शुद्धिकरण

कक्षा 12

कम्प्यूटर-अध्ययन

माध्यम : हिन्दी

गुजरात सरकार तथा गुजरात माध्यमिक और उच्चतर माध्यमिक शिक्षण बोर्ड की सूचनानुसार वर्ष 2021 से प्रकाशित हो रही इस पाठ्यपुस्तक की आवृत्ति में प्रकरण-5 के अंत में 'साइबर सुरक्षा, उसके खतरे तथा उससे बचाव के उपाय' से संबंधित कुछ अतिरिक्त जानकारी दी गई है। वर्तमान में इंटरनेट के बढ़ते उपयोग ने 'साइबर बॉलिंग' (Cyber Bullying), 'साइबर ग्रूमिंग' (Cyber Grooming) और 'ऑनलाइन गेमिंग' (Online Gaming) से उत्पन्न कुछ खतरों को जन्म दिया है। उससे सुरक्षित रहने के उपायों की चर्चा यहाँ की गई है, साथ ही स्वाध्याय में भी तत्संबंधी प्रश्नों का भी समावेश किया गया है।

तमसो मा ज्योतिर्गमय

गुजरात राज्य शाला पाठ्यपुस्तक मंडल

गांधीनगर

सायबर सुरक्षा, उसके खतरे तथा उसके बचाव के उपाय

इंटरनेट का उपयोग करते समय बच्चों द्वारा सामना किए जानेवाले मुद्दे

आजकल हम इंटरनेट आधारित बहुत सारी गतिविधियाँ करते हैं, इन गतिविधियों को साइबर गतिविधियों के रूप में जाना जाता है। साइबर गतिविधियों से कई बार अज्ञात संकट भी आते हैं। लंबे समय तक साइबर गतिविधि में शामिल दो पक्ष एक-दूसरे को नहीं जानते हैं। यह कई बार समस्याएँ उत्पन्न करता है, विशेष रूप से अगर इंटरनेट का उपयोग करनेवाला व्यक्ति बच्चा हो। जिन मुद्दों को यहां चर्चा की जानी चाहिए, उनमें से कुछ साइबर बुलिंग (Cyber Bullying), साइबर ग्रूमिंग (Cyber Grooming) और ऑनलाइन गेमिंग (Online Gaming) हैं।

साइबर बुलिंग (परेशान करना):

साइबर बुलिंग शब्द, दो शब्दों साइबर और बुलिंग के संयोजन से बनाया गया है। बुलिंग शब्द आम तौर पर उस व्यक्ति या पीड़ित के लिए उपयोग किया जाता है,जो आसानी से उसका या खुद का बचाव नहीं कर सकता है वह जिसके खिलाफ एक व्यक्ति या समूह के द्वारा बार-बार जानबूझकर आक्रामक कार्य किए गए हों। साइबर बुलिंग वर्चुअल हरैसमेंट का एक रूप है। यह किसी भी इलेक्ट्रॉनिक उपकरण जैसे स्मार्टफोन, टैबलेट या कंप्यूटर के उपयोग के माध्यम से लागू किया जाता है। आमतौर पर साइबर बुलिंग सोशल मीडिया, चैट रूम और गेमिंग प्लेटफॉर्म पर होती है। लोग सामग्री साझा करने या अन्य लोगों से जुड़ने के लिए इन प्लेटफार्मों का उपयोग करते हैं।

साइबर बुलिंग के कुछ सामान्य प्रकार निम्नानुसार हैं:

- ऑनलाइन माध्यम का उपयोग करते हुए ऐसी धमकी देना जो स्वयं किसी व्यक्ति को या दूसरों को हानि पहुँचाने के लिए उकसा सकता है, गैरकानूनी गतिविधियाँ कर सकता है या किसी पर कार्रवाई करने के लिए दबाव डाल सकता है जो करने का इरादा वह नहीं रखते हैं।
- किसी व्यक्ति, समुदाय या संगठन की टिप्पणियों, फ़ोटो या वीडियो को पोस्ट करें जो अपमानजनक, शर्मनाक और बुरा है।
- किसी व्यक्ति, समुदाय या संगठन का फर्जी वेबपेज बनाना जो अपमानजनक, शर्मनाक और बुरा हो।
- किसी व्यक्ति के बारे में व्यक्तिगत या नकली जानकारी मांगने या पोस्ट करने के लिए ऑनलाइन पहचान करना।

ऑनलाइन माध्यम की विशाल पहुंच के साथ कुछ स्थितियों से बचना मुश्किल हो जाता है। निम्नलिखित चरणों का उपयोग करके साइबर बुलिंग को कुछ हद तक रोका जा सकता है:

- अपने दोस्तों, शिक्षकों और परिवार के साथ हमेशा साइबर बुलिंग के बारे में बात करें।
- इंटरनेट पर प्रकटीकरण के लिए कौन-सी व्यक्तिगत जानकारी उपयुक्त है, यह तय करें।
- इंटरनेट पर अपनी प्राइवेसी का ध्यान रखें ।अपना पासवर्ड, चित्र और अन्य महत्वपूर्ण जानकारी अपने पास रखें।
- किसी के साथ ऑनलाइन बातचीत करते समय क्रोध में उत्तर न दें या ऐसी जानकारी न दें जो आपको नुकसान पहुंचा सकती है, कोई भी गतिविधि को करने से पहले हमेशा कुछ समय लें, विचार करें।
- यदि आपको लगता है कि आप साइबर बुलिंग के शिकार हो रहे हैं, तो व्यक्ति को जवाब न दें। व्यक्ति को ब्लॉक करें और किसीको बताएं।
- अपने कंप्यूटर पर सबूतों को बचाएँ या प्रिंट आउट लें ताकि आवश्यकता पड़ने पर इसका उत्पादन किया जा सके।
- अपने आपको गूगल पर सर्च करें और देखें कि क्या आप से सबंधित ऐसी जानकारी तो नहीं है जो वहाँ नहीं होनी चाहिए।

साइबर ग्रूमिंग

आज बहुत से छोटे बच्चे इंटरनेट का उपयोग कर रहे हैं, इससे साइबर ग्रूमिंग की एक नई समस्या अस्तित्व में आई है। यहां अक्सर एक वयस्क, एक बच्चे के साथ ऑनलाइन दोस्ती करता है और बच्चे के साथ भावनात्मक संबंध बनाता है। साइबर ग्रूमिंग का मुख्य उद्देश्य बच्चे का विश्वास हासिल करना है, बच्चे के बारे में अंतरंग और व्यक्तिगत जानकारी प्राप्त करना है। अपराधी अक्सर यौन वार्तालाप करता है, बच्चे को धमकी देने और ब्लैकमेल करने के लिए यौन चित्रया वीडियो मांगता है।

अपराधी अक्सर उम्र, शौक, स्कूल, परिवार के बारे में सामान्य प्रश्नों के साथ बातचीत शुरू करते हैं और फिर धीरे-धीरे यौन अनुभव के बारे में प्रश्न पूछते हैं। हालांकि, कभी-कभी अनजाने में बच्चा भी ग्रूमिंग की प्रक्रिया में फँस सकता है यदि वह किसी ऐसे वेबसाइट या फोरम में शामिल होता है जो संपर्क विवरण या स्वयं के अंतरंग फोटो के बदले में आकर्षक धन या उपहार प्रदान करता है।

ऑनलाइन गेमिंग

सस्ते उपकरणों पर सस्ते इंटरनेट की उपलब्धता ने बच्चों के बीच इंटरनेट के उपयोग को बढ़ावा दिया है। इसका एक नुकसान यह है कि इससे बच्चे को शारीरिक गेम के बजाय वर्चुअल गेम खेलने की आदत पड़ जाती है। वह खेल जो आंशिक या मुख्य रूप से इंटरनेट या किसी अन्य कंप्यूटर नेटवर्क के माध्यम से खेले जा सकते हैं, उन्हें ऑनलाइन गेम कहा जाता है।

ऑनलाइन गेम एक एकल (सिंगल) उपयोगकर्ता से मल्टीप्लेयर गेम तक बड़े पैमाने पर कई प्रकार के होते हैं । ऑनलाइन गेम के कुछ उदाहरणों में प्रथम-व्यक्ति निशानेबाज, रणनीतिक खेल, ऑनलाइन भूमिका निभाने सबंधी खेल आदि शामिल हैं। ऑनलाइन गेम को बहुत ही सरलता के साथ उपयोग के लिए तैयार किया जाता है, इसमें जटिल ग्राफिक्स और आभासी दुनिया हो सकती है। जटिल ग्राफिक्स और आभासी दुनिया को शामिल करनेवाले खेल बच्चों सहित विभिन्न आयु-वर्ग के लोगों में भी बहुत लोकप्रिय हो गए हैं। ऑनलाइन गेमिंग की संस्कृति कभी-कभी साइबर बुलिंग, साइबर ग्रूमिंग और हिंसा को बढ़ावा दे सकती है। कई बार गेमर्स को गेमिंग की इतनी लत लग जाती है कि जो सामाजिक तौर पर हानिकारक हो सकती है।

इंटरनेट उपयोगकर्ताओं को हमेशा एक प्रिंसिपल (सिद्धांत) का पालन करना चाहिए, किसी भी अज्ञात व्यक्ति को सोशल मीडिया या चैट रूम में न जोड़ें। इस प्रकार से ऐसी समस्याओं से कुछ हद तक बचना संभव होगा।

ई-मेल सिस्टम का उपयोग करते समय सामान्य खतरे

आज ई-मेल प्रणाली का उपयोग लगभग दैनिक आधार पर हर एक व्यक्ति व संगठन द्वारा किया जाता है। यह आमतौर पर दो घटकों के मेल क्लाइंट और मेल सर्वर से बना होता है। लोग जेनेरिक या विशेष मेल क्लाइंट का उपयोग करके अपने ई-मेल को पढ़ते हैं, लिखते हैं, भेजते हैं और संग्रहित करते हैं। मेल क्लाइंट मेल नेटवर्क में अंतर्निहित नेटवर्क इन्फ्रास्ट्रक्चर का उपयोग करके ई-मेल भेजता है। तब जाकर मेल सर्वर ई-मेल संदेशों को डिलीवर, फॉरवर्ड और स्टोर करता है। इस प्रकार एक ई-मेल प्रणाली के समुचित कार्य में शामिल सभी घटकों की सुरक्षा करना अनिवार्य हो जाता है। हमें मेल क्लाइंट्स, सर्वरों के साथ-साथ डिवाइसेज और इंफ्रास्ट्रक्चर की भी सुरक्षा करनी होगी जो ई-मेल सिस्टम का हिस्सा है।

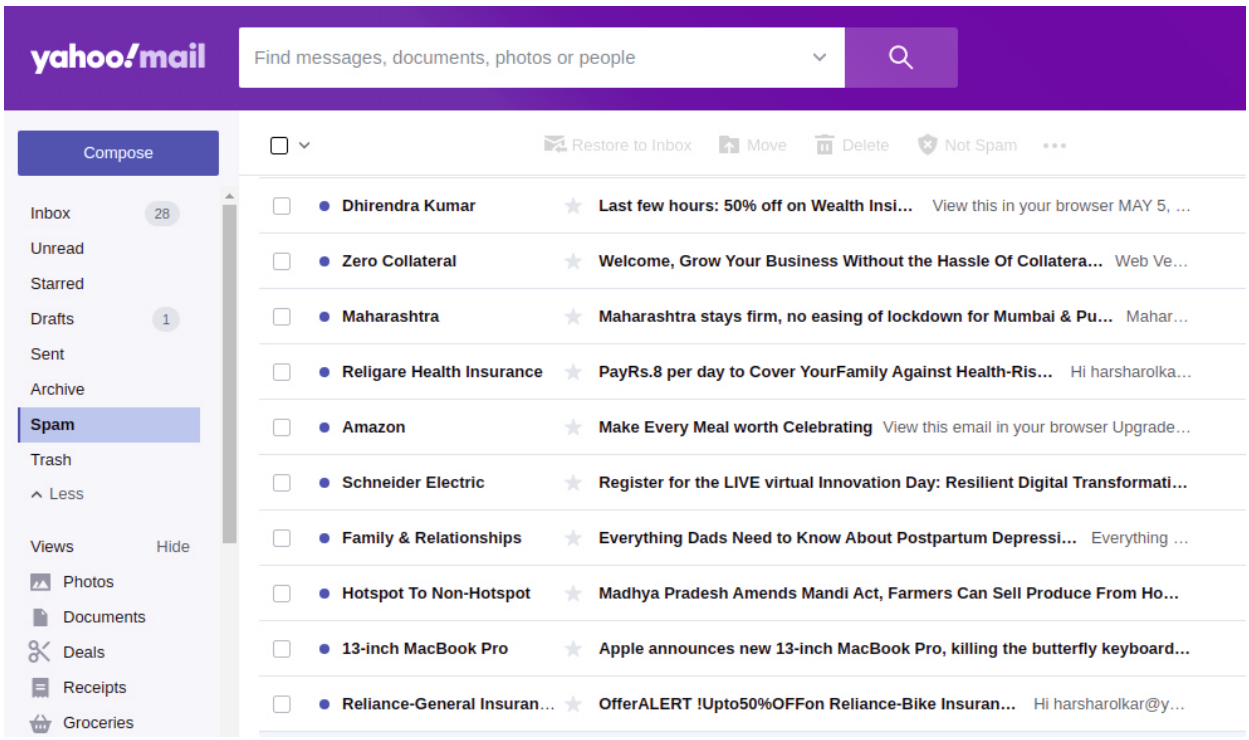
ई-मेल व्यापक रूप से बाहरी दुनिया या संगठन के साथ संवाद करने के लिए उपयोग किया जाता है जो विश्वसनीय या अविश्वसनीय हो सकता है। इस प्रकार हमलावर, ई-मेल के उपयोग का फायदा उठाने की कोशिश कर सकते हैं। हमलावर गोपनीय जानकारी तक पहुँचने का प्रयास कर सकता है, संसाधनों के आई.टी. एक्सेस को बाधित कर सकता है या किसी संगठन पर नियंत्रण हासिल कर सकता है। ई-मेल का उपयोग करते समय कुछ सामान्य खतरे जो लोगों को दिखाई देते हैं, वे हैं मालवेयर, स्पैम, फिशिंग, सोशल इंजीनियरिंग, संसाधनों और सूचना लीक करने की अनधिकृत पहुँच। आइए, हम इस बारे में और विस्तृत रूप से समझें कि ये खतरे किसी व्यक्ति या संगठन को कैसे प्रभावित कर सकते हैं।

मालवेयर :

मालवेयर ''दोषपूर्ण (malicious) सॉफ्टवेयर'' को संदर्भित करता है, जिसमें वायरस, वॉर्म, ट्रोजन हॉर्स और स्पायवेयर शामिल हैं। ये सॉफ्टवेयर आई.टी. इन्फ्रास्ट्रक्चर पर कहर ढाने में सक्षम हैं क्योंकि इनका उपयोग मशीन को नियंत्रित करने, सूचनाओं की निगरानी, गतिविधि पर नजर रखने, लॉग कुँजियाँ और अन्य दोषपूर्ण कार्यों को करने के लिए किया जा सकता है। मालवेयर को एक स्थान से दूसरे स्थान पर आसानी से स्थानांतरित करने के लिए हमलावर ई-मेल का लाभ उठा रहे हैं। हालांकि हमले हमेशा सफल नहीं होते हैं लेकिन यदि ऐसा होता है तो हमलावर हमारे ई-मेल खाते, मशीन, डेटा और अन्य संवेदनशील सूचनाओं पर नियंत्रण कर सकते हैं।

स्पैम :

आपने देखा होगा कि कई बार जब आप अपना ई-मेल खोलते हैं तो आपके इनबॉक्स में बड़ी संख्या में अज्ञात व्यक्तियों द्वारा ई-मेल दिखाई देते हैं। ऐसे अनचाहे ई-मेल जो कॉमर्शियल या नॉन कॉमर्शियल प्रकृति के हो सकते हैं, आमतौर पर जो स्पैम के रूप में जाने जाते हैं। स्पैमिंग शब्द का तात्पर्य यादच्छिक लोगों को बड़ी संख्या में अवांछित कॉमर्शियल ई-मेल संदेश भेजने से है। ऐसे संदेशों में उपयोगकर्ता की उत्पादकता को बाधित करने की प्रवृत्ति होती है, कई बार यह अत्यधिक कंप्यूटर संसाधन जैसे डिस्क स्थान, मेमोरी या प्रोसेसर का भी उपयोग कर सकता है। इसके अलावा इसे मालवेयर वितरित करने के लिए एक उपकरण के रूप में भी इस्तेमाल किया जा सकता है। अधिकांश ई-मेल सिस्टम आज (स्पैम) नामक एक अलग फ़ोल्डर और एक फिल्टर नियम प्रदान करते हैं, जो ई-मेल को स्पैम के रूप में चिह्नित करने के लिए लागू किया जा सकता है। आंकड़ा उन स्पैम ई-मेल की एक नमूना रूप सूची दिखाता है।



स्पैम ई-मेलों की विषय सूची का नमूना

फिशिंग :

यह भ्रामक साधनों के उपयोग को संदर्भित करता है जो आमतौर पर एक फर्जी वेबसाइट पेज या वेब लिंक के रूप में व्यक्तियों को ई-मेल का जवाब देने और संवेदनशील जानकारी का खुलासा करने के लिए उकसाता है। उदाहरण के लिए, किसीको यह बताते हुए एक ई-मेल प्राप्त हो सकता है कि उसने किसी विशेष वेबसाइट पर खेले गए खेल के आधार पर लाखों रुपये का पुरस्कार जीता है। पुरस्कार राशि का दावा करने के लिए उपयोगकर्ता को एक लिंक पर क्लिक करके अपने बैंक का विवरण प्रदान करना होगा। संदेश विषय बहुत ही आकर्षक होते हैं और कई बार तो स्पैमिंग के बारे में जाननेवाला व्यक्ति भी फंस जाता है। फिशिंग हमलों और स्पैम को आमतौर पर शंकास्पद ई-मेल सिस्टम का उपयोग करके लॉन्च किया जाता है ।

सोशल इंजीनियरिंग:

सुरक्षा शृंखला में मानव को सबसे कमजोर कड़ी माना जाता है। मनुष्य दबाव में आकर झुक जाता है और एक व्यक्ति सोशल इंजीनियरिंग द्वारा इस मानवीय दुर्बलता का लाभ ले करके किसी अन्य व्यक्ति या संस्था की सवेंदनशील जानकारी को हस्तगत करता है, ऐसे व्यक्ति को सोशल इंजीनियर कहा जाता है। यहाँ एक कंप्यूटर सिस्टम को हैक करने के बजाय, एक हमलावर किसी संगठन के उपयोगकर्ता से संवेदनशील जानकारी एकत्र करने के लिए एक ई-मेल का उपयोग करता है या उपयोगकर्ता से ऐसी क्रियाएँ करवाता है, जिससे हमला हो सकता है। ई-मेल स्पूफिंग एक सामान्य सोशल इंजीनियरिंग हमला है, यहाँ एक व्यक्ति या एक कार्यक्रम सफलतापूर्वक ई-मेल में दिखाए गए प्रेषक की जानकारी को गलत साबित करके आधिकारिक उपयोगकर्ता होने का दिखावा करता है और अपने वास्तविक मूल को छिपाता है। उदाहरण के लिए, किसी संगठन का एक आई.टी. विभाग अपने सी.ई.ओ. से एक संदेश प्राप्त करता है, जिसमें कहा गया है कि वह एक महत्वपूर्ण आवेदन का पासवर्ड भूल गया है और वह इसे रीसेट करना चाहेगा। यहाँ आवेदक एक हमलावर है, जो सी.ई.ओ. के क्रेडेंशियल्स का उपयोग करता है ।

संसाधनों के लिए अनधिकृत पहुँच:

गलत इरादे के साथ कोई बाहरी हमलावर या कोई अंदरूनी व्यक्ति एक ई-मेल सर्वर पर सफल हमले के माध्यम से संसाधनों तक अनधिकृत पहुँच प्राप्त करने के लिए ई-मेल का उपयोग कर सकता है। एक बार जब मेल सर्वर से समझौता कर लिया जाता है, तो एक हमलावर तब उपयोगकर्ता के विवरण जैसे कि उपयोगकर्ता का नाम, पासवर्ड या किसी अन्य महत्वपूर्ण जानकारी को प्राप्त करने में सक्षम हो सकता है, जो तब संगठन के नेटवर्क के भीतर अन्य कम्प्यूटरों या संसाधनों तक हमलावर की पहुँच आसान हो जाती है ।

सूचना लीक होना:

लोग विभिन्न स्थानों और उपकरणों से अपने ई-मेल का उपयोग करते हैं। ई-मेल का उपयोग घर, कार्यालय, डेस्कटॉप कंप्यूटर, लैपटॉप या हैंडहेल्ड डिवाइस से किया जा सकता है। कई बार अनेक स्थानों से ई-मेल का उपयोग करने के कारण अनजाने में जानकारी लीक हो जाती है। अनजाने में कई स्थानों से ई-मेल का उपयोग करते समय अधिकृत उपयोगकर्ता निजी या अन्य संवेदनशील जानकारी भेज सकते हैं। इस तरह की जानकारी संगठन के लिए कई बार परेशानी पैदा कर सकती है या कानूनी कार्रवाई का कारण भी बन सकती है।

आज जब साइबर स्पेस का उपयोग तेजी से बढ़ रहा है, तो कम से कम संभावना है कि लोग ई-मेल का उपयोग करना बंद कर सकते हैं। इस प्रकार संचार के लिए ई-मेल का उपयोग करते समय सावधानी बरतना आवश्यक हो जाता है। यहाँ बताए गए बिंदु ई-मेल के एहतियाती उपयोग पर संगठनों और उपयोगकर्ता के लिए एक सामान्य दिशानिर्देश प्रदान करते हैं।

मेल सर्वर एप्लिकेशन को सुरक्षित करें:

मेल सर्वर को होस्ट करनेवाले संगठनों को मेल सर्वर को यथासंभव सुरक्षित बनाना चाहिए। मेल सर्वर उपयोगकर्ता द्वारा प्रमाणीकरण, पहुंच और संसाधन नियंत्रण को नियमित आधार पर अपडेट और सत्यापित किया जाना चाहिए।

मेल क्लाइंट को सुरक्षित करें:

मेल सर्वर की तुलना में मेल क्लाइंट की सुरक्षा में अधिक जोखिम होता है क्योंकि क्लाइंट संख्या में अधिक व बिखरे होते हैं। मेल क्लाइंट सुरक्षा सुविधाओं को ठीक से कॉन्फ़िगिर किया जाना चाहिए ताकि संदेशों के स्वचालित शुरू होना व अनुलग्नकों की वायरस जांच को नियंत्रण किया जा सके और उचित स्पैम फिल्टर बनाया जा सके। हमें स्वचालित प्रमाणीकरण और पहुंच तंत्र का उपयोग करने से बचना चाहिए, गतिविधि पूरी होने के बाद ई-मेल से लॉग आउट करना हमेशा एक सबसे अच्छा विकल्प माना जाता है।

ट्रांसमिशन को सुरक्षित करें:

अधिकांश मेल क्लाइंट सादे प्रारूप (प्लेन टेक्स्ट) में उपयोगकर्ता प्रमाणीकरण डेटा और ई-मेल सामग्री भेजते हैं। जब यह नेटवर्क से यात्रा करता है तो प्लेन टेक्स्ट डेटा आसानी से संशोधित किया जा सकता है। एक हमलावर बड़ी आसानी से उपयोगकर्ता के खाते के बारे में विवरण कैप्चर करने में सक्षम हो सकता है या ई-मेल में लिखे गए टेक्स्ट को पढ़ सकता है। इससे बचने के लिए सबसे अच्छा अभ्यास उपयोगकर्ता प्रमाणीकरण और साथ ही ई-मेल डेटा को एन्क्रिप्शन का पालन करना है।

सहायक हार्डवेयर और ऑपरेटिंग एनवायरमेंट को सुरक्षित करें:

यद्यपि ई-मेल सर्वर और क्लाइंट एक ई-मेल सिस्टम के दो मुख्य घटक हैं । वह नेटवर्क, हार्डवेयर और सॉफ्टवेयर से पूर्णत: संबंधित व आश्रित होते हैं। यह सुनिश्चित करना कि यह अतिरिक्त घटक सुरक्षित हैं, ई-मेल प्रणाली की विश्वसनीयता भी बढ़ाते हैं।

अविश्वसनीय स्त्रोतों से कोई भी ई-मेल न खोलें:

यह हमेशा सलाह दी जाती है कि किसी भी व्यक्ति को ऐसा कोई ई-मेल नहीं खोलना चाहिए जो उस व्यक्ति से प्राप्त किया गया हो जिसे आप नहीं जानते हैं। इस तरह के ई-मेल आमतौर पर स्पैम होते हैं या फिशिंग का कारण बन सकते हैं। यदि कोई व्यक्ति किसी मित्र या परिवार के सदस्य के संपर्क से एक संदिग्ध ई-मेल संदेश प्राप्त करता है, तो इस तरह के संदेश के बारे में व्यक्तिगत रूप से या फोन पर उनके साथ जांच करना बेहतर होता है। एक संदेह का लाभ, अजनबियों से प्राप्त ई-मेल को कभी नहीं देना चाहिए ।

स्कैनिंग के बिना कभी भी अनपेक्षित अटैचमेंट न खोलें:

जब कंप्यूटर सिस्टम पर मालवेयर या वायरस फैलने की बात आती है, तो ई-मेल अटैचमेंट मुख्य अपराधी होते हैं। सुरक्षा विशेषज्ञों का सुझाव है कि, किसीको भी किसी भी अनुलग्नक (अटैचमेंट) को स्कैन किए बिना नहीं खोलना चाहिए, भले ही वह किसी ज्ञात स्त्रोत से आया हो।

एक जटिल पासवर्ड का चयन करें:

सामान्यत: लोगों को एक सरल पासवर्ड चुनने की आदत होती है जिन्हें वह आसानी से याद रख सके। एक छोटा पासवर्ड चुनना जो जन्मतिथि का प्रतिनिधित्व करता है या पति / पत्नी / बेटी का नाम होता है । यह उपयोगकर्ता के लिए खतरा पैदा करता है। अक्षरों, संख्याओं, प्रतीकों और विराम चिह्नों के मिश्रण के साथ लंबे पासवर्ड सुरक्षा पहलू के मामले में सबसे उपयुक्त हैं। साथ ही प्रत्येक व्यक्ति को नियमित अंतराल पर पासवर्ड बदलने की आदत डालनी चाहिए।

मेलिंग सिस्टम कुछ सुरक्षा प्रश्नों या अन्य मापदंडों के आधार पर पासवर्ड रिकवरी तंत्र प्रदान करते हैं। एक जटिल सुरक्षा प्रश्न चुनने / बनाने की सलाह दी जाती है। एक अन्य समाधान, मानक प्रश्नों के झूठे उत्तर उत्पन्न करना है; ताकि हमलावर उन उत्तरों का आसानी से पता न लगा सकें । आमतौर पर उपयोगकर्ता २स्र तंत्र के रूप में ज्ञात दो कारक प्रमाणीकरण भी लागू कर सकते हैं जिसमें एक पासवर्ड और एक प्रश्न का उत्तर, लॉगिन के लिए अनिवार्य हो जाता है। ऐसा तंत्र वास्तविक डेटा तक पहुंचने से पहले सुरक्षा की दो परतें प्रदान करता है।

अपडेटेड एंटी-वायरस सॉफ्टवेयर रखें:

उपयोग के लिए सलाह दी जाती है कि वे एंटी वायरस सॉफ्टवेयर्स खरीदें या फ्री एंटी वायरस सॉफ्टवेयर्स का उपयोग करें। हालांकि कोई भी एंटी वायरस, उपयोगकर्ता के प्रत्येक डेटा को खतरे से बचाव की गारंटी नहीं दे सकता है, लेकिन एंटी वायरस हमेशा निश्चित स्तर की सुरक्षा देता है।

सार्वजनिक वाईफाई से कभी ई-मेल का उपयोग न करें:

सार्वजनिक और मुफ्त वाईफाई स्थान सामान्य इंटरनेट सर्फिंग के लिए अच्छे हैं, लेकिन व्यक्तिगत या आधिकारिक ई-मेल और ई-कॉमर्स लेनदेन तक पहुँचने जैसी गतिविधियों का उपयोग कभी नहीं किया जाना चाहिए। सार्वजनिक वाई-फाई हमलावरों के लिए मुफ्त डेटा एकत्र करने के लिए एक आम जगह है।

अपनी मशीनों को खुला न छोड़ें:

घर और दफ्तर के लोगों को जब वह कुछ समय के लिए अपने स्थान पर नहीं होते, तब अपने कंप्यूटर (डेस्कटॉप / लैपटॉप) को खुला छोड़ने की आदत होती है। अपने कंप्यूटर या लैपटॉप स्क्रीन को अतिरिक्त पासवर्ड से लॉक करना हमेशा एक अच्छी आदत है। जब भी आप अपनी मशीन से अल्प अवधि के लिए दूर होते हैं तो स्क्रीन लॉक करना, सुरक्षा की एक अतिरिक्त स्तर प्रदान करता है।

अभ्यास

1. साइबर बुलिंग क्या है? इससे कैसे बचा जा सकता है?

2. ई-मेल का उपयोग करते समय होनेवाले खतरों को सूचीबद्ध करें और समझाएँ।

3. निम्नलिखित शब्दों को परिभाषित करें:

(A) साइबर ग्रूमिंग (B)ऑनलाइन गेमिंग (C) मालवेयर (D) फ़िशिंग

4. निम्नलिखित में से योग्य विकल्प पसंद कीजिए :

(1) ऑनलाइन माध्यम का उपयोग करते हुए धमकी जारी करना, जो स्वयं किसी व्यक्ति को या दूसरों को चोट पहुंचाने के लिए उकसा सकता है, निम्नलिखित में से किसका उदाहरण है?

(a) साइबर बुलिंग (b) साइबर ग्रूमिंग (c) फ़िशिंग (d) स्पैम

(2) एक वयस्क, बच्चे के साथ ऑनलाइन दोस्ती करता है और बच्चे के साथ भावनात्मक संबंध बनाता है, निम्नलिखित में से किसका उदाहरण है?

(a) साइबर बुलिंग (b) साइबर ग्रूमिंग (c) फ़िशिंग (d) सोशल इंजीनियरिंग

(3) निम्नलिखित में से कौन-सा एक अवांछित कॉमर्शियल या नॉन कॉमर्शियल ई-मेल को संदर्भित करता है ?

(a) बुलिंग (b) स्पैम

(c) फ़िशिंग (d) ग्रूमिंग

(4) निम्नलिखित में से की-लॉगेर्स किसका उदाहरण है?

(a) फ़िशिंग (b) मालवेयर

(c) स्पैम (d) सूचना लीक

(5) ई-मेल एक्सेस करते समय निम्नलिखित में से कौन-से खतरे हैं?

(a) सोशल इंजीनियरिंग (b) फ़िशिंग

(c) स्पैम (d) यह सभी

NOTES