शुध्धिपत्रक

कक्षा 9

विषय : 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-14 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 आक्रमण' नामक प्रसिद्ध खतरे को जन्म दिया है । उससे सुरक्षा के उपायों की चर्चा यहाँ की गई है, साथ ही स्वाध्याय में भी तत्संबंधी प्रश्नों का भी समावेश किया गया है ।

सायबर सुरक्षा, उसके खतरे तथा उसके बचाव के उपाय (Cyber Security, its Threats and Solutions)

आज हम में से अधिकांश किसी न किसी उद्देश्य के लिए इंटरनेट का उपयोग करते हैं। यहाँ तक कि हमारे घरों, बुनियादी सुविधाओं, वाहनों और घरेलू उपकरणों को इंटरनेट से जोड़ा जा रहा है। डेटा के अत्यधिक साझा और विभिन्न चीजों के परस्पर संपर्क ने साइबर हमलों को एक नया खतरा पैदा कर दिया है। साइबर हमले ऐसी गतिविधि है, जिसमें इंटरनेट का उपयोग करके दुनिया में कहीं भी बैठा हुआ एक व्यक्ति, दूसरे व्यक्ति को या एक आई टी (इनफार्मेशन टेक्नॉलजी) संगठन के बुनियादी ढांचे को नुकसान पहुँचा सकता है। यह किसी संस्था या व्यक्ति द्वारा, किसी अन्य संगठन या व्यक्ति की प्रणालियों को प्रभावित करने का एक सोचा-समझा प्रयास है। हमलावर के उद्देश्यों में डेटा चोरी, सूचना की चोरी, वित्तीय लाभ, जासूसी या तोड़फोड़ शामिल हो सकते हैं। हालांकि कई साइबर हमले मौजूद हैं, उनमें से अधिकांश निम्नलिखित हमलों में से किसी एक के परिणाम हैं।

फ़िशिंग (Phishing) : 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 प्रेरित करता है। उदाहरण के लिए, किसी को यह बताते हुए एक ई-मेल प्राप्त हो सकता है कि उसने एक गेम के आधार पर लाखों रुपये का पुरस्कार जीता है, जो उसने किसी विशेष वेबसाइट पर खेला 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 जानने वाला व्यक्ति भी फंस जाता है। फ़िशिंग हमलों और स्पैम को आमतौर पर संशोधित ई-मेल सिस्टम का उपयोग करके लॉन्च किया जाता है ।

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

रैंसमवेयर (Ransomware) : इसमें हैकर द्वारा पीड़ित के कम्प्यूटर या फाइलों को लॉक करना शामिल है। इस मामले में हमलावर फिरौती के लिए अर्जित जानकारी रखता है। पीड़ित को उसकी संपत्ति तक पहुँच पाने के लिए हमलावर को भुगतान करने की आवश्यकता होती है। रैंसमवेयर फ़िशिंग ई-मेल के माध्यम से या अनजाने में एक संक्रमित वेबसाइट पर जाने से फैलता है।

डेटा एक्सपोजर (Data Exposer) : यह आज एक बड़ा साइबर सुरक्षा खतरा बन रहा है। यहाँ हमलावर बैंकिंग, सोशल मीडिया, विश्वविद्यालय या किसी अन्य संस्थानों के एप्लिकेशन जैसे डेटा को स्टोर करने वाले एप्लिकेशन की डेटाबेस जानकारी तक पहुँचने का प्रयास करते हैं। डेटा एक्सपोज़र एक अलग तरीके से होता है। हैकर्स सोशल इंजीनियरिंग के माध्यम से किसी उपयोगकर्ता का लॉगइन विवरण चुरा सकते हैं या पहुँच प्राप्त करने के लिए मलवेयर का उपयोग कर सकते हैं। डेटा के आकस्मिक बंटवारे से भी कई बार डेटा एक्सपोज़र हो जाता है। दुर्घटना साझा आमतौर पर मानवीय त्रुटि के परिणामस्वरूप होता है। एक ई-मेल के लिए "Reply All" अर्थात "सभी का जवाब दें" करना, डेटा जोखिम का कारण बन सकती है।

इन हमलों ने साइबर सुरक्षा नामक शब्द को जन्म दिया है। साइबर स्पेस कुछ कम्प्यूटरों के हार्डवेयर, सॉफ़्टवेयर या इलेक्ट्रॉनिक डेटा की चोरी या क्षति से कम्प्यूटर सिस्टम को बचाने के लिए उपयोग किए जाने वाले कुछ तंत्रों का अनुप्रयोग है। यह उन सेवाओं की रक्षा करने का भी इरादा रखता है जो कम्प्यूटर सिस्टम प्रदान करता है। वस्तुत: सबकुछ इंटरनेट के उपयोग के साथ एक दूसरे के साथ जुड़ा होने के कारण, साइबर सुरक्षा कभी भी अधिक महत्वपूर्ण नहीं रही है।

यहाँ बताए गए कुछ कदम, संगठनों और व्यक्ति को बेहतर सुरक्षा प्रदान करने में मदद करेंगे। ठीक से पालन किए जाने पर, ये सभी साइबर हमलों से सुरक्षा में मदद भी करेंगे।

- सर्वर, पर्सनल कम्प्यूटर, लैपटॉप या मोबाइल डिवाइस जैसे कम्प्यूटर सिस्टम का उपयोग करते समय, एक अच्छा एंटी-वायरस या एंटी-मलवेयर सॉफ़्टवेयर इंस्टॉल करना चाहिए।
- सुनिश्चित करें कि उपकरणों पर इंस्टॉल एंटी-वायरस सॉफ़्टवेयर या एंटी-मलवेयर सॉफ़्टवेयर आधुनिकतम है। हर दिन, बाज़ार में वायरस और मलवेयर के नए सेट दिखाई देते हैं। इस प्रकार व्यक्तियों और व्यवसायों के लिए इन वायरस से सुरक्षित रहना महत्वपूर्ण हो जाता है।
- आपके द्वारा उपयोग किए जाने वाले कम्प्यूटर या नेटवर्क की सुरक्षा के लिए फ़ायरवॉल का उपयोग करें। चूंकि मलवेयर ई-मेल के अलावा कई माध्यमों का उपयोग करके फैल सकता है, इसलिए नेटवर्क पर जाने वाले डेटा को नियंत्रित करना महत्वपूर्ण हो जाता है। फ़ायरवॉल, नेटवर्क में प्रवेश करने और छोड़ने की निगरानी करता है। इसी तरह उपयोगकर्ता कम्प्यूटर जैसे कि होम-पर्सनल कम्प्यूटर या लैपटॉप को सुरक्षित रखने के लिए एक व्यक्तिगत फ़ायरवॉल स्थापित करना चाहिए।
- सभी आवक और जावक ई-मेल को कम्प्यूटर वायरस के लिए फ़िल्टर किया जाना चाहिए। फ़िल्टर आदर्श रूप से राउटर या एक्सेस पॉइंट जैसे नेटवर्क के एंट्री पॉइंट पर स्थापित होने चाहिए।
- सभी उपयोगकर्ताओं को कम्प्यूटर का उपयोग करने के सर्वोत्तम तरीकों के बारे में प्रशिक्षित किया जाना चाहिए। उदाहरण के लिए किसीको अटैचमेंट नहीं खोलना चाहिए या किसी ई-मेल के लिंक पर क्लिक नहीं करना चाहिए जिसकी वे अपेक्षा नहीं कर रहे हैं।
- हमें डाउनलोड स्रोत की सही जानकारी प्राप्त किए बिना अज्ञात मूल के प्रोग्राम को डाउनलोड और चलाना नहीं चाहिए।

- सुनिश्चित करें कि महत्वपूर्ण फ़ाइलों और फ़ोल्डरों का नियमित बैकअप लिया जाता है। इस बैकअप को पोर्टेबल ड्राइव जैसे रिमूवेबल मीडिया पर रखना चाहिए। अतिरिक्त सुरक्षा के लिए, बैकअप को किसी अन्य स्थान पर सुरक्षित रूप से संग्रहित किया जाना चाहिए।
- जहाँ संभव हो, एक्सेस कंट्रोल मैकेनिज्म का उपयोग करने की कोशिश करें और एंड यूजर परमिशन को प्रतिबंधित करें। संगठन के अंतिम उपयोगकर्ताओं को उनके उपकरणों पर प्रशासनिक विशेषाधिकार नहीं दिए जाने चाहिए।
- एक संगठन के भीतर नेटवर्क सुरक्षा नीतियों को डिज़ाइन करें और उन्हें सभी उपयोगकर्ताओं के लिए प्रचारित करें।

ई-मेल सिस्टम का उपयोग करते समय सामान्य खतरे (Common threats while using an Email system)

एक ई-मेल प्रणाली आज संगठन में संचार का अभिन्न अंग बन गई है। इसका उपयोग सूचना भेजने और प्राप्त करने की प्रक्रिया को तेज करने के लिए किया जाता है। एक ई-मेल प्रणाली आमतौर पर दो घटकों, एक सर्वर और एक क्लाइंट से बनी होती है। इन घटकों को मेल सर्वर और मेल क्लाइंट के रूप में जाना जाता है। उपयोगकर्ता मेल क्लाइंट का उपयोग करके ई-मेल को पढ़, लिख, भेज सकते हैं और स्टोर कर सकते हैं। मेल क्लाइंट, मेल नेटवर्क में अंतर्निहित नेटवर्क इन्फ्रास्ट्रक्चर का उपयोग करके ई-मेल भेजता है। मेल सर्वर तब ई-मेल संदेशों को डिलीवर, फॉरवर्ड और स्टोर करता है। इस प्रकार एक ई-मेल प्रणाली के समुचित कार्य में शामिल सभी घटकों की रक्षा करना अनिवार्य हो जाता है। हमें मेल क्लाइंट्स, सर्वरों के साथ-साथ डिवाइसेज और इन्फ्रास्ट्रक्चर की सुरक्षा करने भी जरूरत है जो ई-मेल सिस्टम का हिस्सा है।

हमलावर संगठनात्मक या व्यक्तिगत गतिविधि में बाधा पैदा करने के लिए ई-मेल प्रणाली के उपयोग का फायदा उठाने की कोशिश कर सकते हैं। वे गोपनीय जानकारी तक पहुँचने का प्रयास कर सकते हैं, संसाधनों तक आई टी पहुँच को बाधित कर सकते हैं या किसी संगठन पर नियंत्रण हासिल कर सकते हैं। ई-मेल का उपयोग करते समय कुछ सामान्य खतरे जो लोगों को दिखाई देते हैं, वे हैं मलवेयर, स्पैम, फ़िशिंग, सोशल इंजीनियरिंग, संसाधनों और सूचना रिसाव की अनधिकृत पहुँच। आइए , हम इसे अधिक विस्तृत रूप से समझते हैं, कि ये खतरे किसी व्यक्ति या संगठन को कैसे प्रभावित कर सकते हैं।

स्पैम : हमारे मेलबॉक्स में पाए जाने वाले अवांछित वाणिज्यिक या गैर वाणिज्यिक ई-मेल आमतौर पर स्पैम के रूप में जाने जाते हैं। स्पैम में उपयोगकर्ता उत्पादकता को बाधित करने और डिस्क स्थान, मेमोरी या प्रोसेसर जैसे कम्प्यूटर संसाधनों का उपभोग करने की प्रवृत्ति होती है। इसके अलावा इसे मलवेयर वितरित करने के लिए एक उपकरण के रूप में भी इस्तेमाल किया जा सकता है। ई-मेल सिस्टम आज "स्पैम" (Spam) नामक एक अलग फ़ोल्डर और एक फिल्टर नियम प्रदान करता है, जिसे एक ई-मेल को स्पैम के रूप में चिह्नित किया जा सकता है।

सोशल इंजीनियरिंग : सोशल इंजीनियरिंग से तात्पर्य लोगों को कोई भी व्यक्ति या संगठन की संवेदनशील सूचनाओं को सौपने से है। ई-मेल स्पूफिंग एक सामान्य सामाजिक इंजीनियरिंग हमला है, यहाँ एक व्यक्ति या एक कार्यक्रम सफलतापूर्वक प्रेषक जानकारी को गलत तरीके से बताकर आधिकारिक उपयोगकर्ता होने का दिखावा करता है। उदाहरण के लिए किसी संगठन का एक आई टी विभाग अपने लेखा अधिकारी से एक संदेश प्राप्त कर सकता है, जिसमें कहा गया है कि वह एक महत्वपूर्ण आवेदन का पासवर्ड भूल गया है और वह इसे री-सेट करना चाहेगा। यहाँ हमलावर खाता अधिकारी की साख का उपयोग कर रहा है ।

संसाधनों के लिए अनधिकृत पहुँच : एक मलिन इरादे के साथ एक हमलावर या एक अंदरूनी सूत्र एक ई-मेल सर्वर पर एक सफल हमले के माध्यम से संसाधनों तक अनधिकृत पहुँच प्राप्त करने के लिए एक उपकरण के रूप में ई-मेल का उपयोग कर सकता है।

सूचना रिसाव : लोग विभिन्न स्थानों और उपकरणों के ई-मेल का उपयोग करते हैं। कई बार ई-मेल का उपयोग करने के इस अभ्यास से अनजाने में जानकारी लीक हो जाती है।

यह भी ध्यान दें कि पहले के खंड में चर्चा की गई मलवेयर और फ़िशिंग हमलों को भी ई-मेल का उपयोग करके आसानी से लॉन्च किया जा सकता है।

प्रतिदिन ई-मेल के बढ़ते उपयोग के साथ, संचार के लिए ई-मेल का उपयोग करते समय सावधानी रखना आवश्यक हो जाता है। यहाँ वर्णित कदम ई-मेल के एहतियाती उपयोग के लिए संगठनों और उपयोगकर्ता के लिए एक सामान्य दिशानिर्देश प्रदान करते हैं।

- सुनिश्चित करें कि संगठन का मेल सर्वर अनुप्रयोग सुरक्षित है।
- सुनिश्चित करें कि आपके द्वारा उपयोग किए जाने वाले मेल क्लाइंट सुरक्षित हैं।
- सुनिश्चित करें कि ट्रान्सफ़रिंग मेल के लिए उपयोग की जाने वाली ट्रांसमिशन लाइनें सुरक्षित हैं।
- सहायक हार्डवेयर और ऑपरेटिंग वातावरण को सुरक्षित करें।
- अविश्वसनीय स्रोतों से कोई भी ई-मेल न खोलें।
- स्कैनिंग के बिना कभी भी अप्रत्याशित संलग्नक न खोलें।
- अपने मेल खातों के लिए एक जटिल पासवर्ड चुनें।
- उन कम्प्यूटरों पर अपडेट एंटी-वायरस सॉफ़्टवेयर का उपयोग करें जहाँ से आप ई-मेल तक पहुँचते हैं।
- सार्वजनिक वाईफाई स्थानों जैसे रेस्तरां, मॉल और अन्य स्थानों से ई-मेल का उपयोग न करें।
- कोशिश करें कि अपनी मशीनों को दूसरों के उपयोग के लिए न छोड़ें।

समीक्षात्मक प्रश्न

1. साइबर सुरक्षा क्या है?
2. ई-मेल का उपयोग करते समय होने वाले खतरों की सूची बनायें और व्याख्या करें ।
3. डेटा एक्सपोज़र से आपका क्या तात्पर्य है? व्यावसायिक संगठन खुद को इससे कैसे बचा सकते हैं?
4. निम्नलिखित शब्दों को परिभाषित करें :

   (a) स्पैम (b) रैंसमवेयर (c) मलवेयर (d) फ़िशिंग

5. **वस्तुनिष्ठ प्रश्न दिए गए विकल्पों में से योग्य विकल्प चुनें :**

   (1) भ्रामक साधनों का उपयोग करके आमतौर पर एक फर्जी वेबसाइट पेज या वेब लिंक के रूप में व्यक्तियों को धोखा देने के लिए ई-मेल का जवाब देने के लिए मजबूर करना और संवेदनशील जानकारी का खुलासा करना किसके उदाहरण हैं?
   (a) साइबर बुलिंग (b) साइबर ग्रूमिंग (c) फ़िशिंग (d) स्पैम

   (2) निम्नलिखित में से कौन हैकर द्वारा पीड़ित के कम्प्यूटर या फाइलों तक पहुँच को लॉक करता है?
   (a) मलवेयर (b) स्पैम (c) फ़िशिंग (d) रैंसमवेयर

   (3) ई-मेल का उपयोग करते समय निम्नलिखित में से किस खतरे का सामना करना पड़ता है?
   (a) सोशल इंजीनियरिंग (b) फ़िशिंग (c) स्पैम (d) ये सभी