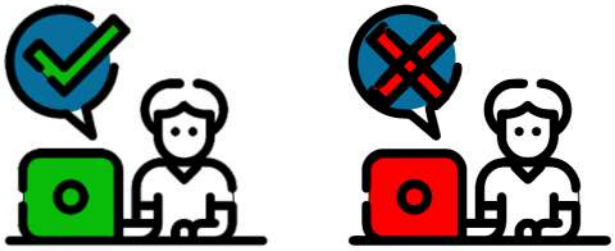
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

साइबर स्वच्छता

साइबर स्पेस के लिए

क्या करें और क्या ना करें



उन्नत (Advanced)

प्रकाशक :

भारतीय साइबर अपराध समन्वय केंद्र (I4C)

साइबर और सूचना सुरक्षा (CIS) प्रभाग

गृह मंत्रालय

भारत सरकार

नॉर्थ ब्लॉक

नई दिल्ली - 110001

परिचय

साइबर जगत, लोगों, सॉफ्टवेयर और सेवाओं के मध्य संवाद का एक जटिल और बहुआयामी वातावरण है, जिसमें सूचना और संचार प्रोद्योगिकी (ICT) उपकरणों और नेटवर्क्स की विश्वव्यापी उपलब्धता से मदद मिलती है। भारत में इंटरनेट उपभोक्ताओं की तेजी से बढ़ती संख्या व विकसित हो रही प्रौद्योगिकियों ने मिलकर अनूठी चुनौतियां पेश की हैं।

गृह मंत्रालय के साइबर एवं सूचना सुरक्षा (CIS) प्रभाग के तहत भारतीय साइबर अपराध समन्वय केंद्र (I4C) ने औद्योगिक निकायों/आम जनता/सरकारी अधिकारियों के लाभ के लिए साइबर स्वच्छता सर्वोत्तम कार्यप्रणाली (Cyber Hygiene Best Practices) का प्रचार -प्रसार करने के लिए यह मैनुअल (manual) तैयार किया है। इसे साइबर स्वच्छता के लिए सावधानियों की एक पूर्ण सूची नही माना जाना चाहिए, बल्कि ये बरती जाने वाली मूलभूत (baseline) सावधानियां हैं।

विषय-वस्तु

परिचय

सूचना प्रौद्योगिकी ने सामाजिक-आर्थिक परिदृश्य में महत्वपूर्ण योगदान दिया है और उस पर प्रभाव डाला है। डिजिटल तकनीक को तेजी से अपनाए जाने से रोजगार सृजन, जीवनयापन में सुविधा, व्यापार करने में आसानी और सूचना तक पहुंच संभव हुई है।

डिजिटल तकनीक और इंटरनेट अपनाए जाने से साइबर अपराध की घटनाएं भी बढ़ी हैं। सावधानी, एहतियात, जागरूकता और सूचना की सुरक्षा के लिए उपयुक्त उपकरणों का प्रयोग करके इसे नियंत्रित या कम किया जा सकता है। इस दस्तावेज़ में दी गई युक्तियां (tips) और अनुशंसाएं (recommendations) प्रयोक्ता को सूचना/डाटा और डिवाइस को सुरक्षित रखने में मदद कर सकती हैं।

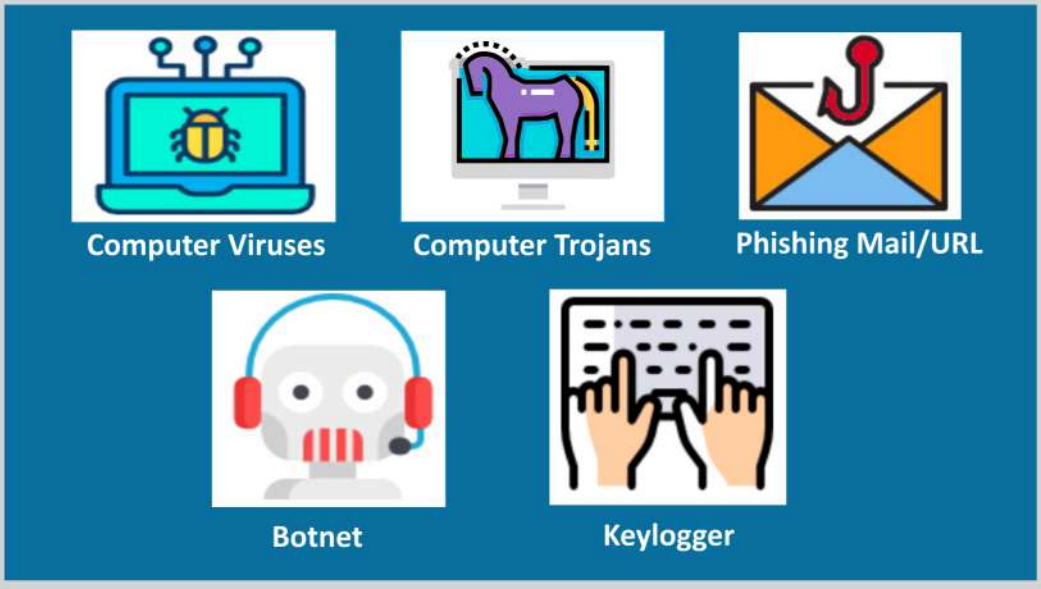
सामान्य कंप्यूटर उपयोग

कंप्यूटर सुरक्षा क्या है ?

कंप्यूटर सिस्टम की सुरक्षा, सूचना की चोरी और अनाधिकृत पहुंच से बचाव, कंप्यूटर सुरक्षा है। यह कंप्यूटर सिस्टम के अनाधिकृत प्रयोग की रोकथाम और उसका पता लगाने की प्रक्रिया है।

कंप्यूटर सुरक्षा को खतरा

कंप्यूटर सुरक्षा खतरे वे संभावित खतरे हैं जो कंप्यूटर के सामान्य कामकाज में बाधा उत्पन्न कर सकते हैं। कुछ सामान्य और हानिकारक कंप्यूटर खतरे नीचे दिए गए हैं: -



क्या करें

सामान्य कंप्यूटर उपयोग

- हमेशा विश्वसनीय (trusted) स्त्रोतों से एप्लिकेशन/ सॉफ्टवेयर डाउनलोड करें
- ऑपरेटिंग सिस्टम, एप्लिकेशन और एंटी-वायरस सॉफ्टवेयर को नियमित रूप से अपडेट रखें
- महत्वपूर्ण डेटा/फाइलों/दस्तावेजों का नियमित अंतराल पर बैकअप सुनिश्चित करें
- उपयोग में न होने पर कंप्यूटर स्क्रीन लॉक रखें
- कंप्यूटर फायरवॉल (firewall) को हमेशा “ON" रखें

क्या करें

सामान्य कंप्यूटर उपयोग

- सिस्टम पर कम सुविधा वाले खाते का उपयोग करें
- हमेशा जेन्युइन (genuine)/लाइसेंस (license) प्राप्त सॉफ्टवेयर एप्लिकेशन के प्रयोग को प्राथमिकता दें
- वेबसाइटों, ई-मेल या यूएसबी (USB) से डाउनलोड की गई सभी फाइलों/सामग्री को स्कैन करें
- अनावश्यक प्रोग्राम या सॉफ्टवेयर अनइंस्टॉल(uninstall) करें

क्या करें

सामान्य कंप्यूटर उपयोग

- कंप्यूटर सिस्टम पर चल रहे किसी भी अवांछित प्रोग्राम की पहचान करने के लिए "Task Manager" का प्रयोग करें
- Server तक पहुंच की अनुमति, मल्टी-फैक्टर ऑथेंटिकेशन (MFA) के माध्यम से होनी चाहिए
- प्रयोग में न होने पर रिमोट डेस्कटॉप कनेक्शन और नेटवर्क फ़ाइल शेयरिंग बंद कर दें
- नियमित अपडेट के लिए ऑपरेटिंग सिस्टम अपडेट सेटिंग्स को "Auto-Download" विकल्प पर सेट करें

क्या ना करें

सामान्य कंप्यूटर उपयोग

- कभी भी सॉफ़्टवेयर/एप्लिकेशन की पायरेटेड (pirated) कॉपी इंस्टाल न करें और न ही उनका इस्तेमाल करें। इनमें मैलवेयर (malware) हो सकता है
- "password@123", आदि जैसे अनुमान योग्य/कमजोर पासवर्ड का प्रयोग न करें
- अविश्वसनीय/अप्रत्याशित पॉप-अप (Pop-Up) विज्ञापनों/ program पर क्लिक न करें
- डेटा को निकाले और मिटाए बिना कंप्यूटर या हार्ड ड्राइव का निपटान (dispose) न करें

सामान्य इंटरनेट सुरक्षा सावधानियां

इंटरनेट के आविष्कार ने संचार और सूचना साझा करने के तरीके में क्रांति ला दी है। हालांकि, इंटरनेट का असुरक्षित इस्तेमाल किसी संगठन के लिए जोखिम पैदा कर सकता है। इंटरनेट सुरक्षा में ब्राउजर (browser) सुरक्षा, वेबसाइट (website) सुरक्षा, नेटवर्क (network) सुरक्षा, सॉफ्टवेयर एप्लिकेशन (software application) आदि शामिल हैं। इनका उद्देश्य, इंटरनेट पर हमलों के विरुद्ध, नियमों और उपायों को लागू करना है।

इंटरनेट के असुरक्षित इस्तेमाल से फ़िशिंग (phishing), ऑनलाइन वायरस (online virus), ट्रोजन (trojan), वर्म्स (worms), रैंसमवेयर (ransomware), व्यावसायिक ईमेल संबंधी क्षति (business e-mail compromise), वित्तीय नुकसान (financial loss) आदि जोखिम हो सकते हैं।

क्या करें

सामान्य इंटरनेट सुरक्षा सावधानियां

संदिग्ध लिंक/यूआरएल (URL) क्लिक/ डाउनलोड करते समय चौकस रहें

गोपनीय गतिविधियों/ लेनदेन के बाद ब्राउजर हिस्ट्री को समाप्त करने की आदत डालें

क्लाउड स्टोरेज का प्रयोग उपयुक्त सुरक्षा/गोपनीयता (privacy) सेटिंग्स के साथ करें

कोई भी सूचना साझा करने से पहले सोशल मीडिया प्रोफाइल की प्रामाणिकता और पहचान सत्यापित करें

उन सेवाओं का विवेकपूर्ण (judiciously) उपयोग करें, जिनके लिए लोकेशन की जानकारी की आवश्यकता होती है। इसके अलावा, GPS coordinates वाली फोटो पोस्ट करने से बचें

क्या करें

सामान्य इंटरनेट सुरक्षा सावधानियां

हमेशा सतर्क रहें और खोज परिणाम या वेबसाइट पर प्राप्त विज्ञापनों/ प्रायोजित सामग्री की प्रामाणिकता की जांच करें

समुचित सुरक्षा सेटिंग्स के अंतर्गत, फाइल शेयरिंग का प्रयोग करें

संगठन में मजबूत या सुरक्षित इंटरनेट/ वायरलेस प्रोटोकॉल का इस्तेमाल करें

क्या ना करें

सामान्य इंटरनेट सुरक्षा सावधानियां

ऑनलाइन शॉपिंग, इंटरनेट बैंकिंग, यूपीआई (UPI), आदि, जैसे वित्तीय लेनदेन के लिए किसी भी सार्वजनिक कंप्यूटर या वाई-फाई (Wi-Fi) का प्रयोग न करें

अविश्वसनीय और असुरक्षित वेबसाइट पर ई-मेल पता, फोन नंबर, भुगतान कार्ड, इत्यादि का विवरण न दें

सोशल मीडिया और मैसेजिंग ऐप्स पर असत्यापित सामग्री पर भरोसा न करें और उसे साझा न करें।

साझा करने से पहले हमेशा स्रोत और सामग्री की प्रामाणिकता (authenticity) जांच लें

यूएसबी (USB) डिवाइस सुरक्षा

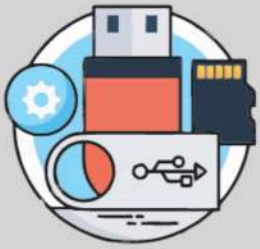
विभिन्न कंप्यूटरों के बीच डेटा का अंतरण करने के लिए यूएसबी (USB) डिवाइस बहुत सुविधाजनक होता है। कोई भी इसे यूएसबी पोर्ट में लगा सकता है, महत्वपूर्ण डेटा ट्रांसफर कर सकता है, हटा सकता है और उसका यथेच्छित प्रयोग कर सकता है। हालांकि, यह पोर्टेबल (portable), सुविधाजनक और लोकप्रिय है, लेकिन सूचना के संबंध में अनेक खतरे पैदा भी हो सकते हैं।

खतरा

यूएसबी ड्राइव के असुरक्षित प्रयोग से डेटा, डेटा लीकेज और मैलवेयर (malware) संक्रमण हो सकता है। सूचना को सुरक्षित करने वाले उपयुक्त स्कैनिंग टूल का सावधानी और समझदारी से प्रयोग करके, यूएसबी (USB) सुरक्षा सुनिश्चित की जा सकती है।

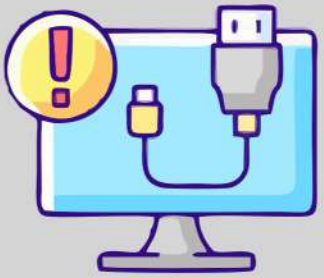
यूएसबी को सपोर्ट करने वाली डिवाइसों का प्रयोग

- फ्लैश ड्राइव/पेन ड्राइव
- पोर्टेबल हार्ड ड्राइव/एसएसडी (SSD)
- मोबाइल फोन



- डिजिटल कैमरा
- कार्ड रीडर
- यूएसबी कीबोर्ड/माउस (mouse)

क्या करें



यूएसबी (USB) डिवाइस सुरक्षा

प्रयोग से पहले यूएसबी डिवाइस को एंटीवायरस (Antivirus)/एंडपॉइंट सुरक्षा (End Point Protection) के द्वारा स्कैन करें

सभी मीडिया को एक सुरक्षित और संरक्षित वातावरण में स्टोर किया जाना चाहिए

यूएसबी (USB) स्टोरेज डिवाइस का रिकॉर्ड/इन्वेंट्री (inventory) रखें

आधिकारिक कार्य के लिए केवल आधिकारिक यूएसबी (USB) स्टोरेज डिवाइस का इस्तेमाल करें।
यह सुनिश्चित करें कि यूएसबी (USB) ड्राइव एन्क्रिप्टेड (encrypted) और पासवर्ड (password) सुरक्षित हो

यूएसबी का प्रयोग करते समय सभी कंप्यूटरों में ऑटोरन (autorun)/ऑटोप्ले (autoplay) फीचर अक्षम (disable) कर दें।

क्या ना करें

यूएसबी (USB) डिवाइस सुरक्षा

संक्रमित (rogue) यूएसबी (USB) डिवाइस का इस्तेमाल न करें { कोई पहले से ही मैलवेयर प्रीलोडेड वाला यूएसबी (USB) ड्राइव या अन्य इलेक्ट्रॉनिक मीडिया, आपके डिवाइस में प्रयोग के लिए इस मंशा से दे सकता है, जिससे कि हैकर कम्प्युटर को आसानी से हैक कर सके}

जब तक बहुत जरुरी न हो, संगठन में यूएसबी(USB) स्टोरेज/ रिमूवेबल मीडिया डिवाइस (removable media device) के प्रयोग की अनुमति न दी जाए

पासवर्ड सिक्योरिटी मैनेजमेंट

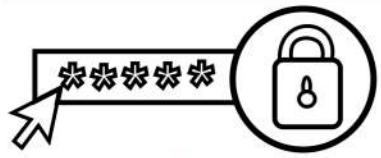
कंप्यूटर के माध्यम से सुगम जानकारी की रक्षा करने में, पासवर्ड मदद करता है। यह केवल अधिकृत प्रयोक्ताओं को सूचना प्राप्त करने देता है। सभी सिस्टम में मजबूत बहु-वर्णीय (multi-character) पासवर्ड लगाया जाने के लिए प्रेरित करना चाहिए।

पासवर्ड अटैक

साइबर अपराधी अकाउंटों तक पहुंचने के लिए कई तरीके प्रयोग में लाते हैं, जिसमें dictionary brute-force attack (पासवर्ड का अनुमान लगाने के लिए किए गए हमले) तथा डिक्शनरी फ़ाइल के विभिन्न शब्द संयोजनों की तुलना करना शामिल है।

साइबर अपराधी, पीड़ित के कंप्यूटर पर "Keylogger" जैसे पासवर्ड कैप्चरिंग टूल का भी प्रयोग कर सकते हैं।

क्या करें



पासवर्ड सिक्योरिटी मैनेजमेंट

- अलग-अलग अकाउंट के लिए हमेशा अलग-अलग पासवर्ड का इस्तेमाल करें। सुनिश्चित करें कि पासवर्ड मजबूत हो
- मजबूत पासवर्ड में अपर केस, लोअर केस, नंबर, "स्पेशल" कैरेक्टर (जैसे, @#$%^&*()+|~-=\'{}[]: ";<>/, आदि का मिश्रण होना चाहिए।)
- ऐसे किसी भी पासवर्ड को, जो गलती से साझा या प्रकट हो गया है, उसे तुरंत बदल दें
- नियमित अंतराल पर पासवर्ड बदलते रहना चाहिए

क्या करें

पासवर्ड सिक्योरिटी मैनेजमेंट

संगठन के लिए जरूरी है की plain text की जगह हैश फॉर्मेट (hash format) में पासवर्ड स्टोर करना चाहिए

क्रिटिकल सिस्टम, एकाउंट आदि तक एक्सेस के लिए मल्टी फैक्टर ऑथेंटिकेशन (MFA) का प्रयोग करें।

जहां भी संभव हो, पासवर्ड हिस्ट्री सेटिंग (password history settings) को लागू करें

पासवर्ड में क्या नहीं होना चाहिए

- जन्म तिथि, नाम, पहचान प्रमाण (ID) और अन्य व्यक्तिगत सूचना जैसे पते और फोन नंबर
- आमतौर पर प्रयुक्त शब्द जैसे परिवार के सदस्यों, पालतू जानवरों, मित्रों, सहकर्मियों, फिल्मों/उपन्यासों/ कॉमिक्स के पात्रों के नाम
- पासवर्ड रिकवरी के उत्तर अनुमान लगाने योग्य नहीं होना चाहिए
- पासवर्ड आठ कैरेक्टर्स (characters) से कम का नहीं होना चाहिए

क्या ना करें

पासवर्ड सिक्योरिटी मैनेजमेंट

- बैंकिंग/संवेदनशील साइट्स पर जाने के लिए सार्वजनिक सिस्टम का प्रयोग न करें
- ई-मेल, चैट या किसी अन्य इलेक्ट्रॉनिक कम्युनिकेशन के जरिए पासवर्ड, ओटीपी (OTP) शेयर न करें
- प्रश्नावलियों या सिक्योरिटी फार्म पर पासवर्ड न बताएं