



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS



साइबर स्वच्छता

साइबर स्पेस के लिए

क्या करें और क्या ना करें



सामान्य (Basic)





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 प्रौद्योगिकी (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।

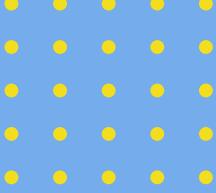
गृह मंत्रालय के साइबर एवं सूचना सुरक्षा (CIS) प्रभाग के तहत भारतीय साइबर अपराध समन्वय केंद्र (I4C) ने औद्योगिक निकायों/आम जनता/सरकारी अधिकारियों के लाभ के लिए साइबर स्वच्छता सर्वोत्तम कार्यप्रणाली (Cyber Hygiene Best Practices) का प्रचार -प्रसार करने के लिए यह मैनुअल (manual) तैयार किया है। इसे साइबर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

अस्वीकरण (Disclaimer): यह दस्तावेज़ केवल मार्गदर्शन और जागरूकता के लिए है। इस दस्तावेज़ की सामग्री का उपयोग जांच आदि में किसी कानूनी सत्यापन में नहीं किया जाना है। इसका उद्देश्य इन मामलों के बारे में बुनियादी जानकारी साझा करना है।



विषय-वस्तु

1. कंप्यूटर सुरक्षा टिप्स -----	5
1.1 यूएसबी (USB) डिवाइस सुरक्षा -----	10
2. पासवर्ड सुरक्षा प्रबंधन -----	12
3. सामान्य इंटरनेट सुरक्षा सावधानियां -----	17
4. वित्तीय लेनदेन-सुरक्षित व्यवहार -----	20
5. सोशल मीडिया प्लेटफॉर्म-सुरक्षा टिप्स -----	24
6. मोबाइल फोन/टैब-सुरक्षा टिप्स-----	27
7. मैलवेयर (Malware) सुरक्षा -----	33
7. ई-मेल सुरक्षा व्यवहार -----	35



परिचय

सूचना प्रौद्योगिकी ने सामाजिक-आर्थिक परिवर्त्य 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:-



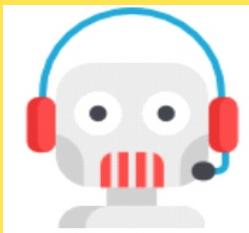
Computer Viruses



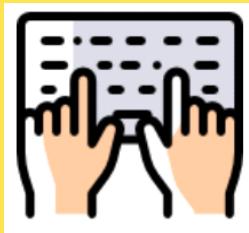
Computer Trojans



Phishing Mail/URL



Botnet



Keylogger



क्या करें



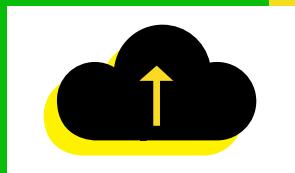
सामान्य कंप्यूटर उपयोग



हमेशा विश्वसनीय (trusted) स्रोतों 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



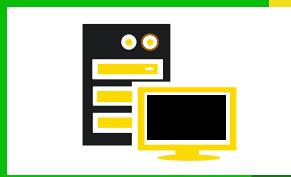
क्या करें



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 सॉफ्टवेयर/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/कमज़ोर 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



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।



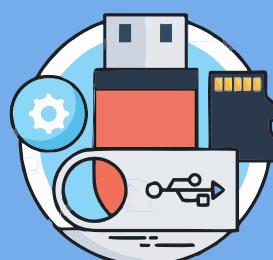
खतरा

- 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 सुरक्षा सुनिश्चित की जा सकती है।



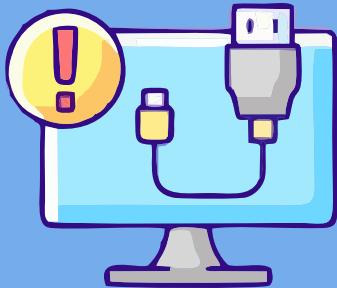
यूएसबी को सपोर्ट करने वाली डिवाइसों का प्रयोग

- फ्लैश ड्राइव/पेन ड्राइव
- पोर्टेबल हार्ड ड्राइव/एसएसडी (SSD)
- मोबाइल फोन
- डिजिटल कैमरा
- कार्ड रीडर
- यूएसबी कीबोर्ड/माउस (mouse)

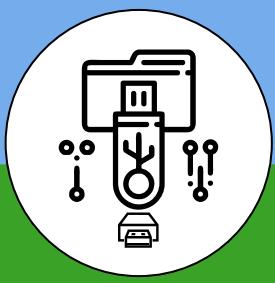




क्या करें



यूएसबी (USB) डिवाइस सुरक्षा



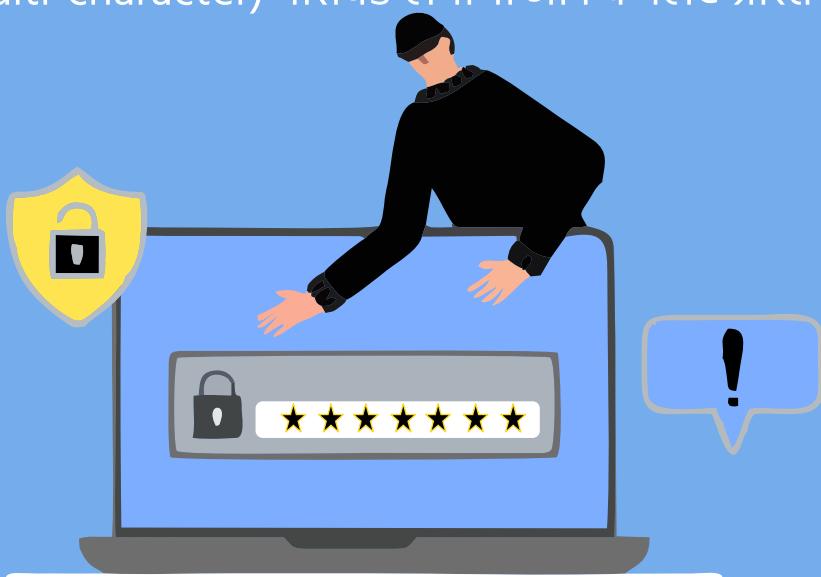
प्रयोग से पहले यूएसबी डिवाइस को एंटीवायरस (Antivirus)/ एंडपॉइंट सुरक्षा (End Point Protection) के द्वारा स्कैन करें



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

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



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

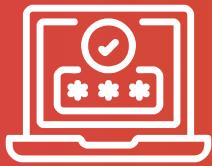


पासवर्ड आठ कैरेक्टर्स (characters) से कम का नहीं होना चाहिए



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

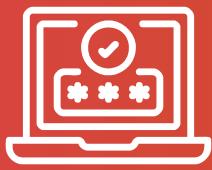


प्रश्नावलियों या सिक्योरिटी फार्म पर पासवर्ड न बताएं



क्या ना करें

पासवर्ड सिक्योरिटी मैनेजमेंट



बैंकिंग/संवेदनशील साइट्स के लिए 'remember my password' विकल्प कभी न चुनें।



अपने पासवर्ड को कहीं भी लिख कर न रखें, खास तौर पर कंप्यूटर पर नोट की तरह।



अविश्वस्त टर्मिनल/स्थानों पर अपने बायोमेट्रिक्स (फिंगरप्रिंट, आदि) का प्रयोग 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 ब्राउज़र
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



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



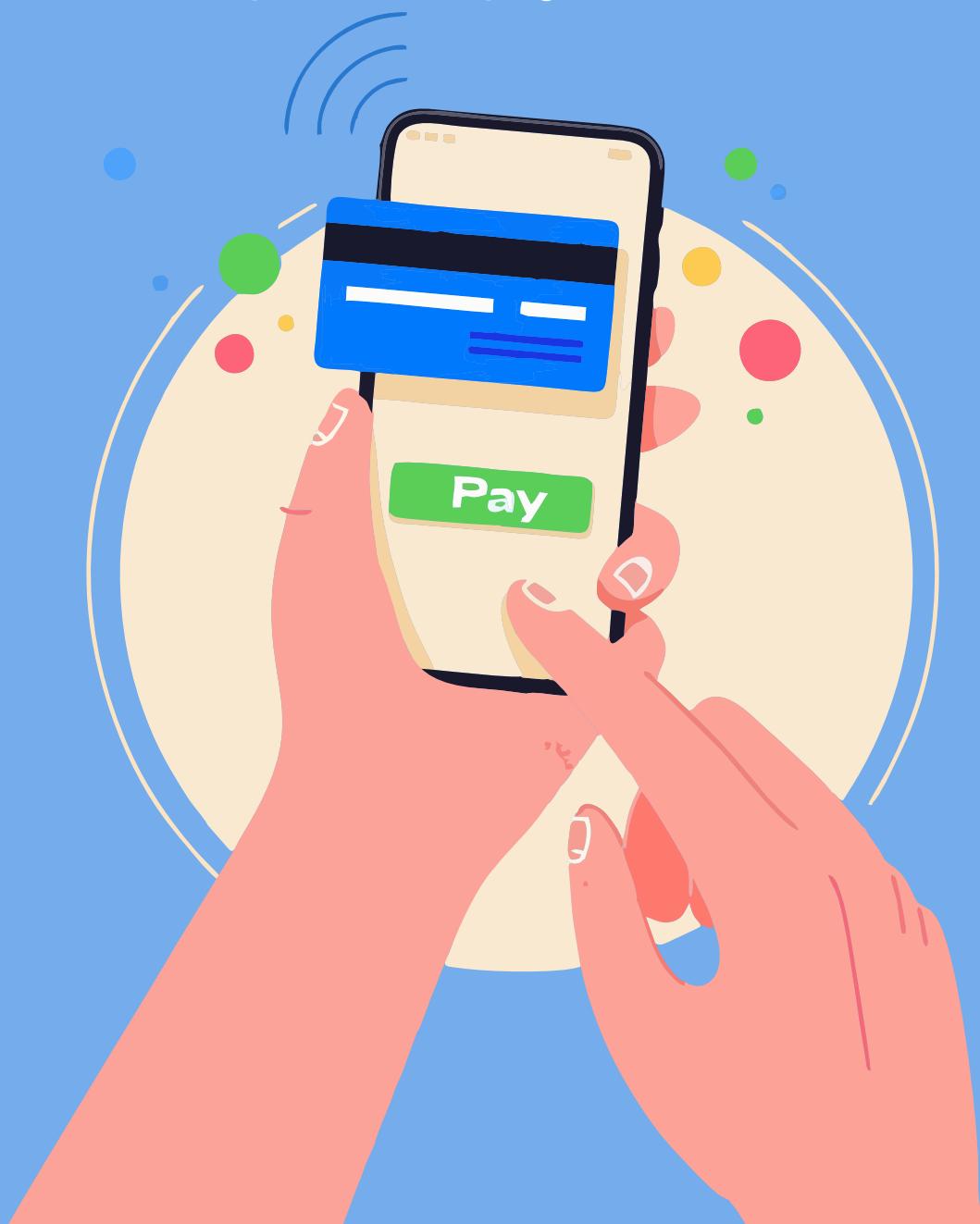
सोशल मीडिया और मैसेजिंग ऐप्स पर असत्यापित सामग्री पर भरोसा न करें और उसे साझा न करें।

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



वित्तीय लेनदेन-सुरक्षित व्यवहार

इंटरनेट बैंकिंग, यूपीआई (UPI), कार्ड, मोबाइल बैंकिंग जैसे भुगतान के डिजिटल तरीकों ने रोजमरा के लेनदेन को काफी सुविधाजनक बना दिया है। पर, ऑनलाइन ट्रांजेक्शन में किसी भी प्रकार की सुरक्षा छूक की वजह से किसी व्यक्ति अथवा किसी संगठन को वित्तीय हानि (financial loss) पहुंचा सकती है।





क्या करें



वित्तीय लेनदेन-सुरक्षित व्यवहार

अपने यूपीआई पिन को सुरक्षित रखें और इसे किसी के साथ साझा न करें

भुगतान प्राप्त करने के लिए यूपीआई पिन की आवश्यकता नहीं होती है

अपने डिवाइस तथा पेमेंट ऐप को पुख्ता पासकोड के साथ सुरक्षित बनाएं

भुगतान करने से पूर्व "प्राप्तकर्ता" के नाम अथवा QR कोड की जांच कर लें

यूपीआई (UPI) सुरक्षा





क्या करें



वित्तीय लेनदेन-सुरक्षित व्यवहार

कार्ड नंबर, वैधता समाप्ति (expiry validity) तथा सीवीवी (CVV) नंबर गोपनीय होते हैं। इन्हें किसी के साथ साझा न करें

पीओएस (PoS)/टर्मिनल/एटीएम (ATM) तथा वेबसाइट की प्रमाणिकता के सत्यापन के उपरांत ही कार्ड का प्रयोग करें

कार्ड सुरक्षा (Card Safety)

अतिरिक्त सुरक्षा के लिए मोबाइल बैंकिंग एप का प्रयोग करते समय अपने कार्ड की कार्ड लिमिट को व्यवस्थित करें

किसी के साथ ओटीपी (OTP) साझा करने से आपके खाते से अनाधिकृत रूप से राशि निकल सकती है



क्या करें



वित्तीय लेनदेन-सुरक्षित व्यवहार

इंटरनेट बैंकिंग लेनदेन के लिए वास्तविक (genuine)/ लाइसेंस (licensed) ऑपरेटिंग सिस्टम का प्रयोग करें।

अपनी पहचान दर्ज करवाने से पूर्व एसएमएस (SMS)/ईमेल (e-mail) में प्राप्त इंटरनेट बैंकिंग यूआरएल (URL) की जांच कर लें

Example
<https://retail.onlinesbi.com> ✓
<http://xyz.com/SBIBank> ✗

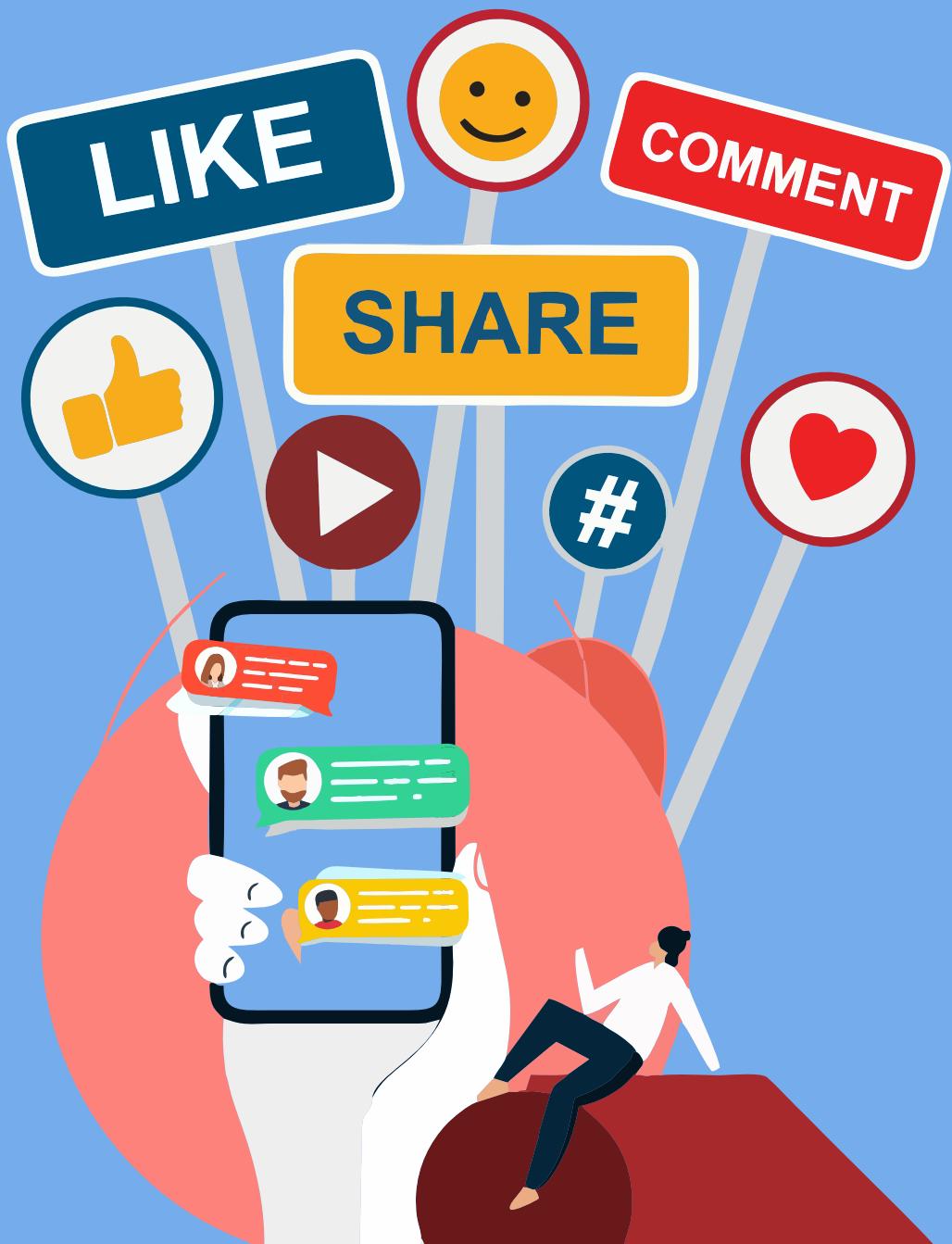
इंटरनेट/मोबाइल बैंकिंग (Internet/Mobile Banking)



सार्वजनिक कंप्यूटर और असुरक्षित इंटरनेट कनेक्शन से अवश्य बचें

एक पुख्ता इंटरनेट बैंकिंग पासवर्ड का प्रयोग करें जो ई-मेल, ई-कॉमर्स इत्यादि जैसे अन्य अकाउंट से भिन्न हो।

सोशल मीडिया प्लॉटफॉर्म-सुरक्षा टिप्स





क्या करें



सोशल मीडिया प्लेटफॉर्म-सुरक्षा टिप्स



इंटरनेट पर किसी भी प्रकार की कोई सामग्री साझा करने से पहले प्राइवेसी सेटिंग (privacy settings) का सावधानीपूर्वक चयन किया जाना चाहिए



इंटरनेट पर अपनी लोकेशन (location) संबंधी सूचना को साझा करने में सतर्क रहें



उचित सावधानी के साथ सत्यापन के उपरांत ही फ्रेंड रिक्यूस्ट (friend request) स्वीकार की जानी चाहिए



सोशल मीडिया पर पोस्ट की गई किसी प्रकार की सामग्री को फॉरवर्ड/शेयर करने से पहले उसकी प्रमाणिकता के लिए जांच की जानी चाहिए



क्या ना करें



सोशल मीडिया प्लेटफॉर्म-सुरक्षा टिप्स



Multi-Factor Authentication (MFA) के बिना सोशल मीडिया अकाउंट का प्रयोग न करें



किसी भी अविश्वसनीय सिस्टम से
सोशल मीडिया अकाउंट में लॉगिन
(log-in) न करें

मोबाइल फोन/टैब-सुरक्षा टिप्स

मोबाइल फोन, संगठन का एक अभिन्न हिस्सा हैं। व्यक्तिगत और संगठन के डाटा की सुरक्षा के लिए फोन का सुरक्षित इस्तेमाल जरूरी है।

मोबाइल फोन के दुरुपयोग से आंकड़ों की चोरी, वित्तीय हानि, अनाधिकृत एक्सेस (unauthorized access), मैलवेयर (malware) संक्रमण आदि हो सकते हैं।





क्या करें

मोबाइल फोन/टैब सुरक्षा टिप्स



- सार्वजनिक वाई-फाई (Wi-Fi) से सावधान रहें, सार्वजनिक नेटवर्क पर साझा की गई जानकारी का दुरुपयोग हो सकता है।



स्मार्टफोन, मोबाइल एप्लिकेशन और सोशल मीडिया एकाउंट की डिफॉल्ट प्राइवेसी सेटिंग्स पर गौर करें।

पब्लिक हस्यता विकल्प के साथ सोशल मीडिया पर पोस्ट की गई व्यक्तिगत तस्वीरों का दुरुपयोग किया जा सकता है



किसी ऐप (App) को डाउनलोड करने से पहले उसकी प्रतिष्ठा/प्रामाणिकता की जांच करें।

ऐप डाउनलोड करने से पहले विक्रेता की गोपनीयता नीतियां पढ़ें और ऐप परमिशन को सत्यापित करें



क्या करें

मोबाइल फोन/टैब
सुरक्षा टिप्स



- विश्वस्त स्रोतों से ही मोबाइल ऐप डाउनलोड करने को प्राथमिकता दें



अनावश्यक ऐप
बंद कर दें/हटा दें



टेलीकॉम ऑपरेटरों
के साथ डू नॉट डिस्टर्ब
(DND) के लिए
पंजीकरण करें।

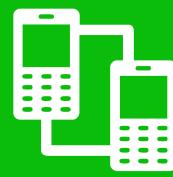


क्या करें

मोबाइल फोन/टैब
सुरक्षा टिप्स



बच्चों या नाबालिंगों को
मोबाइल फोन देते हुए
परेंटल कंट्रोल
(parental control)
मोड का प्रयोग करें



गोपनीय आंकड़ों की
सुरक्षा के लिए डिवाइस
/एसडी (SD) कार्ड
क्रिप्शन का प्रयोग
करें



क्या करें

मोबाइल फोन/टैब सुरक्षा टिप्स



अपने डिवाइस को एक मजबूत पिन/पासवर्ड या बायोमेट्रिक्स (biometrics) के साथ सुरक्षित रखें और मोबाइल फोन में ऑटो लॉक (auto lock) सेटिंग इनेबल करें



हमेशा डाटा (संपर्क, व्यक्तिगत, फोटो आदि) का बैकअप रखें



क्या ना करें

मोबाइल फोन/टैब सुरक्षा टिप्स



अपरिचितों द्वारा
एसएमएस, ई-मेल या
चैट मैसेज के माध्यम से
भेजें गए लिंक का
जबाब न दें अथवा उस
पर क्लिक न करें



डिवाइस में किसी प्रकार
का वर्गीकृत
(classified)/
संवेदनशील
(sensitive) डाटा
(टैक्स/वीडियो/फोटो
ग्राफ) स्टोर न करें



पब्लिक वायरलैस
नेटवर्क का प्रयोग करते
हुए अकाउंट में, खास
तौर से वित्तीय अकाउंट
में लॉगिन न करें

मैलवेयर (Malware) डिफेंस

मैलवेयर 'मेलिशियस' (Malicious) और 'सॉफ्टवेयर' (Software) का संयोजन है। इसे पीड़ित की जानकारी के बगैर पीड़ित के सिस्टम में अनाधिकृत और घातक कार्य करने की मंशा से विकसित किया गया है।

यह विभिन्न कार्य करता है जैसे महत्वपूर्ण फाइलों को लॉक करना, सिस्टम से संवेदनशील जानकारी चुराना, अनाधिकृत रिमोट एक्सेस लेना, प्रयोगकर्ता के कार्यकलापों पर नजर रखना, कम्प्यूटर की मेमोरी को कंज्यूम करना, इंटरनेट bandwidth का प्रयोग, महत्वपूर्ण फाइलों को करए (corrupt) होने से रोकना आदि।

विभिन्न प्रकार के मैलवेयर (malware) हैं, जैसे रैनसमवैयर (Ransomware), स्पाईवेयर (Spyware), वायरेसिस (Viruses), वॉमस् (Worms), रूट किट्स (Root kits), ट्रोजन्स (Trojans), बोटनेट (Botnet) आदि।



मैलवेयर से कैसे सुरक्षा करें?

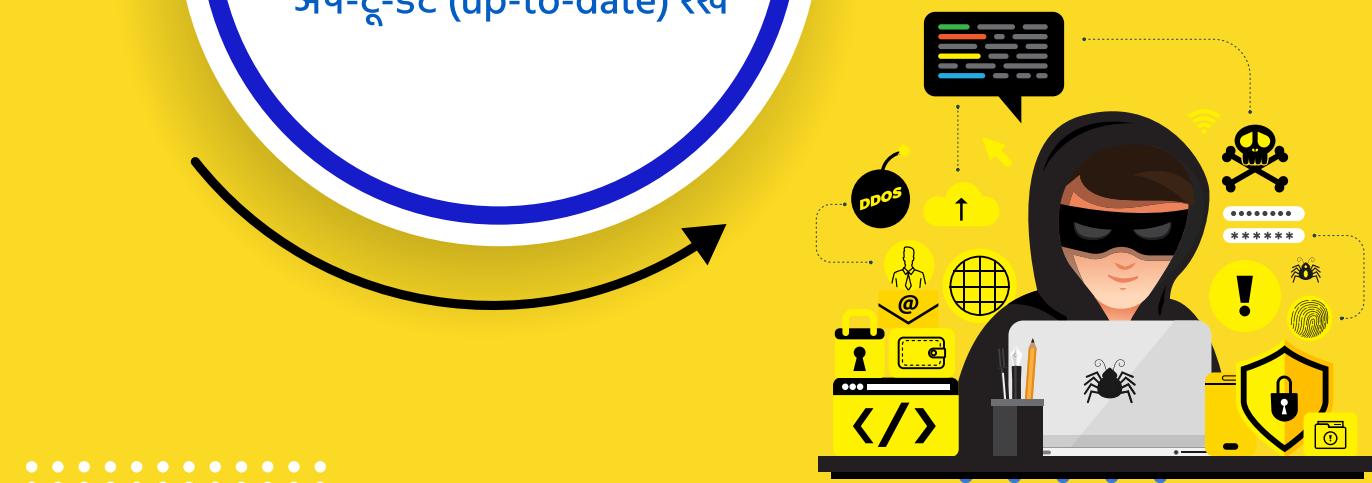
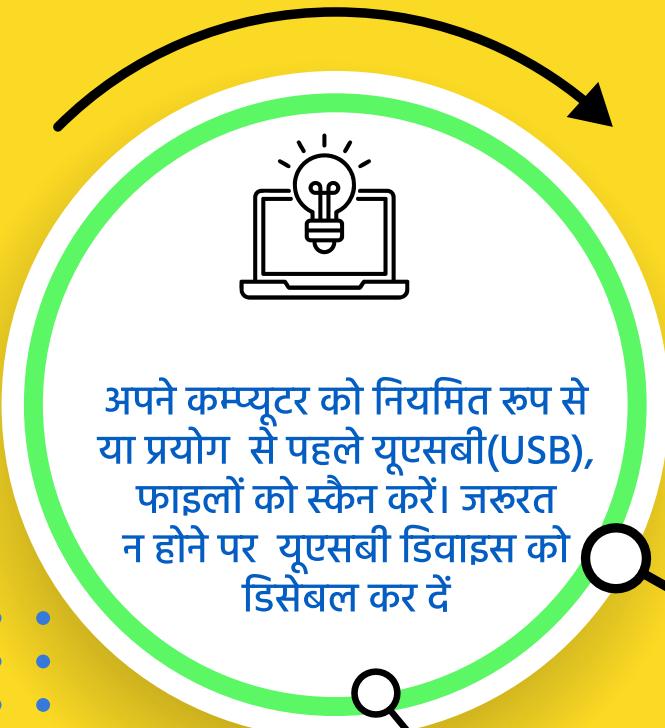
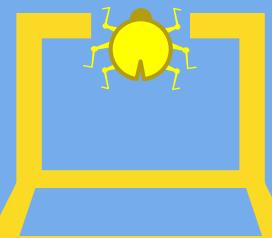
- ऑपरेटिंग सिस्टम और एप्लीकेशन सहित सभी सॉफ्टवैयर को अप-टू-डेट (up-to-date) रखें
- अविश्वसनीय यूआरएल (URL) लिंक पर क्लिक न करें
- एंटी- मैलवेयर (anti-malware) समाधानों का उपयोग
- असुरक्षा से बचने के लिए पैच मैनेजमेंट (patch management) सुनिश्चित करें





क्या करें

मैलवेर
(Malware) डिफेंस



ई-मेल सुरक्षा व्यवहार





ई-मेल सुरक्षा व्यवहार



आकर्षक ऑफर देने वाली ई-मेल लिंक
(हाईपर लिंक/वेब-लिंक/ मेल में
उल्लिखित URL) को न खोले/उसका
उत्तर न दें। इसके फलस्वरूप आपकी
व्यक्तिगत और वित्तीय जानकारी चोरी
हो सकती है।

जब तक प्रेषक का पूर्णतः
सत्यापन न हो जाए, कोई स्पैम ईमेल
(spam e-mail) न देखें



NOTES



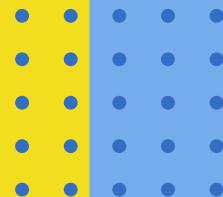
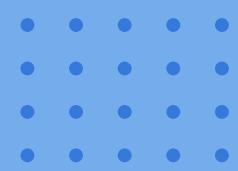
Indian Cyber crime Coordination Centre

NOTES



Indian Cyber crime Coordination Centre





Follow us on:



दिसंबर, 2021

