सूचना सुरक्षा की सर्वोत्तम प्रणालियाँ

गृह मंत्रालय

साइबर दोस्त

भारतीय साइबर क्राइम समन्वय केंद्र

Information Security की **Best Practices**

विषय सूची

1.	परिचय……	3
2.	सामान्य कंप्यूटर प्रयोग……	3
3.	सामान्य इंटरनेट ब्राउजिंग……	5
4.	पासवर्ड प्रबंधन……	9
5.	रिमूवेबल इन्फॉर्मेशन स्टोरेज मीडिया ……	11
6.	ई-मेल संचार……	14
7.	होम Wi-Fi नेटवर्क……	15
8.	सरकारी अधिकारियों/कार्मिकों द्वारा सोशल मीडिया का प्रयोग……	16
9.	सोशल इंजीनियरिंग हमलों से बचाव……	17
10.	शब्दावली……	19

1. परिचय

गृह मंत्रालय, साइबर एवं सूचना सुरक्षा (सीआईएस) प्रभाग ने सरकारी कर्मचारियों /अधिकारियों के हित में सूचना सुरक्षा की सर्वोत्तम प्रणालियों का प्रचार-प्रसार करने के लिए यह दस्तावेज तैयार किया है।

इसे सूचना सुरक्षा संबंधी विवरणों की एक व्यापक सूची के रूप में नहीं समझा जाना चाहिए किंतु बुनियादी न्यूनतम सावधानियां बरतने लायक जानकारी है। प्रत्येक संगठन को अपने उपयोग परिदृश्य, आंकड़ों की संवेदनशीलता, बिजनेस की निरंतरता और अन्य प्रासंगिक घटको के अनुसार, सूचना सुरक्षा संबंधी अतिरिक्त उपायों की पहचान करनी चाहिए।

2. सामान्य कम्प्यूटर प्रयोग

दैनिक आधार पर कम्प्यूटर प्रयोग संबंधी कुछ सर्वोत्तम प्रणालियां निम्नलिखित हैः

2.1 सभी वर्गीकृत कार्यों को केवल ऐसे स्टैंड एलोन कम्प्यूटर में ही किया जाना चाहिए जो इंटरनेट से जुड़े नहीं है ।

2.2 लॉगइन करने के लिए अक्षरों, संख्याओं और विशेष कैरेक्टर का संयोजन करके न्यूनतम दस कैरेक्टर वाले स्ट्रांग पासवर्ड बनाएं।

2.3 आपके संगठन द्वारा प्रयोग हेतु अनुमति प्राप्त एंटी-वॉयरस का प्रयोग करते हुए कम्प्यूटरों को वॉयरस/वर्म्स से सुरक्षित रखना चाहिए।

2.4 यह सुनिश्ति करें कि एंटी-वॉयरस सॉफ्टवेयर सहित आपका आपरेटिंग सिस्टम, अप्लीकेशन और सॉफ्टवेयर पैचेज अप-टू-डेट हैं, और आपके कम्प्यूटर में ऑटो-अपडेट्स सक्रिय हैं।

2.5 कम्प्यूटर को स्क्रीन पर संवेदनशील सूचना के साथ अन-अटेंडेड न छोड़ें।

2.6 कार्य स्थल छोड़ने से पहले अनाधिकृत एक्सेस से बचने के लिए अपने कम्प्यूटर को हमेशा लॉक करें। यूजर कंप्यूटर लॉक करने हेतु Ctrl +

Alt + Del बटन दबाकर, लॉक दिस कंप्यूटर को चुन सकते हैं या विंडो बटन + L दबा कर भी कंप्यूटर लॉक कर सकते हैं ।

2.7 दो मिनट की टाइम आउट अवधि के साथ पासवर्ड- प्रोटेक्टेड स्क्रीन सेवर सक्रिय करें ताकि यह सुनिश्चत किया जा सके कि जिस कम्प्यूटर को आपने असुरक्षित छोड़ दिया है, वह सुरक्षित हो जाए।

2.8 अपने कम्प्यूटर पर आप जो प्लग करते हैं उससे सावधान रहें। मालवेयर इनफेक्टेड यूएसबी ड्राइव, एक्सटर्नल हार्ड ड्राइवस और यहां तक कि स्मार्ट फोन से फैल सकता है।

2.9 कम्प्यूटर को लॉग-इन करने के लिए नॉन-एडमिनिस्ट्रेटर अकाउंट प्रिविलेज का प्रयोग करें और दैनिक प्रयोग के लिए एडमिनिस्ट्रेटर प्रिविलेज वाले एक्सेस से बचे।

2.10 संवेदनशील डाटा को बहुत सावधानीपूर्वक प्रयोग करें और संवेदनशील सूचना को सुरक्षित तरीके से इनकोड करने के लिए इनक्रिप्शन का प्रयोग करें।

2.11 अवांछित क्षति से बचने के लिए अपनी महत्वपूर्ण फाइलों को नियमित अन्तराल पर बैक-अप करें।

2.12 कम्प्यूटर से ऐसे अनावश्यक प्रोग्रामों अथवा सेवाओं को हटा दें जो आपके दिन-प्रतिदिन के कार्यसंचालन के लिए अपेक्षित नहीं है।

2.13 अन्य कम्प्यूटरों को रिमोट एक्सेस, फाइल और प्रिंट शेयरिंग विकल्प न दें।

2.14 फाइल शेयरिंग साफ्टवेयर का प्रयोग न करें क्योंकि फाइल शेयरिंग से आपका कम्प्यूटर मैलिशियस फाइल और अटैक के खतरे के लिए ओपन हो जाता है।

2.15 साइबर कैफे, लाइब्रेरी, कम्प्यूटरों आदि जैसे पब्लिक कम्प्यूटर में संवेदनशील सूचना के प्रयोग से बचे।

2.16 यदि आप साइबर कैफे में कोई व्यक्तिगत सूचना स्टोर अथवा डाउनलोड करते है यह सुनिश्चित करले की अपना काम पूरा कर लेने

के पश्चात सभी दस्तावेजों को स्थाई रूप से डिलीट कर दें। आप डिलीटेड फाइल्स को रिकवर करने के कार्य को मुश्किल बनाने के लिए शिफ्ट और डिलीट बटन को एक साथ दबा सकते हैं।

2.17 ऐसी फाइलों अथवा डाटा को हटा दें जिनकी आपको आगे आवश्यकता नहीं है ताकि ऐसे डाटा के अनधिकृत एक्सेस बचा जा सके। संवेदनशील सामग्री को मात्र डिलीट करना पर्याप्त नहीं है क्योंकि यह आपके सिस्टम से डेटा को वास्तविक रूप से नहीं हटाता है। कम्प्यूटर पर संवेदनशील फाइलों को डिलीट करने के लिए फाइल श्रेडर सॉफ्टवेयर का प्रयोग करना चाहिए।

2.18 कम्प्यूटर पर यूपीएस अथवा अन्य बैक-अप स्रोतों के माध्यम से निर्बाध बिजली आपूर्ति सुनिश्चत करें।

2.19 कम्प्यूटर को सीधे वाल- आउटलेट में प्लग न करें क्योंकि बिजली कम-ज्यादा होने से कम्प्यूटर को नुकसान हो सकता है। कम्प्यूटर प्लग करने के लिए विश्वसनीय सर्ज-प्रोटेक्टर का प्रयोग करें।

2.20 सीपीयू को ओवरहीटिंग से बचाने के लिए सिस्टम को ऐसे कमरें में रखना चाहिए जो डस्ट-फ्री हो और उसमें अच्छा वेंटिलेशन हो ।

3. सामान्य इंटरनेट ब्राउजिंग

इंटरनेट पर ब्राउजिंग करते समय ध्यान में रखी जाने वाली कुछ एक सर्वोत्तम प्रणालियां निम्नलिखित हैः

3.1 लिंक्स अथवा डाउनलोडिंग पर क्लिक करते समय हमेशा सावधान रहें। यदि यह किसी भी कारण से अवांछित अथवा संदिग्ध है तो उस पर क्लिक न करें।

3.2 आपके सिस्टम के एडमिनिस्ट्रेटर/विभाग द्वारा अनुमति प्राप्त स्रोतों के सिवाए किसी अन्य स्रोत से कोई फाइल/सॉफ्टवेयर डाउनलोड न करें।

3.3 उसी वेब-ब्राउजर का प्रयोग करें जिसकी अनुमति आपके संगठन द्वारा दी गई है ।

3.4 ब्राउजिंग के लिए हेमशा अपडेटेड वेब-ब्राउजर का प्रयोग करें। यदि आप ऐसे वेब-ब्राउजर को चलाते हैं जो आउट-डेट है तो इसमें सुरक्षा संबंधी खतरा हो सकता है और आप अपने कम्प्यूटर को जोखिम में डालते है। सुरक्षा एक्सप्लॉएट के आधार पर आपकी व्यक्तिगत जानकारी (ई-मेल, बैंकिंग डिटेल्स, ऑनलाइन ट्रान्जेक्शन्स, फोटो और अन्य संवेदनशील सूचना) को चुराया अथवा नष्ट किया जा सकता है ।

3.5 ऐसी किसी डिवाइस पर कोई संवेदनशील सूचना स्टोर/ शेयर न करें जो इंटरनेट से जुड़ी हुई है।

3.6 यदि लॉग-इन स्क्रीन पर सूचना इंटर करने के पश्चात विंडो में ब्राउजर पर दिया जाने वाला "सेव पासवर्ड" विकल्प आता है और आपको ऐसा करने के लिए कहता है तो उसका चयन नहीं करना चाहिए। वेब ब्राउजर, विशेष रूप से उन पीसी पर जो अन्य यूज़र्स के साथ शेयर हैं, पर पासवर्ड अथवा क्रेडिट कार्ड सूचना जैसी अकाउंट संबंधी जानकारी सेव न करें ।

3.7 ब्राउजर एड्रेस बार में https साइन देखें। https में "एस" का मतलब सुरक्षित से है जिसका तात्पर्य ये है कि वेबसाइट में एसएसएल इनक्रिप्शन सक्रिय है। अपने ब्राउजर एड्रेस बार में ग्रीन पैडलॉक आइकन के साथ https के लिए चेक करें ताकि यह सत्यापित हो सके कि साइट सुरक्षित है।

3.8 प्रत्येक लॉग-आउट सेशन के पश्चात ब्राउजर से हिस्ट्री क्लीयर करने की आदत बनाएं । विभिन्न ब्राउजरों में प्रत्येक ब्राउजर सेशन के अन्त में हिस्ट्री को स्वयमेव क्लीयर करने की निम्नलिखित सेटिंग्स हैं ।

क्रोम

- ऊपरी दाहिने कोने में मेनू आइकन पर क्लिक करें और **सेटिंग्स >** स्लेक्ट करें, **एडवांस्ड सेटिंग्स.. > प्राइवेसी** शो करें और फिर **कंटेंट सेटिंग्स** बटन टैप करें।
- अगली विंडो जो कुकीस के अंतर्गत खुलती है, में यह विकल्प है जो यह कहता है **"लोकल डेटा केवल अपने ब्राउजर के क्विट होने तक रखें"**
- विंडो के वॉटम में **डन** दबाएं **।**

फायरफोक्स

- ऊपरी दाहिने कोने में मेनू आइकन पर क्लिक करें और **ऑप्शन** सलेक्ट करें। फिर जो विंडों खुलता है उसमें **प्राइवेसी** टैब पर क्लिक करें।
- हिस्ट्री के अंतर्गत "फायरफोक्स विल" के बाद ड्रॉप डाउन मेनू पर क्लिक करें और **हिस्ट्री के लिए कस्टम सेटिंग्स** सलेक्ट करें।
- जब **फायरफोक्स बंद हो जाए तो क्लियर हिस्ट्री** का विकल्प चेक करें।
- एक बार आपने यह कर लिया तो **ओके** क्लिक करें।

इंटरनेट एक्सप्लोरर

- ब्राउजर के ऊपरी दाहिने कोने में सेटिंग्स ऑइकन पर क्लिक करें और **इंटरनेट ऑप्शन्स** सलेक्ट करें।
- विंडो में जो **जनरल टैब** दिखाई देती है उसे ओपन करें।
- ब्राउजिंग हिस्ट्री सेक्शन के अंतर्गत, **"डिलीट ब्राउजर हिस्ट्री ऑन इक्जिट"** के बाद बॉक्स चेक करें। एक बार आपने यह कर लिया फिर **ओके** पर क्लिक करें।

3.9 निजी क्लाउड सर्विसेज (गूगल ड्राइव, ड्रॉपबॉक्स, आईक्लाउड आदि) पर सरकार की कोई भी वर्गीकृत सूचना स्टोर नहीं कर सकते और ऐसा करने पर यदि डेटा लीकेज हो जाता है तो आप दांडिक कार्रवाई के भागीदार होंगे ।

3.10 जब आप दौरे पर है तो ऐसी सेवाओं का प्रयोग करने से बचे जिनमें लोकेशन इनफारमेशन अपेक्षित है जब तक कि कार्यालय से संबंधित ड्यूटी के निष्पादन के लिए ऐसा करना आवश्यक न हो ।

3.11 ब्राउजिंग करते समय, क्लोज बटन के विकल्प के साथ कुछ पॉप-अप्स आएंगे। ये फर्जी हो सकते है और जब आप उस पर क्लिक करते है तो वे वस्तुतः स्पाईवेयर इन्स्टॉल करने की कोशिश कर सकते है। ऐसे पोप-अप्स से सावधान रहें और उन पर क्लिक करने से बचे।

3.12 ब्राउजर में पॉप-अप्स ब्लॉकर विकल्प को सक्रिय रखा जाना चाहिए और यदि अपेक्षित हो तो विश्वसनीय साइट के चयन के आधार पर अनुमति दी जाए । ऐसा करने से स्क्रीन पर आने वाले किसी भी प्रकार के न्यूसेंस वेब एड्स अथवा एड्स में मौजूद मालवेयर को रोकने में मदद मिलेगी। विभिन्न ब्राउजरों में पोप-अप्स ब्लॉकर कनफिगर सक्रिय करने की निम्नलिखित सेटिंग्स हैं।

फायरफॉक्स

- मोजिला फायरफॉक्स टास्कबार से **टूल** सेलेक्ट करें
- ड्रॉप-डाउन मेनू से **आप्शन** सेलेक्ट करें
- आप्शन डॉयलॉग बॉक्स से **कन्टेंट** सेलेक्ट करें
- सभी प्रकार के पाप-अप्स को सक्रिय/इनेबल करने के लिए **ब्लॉक पोप-अप्स विंडों** रेडियो बटन चेक करें
- **क्लोज** पर क्लिक करें

क्रोम

- **मेनू** पर क्लिक करें
- **सेटिंग्स** पर किल्क करें
- **प्राइवेसी** पर स्क्रॉल करें, **कंटेंट सेंटिंग्स** पर क्लिक करें
- **पोप-अप्स** पर स्क्रॉल करें
- पोप-अप्स दिखाने के लिए सभी एलाउ साइट्स **अनचेक** करें
- **ओके** पर क्लिक करें

इंटरनेट एक्स्प्लोरर

- **टूल्स** मेनू पर क्लिक करें
- **इंटरनेट ऑप्शन** पर क्लिक करें
- **प्राइवेसी** टैब पर क्लिक करें
- पॉप-अप ब्लॉकर के नीचे, **टर्न ऑन पॉप-अप ब्लॉकर** पर क्लिक करें
- **ओके** पर क्लिक करें

3.13 याद रखें कि इंटरनेट पर कोई भी चीज मुफ्त नहीं होती। "फ्री" स्क्रीनसेवर आदि में अक्सर मैलवेयर होते हैं। इसलिए ऐसे ऑनलाइन मुफ्त ऑफ़र से सावधान रहें।

3.14 किसी भी वित्तीय या संवेदनशील ट्रांजेक्शन में एक्सेस करने और उसे संचालित करने के लिए सार्वजनिक कंप्यूटर और सार्वजनिक वाई-फाई कनेक्शन का उपयोग करने से बचें। ऐसे कंप्यूटरों पर सरकारी ईमेल को एक्सेस करने से सूचना लीक होने का खतरा रहता है।

3.15 यदि आपकी नौकरी में आपको कुछ सूचना प्रणालियों को सुरक्षित तरीके से एक्सेस करना अपेक्षित है, तो सलाह है कि ऐसे एक्सेस के लिए एमपीएलएस लिंक, वीपीएन ओवर इंटरनेट आदि जैसे सुरक्षा नियंत्रण का उपयोग करें।

4. **पासवर्ड प्रबंधन**

ऐसे किसी भी व्यक्ति के लिए अनधिकृत एक्सेस एक बड़ी समस्या है जो कंप्यूटर अथवा स्मार्टफोन या टैबलेट जैसे अन्य उपकरणों का उपयोग करते हैं। इन ब्रेक-इन के पीड़ितों को वर्गीकृत जानकारी, व्यक्तिगत डेटा आदि जैसे मूल्यवान डेटा की हानि उठानी पड़ सकती है। हैकरों का कंप्यूटर से गुप्त जानकारी चुराने का सबसे आम तरीका पासवर्ड का अनुमान लगाना है। साधारण और आमतौर पर इस्तेमाल किए जाने वाले पासवर्ड से हैकर्स को कंप्यूटर तक आसानी से पहुँचने और नियंत्रित करने में आसानी होती है।

पासवर्ड बनाने और प्रबंधित करते समय विचार की जाने वाली निम्नलिखित सर्वोत्तम प्रणालियां हैं :

4.1 वर्णमाला, संख्याओं तथा करेक्टरों का संयोजन करके कम से कम 10 करेक्टर का आदर्श और मजबूत पासवर्ड बनाएं।

4.2 सभी पासवर्ड (अर्थात ईमेल, कंप्यूटर आदि) को प्रत्येक तीन महीने में कम से कम एक बार अवश्य बदलें।

4.3 पुराने पासवर्ड का पुन: उपयोग न करें।

4.4 पासवर्ड को कंप्यूटर, नोटबुक, नोटिस बोर्ड या ऐसे किसी अन्य स्थान पर पठनीय रूप में संग्रहीत नहीं किया जाना चाहिए जहां अनधिकृत व्यक्ति उन्हें ढूंढकर उपयोग कर सकें।

4.5 पासवर्ड को संवेदनशील जानकारी मानें और इसे किसी के साथ साझा न करें।

4.6 अपने हर लॉग-इन खातों के लिए हमेशा अलग-अलग पासवर्ड का उपयोग करें। यदि आपके द्वारा प्रयोग की जा रही एक साइट हैक हो जाए तो एक से अधिक खातों के लिए एक ही पासवर्ड का प्रयोग करने से बहुत सारे जोखिम का खतरा रहता है।

4.7 यदि आपके काम में पासवर्ड बताने की आवश्यकता होती है, तो ईमेल के माध्यम से अटैचमेंट के रूप में भेजी गई एन्क्रिप्टेड फ़ाइल के लिए पासवर्ड भेजते समय इसे फोनकॉल या एसएमएस जैसे एक अलग चैनल के माध्यम से बताया जाना चाहिए।

4.8 यदि एप्लीकेशन द्वारा "रेमेंबर पासवर्ड" फीचर दर्शाया जाता है तो इसे हमेशा डिक्लाइन करें।

4.9 याद रखें कि कमजोर पासवर्ड की निम्नलिखित बातें होती हैं:

- पासवर्ड में 10 से कम करेक्टर होते हैं।
- पासवर्ड एक शब्द है जो शब्दकोश (अंग्रेजी या विदेशी) में पाया जाता है।
- परिवार के सदस्य, पालतू जानवरों, दोस्तों, सहकर्मियों, फिल्मों/उपन्यास/ कार्टूनपात्रों इत्यादि के नाम, कंप्यूटर शब्दावली और नाम, कमांड, साइटें, कंपनी, हार्डवेयर, सॉफ्टवेयर जैसा पासवर्ड एक सामान्य प्रयोग का शब्द है।
- जन्मदिन और पते और फोन नंबर जैसी अन्य व्यक्तिगत जानकारी।
- 123456, aaaaa, qwerty, asdfg, zxcvb इत्यादि जैसी शब्द या संख्या पैटर्न।

4.10 एक मजबूत पासवर्ड बनाने के लिए कुछ सुझाए गए तरीके निम्नलिखित हैं :

- एक सुरक्षित पासवर्ड में केवल अक्षरों की बजाय नंबर, विशेष वर्ण/स्पेशल करैक्टर और कैप्स का प्रयोग भी अवश्य करना चाहिए। एक सुझाव के तौर पर अक्षरों को संख्याओं और विशेष वर्णों से बदलना, जैसे "i" बन जाएगा "!", "o" बदल जाता है "0" में, 's" को "$" लिखा जाता है। इस तरह, Microsoft जैसा सरल शब्द काफी कठिन शब्द "M!cr0$0ft" में बदल जाता है।

- पासवर्ड की लंबाई मायने रखती है, पासवर्ड जितना लंबा होगा उसे क्रेक करना उतना ही कठिन होगा।
- एक वाक्य के बारे में सोचें और एक पंक्ति में प्रत्येक शब्द के पहले अक्षर का चयन करें। इससे एक जटिल और आसानी से याद रखने वाला पासवर्ड मिलेगा। उदाहरण के लिए, इस तरह का वाक्य, " My Name is Dinesh Anandan and I was born on 1January 1986!" से निम्नलिखित पासवर्ड बनेगा : "MNiDAaIwbo1J1986!"। यह लंबा है, इसमें संख्याएँ, विशेष करेक्टर और कैप्स शामिल हैं, और यह याद रखना आसान है और शब्दकोश में नहीं है।

5. **रिमूवेबल इन्फॉर्मेशन स्टोरेज मीडिया**

आज की सबसे बड़ी सुरक्षा चिंता नेटवर्क में रिमूवेबल स्टोरेज डिवाइस (USB डिवाइस जैसे पेन ड्राइव, CD-RW, DVD-RW, ब्लू-रे डिस्क, मीडिया कार्ड इत्यादि) का उपयोग है। डेटा की मात्रा जिसे रिमूवेबल स्टोरेज डिवाइस में तत्काल कॉपी किया जा सकता है, दिन प्रतिदिन बढ़ती जा रही है। जबकि इन डिवाइसों से उत्पादकता में काफी वृद्धि हो जाती है। तथापि, इनसे डेटा सुरक्षा और नियंत्रण नीतियों में अत्यधिक जोखिम रहता है।

एक्सटर्नल रिमूवेबल स्टोरेज डिवाइस उपयोगकर्ताओं को फायरवॉल और ईमेल सर्वर एंटी-मैलवेयर सहित परिधि सुरक्षा को बायपास करने की अनुमति देते हैं, और संभावित रूप से कार्यालय नेटवर्क में मैलवेयर डाल देते हैं। चूंकि, मैलवेयर एक आंतरिक डिवाइस से नेटवर्क में प्रवेश करता है, इसलिए तब तक डिटैक्ट नहीं हो पाता जब तक यह नेटवर्क में बड़ा नुकसान न कर चुका हो। रिमूवेबल स्टोरेज डिवाइस से किसी संगठन के परिसर से संवेदनशील जानकारी को चुराने में आसानी होती है। इस जानकारी में वर्गीकृत जानकारी शामिल हो सकती है।

रिमूवेबल स्टोरेज मीडिया में काम करते समय विचार की जाने वाली कुछ सर्वोत्तम प्रणालियां निम्नलिखित हैं:

5.1 सभी रिमूवेबल स्टोरेज मीडिया के लिए आटोरन/आटोप्ले फीचर डिसेबल किया जाना चाहिए।

5.2 वर्गीकृत सूचना स्टोर करने के लिए निर्धारित रिमूवेबल स्टोरेज मीडिया में कॉपी करने से पहले वर्गीकृत डेटा को इन्क्रिप्टिड किया जाना चाहिए।

5.3 वर्गीकृत सूचना को इस कार्य के प्रयोजन हेतु संगठन को आवंटित रिमूवेबल स्टोरेज मीडिया पर ही स्टोर किया जाना चाहिए।

5.4 यूएसबी स्टोरेज डिवाइस में छुपी मैलिशियस फाइल को देखने के लिए कम्प्यूटर में "**शो हिडन फाइल एंड फोल्डर्स**" विकल्प इनेबल किया जाना चाहिए।

कम्प्यूटर में किसी अनयूजुअल अथवा हिडन फाइल को देखने के लिए हिडन फाइल एंड सिस्टम फाइलस व्यू इनेबल करने के निम्नलिखित तरीके हैं:-

विंडोज 10

- टास्कबार पर सर्च बॉक्स में **फोल्डर** टाइप करें और फिर सर्च रिजल्ट से **शो हिडेन फाइल्स एंड फोल्डर्स** सेलेक्ट करें।
- **एडवांस्ड सेटिंग्स** के **शो हिडेन फाइल्स, फोल्डर्स एंड ड्राइव्स** सेलेक्ट करें और फिर **ओके** सेलेक्ट करें।

विंडोज 8.1

- **सर्च** पर जाएं।
- फिर सर्च बॉक्स में **फोल्डर** टाइप करें, तत्पश्चात सर्च रिजल्ट से **फोल्डर ऑप्शन** सेलेक्ट करें।
- **व्यू** टैब सेलेक्ट करें।
- **एडवांस्ड सेटिंग्स** के **शो हिडेन फाइल्स, फोल्डर्स एंड ड्राइव्स** सेलेक्ट करें और फिर **ओके** सेलेक्ट करें।

विंडोज 7

- **स्टार्ट बटन** सेलेक्ट करें, फिर **कंट्रोल पैनल-> एपीयरेंस एंड पर्सनलाइजेशन** सेलेक्ट करें।
- **फोल्डर ऑप्शन्स** को सेलेक्ट करें, इसके बाद **व्यू** टैब को सेलेक्ट करें।

5.5. यह उपयुक्त होगा कि इस्तेमाल करने से पहले समस्त हटाने योग्य मीडिया को एंटी-वायरस सॉफ्टवेयर से स्कैन कर लें।

5.6. USBs, CDs आदि जैसे हटाने योग्य मीडिया को अरक्षित नहीं छोड़ा जाना चाहिए।

5.7. सरकार के नेटवर्क के बाहर पोर्टेबल स्टोरेज मीडिया ड्राइव्ज के इस्तेमाल को प्रतिबंधित करने के लिए टैक्नीकल कंट्रोल को क्रियान्वित किया जाए।

5.8. जब तक आपके कार्यालय के सक्षम प्राधिकारी द्वारा अनुमति न दे दी जाए तक तक हटाने योग्य मीडिया को कार्यालय से बाहर नहीं ले जाना चाहिए।

5.9. भौतिक जौखिम, क्षति, चोरी अथवा electrical corruption को न्यूनतम रखने के लिए समस्त स्टोरेज मीडिया को समुचित रूप से किसी सुरक्षित एवं संरक्षित वातावरण में ही स्टोर किया जाना चाहिए।

5.10. डिवाईस के क्षतिग्रस्त अथवा कार्य न करने की स्थिति में इसे मरम्मत/बदलने के लिए अपने कार्यालय के संबंधित अधिकारी को वापस किया जाना चाहिए। कभी भी ऐसी डिवाईसेस को मरम्मत के लिए किसी बाहरी व्यक्ति अथवा अन्य विक्रेताओं को न दें क्योंकि इसमें क्लासीफाइड सूचना हो सकती है।

5.11. यदि, जारी होने के बाद USB डिवाइस के प्रयोग की और आवश्यकता न हो तो उसे जारीकर्ता प्राधिकारी को वापस कर दिया जाना चाहिए।

5.12. शासकीय प्रयोजन पूरा हो जाने के बाद रिमूवेबल मीडिया की विषय-वस्तु को अनिवार्य रूप से हटा/मिटा दिया जाना चाहिए।

6. ई-मेल संचार

ई-मेल प्रयोग के संबंध में निम्नलिखित कुछ सर्वोत्तम प्रणालियां हैं:

6.1. शासकीय प्रयोग (अर्थात .nicemail) के लिए केवल सरकार द्वारा मुहैया कराए गए ई-मेल एड्रेस का प्रयोग करें।

6.2. किसी भी शासकीय प्रयोग के लिए निजी ई-मेल एड्रेस के इस्तेमाल को प्रतिबंधित करने के लिए सिस्टम एडमिनिस्ट्रेटर समुचित कंट्रोल डेप्लोय कर सकता है।

6.3. अनजान अथवा अप्रमाणित स्रोतों से प्राप्त ई-मेल अटैचमेंट्स को डाउनलोड करने से बचें या इनसे प्राप्त संदिग्ध लिंकों पर क्लिक करने से भी बचें।

6.4. वर्गीकृत सूचना को ई-मेल द्वारा नहीं संप्रेषित किया जाना चाहिए। यदि आकस्मिक जरूरत की स्थिति में ऐसा करना हो, तो सक्षम प्राधिकारी का अनुमोदन प्राप्त किया जाना चाहिए।

6.5. सार्वजनिक Wi-Fi कनेक्शनों से शासकीय ई-मेल अकाउंट्स को एक्सेस करने से बचे।

6.6. ई-मेल अकाउंट्स के लिए पासवर्ड के आटो सेव को अधिकृत नहीं किया जाना चाहिए।

6.7. अपना कार्य पूरा करने के बाद मेल अकाउंट्स से लॉग आउट करें।

6.8. किसी ई-मेल में प्राप्त हुए लिंकों को क्लिक करने के बजाए प्रयोक्ता को संपूर्ण URL, browser में टाइप करना चाहिए।

6.9. किसी भी संदिग्ध ई-मेल को न खोलें/न अग्रेषित करें/न ही उत्तर दें।

6.10. छोटे या लघुकृत URL (जो http://tiny.cc/ba1j5y जैस दिखते हों) के बारे में सावधान रहें और इन्हें क्लिक न करें क्योंकि यह आपको malware संक्रमित वेबसाइट में ले जा सकता है।

6.11. ऐसे अटैचमेंट को न खोलें जिनमें EXE, DLL, VBS, SHS, PIF, SCR जैसे क्सटेंशन हैं। विशिट उदाहरण txt.exe, .doc.exe हैं।

7. **होम** Wi-Fi **नेटवर्क**

लैपटॉप, स्मार्ट फोन और टैबलेट के बड़ी मात्रा में प्रयोग से, इंटरनेट से कनेक्टिविटी के एक विकल्प के रूप में परवेसिव वायरलेस कनेक्टिविटी का व्यापक रूप से प्रयोग किया जाता है। असुरक्षित बेतार कनफिगरेशन, मैलिशियस थ्रेट एक्टर्स के लिए एक आसान रास्ता उपलब्ध करा सकता है। सरकारी अधिकारी अपने घर के Wi-Fi नेटवर्क का इस्तेमाल कार्यालय के कार्य हेतु कर सकते हैं तथा उनके घर के Wi-Fi नेटवर्क को सुरक्षित रखने के लिए निम्नलिखित कुछ सर्वोत्तम प्रणालियां हैं:

7.1. बेतार राउटर्स में WPA2 अथवा हायर इन्क्रिप्शन फीचर चालू करें।

7.2. नेटवर्क डिवाईस के डिफ़ॉल्ट नाम को बदलें, इसे इसके सर्विस-सेट-आइडेन्टीफायर अथवा "SSID" के रूप में भी जाना जाता है। जब भी बेतार कनेक्शन के साथ कोई कम्प्यूटर search करता है और नजदीकी बेतार नेटवर्क को प्रदर्शित करता है, तो यह प्रत्येक नेटवर्क की सूची दर्शाता है, जो सार्वजनिक रूप से इसके SSID को प्रसारित करता है। यह उचित होगा कि आप ऐसा SSID नाम रखे जो किसी भी रूप में आपकी पहचान को न प्रकट करता हो।

7.3. नेटवर्क डिवाईस डिफॉल्ट पासवर्ड को बदलें। अप्राधिकृत यूजर, डिफॉल्ट पासवर्डस से परिचित हो सकते हैं, इसलिए यह जरूरी है कि आप राउटर डिवाईस का पासवर्ड बदल लें।

7.4. आप अपने बेतार राउटर में मीडिया एक्सेस कंट्रोल, अथवा "MAC," एड्रेस फिल्टर के प्रयोग पर विचार करें। प्रत्येक डिवाईस, जो Wi-Fi नेटवर्क से कनेक्ट हो सकती है, उसकी एक यूनिक आईडी होती है जिसे "फिजीकल एड्रेस" अथवा "MAC" एड्रेस कहा जाता है। बेतार राउटर उन सभी डिवाईसेस के MAC एड्रेसेज को स्क्रीन पर सकता है, जो उनसे

कनेक्ट होते हैं और प्रत्योक्ता MAC एड्रेसेज के साथ केवल उन्हीं डिवाईसेस से कनेक्शन स्वीकार करने हेतु अपने बेतार नेटवर्क को सेट कर सकता है, जिन्हें राउटर मान्यता प्रदान करेगा। अप्राधिकृत एक्सेस के लिए दूसरी बाधा उत्पन्न करने के लिए आप केवल अपनी डिवाईसेस को शामिल करने के लिए अपने बेतार राउटर के MAC एड्रेस फिल्टर को सक्रिय करने पर विचार करें।

7.5. जब लंबे समय तक इसकी जरूरत न हो तो अपने बेतार राउटर को ऑफ कर दें ।

7.6. बेतार डिवाईसेस के फर्मवेयर को नियमित रूप से अद्यतन करते रहें क्योंकि यह डिवाईस में सुरक्षा बचाव की कमियों को कम कर देगा।

7.7. अनधिकृत प्रवेश को रोकने के लिए रूटर्स में रिमोट मैनेजमेंट फीचर को डिसेबल कर दें।

8. **सरकारी अधिकारियों/कार्मिकों द्वारा सोशल मीडिया का प्रयोग**:

सभी कर्मचारी, जिनमें कर्मचारी, संविदा आधारित स्टाफ, परामर्शदाता, साझीदार, थर्ड पार्टी स्टाफ आदि शामिल हैं, और जो सूचना प्रणालियों, सुविधाओं, संचारी नेटवर्कों को व्यवस्थित करते हैं, ऑपरेट करते हैं अथवा सपोर्ट करते हैं, तथा जो स्वयं या भारत सरकार की ओर से कोई सूचना सृजित करते हैं, एक्सेस करते हैं, स्टोर करते हैं और प्रॉसेस करते हैं, को जब तक ऐसा करने के लिए प्राधिकृत न किया जाए, वे:-

क. किसी सरकारी डिवाईस (कम्प्यूटर, मोबाइल आदि) पर सोशल मीडिया को एक्सेस नहीं करेंगे।

ख. सोशल मीडिया अथवा सोशल नेटवर्किंग पोर्टल अथवा एप्लीकेशंस पर सरकारी सूचना को प्रकट नहीं करेंगे।

9. **सोशल इंजीनियरिंग हमलों से बचाव**

सोशल इंजीनियरिंग, गलत प्रतिनिधित्व के माध्यम से सूचना प्राप्त करने के लिए एक प्रवेश-मार्ग है। सूचना प्राप्त करने के लिए यह महसूस किए बिना कि इससे सुरक्षा का उल्लंघन हो रहा है, यह लोगों के साथ जानबूझ कर की जाने वाली धोखेबाजी है। यह टेलीफोन के माध्यम से व्यक्तिगत रूप में और ई-मेल के माध्यम से नकली पहचान के रूप में हो सकती है। नीचे कुछ सर्वोत्तम प्रणालियां हैं जिनका सोशल इंजीनियरिंग के हमलों से दूर रहने के लिए अनुसरण किया जाना चाहिए:

9.1. अप्राधिकृत फोन कॉलों, मुलाकात अथवा व्यक्तियों के ई-मेल संदेशों से सावधान रहें, जो निजी अथवा अन्य सरकारी जानकारी देने के लिए कहते हैं। यदि कोई अनजान व्यक्ति किसी वैध संगठन से होने का दावा करता है तो उसकी पहचान की सत्यता सीधे कंपनी से पता करने की कोशिश करें।

9.2. Phishing एक सामान्य प्रकृति का सोशल इंजीनियरिंग स्कैम है। हैकर किसी ऐसी सूचना की मांग करते हुए, अपने लक्ष्य के लिए कोई ई-मेल अथवा text भेजता है, जो किसी विशेष अपराध में मददगार साबित हो सकती है। इसलिए ई-मेल या संदेशों में निजी, संवेदनशीलता अथवा वित्तीय जानकारियों का खुलासा न करें तथा इस प्रकार की ई-मेल्स का कोई जवाब न दें।

उदाहरण के लिए, हैकर ऐसे ई-मेल्स भेज सकता है, जो पीड़ित को किसी विश्वसनीय स्रोत से आए प्रतीत होते हैं। उदाहरण के लिए ऐसा स्रोत कोई बैंक हो सकता है, जो ई-मेल प्राप्तकर्ता को उसके अकाउंट्स को लॉग-इन करने हेतु किसी लिंक पर क्लिक करने के लिए कह सकता है। यद्यपि जो उस लिंक पर क्लिक करते हैं, उसे एक जाली वेबसाइट पर ले जाया जाता है जो ई-मेल्स की तरह ही वैध प्रतीत होती है। यदि वे उक्त जाली साइट पर लॉगइन करते हैं तो वे आवश्यक रूप से अपने लॉगइन क्रेडेंशियल्स दे रहे होते हैं और इस प्रकार वे धोखेबाज को अपने बैंक खातों तक पहुंचने का रास्ता दे देते हैं।

9.3. Vishing प्ररूप phishing का ही एक voice version है। "V" का आशय voice से होता है, लेकिन अन्यथा स्कैम की कोशिश का तरीका वैसा ही होता है। इसमें हैकर

पीडित को महत्वपूर्ण सूचना देने के लिए फसांने के लिए फोन का प्रयोग करता है। इसलिए फोन कॉल्स पर कोई संवेदनशील जानकारी का खुलासा न करें।

उदाहरण के लिए, कोई हैकर अपने आपको सरकारी अधिकारी बताकर किसी अधिकारी को कॉल कर सकता है। हैकर पीड़ित व्यक्ति को प्रभावित करके उससे लॉग इन आईडी पहचान या अन्य सूचना देने के लिए कह सकता है जिसका उपयोग संगठन को निशाना बनाने के लिए किया जा सकता है।

9.4 Quid pro quo: आपस में लेनदेन का घोटाला सोशल इंजीनियर अटैक का एक दूसरा प्रकार है जिसमें आपस में लेनदेन शामिल होता है जैसे कि मैं आपको यह देता हूं, और आप मुझे यह दे दें। हैकर्स पीड़ित को यह विश्वास दिलाता है कि यह सही लेनदेन है किंतु मामला ऐसा नहीं होता है क्योंकि हैकर के लिए दूसरे को धोखा देना सर्वोपरि होता है।

उदाहरण के लिए कोई हैकर आई टी सपोर्ट तकनीशियन बनकर किसी टारगेट को कॉल कर सकता है। पीड़ित अपने कम्प्यूटर का लॉग-इन क्रिडेंशियल्स यह सोचकर सौंप सकता है कि उसे बदले में तकनीकी सहायता प्राप्त हो रही है। इसके बजाय हैकर अब पीड़ित के कम्प्यूटर का कंट्रोल अपने पास ले सकता है, इसमें मालवेयर लोड करके या शायद कम्प्यूटर से व्यक्तिगत सूचना लेकर पहचान की चोरी कर सकता है।

किसी वेबसाइट के यूआरएल से सावधान रहें। दुर्भावनापूर्ण वेबसाइट वास्तविक साइट की तरह दिख सकती है, लेकिन यूआरएल में स्पेलिंग में अंतर हो सकता है या भिन्न डोमेन (अर्थात् .com vs.net) का प्रयोग किया जा सकता है। सामान्यतया सभी सरकारी वेबसाइट में उनके नाम के अंत में gov.in या nic.in होता है। उदाहरण के लिए दुर्भावनापूर्ण वेबसाइट में वास्तविक नाम www.npa.gov.in के स्थान पर www.npagov.in या www.npa-gov.in का उपयोग किया जा सकता है।

9.6 किसी लिंक पर क्लिक करने के बजाय अपने ब्रोजर में यूआरएल टाइप करना सुरक्षित है। ई-मेल में लिंक पर जाने से नीचे वास्तविक यूआरएल

दिखाई देगा किंतु यहां भी चालाकी भरी जालसाजी आपको गलत जगह ले जा सकती है।

9.7 हैकर यह चाहता है कि आप पहले काम करें और बाद में सोचे। यदि किसी मैसेज में तात्कालिकता का भाव हो या काफी दबाव डाला जाता हो तो आशंकित हो जाएं; कभी भी तात्कालिकता से प्रभावित होकर सावधानीपूर्वक रिव्यू करना नहीं छोड़ें।

9.8 यदि आपको किसी विदेशी लॉटरी या स्विपस्टेक्स से ई-मेल, किसी अंजान रिश्तेदार से पैसे या किसी धनराशि के शेयर के लिए विदेश से कुछ धनराशि ट्रांसफर करने का अनुरोध प्राप्त होता है तो यह निश्चित रूप से घोटाला है और इसका जवाब नहीं दें और ऐसे ई-मेल को डिलीट कर दें।

9.9 यदि आपने किसी को अपना पासवर्ड बताया है तो उसे तुरंत बदल दें। यदि आपने कई रिसोर्सेस के लिए एक ही पासवर्ड का यूज किया है तो प्रत्येक एकाउंट के लिए इसे निश्चित रूप से बदलें तथा भविष्य में उस पासवर्ड का उपयोग न करें।

10. **शब्दावली**

शब्द	**परिभाषा**
डीडीओएस	डिस्ट्रिब्यूटेड डिनाएल ऑफ सर्विस (डीडीओएस) अटैक, कई स्रोतों से जोरदार ट्राफिक द्वारा ऑनलाइन सेवा को समाप्त करने का एक प्रयास है।
डीएचसीपी	डायनेमिक होस्ट कनफिगरेशन प्रोटोकॉल (डीएचसीपी), एक नेटवर्क मैंनेजमेंट प्रोटोकॉल है जिसका उपयोग यूडीपी/आई पी नेटवर्क पर किया जाता है। इसके द्वारा डीएचसीपी सर्वर किसी नेटवर्क पर प्रत्येक डिवाइस को डायनेमिक रूप से एक आई पी एड्रेस तथा अन्य नेटवर्क कनफिगरेशन पैरामीटर्स प्रदान करता है ताकि वे दूसरे आईपी नेटवर्क से संवाद कर सकें।
डिजीटल	डिजीटल हस्ताक्षर यह सुनिश्चित करने का एक तरीका है

हस्ताक्षर	कि कोई इलेक्ट्रॉनिक डाक्यूमेंट (ई-मेल, स्प्रेड शीट, टेक्स्ट फाइल आदि) प्रमाणिक है। प्रमाणिक से मतलब यह है कि आप यह जानते हैं कि यह डाक्यूमेंट किसने तैयार किया और उस व्यक्ति द्वारा तैयार किए जाने के बाद इसे किसी भी तरह बदला नहीं गया है।
डीएनएस	डोमेन नेम सिस्टम (डीएनएस) एक ऐसा तरीका है जिसमें इंटरनेट डोमेन नामों को इंटरनेट प्रोटोकॉल एड्रेसेस में लोकेट किया जाता है और ट्रांसलेट किया जाता है।
इनक्रिप्शन	इनक्रिप्शन किसी मैसेज या सूचना को इस प्रकार इनकोड करने की प्रक्रिया है कि केवल प्राधिकृत पक्ष ही उस तक पहुंच बना सके।
जीपीएस	ग्लोबल पोजिशनिंग सिस्टम (जीपीएस) एक अंतरिक्ष आधारित सेटेलाइट नेवीगेशन सिस्टम है जो स्थान तथा समय की सूचना प्रदान करता है।
एचटीटीपीएस	हाइपर टेक्स्ट ट्रांसफर प्रोटोकॉल ओवर सिक्योर सॉकेट लेअर एक यूआरएल स्कीम है जिसका उपयोग एक सुरक्षित एचटीटीपी कनेक्शन को दर्शाने के लिए किया जाता है।
आईएम	इंस्टेंट मैसेजिंग एक प्रकार की कम्यूनिकेशन सेवा है जिससे आप इंटरनेट पर रियल टाइम में कम्यूनिकेट करने के लिए दूसरे व्यक्ति के साथ एक प्रकार का प्राइवेट चैट रूम सृजित करने में समर्थ होते हैं।
आईओटी	इंटरनेट ऑफ थिंग्स (आईओटी) इंटरनेट के माध्यम से पहुंच योग्य कनेक्टेड आब्जेक्ट का एक ईको सिस्टम है।
मालवेयर	मालवेयर, मलेशियस सॉफ्टवेयर का छोटा नाम है और इसका उपयोग एक शब्द के रूप में वायरस, स्पाय वेयर, वॉर्म आदि के लिए किया जाता है।
एसएमएस	एसएमएस अधिकतर टेलिफोन, इंटरनेट और मोबाइल डिवाइस

	सिस्टम्स का टेक्स्ट मैसेजिंग सर्विस का कम्पोनेंट है।
एसएनएमपी	सिम्पल नेटवर्क मैनेजमेंट प्रोटोकॉल का उपयोग ऐसी स्थितियों, जिनके लिए एडमिनिस्ट्रेटिव का ध्यान आवश्यक होता है, के लिए नेटवर्क से जुड़े डिवाइस की मॉनीटरिंग करने हेतु नेटवर्क मैनेजमेंट सिस्टम में किया जाता है।
एसएसएच	सिक्योर शेल एक नेटवर्क प्रोटोकॉल है जिससे दो कम्प्यूटरों के बीच सिक्योर चैनल का उपयोग करके डाटा को एक्सचेंज किया जा सकता है।
एसएसआईडी	सर्विस सेट आइडेंटिफायर एक ऐसा नाम है जिसका उपयोग उस 802.11 वायरलेस लैन (एलएएन) विशेष को आइडेंटिफाई करने के लिए किया जाता है जिससे क्लाइंट अटैच होना चाहता है।
ट्रॉजन	ट्रॉजन हॉर्स वायरस नहीं है। यह एक डिस्ट्रक्टिव प्रोग्राम है जो वास्तविक अप्लीकेशन के रूप में दिखाई देता है। वायरस से हटकर, ट्रॉजन हॉर्स स्वयं को रेप्लिकेट नहीं करते हैं किंतु वे विनाशकारी हो सकते हैं। ट्रॉजन्स आपके कम्प्यूटर की बैकडोर इंट्री खोलते हैं जिससे दुर्भावनापूर्ण यूजर्स/प्रोग्राम्स को आपके सिटम्स तक पहुंच मिल जाती है जिससे गोपनीय और व्यक्तिगत सूचना की चोरी हो जाती है।
यूआरएल	यूनिफॉर्म रिसोर्स लोकेटर (यूआरएल) जिसे आम भाषा में वेब एड्रेस कहा जाता है, का संदर्भ वेब रिसोर्स से है जिसमें कम्प्यूटर नेटवर्क पर इसके लोकेशन और इसको रिट्राइव करने के लिए एक तंत्र विनिर्दिष्ट किया जाता है।
यूएसबी	यूनिवर्सल सिरीयल बस (यूएसबी) एक कॉमन इंटरफेस है जो डिवाइसेस तथा एक होस्ट कंट्रोलर जैसे कि किसी पर्सनल कम्प्यूटर के बीच कम्युनिकेशन को संभव बनाता है।
वायरस	वायरस एक ऐसा प्रोग्राम है जो आपके कम्प्यूटर में प्रवेश

	करने तथा आपकी फाइल्स/डाटा को क्षति पहुंचाने/बदलने तथा स्वयं को रेप्लिकेट करने के लिए लिखा जाता है।
वीपीएन	वर्चुअल प्राइवेट नेटवर्क किसी पब्लिक नेटवर्क में प्राइवेट नेटवर्क प्रदान करता है तथा यूजर्स को शेयर्ड या पब्लिक नेटवर्क में डाटा भेजने और प्राप्त करने के लिए समर्थ बनाता है, मानो कम्प्यूटिंग डिवाइस प्राइवेट नेटवर्क से सीधे जुड़ा हुआ हो।
वाईफाई सर्टिफाइड	वाईफाई सर्टिफाइड इन्टरऑपरेबलिटी, सिक्युरिटी, आसान इंस्टालेशन तथा रियलाइवलिटी के लिए 802.11 उद्योग मानकों के अनुसार उत्पादों का परीक्षण करने के लिए एक प्रोग्राम है।
वार्म्स	वॉर्म्स दुर्भावनापूर्ण प्रोग्राम है जो लोकल ड्राइव, नेटवर्क शेयर्स आदि पर स्वयं की बार-बार कॉपी करते हैं।

टिप्पणी :

- संदेह होने पर गृह मंत्रालय द्वारा जारी राष्ट्रीय सूचना सुरक्षा नीति और दिशानिर्देश (एनआईएसपीजी) को देखें।
- इस बुकलेट को तैयार करते समय समुचित सावधानी बरती गई है। यदि इसमें सुधार (सुधारों) के लिए कोई सुझाव देना चाहते हैं, तो इसे cyberdost@mha.gov.in पर साझा किया जा सकता है।

version 1.0)