साइबर स्वच्छता हैंडबुक

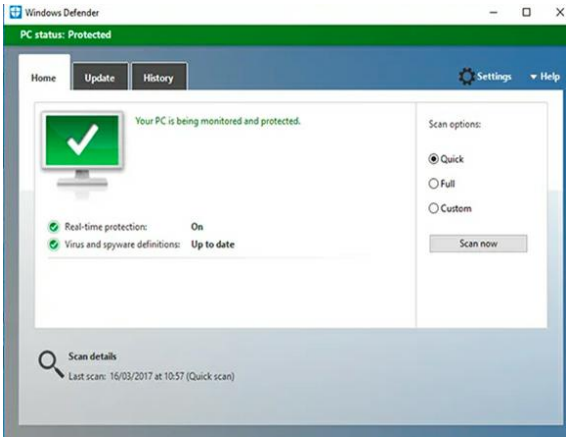
CYBER SAFE BENGAL

साइबर सुरक्षा उत्कृष्टता केंद्र (CS-CoE)
सूचना प्रौद्योगिकी और इलेक्ट्रॉनिक्स विभाग,
पश्चिम बंगाल सरकार
https://cscoe.itewb.gov.in

सामान्य कंप्यूटर उपयोग

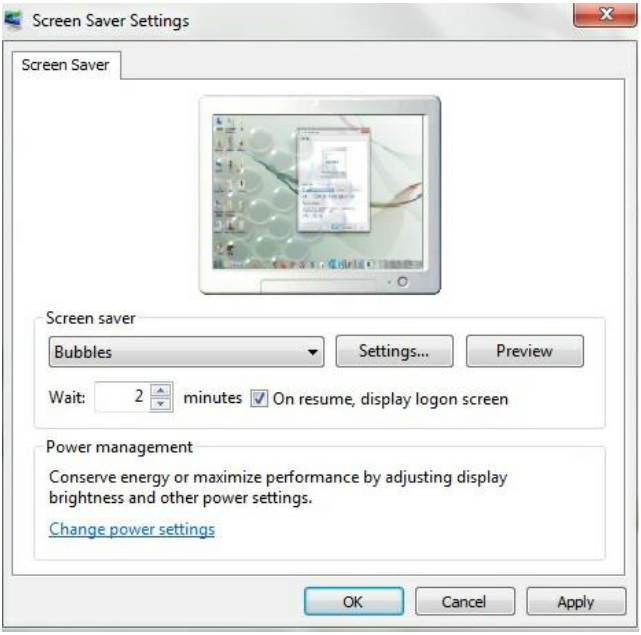
1. पासवर्ड की लंबाई अक्षरों, संख्याओं और विशेष वर्णों के संयोजन का उपयोग करके न्यूनतम 10 वर्ण होनी चाहिए।

2. एंटी-वायरस का उपयोग अनिवार्य है। एंटी-वायरस केवल डिवाइस विशिष्ट पेड लाइसेंस सॉफ्टवेयर अनुप्रयोग होना चाहिए। मुफ्त डाउनलोड के लिए उपलब्ध एंटी-वायरस सॉफ़्टवेयर इंस्टॉल नहीं किया जाना चाहिए।



3. अपने कंप्यूटर को हमेशा "Windows + L" या "Ctrl+Alt+Del" साथ अनुपयोगी छोड़ने पर लॉग-ऑफ करें।

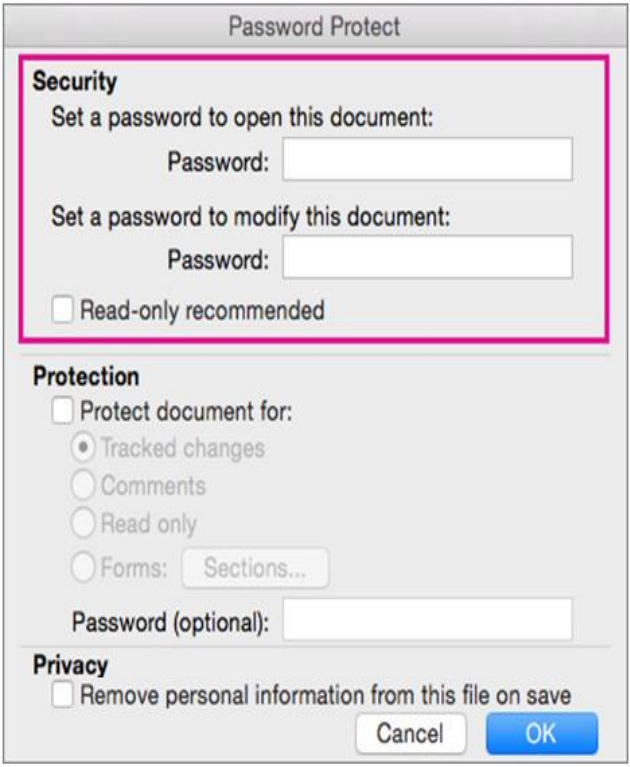
4. अधिकतम 2 मिनट की समयावधि के साथ स्क्रीनसेवर सक्षम होना चाहिए।



5. **वैध विश्वसनीय स्रोतों से भी, कहीं से भी अनावश्यक कार्यक्रम डाउनलोड न करें।**

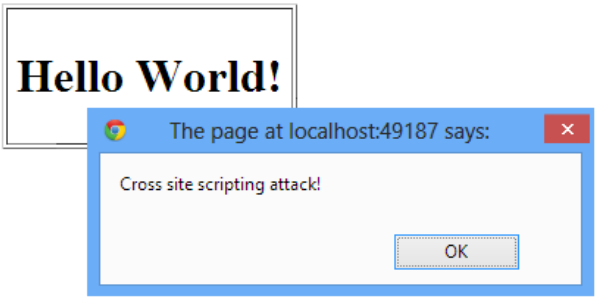
6. **कार्यालय के काम के लिए सार्वजनिक कंप्यूटर / साइबर कैफे का उपयोग न करें।**

7. **संवेदनशील दस्तावेजों के लिए पासवर्ड सुरक्षा लागू करें।**



इंटरनेट ब्राउज़िंग

8. यदि वे एक वैध स्रोत से प्रतीत होते हैं, तो भी अविश्वसनीय लिंक पर क्लिक न करें। उदाहरण के लिए, एयरलाइन टिकट बुकिंग पृष्ठ पर क्रिकेट स्कोर वेबसाइट के लिए कोई लिंक।



9. हमेशा https के हरे / ग्रे पैडलॉक किए गए प्रतीक की तलाश करें। पीला या लाल मतलब वेबसाइट असुरक्षित है।

10. टूर के समय, उन सेवाओं का उपयोग न करें जिनके लिए स्थान की जानकारी की आवश्यकता होती है।

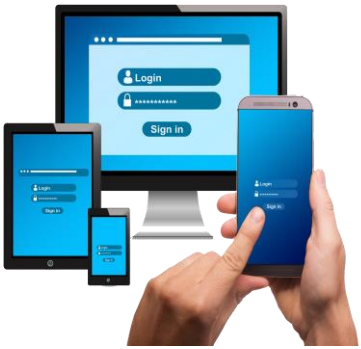
11. सार्वजनिक कंप्यूटर या सार्वजनिक वाई-फाई कनेक्शन का उपयोग करके कोई वित्तीय लेनदेन न करें। इसमें जोखिम है कि आपकी जानकारी को अनधिकृत लोगों द्वारा पढ़ा जा सकता है।

पासवर्ड प्रबंधन

12. दूसरों के सामने पासवर्ड डालते समय सावधानी बरतें। यदि आपको संदेह है कि कोई समझौता किया गया है, तो तुरंत अपना पासवर्ड बदलें।

13. आईटी टीम को संदिग्ध गतिविधियों (जैसे डेस्कटॉप पर धीमी गति / अज्ञात फाइल / अज्ञात स्रोतों द्वारा स्थापित सॉफ्टवेयर अनुप्रयोग) की रिपोर्ट करें।

14. पुराने पासवर्ड का पुन: उपयोग न करें। पुन: उपयोग किए गए पासवर्ड कुंजी-लॉग पैटर्न को देखने या सोशल इंजीनियरिंग के माध्यम से क्रैक करना आसान है।

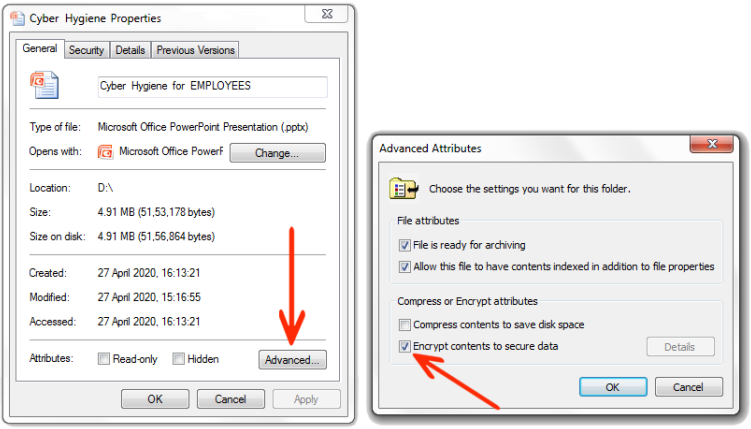


15. कंप्यूटर, नोटबुक, नोटिस बोर्ड आदि में पठनीय रूप में पासवर्ड स्टोर न करें।

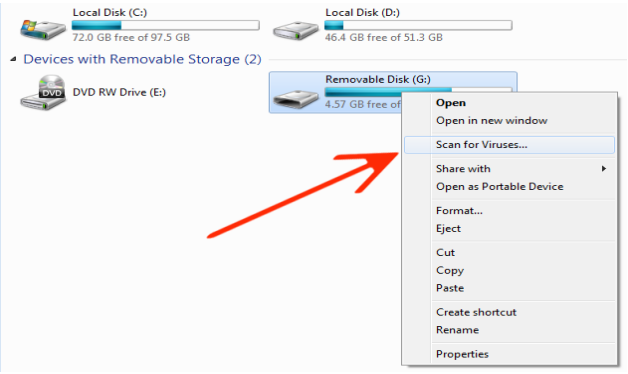
16. सामान्य पासवर्ड जैसे परिवार, पालतू जानवर, मित्रों का नाम, जन्मदिन आदि का उपयोग न करें।

हटाने योग्य सूचना भंडारण मीडिया

17. हटाने योग्य भंडारण मीडिया में कॉपी करने से पहले डेटा को एन्क्रिप्ट करने का प्रयास करें।



18. हमेशा एंटीवायरस के साथ सभी हटाने योग्य मीडिया को स्कैन करें।



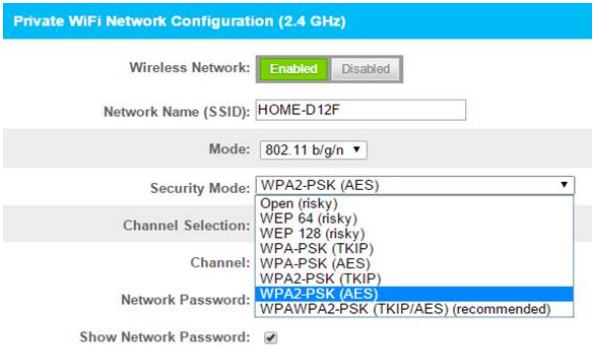
पब्लिक टर्मिनल

19. ऑनलाइन लॉग-इन या लेन-देन करते समय दूसरों को शोल्डर सर्फिंग करने न दें।

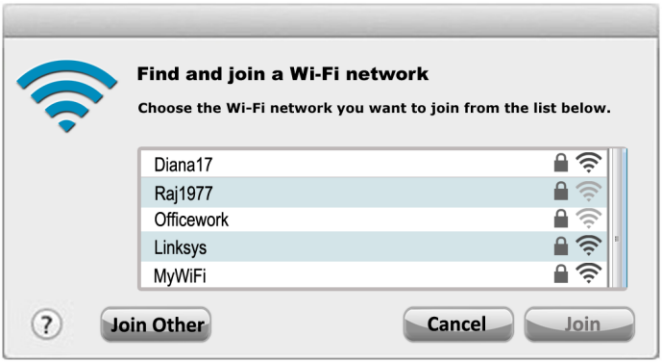
20. **डेस्क पर व्यक्तिगत या गोपनीय जानकारी वाली खुली फाइलें न रखें।**

वाई-फाई नेटवर्क

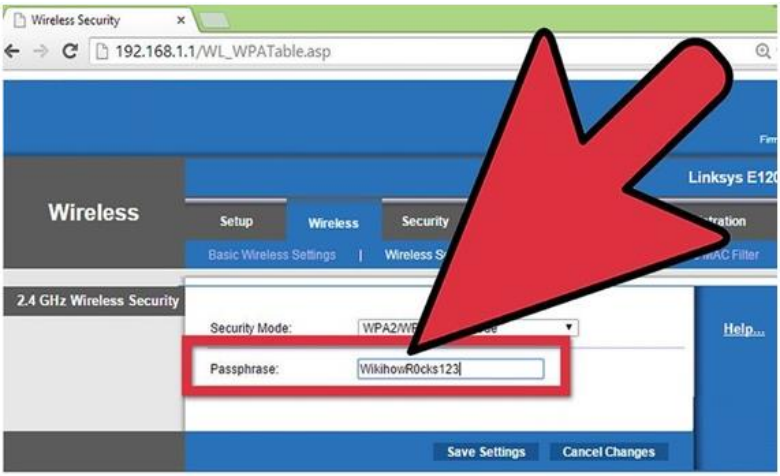
21. हमेशा वायरलेस राउटर / उपकरणों में WPA2 या उच्च एन्क्रिप्शन का उपयोग करें।



22. अपनी पहचान का खुलासा न करें, डिफ़ॉल्ट नेटवर्क डिवाइस नाम / SSID (सेवा सेट पहचानकर्ता) बदलें ।



23. नेटवर्क डिवाइस का डिफ़ॉल्ट पासवर्ड बदलें।



24. अनधिकृत पहुंच से बचने के लिए मैक आईडी फिल्टर को सक्रिय करें।

सोशल मीडिया का उपयोग

25. सभी कर्मचारी, संविदा कर्मचारी, सलाहकार, साझेदार, तीसरे पक्ष के कर्मचारी आदि जो सरकारी कार्यालयों में में या सरकारी परियोजनाओं पर काम कर रहे हैं। सोशल मीडिया पोर्टल या एप्लिकेशन पर आधिकारिक जानकारी का खुलासा कभी नहीं करें

सोशल इंजीनियरिंग हमलों को रोकने

26. अविश्वसनीय फोन कॉल, मीटिंग या ईमेल संदेशों पर किसी भी आधिकारिक जानकारी का खुलासा करने से बचें। हमलावर अक्सर डेटा को भंग करने के लिए गोपनीय आधिकारिक जानकारी हासिल करने के खुद को असली लोगों के रूप में दिखाने की कोशिश करते हैं।

27. फ़िशिंग हमलों से बचें - अविश्वसनीय ईमेल न खोलें। ईमेल अटैचमेंट न खोलें जो किसी आधिकारिक संचार के लिए प्रासंगिक न हों। यदि कोई संदेश या ईमेल तात्कालिकता की भावना व्यक्त करता है या उच्च दबाव रणनीति लागू करने के लिए लगता है फिर वह

लिंक को खोलने या क्लिक करने से सावधान रहें।

28. जब तक स्रोत पूरी तरह से सत्यापित और विश्वसनीय नहीं हो जाता, तब तक वशीकरण हमलों से बचें - फोन कॉल पर किसी भी संवेदनशील जानकारी को प्रकट न करें। कुछ सत्यापन योग्य गुप्त जानकारी के लिए पूछे जैसे कि तत्काल वरिष्ठ का नाम (यदि कॉलर खुद को किसी अन्य सरकारी विभाग के अधिकारी के रूप में प्रस्तुत करता है)। किसी भी महत्वपूर्ण जानकारी का खुलासा करने से पहले फोन करने वाले की पहचान के रूप में एक पूर्ण आश्वासन प्राप्त करने का प्रयास करें।

29. हनी ट्रैप्स / क्विड प्रो क्वो स्कैम से सावधान रहें, जहां हमलावर वास्तविक व्यक्ति के रूप में पोज देते हैं और डेटा चोरी के प्रयास को उचित संचार की तरह प्रतीत होते हैं।

30. अनजान उत्तराधिकार, विदेशी लॉटरी, विदेशी देश से फंड ट्रांसफर अनुरोध आदि के बारे में फोन कॉल / ईमेल / एसएमएस से बचें, ये कुछ पैसे या जानकारी प्राप्त करने के लिए किये गए घोटाले के उदाहरण हैं।

कुछ और डोमेन विशिष्ट उपयोग जागरूकता दिशा-निर्देश:

सामान्य कंप्यूटर उपयोग

1. स्क्रीन पर संवेदनशील जानकारी अगर उपलब्ध हो तो कंप्यूटर को पहुंच के बाहर न रखें।
2. अपने कंप्यूटर को हमेशा "**Windows + L**" या " **Ctrl + Alt + Del** " के साथ अनुपलब्ध छोड़ते समय लॉक करें।
3. अनावश्यक कार्यक्रम डाउनलोड न करें।
4. कार्यालय के काम के लिए सार्वजनिक कंप्यूटर / साइबर कैफे का उपयोग करने से बचें।
5. किसी भी कारण से सार्वजनिक कंप्यूटर पर डाउनलोड किए गए सभी दस्तावेजों को " **Shift+Delete** " के साथ हटा दिया जाना चाहिए।

सामान्य इंटरनेट ब्राउजिंग

6. हमेशा पूर्व-स्थापित या अनुमोदित और अद्यतन किए गए वेब-ब्राउज़र का उपयोग करें।
7. इंटरनेट से जुड़ी किसी भी प्रणाली पर किसी भी जानकारी को संग्रहीत / साझा न करें।

8. ब्राउज़र द्वारा दिए गए "पासवर्ड सहेजें" विकल्प का चयन न करें।
9. ब्राउज़ करते समय, पॉपअप ब्लॉकर को अक्षम करने से बचें / हमेशा ब्राउज़र में पॉपअप ब्लॉकर चालू करें।
10. सार्वजनिक कंप्यूटर और सार्वजनिक वाई-फाई (Wi-Fi) कनेक्शन का उपयोग करके वित्तीय लेनदेन न करें।

पासवर्ड प्रबंधन

11. अक्षरों, संख्याओं और विशेष वर्णों के संयोजन का उपयोग करके 10 वर्णों की न्यूनतम लंबाई के साथ मजबूत पासवर्ड बनाएं।
12. विभिन्न खातों के लिए अलग-अलग पासवर्ड का उपयोग करें। यदि एक पासवर्ड हैक हो जाता है, तो आपके अन्य खातों से समझौता न हो।
13. यदि आपको संदेह है कि कोई समझौता किया गया है, तो तुरंत अपना पासवर्ड बदलें।
14. हमेशा "पासवर्ड याद रखें" के उपयोग को अस्वीकार करें।

हटाने योग्य सूचना संग्रहण मीडिया

15. हटाने योग्य मीडिया को बिना अनुमति के कार्यालय से बाहर न निकालें।

16. उपयोग के बाद हटाने योग्य मीडिया की सामग्री को मिटा दें / हटा दें।

सार्वजनिक टर्मिनल

17. सभी ब्राउज़रों को बंद किए बिना और सार्वजनिक कंप्यूटर से लॉग आउट किए बिना न निकलें।

वाई-फाई नेटवर्क

18. वायरलेस डिवाइस के फर्मवेयर को नियमित रूप से अपडेट करें।
19. अनधिकृत पहुंच से बचने के लिए राउटर में दूरस्थ प्रबंधन सुविधा को अक्षम करें।

सामाजिक इंजीनियरिंग हमलों को रोकना

20. अविश्वसनीय URL पर क्लिक न करें। किसी भी लिंक को खोलने से पहले URL आइकन की प्रमाणपत्र वैधता की जांच करें।
21. यदि कोई संदेश एवं ईमेल तात्कालिकता की भावना व्यक्त करता है, या उच्च दबाव बिक्री रणनीति लागू करने के लिए लगता है, तो अपने लिंक / अनुलग्नक को खोलने या क्लिक करने में सावधानी बरतें।

22. अज्ञात विरासत, विदेशी लॉटरी, विदेशी देश से फंड ट्रांसफर के अनुरोध आदि के बारे में फोन कॉल / ईमेल / एसएमएस से बचें।
23. किसी भी उद्देश्य के लिए किसी के सामने आने पर तुरंत अपना पासवर्ड बदलें।

सामाजिक इंजीनियरिंग हमलों को रोकना

24. सुनिश्चित करें कि आपके मोबाइल / कंप्यूटर में एंटी-वायरस इन्सटाल्ड हो।
25. कभी भी किसी के सामने अपने मोबाइल / नेट-बैंकिंग से संभंधित गुप्त जानकारी का खुलासा न करें।
26. हमेशा अधिक सुरक्षित और गैर-अनुमानित पासवर्ड का ही उपयोग करें जिसमें अक्षर, संख्या और विशेष वर्ण शामिल हो।
27. अपने नेट-बैंकिंग खाते में प्रवेश करने के लिए हमेशा वर्चुअल की-पैड का उपयोग करें।
28. मोबाइल बैंकिंग के लिए - सुनिश्चित करें कि आप अपने बैंक के केवल सत्यापित मोबाइल बैंकिंग एप्लिकेशन को ही डाउनलोड कर रहे है।
29. मोबाइल बैंकिंग के लिए आम पिन सेट न करें क्यूंकि उसका आसानी से अनुमान लगाया जा सकता है।

30. अनचाहे ईमेल पते से फ़िशिंग ईमेल के बारे में पता करने की कोशिश करे और सतर्क रहे।
31. सुनिश्चित करें कि पैडलॉक " **https** " प्रतीक "सुरक्षित" और हरा हो - एम्बर या लाल रंग का नहीं।
32. नेट-बैंकिंग पर लॉगिन के लिए सार्वजनिक वाई-फाई का उपयोग न करें।
33. नेट बैंकिंग पर लॉगिन के लिए इंटरनेट कैफे या सार्वजनिक कंप्यूटर का उपयोग न करें।
34. किसी भी घोखाधघड़ी लेनदेन के बारे में पता चलने पर, तुरंत कॉल और ईमेल के माध्यम से बैंक को रिपोर्ट करें।

ई-मेल का सुरक्षित उपयोग

35. अपने ई-मेल लॉगिन क्रेडेंशियल किसी के साथ साझा न करें।
36. सार्वजनिक / बहु-उपयोगकर्ता प्रणालियों का उपयोग करते समय सुनिश्चित करें कि आप हमेशा सिस्टम छोड़ने से पहले लॉग आउट कर चुके हो।
37. पासवर्ड सर्वोत्तम प्रथाओं का पालन करें - (बिंदु 6 ऊपर)
38. हमेशा न केवल नाम के माध्यम से बल्कि ईमेल पते के माध्यम से भी प्रेषक को सत्यापित करें।
39. यदि ई-मेल पता संदेहास्पद या गैर-भरोसेमंद प्रतीत होता है, तो किसी भी अनुलग्नक या लिंक पर क्लिक न करें।

40. किसी भी लिंक पर क्लिक न करें जो आपको लॉटरी जीतने या लावारिस विरासत का वादा कर रहा हो।
41. अपने क्रेडिट या डेबिट कार्ड का विवरण कभी किसी से सांझा न करें; या ई-मेल के माध्यम से किसी को भी नेट-बैंकिंग का विवरण न दे।

सोशल मीडिया का सुरक्षित उपयोग

42. हमेशा प्रत्येक प्लेटफ़ॉर्म के लिए केवल एक सोशल मीडिया अकाउंट का उपयोग करें (जैसे, व्हाट्सएप, फेसबुक, ट्विटर, इंस्टाग्राम, गूगल प्लस, आदि)
43. अपने लॉगिन क्रेडेंशियल किसी के साथ साझा न करें।
44. केवल उन व्यक्तियों को जोड़ें और उनसे संवाद करें जिन्हें आप सोशल मीडिया प्लेटफॉर्म के माध्यम से सोशल मीडिया के बाहर जानते हैं।
45. सोशल इंजीनियरिंग के माध्यम से जानकारी निकालने के लिए कई सोशल मीडिया प्रोफाइल वास्तव में नकली हो सकते हैं।
46. सोशल मीडिया मैसेंजर या चैट सेवाओं के माध्यम से अपने-आप और दूसरों की किसी भी संवेदनशील व्यक्तिगत / निजी जानकारी का संचार न करें।

47. विपरीत लिंग के आकर्षक प्रोफाइलों के बारे में जागरूक रहें, उनका मतलब आपको निजी जानकारी देने के लिए लालच देना हो सकता है - सत्यापन के बिना ऐसे प्रोफाइल को जोड़ना और संवाद करना उचित नहीं हैं।

सोशल मीडिया के माध्यम से फर्जी खबरों का प्रसारण

48. फर्जी खबरों और छवियों के प्रचार के लिए सोशल मीडिया प्लेटफॉर्म का लगातार इस्तेमाल किया जा रहा है।
49. सोशल मीडिया द्वारा प्राप्त किसी भी छवि / वीडियो या समाचार को तब तक सच न मानें जब तक कि अन्यस्रोतों द्वारा वास्तविकता को सत्यापित नहीं किया गया हो।
50. व्हाट्सएप और फेसबुक के माध्यम से फर्जी समाचारों के वायरल प्रसार के कारण "सार्वजनिक आक्रोश" की विभिन्न वांछनीय घटनाएं हुई हैं।
51. किसी भी विवादास्पद छवि / वीडियो / समाचार को उसकी वास्तविकता की पुष्टि किए बिना अग्रेषित न करें अन्यथा आप आपराधिक रूप से उत्तरदायी हो सकते हैं।

क्रेडिट और डेबिट कार्ड का सुरक्षित उपयोग

52. अपना क्रेडिट / डेबिट कार्ड नंबर, CVV कोड या पिन किसी के साथ साझा न करें।

53. ऑनलाइन भुगतान करते समय, सुनिश्चित करें कि हरे पैडलॉक और।. प्रतीक सक्रिय और मान्य हो । किसी भी असत्यापित वेबसाइट / एप्लिकेशन या पोर्टल में कार्ड विवरण दर्ज करने से बचे।
54. एटीएम **(ATM)** या पीओएस मशीनों **(POS Machine)** में कार्ड का उपयोग करते समय, सुनिश्चित करें कि कार्ड के उपयोग किये जा रहे उपकरणो से छेड़छाड़ नहीं की गई हो ।
55. डेबिट या क्रेडिट कार्ड का उपयोग करने पर अपने बैंकों के दिशानिर्देशों को हमेशा पढ़ें और उनका पालन करें।
56. किसी भी घोखाधड़ी लेनदेन के बारे में पता चलने पर, तुरंत कॉल और ईमेल के माध्यम से बैंक को रिपोर्ट करें।
57. कॉल, ईमेल या किसी अन्य माध्यम से किसी को भी अपना कार्ड पिन या सी-वी-वी नंबर **(CVV number)** साझा न करें, भले ही कोई कहे कि वे बैंक पोस्ट सेंटर से हैं।
58. अपने कार्ड की किसी भी छवि को किसी के साथ साझा न करें - कहीं भी स्टोर न करें।
59. लेन-देन के लिए कभी भी किसी भी कागज के टुकड़े में अपना कार्ड पिन न लिखें - न ही कहीं भी किसी के लिए खुलासा करें।

60. कार्ड के नुकसान या चोरी के मामले में तुरंत अवरुद्ध करने के लिए बैंक को रिपोर्ट करें और पुलिस को जल्द से जल्द रिपोर्ट करें।

<u>लैपटॉप/मोबाइल उपकरणों का सुरक्षित उपयोग</u>

61. हमेशा वास्तविक विक्रेता सॉफ़्टवेयर और ऑपरेटिंग सिस्टम का उपयोग करें।
62. हमेशा अपने लैपटॉप / मोबाइल डिवाइस के लिए पासवर्ड सुरक्षा का उपयोग करें।
63. हमेशा लाइसेंस प्राप्त एंटी-वायरस सॉफ़्टवेयर का उपयोग करें।
64. अविश्वसनीय स्रोतों से कोई सॉफ्टवेयर डाउनलोड न करें।
65. कोई भी एप्लिकेशन या सॉफ्टवेयर ऐसा न रखें जिसका आप नियमित रूप से उपयोग नहीं करते हैं।
66. किसी को भी, विशेषकर अविश्वासी लोगों को अपने फोन / लैपटॉप का उपयोग करने के लिए न दें।
67. अपने लैपटॉप / मोबाइल को नियमित रूप से वायरस स्कैन करते रहे।
68. सुनिश्चित करें कि आपके द्वारा उपयोग किए जा रहे एप्लिकेशन / सॉफ़्टवेयर के सभी सॉफ़्टवेयर अपडेट होते रहे।

इंटरनेट संसाधनों का सुरक्षित और स्वीकार्य उपयोग

69. वेब ब्राउजिंग के लिए हमेशा विश्वसनीय ब्राउजर जैसे गूगल क्रोम, मोजिला फायरफॉक्स, इंटरनेट एक्सप्लोरर आदि का उपयोग करें।
70. किसी भी अविश्वसनीय / अवैध वेब-साइटों पर न जाएं।
71. वास्तविक सॉफ्टवेयर की पुष्टि किए बिना किसी भी अवांछित डाउनलोड लिंक पर क्लिक न करें।
72. हमेशा वास्तविक https और हरे रंग के पैडलॉक की जांच करें ताकि यह सुनिश्चित हो सके कि आपको नकली वेबसाइट पर फिर से निर्देशित नहीं किया जा रहा है।
73. टोरेंट का उपयोग न करें या अवैध सामग्री डाउनलोड न करें - यह एक कानूनन अपराध है।
74. हमेशा सुनिश्चित करें कि आप सार्वजनिक कंप्यूटर का उपयोग करते समय अपनी ब्राउज़िंग सामग्री को बंद रखे या हटा दें।

साइबर अपराध से संबंधित जागरूकता

साइबर पहचान की चोरी और साइबर प्रतिरूपण

अपराध और सजा -

75. किसी और के नाम पर फर्जी अकाउंट बनाना या किसी और के लॉग-इन क्रेडेंशियल्स का दुरुपयोग करना।
76. यह सूचना प्रौद्योगिकी अधिनियम, 2000 की घारा 66 सी और 66 डी के तहत अपराध है।
77. इस तरह के अपराध को करने के लिए 3 साल की जेल और 3 लाख रुपये के जुर्माने का प्रावधान है।

कैसे बचें (सार्वजनिक जानकारी) -

78. पासवर्ड सर्वोत्तम प्रथाओं का पालन करें।
79. फ़िशिंग ईमेल की पहचान करें और फ़िशिंग से बचें।
80. सुरक्षित नेट-बैंकिंग / मोबाइल बैंकिंग प्रथाओं का उपयोग करें।
81. यह सुनिश्चित करें कि क्रेडिट / डेबिट कार्ड का पिन गुप्त रखा जाये।

82. सोशल मीडिया का सुरक्षित तरीके से उपयोग करें।

अश्लील या यौन रूप से स्पष्ट कंटेंट भेजना और प्रकाशित करना

क्या अपराध और सजा शामिल है –

83. **सूचना प्रौद्योगिकी अधिनियम, 2000** की **धारा 67** और **धारा 67-A** के तहत अपराध है
84. **धारा 67** के तहत, अश्लील कंटेंट को प्रकाशित या प्रसारित करने के लिए - 5 लाख रुपये तक के जुमनि के साथ 3 साल की कैद का प्रावधान है।
85. **धारा 67-A** के तहत, यौन रूप से स्पष्ट कंटेंट को प्रकाशित या प्रसारित करने के लिए - 10 लाख रुपये तक के जुमनि के साथ 5 साल की कैद का प्रावधान है।

कैसे बचें (सार्वजनिक जानकारी) –

86. किसी को कोई भी अपमानजनक, अपमानजनक या अश्लील संदेश न भेजें जो किसी व्यक्ति या लोगों के समूह पर नकारात्मक प्रभाव डाल सकता है।

87. किसी भी व्हाट्सएप ग्रुप, मैसेंजर इत्यादि के साथ किसी भी प्रकार की यौन स्पष्ट कंटेंट को प्रसारित न करें। यदि ऐसा कोई संदेश प्राप्त होता है, तो तुरंत हटा दें, ताकि अनजाने में फॉरवर्डिंग की कोई गुंजाइश न हो।
88. सुरक्षित ब्राउज़िंग आदतों का पालन करें।

बिना किसी व्यक्ति की निजी क्षेत्र की छवि को कैप्चर, प्रकाशित और प्रसारित करने के माध्यम से गोपनीयता का उल्लंघन करना

89. **सूचना प्रौद्योगिकी अधिनियम, 2000** की **धारा 66-E** के तहत अपराध है।
90. इस अपराध 3 साल की कैद और 2 लाख रुपए जुर्माने में प्रावधान है।
91. चाइल्ड पोर्नोग्राफी - यौन शोषण, वीडियो क्लिप बनाना, प्रकाशित करना, किसी भी तरह से इनका प्रसारण या सुविधा प्रदान करना, 18 वर्ष से कम उम्र के किसी भी व्यक्ति - **सूचना प्रौद्योगिकी अधिनियम, 2000** की **धारा 67-B** के तहत एक अपराध है।
92. **धारा 67-B** में पहले उदाहरण के लिए 5 साल की कैद और 10 लाख रुपए के जुर्माने का प्रावधान है,

जो कि बार-बार अपराध करने पर 7 साल की कैद और 10 लाख रुपए के जुर्माने तक जा सकता है।

कैसे बचें -

93. किसी भी इलेक्ट्रॉनिक उपकरणो का प्रयोग करके, अपने आप को / या किसी और को अपनी निजी छवियों पर कब्जा करने की अनुमति न दें।
94. किसी पर भी शारीरिक रूप से निजी स्थान पर कब्जा न करें।
95. सार्वजनिक स्थानों जैसे कि रिटेल स्टोर या मॉल के ट्रायल रूम में संभावित कैमरों से अवगत रहें।
96. किसी पर भी भरोसा न करें - अपनी निजी छवियों / वीडियो को कैप्चर करने के लिए I कोई फर्क नहीं पड़ता कि कितना अंतरंग है।

साइबर आतंकवाद से भारत की एकता, अखंडता, सुरक्षा या संप्रभुता को खतरा

97. **साइबर आतंकवाद सूचना प्रौद्योगिकी अधिनियम, 2000** की धारा **66-F** के तहत अपराध है। यह आजीवन कारावास के साथ दंडनीय है।

98. साइबर आतंकवाद जैसा कि नाम से पता चलता है- कंप्यूटर संसाधनों (मोबाइल फोन सहित) से संबंधित एक गतिविधि है, जो नेतृत्व कर सकता है -
    a. किसी भी व्यक्ति की मृत्यु या उसे घायल करने के लिए।
    b. महत्वपूर्ण सार्वजनिक सेवाओं के विघटन के लिए।
    c. किसी भी विदेशी राज्य के साथ इस देश के संबंधों को नकारात्मक रूप से प्रभावित कर सकता है।
    d. राष्ट्रीय सुरक्षा एवं अखंडता या संप्रभुता को नुकसान पहुंचा सकता है।

<u>नागरिकों के लिए जागरूकता योजना</u>

99. किसी भी संदिग्ध साइबर गतिविधि को लेकर सतर्क रहें जिससे देश और समाज की एकता और अखंडता को खतरा हो सकता है।

<u>अनुमोदकों और मध्य स्तर के अधिकारियों के लिए साइबर सर्वोत्तम प्रथाएं:</u>

1. सभी वर्गीकृत कार्य स्टैंडअलोन कंप्यूटर पर किए जाने चाहिए।

2. सभी महत्वपूर्ण जानकारी और फ़ाइलों का बैकअप लें।

3. दूरस्थ खातों से दूरस्थ पहुँच या फ़ाइल साझाकरण को सक्षम न करें।

4. सुरक्षित फ़ाइल शुद्धिकरण के लिए सुरक्षित विलोपन सॉफ़्टवेयर का उपयोग करें।

5. सार्वजनिक कंप्यूटर पर निजी ब्राउज़िंग मोड का उपयोग करें

6. गूगल ड्राइव, ड्रॉपयबॉक्स, आई-क्लाउड आदि जैसी निजी क्लाउड सेवाओं पर जानकारी संग्रहीत न करें।

7. केवल संगठन द्वारा हटाए जाने योग्य संग्रहण मीडिया पर जानकारी स्टोर करें।

8. सार्वजनिक कंप्यूटर का उपयोग करने के लिए आवश्यकता अनुसार हमेशा रिबूट करें।

9. उपयोग के बाद कैशे फ़ाइलों को हटा दे।

10. वायरलेस डिवाइस के फर्मवेयर को नियमित रूप से अपडेट करें।

11. अनधिकृत पहुंच से बचने के लिए राउटर में दूरस्थ प्रबंधन सुविधा को लागू करें।

सिस्टम और नेटवर्क प्रशासकों के लिए साइबर सर्वोत्तम प्रथाएं:

1. व्यवस्थापक लॉगिन को खाता प्रबंधन के माध्यम से प्रतिबंधित किया जाना चाहिए।
2. सभी सिस्टम पर नियमित रूप से सॉफ़्टवेयर पैचेज अपडेट करें।
3. व्यवस्थापक कार्यों या गतिविधियों के लिए अंतर्निहित विंडोज व्यवस्थापक खातों का उपयोग न करें।
4. सेवा खातों के रूप में सामान्य उपयोगकर्ता खातों का उपयोग न करें।
5. सिस्टम को रिबूट न करें यदि -
    a. आप नहीं जानते कि इस पर किसने लॉग इन किया है?
    b. आप सिस्टम मॉनिटर को निलंबित नहीं करते हैं?
6. सभी महत्वपूर्ण प्रणालियों के नियमित बैकअप लें।
7. किसी भी त्रुटि और चेतावनियों के लिए नियमित रूप से अपनी लॉग फाइल की जाँच करें, ताकि खतरा बनने से पहले वे आपको समस्याओं के प्रति सचेत कर सकें।
8. यू-पी-एस **(UPS)** या महोर्मि रक्षक के माध्यम से बिजली की आपूर्ति को नियंत्रित किया जाना चाहिए।
9. घूल भरे वातावरण में कंप्यूटर सिस्टम स्थापित न करें।
10. मजबूत सुरक्षा प्रोटोकॉल्स और नीतियों को लागू करें।

11. हमेशा " छुपी हुई फाइल्स एवं फ़ोल्डर्स दिखाएं" के साथ कंप्यूटर में विकल्पों को लागू करें।

12. उचित प्रलेखन के साथ एक कार्यप्रवाह प्रक्रिया को लागू करें।

13. सभी सिस्टम परिवर्तन केवल प्रलेखित अनुमोदन के आधार पर होना चाहिए।

14. उन कार्यों को न करें जो समय पर पूरे नहीं हो सकते हैं - शुक्रवार की दोपहर के टास्क से सावधान रहें।

15. नियमित सुरक्षा ऑडिट और टेस्ट करें।

16. लगातार अपने नेटवर्क एवं उपकरणों को अपडेट और पैच करें।

17. डाउनलोड किए गए सॉफ़्टवेयर ऍप्लिकेशन्स के लिए ऑटो रन / ऑटो प्ले सुविधा को लागू करें।

18. नीतियां एवं प्रक्रियाएं बनाएं और लागू करें:

a. मोबाइल डिवाइस सुरक्षा नीति,
b. कंप्यूटर उपयोग नीति,
c. सामाजिक मीडिया नीति,
d. पासवर्ड नीति,
e. ईमेल नीति,
f. कम से कम विशेषाधिकार सुरक्षा नीति,
g. व्यापार निरंतरता (BCP) योजना, तथा
h. डाटा बैकअप और डिजास्टर रिकवरी (DR) प्लान

19. उपयोगकर्ताओं को याद दिलाएं कि वो कठिन और असामान्य पासवर्ड का ही प्रयोग करे जिनका अनुमान आसानी से न लगाया जा सके।

20. गैर-व्यवस्थापक उद्देश्यों के लिए अपने व्यवस्थापक खाते का उपयोग न करें।

21. पासवर्ड प्रोटेक्शन की दया पर अपना नेटवर्क मत छोड़ो।

22. सुनिश्चित करें कि सभी कर्मचारियों द्वारा नियमित रूप से साइबर सुरक्षा अपडेटस प्राप्त किए जाएं।

23. वायरस-अपडेटेड रहें। सर्ट-इन एडवाइजरी का पालन करके नए कारनामों और हैकर के हमलों के बारे में लगातार बुलेटिन प्राप्त करते रहे।

24. अपने ई-मेल प्रोग्राम को "ऑटो ओपन" अटैचमेंट की अनुमति न दें।

॥ सुरक्षित रहे ॥

https://cscoe.itewb.gov.in

© प्रथम संस्करण प्रकाशित 2020

© दूसरा संस्करण प्रकाशित 2021

साइबर सिक्योरिटी सेंटर ऑफ़ एक्सेलन्स
वेबेल भवन ग्राउंड फ्लोर ब्लॉक – EP & GP
सेक्टर – V, बिधाननगर
साल्ट लेक, कोलकाता - 700156
फ़ोन नंबर – 033 2357-5218
ईमेल – cscoe@wb.gov.in