईआई नंबर की जरूरत पड़ती है, जिस वजह से सेवा प्रदाता के माध्यम से आपके मोबाईल फोन के मार्ग को ढूँढने में यह मददगार हो सकता है

उपकरण में लॉकिंग उपलब्ध कराना

ऑटोलॉक का इस्तेमाल करें, जिससे फोन या कीपेड स्वतः ही लॉक हो जाएँ और तब आपके मोबाईल फोन पर पहुँच प्रतिबंधित रहे, इसलिए वे पासकोड/ सुरक्षा पैटर्न से संरक्षित रहते हैं

एसआईएम कॉर्ड को लॉक करने के लिए पीआईएन का उपयोग करें

एसआईएम ग्राहक पहचान माड्यूल कॉर्ड के लिए पीआईएन व्यक्तिगत पहचान नंबर का उपयोग करें, जिससे जब चोरी हो जाए, तब वह लोगों को उसका उपयोग करने से रोकें एसआईएम सुरक्षा को चालू करने के बाद फोन के शुरूहोने पर हर बार प्रेरित करेगा कि उसमें एसआईएम पीआईएन प्रविष्ट करें

स्मृति कार्ड की जानकारियों के संरक्षण के लिए पासवर्ड का उपयोग करें

गुम या चोरी गए साधनों की रिपोर्ट करें

गुम हुए या चोरी चले गए साधनों की रिपोर्ट तुरंत पुलिस स्टेशन में तथा संबंधित सेवा प्रदाता को दर्ज कराएँ

मोबाईल ट्रेकिंग विशेषता का उपयोग करें

मोबाईल ट्रेकिंग विशेषता का उपयोग करें, जिससे गुम हुए/ चोरी चले गए मोबाईल फोन का पता लगाने में मदद मिल सकती है हर बार एक नया एसआईएम कार्ड डाला जाता है, जिससे वह आपकी पसंद के पहले से ही चयनित दो फोन नंबर्स पर स्वमेव सन्देश भेजेगा, जिससे आप आपके मोबाईल साधन को ट्रेक कर सकें

न करें

कभी भी किसी की निगरानी के बगैर आप आपके मोबाईल साधन को न छोड़े

जब इस्तेमाल में न आ रहे हों, तब वस्तुओं कैमरा, ऑडियो/ विडिओ प्लेयर्स व संयोजन ब्ल्यू टूथ, इन्फ्रारेड, वायफाय को बंद कर दें संयोजन को चालू रखे रहने से सुरक्षा के मुद्दे उठ सकते हैं व साथ ही इससे बैटरी कमजोर हो सकती है

डाटा की सुरक्षा के लिए

करें

नियमित रूप से डाटा बेकअप करें

नियमित रूप से डाटा बेकअप करें और अपने फोन को इस तरह सेट करें, जिससे जब आप उन्हें सिंक करें, तब वे आपके डाटा को बैक अप करें आप एक पृथक स्मृति कार्ड पर भी बेकअप ले सकते हैं इसे विकेता की बेकअप क्रियाविधि दस्तावेज का इस्तेमाल कर भी किया जा सकता है

कारखाने की सेटिंग्स को पुनः सेट करें

जब फोन स्थायी रूप से किसी अन्य उपयोगकर्त्ता को दिया जाए तब यह सुनिश्चित करें कि कारखाने की सेटिंग्स को पुनः सेट करना है, यह सुनिश्चित करने के लिए कि फोन में से व्यक्तिगत डाटा हटा दिए गए हैं

मोबाईल संयोजन सुरक्षा आक्रमण में कमी

ब्ल्यूटूथ

ब्ल्यूटूथ एक बेतार के तार की तकनीक है, जिससे विभिन्न साधन एक दूसरे से जुड़ जाते हैं और वे तब डाटा जैसे कि रिंगटोंस या फोटोस को साझा करने लगते हैं ब्ल्यूटूथ से भेजे जानेवाले बेतार के सिग्नल्स छोटी दूरियाँ ही समाहित कर पाते हैं, ३० फीट की १० मीटर्स

करें

- ब्ल्यूटूथ को छिपे हुए मोड में उपयोग करें, जिससे यदि साधन ब्ल्यूटूथ का उपयोग कर रहा होगा, तब भी वह अन्य किसी को दिखाई नहीं देगा साधन का नाम परिवर्तित कर कोई भिन्न नाम दे दें, जिससे आपके मोबाईल फोन के मॉडल की पहचान को टाला जा सके
- नोट ब्ल्यूटूथ साधनों के लिए चूक का नाम ही मोबाईल का मॉडल नम्बर होगा

- अन्य साधनों के साथ जोड़ बनाते समय एक पासवर्ड डालें समान पासवर्ड के साथ के साधन आपके कंप्यूटर से जोड़ सकते हैं यदि ऐसा है तो स्वचलित जोड़ बनाने के विकल्प को असमर्थ कर दें
- ब्ल्यूटूथ को असमर्थ कर दें, यदि वह सक्रिय रूप से जानकारियों को संचारित नहीं कर रहा है
- ब्ल्यूटूथ का इस्तेमाल अस्थायी समयावधि में करें, जिससे बाद वह स्वतः ही असमर्थ हो जाता है, जिससे साधन दूसरों को सतत उपलब्ध नहीं रहता है

न करें

- ब्लूटूथ के माध्यम से अनजान साधनों को कभी नहीं जोड़ें
- ब्लूटूथ को कभी भी सतत चालू नहीं रखें
- ब्लूटूथ को सदैव कभी भी खोजने योग्य मोड में न रखें
- नोट हमलावर इस चूक का फायदा उठा सकते हैं सदैव ऑन, हमला शुरु करने के लिए सदैव खोजने योग्य की सेटिंग्स

यूएसबी के रूप में मोबाईल

जब किसी कंप्यूटर से जोड़ा जाता है, तब मोबाईल्स फोन का उपयोग यूएसबी स्मृति साधन के रूप में किया जा सकता है कंप्यूटर से जोड़ने के लिए मोबाईल फोन के साथ एक यूएसबी केबल भी उपलब्ध कराया जाता है

आपके मोबाईल फोन की स्मृति व स्मृति स्टिक को यूएसबी साधनों का अनुषंगी मान सकते है

करें

- जब एक मोबाईल फोन किसी व्यक्तिगत कंप्यूटर से जोड़ा जाए, तब अद्यतन एंटी वायरस का उपयोग करते हुए बाहरी फोन स्मृति व स्मृति कार्ड स्केन करें
- आपके फोन व बाहरी स्मृति कार्ड का नियमित बेकअप लें, क्योंकि यदि प्रणाली केश होती है या मेलवेयर हमला होता है, तब कम से कम आपके डाटा सुरक्षित रहेंगे
- कंप्यूटर से मोबाईल में डाटा अंतरित करने के पहले, नवीनतम व अद्यतन एंटीवायरस के साथ डाटा स्केन होना चाहिए

न करें

- मोबाईल फोन्स पर संवेदनशील जानकारियाँ जैसे कि उपयोगकर्त्ता के नाम/ पासवर्ड्स नहीं रखें
- अन्य मोबाईल्स पर कभी भी वायरस से प्रभावित डाटा फारवर्ड नहीं करें

वायफाय

वायफाय वायरलेस फिडेलिटीका संक्षिप्त रूप है वायफाय से अर्थ है नेट्वर्किंग की बेतार तकनीक, जिसके द्वारा कंप्यूटर्स व अन्य साधन बेतार के सिग्नल पर संचार करते हैं

कई मोबाईल उपकरण, वीडियो गेम सिस्टम्स व अन्य अकेले साधन जिसमें वायफाय सक्षमता भी शामिल है, वे बेतार के नेटवर्क्स से जोड़ने हेतु उन्हें सक्षम बनाते हैं ये साधन वायफाय का उपयोग कर इंटरनेट से जोड़ने में समर्थ हो सकते हैं

करें

- केवल विश्वसनीय नेटवर्क्स से ही जोड़ें
- जब जरूरत हो तब ही वायफाय का इस्तेमाल करें यह सलाह दी जाती है कि जब वह उपयोग में न हो, तब उसका स्विच ऑफ कर दें
- सार्वजनिक नेटवर्क से जोड़ते समय सावधानी बरतें, क्योंकि वे सुरक्षित न भी हो सकते हैं

न करें.

- अनजान नेटवर्क्स या अविश्वसनीय नेटवर्क्स से कभी भी न जोड़ें
- यदि मोबाईल अधिक कष्ट सहने में समर्थ होने का विकल्प देता है, तो उसे पासवर्ड के साथ संरक्षित करें

मोबाईल एप्लीकेशन व संचालन प्रणाली के हमलों में कमी

एप्लीकेशन व मोबाईल संचालन प्रणाली

- मोबाईल संचालन प्रणाली को नियमित अद्यतन करते रहें
- नवीनतम संस्करण में संचालन प्रणाली को अद्यतन बनाएँ
- सदैव विश्वस्त स्त्रोतों से ही एप्लीकेशंस संस्थापित कराएँ
- प्रतिष्ठित प्रदाता से ही सुरक्षा साफ्टवेयर के संस्थापन पर विचार करें और उन्हें नियमित तौर पर अद्यतन करते रहें
- किसी एप्लीकेशन को डाउनलोड करने से पहले, उसकी विशिष्टताओं की जाँच करना सदैव मददगार रहता है कुछ एप्लीकेशंस आपके व्यक्तिगत डाटा का उपयोग कर सकते हैं
- यदि आप किसी तीसरे पक्ष से कोई एप डाऊनलोड कर रहे हैं, तो कुछ शोध कर यह सुनिश्चित करें कि एप प्रतिष्ठित है

> संकेत स्थल ट्रेकिंग सेवाओं के द्वारा पंजीकृत सेल फोंस कहाँ हैं, वह जाना जा सकता है और उन्हें नियंत्रित किया जा सकता है यद्यपि वैधानिक उद्देश्यों के लिए इसका उपयोग मुक्त रूप से किया जा सकता है, लेकिन इसका इस्तेमाल दुर्भावनापूर्ण उद्देश्यों के लिए भी हो सकता है
>
> संकेत आपकी सभी फाईल्स व एप के स्त्रोत की जाँच यह सुनिश्चित करने के लिए करें कि आप उन्हें डाऊनलोड करें, उसके पहले वे सुरक्षित हैं

९२ या ३४४ से शुरुआती नंबरों से आए मिस्ड कॉल पर वापस कॉल बैक नहीं करें

Never respond to the calls from the following country codes +92, +90, +09 or +344, if you don't have relative / friends in those countries

९२, (हैश) ९०, (हैश) ०९ या ३४४ के शुरुआती नंबर वाले फोन नंबर वाले देशों में आपके रिश्तेदार या दोस्त के नहीं होने पर उन नंबरों के फोन का जवाब नहीं दें।

If you pick/call back it could lead to your SIM Cloning and may lure you with Spoofed Offers

कॉलबैक/फोन रिसीव होने की स्थिति में सिम क्लोन की जा सकती है एवं कॉल से धोखे से भरा लालच दिया जा सकता है।

www.InfoSecawareness.in

क्रेडिट और डेबिट कार्ड / एटीएमका सुरक्षित उपयोग

सुरक्षाके जोख़िमो

पहचानकी चोरी :

धोखाधड़ी अधिग्रहण और व्यक्तिकी निजी पहचानके लिए जानकारीका उपयोग, आमतौर पर आर्थिक लाभके लिए | इसको दो व्यापक श्रेणीयोंमें बांटा जा सकता है:

- **आवेदन धोखाधड़ी:**
  जब कोई अपराधी चोरी किया हुआ और नकली दस्तावेजोंका उपयोग किसी दूसरेके नाममें खाता खोलनेके लिए करता है वह आवेदन धोखाधड़ी है | अपराधियों उपयोगी निजी जानकारी बनानेके लिए उपयोगिता बिल और बैंक विवरण जैसे दस्तावेजोंकी चोरी करनेकी कोशिश कर सकते हैं |
- **खाते का अधिग्रहण:**
  जब कोई अपराधी दूसरे व्यक्तिका खाता निम्नलिखित तरीकों से अधिग्रहण करनेकी कोशिश करता है वह खाते का अधिग्रहण है इच्छित शिकार के बारे में जानकारी इकट्ठा कर के वास्तविक कार्डधारक का अभिनय कर के उनके कार्ड जारीकर्ता से संपर्क करके मेल को पुनःनिर्देशित करके नए पते पर भेजनेके लिए कह कर | अपराधी तब कार्ड गुम जानेका रिपोर्ट करता है और एवज में दूसरा कार्ड भेजनेके लिए कह कर

क्रेडिट कार्ड धोखाधड़ी

क्रेडिटकार्ड धोखाधड़ी, लेन-देनमें धोखाधड़ीसे धन प्राप्त करने के लिए क्रेडिटकार्ड या अन्य समान भुगतान पध्दतिका उपयोग करके चोरी और धोखा करनेके लिए एक व्यापक परिभाषा है |

क्रेडिटकार्ड धोखाधड़ी दूसरो के केडिट / डेबिट कार्डका उपयोग करके वस्तुओं और सेवाओं प्राप्त करनेके लिए की जाती है | यह खतरा जानकारीकी चोरी जैसेकि क्रेडिटकार्ड नंबर, श नंबर, पासवर्ड वि. से उभरता है | काड्र्स की चोरी और काड्र्स की क्लोनिंग भी ऐसी धोखाधड़ी करनेके लिए काममें ली जाती है

- **फिशिंग:**

  उपयोगकर्ताको स्थापित वैध उपक्रम होनेका झूठा दावा करते हुए इ-मेल भेजने का कार्य, उपयोगकर्ताको निजी जानकारी जो पहचानकी चोरीके लिए उपयोग की जाएगी दे देनेका घोटाला करनेका प्रयास |

  फिशिंग इ-मेल आमतौर पर उपयोगकर्ताको एक वेबसाइट पर जानेके लिए कहता है जहाँ उनको निजी जानकारी अद्यतन करनेके लिए कहा जाता है जैसे पासवर्ड, क्रेडिटकार्ड, सामाजिक सुरक्षा या बैंक खाता नंबरों जो वैध संस्था के पास पहलेसे ही है | हालांकि यह वेबसाइट फ़र्जी है और उपयोगकर्ता जो भी जानकारी पृष्ठ पर दर्ज करता है उसको पकड़ लेगी और चोरी करेगी |

- **स्किम्मिंग:**

  स्किम्मिंग क्रेडिटकार्ड / डेबिटकार्ड जानकारीकी चोरी है | चुरानेवाला पीड़ितका केडिटकार्ड नंबर प्राप्त कर सकता है, बुनियादी तरीकों जैसे रसीदोंकी फोटोकॉपी या अधिक विकसित तरीकोंका उपयोग करके जैसे छोटा इलेक्ट्रॉनिक उपकरण(स्किम्मर)स्वाइप करके पीड़ितोंके सैंकड़ो केडिटकार्ड नंबरों इकट्ठा करता है | स्किम्मिंगके लिए आम परिद्रश्यो है रेस्तरां या बार जहाँ स्किम्मरके पास पीड़ितके केडिटकार्डका कब्ज़ा होता है और वह कार्डके विवरणकी आगे उपयोगके लिए नोंद कर लेता है |

- **विशिंग**

  यह सोशल इंजीनियरिंगकी टेलीफोन प्रणाली पर एक पध्दति है,सबसे अधिक बार वोइस ओवर (फ) द्वारा आसान की गई विशेषताओंका उपयोग करके,वित्तीय इनामके प्रयोजनसे प्राइवेट, निजी और वित्तीय जानकारी तक पहुँचने के लिए | यह पारिभाषिक शब्द "वोइस" और "फिशिंग"का संयोजन है |

- **सोशल इंजीनियरिंग**

  सोशल इंजीनियरिंग लोगोंको सफाईसे उल्लू बनानेकी कला है जिससे वे गोपनीय जानकारी दे दें | यहाँ जालसाज स्टाफ़का सदस्य या यहाँ तक की सुरक्षा कर्मीका ढोंग करके उपयोगकर्ताको क्षति के लिए कार्डकी जाँच करनेके लिए कहता है |

  जालसाज विभिन्न दांवपेंचका उपयोग कर सकता है जैसे ग्राहकको सहायताका प्रस्ताव दे कर जिसने शायद एटीएमका उपयोग बिना सफलतासे किया है या शायद ग्राहक एटीएमके उपयोगसे परिचित नहीं है और उन्हें सहायताकी जरुरत है |

इच्छित शिकार के बारे में जानकारी इकट्ठा कर के

क्रेडिटकार्ड और डेबिटकार्ड / एटीएम कार्ड के उपयोगसे पहले अनुसरने के कदमों:

वास्तविक कार्डधारक
का अभिनय कर के उनके
कार्ड जारीकर्ता
से संपर्क करके

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

- जब भी आप बैंक से कार्ड प्राप्त करें, यह सुनिश्चित कर लें कि डाक पूर्णतया मोहरबंद है और कोई नुकशान नहीं है ्र
- जब आप बैंक से कार्ड प्राप्त करें तुरंत कार्ड पर दस्तखत कर दें |
- कार्ड के अंतिम तीन अंकों को ढँक देने का प्रयास करें |
- खाते की लेन – देन जाँच करनेके लिए आपका फ़ोन नंबर दर्ज कराएँ |
- श नंबर तुरंत बदल दीजिए |

शॉपिंग मॉल और रेस्तरांमें क्रेडिट / डेबिट कार्ड का सुरक्षित उपयोग

- विकेता किस तरह आपका कार्ड स्वाइप करता है उस पर नज़र रखो |
- हमेशा यह सुनिश्चित करो कि लेन-देन आपकी उपस्थिति में हो |
- कभी भी कोरी क्रेडिटकार्ड रसीद पर दस्तखत मत करो | रसीदके खाली भागों में से सावधानीसे रेखा खींचे |
- रेस्तरा/शॉपिंग मॉलमें दिए गए सर्वेक्षण फॉर्ममें आपकी निजी जानकारी नहीं दे देना |

इन्टरनेट पर क्रेडिट / डेबिट कार्ड का सुरक्षित उपयोग

- लेन-देन और खरीदी के लिए हमेशा सुरक्षित वेबसाइटका उपयोग करें |
- कृपया सुरक्षा के संकेत ढूंढें |

सुरक्षा सुराग की पहचान करें जैसेकि आपके ब्राउज़रके तल पर तालाकी छवि,
जिसकी शुरुआत शॉजः से होती है(इन निशानियों सूचित करती है कि आपकी खरीदी हुई वस्तुओं एन्क्रिप्शनसे सुरक्षित है,
आपके अकाउंट जानकारीको सुरक्षित रखनेके लिए)

- हमेशा जिन व्यापारियोंको आप जानते है और भरोसा करते है उनसे खरीदारी करें
- आपके क्रेडिट/डेबिट कार्डसे ऑनलाइन लेन-देन समाप्त करने के बाद वेबसाइटसे हमेशा लॉगऑफ करें और ब्राउज़र कूकीजको नष्ट करें
- फिशिंग स्कैमसे बचने के लिए सभी इ-मेल सन्देशोंको संदेह की नज़रसे देखें | इ-मेल सन्देशों जो वित्तीय जानकारी सहित निजी जानकारी पूछते हैं उनको उत्तर न दें, क्योंकि बैंक ऐसी जानकारी पूछती नहीं है |
- भुगतानकी जानकारी कभी भी इ-मेल से न भेजें | इन्टरनेट पर जो जानकारी सफ़र करती है(जैसे कि इ-मेल) वह बाहरी पक्षों द्वारा पढ़े जानेसे सम्पूर्ण सुरक्षित नहीं है |
- निजी जानकारी ऑनलाइन देते वक्त सावधानी बरतें |
- प्रचार घोटालेसे सावधान रहनेकी जरूरत है | पहचान चुराने वाले जाली प्रस्ताव दे सकते हैं जो आपकी निजी जानकारीके बारेमें पूछते हैं |
- कृपया आपका पासवर्ड गोपनीय रखें | कुछ ऑनलाइन स्टोर्स पर खरीदी करनेसे पहले आपको उनके साथ यूजरनाम और पासवर्ड द्वारा रजिस्टर करनेकी आवश्यकता हो सकती है | ऑनलाइन पासवर्ड बाहरी पक्षोंसे गुप्त रखें, जिस तरह आप अपना एटीएम श सुरक्षित रखते हैं |
- नेटबैंकिंगके लिए हमेशा वर्चुअल कीबोर्ड का उपयोग सुनिश्चित करें ्र

करो :

- आप एटीएमका उपयोग करें उससे पहले यह कृपया सुनिश्चित कर लें कि एटीएमके प्रविष्टि पैनलमें कोई अजीब वस्तुओं नहीं है |(स्किम्मिंग से बचने के लिए)
- लेन-देन के दरम्यान एटीएम ँह नंबरको बचाके रखो | लेन-देन की रसीदें साथमें मत रखें |
- जैसे बैंक सलाह देती है वैसे पिन ३ महीनेमें एक बार बदल दें |
- आपकी केडिटकार्ड रसीदोंको लेन-देन धोखाधड़ीसे बचानेके लिए संभाल कर रखें, आपके मासिक विवरणके साथ आपकी रसीदोंको जांचे |
- जिन क्रेडिटकार्ड्स की आपको सख्त जरूरत हो वही साथमें रखें |
- जिनके ऊपर भी आपका क्रेडिटकार्ड नंबर लिखा हुआ हो उनके टुकड़े टुकड़े कर दो |(बिल्स)
- आप अपने घरका पता बदलें उसके काफी पहले आपके क्रेडिटकार्ड प्रदाताको पतेमें बदलावके बारेमें सूचित करें |
- अगर आपका कार्ड खो जाता है तो कृपया तुरंत उसकी जान करें |
- नवीकरण / उन्नयनके वक्त जब आप कार्ड का निपटारा करते हो, उसको निपटारे से पहले कृपया तिरछे काटनेका सुनिश्चित करें |

मत करो

- बैंक से प्राप्त हुआ कार्ड अगर क्षतिग्रस्त है या सील खुला है तो उसे मत स्वीकारो |
- आपके क्रेडिटकार्ड पर आपका पिन नंबर मत लिखो |
- आपका क्रेडिटकार्ड नंबर / एटीएम श किसीके सामने जाहेर मत करो |
- भले ही कोई दावा करे कि वह बैंकका प्रतिनिधि है, किसीको भी कार्ड मत सौंप दो |
- आपको एटीएम मशीनके उपयोगमें मदद करनेवाले अजनबियों के बहकावे में मत आओ |
- अगर उपकरण अच्छी स्थितिमें नहीं है तो एटीएम मशीनों का उपयोग मत करो |
- आपके खातेकी जानकारी कोई अनजान/गैर मान्य स्त्रोतके साथ हस्तांतरित या साझा न करें |
- जाहेर स्थानों में असुरक्षित कंप्यूटरसे क्रेडिट/डेबिट कार्डका उपयोग करके नेटबैंकिंग पर न जाये या भुगतान न करें |
- अनपेक्षित स्त्रोतोंसे मिले अनपेक्षित संलग्नक या इंस्टेंट मेसेजसे डाउनलोड की हुई लिंक्स न खोलें | संदिग्ध इ-मेल तुरंत नष्ट करें |
- फ़ोन पर आपका अकाउंट नंबर नहीं देना जब तक आपने खुद कॉल न किया हो या आप न जानते हो कि कंपनी प्रतिष्ठित है | जब आप कोई कॉल स्वीकारते हो तो कदापि आपकी क्रेडिटकार्ड जानकारी मत दो |(इसे विशिंग कहते हैं)
- आपके क्रेडिटकार्डकी जानकारी वेबसाइट पर प्रदान न करें जो सुरक्षित साईट नहीं है |
- कोई भी गुप्त जानकारी जैसे पासवर्ड, ग्राहकघ, डेबिट कार्ड नंबर, श भफ्फ्र, जन्मतिथि इ-मेल अनुरोध पर साझा न करें, अगर यह अनुरोध सरकारी प्राधिकारी जैसे आयकर विभाग, इळ या कोई कार्ड एसोसिएशन कम्पनी जैसे फ्झछ या मास्टर कार्ड से मिला हो फिर भी |
- आपके बैंक खातेकी समस्या या आपके खातेकी जानकारी और पासवर्ड सोशल नेटवर्किंग साइट्स या ब्लोग्स पर जिक्र या संबोधन न करें |
- महत्वपूर्ण जानकारी जैसे आपका एटीएम श नंबरका संग्रह आपके मोबाइल फ़ोनमें न करें |

Don't share bank account, Credit/Debit card details through E-mail or phone

कभी भी बैंक खाते, क्रेडिट/डेबिट कार्ड के विवरण ईमेल या फोन पर शेयर नहीं करें।

Don't hand over Debit/ Credit Card to strangers They may misuse

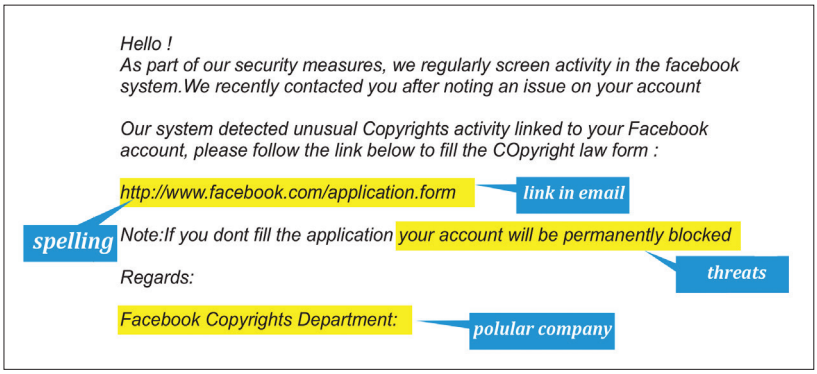
अजनबी को डेबिट/क्रेडिट कार्ड देने पर उसका दुरुपयोग हो सकता है।

फिशिंग हमले

फिशिंग उस प्रकार का प्रयास है, जिसमें इलेक्ट्रोनिक संचार जैसे कि ई-मेल द्वारा कोई विश्वसनीय सत्ता बता कर उपयोगकर्त्ताओं के नाम, पासवर्ड्स, पीआईएन, बैंक खाते, केडिट कार्ड के विवरण जैसी जानकारियाँ प्राप्त की जाती हैं।

फिशिंग प्रतीकात्मक रूप से किसी फर्जी ई-मेल या त्वरित सन्देश के द्वारा की जाती है और इसमें अक्सर उपयोगकर्त्ताओं को किसी ऐसी जाली वेबसाईट पर विवरण डालने के लिए कहा जाता है जो लगभग हर दृष्टि से विधिसम्मत लगती है। सोशल इंजीनियरिंग तकनीक का फिशिंग एक उदाहरण है, जिसका इस्तेमाल उपयोगकर्त्ताओं को धोखा देने के लिए किया जाता है।

फिशिंग ई-मेल सन्देश किस तरह का दिखता है? विस्तार से...



- वर्तनी व व्याकरण
- लिंक्स संभवतः आपको ईएक्सई फाईल्स की ओर ले जा सकती हैं्र इस प्रकार की फाईल दुर्भावनापूर्ण साफ्टवेयर को फैलाने के लिए जानी जाती हैं्र

धमकियाँ:

- कभी आप धमकीभरा मेल प्राप्त कर सकते हैं, जिसमें बताया गया हो कि यदि इस ई-मेल संदेश के अनुरूप आप प्रतिक्रिया नहीं देंगे, तो आपका वेब-मेल खाता बंद कर दिया जाएगाा्र ऊपर बताया गया ई-मेल सन्देश इस तरह की चालबाजी का एक उदाहरण हैं्र सायबर-अपराधी अक्सर ऐसी तकनीक का इस्तेमाल करते हैं, जिससे कोई यह विश्वास कर लेगा कि सुरक्षा के साथ समझौता हुआ हैं्र
- लोकप्रिय वेबसाईट्स या कंपनीज को झाँसा
- घोटालों के कलाकार ई-मेल में चित्रों का उपयोग करते हैं, जिससे वे विधिसम्मत वेबसाईट लगें, लेकिन वे आपको वास्तव में किसी आवाज के घोटाले की साईट्स पर या विधिसम्मत दिखनेवाली पॉप-अप विंडोज पर ले जाते हैं्र
- सायबर-अपराधी वेब पतों का भी इस्तेमाल करते हैं, जो प्रसिद्ध कंपनीज के नाम से मेल खाती हैं, लेकिन उनमें थोड़ा-सा बदलाव किया हुआ होता हैं्र
- सायबर-अपराधी आपको फोन कर सकते हैं, जिसमें आपकी कंप्यूटर की किसी समस्या को हल करने में मदद प्रदान करने का प्रस्ताव देते हैं या फिर साफ्टवेयर लायसंस बेचने के लिए कहते हैं्र
- संकेतः यह जान लें कि फिशिंग फोन द्वारा भी की जा सकती हैं्र इसलिए कभी भी व्यक्तिगत जानकारी फोन के द्वारा न दें्र

कभी भी संदेहास्पद ई-मेल को न खोलें/ न जवाब दें/ न फॉरवर्ड करें्र

याद रखने के चरण:

चरण 1: ब्राउसर में यूआरएल का प्रति-परीक्षण करेंऱ

संख्याओं से शुरूहोने वाली वेबसाईट्स पर आपकी जानकारियाँ प्रविष्ट न करेंऱ

चरण 2: गलत वर्तनी वाली यूआरएल की सदैव जाँच करेंऱ

इसलिए स्वयं सदैव यूआरएल में पते के बार में की करें, कभी भी उसे कॉपी- पेस्ट न करेंऱ

चरण 3: सदैव सुरक्षित चैनल पर ऑनलाइन बैंकिंग निष्पादित करें, अर्थात् लॉक करने की जाँच करें और सुरक्षित बैंकिंग के लिए चैनल को सुरक्षित करेंऱ

वश्वसनीय वेबसाईट की सदैव जाँच करें, जिनके एचटीटीपीएस और पैडलाक हैं

चरण 4 : वत्तीय या अन्य व्यक्तिगत जानकारियों के लिए किसी भी ई-मेल अनुरोध को सदैव संदेह के साथ देखें, विशेषकर किसी "तत्काल" अनुरोध कोऱ जब संदेह हो तब वह ई-मेल जो सवालों के घेरे में है, उस पर प्रतिक्रिया न दें या ऐसी सवालिया वेबसाईट्स में कोई जानकारी प्रविष्ट न करेंऱ आपको जो संचार प्राप्त हुआ है, उसकी विधिसम्मतता की पुष्टि के लिए आप आरोपित प्रेषक से भी संपर्क कर सकते हैंऱ

फिशिंग साईट का एक उदाहरण- पंजाब नेशनल बैंक हेतु बाह्य दृष्टि व अनुभूति समान हैऱ

चरण 5 : ऐसे किसी ई-मेल का प्रत्युत्तर न दें, जो आपकी व्यक्तिगत जानकारी जैसे कि केडिट कार्ड/ डेबिट कार्ड/ बैंक की जानकारी के बारे में पूछता होऱ

ये कुछ फिशिंग तकनीक हैं....

- सोशल नेटवर्किंग साईट्स आजकल फिशिंग में प्रमुख लक्ष्य होती हैं, क्योंकि ऐसी साईट्स पर व्यक्तिगत विवरणों का इस्तेमाल चोरी का पता लगाने के लिए किया जा सकता है़
- टेबनेबिंग अद्यतन फिशिंग तकनीक में से एक है़ जो उपयोगकर्त्ता इस्तेमाल करते हैं, उन बहु टेब होने का इसमें फायदा उठाया जाता है और उपयोगकर्त्ता को आहिस्ते प्रभावित साईट की ओर भेजा जाता है़
- फिल्टर बचाव- उद्धरण के स्थान पर फिशर्स बिंबों का उपयोग करते हैं, क्योंकि एंटी-फिशिंग फिल्टर्स के लिए भी यह मुश्किल होता है कि वह फिशिंग के ई-मेल्स में सामान्य रूप से उपयोग में आने वाले उद्धरण की जाँच करें़
- फोन फिशिंगः सभी फिशिंग हमलों के लिए फर्जी वेबसाइट की जरूरत नहीं रहती है़ वे सन्देश जिनके लिए कहा जाता है कि वे बैंक से हैं, वे उपयोगकर्त्ता को कहते हैं कि वे बैंक खाते से संबंधित समस्याओं के बारे में फोन नम्बर पर डायल करें़ एक बार फोन नम्बर (फिशर की मिल्कियत का, जिसे वाईस ओवर आईपी सेवा ने उपलब्ध कराया) जैसे ही डायल किया गया, अनुबोधक उपयोगकर्त्ताओं को कहेगा कि तुरंत खाता नम्बर व पीआईएन प्रविष्ट करें़ विशर कभी जाली कॉलर आईडी का उपयोग करते हैं, जिससे कॉल के लिए बाहर से लगे कि वह एक विश्वसनीय संगठन से है़
- दूसरा हमला जो सफलतापूर्वक किया जाता है, वह है ग्राहक को बैंक की विधिसम्मत वेबसाइट की ओर भेजना और उसके बाद एक पॉपअप विंडो रखना और यह अनुरोध करना कि वे प्रत्यय-पत्र वेबसाइट के शीर्ष पर इस तरह रखें, जिससे ऐसा लगे कि बैंक ही इस नाजुक जानकारी के लिए अनुरोध कर रही है़

Never open/reply/forward suspicious e-mail.

मैं फिशिंग के सन्देश को कैसे पहचान सकता हूँ?

- सामान्यतः फिशिंग की ई-मेल्स में व्याकरण की भूलें प्रदर्शित होती हैं या उद्धरण ढक जाता है़
- वास्तविक जानकारी रखने के पहले परीक्षण में गलत डाटा का उपयोग करते हैं़

मुझे क्या करना चाहिए, यदि मुझे ऐसा लगे कि मैंने किसी फिशिंग घोटाले का प्रत्युत्तर दिया है?

- इन चरणों को उठाएँ, जिससे नुकसान न्यूनतम हो सके, यदि आपको ऐसा लगे कि आपने किसी फिशिंग घोटाले के प्रत्युत्तर में व्यक्तिगत या वित्तीय जानकारी दी है या किसी फर्जी वेबसाइट पर यह जानकारी प्रविष्ट की है़
- आपके उन सभी ऑनलाइन खातों के पासवर्ड्स या पीआईएन-एस को बदल दें, जिनके बारे में आपको लगता है कि उनमें समझौता हुआ होगा़
- आपकी केडिट रिपोर्ट्स पर एक जालसाजी की चेतावनी रख देंं़ यदि आप सुनिश्चित नहीं हैं, कि उसे कैसे करना है, तो आपकी बैंक या वित्तीय सलाहकार से उस बारे में जाँच कर लेंं़
- बैंक या ऑनलाइन मर्चेंट से सीधे ही संपर्क करें़ कपट-युक्त ई-मेल की लिंक का अनुसरण न करें़
- वे प्रभार जो स्पष्ट नहीं किए गए हैं या वे पूछताछ जिनकी शुरुआत आपने नहीं की है, उस सम्बन्ध में आपके बैंक व केडिट कार्ड के विवरणों की समीक्षा नियमित रूप से करते रहें़

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

करें

- कोई भी अटैचमेंट खोलते समय या किसी फाईल को डाउनलोड करते समय सावधानी बरतें, फिर उन्हें भेजनेवाला चाहे कोई भी हो।
- आप जब कोई भी व्यक्तिगत जानकारी प्रविष्ट करें/ दें, उसके पहले भेजने वाले की ई-मेल आईडी पर नजर करें।
- एंटीवायरस, एंटीस्पायवेयर व फायरवाल साफ्टवेयर (उन्हें नियमित रूप से अद्यतन भी करतें रहें) का उपयोग करें।
- आपके वेब ब्राउसर को सदैव अद्यतन रखें और फिशिंग फिल्टर को समर्थ रखें।
- यदि आप कोई भी संदेहास्पद ई-मेल प्राप्त करें, तब कंपनी को फोन कर अवश्य पुष्टि प्राप्त करें कि वह विधिसम्मत है अथवा नहीं है।
- शापिंग ऑनलाइन, व्यक्तिगत आदि के लिए पृथक खोले हुए खातों का उपयोग करें।

न करें

- ऐसे किसी भी ई-मेल या पॉप-अप सन्देश का जवाब न दें, जो व्यक्तिगत या वित्तीय जानकारी की मांग करता हो।
- व्यक्तिगत या वित्तीय जानकारी जैसे कि केडिट कार्ड या अन्य नाजुक जानकारियाँ ई-मेल के माध्यम से न भेजें।
- किसी भी ई-मेल या सोशल मीडिया के सन्देश पर क्लिक न करें, जिसकी आपको प्रत्याशा नहीं है या जरूरत नहीं है।
- आपको जिस पर भी संदेह हो, ऐसे किसी भी ई-मेल को न खोलें, क्योंकि वे शायद विधिसम्मत न हो। यदि वह विधिसम्मत है और उस व्यक्ति को वास्तव में आपसे संपर्क करने की जरूरत है, तब वे अन्य साधनों पर प्रयास करेंगे।
- उन अटैचमेंट को न खोलें, जिनकी आप आशा नहीं कर रहे थे, विशेष रूप से झेडआईपी फाईल्स और कभी भी ईएक्सई फाईल्स न चलाएँ।
- व्यक्तिगत वस्तुओं के लिए आपकी कंपनी के ई-मेल पते का इस्तेमाल न करें।
- किसी भी स्पाम ई-मेल को न खोलें।
- सोशल नेटवर्किंग साईट्स पर संदेहास्पद वीडियोज या बिंबों को न खोलें, क्योंकि फिशिंग में सोशल नेटवर्किंग प्रमुख लक्ष्य होते हैं।
- जिन फोन काल्स में बैंक के विवरण मांगे जाएँ, उनके प्रत्युत्तर न दें। वे विशिंग (आवाज-फिशिंग) हो सकते हैं।
- फिशिंग फोन काल्स के प्रति सावधान रहें।
- यदि आप कोई भी सन्देश (एसएमएस) प्राप्त करें, जिसमें आप से उस खाते की जानकारियों की पुष्टि करने के लिए कहा जाए, जो "चुराया" या "गुम" हो गया है, या जिसमें आपको व्यक्तिगत जानकारी उजागर करने के लिए प्रोत्साहित किया जा रहा हो, यह बताकर कि आपने कोई पुरस्कार जीता है, उस बारे में आप कोई भी प्रत्युत्तर न दें, क्योंकि ऐसे में अधिकतर इसके फिशिंग होने की संभावना रहती है।

वायफाय सुरक्षा

इंटरनेट उपयोगकर्त्ता, इंटरनेट के लिए वाय-फाय साधनों का इस्तेमाल बड़े पैमाने पर कर रहे हैं। हर वर्ष बाजार में कई मिलियन वाय-फाय साधनों की बिक्री हो रही है। इनमें से कई बेतार वाले साधन हैं, जो अपने चूक के कंफिगिरेशन मोड में संवेदनशील हैं। चूँकि अंतिम उपयोगकर्त्ता सेट किए जानेवाले इन साधनों के सुरक्षा स्तर के बारे में जागरूक नहीं होते हैं और इसलिए ये संवेदनशील रह जाते हैं। इन असुरक्षित वाय-फाय साधनों को फायदा उठाकर आतंकवादी व हैकर्स अपनी इच्छाएँ पूरी करते हैं।

वह कोई भी जिसके कंप्यूटर, लेपटाप या मोबाईल में वाय-फाय का संयोजन रहता है, वह असेस के असुरक्षित बिन्दुओं (बेतार राउटर्स) से सम्बद्ध हो सकता है। वह कोई भी जो असेस के बिंदु की श्रेणी में हो, वह असेस के बिंदु से जुड़ सकता है, यदि वह असुरक्षित है। एक बार यह संयोजन स्थापित हो जाए, तब हमलावर मेल्स भेज सकता है, वर्गीकृत/ गोपनीय सामग्री को डाउनलोड कर सकता है, नेटवर्क के अन्य कंप्यूटर्स पर हमले की पहल कर सकता है, दूसरों को दुर्भावनापूर्ण कोड भेज सकता है, पीड़ित के कंप्यूटर पर ट्रोजन या बोटनेट संस्थापित कर सकता है, जिससे इसके द्वारा इंटरनेट आदि पर दीर्घावधि का नियंत्रण प्राप्त हो जाता है।

ये सभी आपराधिक गतिविधियाँ स्वभाविक रूप से असेस के बिन्दु (बेतार राउटर) के कानूनी उपयोगकर्त्ता से सम्बद्ध रहेगी। अब यह असेस के बिन्दु के कानूनी उपयोगकर्त्ता पर निर्भर रहेगा कि वह यह सिद्ध करने के लिए कि वह इन गतिविधियों में शामिल नहीं है, वह स्वयं का बचाव करे। अब यह उपयोगकर्त्ता की जिम्मेवारी है कि वह अपने असेस के बिन्दु को सुरक्षित करे।

चलिए हाल ही के वर्षों में घटित कुछ वास्तविक घटनाओं का जायजा लें।

- आतंकवादी व हैकर्स ने इंटरनेट पर गैर-कानूनी गरिविधियों को निष्पादित करने के लिए असेस के असुरक्षित बिन्दुओं का इस्तेमाल किया।
- न्यूयार्क, लॉसएंजिल्स व वाशिंगटन डीसी स्थित थाम्पसन समूह की लक्जरी होटल्स के वाय-फाय नेटवर्क में हैकर्स ने प्रविष्टि ली और मेहमानों द्वारा भेजे उनके निजी ई-मेल्स की चोरी की। इसके बाद हैकर्स ने ई-मेल्स को प्रकाशित करने की धमकी देकर हॉटल चेन से बड़ी रकम हड़पने का प्रयास किया। (www.crpcc.in)

> *सार्वजनिक स्थलों पर कभी भी खुले वाय-फाय नेटवर्क से स्वतः कनेक्ट न होंय्*

- सितम्बर 2008 में दिल्ली में जो बम विस्फोट हुए, उसके मात्र ५ मिनट पहले आतंकवादियों ने अधिकारियों व न्यूज चैनल्स को आतंक के ई-मेल्स भेजने के लिए चेम्बूर मुंबई स्थित एक कंपनी के असुरक्षित वाय-फाय कनेक्शन का इस्तेमाल किया थाय्र किसी तर्कयुक्त निष्कर्ष पर पहुंच सकें, इसलिए ये हैकर्स जाँचकर्त्ताओं के लिए कुछ भी निशान शेष नहीं छोड़ते हैंय्र ऑडिट जाँच कानूनी उपयोगकर्त्ता के वाय-फाय असेस बिंदु पर समाप्त हो जाती हैय्र उपयोगकर्त्ताओं के लिए यह आवश्यक हो गया है कि वे अपने असेस- बिन्दु (बेतार राउटर) को सुरक्षित करेंय्र असेस के बिन्दु को सुरक्षित करने के लिए उठाए जाने हेतु निम्न कदम हैंय्र

बेतार के वातावरण पर हमलों के प्रकार

- **हमला सेवा का त्याग**

  हमला सेवा के त्याग का लक्ष्य होता है कि उपयोगकर्त्ताओं को नेटवर्क स्त्रोतों की पहुँच से रोका जाएय्र बेतार के नेटवर्क में हमला सेवा का त्याग विभिन्न तरीकों से किया जा सकता हैय्र

- **वाय-फाय साधनों में बीच-हमले में आदमी**

  यदि वायर्ड नेटवर्क से तुलना की जाए तो वायरलेस नेटवर्क पर वाय-फाय साधनों के बीच-हमले में आदमी का निष्पादन बहुत आसान हैय्र जैसा कि असेस के बिंदु से संचारण का प्रसारण होता है, इसलिए अप्राधिकृत उपयोगकर्त्ता के लिए बहुत आसान होता है कि वह अन्य बेतार- ग्राहकों द्वारा भेजी गई सामग्री को एकत्रित करेंय्र और इस प्रकार एकत्रित किए गए पैकेट्स को इवसड्रोपिंग कहते हैंय्र साथ ही तीसरे पक्ष के उपयोगकर्त्ता इन विधि-सम्मत उपयोगकर्त्ता को भेजे गए पैकेट्स में जोड़-तोड़ कर सकते हैं और उस वजह से उपयोगकर्त्ता की गोपनीयता समाप्त हो जाती हैय्र

  इसलिए इस प्रकार के हमलों को टालने हेतु बेतार ग्राहक व असेस बिंदु के बीच डाटा संचरण के लिए सशक्त एनक्रिप्शन का इस्तेमाल किया जाएय्र

- **वार-ड्रायविंग**

  यह किसी निश्चित स्थल पर वाय-फाय हॉटस्पॉट्स की ट्रैकिंग की वह प्रक्रिया है, जिसमें गतिशील स्थिति में किसी वाहन पर हाथ में कोई साधन या कोई लेपटाप होता हैय्र इससे उपयोगकर्त्ता को उन असेस बिन्दुओं का पता लगाने में मदद मिलती है, जो एनक्रिप्शन का इस्तेमाल नहीं करते हैं और नेटवर्क पर हमले के निष्पादन के लिए उस पर नियंत्रण ले लेते हैंय्र

वाय-फाय वातावरण में हमला कैसे होता है?

- टीसीपी/ आईपी मॉडेल की भौतिक पर्त पर हमला सेवा के त्याग का कार्यान्वयन उस साधन के प्रवेश द्वारा किया जा सकता है, जो उसी आवृत्ति के बैंड पर शोर उत्पन्न करेगा, जिस पर बेतार पहुँच बिंदु संचालित हो रहा होय्र उस वजह से वे उपयोगकर्त्ता जो पहुँच बिंदु से संबद्ध होने की कोशिश कर रहे हों, वे उससे शायद संबद्ध न हो पा रहे होंय्र
- साथ ही हमला सेवा के त्याग की अन्य संभावना होती है असेस बिंदु के झांसे कीय्र सामान्यतः बेतार- ग्राहक असेस बिंदु की मदद से वायर्ड नेटवर्क से जुड़ते हैंय्र असेस बिंदु से जुड़ने के लिए उन्हें इसके एसएसआईडी की जरूरत पड़ती

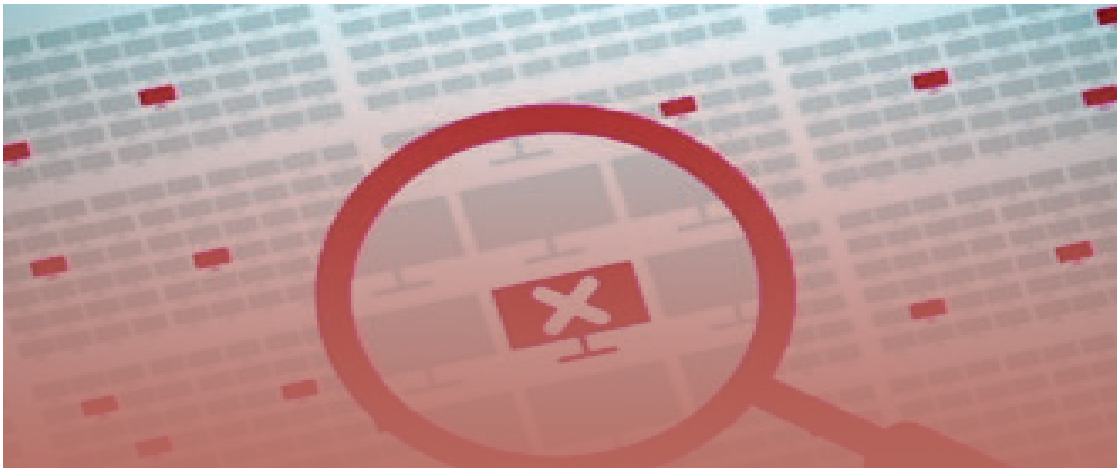
है। जब कोई अनाधिकृत उपयोगकर्त्ता उसी एसएसआईडी पर असेस बिंदु रखता है, तब यह एक मौका रहता है कि अधिकृत उपयोगकर्त्ता हमलावर के असेस बिंदु से संबद्ध हो जाए। यदि ऐसा होता है, तब हमलावर कोशिश करेगा कि वह बेतार- ग्राहक से पर्याप्त संख्या में पैकेट्स प्राप्त कर ले और विधिसम्मत असेस बिंदु के द्वारा इस्तेमाल की गई डब्ल्यूईपी की की को समाप्त कर दे। फिर हमलावर विधिसम्मत असेस बिंदु से संबद्ध हो जाता है जिससे नेटवर्क पर बड़े पटाखे के अनुरोध का उद्भव होता है या वह असामान्य सामग्री को उत्पन्न करता है और उसके फलस्वरूप अंत में हमला सेवा का त्याग हो सकता है।

- एनक्रिप्शन के कुछ रूप को सभी वाय-फाय उपकरण सहयोग करते हैं। अतः उन्हें समर्थ बनाएँ
- वाय-फाय साधनों पर एमएसी एड्रेस फिल्टरिंग को समर्थ बनाएँ
- घर के हाय-फाय के लिए गतिशील आईपी पतों को टालें, इसके बनिस्बत स्थिर आईपी पतों का इस्तेमाल करें
- बेतार नेटवर्क पर संवेदनशील डाटा के लिए एनक्रिप्शन तकनीक का उपयोग करें

बेतार संचार सुरक्षित करने के लिए युक्तियाँ

- **एनक्रिप्शन के लिए सदैव सशक्त पासवर्ड का इस्तेमाल करें**
  एक सशक्त पासवर्ड में न्यूनतम १५ लिपिचिन्ह होने चाहिए, जिनमें बड़े अक्षर, छोटे अक्षर, संख्याएँ व निशान हों। साथ ही यह भी अनुशंसा की जाती है कि एनक्रिप्शन की को बारंबार बदलते रहें, जिससे नष्ट करने वाले के लिए एनक्रिप्शन की को तोड़ना कठिन हो जाए। एनक्रिप्शन के लिए डब्ल्यूईपी का उपयोग न करें, इसके स्थान पर डब्ल्यूपीए/ डब्ल्यूपीए २ का इस्तेमाल करें।
- **एनक्रिप्शन के लिए सदैव अधिकतम आकार की का उपयोग करें, जिसमें असेस बिंदु से भी मदद हो**
  यदि की का आकार पर्याप्त रूप से बड़ा होगा, तब हैकर को की को तोड़ने के लिए अधिक वक्त की जरूरत रहेगी। इसलिए यह भी अनुशंसा की जाती है कि एनक्रिप्शन की को बारंबार बदलते रहें, जिससे नष्ट करने वाले के लिए एनक्रिप्शन की को तोड़ना कठिन हो जाए।
- **वायर्ड नेटवर्क से बेतार के नेटवर्क को फायरवाल व एंटीवायरस गेटवे के द्वारा पृथक कर दें।**
  वायर्ड नेटवर्क से असेस बिंदु को सीधे नहीं जोड़ें। चूँकि बेतार के ग्राहक के साथ समझौते के मौके हैं, जिसके फलस्वरूप वायर्ड नेटवर्क के सिस्टम्स पर प्रभाव रहेगा एवं एक फायरवाल व एक एंटीवायरस गेटवे को असेस बिंदु व वायर्ड नेटवर्क के बीच रख दिया जाए।
- **एमएसी पते पर असेस बिंदु आधारित असेस को प्रतिबंधित करें।**
  असेस बिंदु से अधिकृत उपयोगकर्त्ता से जुड़ सकें, इसलिए बेतार- ग्राहकों को असेस बिंदु आधारित असेस उपलब्ध कराया जाए।

- **चूक के उपयोगकर्त्ता के नाम व असेस बिंदु के पासवर्ड को बदल दें**
  असेस बिंदु के कंफिगुरेशन के वक्त अधिकांश उपयोगकर्त्ता चूक के पासवार्ड को नहीं बदलते हैंप्र लेकिन यह अनुशंसा की जाती है कि कोई सशक्त पासवर्ड रखें, क्योंकि इस चूक के पासवर्ड की जानकारी उत्पाद के उत्पादकों से प्राप्त की जा सकती हैप्र
- जब असेस बिंदु उपयोग में नहीं हो, तब उसे बंद कर दें
  हैकर्स कोशिश करते हैं कि की को तोड़ने के लिए वे कठोर दबाव बनाएँ, इसलिए यह अच्छा रहता है कि गैर-उपयोगिता की बढ़ी हुई अवधि में असेस बिन्दुओं को बंद कर देंप्र
- **आपके नेटवर्क के नाम को प्रसारित नहीं करें**
  नेटवर्क पर असेस बिंदु की पहचान के लिए तथा एसएसआईडी की सूचनाओं का उपयोग किया जाता है तथा नेटवर्क से बेतार- ग्राहकों को जोड़ने के लिए भी इन सूचनाओं का उपयोग किया जाता हैप्र अधिकृत उपयोगकर्त्ता नेटवर्क से जुड़ सकें, इसलिए ये सूचनाएँ सार्वजानिक रूप से उपलब्ध न कराई जाएँप्र
- **सदैव अद्यतन फर्मवेयर बनाए रखें**
  असेस बिंदु के फर्मवेयर को अद्यतन रखने की अनुशंसा की जाती है, क्योंकि यह असेस बिंदु की सुरक्षा की खामियों की संख्या को कम कर देगीप्र
- **संचारण को संरक्षित करने के लिए वीपीएन या आईपीएसईसी का उपयोग करेंप्र**
  जब बेतार-ग्राहक से सूचनाएँ वायर्ड नेटवर्क में बहती हैं और रिसीवर नाजुक होता है, तब यह अनुशंसा की जाती है कि वीपीएन या आईपीएसईसी पर आधारित संचार का उपयोग करें, जिससे नेटवर्क में सूचनाएँ भाँपने वालों से सुरक्षित रहेंप्र
- **एसएसआईडी की सूचनाओं को सार्वजनिक न करें**
  नेटवर्क पर असेस बिंदु की पहचान के लिए तथा एसएसआईडी की सूचनाओं का उपयोग किया जाता है तथा नेटवर्क से बेतार के ग्राहकों को जोड़ने के लिए भी इन सूचनाओं का उपयोग किया जाता हैप्र अधिकृत उपयोगकर्त्ता नेटवर्क से जुड़ सकें, इसलिए ये सूचनाएँ सार्वजानिक रूप से उपलब्ध न कराई जाएँप्र
- **डीएचसीपी सेवा को असमर्थ कर दें**
  जब असेस बिंदु पर पहुँचने वाले उपयोगकर्त्ताओं की संख्या कम हो, तब यह अनुशंसा की जाती है कि डीएचसीपी सेवा को असमर्थ कर देंप्र अन्यथा इसके कारण हमलावरों के लिए आसान हो जाता है कि वे जैसे ही असेस बिंदु से संबद्ध होते हैं, वे नेटवर्क से जुड़ जाएँप्र



विंडोज की संचालन प्रणाली हेतु सुरक्षा साधन

दुर्भावनायुक्त साफ्टवेयर को हटाने हेतु साधन

दुर्भावनायुक्त साफ्टवेयर को हटाने हेतु माइक्रोसॉफ्ट विंडोज साधन, उन कंप्यूटर्स से विशिष्ट व प्रचलित दुर्भावनायुक्त साफ्टवेयर को हटाने में मदद करता है, जिस पर विंडोज ७, विंडोज विस्ट ा, विंडोज सर्वर २००३, विंडोज सर्वर २००८ या विंडोज एक्सपी चलते हैं जब पता लगाने व हटाने की प्रक्रिया पूरी हो जाती है, तब साधन एक रिपोर्ट प्रदर्शित करता है, जिसमें परिणाम का वर्णन रहता है और उसमें यदि कोई दुर्भावनायुक्त साफ्टवेयर को पता लगा कर यदि हटाया गया हो, तो वह भी उसमें शामिल रहता है

ऋण्ड्ड ड्डक्नुद्यात्ड्डद्यद्य ध्क्ष्ठ द्यदृ ड्डदृध्दथदृठ्ठड्ड ठ्ठदड्ड द्धद्मद द्यण्ड्ड द्यदृदृथ् त्द्य द्यदृ द्यद्मद्धद दृद ऋ्क्षद्यदृध्ठ्ठद्यात्ड् छद्मड्डठ्ठद्यड्डद्ध; द्यण्त्द्य ढ़द्मठ्ठ्ड्डद्मदद्यड्डड्डद्ध द्यण्ठ्ठद्य ऋद्मद्र द्धड्ढड्डड्डत्ड्ड द्यण्ड्ड द्यदृदृथ् ठ्ठद्मद्यदृध्ठ्ठद्यात्ड्ड्ठथ्ठ्र ड्डध्ड्डद्धद्र थ्दृदद्यण. क्ष्ठ ऋद्मद्र ण्ठ्ठध्ड्ड ऋ्क्षद्यदृध्ठ्ठद्यात्ड् छद्मड्डठ्ठद्यड्डद्ध द्यद्मद्धदड्डड्ड दृद, ऋद्मद्र ण्ठ्ठध्ड्ड ठ्ठथ्द्धड्डठ्ठड्डद्र डड्डड्डद द्धड्ढड्डठ्ठड्डत्ध्त्दढ़ दड्ड्ध ध्ड्डद्धद्मात्दृदद्ध दृढ द्यण्त्द्य द्यदृदृथ् थ्दृदद्यण्ठ्र. ऋण्ड्ड द्यदृदृथ् द्धद्मदद्ध त्द द्यद्मत्ड्डद्य थ्दृड्डड्ड द्मदथ्ड्डद्धद्य त्द्य ढत्दड्डद्ध ठ्ठद त्दढड्ढड़द्यात्दृद. क्ष्ठ ऋद्मद्र ण्ठ्ठध्ड्ड ददृद्य डड्डड्डद ददृद्यात्ढड्डड्ड दृढ ठ्ठद त्दढड्ढड़द्यात्दृद, ददृ थ्ठ्ठथ्ड़त्दृद्मद्ध द्यादृढद्यध्ड्ठद्धड्ड ण्ठ्ठद्ध डड्डड्डद ढदृद्मद्मड्ड द्यण्ठ्ठद्य दड्डड्डड्डद्ध ऋद्मद्रद्ध ठ्ठद्यद्यड्डदद्यात्दृद.

नोट यदि आपके कंप्यूटर पर विंडोज एक्सपी सर्विस पैक २ (एसपी २) चल रहा है तो चूक से स्वचालित अपडेट्स चालू हो गया है

दुर्भावनायुक्त साफ्टवेयर को हटाने हेतु माइक्रोसॉफ्ट साधन, किसी एंटीवायरस उत्पाद को प्रस्थापित नहीं करता है यह साधन तीन मुख्य तरीके से एंटीवायरस उत्पाद से भिन्न है

- पहले से ही संक्रमित कंप्यूटर में से यह दुर्भावनायुक्त साफ्टवेयर को हटाता है एंटीवायरस उत्पाद दुर्भावनायुक्त साफ्टवेयर को कंप्यूटर पर चलने से अवरूद्ध कर देते हैं संक्रमण के बाद हटाने की अपेक्षा यह उल्लेखनीय रूप से बेहतर है कि दुर्भावनायुक्त साफ्टवेयर को कंप्यूटर पर चलने से अवरूद्ध किया जाए
- यह केवल विशिष्ट प्रचलनवाले दुर्भावनायुक्त साफ्टवेयर को हटाता है विशिष्ट प्रचलनवाले दुर्भावनायुक्त साफ्टवेयर जो आज मौजूद हैं, उन सभी दुर्भावनायुक्त साफ्टवेयर के छोटे सबसेट हैं
- यह सक्रिय दुर्भावनायुक्त साफ्टवेयर की जाँच व उनके हटाने पर केन्द्रित रहता है सक्रिय दुर्भावनायुक्त साफ्टवेयर वह दुर्भावनायुक्त साफ्टवेयर है, जो इस समय कंप्यूटर पर चल रहा है जो नहीं चल रहा है, उस दुर्भावनायुक्त साफ्टवेयर को यह साधन नहीं हट ा सकता है फिर भी एंटीवायरस उत्पाद इस काम को कर सकता है

नोट अधिक जानकारी के लिए देख http://www.microsoft.com/security/default.aspx

माइक्रोसॉफ्ट बेसलाईन सुरक्षा विश्लेषक

माइक्रोसॉफ्ट बेसलाईन सुरक्षा विश्लेषक एमबीएसए, उपयोगकर्त्ताओं, प्रशासकों को स्थानीय व दूरस्थ जाँच प्रणाली को करने देता है, जो लुप्त सुरक्षा अपडेट व साथ ही सामान्य सुरक्षा मिसकंफ्यूगिरेशन के लिए है

https://www.microsoft.com/en-us/download/details.aspx?id=7558 से डाऊनलोड करें

माइक्रोसॉफ्ट सुरक्षा अनुपालन प्रबंधन साधन एससीएम्

सिरे से सिरे तक का समाधान एक्सीलेटर, जो विंडोज के ग्राहकों हेतु एवं सर्वर संचालन सिस्टम व माइक्रोसॉफ्ट अनुप्रयोग हेतु आपको आयोजना, विस्तार, संचालन व सुरक्षा बेसलाईन में मदद पहुँचायगा केन्द्रीकृत सुरक्षा बेसलाईन प्रबंधन में विशिष्टताएँ, बेसलाईन पोर्टफोलिओ व ग्राहकीकृत दक्षताएँ हैं व यह सुरक्षा बेसलाईन निर्यात लचीलेपन समाधान एक्सीलेटर उपलब्ध कराता है, जिससे आपके संगठन की दक्षता में वृद्धि हो और जिससे सर्वाधिक विस्तृत रूप से उपयोग में आनेवाली माइक्रोसॉफ्ट तकनीक की अनुपालन प्रक्रिया व सुरक्षा का प्रबंधन उत्कृष्टतापूर्वक किया जा सके

https://www.microsoft.com/en-us/download/details.aspx?id=16776 से डाऊनलोड करें

यूआरएलस्कान सुरक्षा साधन

सर्वर को मिलनेवाले सभी अनुरोधों को यूआरएलस्कान उन्हीं नियमों के आधार पर छाँटता है, जो प्रशासक ने स्थापित किए हैं अनुरोधों की छंटनी से सर्वर सुरक्षित होता है, जिससे यह सुनिश्चित करने में मदद मिलती है कि केवल वैध अनुरोध ही संसाधित किए जा रहे हैं यूआरएलस्कान सुरक्षा साधन में दो फाईल्स हैं? निझबचह.गनन एवं निझबचह.है ?, जिन्हें एक साथ निझबचह.टी में पॅकेज किया गया है यूआरएलस्कान २.५ के नवीनतम अपडेट के कारण प्रशासक यूआरएलस्कान कन्फ्यूगिरेशन पर अधिक नियंत्रण रख सकते हैं और वे कार्य उपलब्ध करा सकते हैं, जिससे प्रशासकों को मदद मिलती है और वे सर्वर को और अधिक सुरक्षा मुहैया करा सकें और सर्वर को लॉकडाउन कर सकें

http://www.iis.net/learn/extensions/working-with-urlscan/urlscan-3-reference से डाऊनलोड करें

माइक्रोसॉफ्ट सिक्यूरिटी एशेंशियल्स

माइक्रोसॉफ्ट से मुफ्त डाउनलोड किया जानेवाला माइक्रोसॉफ्ट सिक्यूरिटी एशेंशियल्स है, जो संस्थापित करने में, इस्तेमाल करने में आसान है और उसे सदैव अद्यतन रखते हैं, जिससे आप सुनिश्चित हो सकें कि आपका पीसी नवीनतम तकनीक के साथ सुरक्षित है

माइक्रोसॉफ्ट सिक्यूरिटी एशेंशियल्स शांति से व उत्कृष्टता के साथ पृष्ठभूमि में काम करता है, जिससे आप आपके विंडो आधारित पीसी का जिस प्रकार चाहें, बिना किसी रुकावट के या कंप्यूटर पर लंबी प्रतीक्षाअवधि में उपयोग कर सकें

हम अनुशंसा करते हैं कि माइक्रोसॉफ्ट सिक्यूरिटी एशेंशियल्स को संस्थापित करने से पूर्व आपके पीसी पर पहले से ही चल रहे एंट ीवायरस साफ्टवेयर को हटा दें एक से अधिक एंटीवायरस प्रोग्राम के चलने से कभी संघर्ष की संभावना हो सकती है और उससे पीसी के निष्पादन पर फर्क पड़ सकता है

https://www.microsoft.com/en-us/download/details.aspx?id=5201 से डाऊनलोड करें

नोट माइक्रोसॉफ्ट का दुर्भावनायुक्त साफ्टवेयर को हटाने का साधन, स्पायवेयर को नहीं हटाता है स्पायवेयर का पता लगा कर उसके हटाने में मदद के लिए आप षैबर्जिक्ष झीर्बोंअ डजजीहौचनज. को डाऊनलोड कर सकते हैं

सिक्योर इट प्रो 4.70.0117

आपके कंप्यूटर को तब लॉक करने के लिए, जब आप वहाँ नहीं हों, सिक्योर इट प्रो का उपयोग करें इस प्रोग्राम में कई विशेषताएँ हैं भानिछनाधीन, छनाचम, विंडोज की की, तथा भानिडजब मुख्य संयोजन जैसे मुख्य विंडोज कार्यों को असमर्थ बना देती है सिक्योर इट प्रो, विंडोज की बूट की को असमर्थ कर सकता है, कोल्ड बूट्स का पता लगा सकता है व अन्य लोगों को सन्देश छोड़ने के लिए समर्थ कर सकता है, गलत पासवर्ड के प्रयासों को लॉग कर सकता है या प्रत्येक कुछ सेकंड्स पर स्वयं को छिपा सकता है इस प्रोग्राम में पासवर्ड याद दिलाने के विकल्प भी सम्मिलित हैं, जो आपको तब सहायता पहुँचा सकते हैं, जब आप पासवर्ड तथा कई उन्नत कंफिगिरेशन के विकल्पों तथा स्क्रीन सेवर को लॉक करना पूरी तरह भूल जाएँ

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

पीसी लॉकर प्रो

पीसी लॉकर प्रो एक फ्रीवेयर है, जो आपके बाहर जाने पर आपके कंप्यूटर को लॉक करता है व संरक्षित करता है

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

स्थिर स्थिति

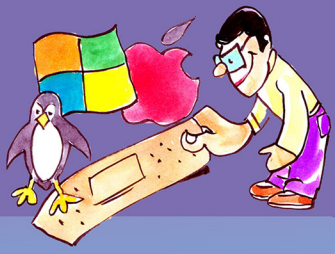
विंडोज की स्थिर स्थिति में उपयोगकर्त्ता की प्रोफाईल्स को तैयार करना, उसे संशोधित करना व उसे हटाना सरल है उपयोगकर्त्ता के खाते को लॉग करने की, रजिस्ट्री को सम्पादित करने की या हार्ड ड्राइव पर फाईल्स या फोल्डर्स में जोड़तोड़ करने की कोई जरूरत नहीं है मुख्य कंसोल से आप सीधे ही उपयोगकर्त्ता के सभी प्रतिबंधों को नियंत्रित करते हैं प्रोफाईल को प्रत्येक उपयोगकर्त्ता शीघ्रता से उच्च, मध्यम या निम्न सुरक्षा चूक प्रदान करें इसके बाद विंडोज की स्थिर स्थिति में उपलब्ध कई विकल्पों का उपयोग कर प्रोफाईल्स को पूर्णता से ठीक करें

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

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

Secure your Desktop

By using latest Antivirus with automated scanning



Always update Operating System with latest patches before using them

Filter communication with Desktop Firewall

वायरस से संरक्षण व स्वच्छता के साधन

विंडोज आधारित साधन

- गृह संस्करण की रोक
  - मानक शील्ड वास्तविक समय संरक्षण
  - आईएम शील्ड तत्काल सन्देशवाहक संरक्षण
  - पीरपी शील्ड पीरपी संरक्षण
  - इंटरनेट मेल ईमेल संरक्षण
  - दृष्टिकोण/ विनिमय माइक्रोसॉफ्ट दृष्टिकोण/ विनिमय संरक्षण
  - वेब शील्ड एचटीटीपी संरक्षण (स्थानीय पारदर्शी (स्थानीय पारदर्शी अधिकृतप्रतिनिधि)
  - स्क्रिप्ट ब्लाकर स्क्रिप्ट जाँचकर्त्ता (केवल संस्करण उन्मुख)
  - नेटवर्क शील्ड प्रसिद्ध नेटवर्क कीटाणुओं के समक्ष बुनियादी संरक्षण
  - कमवजन के अंतर्वेधन जाँच प्रणाली के रूप में काम करता है
  - श्रव्य अलार्म मौखिक चेतावनी जैसा कि, सावधान, एक वायरस का पता लगा है!
  - बूटसमय स्कान प्रोग्राम अंतरफलक के माध्यम से विंडोज स्टार्टअप के दौरान वायरसों को दूर करने के लिए, उपयोगकर्त्ता बूटसमय स्कान की सूची तैयार कर सकता है और इसलिए हटाना कठिन रहता है

रोको! एंटीवायरस सामान्यतः इस्तेमाल के पहले के १४ महीने स्वयं ही मुफ्त रूप से स्वयं को तब तक अद्यतन कर लेता है, जब तक कि इस्तेमाल में जो कंप्यूटर है, उसे इंटरनेट से जोड़ा हुआ है प्रत्येक १४ माह की अवधि के बाद, साफ्टवेयर के उपयोगकर्ता को नए लायसेंस की प्राप्ति के लिए पुनःपंजीकृत करवाना चाहिए जब तक कि भुगतान संस्करण उन्नत नहीं हो जाता है, पंजीकरण वर्तमान में मुफ्त रहता है
http://www.avast.com/eng/download-avast-home.html

एवीजी मुफ्त संस्करण

ग्रीसॉफ्ट के अनुसार ६० मिलियन उपयोगकर्ताओं के पास एवीजी एंटीवायरस संरक्षण है, इनमें मुफ्त संरक्षण के उपयोगकर्ता भी शामिल हैं एवीजी एंटीवायरस मुफ्त संरक्षण, एवीजी एंटीवायरस व्यवसायिक संस्करण उत्पाद के समान ही है, लेकिन उसमें सभी विशिष्टताएँ नहीं हैं इसमें कमी है उस सूक्ष्म नियंत्रण की, कि स्केन्स का संचालन किस प्रकार होता है इसके अतिरिक्त मुफ्त रूपों को ग्रीसॉफ्ट का तकनीकी सहयोग नहीं मिलता है तथा अंग्रेजी ही उपलब्ध भाषा है ग्रीसॉफ्ट ने घोषणा की है कि एवीजी एंटीवायरस मुफ्त संस्करण रूप ७.१, १८ फरवरी, २००७ को समाप्त हो चुका है उपयोगकर्त्ताओं को चाहिए कि वे एवीजी एंटीवायरस मुफ्त संस्करण रूप ७.५ को अपग्रेड करा लें
http://free.grisoft.com/doc/5390/us/frt/0

अवीरा एंटीवायरस पर्सनल एडिशन पारंपरिक

एंटीवीर व्यक्तिगत संस्करण पारंपरिक (विंडोज, लायनक्स) फ्रीवेयर है इसका प्रयोग केवल व्यक्तिगत उपयोग के लिए है अधिकांश एंटीवायरस साफ्टवेयर की तरह, यह वायरसों के लिए डिस्क स्केन करता है व साथ ही पृष्ठभूमि की प्रक्रिया के बतौर चलता भी है और प्रत्येक खुली हुई व बंद फाईल की जाँच करता है यह रूट किट्स की जाँच कर सकता है और संभवतः उन्हें दूर कर देता है यह इंटरनेट अपडेट्स (प्रतिदिन चूक से) का निष्पादन भी करता है, जिसमें यह एक विज्ञापन के साथ विंडो खोलता है और उपयोगकर्त्ता

को सलाह देता है कि वह एंटीवायरस व्यक्तिगत संस्करण प्रीमियम खरीदे
एंटीवायरस पर्सनल एडिशन प्रीमियम की कीमत वार्षिक च२० है मुफ्त संस्करण की तुलना में, इसमें कई सुधार हैं, जो उल्लेखनीय हैं

- एडवेयर व स्पायवेयर की जाँच
- विशिष्ट डाऊनलोड सर्वर
- ईमेल स्केनिंग

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

बिट डिफेंडर १० मुफ्त संस्करण

बिट डिफेंडर एक एंटीवायरस साफ्टवेयर सूट है, जिसे बुखारेस्ट की एक साफ्टवेयर कंपनी ने तैयार किया है इसे नवंबर २००१ में शुरु किया गया और वर्तमान में इसका दसवाँ संस्करण उपलब्ध है बिट डिफेंडर को साफ्ट विन के पहले के एवीएक्स (एंटीवायरस एक्सप्रेस) उत्पाद की श्रेणी में रखा गया है बिट डिफेंडर की श्रेणी में शामिल हैं, वे एंटीवायरस उत्पाद जो घर में उपयोग करने वाले, व्यावसायिक, उद्यम के उपयोगकर्त्ता तथा इंटनेट सेवा प्रदातागण के लिए है
http://www.bitdefender.com/PRODUCT-14-en--BitDefender-Free-Edition.html

मेक्फी वायरस स्केन प्लस

- वायरस संरक्षण आपके संपूर्ण पीसी की चौकसी करता है
- स्पायवेयर संरक्षण संभवित अवांछित प्रोग्राम्स को अवरूद्ध कर देता है
- हैकर्स को बाहर रखने में फायरवाल मददगार रहती है

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

कोमोडो एंटीवायरस

कोमोडो एंटीवायरस २.० बीटा विशिष्ट रूप से तैयार किया गया है, जिससे सभी ज्ञात वायरस ट्रोजन्स व वार्म्स के समक्ष संरक्षण दिया जा सके इसका संस्थापन, कंफिग्यूरेशन व इस्तेमाल आसान है उद्योग के प्रमुख कार्यों की सूची, जिसमें अद्यतन व अत्यंत परिष्कृत तकनीक समाहित हैं, उनके लिए कोमोडो एंटीवायरस की तारीफ है
http://antivirus.comodo.com/download.html

क्लामएवी (खुला स्त्रोत)

क्लाम एंटीवायरस (क्लाम एवी) मुफ्त खुले स्त्रोत का विंडोज व यूनिक्स जैसी संचालन प्रणालियों के लिए एक एंटीवायरस साफ्टवेयर टूलकिट है इसके मुख्य उपयोग में से एक मेल विनिमय सर्वर्स के साथ सर्वर साईड ईमेल वायरस स्केनर के रूप में है क्लाम एवी का वितरण जीएनयू, सामान्य लोक लायसेंस (जीपीएल) के नियमों के अधीन है क्लाम एवी व उसके अपडेट्स दोनों बिना किसी शुल्क के उपलब्ध हैं
http://www.clamwin.com/content/view/18/46/

विन पूछ (खुला स्त्रोत)

विन पूछ एक मुफ्त व खुले स्त्रोत का प्रोग्राम है, जो उन कंप्यूटर्स को जिन पर माइक्रोसॉफ्ट विंडोज चलते हैं, उनके स्पायवेयर की जाँच कर उन्हें अवरूद्ध कर देता है यह ट्रोजन्स की भी जाँच करता है और यह क्लाम विन व बिट डिफेंडर एंटीवायरस साफ्टवेयर से संबद्ध हो सकता है, जिससे वास्तविक समय संरक्षण उपलब्ध कराया जा सके कर्नेल मोड ड्रायवर की मदद से संस्करण ०.६.० कर्नेल मोड हुकिंग का अमलीकरण हुआ है, जिससे विन पूछ विंडोज कर्नेल व सिस्टम सेवाओं को नियंत्रित कर सकता है यद्यपि ब्ल्यू स्क्रीन्स की समाप्ति के लिए यह कुख्यात था
http://www.clamwin.com/content/view/18/46/

दुर्भावनायुक्त साफ्टवेयर को हटाने हेतु साधन

दुर्भावनायुक्त साफ्टवेयर को हटाने हेतु माइक्रोसॉफ्ट साधन, एक गैरमालवेयर उपयोग के लिए है, जो विशिष्ट मौजूद दुर्भावनायुक्त साफ्टवेयर, जिनमें ब्लास्टर, सासेर व मायडूम शामिल हैं, के द्वारा उन कंप्यूटर्स की जाँच संक्रमण के लिए करता है, जो विंडोज ८, विंडोज ७, विंडोज विस्टा, विंडोज एक्सपी, विंडोज सर्वर २०१२, विंडोज सर्वर २००८ और विंडोज सर्वर २००३ पर चलते हैं और यह मालवेयर व अन्य पाए जानेवाले संक्रमणों को हटाता जब है मालवेयर का पता लगाने व हटाने की प्रक्रिया पूरी हो जाती है, तब साधन एक रिपोर्ट प्रदर्शित करता है, जिसमें परिणाम का वर्णन रहता है और उसमें यदि कोई मालवेयर का पता लगा कर यदि हट ाया गया हो, तो वह भी उसमें शामिल रहता है

http://www.microsoft.com/security/pc-security/malware-removal.aspx

माइक्रोसॉफ्ट सिक्यूरिटी एशेंशियल्स

माइक्रोसॉफ्ट सिक्यूरिटी एशेंशियल्स (एमएसई), एक एंटीवायरस (एवी) उत्पाद है, जो विभिन्न प्रकारों के मालवेयर जैसे कि कंप्यूटर वायरस, स्पायवेयर, रूटकिट्स व ट्रोजन हार्सेस के समक्ष संरक्षण उपलब्ध कराता है यह विंडोज एक्सपी, विंडोज विस्टा व विंडोज ७ पर चलता है, लेकिन विंडोज ८ पर नहीं चलता है, जिसमें एवी घटक का भाग बना हुआ रहता है घर पर उपयोग करनेवालों व छोटे व्यवसायियों को लायसंसकरार उसे संस्थापित करने व उस उत्पाद को निशुल्क उपयोग की अनुमति देता है

http://windows.microsoft.com/en-us/windows/security-essentials-download

विंडोज डिफेंडर

विंडोज डिफेंडर को पहले माइक्रोसॉफ्ट एंटीस्पायवेयर के रूप में जानते थे, यह वह साफ्टवेयर है जो मालवेयर के साथ संघर्ष करने में मदद करता है आरम्भ में विंडोज डिफेंडर एक एंटीस्पायवेयर प्रोग्राम था और यह विंडोज विस्टा व विंडोज ७ में शामिल है तथा विंडोज एक्सपी एवं विंडोज सर्वर २००३ के लिए मुफ्त डाऊनलोड करने हेतु उपलब्ध है विंडोज ८ में यद्यपि यह एक एंटीवायरस प्रोग्राम के रूप में उन्नत किया गया है इसमें कई वास्तविक समय के सुरक्षा एजेंट्स शामिल किए गए हैं, जिन्होंने बदलाव के लिए विंडोज के बहुत से सामान्य क्षेत्रों को नियंत्रित किया है, जो स्पायवेयर के द्वारा हो सकते थे इसमें वह सामर्थ्य शामिल है, जिससे संस्थापित किए गए सक्रिय एक्स साफ्टवेयर को आसानी से हटा देती है

http://en.wikipedia.org/wiki/Windows_Defender

माइक्रोसॉफ्ट सक्रिय संरक्षण सेवा

माइक्रोसॉफ्ट सक्रिय संरक्षण सेवा (संक्षिप्त कर यह एमएपीएस है, जिसे पहले माइक्रोसॉफ्ट स्पायनेट के नाम से जानते थे) विंडोज डिफेंडर व माइक्रोसॉफ्ट सिक्यूरिटी एशेंशियल्स के उपयोगकर्त्ताओं का नेटवर्क है, जो यह पता लगाने में मददगार रहता है कि कौनसे प्रोग्राम स्पायवेयर के रूप में वर्गीकृत किए गए हैं उत्पाद के उपयोगकर्त्ताओं के द्वारा किसी भी प्रस्तुत किए गए प्रोग्राम के लिए तैयार किए गए हस्ताक्षर सभी उपयोगकर्त्ताओं के लिए उपलब्ध हैं और जो बारग्राफ के रूप में प्रदर्शित किए गए हैं, जो उन लोगों का प्रतिशत बताते हैं, जिन्होंने उस वस्तु को मंजूर किया, अवरूद्ध किया या हटा दिया स्पायवेयर के वर्गीकरण का यह तरीका मंजूर करता है कि विरल, अज्ञात या नए स्पायवेयर को इस प्रकार वर्गीकृत किया जाए कि अधिकांश लोग अपने डाटा भेजने के लिए उसका चयन करें

http://en.wikipedia.org/wiki/Microsoft_Active_Protection_Service

माइक्रोसॉफ्ट सुरक्षा स्केनर

माइक्रोसॉफ्ट सुरक्षा स्केनर एक मुफ्त डिस्पोसेबल वायरस स्केनर है, जो दुर्भावनायुक्त साफ्टवेयर को हटाने हेतु विंडोज साधन के समान है, जिसका इस्तेमाल कंप्यूटर वायरस व अन्य प्रकार के मालवेयर के सिस्टम को स्केन करने के लिए किया जा सकता है माइक्रोसॉफ्ट सुरक्षा स्केनर रोजमर्रा के उपयोग के लिए नहीं बनाया गया है, क्योंकि यह वायरसों के समक्ष वास्तविक समय सुरक्षा

उपलब्ध नहीं कराता है और इसलिए यह अपनी वायरस व्याख्या को अद्यतन नहीं कर सकता है और दस दिनों के बाद यह समाप्त हो जाता है जबकि दूसरी ओर यह ऐसे कंप्यूटर पर बिना किसी संभवित हस्तक्षेप के चल सकता है, जिसमें पहले से ही एंटीवायरस उत्पाद है इसलिए इसे ऐसे किसी कंप्यूटर के स्केन के लिए काम में लिया जा सकता है, जहाँ संभवित संक्रमण हो व उपयोगकर्त्ता अन्य एंटीवायरस से दूसरी जाँच चाहता हो

http://en.wikipedia.org/wiki/Microsoft_Safety_Scanner

विंडोज लाइव वनकेयर

विंडोज लाइव वनकेयर में इस समय एकीकृत एंटीवायरस, फायरवाल, बेकअप व उपयोगिता बहाली व उपयोगिता को दुरुस्त करने की विशिष्टताएँ व साथ ही मालवेयर संरक्षण के लिए विंडोज डिफेंडर के एकीकृत कार्य इसमें हैं रजिस्ट्री सफाई करनेवाले के भविष्य के संस्करण पर विचार किया गया, लेकिन उसे जोड़ा नहीं गया, क्योंकि, इस कार्य के लिए ग्राहक को कोई उल्लेखनीय लाभ नहीं थेसंस्करण २ में विशिष्टताएँ हैं, जैसे कि बहुपीसी व गृह नेटवर्क प्रबंधन, प्रिंटर साझा सहयोग, शुरुआतीसमय हेतु आशावादी, सक्रिय स्थिरता व अनुशंसाएँ, मासिक रिपोर्ट्स, केन्द्रीकृत बेकअप व ऑनलाइन फोटो बेकअप

विंडोज लाइव वनकेयर को उपयोग में आसानी के लिए बनाया गया है और घरेलू उपयोगकर्त्ताओं के लिए इसे डिजाईन किया गया है वनकेयर अल्पतम अंतरफलक प्रयास करता है, जिससे उपयोगकर्त्ता के भ्रम व स्त्रोत के इस्तेमाल को कम किया जा सके अधिसूचना के क्षेत्र में यह एक प्रतीक स्थापित करता है, जो उपयोगकर्त्ता को तीन चेतावनी के रंगों हरा (अच्छा), पीला ((स्वच्छ) व लाल (जोखिम पर) का इस्तेमाल कर सिस्टम के स्वास्थ्य के बारे में इसे सरसरी तौर पर बताता

http://en.wikipedia.org/wiki/Windows_Live_OneCare_Safety_Scanner

स्कैटबस्टर

ट्रेंड माइक्रो स्कैटबस्टर एक मुफ्त साधन है, जो छिपी फाईल्स, रजिस्ट्री प्रविष्टियों, प्रक्रियाओं, ड्रायवर्स व मास्टर बूट रिकार्ड (एमबीआर) को स्केन करता है, जिससे स्कैट्स को मालूम कर उन्हें हटा सकें ट्रेंड माइक्रो स्कैटबस्टर के अद्यतन संस्करण में संवेदनात्मक जाँच प्रणाली की और भी अधिक विशेषताएँ हैं ट्रेंड माइक्रो स्कैटबस्टर निम्न की जाँच कर स्कैट्स का पता लगा सकता है

- मास्टर बूट रिकार्ड (एमबीआर)
- फाईल्स
- रजिस्ट्री प्रविष्टियाँ
- मूलआधार कोड पेचेस
- संचालन प्रणाली सेवा हुक्स
- फाईल प्रवाह
- ड्रायवर्स
- पोर्ट्स
- प्रक्रियाएँ
- सेवाएँ

छिपी फाईल्स, रजिस्ट्री प्रविष्टियों व सेवाओं को स्वच्छ कर या उन्हें दूर कर ट्रेंड माइक्रो स्कैटबस्टर विस्तृत व सदैव बढ़ रहे विभिन्न स्कैट को दूर कर सकता है

ण्द्यद्यद्रः//ढद्धड्डड्ड.ड्डदद्यत्थ्द्धद्वद्वद्य.ड़दृश्/द्वद्य/द्धदृदृद्यत्तद्य-ड्डद्वद्यद्यड्डद्ध/त्दड्डड्ड-ण्द्य१५

आरयूबोटेड

आरयूबोटेड आपके कंप्यूटर की संभवित संक्रमण तथा उन संदेहास्पद गतिविधियों के बारे में जो बोट्स से संबंधित हैं, उनके बारे में निगरानी रखता है बोट्स वे दुर्भावनापूर्ण फाईल्स हैं, जिससे साईबर अपराधी आपके कंप्यूटर को रहस्यमय तरीके से नियंत्रण में ले लेते हैं संभवित संक्रमण का पता लगा कर आरयूबोटेड उसे हॉउसकॉल से पहचान कर उसे स्वच्छ करेगा आपके कंप्यूटर की सतत निगरानी के साथ संभवित संक्रमण तथा संदेहास्पद गतिविधियों के बारे में आपके सिस्टम को आरयूबोटेड से संरक्षित करें
http://free.antivirus.com/us/rubotted/

ब्राउसर गार्ड

आगे से सक्रिय होकर आपके ब्राउसर को वेब की नई आशंकाओं के समक्ष संरक्षण दें ब्राउसर गार्ड २०११ में शून्यदिवस असुरक्षित प्रतिबंध है और अग्रणी अनुभव व समानुकरण तकनीकों का उपयोग कर यह दुर्भावनापूर्ण जावास्क्रिप्ट के समक्ष संरक्षण देता है ब्राउसर गार्ड तुरंत व सतत अद्यतन किया जाता है, जिससे सर्वाधिक सुरक्षित व अधुनातन तकनीक प्रदान की जा सके इसके नवीनतम संस्करण में शामिल हैं वेब ट्रोजन्स के लिए और संक्रमण की श्रंखला का पता लगाने के लिए पड़ताल में वृद्धि
http://free.antivirus.com/us/browser-guard/

मालवेयरबाईट्स एंटीमालवेयर फ्री

किसी भी एंटीवायरस प्रोग्राम के लिए मालवेयरबाईट्स एंटीमालवेयर फ्री एक उत्कृष्ट पूरक है इस साफ्टवेयर में लेजर जैसा फोकस है, जिससे आपके पीसी से शून्यदिवस ट्रिकी मालवेयर को दूर किया जा सके हम उसकी गिरगिट जैसी विशिष्टता को विशेष रूप से पसंद करते हैं, जो आपके साफ्टवेयर को छिपा देता है, जिससे दुर्भावनापूर्ण प्रोग्राम्स उसे नहीं ढूंढ सकते हैं हम प्रत्येक पीसी उपयोगकर्त्ता को मालवेयरबाईट्स एंटीमालवेयर फ्री के लिए अनुशंसा करते हैं
http://www.tomsguide.com/us/malwarebytes-free,review-2204.html

पांडा इंटरनेट सुरक्षा २०१५

पांडा इंटरनेट सुरक्षा २०१५ को इस प्रकार डिजाईन किया गया है, जिससे यह सुनिश्चित किया जा सके कि आप आपकी ऑनलाईन जिन्दगी का आनन्द, आपकी पूर्ण दिमागी शांति के साथ ले सकें यह आपके पीसी, फायरवाल, व वायफाय को एंटीवायरस व ऑनलाइन धोखाधड़ी के समक्ष अधिकतम संरक्षण प्रदान करता है आपके डाटा, दस्तावेजों या किसी भी नाजुक जानकारियों के समक्ष यह नियंत्रण व सुरक्षा की पहुँच देता है हमारी इंटरनेट सुरक्षा आपको मन की शांति प्रदान करती है अनुपयुक्त विषयसामग्री (अश्लील सामग्री, ड्रग्स, हथियार आदि) से आपके परिवार को पांडा इंटरनेट सुरक्षा २०१५ संरक्षण प्रदान करता है मातापिता का नियंत्रण आपके बच्चों को इंटरनेट के इस्तेमाल की आजादी देता है और उसी समय ऐसे किसी भी व्यवहार को यह मंद कर देता है, जिसके लिए आप अनुभव करते हैं कि वह अनुपयुक्त है
http://www.pandasecurity.com/india/homeusers/solutions/internet-security/

क्लामविन पोर्टेबल

क्लामविन पोर्टेबल बहुत कुछ बड़े भाई की तरह है यह मुफ्त है, खुला स्त्रोत है और मशीनों को असंक्रमित करने के लिए यह बड़ा काम करता है क्लामविन की पड़ताल की दर बहुत अधिक है और उसकी व्याख्याएँ बारबार अद्यतन होती रहती हैं और इसमें ग्राफिकल इंटरफेस को उपयोग करना बहुत आसान होता है क्लामविन के उपयोग हेतु केवल यही आपत्तिसूचना है कि यह वास्तविकसमय स्केनर प्रस्तुत नहीं करता है जो पोर्टेबल संस्करण के लिए कोई मुद्दा नहीं है यह मेरा इरादे वाला पोर्टेबल वायरस स्केनिंग साफ्टवेयर है
http://www.techrepublic.com/blog/five-apps/five-portable-antivirus-and-antimalware-tools-to-carry-with-you-at-all-times/

सोफोस एंटी स्क्रिकट पोर्टेबल

सोफोस एंटी स्क्रिकट पोर्टेबल यह उन साधनों में से है, जिसके लिए आप आशा करते हैं कि आपको उसे कभी इस्तेमाल नहीं करना है; लेकिन आप जानते हैं कि किसी समय मौका आने पर करना पड़ेगा सोफोस उल्लेखनीय रूप से रूट किट्स का पता लगाने में दक्ष हैविशेषकर पोर्टेबल एप के लिए स्क्रिकट्स को सोफोस स्केन करता है, पड़ताल करता है और दूर करता है और यह १०० मुफ्त है तथा विंडोज एक्सपी, विस्टा व ७ को सहयोग प्रदान करता है और आपके वर्तमान के एंटीवायरस के साथ काम में आता है मैंने पाया है कि सोफोस पर्याप्त रूप से उपयोग करने के लिए विश्वसनीय है, जब वह पीसी जिसे स्केन करना हो, वह उपयोग में हो
http://www.techrepublic.com/blog/five-apps/five-portable-antivirus-and-antimalware-tools-to-carry-with-you-at-all-times/

एमसीसाफ्ट फ्री इमरजेंसी टूलकिट

मालवेयर को हटाने के लिए एमसीसाफ्ट फ्री इमरजेंसी टूलकिट एक सशक्त साधन है, जो स्केन कर सकता है और आपके पीसी से छह मिलियन से भी अधिक खतरों को दूर कर सकता है एमसीसाफ्ट फ्री इमरजेंसी टूलकिट में दोनों है, जीयूआई व कमांड लाईन, संस्करण, जिससे आप आपकी मशीन को तब भी स्केन कर सकें, जब यदि जीयूआई के साथ कोई समस्या हो इस टूलकिट के साथ आप न केवल मालवेयर स्केनर प्राप्त करते हैं, बल्कि साथ ही हाईजैकफ्री व ब्लिट्जब्लैंक भी प्राप्त करते हैं एमसीसाफ्ट मुफ्त डाऊनलोड मुहैया कराता है या आप पहले से ही कम्पाईल की गई यूएसबी स्टिक खरीद सकते हैं
http://www.techrepublic.com/blog/five-apps/five-portable-antivirus-and-antimalware-tools-to-carry-with-you-at-all-times/

विप्रे रेसक्यू

विप्रे रेसक्यू वह साधन है, जिसका इस्तेमाल आप तब करते हैं, जब आपकी मशीन बहुत संक्रमित हो गई हो विप्रे सुरक्षित मोड में चलाई जाती है और इसके इस्तेमाल के लिए जीयूआई साधन पर निर्भर नहीं रहना पड़ता है निष्पादन के योग्य आपकी दोहरी क्लिक और एक कमांड, विंडो को स्केनर के चलते हुए (तड़कभड़क की चाल के साथ) खोल देते हैं यदि आप पहले से ही विप्रे के पूर्ण संस्करण का उपयोग कर रहे हैं, तब भी आप इस साधन का उपयोग कर सकते हैं, यदि आपकी मशीन बहुत संक्रमित हो गई हो, तो विप्रे नहीं चलेगा
http://www.techrepublic.com/blog/five-apps/five-portable-antivirus-and-antimalware-tools-to-carry-with-you-at-all-times/

स्पायबोट सर्च व डिस्ट्राय पोर्टेबल

स्पायबोट सर्च व डिस्ट्राय पोर्टेबल अत्यधिक लोकप्रिय पूर्ण स्पायबोट सर्च व डिस्ट्राय का पोर्टेबल संस्करण है दुर्भावनापूर्ण साफ्टवेयर का पता लगाने व उसे हटाने हेतु यह एंटीमालवेयर साधन बड़ा काम करता है सब कुछ आपके फ्लैश ड्राइव के साथ स्पायबोट में एक अद्भुत विशिष्टता है कि आप स्केन शुरूकरें, उसके पहले आपकी रजिस्ट्री के बेकअप में आपको इससे मदद मिलेगी स्पायबोट आपकी पीसी रजिस्ट्री को क्षतिग्रस्त कर दे तब उसकी बहाली के लिए आपके पास बेकअप है सुरक्षित व दुरूस्त
http://www.techrepublic.com/blog/five-apps/five-portable-antivirus-and-antimalware-tools-to-carry-with-you-at-all-times/

एडअवेयर फ्री एंटीवायरस

लेवासोफ्ट का एडअवेयर सर्वाधिक विश्वसनीय स्पायवेयर साधनों में से एक है और यह वर्षों से उद्योग में एक निर्देशचिन्ह है और यह संस्थापन में आश्चर्यजनक रूप से सरल है, इससे गैरअतिक्रमणयुक्त अधिसूचनाएँ और विलक्षण परिणाम मिलते हैं साफ्टवेयर का मुफ्त संस्करण वास्तविक समय का एंटी वायरस व मालवेयर संरक्षण प्रदान करता है व साथ ही रेटबॉक्स की समानुकरण तकनीक

में अद्यतन भी है और इस प्रकार पर्याप्त संरक्षण देना, फिर चाहे आप वेब का ब्राउसिंग कर रहे हों, फाईल्स डाऊनलोड कर रहे हों या मात्र आप अपनी ईमेल ही जाँच रहे हों
http://www.digitaltrends.com/computing/best-free-antivirus-software/

फ्रोजन सॉफ्ट वायरस टोटल अपलोडर

फ्रोजन सॉफ्ट वायरस टोटल अपलोडर के द्वारा आप किसी भी फाईल को वायरस टोटल की मुफ्त सेवा से अपलोड कर सकते हैं, जहाँ ४० से अधिक प्रमुख एंटी वायरस उत्पाद स्केन किए जाते हैं विंडोज के बाएँ क्लिक मेनू में अपलोड के विकल्प को यह प्रोग्राम जोड़ता है तथा आप ड्राप फाईल्स को डेस्कटॉप विडगेट या एप्लीकेशन इंटरफेस पर ला सकते हैं एक बार आपकी फाईल्स अपलोड और स्केन हो गई, आप अधिसूचित किए जाएँगे और एकीकृत रिपोर्ट प्रेक्षक से स्केन के परिणामों की समीक्षा कर सकते हैं इस प्रोग्राम में कार्य प्रबंधक भी शामिल हैं, जो चल रही प्रक्रियाओं, सक्रिय जोड़, सेवाएँ व स्टार्टअप कार्यक्रम दर्शाते हैं और स्केनिंग के लिए आपको शीघ्र संदेहास्पद वस्तुओं को वायरस टोटल को प्रस्तुत करने देता है अन्य विशिष्टताओं में शामिल हैं विस्तृत लागिंग अपलोड्स व परिणाम, ग्राहकीकृत अधिसूचना विकल्प व व्यक्तिगत वायरस टोटल एपीआईएस के लिए सहयोग
http://www.spychecker.com/program/vtu.html

मैकेफी स्टिंजर

मैकेफी स्टिंजर एक पोर्टेबल एंटी वायरस स्केनर है, जो विशिष्ट वायरसों की जाँच कर उन्हें दूर करता है यह पूर्ण फीचरवाले एंट ीवायरस संरक्षण का स्थानापन्न नहीं है, बल्कि यह एक साधन है, जिसके द्वारा प्रशासकों व उपयोगकर्त्ताओं को मदद मिलती है, जब उनका सामना संक्रमित प्रणाली के साथ होता है यह प्रोग्राम मैकेफी स्केन इंजिन तकनीक का उपयोग करता है, जिसमें प्रक्रिया की स्केनिंग, डिजिटली हस्ताक्षरित फाईल्स व स्केन निष्पादन अनुकूलन भी शामिल हैं स्टिंजर ३००० से अधिक वायरस, ट्रोजन्स व ऐसे ही अनूठों की जाँच करता है व साथ ही मालवेयर की जो वैधानिक सुरक्षा एप्लीकेशन के लिए मुखौटा रहता है (फर्जी चेतावनी)
http://www.spychecker.com/program/stinger.html

इम्युनेट

यह आपके पीसी को वास्तविक समय का संरक्षण देता है इसने प्रतिदिन १३ मिलियन से अधिक वायरस व हजारों नई धमकियों के समक्ष संरक्षण दिया है, दूसरी किसी वायरस की पड़ताल की फाईल को डाऊनलोड किए बगैर अन्य समाधानों के विपरीत, इम्युनेट की लो डिस्क व स्मृति का उपयोग आपके पीसी को नहीं दबाता है यह समुदाय आधारित संरक्षण है, जो आपके मित्रों को मुफ्त संरक्षण मुहैया कराता है इम्युनेट फ्री पहला एंटीवायरस एप्लीकेशन है, जो आपके समुदाय व सोशल नेटवर्क को संरक्षण देने के लिए तैयार किया गया है इम्युनेट समुदाय में आसानी से लोगों को जोड़ें और उनकी संरक्षण की स्थिति को ऑनलाइन देखें
किसी भी वायरस सिग्नेचर की फाईल को डाऊनलोड किए बगैर, वायरस, स्पायवेयर, बोट्स, वार्म्स, ट्रोजन्स व मुख्य लागर्स के समक्ष इम्युनेट क्लाउड से वास्तविकसमय की जाँच है सामूहिक असंक्रमणीकरण व चतुर वायरस जाँच तकनीक के साथ संरक्षित रहिए, जो आपके पीसी को धीमा नहीं होने देती है
http://www.immunet.com/free/features/index.html

टीडीएसएसकिलर

टीडीएसएसकिलर एक एकल उपयोगिता है, जो रूटकिट में से रूटकिट का पता लगा कर उन्हें हटाने में विशेषज्ञ हैं विन ३२ टीडीएसएस परिवार, जिसमें शामिल हैं एसएसटी, पिहार, शून्य पहुँच, सिनोवाल, फांटा, स्टोंड, आरलोडर, सीमोसर व सीडोक्स मात्र एप्लीकेशन चलाएँ, स्केन बटन को दबाएँ और फिर परिणाम के लिए प्रतीक्षा करें
http://www.spychecker.com/program/tdsskiller.html

इंटरनेट सुरक्षा

इंटरनेट सुरक्षा सम्पूर्ण फीचर वाला एंटीवायरस प्रोग्राम है, जिसे तीन स्केनिंग इंजिन्स ३६० ह्यूरेस्टिक इंजिन, ३६० क्लाउड इंजिन व बिटडिफेंडर से शक्ति मिलती है वास्तविक समय संरक्षण, सुरक्षित ब्राउसिंग, डाऊनलोड संरक्षण, निजता संरक्षण, वेबकेम संरक्षण, यूएसबी संरक्षण व साथ ही एक सुरक्षित रेतबॉक्स यह प्रोग्राम प्रदान करता है, जो आपके पीसी के वातावरण में से प्रक्रियाओं को पृथक करने में समर्थ बनाता है अन्य विशिष्टताओं में शामिल हैं स्वमेव नवीनीकरण, निर्धारित व माँग पर स्केनिंग, आगे से सक्रिय होकर रक्षा, नेटवर्क संरक्षण, निजता सफाई (गुप्त वस्तुएँ, बिस्किट, इतिहास आदि) एवं स्वसंरक्षण, जिससे आपके एंटीवायरस संरक्षण के हस्तक्षेप के द्वारा मालवेयर की रोकथाम हो सके

http://www.spychecker.com/program/360is.html

कासपरस्की वायरस हटाने का साधन

कासपरस्की वायरस हटाने का साधन एक एकल वायरस स्केनर है, जिसे इस प्रकार डिजाईन किया गया है, जिससे यह आपके कंप्यूटर से सभी प्रकार के संक्रमणों को हटा सके जाँच के लिए यह वैसे ही प्रभावी अल्गोरिदम्स की ओर संकेत करता है, जैसे कि कासपरस्की उत्पादों के लिए उपयोग में लिया जाता है, लेकिन यह किसी भी प्रकार का वास्तविक समय संरक्षण प्रदान नहीं करता है कासपरस्की वायरस हटाने का साधन उपयोगी हो सकता है, यदि आप कोई संक्रमित मशीन की सफाई तो करना चाहते हैं, लेकिन संपूर्ण फीचरवाला एंटीवायरस साधन को संस्थापित नहीं करना चाहते हैं

http://www.spychecker.com/program/kremoval.html

एमसीशील्ड

एमसीशील्ड एक एंटीमालवेयर प्रोग्राम है, जिसे इस प्रकार डिजाईन किया गया है, जिससे पोर्टेबल यूएसबी ड्राइव्स से मालवेयर व वायरस संक्रमण की रोकथाम की जा सके यह डाले गए प्रत्येक के लिए हटाने योग्य ड्राइव को स्वतः स्केन करता है और जाँच करता है कि क्या उसमें कोई संभवित धमकी है यह प्रोग्राम अनुभवात्मक जाँच इंजिन का प्राथमिक उपयोग करता है, लेकिन साथ ही इसमें सम्मिलित होते हैं जानी हुई ख़राब वस्तुओं के हस्ताक्षर डाटाबेस, जिसे इसके अंदर निर्मित अपडेटर के साथ समयसमय पर अद्यतन किया जा सकता है

http://www.spychecker.com/program/mcshield.html

रोबोस्केन इंटरनेट सिक्योरिटी फ्री

रोबोस्केन एक इंटरनेट सिक्योरिटी सूट है, जिसमें वास्तविकसमय एंटीवायरस स्केनिंग, मालवेयर संरक्षण व एक व्यक्तिगत फायरवाल तथा साथ ही अन्य कई साधन भी शामिल हैं, जो आपके सिस्टम की सामान्य नजाकत व टुकड़े हुई नाजुक फाईल्स को जानने में मदद दे सकते हैं एंटीवायरस संरक्षण वीबी १०० प्रमाणित दो इंजिन्स (ईएसटी सॉफ्ट के टेरा इंजिन व बिटडिफेंडर) इस्तेमाल करता है तथा वास्तविक समय संरक्षण, निर्धारित स्केन्स व स्वमेव अपडेट्स प्रस्तुत करता है

http://www.spychecker.com/program/roboscan.html

पीसी टूल्स एंटीवायरस फ्री एडिशन

पीसी टूल्स एंटीवायरस फ्री एडिशन एक एंटीवायरस स्केनर है, जो वायरस, वार्म्स व ट्रोजन्स के समक्ष बुनियादी संरक्षण उपलब्ध कराता है इसमें शामिल हैं फाईल्स का वास्तविक समय स्कान व साथ ही आनेवाले व जानेवाले ईमेल सन्देश एवं एक वैकल्पिक ब्राउसर टूलबार (ब्राउजर डिफेंडर) जो दुर्भावनापूर्ण वेबसाईट्स से आपको संरक्षण प्रदान करता है मुफ्त संस्करण में असमर्थ की गई विभिन्न अग्रिम विशिष्टताएँ हैं

http://www.spychecker.com/program/pctoolsav.html

वायरस टोटल अपलोडर

वायरस टोटल अपलोडर के द्वारा आप फाईल को लोकप्रिय वायरस टोटल सेवा पर अपलोड कर सकते हैं और उसे ४० प्रमुख एंटीवायरस उत्पाद जिनमें नार्टन, मेकाफी, एवास्ट, एवीजी जैसे कई शामिल हैं, के साथ उसे स्केन कर सकते हैं उसके बाद आप रिपोर्ट की समीक्षा कर सकते हैं, जिसमें प्रत्येक उत्पाद के स्केन के परिणाम शामिल होते हैं वायरस टोटल अपलोडर फिर विंडोज एक्सप्लोरर सेंड तो मेनू के साथ एकीकृत होता है और उससे आप जो फाईल्स पहले ही डाऊनलोड की गई हैं, उन फाईल्स को जल्दी से अपलोड कर सकते हैं या फिर आप फाईल के यूआरएल के डाऊनलोड को प्रस्तुत कर सकते हैं और आपके कंप्यूटर पर स्टोर किए बगैर सेवा के लिए भेज सकते हैं

http://www.spychecker.com/program/virustotal.html

सोफोस एंटीस्रकिट

आपके कंप्यूटर में जो भी स्रकिट छिपे हों, उन्हें सोफोस एंटीस्रकिट पता लगा कर दूर कर देता है यह साथ चल रही प्रक्रियाओं को स्केन करता है व साथ ही ज्ञात स्रकिट्स के लिए रजिस्ट्री व स्थानीय हार्ड ड्राइव्स करता है व सिस्टम की निष्ठा के साथ कोई समझौता किए बगैर हटाने के लिए फाईल्स का चयन स्वतः करता है साथ ही शामिल है कमांडलाईन के कार्य

http://www.spychecker.com/program/sophosantiroot.html

सोफोस कॉन्फिकर रिमोवल टूल

कॉन्फिक संक्रमण को समाप्त करने के लिए सोफोस कॉन्फिकर रिमोवल टूल एक मुफ्त साधन है, जिसके द्वारा आपके नेटवर्क पर के कॉन्फिकर वायरस का पता लगाता है, उसे पृथक करता है और उन्हें दूर करता है

http://www.spychecker.com/program/sophosconfrem.html

एफसिक्योर ब्लेकलाईट

एफसिक्योर ब्लेकलाईट उपयोगकर्त्ता व मानक सुरक्षा साफ्टवेयर से तथाकथित छिपे हुए स्रकिट्स को आपके सिस्टम में से स्केन करता है यदि स्केन में कोई संदेहास्पद वस्तु पाई जाती है, तब आपके पास विकल्प होगा कि उसे हटा दें

http://www.spychecker.com/program/fsblacklight.html

अमिति एंटीवायरस

अमिति एंटीवायरस एक मुफ्त एंटीवायरस प्रोग्राम है, जिसमें अनुभवजन्य स्केनिंग शामिल है और यह ४ विभिन्न प्रकार के स्केन में सहयोग करता है, जिसमें वह भी शामिल है जो उन वायरसों की जाँच कर सकता है जो इस समय स्मृति में चल रहे हैं अमिति एंट ीवायरस का इस्तेमाल विंडोज ८, ७, विस्टा व एक्सपी के साथ किया जा सकता ह

http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.htm

बैडू एंटीवायरस २०१५

क्लाउड आधारित वायरस डाटाबेस के माध्यम से मॉलवेयर से संघर्ष करने हेतु बैडू एंटीवायरस २०१५ कम वजनवाला है विंडोज ८, विंडोज ७, विंडोज विस्टा व विंडोज एक्सपी पर बैडू एंटीवायरस २०१५ काम करता है संरक्षण में वृद्धि के लिए अन्य एंटीवायरस साफ्टवेयर के साथ बैडू एंटीवायरस २०१५ संस्थापित कीजिए यह स्वमेव यूएसबी साधनों व विंडोज रजिस्ट्री को अद्यतन करता है और स्केन करता है और इसमें क्लाउड फाईल स्केनर निर्मित है, जिससे स्केन की जाने वाली बैडू की संदेहास्पद फाईल्स को अपलोड कर सकें और इसमें अन्य कई उपयोगी साधन शामिल रहते हैं जैसे कि यातायात नियंत्रक व निजी ब्राउसर साधन

http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.htm

कोमोडो एंटीवायरस

कोमोडो सुरक्षा समाधानों का कोमोडो एंटीवायरस एक और उत्कृष्ट प्रोग्राम है और मुफ्त एंटीवायरस के श्रेष्ठ विकल्पों में यह आसान है कोमोडो एंटीवायरस अन्य धमकी के स्त्रोतों से आपको संरक्षण दिलाता है, अन्य अधिकांश मुफ्त एंटीवायरस प्रोग्राम की तरह, जो इस सूची जैसा करते हैं विंडोज ८, विंडोज ७ व विंडोज विस्टा पर कोमोडो एंटीवायरस काम करता है
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.htm

फोर्टीक्लाएंट

फोर्टीक्लाएंट एक एंटीवायरस, वेबफिल्टरिंग, फायरवाल, मातापिता नियंत्रित , इष्टतम, (और फिर कुछ) एक प्रोग्राम है और जो किसी व्यवसाय के इस्तेमाल के लिए पर्याप्त शक्तिशाली है यह अधिक परिशुद्धता के साथ धमकी प्रबंधनसाधन के रूप में व्याख्यायित किया जाता है विंडोज ८, विंडोज ७, विंडोज विस्टा व विंडोज एक्सपी पर फोर्टीक्लाएंट काम करता है
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.htm

किंगसॉफ्ट एंटीवायरस २०१२

किंगसॉफ्ट एंटीवायरस २०१२ एक क्लाउड आधारित एंटीवायरस प्रोग्राम है, वैसे ही जैसे कि पांडा क्लाउड एंटीवायरस व इम्यूनेट फ्री एंटीवायरस है फाईल्स की डाउनलोडिंग के समय, आईएम पर चैटिंग आदि के समय किंगसॉफ्ट एंटीवायरस स्थानीय रूप से मालवेयर पर नजर रखता है विंडोज ८, विंडोज ७, विंडोज विस्टा व विंडोज एक्सपी पर किंगसॉफ्ट एंटीवायरस २०१२ काम करता है
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.01.htm

आउटपोस्ट सिक्योरिटी सूट फ्री

आउटपोस्ट सिक्योरिटी सूट फ्री एक मुफ्त एंटीवायरस प्रोग्राम है, जो वेब व ईमेल स्केनिंग व साथ ही फायरवाल के लिए सहयोग करता है एप्लीकेशंस व नेटवर्क पैकेट्स पर फिल्टर व साथ ही स्थानीय नेटवर्क योजनाओं के द्वारा अंदर निर्मित फायरवाल नियंत्रण कर सकता है आउटपोस्ट सिक्योरिटी सूट फ्री में यह योग्यता भी शामिल हैं कि वह सिस्टम की नाजुक सेटिंग्स को हस्तक्षेप से सुरक्षित रखे
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.01.htm

राइजिंग एंटीवायरस फ्री एडिशन

चीन के सबसे बड़े एंटीवायरस निर्माता राइजिंग साफ्टवेयर की ओर से राइजिंग एंटीवायरस फ्री एडिशन एक मुफ्त एंटीवायरस प्रस्तुति है विंडोज ७, विंडोज विस्टा व विंडोज एक्सपी पर राइजिंग एंटीवायरस फ्री एडिशन काम करता है
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.01.htm

अनथ्रेट फ्री एंटीवायरस २०१४

अनथ्रेट फ्री एंटीवायरस २०१४, मानक मालवेयर संरक्षण प्रदान करता है, जिसमें ईमेल के माध्यम की धमकियाँ भी सम्मिलित हैं इसकी कीमत .....या उसकी कमी, को एक ओर रख मैंने इस प्रोग्राम में कुछ भी प्रभावशाली नहीं पाया, ऐसा मैं मानता हूँ विंडोज ८, विंडोज ७, विंडोज विस्टा व विंडोज एक्सपी पर अनथ्रेट फ्री एंटीवायरस २०१४ काम करता है
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.01.htm

झिल्या! एंटीवायरस

झिल्या! एंटीवायरस, एक और मुफ्त एंटीवायरस प्रोग्राम है, जो विंडोज के साथ काम करता है यह इस सूची के लगभग अन्य अधिकांश प्रोग्राम्स की तरह ही है यह सक्रियता से ईमेल्स व यूएसबी साधनों को स्केन करता है और आप शीघ्र, पूर्ण या चलन के वायरस स्केन का चयन कर सकते हैं इसमें अपवर्जन श्रेणी है, अतः आप स्केन करने से कुछ फोल्डर्स/ या फाईल्स को हटा सकते हैं

झिल्या ! एंटीवायरस में कुछ अतिरिक्त विशिष्टताएँ हैं, जैसे कि तैयार कार्यप्रबंधक व स्टार्टअप प्रबंधक, जिससे स्टार्टअप मदों को असमर्थ कर सकें व्याख्याअद्यतन को शारीरिक रूप से संस्थापित किया जाना चाहिए और ये आकार में सामान्यतः बहुत बड़े होते हैं और जब आप अन्य एंटीवायरस प्रोग्राम्स से तुलना करते हैं, तो यह एक कठिन मामला होता है
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.01.htm

झोनअलार्म फ्री एंटीवायरस फायरवाल २०१५

झोनअलार्म फ्री एंटीवायरस फायरवाल २०१५ मात्र मुफ्त एंटीवायरस व फायरवाल साधन का मिश्रण है झोनअलार्म फ्री एंट ीवायरसफायरवाल २०१५ के निर्माता चेक पेंट साफ्टवेयर लंबे समय से फायरवाल के व्यवसाय में हैं वे अच्छे साफ्टवेयर निर्मित करते हैं और यह प्रोग्राम इसका कोई अपवाद नहीं है इस प्रोग्राम के एंटीवायरस भाग के बारे में मैंने कुछ भी भव्य नहीं पाया, एंट ीवायरस व फायरवाल इसमें कस कर एकीकृत किए हुए हैं और उसके कुछ लाभ हैं
http://freebies.about.com/od/computerfreebies/tp/best-free-antivirus.01.htm

इस्कान एंटीवायरस

नई अद्यतन वायरस नियंत्रण तकनीक व उच्च परिष्कृत अनुभव अलगोरिदम के साथ इस्कान प्रभावी ढंग से मालवेयर के लेखकों के द्वारा सतत जारी किए जानेवाले मालवेयर के समक्ष वास्तविक समय संरक्षण उपलब्ध कराते हैं यह उपयोगकर्त्ताओं का पता लगते हैं और उन एप्लीकेशंस के लिए चेतावनी देते हैं, जो संदेहास्पद ढंग से व्यवहार करते हैं और इस प्रकार शून्यदिवस धमकी से संरक्षण प्रदान करते हैं इस्कान के द्वी मार्गी फायरवाल फीचर कंप्यूटर पर आनेवाले व जानेवाले नेटवर्क यातायात को छानते हैं व साथ ही नियंत्रित करते हैं तथा नेटवर्क आधारित सभी प्रकार के हमलों से संरक्षित करते हैं वायरस व अन्य साइबर धमकियों के समक्ष इस्कान अपनी उन्नत व नवप्रवर्तित तकनीकों के द्वारा प्रभावी ढंग से वास्तविक समय पर आधारित संरक्षण प्रदान करते हैं सिस्टम के स्टार्टअप के दौरान उपयोगकर्त्ता सुरक्षित वातावरण में इस्कान रेसक्यू मोड फीचर के साथ बिना किसी आप्टिकल मीडिया का उपयोग करते हुए बूट कर सकता है
http://www.escanav.com/english/content/products/escan_soho/escan_universal_security_suite.asp

सिमांटेक एंडपाईंट प्रोटेक्शन

सिमांटेक कार्पोरेशन के द्वारा सिमांटेक एंडपाईंट प्रोटेक्शन तैयार किया गया है और यह एंटीवायरस व व्यक्तिगत फायरवाल उत्पाद है, जिसे सर्वर्स व कार्यस्थलों की केन्द्रीकृत प्रबंधन कार्पोरेट में वातावरण सुरक्षा के लिए लगाया जाता है
http://en.wikipedia.org/wiki/Symantec_Endpoint_Protection

लायनक्स आधारित साधन

गृह संस्करण की रोक

रोको ! लायनक्स मंच की बढ़ती हुई लोकप्रियता के लिए लायनक्स गृह संस्करण एक एंटीवायरस समाधान प्रस्तुत करता है यह साफ्टवेयर मात्र गृह उपयोगकर्त्ताओं तथा गैरवाणिज्यिक उपयोग के लिए डिजाईन किया गया है

एवीजी मुफ्त संस्करण

लायनक्स की ऊर्जा से युक्त मशीनों के लिए वायरस के समक्ष लायनक्स के लिए एवीजी ७.५ व्यापक व विश्वसनीय संरक्षण उपलब्ध कराता है यह कई विशिष्टताएँ देता है, जैसे कि अनुसूचित व मांग पर फोल्डर्स की स्केनिंग, फाईल्स व संभवित वायरस संक्रमण के लिए सामान्य आर्चिव के प्रकार इंटरनेट या स्थानीय अपडेट स्त्रोतों से आपके एवीजी को अनुसूचित या मांग पर अपडेट निष्पादित कर सकते हैं

क्लामटीके

क्लाम एंटीवायरस के लिए जीटीके२ पर्ल का इस्तेमाल करते हुए क्लामटीके एक जीयूआई अग्रिमअंत है इस्तेमाल में आसानी और कम वजन के रूप में इसे डिजाईन किया गया है और लायनक्स के लिए यह पाइंट व क्लिक डेस्कटॉप वायरस स्केनर है

http://sourceforge.net/projects/clamtk/

बिटडिफेंडर

यूनिसेस हेतु बिटडिफेंडर एंटीवायरस स्केनर में दोनों हैं ग्राफिकल उपयोगकर्त्ता इंटरफेस जिससे स्केनर पर सीधे एप्लीकेशन मेनू सूची से पहुँच सकें और कमांड लाईन इंटरफेस जो अधिक उन्नत उपयोगकर्ताओं के लिए हैं स्क्रिप्ट व विस्तार आधारित एकीकरण के माध्यम से आपके पसंदीदा फाईल प्रबंधक, ईमेल या समाचार ग्राहक की कंफिगुरिंग में मदद मिलती है, जिससे यूनिसेस के लिए बिट डिफेंडर एंटीवायरस स्केनर का इस्तेमाल आसानी से किया जा सकता है

संक्रमण की और अधिक जोखिम को न्यूनतम करने तथा सुरक्षित विश्लेषण करने हेतु यूनिसेस के बिटडिफेंडर एंटीवायरस स्केनर संक्रमित फाईल्स को संरक्षित डिरेक्ट्री में पृथक कर सकता है संक्रमित फाईल्स के आलावा संदेहास्पद फाईल्स को भी पृथक क्षेत्र में ले जाया जा सकता है, क्योंकि अनुभवात्मक विश्लेषण के द्वारा उन्हें पहचाना गया है तथा दुर्भावनापूर्ण कोड की ज्ञात खूबियाँ उनमें होती हैं और ज्ञात वायरस हस्ताक्षर के साथ उनका मिलान नहीं होता है

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

कोमोडो एंटीवायरस

कोमोडो एंटीवायरस विशिष्ट रूप से तैयार किया गया है, जिससे सभी ज्ञात वायरस ट्रोजन्स व वार्म्स के समक्ष संरक्षण दिया जा सके इसका संस्थापन, कंफिग्यूर व इस्तेमाल आसान है उद्योग के प्रमुख कार्यों की सूची, जिसमें अद्यतन व अत्यंत परिष्कृत तकनीक समाहित हैं, उनके लिए कोमोडो एंटीवायरस की प्रशंसा है

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

बिटडिफेंडर एंटीवायरस स्केनर

यूनिसेस के लिए बिटडिफेंडर एंटीवायरस स्केनर में दोनों हैं ग्राफिकल उपयोगकर्त्ता इंटरफेस जिससे स्केनर पर सीधे एप्लीकेशन मेनू सूची से पहुँच सकें और कमांड लाईन इंटरफेस जो अधिक उन्नत उपयोगकर्ताओं के लिए हैं स्क्रिप्ट व विस्तार आधारित एकीकरण के माध्यम से आपके पसंदीदा फाईल प्रबंधक, ईमेल या समाचार ग्राहक की कंफिगुरिंग में मदद मिलती है, जिससे यूनिसेस के लिए बिटडिफेंडर एंटीवायरस स्केनर का इस्तेमाल आसानी से किया जा सकता है संक्रमण की और अधिक जोखिम को न्यूनतम करने तथा सुरक्षित विश्लेषण करने हेतु यूनिसेस के बिटडिफेंडर एंटीवायरस स्केनर संक्रमित फाईल्स को संरक्षित डिरेक्ट्री में पृथक कर सकता है संक्रमित फाईल्स के आलावा संदेहास्पद फाईल्स को भी पृथक क्षेत्र में ले जाया जा सकता है, क्योंकि अनुभवात्मक विश्लेषण के द्वारा उन्हें पहचाना गया है तथा दुर्भावनापूर्ण कोड की ज्ञात खूबियाँ उनमें होती हैं और ज्ञात वायरस हस्ताक्षर के साथ उनका मिलान नहीं होता है

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

पांडा एंटीवायरस

लायनक्स सर्वर्स व डेस्कटॉप के लिए पांडा एंटीवायरस हेतु लायनक्स है यह एक एंटीवायरस है, जिसे कमांड लाईन या कंसोल से प्रबंधित करने के लिए डिजाईन किया गया है ऐसा करने के लिए निष्पादन करने वाले जिसे पीएवीसीएल कहते हैं का उपयोग किया जाता है पांडा एंटीवायरस का लक्ष्य होता है कि उन विंडोज व डीओएस कार्यस्थलों को स्केन कर असंक्रमित किया जाए, जो लायनेक्स सर्वर से संबद्ध व साथ ही जो लायनेक्स सर्वर हैं पांडा एंटीवायरस दोनों का स्ट्रिंग सर्चेस व ह्यूरिस्टिक तरीके का उपयोग कर फाईल्स स्केन करता है लक्ष्य फाईल्स हैं वर्ड दस्तावेज, जावा एप्लेट्स, एक्टिव एक्स को यह नियंत्रित करता व सिकोड़ता है

(झेडआईपी, आरएआर आदि) इस समय यह बूट खंड या विभाजन टेबल को स्केन नहीं कर सकता है
http://pandacloudcleaner.pandasecurity.com/facebook/

एफपीआरओटी एंटीवायरस

लायनक्स कार्यस्थल विशिष्टताओं के लिए एफपीआरओटी २११९९५८ से अधिक ज्ञात वायरस व उनकी किस्मों को स्केन करता है क्रोन उपयोगिता के साथ जब इस्तेमाल किया जाता है, तब अनुसूचित स्कान को निष्पादित करने की योग्यता रहती है हार्ड ड्राइव्स, सीडीरोम्स, डिस्केट्स, नेटवर्क ड्राइव्स, डिरेक्ट्रीस व विशिष्ट फाईल्स को स्कान करता है बूट खंड के वायरसेस, मेक्रो वायरसेस व ट्रोजन हार्सेस के बिम्बों के लिए स्केन करता है
http://www.f-prot.com/products/home_use/linux/

पांडा एंटीवायरस

पांडा इंटरनेट सुरक्षा २०१५ को इस प्रकार डिजाईन किया गया है, जिससे यह सुनिश्चित किया जा सके कि आप आपकी ऑनलाईन जिन्दगी का आनन्द आपकी पूर्ण दिमागी शांति के साथ ले सकें यह आपके पीसी, फायरवाल, व वायफाय को अधिकतम एंटीवायरस व ऑनलाइन धोखाधड़ी के समक्ष अधिकतम संरक्षण प्रदान करता है आपके डाटा, दस्तावेजों या किसी भी नाजुक जानकारियों के समक्ष यह नियंत्रण व सुरक्षा की पहुँच देता है हमारी इंटरनेट सुरक्षा आपको मन की शांति प्रदान करती है अनुपयुक्त विषयसामग्री (अश्लील सामग्री, ड्रग्स, हथियार आदि) से आपके परिवार को पांडा इंटरनेट सुरक्षा २०१५ संरक्षण प्रदान करता है मातापिता का नियंत्रण आपके बच्चों को इंटरनेट के इस्तेमाल की आजादी देता है और उसी समय ऐसे किसी भी व्यवहार को यह मंद कर देता है, जिसके लिए आप अनुभव करते हैं कि वह अनुपयुक्त है
http://www.pandasecurity.com/india/homeusers/solutions/internet-security/

इस्कान एंटीवायरस

माँग पर साफ्टवेयर एप्लीकेशन के रूप में इस्कान कार्य करता है, जिसे आपकी जरूरतों के अनुसार लगाया जा सकता है इसमें कमांड लाईन व ग्राफिकल यूसर इंटरफेस (जीयूआई) स्केनर होते हैं यह चयनित डिरेक्टरी स्केन, स्थानीय हार्ड डिस्क व होम डिरेक्टरी स्केनिंग की सुविधा देता है व साथ ही मेमोरी स्केन की भी, जिससे यह सुनिश्चित किया जा सके कि यह सायबर धमकियों से सम्पूर्ण संरक्षण है किसी फाईल के डाटा के प्रवाह को इस्कान स्केन करता है, जिससे उन छिपे मालवेयर को मालूम किया जा सके, जिनमें झिप्ड व आर्चिव्ड सहित सब प्रकार की फाईल्स हैं कमांड लाईन स्केनर के साथ स्केनिंग के अनुसूचित विकल्प इस समय आपके सिस्टम पर अनुसूचित स्वमेव स्केन हेतु मदद देते हैं स्केनिंग गतिविधि के व्यापक लॉग को इस्कान आगे के विश्लेषण के लिए स्केनिंग के दिनांक व समय के साथ तथा मार्ग व स्केन की गई वस्तुओं के नाम के साथ उत्पन्न करता है
http://www.escanav.com/english/content/products/escan_soho/escan_universal_security_suite.asp

एफसिक्योर ब्लेकलाईट

एफसिक्योर ब्लेकलाईट उपयोगकर्त्ता व मानक सुरक्षा साफ्टवेयर से तथाकथित छिपे हुए रूटकिट्स को आपके सिस्टम में से स्केन करता है यदि स्केन में कोई संदेहास्पद वास्तु पाई जाती है, तब आपके पास विकल्प होगा कि उसे हटा दें
http://www.spychecker.com/program/fsblacklight.html

कासपरस्की एंटीवायरस

कासपरस्की एंटीवायरस की विशिष्टताओं में शामिल हैं वास्तविकसमय संरक्षण, वायरसों की पड़ताल और उन्हें हटाना, ट्रोजन के वार्म्स, स्पायवेयर, एडवेयर, कीलागर्स के दुर्भावनापूर्ण साधन व स्वतः डायलर्स व साथ ही रूटकिट्स की पड़ताल और उन्हें हटाना इसमें कासपरस्की सुरक्षा नेटवर्क सेवा के माध्यम से तात्कालिक स्वतःअपडेट्स भी शामिल हैं
http://en.wikipedia.org/wiki/Kaspersky_Anti-Virus

मेक्फी वायरस स्केन प्लस

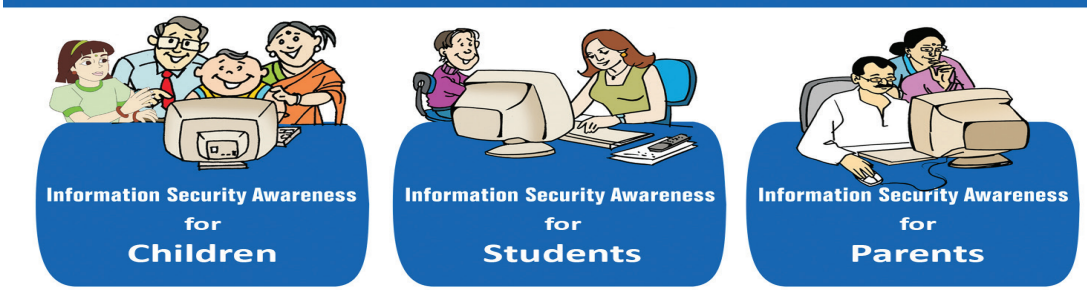
- वायरस संरक्षण आपके संपूर्ण पीसी की चौकसी करता है
- स्पायवेयर संरक्षण संभवित अवांछित प्रोग्राम्स को अवरुद्ध कर देता है
- हैकर्स को बाहर रखने में फायरवाल मददगार रहता है

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

सिमांटेक एंडपाइंट संरक्षण

सिमांटेक कार्पोरेशन के द्वारा सिमांटेक एंडपाईंट प्रोटेक्शन तैयार किया गया है और यह एंटीवायरस व व्यक्तिगत फायरवाल उत्पाद है, जिसे सर्वर्स व कार्यस्थलों की केन्द्रीकृत प्रबंधन कार्पोरेट वातावरण सुरक्षा के लिए लगाया जाता है

http://en.wikipedia.org/wiki/Symantec_Endpoint_Protection



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**

सुरक्षा मूल्यांकन साधन

माइक्रोसाफ्ट सुरक्षा मूल्यांकन साधन (विंडोज)

माइक्रोसाफ्ट सुरक्षा मूल्यांकन साधन एमएसएटी एक जोखिम मूल्यांकन का एप्लीकेशन है, जो इस तरह डिजाईन किया गया है कि वह सूचना प्रौद्योगिकी आईटी इंफ्रास्ट्रक्चर के अंतर्गत सुरक्षा हेतु श्रेष्ठ व्यवहार के बारे में जानकारियाँ व अनुशंसाएँ दें

http://www.microsoft.com/downloads/details.aspx?FamilyID=6d79df9c-c6d1-4e8f-8000-0be72b430212&displaylang=en

नेसस (, लायनक्स, विंडोज)

सक्रिय स्केनर्स में नेसस कोमलता स्केनर विश्व में अग्रणी हैं, जिसमें आपकी सुरक्षा स्थिति के लिए तेज गति की खोज, कंफिगुरेशन ऑडिटिंग, असेट प्रोफाईलिंग, संवेदी डाटा खोज व कोमलता विश्लेषण की विशेषताएँ हैं नेसस स्केनर्स को किसी उद्यम में संपूर्ण रूप से, डीएमझेडएस में व भौतिक रूप से पृथक नेटवर्क्स में वितरित किया जा सकता है

http://www.nessus.org/download/

रेटिना (विंडोज)

रेटिना नेटवर्क सुरक्षा स्केनर, बहुमंच कोमलता प्रबंधन के लिए उद्योग व शासकीय मानक, ज्ञात व शून्य दिन की कोमलताओं का पता लगाते हैं और सुरक्षा जोखिम मूल्यांकन उपलब्ध कराते हैं व सुरक्षा के श्रेष्ठ व्यवहार, नीति प्रवर्तन व नियमन ऑडिटस उसे हेतु समर्थ बनाते हैं

http://www.eeye.com/html/products/retina/download/index.html

आईबीएम आंतरिक स्केनर

आपके नेटवर्क पर जिनमें डेस्कटॉप, सर्वर्स, राउटर्स/ स्विचेस, फायरवाल्स, सुरक्षा साधन व एप्लीकेशन राउटर्स भी शामिल हैं, उनके १,३०० से अधिक नेटवर्क साधनों का आईबीएम आंतरिक स्केनर पता लगा सकता है एक बार जैसे ही आपके समस्त नेटवर्क साधनों का पता लगा कि कंफिगुरेशन, पेच लेवल्स, खुलने के सिस्टम का व संस्थापित एप्लीकेशंस का आंतरिक स्केनर विश्लेषण करता है, जिससे उन नाजुक मुद्दों को मालूम किया जा सके, जिनका फायदा उठाते हुए हैकर्स अनाधिकृत पहुँच प्राप्त करने की कोशिश कर सकते हैं

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

पैच लिंक कोमलता मूल्यांकन साधन

संचालन प्रणाली व एप्लीकेशन की कोमलताओं के लिए आगे से सक्रिय होकर समय पर दूर कर यह कार्पोरेट की जोखिम को कम करता है

- आईटी के खर्च को कम करता है और उच्च स्वचालन व सबस्क्रिप्शन आधारित पेच प्रबंधन समाधान के द्वारा यह उत्पादकता में सुधार लाता है
- पेच विचलन के द्वारा पुनः घटित होने वाली जोखिम को दूर करता है
- सतत पेच निगरानी व व्यापक रिपोर्टिंग के द्वारा यह सुरक्षा नीतियों व शासकीय विनियमों के साथ अनुपालन प्रदर्शित करता है

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

क्वालिस गार्ड (लायनक्स व विंडोज)

मुफ्त स्केन के द्वारा आप शीघ्र व यथार्थता के साथ आपके सर्वर की उन हजारों कोमलताओं को स्केन कर सकते हैं, जिनका हमलावर फायदा उठा सकते हैं यदि दिए गए आईपी पते पर कोमलताएँ मौजूद हैं, तब प्रत्येक जोखिम पर मुफ्त स्केन उनका पता लगाएगा और उनके के बारे में विस्तृत जानकारी देगा, जिसमें उनकी गंभीरता, संबंधित भय व संभवित प्रभाव भी शामिल होंगे यह वे लिंक्स भी प्रदान करता है, जिससे आप कोमलताओं के बारे में और अधिक जानकारी प्राप्त कर सकें व यह भी कि उन्हें फिर कैसे सुधारें

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

जीएफआई एलएएन गार्ड (विंडोज)

जीएफआई एलएएन गार्ड नेटवर्क सुरक्षा स्केनर एन.एस.एस. एक पुरुस्कृत साधन है, जिसके द्वारा आप आपके नेटवर्क पर किसी भी सुरक्षा से संबंधित कमजोरी को स्केन कर उसके बारे में मालूम कर सकते हैं व उसका मूल्यांकन कर उसे दुरुस्त कर सकते हैं एक प्रशासक के रूप में बहु उत्पाद का इस्तेमाल करते हुए आपको समस्याओं से संबंधित कोमलताओं के मुद्दों, पेच प्रबंधन व नेटवर्क ऑडिटिंग पर आपको पृथकता से निबटना पड़ता है यद्यपि जीएफआई एलएएन गार्ड एन.एस.एस. के साथ कोमलता प्रबंधन के इन तीन स्तंभों को एक ही पैकेज में संबोधित किया गया है विस्तृत रिपोर्टिंग कार्य के साथ एक ही आश्वासन का उपयोग करते हुए, जीएफआई एलएएन गार्ड एन.एस.एस. का एकीकृत समाधान आपको इन समस्याओं को तेज व प्रभावी ढंग से निबटाने में मददगार रहता है

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

सार प्रभाव (विंडोज)

सार सुरक्षा तकनीकों के द्वारा सार प्रभाव, एक वाणिज्यिक भेदन परीक्षण एप्लीकेशन है, जिसके द्वारा उपयोगकर्त्ता कंप्यूटर नेटवर्क में सुरक्षा कोमलताओं को मालूम कर सकता है और उनका दोहन कर सकता है यह अंतरफलक इस प्रकार डिजाईन किया गया है कि व्यक्ति को कंप्यूटर सुरक्षा के संबंध में बिना किसी विशिष्ट परीक्षण के वह उसके लिए उपयोगी रहता है और उसमें प्राप्त की गई जानकारियों से रिपोर्ट तैयार करने का काम भी उसमें शामिल रहता है इसका ६०० से अधिक कंपनियों व सरकारी सत्ताओं द्वारा उपयोग किया गया है

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

आईएसएस इंटरनेट स्केनर (विंडोज)

खरीदने की न्यूनतम मात्रा १० आईपीएस है ज्ञात कोमलताओं के आईएसएस के डाटाबेस का इस्तेमाल करते हुए, नेटवर्क पर एक कंप्यूटर, स्केन्स कंप्यूटर्स व राउटर्स पर संचालन प्रणाली, मुख्य एप्लीकेशंस व कन्फ्यूगिरेशन में सुरक्षा कोमलताओं के मद्देनजर

आईएसएस इंटरनेट स्केनर संस्थापित किया गया है स्थायी लायसेंस में वार्षिक सहयोग व रखरखाव की जरूरत रहती है इस संस्करण में ५०० आईपीएस तक के लायसंस के लिए स्थल संरक्षक प्रबंधन शामिल है
https://www.securehq.com/group.wml&storeid=1&deptid=75&groupid=928&ds=wpshop_store&SessionID=20091285321932563

निक्टो (लायनक्स)

अधिक व्यापक वेब स्केनर निक्टो एक खुला स्त्रोत वेब सर्वर स्केनर (जीपीएल) है, जो कई वस्तुओं के लिए वेब सर्वर्स के समक्ष व्यापक परीक्षण निष्पादित करता है, जिनमें ३२०० से अधिक संभवित खतरनाक फाईल्स/ सीजीआईएस, ६२५ से अधिक सर्वर्स पर संस्करण तथा २३० सर्वर्स से अधिक की संस्करण से संबंधित विशिष्ट समस्याएँ सम्मिलित हैं स्केन की वस्तुओं व प्लगइन्स को बारंबार अद्यतन किया जाता है और उसे स्वतः अद्यतन भी किया जा सकता है (यदि इच्छुक हों) यह एक बड़ा साधन है, लेकिन उसका मूल्य विरल अद्यतन के कारण सीमित है नवीनतम व सर्वाधिक नाजुक कोमलताएँ अक्सर पता नहीं लगती हैं
http://linux.softpedia.com/get/System/Networking/Nikto-10271.shtml

एक्स स्केन (विंडोज)

एक्स स्केन एक बुनियादी नेटवर्क कोमलता का स्केनर है, जिसमें मल्टी थ्रेडिंग स्केन पहुँच को उपयोग में लिया जाता है स्केनर का उपयोग दोनों में किया जा सकता है, कमांड लाईन पर व उसमें आसानी से उपयोग में आनेवाला जीयूआई अग्रिमअंत है निम्न वस्तुएँ स्केन की जा सकती हैं

- दूरस्थ ओएस प्रकार एवं संस्करण का पता लगाना
- मानक पोर्ट स्थिति एवं बैनर जानकारी
- एसएनएमपी जानकारियाँ
- सीजीआई कोमलता का पता लगाना
- आईआईएस कोमलता का पता लगाना
- आरपीसी कोमलता का पता लगाना
- एसएसएल कोमलता का पता लगाना
- एसक्यूएल सर्वर
- एफटीपी सर्वर
- एसएमटीपी सर्वर
- पीओपी ३ सर्वर
- प्राधिकरण माड्यूल की एनटी सर्वर कमजोर उपयोगकर्त्ता / पासवर्ड जोड़ बनाता है
- एनटी सर्वर एनईटीबीआईओएस जानकारियाँ
- दूरस्थ रजिस्टर जानकारियाँ आदि

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

सारा (लायनक्स, विंडोज, खुला स्त्रोत)

फिंगर, एनएफएस, एनआईएस, एफटीपी व टीएफटीपी, आरईएक्सडी व अन्य सेवाओं जैसी नेटवर्क सेवाओं की जाँच कर यह दूरस्थ मेजबान व नेटवर्क के बारे में इसके सबसे सरल मोड में यह जितनी अधिक संभव हो सके, उतनी जानकारियाँ एकत्र करता है एकत्र की गई जानकारियों में विभिन्न नेटवर्क सूचना सेवाओं की मौजूदगी व साथ ही संभवित सुरक्षा कमियाँ भी शामिल रहती है जो सामान्यतः गलत सेटअप या कंफिगुअर्ड नेटवर्क सेवाओं, सिस्टम के ठीक तरह से ज्ञात दोषों या नेटवर्क उपयोग या खराब या

अनभिज्ञ नीतिगत निर्णयों के रूप में होती हैं

किसी भी संभवित सुरक्षा समस्याओं की जाँच के लिए, यह या तो इस डाटा पर रिपोर्ट करती है या सामान्य नियम आधारित सिस्टम का उपयोग करती है तब उपयोगकर्त्ता मोजेक या नेटस्केप जैसे एचटीएमएल ब्राउजर के साथ परिणाम के बारे में जाँच कर सकते हैं और संदेह व्यक्त कर विश्लेषण कर सकते हैं जबकि प्रोग्राम को प्राथमिक रूप से परिणाम के सुरक्षात्मक प्रभावों के विश्लेषण की ओर डाल दिया जाता है तब साधन नेटवर्क टोपोलोजी, चल रही नेटवर्क सेवाओं, नेटवर्क पर उपयोग में लिए जानेवाले हार्डवेयर व साफ्टवेयर के प्रकार आदि, का उपयोग कर सामान्य नेटवर्क जानकारियों के बड़े काम को हासिल क्र सकते हैं

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

एसएआईएनटी (लायनक्स एवं खुला स्त्रोत)

एसएआईएनटी या सुरक्षा प्रशासक का एकीकृत नेटवर्क साधन, कमजोरी के क्षेत्रों को उजागर करता है और दुरूस्ती के बारे में अनुशंसाएँ करता है एसएआईएनटी कोमलता मूल्यांकन साधन के द्वारा आप कर सकते हैं

- अतिक्रमण वालों के द्वारा उनका दोहन हो, उसके पहले आपके नेटवर्क की सुरक्षा की संभवित कमजोरियों को मालूम कर उन्हें व्यवस्थित करें
- सिस्टम की सामान्य कोमलताओं की आशा कर उनकी रोकथाम करें
- सरकार के वर्तमान विनियमों जैसे कि एफआईएसएमए, एसओएक्स, जीएलबीए, एचआईपीएए व सीओपीपीए तथा पीसीआईडीएसएस जैसे उद्योग के विनियमों के अनुपालन को प्रदर्शित करें
- आपकी कोमलता के मूल्यांकन कार्यक्रम के लिए एसएआईएनटी स्केनिंग इंजन एक आदर्श नींव का पत्थर है ग्राफिकल उपयोगकर्त्ता इंटरफेस के लिए एसएआईएनटी रूपरेखा देते हैं जो अंतःप्रज्ञा है और उपयोग में आसान है

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

एमबीएसए (विंडोज

माइक्रोसॉफ्ट बेसलाईन सुरक्षा विश्लेषक एमबीएसए आसानी से उपयोग में आनेवाला साधन है, जो आईटी व्यवसायिकों के लिए डिजाईन किया गया है और जो लघु व मध्यम आकार के व्यवसायों के लिए मददगार रहता है और जिसके द्वारा माइक्रोसॉफ्ट सुरक्षा अनुशंसाओं के अनुसार उनकी सुरक्षा की स्थिति को मालूम किया जा सकता है और यह पुनः मनन का विशिष्ट मार्गदर्शन प्रस्तुत करता है विंडोज अपडेट एजेंट और माइक्रोसाफ्ट अपडेट इन्फ्रास्ट्रक्चर पर निर्मित एमबीएसए अन्य माइक्रोसाफ्ट प्रबंधन के उत्पादों, जिनमें सम्मिलित हैं माइक्रोसाफ्ट अपडेट एमयू, विंडोज सर्वर अपडेट सेवाएँ डब्ल्यूएसयूएस, सिस्टम मेनेजमेंट सर्वर एसएमएस एवं माइक्रोसाफ्ट आपरेशंस मैनेजर एमओएम, के साथ सामंजस्य सुनिश्चित करता है स्पष्टतः एमबीएसए औसतन प्रति सप्ताह ३ मिलियन कंप्यूटर से अधिक स्केन करता ह

पेरोस प्राक्सी (लायनक्स, विंडोज, खुला स्त्रोत)

हमने एक प्रोग्राम लिखा, जिसे पेरोसकहा गया, उन लोगों के लिए जिन्हें उनके वेब एप्लीकेशंस की सुरक्षा के मूल्यांकन की जरूरत है यह मुफ्त है और पूर्णतः जावा में लिखी गई है पेरोस की प्राक्सी की प्रकृति के माध्यम से सर्वर व ग्राहक के बीच सभी एचटीटीपी व एचटीटीपीएस डाटा जिनमें कुकीज व फार्म क्षेत्र भी शामिल हैं उन्हें अवरोधित व संशोधित किया जा सकता है

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

वेब स्कारब (लायनक्स, विंडोज, खुला स्त्रोत)

एप्लीकेशंस के विश्लेषण के लिए वेब स्कारब वह फ्रेमवर्क है, जो एचटीटीपी व एचटीटीपीएस का इस्तेमाल कर संचार करता है यह जावा में लिखा गया है, इसलिए यह कई मंचों के लिए पोर्टेबल है वेब स्कारब के संचालन के कई तरीके हैं और कई प्लगइन्स के द्वारा इसका कार्यान्वयन हुआ है यह सर्वाधिक काम में आनेवाला उपयोग है और वेब स्कारब एक अवरोधक प्राक्सी के रूप में

संचालन करता है, जिससे सर्वर को भेजे जाने के पहले ब्राउसर के द्वारा तैयार अनुरोधों की वह समीक्षा कर सकता है व संशोधित कर सकता है और जिससे वह ब्राउसर को प्राप्त हो, उसके पहले प्रतिक्रियाओं की वह समीक्षा कर सकता है व संशोधित कर सकता है
http://www.net-security.org/software.php?id=504

वेब निरीक्षण (विंडोज)

वेब एप्लीकेशन पर्त के अंदर की ज्ञात व अज्ञात कोमलताओं को पहचानकर, वेब निरीक्षण एप्लीकेशन सुरक्षा मूल्यांकन साधन आपके संगठन की वेब सुरक्षा तथा आपकी सर्वधिक नाजुक जानकारियों की सुरक्षा सुनिश्चित करता है उस जाँच को शामिल कर वेब सर्वर सुरक्षा को सुनिश्चित करने में भी वेब निरीक्षण आपके लिए मददगार रहता हैं, जो मान्य करता है कि वेब सर्वर का ठीक से कंफिगुरेशन हुआ है वेब निरीक्षण के द्वारा ऑडिटर्स, अनुपालन अधिकारीगण व सुरक्षा विशेषज्ञ, वेब एप्लीकेशंस व वेब सेवाओं के लिए सुरक्षा मूल्यांकन निष्पादित कर सकते हैं
https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-201-200%5e9570_4000_100__

व्हिस्कर/ लिबव्हिस्कर (लायनक्स, विंडोज, खुला स्त्रोत)

लिबव्हिस्कर एक पर्ल माड्यूल है, जिसे एचटीपीपी निरीक्षण के लिए जोड़ा गया है कई ज्ञात सुरक्षा छिद्रों विशेष कर खतरनाक सीजीआईएस की मौजूदगी के लिए यह एचटीपीपी सर्वर्स के परीक्षण के लिए कई कार्य उपलब्ध कराता है व्हिस्कर एक स्केनर है, जिसने लिबव्हिस्कर का उपयोग किया है, लेकिन अब यह निक्टो के पक्ष में रूक गया है और वह भी लिबव्हिस्कर का उपयोग करता है
http://www.wiretrip.net/rfp/

बर्प सूट (लायनक्स, विंडोज, खुला स्त्रोत)

वेब एप्लीकेशंस पर हमला करने के लिए बर्प सूट एक एकीकृत मंच है इसमें समग्र बर्प साधन है, जिसमें उनके बीच बहुत से अंतरफलक हैं, जो इस प्रकार डिजाईन किए गए हैं, जिसके द्वारा किसी एप्लीकेशन पर हमला करने की प्रक्रिया को सुविधा व गति मिलती है एचटीपीपी अनुरोधों, प्राधिकरण, ऊपर से नीचे की प्राक्सीस, लॉगिंग, सावधानी व व्यापकता के व्यवहार के लिए सभी साधन उसी सशक्त फ्रेमवर्क को साझा करते हैं वेब एप्लीकेशंस की गणना, विश्लेषण, हमला व उनके दोहन के लिए बर्प सूट के द्वारा आप शारीरिक व स्वचालित तकनीकों को संयुक्त कर सकते हैं विभिन्न बर्प साधन प्रभावी तरीके से साथ काम करते हैं, जिससे वे जानकारियाँ साझा कर सकें और एक ही साधन से जो प्राप्तियाँ मालूम की गई हों, उन्हें दूसरे का इस्तेमाल कर हमले का आधार बनाया जा सके
http://portswigger.net/suite/download.html

विक्टो (विंडोज, खुला स्त्रोत)

विक्टो वह साधन है, जो वेब सर्वर्स की कमियों की जाँच करता है यह अधिकांश रूप से वे ही कार्य संपन्न करता है, जो निक्टो के द्वारा किए जाते हैं लेकिन उसमें कार्यों के विभिन्न दिलचस्प अंश जैसे कि बेकएंड माईनर व क्लोज गूगल एकीकरण जुड़ते जाते हैं विक्ट ो को षझ .शड्ीहपैहिसीहा के लिए लिखा गया है और बायनरी एवं/ या स्त्रोत कोड को डाउनलोड करने के लिए पंजीकरण चाहिए
http://www.sensepost.com/research/wikto/

एक्यूनेटीक्स वेब कोमलता स्केनर (विंडोज)

एक्यूनेटीक्स डब्ल्यूवीएस के द्वारा स्केन की गई १०,००० वेबसाईट्स में से, ४२ क्रास साईट स्क्रिप्टिंग हेतु कोमल पाई गईं एक्सएसएस बहुत ही खतरनाक है और हमलों की संख्या बढ़ रही है संघटनों के संवेदनशील डाटा चुराने के लिए हेकर्स इन कोमलताओं से जोड़तोड़ करते हैं क्या आप अगले को वहन करने में समर्थ हैं? क्रास साईट स्क्रिप्टिंग के द्वारा हमलावर दुर्भावनापूर्ण जावास्क्रिप्ट,

वीबी स्क्रिप्ट, एक्टिव एक्स, एचटीएमएल को अंतः स्थापित करता है या उपयोगकर्त्ता को मूर्ख बनाने के लिए उसकी मशीन पर स्क्रिप्ट को निष्पादित करने के लिए कोमल गतिशील पृष्ठ को फ्लेश करता है, जिससे डाटा एकत्रित किए जा सकें इस प्रकार दोहन की गई क्रास साईट स्क्रिप्टिंग का सामान्यतः उपयोग निम्न दुर्भावनापूर्ण परिणामों तक पहुँचने के लिए किया जाता है

- चोरी का पता लगाना
- संवेदनात्मक व प्रतिबंधित जानकारियों तक पहुँचना
- विषयसामग्री तक मुफ्त पहुँच हासिल करना, अन्यथा उसके लिए भुगतान करना पड़ता
- उपयोगकर्त्ता की वेब ब्राउसिंग आदतों के बारे में जासूसी करना
- ब्राउसर के कार्यों के बारे में चौकसी
- किसी व्यक्ति या निगम की सार्वजानिक मानहानि
- वेब एप्लीकेशन की छवि को खराब करना
- सेवा हमलों से इंकार

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

वाचफायर एपस्केन (विंडोज)

वेब एप्लीकेशन सुरक्षा ऑडिटस को वाचफायर एपस्केन स्वचालित करने में मदद करता है, जिससे वेबसाईट्स की सुरक्षा व उनका अनुपालन सुनिश्चित किया जा सके गार्टनर व आईडीसी के अनुसार बाजार में हिस्सेदारी में विश्वव्यापी अगुआ का नाम दें और हमारे एपस्केन उत्पाद सूट सभी प्रकार की सुरक्षा परीक्षण की जरूरतों के लिए समाधान प्रस्तुत करते हैंजो आउटसोर्सस्ड, व्यक्तिगत स्केन्स या जिनका उद्यम अनुसार विश्लेषण हों व सभी प्रकार के उपयोगकर्त्ताओं के लिए जो चाहें एप्लीकेशन डेवलपर्स, गुणवत्ता आश्वासन दल, वेधन परीक्षक, सुरक्षा ऑडिटर्स व वरिष्ठ प्रबंधन हो

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

एनस्टील्थ (विंडोज)

एनस्टील्थ एक व्यापक वेब सर्वर सुरक्षा ऑडिटिंग साधन है, जो ३०,००० से अधिक कोमलताओं को स्केन करता है यह सिस्टम प्रशासकों, सुरक्षा परामर्शदाता व आईटी व्यवसायिकों के लिए आदर्श है

http://www.nstalker.com/products/free/

मेटास्पलोयिट

मेटास्पलोयिट एक अद्भुत व सशक्त खुले स्त्रोत का फ्रेमवर्क है और यह आईपी पतों के सेट के समक्ष कठिन स्केन निष्पादित करता है अन्य कई फ्रेमवर्क के विपरीत, इसका उपयोग अन्य कई गैरन्यायिक उद्देश्य के लिए किया जा सकता है किसी विशेष कोमलता का दोहन करनेवाले टुकड़े को प्रोग्रामर्स विशेषज्ञ लिख सकते हैं और यह देखने के लिए कि क्या उसका पता लग गया है, उसका परीक्षण मेटास्पलोयिट के साथ कर सकते हैं इस प्रक्रिया को तकनीकी रूप से उल्टा भी किया जा सकता है जब कोई अज्ञात कोमलता का उपयोग करते हुए कोई वायरस हमला करता है, तब इसके पेच के परीक्षण हेतु मेटास्पलोयिट का उपयोग किया जा सकता है

http://www.metasploit.com/

खुला वीएएस

नेसस स्केनर एक लोकप्रिय वाणिज्यिक उपयोग है, जिससे कुछ वर्ष पहले खुला वीएएस एक खुले स्त्रोत के रूप में फैला यद्यपि मेटास्पलोयिट व खुला वीएएस बहुत कुछ समान हैं, लेकिन फिर भी उनमें कुछ विशष्ट अंतर हैं खुला वीएएस दो प्रमुख घटकों में विभाजित हैं एक स्केनर व एक प्रबंधक कोई स्केनर किसी स्केन किए जानेवाले लक्ष्य पर रह सकता है और प्राप्त कोमलताओं को प्रबंधक प्रदान कर सकता है विविध स्केनर्स से प्रबंधक इनपुट्स एकत्रित करता है और रिपोर्ट तैयार करने के लिए स्वयं की बुद्धि का

उपयोग करता है सुरक्षा की दुनिया में सुरक्षा के नवीनतम बचावों की पड़ताल के लिए, रिपोर्ट्स उपलब्ध कराने के लिए व इनपुट स को व्यवस्थित करने के लिए, खुला वीएएस को बहुत स्थायी व विश्वसनीय माना जाता है अंदरनिर्मित ग्रीनबॉन सुरक्षा सहायक, सभी कोमलताओं व नेटवर्क की प्रभावित मशीनों को सूचीबद्ध करने के लिए जीयूआई डेशबोर्ड उपलब्ध कराता है विस्तृत रिपोर्ट तैयार करना, वह चीज है, जिसके द्वारा खुला वीएएस वह साधन बन जाता है, जिससे वह इन्फ्रास्ट्रक्चर सुरक्षा प्रबंधकों का पसंदीदा हो जाता है

http://www.openvas.org/

समुराई फ्रेमवर्क

जब निक्टो के द्वारा एक बार बेसलाईन की जाँच निष्पादित हो जाती है, तब उसका दूसरा चरण होता है गहनगोताअभिगम को अपनाना समुराई एक फ्रेमवर्क है शक्तिशाली उपयोगों का एक समूह, जिसमें प्रत्येक के लिए कोमलताओं के विशिष्ट सेट का लक्ष्य होता है

http://samurai.inguardians.com/

सुरक्षित ३ स्केनर

जबकि पहले दो साधन स्थायी वेबसाईट्स के लिए अच्छे होते हैं, पोर्टल्स के लिए, जिसमें उपयोगकर्त्ता आईडी व पासवर्ड की जरूरत रहती है, तब हमें ऐसा कुछ चाहिए जो एचटीपीपी सत्रों व कुकीज से निपट सके सुरक्षित ३ स्केनर एक अद्भुत खुली स्त्रोत परियोजना है, जिसने संवेग व प्रसिद्धि प्राप्त की है, क्योंकि यह सभी प्रकार के प्राधिकरण से व्यवहार कर सकता है, जिसमें एनटीएलएम भी शामिल हैं इसमें एक रेंगनेवाला वेब (एक मकड़ी की तरह का सर्च इंजन) होता है, जो डुप्लीकेट पृष्ठ की स्केनिंग को उपेक्षित करने में सक्षम है, लेकिन फिर भी ग्राहक की ओर से जावास्क्रिप्ट कोमलताओं का पता लगा सकता है अद्यतन एजेएएक्स आधारित हमलों की संभावनाओं का पता भी लगा लेता है और वह कोमल स्क्रिप्ट ग्रंथालयों की रिपोर्ट भी करता है जीयूआई जो उपयोगकर्त्ता के लिए मित्रवत है, यह वहाँ से है और उत्तम प्रबंधन रिपोर्ट तैयार करने में दक्ष है

http://opensourceforu.com

वेबसिक्योरिटी

यद्यपि वेबसिक्योरिटी समुराई के बहुत समान है और यह एप्लीकेशन स्तर का मूल्यांकन खेल में लाता है बड़े वेब फ़ार्म के मामले में, जहाँ कोड को डेवलपर्स के दल द्वारा बनाए रखा जाता है, तब निम्न मानक कोड, कभी असुरक्षित कोड में लब्धि दे सकते हैं, जैसे कि पासवर्ड, ग्रंथालयों आदि के भौतिक फाईल मार्ग आदि में जिन कोड का उल्लेख है वेबसिक्योरिटी कोड के आरपार जा सकती हैं और इस प्रकार की कमियों का जल्दी से पता लगा लेती है इसका अच्छा कार्य है, जिसके द्वारा आप स्वचालित रूप से समस्या के क्षेत्र के स्क्रीनशाट्स तैयार कर सकते हैं, जिससे ऑडिट रिपोर्ट की तैयारी में मदद मिलती है मंच से स्वतंत्र कुछ साधनों में से यह एक है और मोबाईल कोडिंग के लिए इसमें सहयोग है, जिससे सायबर सुरक्षा मूल्यांकन की दुनिया में अधिक लोकप्रियता हेतु इसमें मदद मिलती है

http://opensourceforu.com

एसक्यू लैम्प

एसक्यू लैम्प मात्र एसक्यूएलइंजेक्शन की गल्तियों का दोहन करने में ही दक्ष नहीं है, बल्कि यह डाटाबेस सर्वर को भी नियंत्रण में ले लेता है चूँकि यह विशिष्ट कार्य पर ही केन्द्रित रहता है, इसलिए यह अंगुली के निशान के डाटाबेस के लिए तेज गति से काम करता है और अंतर्निहित फाईल सिस्टम और ओएस का पता लगाता है और अंत में सर्वर से आँकड़े अपने पास ले लेता है यह लगभग सभी ठीक तरह से ज्ञात डाटाबेस इंजिन्स को सहयोग करता है और पासवर्डअनुमान के हमलों को निष्पादित करता है वेबसाईट् को आक्रामक ढंग से स्केन करने के लिए, उपरोक्त बताए गए चार साधनों को इस साधन से संयुक्त कर सकते हैं कोमलता मूल्यांकन

साधन में नेटवर्क स्केनिंग व साथ ही वेबसाईट कोमलता दोहन भी शामिल होना चाहिए एक बार जब खुला स्त्रोत साफ्टवेयर हमले के लिए उन्मुख होता है, तब नेटवर्क प्रशासकों को प्रतिष्ठित स्केनर्स के बारे में मालूम होना चाहिए और रोज के कामकाज में उनका इस्तेमाल करना चाहिए, जिससे उनका इंफ्रास्ट्रक्चर सुरक्षित व स्थायी रहे

http://sqlmap.org

आईपीलॉक्स

डाटाबेस से संबंधित कमजोरियों का पता लगाने व उनकी मरम्मत करने हेतु आईपीलॉक्स कवच उद्योग में सबसे सशक्त समाधान उपलब्ध करता है आईपीलॉक्स की मापनीयता, अनुकूलता व प्रभावी लागत के संबंध में अन्य कोई बिक्रीकर्त्ता, इस संयोजन के मेल का नहीं हो सकता है नाजुक पहल में सहयोग हेतु दुनिया की सब ओर की कंपनियाँ आईपीलॉक्स कवच का उपयोग करती हैं, जैसे कि

- उपयोगकर्त्ता विशेषाधिकार रिपोर्टिंग
- आंतरिक सुरक्षा
- एसओएक्स अनुपालन
- पीसीआई अनुपालन
- जोखिम प्रबंधन

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

एप डिटेक्टिव

नेटवर्क आधारित कोमलता मूल्यांकन स्केनर एप डिटेक्टिव प्रो आपके इंफ्रास्ट्रक्चर में ही डाटाबेस एप्लीकेशंस को खोजता है और उनकी सुरक्षा शक्ति का मूल्यांकन करता है टुकड़ोंटुकड़ों में समाधानों के विपरीत एप डिटेक्टिव प्रो माड्यूल से एकल इंटरफेस के द्वारा उद्यमों की दो प्राथमिक एप्लीकेशन कतारों एप्लीकेशन/ मिडिलवेयर एवं बेकएंड डाटाबेस का मूल्यांकन होता है सिद्ध सुरक्षा कार्यप्रणाली व एप्लीकेशन स्तर की कोमलताओं के विस्तृत ज्ञान के सहयोग से एप डिटेक्टिव प्रो सुरक्षा छिद्रों व मिसकन्फ्यूगरेशन का पता लगाता है, जाँच करता है, रिपोर्ट करता है और उन्हें व्यवस्थित करता है इसके फलस्वरूप उद्यम उनके डाटाबेस एप्लीकेशन्स को आगे से सक्रिय होकर सख्त बना सकता है, जबकि उसी समय नियमित ऑडिटस में सुधार लाकर उसे आसान बनाता है

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

वॉच फायर

वेब एप्लीकेशन सुरक्षा ऑडिटस को वाचफायर एपस्केन स्वचालित करने में मदद करता है, जिससे वेबसाईट्स की सुरक्षा व उनका अनुपालन सुनिश्चित किया जा सके गार्टनर व आईडीसी के अनुसार बाजार में हिस्सेदारी में विश्वव्यापी अगुआ का नाम दें और हमारे एपस्केन उत्पाद सूट सभी प्रकार की सुरक्षा परीक्षण की जरूरतों के लिए समाधान प्रस्तुत करते हैंजो आउटसोर्सस्ड, व्यक्तिगत स्केन्स या उद्यम अनुसार विश्लेषण होते हैं व सभी प्रकार के उपयोगकर्त्ताओं के लिए जो चाहें एप्लीकेशन डेवलपर्स, गुणवत्ता आश्वासन दल, वेधन परीक्षक, सुरक्षा ऑडिटर्स व वरिष्ठ प्रबंधन हों

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

एनस्टाल्कर

एनस्टाल्कर वेब एप्लीकेशन सुरक्षा स्केनर २००६, एक वेब सुरक्षा मूल्यांकन समाधान है, जो एनस्टाल्कर द्वारा तैयार किया गया है प्रसिद्ध एनस्टील्थ एचटीपीपी सुरक्षा स्केनर व उसके ३५,००० वेब हमला हस्ताक्षर डाटाबेस को, पेटेंटलंबित घटक उन्मुख वेब एप्लीकेशन सुरक्षा मूल्यांकन तकनीक के साथ सम्मिलित करता है, एनस्टाल्कर सक्षम है कि इस वातावरण में जो सामान्य हैं उन विशाल संख्याँ की कोमलताओं वाले वेब एप्लीकेशन को हटा दे, जिनमें क्राससाईट स्क्रिप्टिंग व एसक्यूएल इंजेक्शन, बफर

ओवरफ्लो व पैरामीटर तोड़मरोड़ हमले व ऐसे ही और भी अधिक सम्मिलित हैं
http://www.nstalker.com/products/free/download-free-edition

स्पारजेक्स (एजेएएक्स के लिए)

स्पारजेक्स एक खुले स्त्रोत का काले बॉक्स का सुरक्षा स्केनर है, जिसका उपयोग एजेएएक्स से समर्थ एप्लीकेशन्स की सुरक्षा के मूल्यांकन के लिए किया जाता है उपयोग में आनेवाले विशिष्ट एजेएएक्स फ्रेमवर्क्स को मालूम कर स्पारजेक्स इस योग्य हो जाता है कि परीक्षण के अनुरोधों को वह बेहतर ढंग से फार्मुलेट कर सके और संभवित कोमलताओं की पहचान कर सके
http://www.owasp.org/index.php/Category:OWASP_Sprajax_Project

पिक्सी (पीएचपी के लिए)

पिक्सी एक खुले स्त्रोत का कोमलता का स्केनर है, जो पीएचपी एप्लीकेशंस में एसक्यूएल, एक्सएसएस समस्याओं की पहचान करता है
http://pixybox.seclab.tuwien.ac.at/pixy/download.php

प्रिवेक्स

फिर भी आपके कंप्यूटर पर फाईल्स साझा करने के लिए व कभी बिट टोरेंट जैसे पीरपी नेटवर्क के अंदर अन्य कंप्यूटर्स में आप फाईल्स पर पहुँच सके, उसके लिए पीरपी साफ्टवेयर पर संचार हेतु फायरवाल के द्वारा आपको विशिष्ट टीसीपी पोर्ट खोलना चाहिए आप जैसे ही एक बार पोर्ट खोलते हैं, तब उसमें से आनेवाले दुर्भावनापूर्ण यातायात से आप संरक्षित नहीं रह सकते हैं नौसिखिए उपयोगकर्त्ताओं को इसमें उसी प्रकार बहुत भ्रम हो सकता है, जैसे कि व्यक्तिगत फायरवाल साफ्टवेयर में झोन अलार्म का होता है, क्योंकि बड़े पैमाने पर क्रियाओं को मंजूर करने या उन पर रोक लगाने के फलस्वरूप या तो बड़ी संख्याँ में संदेहास्पद क्रियाएँ बिना नजर में आए मंजूर हो जाएँगी या सौम्य क्रियाएँ जैसे कि उपयोगकर्त्ता के स्वयं के साफ्टवेयर के संस्थापन की कोशिश पर रोक लग जाएगी, इसलिए उपयोगकर्त्ता से प्रिवेक्स पूछता है कि वह गतिविधि से किस प्रकार का व्यवहार करना चाहता है किसी भी समय कोई एप्लीकेशन कोशिश करता है कि वह सिस्टम की स्मृति या नाजुक फाईल्स पर पहुँचे या रजिस्ट्री में बदलाव करे, तब प्रिवेक्स होम साफ्टवेयर उस गतिविधि का पता लगाता है और उसे पूरी तरह अवरूद्ध कर देता है या उपयोगकर्त्ता से पूछता है कि आगे किस तरह बढ़ें प्रिवेक्स के अनुसार साफ्टवेयर बफर ओवरफ्लो व ओवररन्स की जाँच करेगा और नाजुक फाईल्स व डायरेक्टरीज में संशोधन को तथा सिस्टम रजिस्ट्री के नाजुक क्षेत्रों में बदलाव को और इसी प्रकार की क्रियाओं को रोकेगा समग्र सप्ताह के लिए मैंने मेरे एंट ीवायरस व फायरवाल साफ्टवेयर को मेरे परीक्षण के दौरान हटा दिया और फिर भी बिना किसी वायरस, अन्य कोई दुर्भावनापूर्ण कोड या स्पायवेयर के चलता रहा एडएडवेयर के साथ के स्केन में कुछ ट्रेकिंग कुकीज पाए गए, लेकिन उसमें दुर्भावनापूर्ण कुछ भी नहीं था
http://info.prevx.com/downloadprevx2.asp

हनी ट्रेप

नेटवर्क सेवाओं के समक्ष हमलों के अवलोकन के लिए हनी ट्रेप लिखा गया एक नेटवर्क सुरक्षा साधन है कम परस्पर सक्रियता के हनीपॉट के रूप में, नेटवर्क आधारित ज्ञात या अज्ञात हमलों से संबंधित जानकारियों को यह एकत्रित करता है और इस तरह पूर्वचेतावनी की जानकारियाँ उपलब्ध करा सकता है
http://honeytrap.mwcollect.org/download-Download%20Honeytrap

Connect us with

Facebook

https://www.facebook.com/infosecawarenesss

YouTube

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

Twitter

https://twitter.com/CDAC_ISEA

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

Toll Free No.
1800 425 6235

www.InfoSecAwareness.in

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

Supported by

Ministry of Electronics & Information Technology,
Government of India

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India

www.cdac.in

Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 500005, Telangana(India)
E-mail : isea@cdac.in