इकाई 10 साइबर सुरक्षा

इकाई की रूपरेखा

10.0 उद्देश्य

इस इकाई का अध्ययन करने के बाद, आप इस योग्य हो सकेंगे कि:

- सूचना सुरक्षा और साइबर सुरक्षा के बीच अंतर कर सकें;
- साइबर दुनिया से संबंधित बुनियादी शब्दावली को समझ सकें;
- साइबर खतरों और इसके प्रकारों को समझ सकें; तथा
- साइबर अपराध और कानून को समझ सकें।

10.1 प्रस्तावना

आजकल स्मार्ट फोन और गैजेट्स का इस्तेमाल एक आम बात है। यह सबसे उल्लेखनीय वस्तुओं में से एक है जिसे साइबर और इसके उपयोगों पर गहराई से देखने से पहले विचार करने की आवश्यकता है। वर्तमान परिदृश्य में साइबर और इसकी सुरक्षा हमारे जीवन का एक अनिवार्य घटक बन गया है क्योंकि सभी डेटा स्वास्थ्य जानकारी, व्यक्तिगत जानकारी और वित्तीय जानकारी इंटरनेट और वेब में संग्रहीत होते हैं जिसे वर्तमान परिदृश्य में हम क्लाउड कहते हैं। वर्चुअल प्लेटफॉर्म पर जानकारी डालना हम सभी को दुनिया भर में परिचित कराता है कि हम दूसरों के साथ कैसे जुड़ें, चीजों के प्रवाह को व्यवस्थित करें, और जानकारी साझा करें।

यह एक ऐसी जगह है जहां डेटा हमेशा के लिए रहेगा लेकिन यह सुरक्षित नहीं है जब तक कि इसे सुरक्षा प्रदान नहीं की जाती है। वर्तमान परिदृश्य में कृत्रिम बुद्धिमत्ता (ए आई) को पारस्परिक रूप से पेश किया गया है, एआई और इंटरनेट ऑफ थिंग्स (आई ओ टी) इंटरनेट और वैश्विक अर्थव्यवस्था दोनों को बदल देगा। अगले पांच वर्षों में, हम ए आई और मशीन लर्निंग (एम एल) का अनुमान लगा सकते हैं कि यह प्रौद्योगिकी के सभी रूपों में शामिल हो जाएगा जिसमें डेटा विनिमय और विश्लेषण शामिल है।

हम में से ज्यादातर लोग स्मार्ट फोन, लैपटॉप, होम राउटर, स्मार्ट टीवी, हाई एंड कारों, डी वी आर और कैमरा आदि के माध्यम से हर दिन इंटरनेट से जुड़े रहते हैं, जबकि इंटरनेट से जुड़े रहने से हमें ऑनलाइन शॉपिंग करने, मूवी देखने, संगीत का आनंद लेने, मानचित्रों का उपयोग करने, ऑनलाइन खोज करने, हमारे बिलों का भुगतान आदि करने की सुविधा मिलती है। लेकिन आई ओ टी (इंटरनेट ऑफ थिंग्स) के आगमन के साथ और भी अधिक गैजेट्स जैसे बल्ब, थर्मोस्टेट, एयर कंडीशनर आदि जुड़े हुए हैं। दुर्भाग्य से, इनमें से कई कनेक्टेड डिवाइस ऐसे होंगे, जिनको नई साइबर समस्याओं के लिए अग्रणी सुरक्षा को ध्यान में रखते हुए नहीं बनाया गया है।

कंप्यूटर सुरक्षा और साइबर सुरक्षा कंप्यूटर सिस्टम की चोरी या उनके हार्डवेयर, सॉफ्टवेयर या इलेक्ट्रॉनिक डेटा को नुकसान के साथ-साथ सेवाओं को बाधित करने से भी बचाती है। साइबर सुरक्षा जीवन की अनिवार्य विशेषता बनती जा रही है और इस तरह के दृष्टिकोण के पीछे कारण कुछ और नहीं बल्कि तकनीकी निर्भरता का विकास है। साइबर सुरक्षा सूचना प्रौद्योगिकी (आईटी) में एक विशेष क्षेत्र है जिसे कंप्यूटर विज्ञान में एक उप धारा के रूप में माना जाता है।

साइबर सिक्योरिटी पर यह इकाई कंप्यूटरों के ऑपरेटिंग सिस्टम, नेटवर्क और डेटा को साइबर हमलों से निपटने के लिए आवश्यक ज्ञान और कौशल से लैस करती है। ई-कॉमर्स में सीखने के साथ-साथ इसके कार्यान्वयन के साथ-साथ बड़े पैमाने पर वित्तीय निहितार्थ के उपयोग की तकनीक की मदद से इसका व्यापक उपयोग होता है।

10.2 साइबर सुरक्षा का अर्थ

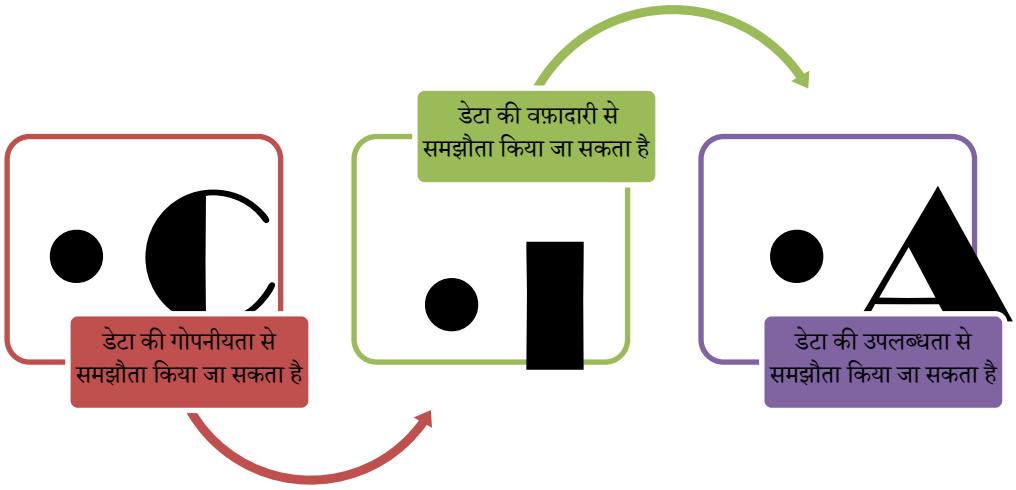
साइबर खतरे एक वैश्विक जोखिम है जिससे सरकारों, निजी क्षेत्र, गैर-सरकारी संगठनों - और वैश्विक समुदाय को समग्र रूप से निपटना चाहिए। कंप्यूटर सुरक्षा, साइबर सुरक्षा या सूचना

प्रौद्योगिकी सुरक्षा सूचनाओं के प्रकटीकरण, उनके हार्डवेयर, सॉफ़्टवेयर या इलेक्ट्रॉनिक डेटा को नुकसान या चोरी करने के साथ-साथ उनके द्वारा प्रदान की जाने वाली सेवाओं के विघटन या गलत विकास से कंप्यूटर सिस्टम और नेटवर्क की सुरक्षा है। कंप्यूटर सिस्टम पर प्रवर्धित निर्भरता, ब्लूटूथ और वाई-फाई जैसे इंटरनेट और वायरलेस नेटवर्क मानकों और स्मार्टफ़ोन, टीवी और विभिन्न उपकरणों सहित "स्मार्ट" उपकरणों के विकास के कारण साइबर क्षेत्र धीरे-धीरे अधिक उल्लेखनीय होता जा रहा है, जो "इंटरनेट ऑफ़ थिंग्स" का गठन करता है।

आज की दुनिया में ई-कॉमर्स की अधिकता है जिसमें एहतियाती उपाय करने के लिए खुद को एक साइबर के साथ सुरक्षित रखने की आवश्यकता है। साइबर सुरक्षा को ध्यान में रखते हुए डिजिटल हमलों से सिस्टम, नेटवर्क और कार्यक्रमों की सुरक्षा या अभ्यास करने का तरीका है। इन साइबर हमलों का उद्देश्य अक्सर अतिसंवेदनशील जानकारी को एक्सेस करना, बदलना या नष्ट करना, उपयोगकर्ताओं से पैसा निकालना; या सामान्य व्यावसायिक प्रक्रियाओं को बाधित करना है। प्रभावी साइबर सुरक्षा उपायों को लागू करना आजकल मुख्य रूप से चुनौतीपूर्ण है क्योंकि लोगों की तुलना में अधिक उपकरण हैं, और हमलावर इलेक्ट्रॉनिक उपकरणों का उपयोग करने के लिए और इलेक्ट्रॉनिक रूप से धमकी देने के लिए अत्याधुनिक उपकरणों का उपयोग कर रहे हैं।

10.2.1 ई-कॉमर्स पर साइबर सुरक्षा प्रभाव

साइबर सुरक्षा एक व्यवसाय, या संगठन के भीतर सुरक्षा का एक हिस्सा है जो आई टी सिस्टम के अधिकृत उपयोग को सक्षम करने, साथ ही अनधिकृत पहुंच को रोकने के लिए केंद्रित है । साइबर सुरक्षा का मुख्य उद्देश्य व्यवसाय को अधिक सफल बनाने में मदद करना है। इसमें व्यापारिक ब्रांड को होने वाली क्षति, वास्तविक नुकसान और व्यावसायिक व्यवधानों को रोकने के लिए शेयरधारकों, ग्राहकों और हितधारकों के साथ विश्वास बढ़ाने वाली रणनीतियाँ शामिल हो सकती हैं। साइबर सुरक्षा को डेस्कटॉप डिवाइस, जैसे डेस्कटॉप, सर्वर, लैपटॉप, नोटबुक, स्मार्ट फोन और नेटवर्क पर लागू किया जाना चाहिए। इस क्षेत्र में वे सभी प्रक्रियाएं और तंत्र शामिल हैं जिनके द्वारा डिजिटल उपकरण, सूचना और सेवाओं को गैर-इच्छित या अनधिकृत पहुंच, परिवर्तन, या नष्ट होने से बचाया जाता है और अधिकांश समाजों में कंप्यूटर सिस्टम पर बढ़ती निर्भरता के कारण बढ़ते महत्व के हैं। पेशेवर साइबर सुरक्षा सलाहकार के अनुसार ऐसे किसी संगठन का पता लगाना बहुत कठिन है, जिसके डेटा से किसी तरह का समझौता नहीं किया जाता है। साइबर सुरक्षा में संक्षिप्त सी.आई.ए. उन प्रमुख तरीकों को बताता है जिनमें डेटा जोखिम में हो सकता है।



चित्र 10.1: सी.आई.ए.

कोई भी तीन व्यवसाय के लिए बड़े पैमाने पर गिरावट का कारण बन सकते हैं, विशेष रूप से वे जो अपने व्यापार का ऑनलाइन संचालन करते हैं। जैसे-जैसे कई संगठनों में साइबर सुरक्षा का महत्व बढ़ता जाता है, पेशेवर यह समझते हैं कि व्यापक संगठनात्मक लक्ष्यों के साथ साइबर सुरक्षा उद्देश्य कैसे तेजी से महत्वपूर्ण होंगे।

10.2.2 साइबर सुरक्षा प्रासंगिकता

साइबर सुरक्षा निम्नलिखित के लिए विशेष रूप से प्रासंगिक है:

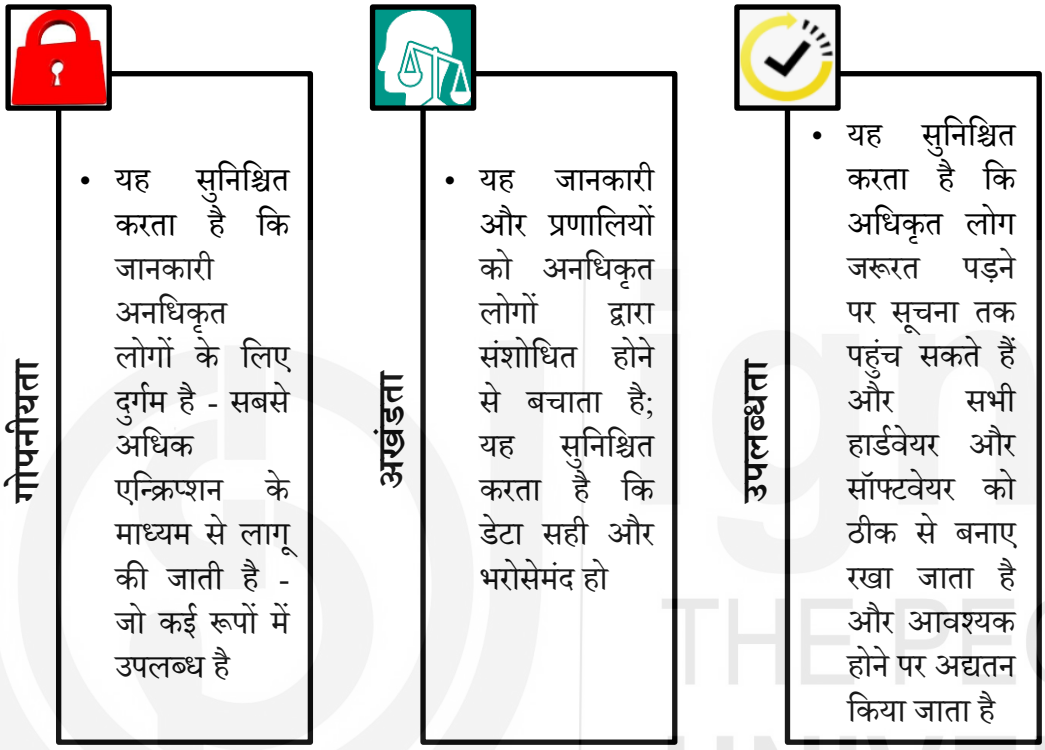
- इंटरनेट से जुड़ी सेवाओं, स्मार्ट उपकरणों और संचार प्रणालियों के सुरक्षित उपयोग को सक्षम करना।
- सभी आईटी नियंत्रित व्यावसायिक कार्यों, महत्वपूर्ण राष्ट्रीय अवसंरचनाओं के सुरक्षित उपयोग को सक्षम करना।
- अनधिकृत पहुंच का पता लगाना और उसकी रोकथाम करना।
- आईटी सिस्टम और क्लाउड सेवाओं की उपलब्धता।
- ग्राहकों की निजी और अंतरंग जानकारी और डेटा का सुरक्षित भंडारण।
- कानूनी और नियामक अनुपालन।

इस इकाई में शामिल सामग्री मौजूदा दुनिया के भीतर साइबर सुरक्षा और अन्य संबंधित सुरक्षा कार्यों की भूमिका को समझने के लिए पर्याप्त विवरण प्रदान करेगी।

10.3 सूचना सुरक्षा बनाम साइबर सुरक्षा

ये दो शब्द "साइबर सुरक्षा" और "सूचना सुरक्षा" आमतौर पर सुरक्षा शब्दावली में समानार्थक शब्द के रूप में उपयोग किए जाते हैं, और सुरक्षा पेशेवरों के बीच बहुत भ्रम पैदा करते हैं। कुछ सूचना सुरक्षा पेशेवरों को लगता है कि साइबर सुरक्षा सूचना सुरक्षा के सबसेट है जबकि अन्य इसके विपरीत सोचते हैं। इसलिए, इस भ्रम को दूर करने के लिए, डेटा सुरक्षा के साथ शुरुआत करें। डेटा सुरक्षा डेटा को सुरक्षित करने के बारे में है। अब यहां एक और सवाल उठता है कि

डेटा और सूचना के बीच अंतर क्या है। हर डेटा जानकारी नहीं हो सकता। जब किसी संदर्भ में व्याख्या की जाती है और अर्थ दिया जाता है तो डेटा को सूचना कहा जा सकता है। उदाहरण के लिए, "14041989 4 डेटा है। और अगर हम जानते हैं कि यह किसी व्यक्ति की जन्म तिथि (DOB) है, तो यह जानकारी है। तो, सूचना का अर्थ डेटा है जिसका कुछ अर्थ है, और सूचना सुरक्षा (जिसे इन्फोसेक भी कहा जाता है) जानकारी की सुरक्षा के बारे में है, जो आम तौर पर सूचना की गोपनीयता, अखंडता, उपलब्धता (सी.आई.ए.) पर ध्यान केंद्रित करती है। सी.आई.ए. के घटक हैं:



चित्र 10.2: सी.आई.ए. के घटक

सी.आई.ए. संयोजन संगठन को सुरक्षित रखने के लिए वास्तविक मानक मॉडल बन गया है। तीन मूलभूत सिद्धांत आपके डेटा को संरक्षित और संरक्षित करने के लिए सुरक्षा नियंत्रण का एक मजबूत सेट बनाने में मदद करते हैं।

सूचना सुरक्षा सुनिश्चित करती है कि भौतिक और डिजिटल दोनों डेटा अनधिकृत पहुँच, उपयोग, प्रकटीकरण, व्यवधान, संशोधन, निरीक्षण, रिकॉर्डिंग या नष्ट होने से सुरक्षित हैं। सूचना सुरक्षा साइबर सुरक्षा से भिन्न होती है, जिसमें इंफोसेक का उद्देश्य किसी भी रूप में डेटा की सुरक्षा बनाए रखना है। जबकि साइबर सुरक्षा केवल डिजिटल डेटा की रक्षा करती है यानी साइबर सुरक्षा आई.सी.टी के माध्यम से असुरक्षित चीजों को सुरक्षित करने के बारे में है। यह भी माना जाता है कि डेटा कहाँ संग्रहीत किया जाता है और डेटा को सुरक्षित करने के लिए कौन सी तकनीकों का उपयोग किया जाता है अर्थात, साइबर सुरक्षा सूचना सुरक्षा का एक सबसेट है, और यह आपके संगठन के नेटवर्क, कंप्यूटर और डेटा को अनधिकृत डिजिटल पहुँच, हमले या क्षति से बचाने का अभ्यास है जो विभिन्न प्रक्रियाओं, प्रौद्योगिकियों और प्रथाओं को लागू करके किया जाता है।

एक और तुलना पर ध्यान देने की आवश्यकता है यानी साइबर सुरक्षा और कंप्यूटर सुरक्षा, दोनों शब्द अलग हैं। हालांकि दोनों संबंधित हैं और एक जैसे लगते हैं, लेकिन वे दो अलग-अलग शब्द हैं। कंप्यूटर सुरक्षा में आम तौर पर कंप्यूटर हार्डवेयर जैसे कंप्यूटर के विभिन्न भागों की सुरक्षा शामिल होती है और यह कंप्यूटर में संग्रहीत जानकारी के बैकअप से भी संबंधित है, जबकि साइबर बहुत अधिक जटिल और व्यापक क्षेत्र है। यह उन सभी खतरों से संबंधित है जो साइबर (कंप्यूटर- ऑनलाइन और ऑफलाइन) दुनिया में हो सकते हैं। यह वायरस हो सकता है, आपकी व्यक्तिगत जानकारी चुराते हुए, साइबर अपराधियों द्वारा की गई धोखाधड़ी और कई और बातों पर ध्यान दिया जाता है। यदि आपका व्यवसाय एक सुरक्षा कार्यक्रम विकसित करना शुरू कर रहा है, तो सूचना सुरक्षा आपको सबसे पहले शुरू करना चाहिए, क्योंकि यह डेटा सुरक्षा की नींव है।

10.4 साइबर वर्ल्ड की मूल बातें

जैसा कि हम जानते हैं कि साइबर सुरक्षा का इतिहास 1970 के दशक के दौरान एक शोध परियोजना के साथ शुरू हुआ था, जिसे तब ARPANET (उन्नत अनुसंधान परियोजना एजेंसी नेटवर्क) के रूप में जाना जाता था। बॉब थॉमस नाम के एक शोधकर्ता ने एक कंप्यूटर प्रोग्राम बनाया जो ARPANET के नेटवर्क को स्थानांतरित करने में सक्षम था, जहां भी वह गया, एक छोटा सा निशान छोड़ गया। साइबर वर्ल्ड, या साइबरस्पेस, केवल इंटरनेट से अधिक है। यह एक ऑनलाइन वातावरण को संदर्भित करता है जहां कई प्रतिभागी सामाजिक बातचीत में शामिल होते हैं और एक-दूसरे को प्रभावित करने की क्षमता रखते हैं। लोग डिजिटल मीडिया के उपयोग के माध्यम से साइबरस्पेस में बातचीत करते हैं।

10.4.1 इंटरनेट और वर्ल्ड वाइड वेब

अब, साइबर सुरक्षा के लिए अगले स्तर की समझ के लिए इंटरनेट और डब्ल्यू.डब्ल्यू.डब्ल्यू (वर्ल्ड वाइड वेब) के बीच अंतर को समझना आवश्यक है। अधिकांश लोग इंटरनेट और डब्ल्यू.डब्ल्यू.डब्ल्यू (www) शब्दों का परस्पर उपयोग करते हैं। वास्तव में, वे दोनों के बीच कोई अंतर नहीं देखते हैं। केवल कुछ उत्सुक लोग इंटरनेट और डब्ल्यू. डब्ल्यू. डब्ल्यू के बीच अंतर के बारे में पूछते हैं। उन्हें आश्चर्य होता है कि क्या ये दोनों चीजें समान हैं। यदि नहीं, तो दोनों में क्या अंतर हैं? इसका त्वरित उत्तर यह है कि तकनीकी रूप से इंटरनेट और डब्ल्यू.डब्ल्यू.डब्ल्यू एक ही चीजें नहीं हैं, और इस खंड में, हम इन दो शब्दों के बीच के प्रमुख अंतरों को समझेंगे।

इंटरनेट: इंटरनेट नेटवर्क का एक विशाल नेटवर्क है। यह अनिवार्य रूप से दुनिया भर में बिखरे लाखों छोटे कंप्यूटर नेटवर्क के बीच एक दूसरे का संबंध है। ये नेटवर्क ओवर केबल, भूमिगत केबल, उपग्रह लिंक और उप-महासागरीय केबलों आदि के माध्यम से एक दूसरे से जुड़े हुए हैं। "इंटरनेट" शब्द वास्तव में नेटवर्क में मौजूद पूरे हार्डवेयर बुनियादी ढांचे को संदर्भित करता है। इस तरह के हार्डवेयर में कंप्यूटर सिस्टम, राउटर, केबल, ब्रिज, सर्वर, सेलुलर टॉवर, उपग्रह और अन्य वस्तुएँ शामिल हैं। हार्डवेयर के ये सभी वस्तुएँ इंटरनेट प्रोटोकॉल (आईपी) के तहत काम करते हैं। इंटरनेट में विभिन्न कंप्यूटिंग उपकरणों की पहचान उनके आई पी पते से की जाती है।

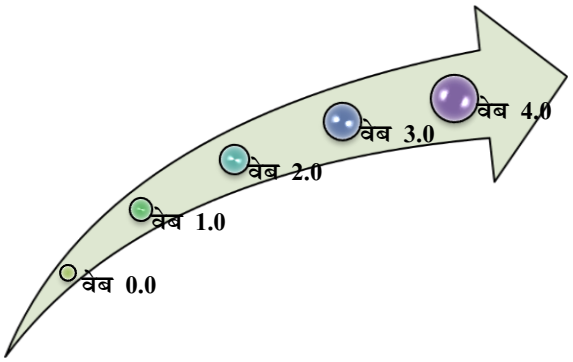
वर्ल्ड वाइड वेब (डब्ल्यू.डब्ल्यू.डब्ल्यू): जीवन के दौरान, जब लोग "इंटरनेट" कहते हैं, तो अधिकांश समय वे वास्तव में वर्ल्ड वाइड वेब या डब्ल्यू.डब्ल्यू.डब्ल्यू का उल्लेख करते हैं। डब्ल्यू.डब्ल्यू.डब्ल्यू इंटरनेट में उपलब्ध सभी सूचनाओं का संग्रह है। तो, सभी पाठ, चित्र, ऑडियो, वीडियो ऑनलाइन डब्ल्यू.डब्ल्यू.डब्ल्यू बनाते हैं। इस जानकारी को ज्यादातर वेबसाइटों के माध्यम से एक्सेस किया जाता है और हम वेबसाइटों को उनके डोमेन नामों से पहचानते हैं। डब्ल्यू.डब्ल्यू.डब्ल्यू में भारी मात्रा में जानकारी उपलब्ध है। इस जानकारी का केवल एक छोटा सा हिस्सा गूगल जैसे लोकप्रिय खोज इंजन के माध्यम से खोजा जा सकता है। हालाँकि, अधिकांश जानकारी डीप वेब और डार्क वेब में निहित है। डब्ल्यू.डब्ल्यू.डब्ल्यू विभिन्न सर्वरों से जानकारी तक पहुंचने के लिए एच टी टी पी (http) प्रोटोकॉल का उपयोग करता है। सूचना वेब पेजों के रूप में भेजी जाती है जो वेबसाइटों के रूप में व्यवस्थित होती हैं। हाइपरलिंक के माध्यम से विभिन्न वेब पेज एक-दूसरे से जुड़े हुए हैं। वेब पेज और डब्ल्यू.डब्ल्यू.डब्ल्यू में अन्य जानकारी उनके पते से पहचाने जाते हैं। निम्न तालिका दो शब्दों के बीच के प्रमुख अंतरों को सूचीबद्ध करती है।

तालिका 10.1 इंटरनेट और डब्ल्यू.डब्ल्यू.डब्ल्यू के बीच अंतर

क्र. स.	इंटरनेट	डब्ल्यू.डब्ल्यू.डब्ल्यू
1.	1960 के दशक के अंत में इंटरनेट की उत्पत्ति हुई।	अंग्रेजी वैज्ञानिक टिम बर्नर्स-ली ने 1989 में वर्ल्ड वाइड वेब का आविष्कार किया था।
2.	इंटरनेट की प्रकृति हार्डवेयर है।	डब्ल्यू.डब्ल्यू.डब्ल्यू की प्रकृति सॉफ्टवेयर है।
3.	इंटरनेट में कंप्यूटर, राउटर, केबल, ब्रिज, सर्वर, सेल्युलर टॉवर, सैटेलाइट आदि होते हैं।	डब्ल्यू.डब्ल्यू.डब्ल्यू में टेक्स्ट, इमेज, ऑडियो, वीडियो जैसी जानकारी होती है।
4.	इंटरनेट के पहले संस्करण को ARPANET के रूप में जाना जाता था।	शुरुआत में डब्ल्यू.डब्ल्यू.डब्ल्यू को NSFNET के रूप में जाना जाता था।
5.	इंटरनेट प्रोटोकॉल (आई पी) के आधार पर इंटरनेट काम करता है।	डब्ल्यू.डब्ल्यू.डब्ल्यू हाइपर टेक्स्ट ट्रांसफर प्रोटोकॉल (एच टी टी पी) के आधार पर काम करता है।
6.	इंटरनेट डब्ल्यू.डब्ल्यू.डब्ल्यू से स्वतंत्र है।	डब्ल्यू.डब्ल्यू.डब्ल्यू के लिए इंटरनेट मौजूद होना आवश्यक है।
7.	इंटरनेट डब्ल्यू.डब्ल्यू.डब्ल्यू का सुपरसेट है।	डब्ल्यू.डब्ल्यू.डब्ल्यू इंटरनेट का एक सबसेट (भाग) है। डब्ल्यू.डब्ल्यू.डब्ल्यू का समर्थन करने के अलावा, इंटरनेट के हार्डवेयर बुनियादी ढांचे का उपयोग अन्य चीजों के लिए भी किया जाता है (जैसे, एफ़ टी पी, एस एम टी पी)
8.	आई.पी पते द्वारा कम्प्यूटिंग उपकरणों की पहचान की जाती है।	सूचना यूनिफ़ॉर्म रिसोर्स लोकेटर (यू आर एल) द्वारा पहचाने जाते हैं।

10.4.2 वर्ल्ड वाइड वेब (WWW) का विकास

वर्ल्ड वाइड वेब वेब 0.0 वेब 1.0 वेब 2.0, वेब 3.0 और अब वेब 4.0 से विकसित हुआ है, प्रत्येक पीढ़ी के लिए संक्षिप्त विवरण निम्नलिखित हैं:



चित्र 10.3: वर्ल्ड वाइड वेब का विकास

1) **वेब 0.0 (इंटरनेट का विकास करना):** यह चरण इंटरनेट के विकास के चरण को संदर्भित करता है।

2) **वेब 1.0 (शॉपिंग कार्ट और स्टैटिक वेब):** विशेषज्ञ 1999 के पहले इंटरनेट को "रीड ओनली" वेब कहते हैं। औसत इंटरनेट उपयोगकर्ता की भूमिका उस जानकारी को पढ़ने तक सीमित थी जो उसे प्रस्तुत की गई थी। टिम बर्नर्स-ली के अनुसार वेब का पहला कार्यान्वयन, वेब 1.0 का प्रतिनिधित्व करता है, इसे "केवल पढ़ने के लिए वेब" माना जा सकता है।

3) **वेब 2.0 (लेखन और भाग लेने वाला वेब):** वेब 2.0 का जन्म वेब लीड के साथ आम उपयोगकर्ताओं की सक्रिय बातचीत की कमी के कारण हुआ। इस युग ने आम उपयोगकर्ता को ब्लॉग, सोशल-मीडिया और वीडियो-स्ट्रीमिंग जैसी कुछ नई अवधारणाओं के साथ सशक्त बनाया।

4) **वेब 3.0 (सिमेंटिक एक्ज़ीक्यूटिंग वेब):** वेब 3.0 एक "रीड-राइट-एक्ज़ीक्यूट" वेब है।

5) **वेब 4.0 (मोबाइल वेब):** अगला चरण वास्तव में एक नया संस्करण नहीं है, लेकिन हमारे पास पहले से मौजूद एक वैकल्पिक संस्करण है। हमें इसके मोबाइल परिवेश के अनुकूल होने की आवश्यकता थी। वेब 4.0 वास्तविक समय में सभी उपकरणों को वास्तविक और आभासी दुनिया में जोड़ता है।

6) **वेब 5.0 (खुला, जुड़ा हुआ और बुद्धिमान वेब = भावनात्मक वेब):** "अगला वेब" यद्यपि वेब 5.0 अभी भी विकासशील मोड में है और सही आकार अभी भी बन रहा है, पहले संकेत हैं कि वेब 5.0 एक जुड़े हुए वेब के बारे में होगा जो हमारे साथ संचार करता है जैसे हम एक दूसरे के साथ संवाद करते हैं (एक व्यक्तिगत सहायक की तरह)। वेब 5.0 को "सहजीवी" वेब कहा जाता है। यह वेब बहुत शक्तिशाली और पूरी तरह से क्रियान्वित होगा। वेब 5.0 रीड-राइट-एग्जीक्यूशन-कॉन्सेप्ट वेब होगा। वेब 5.0 मानव और कंप्यूटर के बीच (भावनात्मक) बातचीत के बारे में होगा। न्यूरो तकनीक पर आधारित बहुत से लोगों के लिए बातचीत एक दैनिक आदत बन जाएगी। एक पल के लिए वेब "भावनात्मक रूप से" तटस्थ है, जिसका अर्थ है कि वेब उपयोगकर्ताओं को महसूस और भावनाओं का अनुभव नहीं करता है। यह वेब

5.0 के साथ बदल जाएगा - भावनात्मक वेब। इसका एक उदाहरण www.wefeelfine.org है, जो लोगों की भावनाओं को दर्शाता है। हेडफ़ोन ऑन के साथ, उपयोगकर्ता उन सामग्रियों के साथ बातचीत करेंगे जो उनकी भावनाओं के साथ बातचीत करती हैं या चेहरे की पहचान में परिवर्तन करती हैं।

जैसे-जैसे डब्ल्यू.डब्ल्यू.डब्ल्यू की बैंडविड्थ आवश्यकताएं बढ़ रही हैं, अधिक से अधिक उपयोगकर्ता अपने स्मार्ट गैजेट्स के माध्यम से डब्ल्यू.डब्ल्यू.डब्ल्यू से जुड़ रहे हैं और इसलिए डब्ल्यू.डब्ल्यू.डब्ल्यू पर इन गैजेट्स का प्रबंधन करना बेहद महत्वपूर्ण है, डब्ल्यू.डब्ल्यू.डब्ल्यू पर डिवाइस को ट्रैक करने के लिए इस्तेमाल किया जाने वाला कनेक्शन कम एड्रेसिंग प्रोटोकॉल आपका इंटरनेट प्रोटोकॉल (आई.पी) है।

आई.पी (इंटरनेट प्रोटोकॉल का संक्षिप्त रूप) एक नेटवर्क पर संचार करने के लिए पैकेट के तकनीकी प्रारूप और कंप्यूटर के लिए एड्रेसिंग स्कीम को निर्दिष्ट करता है। अधिकांश नेटवर्क एक उच्च-स्तरीय प्रोटोकॉल के साथ आईपी को जोड़ते हैं जिसे ट्रांसमिशन कंट्रोल प्रोटोकॉल (टी.सी.पी) कहा जाता है, जो गंतव्य और स्रोत के बीच एक आभासी संपर्क स्थापित करता है। आई.पी की डाक प्रणाली की तरह तुलना की जा सकती है। यह आपको एक पैकेज को संबोधित करने और इसे सिस्टम में छोड़ने की अनुमति देता है, लेकिन आपके और प्राप्तकर्ता के बीच कोई सीधा संबंध नहीं होता है। दूसरी ओर, टी.सी.पी / आई.पी (TCP/IP) दो मेजबानों के बीच एक संबंध स्थापित करता है ताकि वे समय-समय पर संदेश भेज सकें।

आने वाली प्रौद्योगिकियां जैसे कि आई. ओ. टी (इंटरनेट ऑफ थिंग्स), ब्लॉकचेन, क्लाउड कम्प्यूटिंग आदि, डब्ल्यू.डब्ल्यू.डब्ल्यू की बैंडविड्थ आवश्यकता में निरंतर वृद्धि का परिणाम हैं, इस प्रकार अधिक से अधिक डिवाइस इंटरनेट / डब्ल्यू.डब्ल्यू.डब्ल्यू से कनेक्ट हो रहे हैं। अब, इन उपकरणों को विशिष्ट रूप से पहचानने के लिए, आई.पी एड्रेसिंग पर भी ध्यान देने की आवश्यकता है। इस प्रकार, इंटरनेट (डब्ल्यू.डब्ल्यू.डब्ल्यू) पर उपकरणों की इन बढ़ती संख्या को संबोधित करने के लिए आई पी वी -4 (इंटरनेट प्रोटोकॉल संस्करण -4) से आई पी वी -6 (इंटरनेट प्रोटोकॉल संस्करण -6) पर जाना आवश्यक है, क्योंकि आई पी वी -6 प्रोटोकॉल में अधिक उपकरणों को संबोधित करने की क्षमता है । यह आई पी वी 6 अगली पीढ़ी का इंटरनेट प्रोटोकॉल (आई पी) मानक है जिसका उद्देश्य अंततः आई पी वी 4 को बदलना है, प्रोटोकॉल कई इंटरनेट सेवाएं आज भी उपयोग करती हैं। प्रत्येक कंप्यूटर, मोबाइल फोन और इंटरनेट से जुड़े किसी भी अन्य डिवाइस को अन्य उपकरणों के साथ संचार करने के लिए संख्यात्मक आई पी पते की आवश्यकता होती है। आई पी वी 4 नामक मूल (आई पी) पता योजना, पतों से बाहर चल रही है, क्योंकि आई पी वी 4 कुल 2 ^ 32 पतों (सिर्फ 4 बिलियन से अधिक पतों) के लिए 32-बिट एड्रेस स्कीम का उपयोग करता है। जबकि आई पी वी 6 पते हेक्साडेसिमल (hexadecimal) में लिखे गए 128-बिट आई.पी पते और कॉलन द्वारा अलग किए गए हैं, इस प्रकार यह बड़ी संख्या में उपकरणों को पूरा करता है और इसलिए वर्तमान तकनीकी जरूरतों के लिए काफी उपयुक्त है।

10.4.3 साइबर स्पेस

अब डब्ल्यू.डब्ल्यू.डब्ल्यू पर उपकरणों की बढ़ती संख्या और डब्ल्यू.डब्ल्यू.डब्ल्यू की बढ़ती बैंडविड्थ के कारण, अधिक से अधिक उपयोगकर्ता डब्ल्यू.डब्ल्यू.डब्ल्यू से जुड़े हुए हैं,

जिससे साइबर दुनिया से सुरक्षा के उल्लंघन और खतरों की संभावना बढ़ जाती है, इस प्रकार हमें साइबर सुरक्षा की आवश्यकता है और यह समझने के लिए कि साइबर सुरक्षा का क्या मतलब है इसकी शरुआत साइबरस्पेस की परिभाषा को देखते हुए करना मददगार है।

साइबरस्पेस डिजिटल नेटवर्क से बना एक इंटरैक्टिव डोमेन है जिसका उपयोग सूचनाओं को संग्रहीत करने, संशोधित करने और संचार करने के लिए किया जाता है। इसमें इंटरनेट भी शामिल है, लेकिन हमारी कंपनियों, बुनियादी ढांचे और सेवाओं का समर्थन करने वाली अन्य सूचना प्रणालियाँ भी शामिल हैं। साइबरस्पेस को एक बहु-परत मॉडल में विभाजित किया जा सकता है, जिसमें निम्न शामिल हैं:

1) **भौतिक नींव:** जैसे कि भूमि और पनडुब्बी केबल, और उपग्रह जो मार्ग प्रदान करते हैं, साथ ही राउटर भी होते हैं जो इसकी जानकारी को सीधे गंतव्य तक पहुंचाते हैं।

2) **लॉजिकल बिल्डिंग ब्लॉक्स:** जिसमें स्मार्ट फोन ऐप, ऑपरेटिंग सिस्टम या वेब ब्राउजर जैसे सॉफ्टवेयर शामिल हैं, जो फिजिकल फाउन्डेशन को कार्य करने और संचार करने की अनुमति देते हैं।

3) **सूचना:** जो सोशल मीडिया पोस्ट, ग्रंथ, वित्तीय स्थानान्तरण या वीडियो डाउनलोड जैसे साइबरस्पेस को स्थानांतरित करती है। पारगमन से पहले और बाद में, यह जानकारी अक्सर (और संशोधित) कंप्यूटर और मोबाइल उपकरणों, या सार्वजनिक या निजी क्लाउड स्टोरेज सेवाओं पर संग्रहीत होती है।

4) **लोग:** यह साइबरस्पेस के भौतिक और तार्किक घटकों की जानकारी, संचार और डिजाइन में हेरफेर करता है।

सामूहिक रूप से इन मूर्त और अमूर्त परतों में साइबर स्पेस शामिल है, जिसे हम दैनिक जीवन के आवश्यक घटकों पर निर्भर कर रहे हैं। महत्वपूर्ण बुनियादी ढाँचे के सुचारू संचालन के लिए एक भरोसेमंद और स्थिर साइबरस्पेस आवश्यक है, जिसमें सॉफ्टवेयर, हार्डवेयर और नेटवर्क शामिल हैं।

10.4.4 साइबर सुरक्षा

साइबर सुरक्षा कंप्यूटर सिस्टम की चोरी या क्षति से उनके हार्डवेयर, सॉफ्टवेयर या इलेक्ट्रॉनिक डेटा की सुरक्षा के साथ-साथ उनके द्वारा प्रदान की जाने वाली सेवाओं के विघटन या गलत तरीके से संरक्षण है। इसे तीन श्रेणियों में वर्गीकृत किया जा सकता है:

1) **सूचना सुरक्षा:** सूचना सुरक्षा का उद्देश्य उपयोगकर्ताओं की निजी जानकारी को अनधिकृत पहुंच और पहचान की चोरी से बचाना है। यह डेटा और हार्डवेयर की गोपनीयता की रक्षा करता है जो उस डेटा को संभालता है, संग्रहीत करता है और संचारित करता है। सूचना सुरक्षा के उदाहरणों में उपयोगकर्ता प्रमाणीकरण और क्रिप्टोग्राफी शामिल हैं।
2) **नेटवर्क सुरक्षा:** नेटवर्क सुरक्षा का उद्देश्य किसी नेटवर्क, संबद्ध घटकों और नेटवर्क पर साझा किए गए डेटा की उपयोगिता, अखंडता और सुरक्षा की रक्षा करना है। जब कोई नेटवर्क सुरक्षित होता है, तो संभावित खतरों को उस नेटवर्क में प्रवेश करने या फैलने से रोक दिया जाता है। नेटवर्क सुरक्षा के उदाहरणों में एंटीवायरस और एंटीस्पायवेयर प्रोग्राम,

फ़ायरवॉल शामिल हैं जो सुरक्षित रिमोट एक्सेस के लिए उपयोग किए जाने वाले नेटवर्क और वी पी एन (वर्चुअल प्राइवेट नेटवर्क) तक अनधिकृत पहुंच को ब्लॉक करते हैं।

3) **एप्लीकेशन सुरक्षा:** एप्लीकेशन सुरक्षा का उद्देश्य सॉफ्टवेयर एप्लिकेशन को उन कमजोरियों से बचाना है जो एप्लिकेशन डिजाइन, विकास, इंस्टॉलेशन और अपग्रेड या रखरखाव चरणों की खामियों के कारण होती हैं।

साइबर दुनिया की बुनियादी समझ रखने के लिए, किसी को साइबर स्पेस की बुनियादी शर्तों के साथ मूल शब्दों से परिचित होना चाहिए, कुछ सबसे महत्वपूर्ण साइबर सुरक्षा शब्दावली जो किसी को पता होनी चाहिए, इस प्रकार हैं:

1) **क्लाउड:** एक तकनीक जो हमें दुनिया में कहीं से भी इंटरनेट के माध्यम से हमारी फ़ाइलों और / या सेवाओं तक पहुंचने की अनुमति देती है। तकनीकी रूप से, यह बड़ी भंडारण क्षमताओं वाले कंप्यूटरों का एक संग्रह है जो दूरस्थ रूप से अनुरोधों को पूरा करता है।
2) **सॉफ्टवेयर:** प्रोग्राम का एक सेट जो कंप्यूटर को किसी कार्य को करने के लिए कहता है। इन निर्देशों को एक पैकेज में संकलित किया जाता है जिसे उपयोगकर्ता इंस्टॉल और उपयोग कर सकते हैं। उदाहरण के लिए, माइक्रोसॉफ्ट ऑफिस एक अनुप्रयोग सॉफ़्टवेयर (Application Software) है।
3) **डोमेन:** कंप्यूटर, प्रिंटर और उपकरणों का एक समूह जो एक दूसरे के रूप में परस्पर जुड़े और संचालित होते हैं। उदाहरण के लिए, आपका कंप्यूटर आमतौर पर आपके कार्यस्थल पर एक डोमेन का हिस्सा होता है।
4) **वर्चुअल प्राइवेट नेटवर्क (वी.पी.एन):** एक उपकरण जो उपयोगकर्ता को स्थान का उपयोग करके और ट्रैफ़िक को एन्क्रिप्ट करके इंटरनेट का उपयोग करते समय गुमनाम रहने की अनुमति देता है।
5) **आई.पी पता:** आपके कंप्यूटर के लिए एक घर के पते का एक इंटरनेट संस्करण, जिसे नेटवर्क पर संचार करने पर पहचाना जाता है; उदाहरण के लिए, इंटरनेट से कनेक्ट करना (नेटवर्क के द्वारा नेटवर्क)।
6) **शोषण:** एक दुर्भावनापूर्ण एप्लिकेशन या स्क्रिप्ट जिसका उपयोग कंप्यूटर की भेद्यता का लाभ उठाने के लिए किया जा सकता है।
7) **ब्रीच:** एक हैकर एक कंप्यूटर या डिवाइस में भेद्यता का सफलतापूर्वक शोषण करता है, और अपनी फ़ाइलों और नेटवर्क तक पहुंच प्राप्त करता है।
8) **फ़ायरवॉल:** बुरे लोगों (साइबर खतरों) को बाहर रखने के लिए डिज़ाइन की गई एक रक्षात्मक तकनीक है। फायरवॉल हार्डवेयर या सॉफ्टवेयर आधारित हो सकता है।
9) **मालवेयर:** यह शब्द कंप्यूटर पर कहर बरपाने के लिए डिज़ाइन किए गए सभी प्रकार के दुर्भावनापूर्ण सॉफ़्टवेयर का वर्णन करता है। सामान्य रूप से इसमें निम्नलिखित शामिल हैं; वायरस, ट्रोजन, वार्म और रैंसमवेयर जिनका विवरण निम्न है।
   i) **वायरस:** एक प्रकार का मैलवेयर जिसका उद्देश्य दूसरों तक फैलने से पहले कंप्यूटर पर जानकारी को भ्रष्ट करना, मिटाना या संशोधित करना है। हालांकि, हाल के वर्षों में, स्टक्सनेट जैसे वायरस ने शारीरिक क्षति पहुंचाई है।
   ii) **रैंसमवेयर:** मालवेयर का एक रूप जो जानबूझकर आपको अपने कंप्यूटर पर फ़ाइलों तक पहुँचने से रोकता है, आपके डेटा को बंधक बनाकर रखता है। यह आम तौर पर फ़ाइलों को एन्क्रिप्ट करता है और अनुरोध करता है कि उन्हें फिर से

डिक्रिप्ट या पुनर्प्राप्त करने के लिए भुगतान किया जाना चाहिए। उदाहरण के लिए, वनाक्राई रैंसमवेयर।

iii) **ट्रोजन हॉर्स:** मैलवेयर का एक प्रकार जो अक्सर एक हैकर को "बैक डोर" के माध्यम से कंप्यूटर तक दूरस्थ पहुंच प्राप्त करने की अनुमति देता है।

iv) **वार्म:** मैलवेयर का एक प्रकार जो अन्य जुड़े हुए कंप्यूटरों में संक्रमण फैलाने के लिए खुद को दोहरा सकता है।

v) **बॉट / बोटनेट:** एक प्रकार का सॉफ़्टवेयर एप्लिकेशन या स्क्रिप्ट जो कमांड पर कार्य करता है, एक हमलावर को एक प्रभावित कंप्यूटर के दूरस्थ रूप से पूर्ण नियंत्रण लेने की अनुमति देता है। इन संक्रमित कंप्यूटरों के संग्रह को "बॉटनेट" के रूप में जाना जाता है और हैकर या "बॉट-हैडर" द्वारा नियंत्रित किया जाता है।

vi) **डी डी ओ एस:** यह एक संक्षिप्त नाम जो सेवा से वंचित करने के लिए खड़ा है - साइबर-हमले का एक रूप है। इस हमले का उद्देश्य एक ऐसी वेबसाइट बनाना है, जो दुर्भावनापूर्ण ट्रैफ़िक या कई स्रोतों (अक्सर बॉटनेट) से डेटा की बहुलता द्वारा बेकार हो जाती है।

vii) **फ़िशिंग या स्पीयर फ़िशिंग:** यह संवेदनशील जानकारी प्राप्त करने के लिए हैकर्स द्वारा उपयोग की जाने वाली तकनीक। उदाहरण के लिए, हाथ से तैयार किए गए ईमेल संदेशों का उपयोग करके लोगों को पासवर्ड या बैंक खाते की जानकारी जैसे व्यक्तिगत या गोपनीय डेटा को विभाजित करने के लिए डिज़ाइन किया गया है।

यह विभिन्न शब्दों का संक्षिप्त परिचय है। हम इस इकाई के आने वाले वर्गों में कई और अवधारणाओं पर चर्चा करेंगे।

10.5 सुरक्षा की आवश्यकता एवं अवधारणा

"सुरक्षा ज्ञान इतना महत्वपूर्ण क्यों है?" आइए सबसे पहले हम इस आधारभूत आधार को स्थापित हममें से अधिकांश का दैनिक जीवन कैसे संचालित होता है। "ऐसे कोई करियर नहीं बचे हैं, जो तकनीक पर आधारित नहीं हैं, आजकल क्लासरूम में भी शिक्षक स्मार्ट बोर्ड का उपयोग कर रहे हैं, और कई बार कोई ऐसा व्यक्ति जो आपके घर अनुबंध कार्य करने के लिए आता है एक स्मार्ट फोन या टैबलेट का उपयोग कर ऐप पर जानकारी जोड़ता है। मौके पर किसी ऐप की जानकारी, ईमेल में अटैचमेंट पर क्लिक करने जितना छोटा है, बिना यह जाने कि वह सुरक्षित है या और भी कई घटनाएं हैं जहां हमें यह समझने की जरूरत है कि ऐसी चीजें हमारी सुरक्षा को कैसे प्रभावित कर सकती हैं। कंपनियां निश्चित रूप से, सुरक्षा हेतु कार्य करती है क्योंकि यदि कोई भी गलती होती है तो उससे नुक्सान हो सकता है।

हमें यह समझने की आवश्यकता है कि "बुनियादी सुरक्षा ज्ञान किसी भी कैरियर को कैसे मदद कर सकता है?" केवल संदिग्ध ईमेल अटैचमेंट पर क्लिक न करने से, लगभग सभी कर्मचारी कंपनी सुरक्षा बढ़ाने और खुद को अधिक मूल्यवान श्रमिक बनाने के लिए काम कर सकते हैं। संगठन में किसी भी भूमिका हेतु सुरक्षा के बारे में सीखने से किसी व्यक्ति को जोखिमों को समझने और उनके प्रमुख हितधारकों के लिए सूचित निर्णय लेने में मदद मिल सकती है, यहां कुछ उदाहरण दिए गए हैं:

- बिक्री में, संगठन के ग्राहकों को पुन: बार-बार आश्वस्त करता है।
- कॉर्पोरेट संचार में, आपको व्यावसायिक प्रतिष्ठा और ब्रांड ट्रस्ट के संदर्भ में आकलन करना चाहिए।
- कानूनी टीम को यह सुनिश्चित करना चाहिए कि आपूर्तिकर्ता और ग्राहक अनुबंधों में सही सुरक्षा प्रावधान बनाए जाएं।
- मानव संसाधन और / या सुरक्षा के बारे में, बेहतर सुरक्षा जागरूकता और प्रशिक्षण के लिए क्या आवश्यक है जानें।
- उत्पाद प्रबंधकों को अच्छी सुरक्षा सुविधाओं पर सलाह देनी चाहिए।
- इंजीनियरिंग विकास में, सुनिश्चित करें कि आप सुरक्षित कोड विकसित करते हैं।
- सुरक्षा पेशेवरों को कार्यात्मक और सुरक्षा सत्यापन के लिए समीक्षा और गुणवत्ता आश्वासन परीक्षण करना चाहिए।
- कॉर्पोरेट प्रबंधन को यह सुनिश्चित करना चाहिए कि किसी भी भेद्यता का समाधान करने के लिए एक अच्छी सुरक्षा घटना प्रतिक्रिया योजना है।

जैसा कि आप देख सकते हैं, निश्चित रूप से सुरक्षा से संबंधित परियोजनाओं और जागरूकता में योगदान करने के लिए सुरक्षा पेशेवर होने की आवश्यकता नहीं है। वास्तव में, जितना अधिक कार्यबल इस ज्ञान के साथ है, उतना ही कम धन और समय सुरक्षा उल्लंघनों के लिए खर्च होगा । विभिन्न साइबर खतरों के विश्लेषण के आधार पर यह पाया गया है कि साइबर हमलावर मानव त्रुटि पर भरोसा करते हैं, हैकर्स केवल उनके सुरक्षा-प्रवेश कौशल पर आंशिक रूप से ही भरोसा करते हैं। दूसरी चीज़ जो उन्हें चाहिए, लोग गलती कर रहे हैं। जो लोग आईटी में काम नहीं करते हैं, लेकिन काम के लिए कंप्यूटिंग उपकरणों का उपयोग करते हैं, उनके लिए साइबर सुरक्षा प्रशिक्षण होना आवश्यक है ताकि वे यह समझ सकें कि मामूली गलतियों या साधारण ओवरसाइट्स से उनके संगठन की सुरक्षा या बुनियाद के बारे में विनाशकारी परिदृश्य कैसे हो सकता है। व्यक्तिगत स्तर पर भी यह एक समझदारी भरा कदम है, भले ही आपकी गलती पूरी तरह से अनजाने में हो, आप परिणामों से बचेंगे नहीं। कोई भी जॉब से निकाला जाना नहीं चाहता है, खासकर जब आपने अपनी कंपनी को नुकसान पहुंचाने के लिए कुछ भी दुर्भावनापूर्ण नहीं किया है, लेकिन यह बिल्कुल वैसा ही हो सकता है यदि आप किसी ईमेल फ़िशिंग अभियान या अन्य सामाजिक इंजीनियरिंग हमले के शिकार हो जाते हैं और वह वेक्टर बन जाता है जिससे आपकी कंपनी प्रभावित होती है। संवेदनशील जानकारी को उजागर करता है। परिचालन सुरक्षा की बात होने पर खुद को समझदार और सतर्क रहने के लिए शिक्षित करें।

10.5.1 साइबर सुरक्षा क्यों महत्वपूर्ण है?

आज की संलग्न दुनिया में, उन्नत साइबर रक्षा कार्यक्रमों से एक और सभी लाभ। व्यक्तिगत स्तर पर, एक साइबर-सुरक्षा हमला पहचान की चोरी से लेकर, जबरन वसूली के प्रयासों तक, पारिवारिक फोटो जैसे महत्वपूर्ण डेटा के नुकसान तक सब कुछ कर सकता है। प्रत्येक व्यक्ति बिजली संयंत्र, अस्पताल और वित्तीय सेवा कंपनियों जैसे महत्वपूर्ण बुनियादी ढांचे पर निर्भर करता है। इन और अन्य संगठनों को सुरक्षित करना हमारे समाज को कार्यशील रखने के लिए

आवश्यक है। दूसरी ओर साइबर सुरक्षा के महत्व पर जनता को शिक्षित करना, और खुले स्रोत उपकरण बनाना जो इंटरनेट को सभी के लिए सुरक्षित बना देगा।

बोध प्रश्न क:

1) CIA त्रय के विभिन्न घटक क्या हैं?

……

……

……

2) सुरक्षा ज्ञान इतना महत्वपूर्ण क्यों है?

……

……

……

……

3) साइबर स्पेस के विभिन्न स्तर क्या हैं?

……

……

……

……

4) रिक्त स्थान भरें:

1) …… डेटा को सुरक्षित करने के बारे में है।

2) क्लाउड एक ऐसी तकनीक है जो हमें अपनी फ़ाइलों और / या सेवाओं को …… के माध्यम से एक्सेस करने की अनुमति देती है। जो दुनिया में कहीं से भी किया जा सकता है।

3) एक दुर्भावनापूर्ण एप्लिकेशन या स्क्रिप्ट जिसका उपयोग कंप्यूटर के …… का लाभ उठाने के लिए किया जा सकता है

4) साइबरस्पेस एक …… .. डोमेन है जो डिजिटल नेटवर्क से बना है जिसका उपयोग सूचनाओं को संग्रहीत, संशोधित और संचार करने के लिए किया जाता है।

5) इंटरनेट एक विशाल …… का नेटवर्क है।

10.6 आई ओ टी और साइबर वर्ल्ड

साइबर सुरक्षा जीवन का एक महत्वपूर्ण पहलू बनती जा रही है और इस तरह के रवैये के पीछे तकनीकी निर्भरता के विकास के अलावा कुछ नहीं है। आजकल एक ऐसा कंप्यूटर होना चाहिए जो हर घर में व्यक्तिगत जानकारी से भरा हो, एक सामान्य बात है। यह सबसे महत्वपूर्ण चीजों में से एक है जिसे ध्यान में रखा जाना आवश्यक है कि अच्छी तरह के खतरों के साथ एक उपाय आता है। इस मामले में उपाय साइबर सुरक्षा के विकास के अलावा और कुछ नहीं

है। यह हमारे जीवन का एक आवश्यक घटक बन रहा है क्योंकि सुरक्षा जानकारी, स्वास्थ्य जानकारी, व्यक्तिगत जानकारी, वित्तीय जानकारी से संबंधित सभी डेटा इंटरनेट में संग्रहीत हैं। यह एक ऐसी जगह है जहां डेटा हमेशा के लिए रहेगा लेकिन यह सुरक्षित नहीं है जब तक कि इसे सुरक्षा प्रदान नहीं की जाती है। हम में से ज्यादातर लोग हमेशा स्मार्ट फोन, लैपटॉप, होम राउटर, स्मार्ट टीवी, हाई एंड कार, डीवीआर और कैमरा आदि के माध्यम से हर दिन इंटरनेट से जुड़े रहते हैं, जबकि इंटरनेट से जुड़े रहने से हमें ऑनलाइन शॉपिंग करने, मूवी देखने, संगीत का आनंद लेने मानचित्रों का उपयोग, ऑनलाइन खोज, हमारे बिलों का भुगतान आदि की सुविधा मिलती है, लेकिन इंटरनेट ऑफ थिंग्स के आगमन के साथ और भी अधिक गैजेट्स जैसे बल्ब, थर्मोस्टेट, एयर कंडीशनर इत्यादि जुड़े हुए हैं। दुर्भाग्य से, इनमें से कई कनेक्टेड डिवाइस को नई साइबर समस्याओं के लिए अग्रणी सुरक्षा को ध्यान में रखते हुए नहीं बनाया गया है। कंप्यूटर सुरक्षा और साइबर सुरक्षा चोरी, क्षति या उनके हार्डवेयर, सॉफ़्टवेयर या इलेक्ट्रॉनिक डेटा के साथ-साथ उनके द्वारा प्रदान की जाने वाली सेवाओं के विघटन या गलत व्यवहार से कंप्यूटर सिस्टम की सुरक्षा है। नीचे दिए गए कारण साइबर सुरक्षा को पहले से कहीं अधिक महत्वपूर्ण मानते हैं।

1) **उल्लंघनों की बढ़ती लागत:** तथ्य यह है कि व्यवसायों के लिए साइबर-हमलों को सहना बहुत महंगा हो सकता है। हाल के आंकड़ों ने सुझाव दिया है कि एक बड़ी फर्म में डेटा उल्लंघन की औसत लागत बहुत अधिक है। लेकिन यह वास्तव में एक कंपनी के खिलाफ हमले के वास्तविक खर्च को कम करके आंका जाता है। यह व्यवसाय के लिए केवल वित्तीय क्षति या बचाव का खर्च नहीं है; एक डेटा ब्रीच व्यवसायिक प्रतिष्ठित का भी नुकसान पहुंचा सकता है। साइबर-हमले का शिकार होने से ग्राहकों का व्यापार में विश्वास खो सकता है और वह अपना पैसा कहीं और खर्च कर सकता है। इसके अतिरिक्त, खराब सुरक्षा के लिए एक प्रतिष्ठा होने से नए अनुबंध जीतने में विफलता भी हो सकती है।

2) **तेजी से परिष्कृत हैकर्स:** लगभग हर व्यवसाय में एक वेबसाइट और बाहरी रूप से उजागर सिस्टम हैं जो अपराधियों को आंतरिक नेटवर्क में प्रवेश प्रदान कर सकते हैं। सफल डेटा उल्लंघनों से हैकर्स को बहुत फायदा होता है, और यूके में कुछ बड़ी कंपनियों के खिलाफ अच्छी तरह से वित्त पोषित और समन्वित साइबर हमलों के अनगिनत उदाहरण हैं। अब अत्यधिक परिष्कृत हमलों के साथ, व्यवसायों को यह समझने की ज़रूरत है कि वे कुछ बिंदु पर डेटा उल्लंघन हो जाएंगे और कंपनियों को नियंत्रणों को लागू करने होंगे जो उन्हें नुकसान और व्यवधान पैदा करने से पहले दुर्भावनापूर्ण गतिविधि का पता लगाने और प्रतिक्रिया देने में मदद करते हैं।

3) **व्यापक रूप से उपलब्ध हैकिंग टूल:** जबकि अच्छी तरह से वित्त पोषित और अत्यधिक कुशल हैकर्स आपके व्यवसाय के लिए एक महत्वपूर्ण जोखिम रखते हैं, इंटरनेट पर हैकिंग टूल और कार्यक्रमों की व्यापक उपलब्धता का मतलब यह भी है कि कम कुशल व्यक्तियों से भी खतरा बढ़ रहा है। साइबर अपराध के व्यावसायीकरण ने किसी के लिए उन संसाधनों को प्राप्त करना आसान बना दिया है जिनके लिए उन्हें हानिकारक हमलों को शुरू करने की आवश्यकता है, जैसे कि रैनसम वेयर और क्रिप्टो खनन।

4) **आई.ओ.टी उपकरणों का प्रसार:** पहले से कहीं अधिक स्मार्ट डिवाइस इंटरनेट से जुड़े हैं। इन्हें इंटरनेट ऑफ थिंग्स, या आई.ओ.टी, उपकरणों के रूप में जाना जाता है और ये

घरों और कार्यालयों में तेजी से बढ़ रहे हैं। ये उपकरण कार्यों को सरल और तेज कर सकते हैं, साथ ही नियंत्रण और पहुंच के अधिक से अधिक स्तर प्रदान करते हैं। हालाँकि, उनका प्रसार एक समस्या प्रस्तुत करता है। यदि ठीक से प्रबंधित नहीं किया जाता है, तो प्रत्येक आई.ओ.टी डिवाइस जो इंटरनेट से जुड़ा है, साइबर अपराधियों को एक व्यवसाय में एक रास्ता प्रदान कर सकता है। आई.टी सेवाओं की दिग्गज कंपनी सिस्को का अनुमान है कि 2021 तक वैश्विक स्तर पर 27.1 बिलियन कनेक्टेड डिवाइस होंगे इसलिए यह समस्या केवल समय के साथ बिगड़ जाएगी। आई.ओ.टी उपकरणों के उपयोग से संभावित रूप से सुरक्षा कमजोरियों की एक विस्तृत श्रृंखला को पेश किया जाता है, इन परिसंपत्तियों द्वारा प्रस्तुत जोखिमों की पहचान करने और पता लगाने में मदद करने के लिए नियमित भेद्यता आकलन करना बुद्धिमानी है।

5) **सख्त नियम:** यह सिर्फ आपराधिक हमला नहीं है, जिसके कारण व्यवसायों को पहले से कहीं अधिक साइबर सुरक्षा में निवेश करने की आवश्यकता है। जी.डी.पी.आर (जनरल डेटा प्रोटेक्शन रेगुलेशन) जैसे विनियमों की शुरूआत का मतलब है कि संगठनों को सुरक्षा को पहले से अधिक गंभीरता से लेने या भारी जुर्माना लगाने की आवश्यकता है।

जी.डी.पी.आर (GDPR) को यूरोपीय संघ द्वारा संगठनों को उनके द्वारा धारण किए गए व्यक्तिगत डेटा की बेहतर देखभाल करने के लिए मजबूर करने के लिए लागू किया गया है। जी.डी.पी.आर की आवश्यकताओं के बीच व्यक्तिगत डेटा की सुरक्षा, नियमित रूप से समीक्षा नियंत्रण, जांच और रिपोर्ट उल्लंघनों का पता लगाने के लिए उपयुक्त तकनीकी और संगठनात्मक उपायों को लागू करने के लिए संगठनों की आवश्यकता है।

10.6.1 साइबर धमकी

साइबर सुरक्षा विशेषज्ञ के लिए, साइबर खतरे को ऑक्सफोर्ड डिक्शनरी की परिभाषा में "कंप्यूटर नेटवर्क या सिस्टम को नुकसान या बाधित करने के लिए एक दुर्भावनापूर्ण प्रयास की संभावना" के रूप में दिया गया है। फ़ाइलों तक पहुँचने और घुसपैठ या डेटा चोरी करने के प्रयास को शामिल किए बिना यह परिभाषा अधूरी है। इस परिभाषा में, खतरे को एक संभावना के रूप में परिभाषित किया गया है। हालांकि, साइबर सुरक्षा समुदाय में, खतरे को कर्ता या विरोधी के साथ एक प्रणाली तक पहुंच प्राप्त करने के प्रयास के साथ अधिक बारीकी से पहचाना जाता है। या जो खतरा हो रहा है, चोरी होने या टैक्टिक्स, टेक्नीक और प्रोसीजर (टी.टी.पी) के इस्तेमाल से होने वाले खतरे की पहचान की जा सकती है।

सिर्फ यह समझने के लिए कि तकनीक साइबर अपराध या खतरे के प्रति कैसे संवेदनशील हो जाती है, यह सबसे पहले खतरों की प्रकृति को समझने में मदद करता है और कैसे वे तकनीकी प्रणालियों का शोषण करते हैं। आप पहले पूछ सकते हैं कि प्रौद्योगिकी बिल्कुल कमजोर क्यों है, और इसका उत्तर सरल है जो विश्वास है। अपनी स्थापना से, इंटरनेट, द्वारा और बड़े पैमाने पर ड्राइव करने वाले प्रोटोकॉल भविष्य के लिए डिज़ाइन नहीं किए गए थे जिनमें शोषण शामिल था, इसके जन्म के समय बहुत कम उम्मीद थी कि हमें एक दिन हमलों के खिलाफ काम करना पड़ सकता है जैसे कि (डी.डी.एस.एस)), या आप एक जो वेब कैमरा खरीदते हैं, उसे हैक होने से बचाने के लिए आपको सुरक्षा प्रोटोकॉल की आवश्यकता हो सकती है अन्यथा वो आपकी जासूसी करने के लिए इस्तेमाल किया जा सकता है। आज बहुत अधिक जागरूकता है, लेकिन फिर भी आप अभी भी उन उपकरणों को खरीद सकते हैं जो इंटरनेट से

कनेक्ट होते हैं जिनके पास खराब सुरक्षा उपाय हैं या बिल्ट-इन में कोई सुरक्षा नहीं है, क्योंकि हाल ही में जब तक यह डिज़ाइन गुंजाइश का हिस्सा नहीं था। कई मामलों में, इस विचार का उपयोग किया जा सकता है कि एक उपकरण का उपयोग नापाक उद्देश्यों के लिए किया जा सकता है, यहां तक कि विचार नहीं किया जाता है। और नतीजा यह है कि आज साइबर अपराध आपके स्मार्ट फोन और वेब ब्राउज़र से आपके क्रेडिट कार्ड और यहां तक कि आपकी कार में इलेक्ट्रॉनिक सिस्टम के माध्यम से सुरक्षा-केंद्रित डिज़ाइन की कमी का लाभ उठाता है। साइबर खतरों / साइबर क्राइम की प्रकृति वेबसाइटों पर सेवा हमलों के खंडन से लेकर चोरी, ब्लैकमेल, जबरन वसूली, हेरफेर और विनाश तक के विभिन्न रूपों में आती है। उपकरण कई और विविध हैं, और इसमें मैलवेयर, फिरौती, स्पाईवेयर, सोशल इंजीनियरिंग और यहां तक कि भौतिक उपकरणों में परिवर्तन शामिल हो सकते हैं (उदाहरण के लिए, एटीएम स्किमर्स)। यह कोई आश्चर्य की बात नहीं है कि संभावित हमलों का व्यापक दायरा बड़ा है, एक समस्या जिसे हमले की सतह के रूप में जाना जाता है जो हार्डवेयर और सॉफ्टवेयर द्वारा प्रस्तुत भेद्यता का आकार है।

10.6.2 साइबर खतरों के प्रकार

हमारी आधुनिक तकनीक से प्रेरित युग में, हमारी निजी जानकारी को निजी रखना अधिक कठिन होता जा रहा है। सच्चाई यह है कि, उच्च श्रेणी का विवरण सार्वजनिक डेटाबेस के लिए अधिक उपलब्ध हो रहा है, क्योंकि हम पहले से कहीं अधिक परस्पर जुड़े हुए हैं। हमारा डेटा लगभग किसी के लिए इस इंटर-कनेक्टिविटी के कारण बदलाव के लिए उपलब्ध है। यह एक नकारात्मक कलंक बनाता है कि तकनीक का उपयोग खतरनाक है क्योंकि व्यावहारिक रूप से कोई भी एक मूल्य के बदले एक निजी जानकारी का उपयोग कर सकता है। प्रौद्योगिकी हमारे दैनिक जीवन को आसान बनाने का वादा करती है; हालाँकि, प्रौद्योगिकी के उपयोग के खतरे हैं। प्रौद्योगिकी का उपयोग करने का एक मुख्य खतरा साइबर अपराधों का खतरा है।

आम इंटरनेट उपयोगकर्ता साइबर अपराधों से अनजान हो सकते हैं, और नियमित आधार पर साइबर हमलों के शिकार हो सकते हैं। कई निर्दोष व्यक्ति दुनिया भर में साइबर अपराधों के शिकार होते हैं, खासकर जब से तकनीक तीव्र गति से विकसित हो रही है। साइबर क्राइम ऐसे अपराध हैं जो कंप्यूटर और नेटवर्क का उपयोग करके किसी अन्य व्यक्ति को नुकसान पहुंचाते हैं। गोपनीयता और उससे संबंधित मुद्दों से साइबर अपराध हो सकते हैं। जब गैरकानूनी तरीके से व्यक्तियों द्वारा निजी और गोपनीय जानकारी खो जाती है या बाधित हो जाती है, तो यह हाई प्रोफाइल अपराधों जैसे हैकिंग, साइबर आतंकवाद, जासूसी, वित्तीय चोरी, कॉपीराइट का उल्लंघन, स्पैमिंग, साइबर युद्ध और कई अन्य अपराधों को जन्म देता है जो सीमाओं के पार होते हैं। एक गैरकानूनी उपयोगकर्ता द्वारा जानकारी का उल्लंघन करने पर साइबर अपराध किसी के भी साथ हो सकता है। कंप्यूटर सुरक्षा खतरे लगातार अविवेकी हैं। परिवर्तन और हेरफेर के कारण, ये धमकियां लगातार कष्टप्रद, चोरी और नुकसान के नए तरीके खोजने के लिए विकसित होती हैं। हमें जटिल और बढ़ते कंप्यूटर सुरक्षा खतरों से बचाव के लिए सूचना और संसाधनों से लैस करना होना और ऑनलाइन सुरक्षित रहना होगा। नीचे उल्लिखित ऑनलाइन साइबर सुरक्षा खतरों के कुछ उदाहरण हैं।

1) **कंप्यूटर वायरस:** कंप्यूटर वायरस एक प्रोग्राम है जो उपयोगकर्ता की अनुमति या ज्ञान के बिना, कंप्यूटर को संचालित करने के तरीके को बदलने के लिए लिखा जाता है। एक

वायरस खुद को दोहराता है और निष्पादित करता है, आमतौर पर इस प्रक्रिया में कंप्यूटर को नुकसान पहुंचाता है। यह सबसे प्रसिद्ध कंप्यूटर सुरक्षा खतरा है। सहकर्मी से सहकर्मी फ़ाइल साझाकरण साइटों से मुक्त सॉफ़्टवेयर डाउनलोड का सावधानीपूर्वक मूल्यांकन, और अज्ञात प्रेषकों के ईमेल वायरस से बचने के लिए महत्वपूर्ण हैं। अधिकांश वेब ब्राउज़र में आज सुरक्षा सेटिंग्स हैं जिन्हें ऑनलाइन खतरों के खिलाफ इष्टतम रक्षा के लिए रैंप किया जा सकता है। लेकिन, वायरस से दूर रहने वाला सबसे प्रभावी तरीका एक प्रतिष्ठित प्रदाता से एंटीवायरस सॉफ़्टवेयर है।

2) **स्पाइवेयर खतरे:** एक गंभीर कंप्यूटर सुरक्षा खतरा, स्पायवेयर एक प्रोग्राम है जो आपकी ऑनलाइन गतिविधियों पर लाभ के लिए नज़र रखता है वो भी सहमति के बिना या व्यक्तिगत जानकारी कैप्चर करने के लिए प्रोग्राम इंस्टॉल करता है। जबकि कई उपयोगकर्ता इसे सुनना नहीं चाहेंगे, नियम और शर्तों को पढ़ना आपकी गतिविधि को ऑनलाइन ट्रैक करने की समझ बनाने का एक अच्छा तरीका है। और निश्चित रूप से, यदि कोई कंपनी नहीं पहचानती है तो यह एक ऐसे सौदे के लिए विज्ञापन है जो सच होने के लिए बहुत अच्छा लगता है, सुनिश्चित करें कि हमारे पास एक इंटरनेट सुरक्षा समाधान है और सावधानी के साथ क्लिक करें।

3) **हैकर्स और प्रीडेटर्स:** हैकर्स और प्रीडेटर्स प्रोग्रामर होते हैं, जो साइबर आतंकवाद के रूप में जानकारी को चुराने, बदलने या नष्ट करने के लिए कंप्यूटर सिस्टम में सेंध लगाकर दूसरों को अपने लाभ के लिए शिकार करते हैं। ये ऑनलाइन शिकारी क्रेडिट कार्ड की जानकारी से समझौता कर सकते हैं, आपको अपने डेटा से बाहर कर सकते हैं और आपकी पहचान चुरा सकते हैं। जैसा कि हमने अनुमान लगाया है, पहचान की सुरक्षा के साथ ऑनलाइन सुरक्षा उपकरण साइबर ब्रांड के इस ब्रांड से खुद को बचाने के सबसे प्रभावी तरीकों में से एक हैं।

4) **फ़िशिंग:** फ़िशिंग अटैक साइबर अपराधियों के लिए कुछ सबसे सफल तरीके हैं जो डेटा ब्रीच को खींचते हैं। एक भरोसेमंद व्यक्ति या व्यवसाय के रूप में संदेश भेजना, धोखाधड़ी वाले ईमेल या त्वरित संदेशों के माध्यम से संवेदनशील वित्तीय या व्यक्तिगत जानकारी चोरी करने का प्रयास करता है। पहचान की सुरक्षा के साथ एंटीवायरस समाधानों का उपयोग दूसरे के अंशों में फ़िशिंग के खतरों को पहचानने के लिए किया जा सकता है।

10.7 साइबर अपराध और कानून

साइबर क्राइम की एक आम तौर पर स्वीकृत परिभाषा "एक कंप्यूटर और इंटरनेट का उपयोग करके किया गया अपराध है जो किसी व्यक्ति की पहचान को चोरी करने के लिए या वर्जित वस्तुओं को बेचने या पीड़ितों से जानकारी छिपाने या हेषपूर्ण कार्यक्रमों के साथ संचालन को बाधित करता है"। हालांकि साइबर अपराध की कई अलग-अलग परिभाषाएं हैं, लेकिन सभी में कुछ महत्वपूर्ण अवधारणाएं हैं। ये प्रमुख अवधारणाएं आपराधिक गतिविधि और कंप्यूटर का उपयोग या दुरुपयोग हैं। मन में इन अवधारणाओं के साथ साइबर क्राइम को एक आपराधिक कृत्य करने के लिए कंप्यूटर का उपयोग करने के रूप में आसानी से परिभाषित किया जा सकता है।

साइबर क्राइम कानून प्रवर्तन ब्यूरो के लिए एक बहुत बड़ा काम है क्योंकि वे बेहद तकनीकी अपराध हैं। कानून प्रवर्तन संगठनों के पास कंप्यूटर अपराधों और कंप्यूटर फोरेंसिक में प्रशिक्षित व्यक्ति होने चाहिए जो कंप्यूटर अपराधों या साइबर क्राइम की सही जांच कर सकें। इसके अतिरिक्त, राज्यों को कानून का आधुनिकीकरण और निर्माण करना चाहिए, जो साइबर अपराधों को रोकता है और उन अपराधों के लिए उपयुक्त दंड की रूपरेखा तैयार करता है। एडवांस तकनीकों के आने से साइबर क्राइम की संभावना अधिक हो जाएगी। यह महत्वपूर्ण है कि नागरिकों, कानून अधिकारियों, और न्याय प्रणाली के अन्य सहयोगियों को साइबर क्राइम के बारे में अच्छी तरह से सूचित किया जाता है ताकि उनके कारण होने वाले खतरे को कम किया जा सके।

साइबर अपराधों के खतरे को समझना एक बहुत ही महत्वपूर्ण मुद्दा है क्योंकि प्रौद्योगिकी हमारे समाज पर महत्वपूर्ण प्रभाव डालती है। साइबर अपराध हर दिन बढ़ रहा है क्योंकि कंप्यूटरों में तकनीकी प्रगति किसी को भी शारीरिक रूप से नुकसान पहुंचाने के बगैर चोरी करना बहुत आसान बना देती है, क्योंकि साइबर अपराध कैसे होते हैं और आम लोग कैसे खुद की रक्षा कर सकते हैं, इसके बारे में आम जनता को कोई जानकारी नहीं होने के कारण साइबर अपराध होते हैं। । कई तरीके या साधन हैं, जहां साइबर अपराध हो सकते हैं। यहां कुछ कारण और तरीके दिए गए हैं कि दैनिक आधार पर साइबर अपराध कैसे घटित होते हैं।

1) **हैकिंग:** दूसरे शब्दों में, किसी भी कंप्यूटर सिस्टम या नेटवर्क पर अनधिकृत पहुंच के रूप में जाना जा सकता है। यह तब हो सकती है जब कंप्यूटर हार्डवेयर और सॉफ़्टवेयर में कोई कमज़ोरी हो, जिसे घुसपैठ किया जा सकता है यदि ऐसे हार्डवेयर या सॉफ़्टवेयर में पैचिंग, सुरक्षा नियंत्रण, कॉन्फ़िगरेशन या खराब पासवर्ड विकल्प की कमी है।

2) **इलेक्ट्रॉनिक रूप में निहित जानकारी की चोरी:** इस प्रकार की विधि तब होती है जब कंप्यूटर सिस्टम में संग्रहीत जानकारी को घुसपैठ किया जाता है और हार्ड डिस्क के माध्यम से बदल दिया जाता है या भौतिक रूप से जब्त किया जाता है; हटाने योग्य भंडारण मीडिया या एक और आभासी माध्यम।

3) **ई मेल बॉम्बिंग:** यह इंटरनेट के दुरुपयोग का एक और रूप है जहां व्यक्ति मेल को ओवरफ्लो करने के प्रयास में पीड़ित को मेल के नंबर या एक पते को निर्देशित करते हैं, जो कि एक व्यक्ति या कंपनी या यहां तक कि मेल सर्वर हो सकता है जो अंततः दुर्घटनाग्रस्त हो जाता है। । ईमेल बम को नष्ट करने की दो विधियाँ हैं जिनमें सामूहिक मेलिंग और सूची लिंकिंग शामिल हैं।

4) **डेटा डीडलिंग:** यह कंप्यूटर सिस्टम में घुसपैठ के पहले या दौरान डेटा का बदलना है। इस तरह की घटना में कंप्यूटर को संसाधित करने से पहले कच्चे डेटा को शामिल करना और प्रसंस्करण पूरा होने के बाद इसे वापस बदलना शामिल है।

5) **सलामी हमले:** इस तरह का अपराध आम तौर पर कई छोटे डेटा सुरक्षा हमलों से मिलकर होता है, जिसके परिणामस्वरूप एक बड़ा हमला होता है। यह विधि आम तौर पर वित्तीय संस्थानों में या वित्तीय अपराधों को करने के उद्देश्य से होती है। इस प्रकार के अपराध की एक महत्वपूर्ण विशेषता यह है कि परिवर्तन इतना छोटा है कि यह सामान्य रूप से किसी का ध्यान नहीं जाएगा। साइबर अपराध का यह रूप उन बैंकों में बहुत

आम है जहां कर्मचारी छोटी राशि की चोरी कर सकते हैं और उसका पता लगाना बहुत मुश्किल है जैसे "ज़िग्लर मामला" जिसमें एक लॉजिक बम बैंक के सिस्टम में घुस गया, जिसने हर खाते से 10 सेंट घटा दिए और और दूसरे यह एक विशेष खाते में जमा कर दिया जिसे "पेनी शेविंग" के रूप में जाना जाता है।

6) **सेवा हमले से इनकार:** यह मूल रूप से एक कंप्यूटर सिस्टम अपने अधिकृत एंड यूज़र के लिए अनुपलब्ध हो जाता है। हमले का यह रूप आम तौर पर कंप्यूटर नेटवर्क से संबंधित होता है, जहां पीड़ित का कंप्यूटर अधिक अनुरोधों कारण निष्क्रिय हो जाता है जिससे पी.सी दुर्घटनाग्रस्त हो सकता है जैसे, अमेज़न, याहू। एक अन्य घटना व्हिसल ब्लोअर साइट wikileaks.org में हुई थी जो डी डी ओ एस हमला था ।

7) **वायरस / वार्म के हमले:** वायरस ऐसे प्रोग्राम हैं जो खुद को किसी भी फाइल में एम्बेड कर सकते हैं। कार्यक्रम तब खुद को कॉपी करता है और एक नेटवर्क पर अन्य कंप्यूटरों में फैलता है जो वे उन पर कुछ भी प्रभावित करते हैं, या तो इसे बदलकर या हटाकर । हालांकि, वार्म वायरस की तरह नहीं होते हैं, उन्हें मेजबान को खुद को संलग्न करने की आवश्यकता नहीं होती है, लेकिन उनमें से उपयोगी प्रतियां बनाते हैं और लगातार ऐसा करते हैं जब तक वे कंप्यूटर की मेमोरी पर सभी उपलब्ध स्थान का उपभोग नहीं करते हैं। जैसे बग वायरस, जो दुनिया भर के कम से कम 5% कंप्यूटरों को प्रभावित करता है।

8) **लॉजिक बम:** वे मूल रूप से निर्देशों का एक समूह हैं जो गुप्त रूप से एक कार्यक्रम में निष्पादित कर सकता है जहां यदि कोई विशेष स्थिति सच है तो अंतिम परिणाम आमतौर पर हानिकारक प्रभावों के साथ समाप्त होता है। इससे पता चलता है कि इन प्रोग्रामों का उत्पादन प्रयोग केवल तभी किया जाता है जब कोई विशिष्ट घटना (ट्रिगर इवेंट के रूप में जानी जाती है) होती है। जैसे चेरनोबिल वायरस।

9) **ट्रोजन हमले:** यह शब्द बताता है कि जहां एक प्रोग्राम या प्रोग्राम्स खुद को मूल्यवान उपकरण के रूप में मास्क करते हैं, लेकिन कंप्यूटर के लिए हानिकारक कार्यों को पूरा करते हैं। ये प्रोग्राम गैरकानूनी हैं जो एक अधिकृत कार्यक्रम के रूप में भूमिका मानकर दूसरे के सिस्टम पर नियंत्रण प्राप्त करते हैं। ट्रोजन का सबसे आम रूप ई-मेल के माध्यम से है। जैसे महिला फिल्म निर्देशक यू.एस ।

10) **इंटरनेट समय की चोरी:** यह फॉर्म गबन का प्रकार है जहाँ धोखाधड़ी करने वाले पीड़ित के इंटरनेट सर्फिंग घंटों का उपयोग अपने स्वयं के रूप में करते हैं जो लॉगिन आई.डी और पासवर्ड तक पहुंच प्राप्त करके पूरा हो सकता है, इसका एक उदाहरण कर्नल बाजवा का मामला है जिसमे इंटरनेट समय एक अनधिकृत व्यक्ति द्वारा इस्तेमाल किया गया।

11) **वेब जैकिंग:** इसमें हैकर पहुंच प्राप्त करता है और किसी अन्य व्यक्ति की वेब साइट को नियंत्रित कर सकता है, जहां वह साइट पर जानकारी को नष्ट या बदल सकता है जैसा कि उनके लिए उपयुक्त हैं। साइबर क्राइम का यह तरीका राजनीतिक एजेंडा को संतुष्ट करने या विशुद्ध मौद्रिक साधनों के लिए किया जाता है। ऐसी विधि का एक उदाहरण एम. आई. टी. (सूचना प्रौद्योगिकी मंत्रालय) पाकिस्तानी हैकर्स द्वारा हैक किया गया

था, जबकि एक और 'गोल्ड फिश' केस था जिसमे, साइट को हैक कर लिया गया था और गोल्ड फिश से संबंधित जानकारी में बदलाव किया गया था और $ 1 मिलियन की राशि की मांग की गई थी।

साइबर आतंकवाद को ऐसी गतिविधियों के रूप में परिभाषित किया जा सकता है, जहां वर्चुअल मशीन के माध्यम से विघटनकारी गतिविधियों, या इसके जोखिम का जानबूझकर उपयोग, सार्वजनिक, राजनीतिक, आध्यात्मिक, कट्टरपंथी या इस तरह के उद्देश्यों की निरंतरता में किसी भी व्यक्ति को धमकी देने के उद्देश्य से किया जाता है। चोरी के अपराधों में निम्नलिखित शामिल हैं:

1) **क्रेडिट / डेबिट कार्ड धोखाधड़ी:** यह पैसे / सामान को गलत तरीके से प्राप्त करने के लिए क्रेडिट / डेबिट कार्ड का गैरकानूनी उपयोग है। क्रेडिट / डेबिट कार्ड नंबर को असुरक्षित वेब साइटों से चुराया जा सकता है, या एक पहचान चोरी योजना में प्राप्त किया जा सकता है।

2) **पहचान की चोरी:** पहचान की चोरी तब होती है जब कोई व्यक्ति चोरी या धोखाधड़ी करने के लिए जानकारी के बिना किसी अन्य व्यक्ति की व्यक्तिगत जानकारी को जब्त कर लेता है। आमतौर पर, पीड़ित को यह विश्वास करने के लिए प्रेरित किया जाता है कि वे एक वास्तविक व्यवसाय के लिए संवेदनशील निजी डेटा का खुलासा कर रहे हैं, जो कभी-कभी बिलिंग या सदस्यता जानकारी आदि के आधुनिकीकरण के लिए ई-मेल की प्रतिक्रिया के रूप में होता है।

3) **वस्तुओं और सेवाओं की गैर-वितरण:** ये वे वस्तुएं या सेवाएं जिन्हें व्यक्तियों द्वारा ऑनलाइन ख़रीदा गया था, जो कभी भेजे नहीं गए।

4) **फोनी एस्क्रो सर्विसेज:** यह वह जगह है जहां नीलामी में भाग लेने वाले धोखेबाज को राजी करते है, जहां वह पैसे और माल की अदला-बदली में मदद करने के लिए एक थर्ड पार्टी एस्क्रो सर्विस के इस्तेमाल की सिफारिश करेगा। पीड़ित को जानकारी नहीं होती की एस्क्रो सेवा द्वारा धोखा दिया गया है, इसमें पीड़ित व्यक्ति एस्क्रो में भुगतान या उत्पाद भेजता है और बदले में कुछ भी प्राप्त नहीं करता है।

5) **पोंजी / पिरामिड विधि:** इसमें निवेशकों को अनियमित या असामान्य रूप से उच्च लाभ के वादे द्वारा इस झूठी व्यवस्था में पूंजी लगाने का लालच दिया जाता है, लेकिन वास्तव में तथाकथित "निवेश फर्म" द्वारा कोई भी धन नहीं बनाया जाता है।

कई देशों द्वारा की जा रही प्रगति के बावजूद साइबर अपराध हमेशा एक चुनौती होगी। साइबर अपराध से निपटने के लिए अधिकांश देशों के अपने कानून हैं, लेकिन कुछ के पास कोई नया कानून नहीं है, लेकिन इन अपराधों पर मुकदमा चलाने के लिए पूरी तरह से मानक स्थलीय कानून पर निर्भर करता है।

साइबरस्पेस, साइबर कानून से संबंधित इन बिल्कुल जटिल और नए उभरते कानूनी मुद्दों के जवाब में इंटरनेट का कानून अस्तित्व में आया। साइबरस्पेस की वृद्धि के परिणामस्वरूप साइबर कानूनों यानी इंटरनेट और वर्ल्ड वाइड वेब के कानूनों की एक नई और अत्यधिक विशिष्ट शाखा का विकास हुआ है। साइबर कानून एक सामान्य शब्द है जो इंटरनेट और वर्ल्ड

वाइड वेब के सभी कानूनी और नियामक पहलुओं को संदर्भित करता है। किसी भी कानूनी पहलुओं से संबंधित साइबरस्पेस के विषय में से संबंधित के साथ या संबंधित कुछ भी साइबर कानून के दायरे में आता है।

हम कह सकते हैं कि साइबर क्राइम गैरकानूनी काम है जिसमें कंप्यूटर या तो एक उपकरण या एक लक्ष्य या दोनों है, साइबर क्राइम आपराधिक गतिविधियों में शामिल हो सकते हैं जो प्रकृति में पारंपरिक हैं, जैसे कि चोरी, धोखाधड़ी, जालसाजी, मानहानि और शरारत, जो सभी भारतीय दंड संहिता में शामिल है। कंप्यूटरों के दुरुपयोग ने नए युग के अपराधों को जन्म दिया है जिसे सूचना प्रौद्योगिकी अधिनियम, 2008 द्वारा संबोधित किया गया है। साइबर अपराधों को दो तरीकों से वर्गीकृत किया गया है:

- **कंप्यूटर एक लक्ष्य के रूप में:** - अन्य कंप्यूटरों पर हमला करने के लिए एक कंप्यूटर का उपयोग करना। जैसे हैकिंग, वायरस / वर्म अटैक, डॉस अटैक आदि।
- **कंप्यूटर एक हथियार के रूप में:** - वास्तविक दुनिया के अपराधों के लिए कंप्यूटर का उपयोग करना। जैसे साइबर आतंकवाद, आई.पी.आर उल्लंघन, क्रेडिट कार्ड धोखाधड़ी, ई.एफ.टी धोखाधड़ी, पोर्नोग्राफी आदि।

साइबर अपराध को साइबर कानून या इंटरनेट कानून द्वारा नियंत्रित किया जाता है, भारत में इसे सूचना प्रौद्योगिकी अधिनियम, 2008 द्वारा संबोधित किया जाता है।

तालिका 10.2: भारत में महत्वपूर्ण साइबर कानून प्रावधानों का स्नैपशॉट

अपराध	आई.टी अधिनियम के अंतर्गत धारा
कंप्यूटर स्रोत दस्तावेजों के साथ छेड़छाड़	धारा 65 (आई.टी अधिनियम)
कंप्यूटर सिस्टम, डेटा परिवर्तन के साथ हैकिंग	धारा 66 (आई.टी अधिनियम)
अश्लील जानकारी प्रकाशित करना	धारा 67 (आई.टी अधिनियम)
संरक्षित प्रणाली तक गैर-अधिकृत पहुंच	धारा 70 (आई.टी अधिनियम)
गोपनीयता और निजता का उल्लंघन	धारा 72 (आई.टी अधिनियम)
झूठे डिजिटल हस्ताक्षर प्रमाण पत्र प्रकाशित करना	धारा 73 (आई.टी अधिनियम)
ईमेल द्वारा धमकी भरे संदेश भेजना	धारा 503 (आई पी सी)
ईमेल द्वारा मानहानि संदेश भेजना	धारा 499 (आई पी सी)
इलेक्ट्रॉनिक रिकॉर्ड की जालसाजी	धारा 463 (आई पी सी)
फर्जी वेबसाइट, साइबर धोखाधड़ी	धारा 420 (आई पी सी)
ईमेल स्पूफिंग	धारा 463 (आई पी सी)
वेब-जैकिंग	धारा 383 (आई पी सी)
ई-मेल का दुरुपयोग	धारा 500 (आई पी सी)
ड्रग्स की ऑनलाइन बिक्री	एनडीपीएस अधिनियम
शस्त्रों की ऑनलाइन बिक्री	शस्त्र अधिनियम

जब तक अलग-अलग कानूनी कार्रवाई नहीं की जा सकती, जब तक कि व्यक्तिगत देशों और उत्पीड़न अपराधियों के वैश्विक तरीके, आत्म-सुरक्षा ही बचाव है। व्यक्तियों और व्यवसायों को यह सुनिश्चित करने की आवश्यकता है कि वे साइबर अपराध के अगले शिकार बनने से बचने

के लिए क्या करना है, उसके बारे में जागरूक हों। यह बुनियादी जागरूकता उनके खिलाफ संभावित साइबर अपराधों को रोकने में मदद कर सकती है। एकमात्र संभव कदम लोगों को उनके अधिकारों और कर्तव्यों के बारे में जागरूक करना और अधिक दंडनीय कानून बनाना है जो उन्हें जांचने के लिए अधिक कठोर हों।

10.8 सुरक्षा बाधाएं

यद्यपि खोए हुए डेटा या फिरौती के भुगतान के मामले में सुरक्षा घटनाओं से जुड़ी महत्वपूर्ण लागतें हैं, कार्यकारी नेतृत्व को अन्य व्यावसायिक प्रभावों जैसे ब्रांड के क्षरण, ग्राहक की साख की हानि, शेयरधारक की निराशा और कमाई की अस्थिरता के लिए भी तैयार रहना होगा, जो सभी को प्रभावित कर सकते हैं जो प्रारंभिक सुरक्षा घटना के बाद महीने और यहां तक कि वर्षों तक उसका प्रभाव पड़ सकता है। हर कोई जानता है कि उन्हें अपने नेटवर्क और सिस्टम को सुरक्षित करने की आवश्यकता है, लेकिन जिन उद्यमों में आईटी संसाधनों की कमी है, बजट घटते जा रहे हैं और प्रबंधन करने के लिए जोखिम की भारी मात्रा; आजकल सुरक्षा संभालना एक असंभव सा काम बन गया है। नतीजतन, अधिक से अधिक व्यवसाय मदद के लिए प्रबंधित सुरक्षा सेवा प्रदाताओं (MSSP) की ओर देख रहे हैं। तीन सामान्य सुरक्षा चुनौतियां जिनका कंपनियां सामना कर रही हैं और एम एस एस पी उन्हें कैसे हल करने में मदद कर सकते हैं का विवरण निम्नवत है :-

1) **विशिष्ट प्रतिभा की कमी:** योग्य आई टी सुरक्षा कर्मचारियों की कमी है, जिससे प्रबंधन को योग्य कर्मियों को आकर्षित करने और भर्ती करने में कठिनाई होती है। वेतन आवश्यकताओं में वृद्धि से स्थिति और जटिल हो गई है। नतीजतन, कई कंपनियां सुरक्षा प्रबंधन की कुछ बुनियादी बातों को केवल इसलिए छोड़ देती हैं क्योंकि उनके पास इन प्रथाओं को लागू करने के लिए आवश्यक समय या स्टाफ नहीं होता है, जिससे वे मुख्य हैकिंग लक्ष्य बनते हैं। एक एम एस एस पी (प्रबंधित सुरक्षा सेवा प्रदाता) कई प्रकार की क्षमताओं में काम कर सकता है और एक कंपनी के पास जो भी सुरक्षा कमियां है उसे पूरी सकता है। इसमें न केवल नेटवर्क और उपकरणों के लिए एक सुरक्षा और अनुपालन रणनीति तैयार करना शामिल है, बल्कि दैनिक सुरक्षा प्रबंधन भी शामिल है। एम एस एस पी के साथ साझेदारी करके, न केवल आपके पास एक समर्पित और विशिष्ट कार्यबल उपलब्ध होता है, बल्कि आप विशेषज्ञों की एक टीम से भी लाभान्वित होते हैं जो गतिशील सुरक्षा परिदृश्य और नवीनतम खतरों को समझते हैं। जिस तरह आप कर कानून के अपने ज्ञान के कारण अपने टैक्स फाइलिंग को प्रबंधित करने के लिए एक CPA (प्रमाणित सार्वजनिक लेखाकार) पर निर्भर करते हैं, एक एम एस एस पी सुरक्षा विशेषज्ञता का एक स्तर प्रदान कर सकता है जो स्वयं प्राप्त करना कठिन है।

2) **जोखिम को प्राथमिकता देना:** सही सुरक्षा जैसी कोई चीज नहीं है, बल्कि, यह उचित रूप से जोखिम को प्रबंधित करने और क्या करना है, और शायद इससे भी महत्वपूर्ण बात यह है कि क्या नहीं करना है, के बारे में जागरूक निर्णय लेने की बात है। उदाहरण के लिए, जब आप सुरक्षा के कई स्तरों के साथ एक डिजिटल सुरक्षा के निर्माण के लिए समर्पित हो सकते हैं, तो सरासर मात्रा और विभिन्न प्रकार के खतरे

आपकी वर्तमान कमजोरियों का आकलन करने और कार्रवाई के एक उचित पाठ्यक्रम की योजना बनाना मुश्किल बनाते हैं। एक एम एस एस पी आपकी सुरक्षा कमजोरियों और अनुपालन आवश्यकताओं की पहचान कर सकता है और आपको एक योजना लागू करने में मदद कर सकता है जो आपके संगठन और व्यावसायिक स्थिति के लिए अद्वितीय है। वहां से, आपके पास दो विकल्प हैं। आपकी आई टी टीम सुरक्षा योजना को निष्पादित कर सकती है या आप अपनी दिन-प्रतिदिन की सुरक्षा जरूरतों को प्रबंधित करने के लिए एम एस एस पी का लाभ उठा सकते हैं। उदाहरण के लिए, सेंचुरी लिंक पर, हम अपने ग्राहकों को एक सुरक्षा योजना बनाने में कुशलता से जोखिम का प्रबंधन करने में मदद करते हैं, जिसमें खतरे की खुफिया जानकारी, पहचान और सुरक्षा चिंताओं की असंख्य प्रतिक्रिया शामिल है।

4) **सुरक्षा खर्चों का प्रबंधन:** जबकि खरीदार सुरक्षा-संबंधित हार्डवेयर और सॉफ़्टवेयर पर पहले से कहीं अधिक खर्च कर रहे हैं, कई कंपनियां अभी भी उजागर हैं और अपर्याप्त रूप से सुरक्षा घटना के लिए तैयार हैं। इसके साथ ही, खरीदार भी खर्च कम करने और अधिक अनुमानित परिचालन खर्च प्रदान करने के लिए प्रबंधन से दबाव में हैं। लेकिन वहां अच्छी ख़बर है कि आवश्यक रूप से प्रभावी निवारक उपाय निषेधात्मक नहीं हैं। एक एम एस एस पी आपको अपनी सुरक्षा अनुपालन पर सबसे अधिक प्रभाव डालने वाली प्राथमिकताओं पर अपने खर्च पर ध्यान केंद्रित करके सुरक्षा खर्च को कम करने में मदद कर सकता है। एक प्रबंधित सुरक्षा दृष्टिकोण के साथ, आप स्वामित्व की लागत को स्थानांतरित करते हैं, जिससे पूंजी निवेश की आवश्यकता कम हो जाती है। आप एक पूर्वानुमानित OpEx मॉडल प्राप्त करेंगे जो पूर्वानुमान और बजट के लिए आसान है, विशेष रूप से महत्वपूर्ण है जब आई टी बजट के समान रहने की उम्मीद है।

प्रबंधित सुरक्षा सेवाओं का लाभ उठाने वाले ग्राहक तेजी से बदलते खतरे के परिदृश्य के खिलाफ सक्रिय सुरक्षा रणनीति के लिए प्रतिक्रियात्मक रुख से आगे बढ़ने में सक्षम हैं। आज की वास्तविकता यह है कि आपको इस धारणा के साथ काम करने की आवश्यकता है कि आपका संगठन नष्ट हो जाएगा। हालाँकि, एक एम एस एस पी के साथ साझेदारी करके, आप एक खुफिया परिप्रेक्ष्य से "संख्या में ताकत" से लाभान्वित होते हैं और संभावना को बढ़ाते हैं कि आप संभावित हैकर्स से एक कदम आगे रह सकते हैं। इस आधुनिक युग में, साइबर अपराध का शिकार होने से बचना लगभग असंभव है, प्रौद्योगिकी में प्रगति के साथ किसी के लिए भी साइबर क्राइम करना आसान हो गया है। ।

इसके संदर्भ में, साइबर क्राइम का शिकार होने से बचने के कुछ तरीके हैं। अधिकांश इंटरनेट ब्राउज़र ईमेल सेवा, और इंटरनेट प्रदाता अनचाहे संदेशों को रोकने के लिए एक स्पैम-ब्लॉकिंग सुविधा प्रदान करते हैं, जैसे कि धोखाधड़ी वाले ईमेल और फ़िशिंग ईमेल, आपके इनबॉक्स में जाने से रोकता है। हालांकि, प्रत्येक उपयोगकर्ता को उन्हें चालू करना सुनिश्चित करना चाहिए और जो भी उन्हें बंद करना है उसे न करें। इसके अलावा, उपयोगकर्ताओं को अप-टू-डेट एंटीवायरस प्रोग्राम, फायरवॉल और स्पाईवेयर चेकर्स इनस्टॉल रखना चाहिए। उन्हें अद्यतित रखने के साथ, उपयोगकर्ताओं को यह सुनिश्चित करना होगा कि वे नियमित रूप से स्कैन चलाते हैं। वहाँ कई कंपनियां हैं जो मुफ्त सॉफ्टवेयर प्रदान करती हैं, लेकिन कुछ अन्य हैं जिन्हें आप खरीद सकते हैं, इसके साथ ही कई प्रमुख कंपनियों के प्रदाताओं द्वारा उत्पादित किया

जाता है; इसके अलावा, वे कंपनियां अपने सशुल्क या सब्सक्रिप्शन एंटीवायरस सॉफ़्टवेयर का मुफ्त संस्करण प्रदान करती हैं। जानकारी का एन्क्रिप्शन जो आप नहीं चाहते कि किसी के पास अनधिकृत पहुंच हो, कुछ साइबर अपराधों से बचने का एक अच्छा तरीका है; उदाहरण के लिए पासवर्ड और क्रेडिट कार्ड की जानकारी जैसी जानकारी। एन्क्रिप्शन सॉफ़्टवेयर आपके डेटा को एन्क्रिप्शन एल्गोरिदम के माध्यम से चलाता है जो इसे आपके कंप्यूटर में हैक करने की कोशिश करने वाले व्यक्ति के लिए अनजाने में बनाता है।

एक और अच्छा एहतियात है कि आप अपनी व्यक्तिगत जानकारी को विभाजित करें। अज्ञात वेबसाइटों से बचने की कोशिश करें, विशेष रूप से उन लोगों से जो आपका नाम, मेलिंग पता, बैंक खाता संख्या या सामाजिक सुरक्षा नंबर पूछते हैं। ऑनलाइन शॉपिंग करते समय सुनिश्चित करें कि वेबसाइट सुरक्षित है, उन यू आर एल की तलाश करें जो "https" से शुरू होते हैं और / या ट्रस्टी या वेरिग्निन सील होते हैं ।

चित्र 10.4: सुरक्षित वेबसाइट का ट्रस्टी और वेरिग्न सिंबल

यदि आपको साइट पर कहीं भी ये नहीं दिखते हैं, तो आप क्रेडिट कार्ड की जानकारी और अन्य व्यक्तिगत जानकारी साइट पर भेजने का जोखिम उठाते हैं जो शायद एक धोखाधड़ी है। साइबर क्राइम का शिकार होने से बचने का एक और तरीका है, आम धोखाधड़ी जैसे अतिसंवेदनशील पत्र, विदेशी बैंक खातों, विदेशी लॉटरी और फॉर्नी स्वीपस्टेक्स में बड़ी रकम रखने में आपकी मदद माँगने वाले पत्र के प्रति अतिसंवेदनशील होने से बचना। इन सभी उल्लिखित गतिविधियों में साइबर अपराधियों द्वारा आपकी व्यक्तिगत जानकारी और धन प्राप्त करने के लिए उपयोग की जाने वाली सभी विधियाँ हैं। अगर यह सच होने पर बहुत अच्छा लगता है, तो यह शायद है।

बच्चों को कंप्यूटर और इंटरनेट के उचित उपयोग के बारे में शिक्षित करें और घर और स्कूल में समान रूप से उनकी ऑनलाइन गतिविधियों की निगरानी करना सुनिश्चित करें। उन्हें केवल आपके घर के मध्य क्षेत्र में स्थित कंप्यूटर तक पहुंच होनी चाहिए और आपको नियमित रूप से सभी ब्राउज़र और ईमेल गतिविधि की जांच करनी चाहिए। एक बुद्धिमान बात माता-पिता के नियंत्रण सॉफ्टवेयर का उपयोग करना है जो उन साइटों के प्रकार को सीमित करता है जो

उपयोगकर्ता तक पहुंच सकता है। स्कूलों में, प्रतिबंधित वेबसाइट और अन्य उपयोगकर्ता प्रतिबंध होने चाहिए जो उपयोगकर्ता और संस्था को साइबर अपराध से बचाने में मदद करेंगे। इसी तरह, कंपनियों को शिक्षित होना चाहिए और वर्कप्लेस पीसी को नियंत्रित करने वाली नीतियों को लिखना चाहिए और कंपनी के खिलाफ साइबर अपराध के जोखिम को कम करने के लिए इसके नेटवर्क का उपयोग करना चाहिए। यह सुनिश्चित करने का एक निश्चित तरीका है कि साइबर अपराध के शिकार एक व्यक्ति को पूरी तरह से इंटरनेट से कंप्यूटर को डिस्कनेक्ट नहीं करना है। यदि कोई नेटवर्क नहीं है, तो किसी भी साइबर हमले के बारे में चिंता करने की ज़रूरत नहीं है। हालाँकि, यह विकल्प हमारे परस्पर समाज में सबसे व्यवहार्य नहीं है। सच्चाई यह है कि संभावित साइबर अपराधों से बचने के लिए आवश्यक सावधानी बरतना आपके ऊपर है।

बोध प्रश्न ख:

1) सलामी हमलों से आप क्या समझते हैं?

……

……

……

……

2) साइबर क्राइम क्या हैं? साइबर अपराध की विभिन्न श्रेणियों के बारे में बताएं।

……

……

……

……

……

……

3) भारत में महत्वपूर्ण साइबर कानून प्रावधानों का उदाहरण दें।

……

……

……

……

……

4) पहचान की चोरी क्या है?

……

.....

.....

.....

.....

10.9 सारांश

इस आधुनिक युग में, साइबर अपराध का शिकार होने से बचना लगभग असंभव है, प्रौद्योगिकी में सभी प्रगति के साथ किसी के लिए साइबर क्राइम करना आसान बन गया है। इसके आलोक में, साइबर क्राइम का शिकार बनने से बचने के कुछ तरीके हैं। अधिकांश इंटरनेट ब्राउज़र ईमेल सेवा, और इंटरनेट प्रदाता अनचाहे संदेशों को रोकने के लिए एक स्पैम-ब्लॉकिंग सुविधा प्रदान करते हैं, जैसे कि धोखाधड़ी वाले ईमेल और फ़िशिंग ईमेल, आपके इनबॉक्स में न पहुँचे । हालांकि, प्रत्येक उपयोगकर्ता को उन्हें चालू करना सुनिश्चित करना चाहिए और उन्हें बंद न करें। इसके अलावा, उपयोगकर्ताओं को अप-टू-डेट एंटीवायरस प्रोग्राम, फायरवॉल और स्पाईवेयर चेकर्स स्थापित और रखना चाहिए। उन्हें अद्यतित रखने के साथ, उपयोगकर्ताओं को यह सुनिश्चित करना होगा कि वे नियमित रूप से स्कैन चलाते हैं। कई कंपनियां हैं जो मुफ्त सॉफ्टवेयर प्रदान करती हैं, लेकिन कुछ अन्य हैं जिन्हें आप खरीद सकते हैं, इसके साथ ही कई प्रमुख कंपनियों के प्रदाताओं द्वारा उत्पादित किया जाता है; इसके अलावा, वे कंपनियां अपने सशुल्क या सब्सक्रिप्शन एंटीवायरस सॉफ़्टवेयर का मुफ्त संस्करण प्रदान करती हैं। जानकारी का एन्क्रिप्शन जो आप नहीं चाहते कि किसी के पास अनधिकृत पहुंच हो, कुछ साइबर अपराधों से बचने का एक अच्छा तरीका है; उदाहरण के लिए पासवर्ड और क्रेडिट कार्ड की जानकारी । एन्क्रिप्शन सॉफ्टवेयर एन्क्रिप्शन एल्गोरिदम के माध्यम से डेटा चलाता है जो इसे कंप्यूटर में हैक करने की कोशिश करने वाले किसी भी व्यक्ति के लिए अनजाने में बनाता है।

एक और अच्छा एहतियात है कि व्यक्तिगत जानकारी को विभाजित करने वाले अज्ञात वेबसाइटों से बचने की कोशिश करें, विशेष रूप से उन लोगों के लिए जो नाम, मेलिंग पता, बैंक खाता संख्या या सामाजिक सुरक्षा संख्या पूछते हैं। ऑनलाइन शॉपिंग करते समय सुनिश्चित करें कि वेबसाइट सुरक्षित है, उन URL की तलाश करें जो "https" से शुरू होते हैं और / या ट्रस्टी या वेरिग्निन सील होते हैं। यदि कोई साइट पर कहीं भी इनको नहीं देखता है, तो क्रेडिट कार्ड की जानकारी और अन्य व्यक्तिगत जानकारी साइट पर जमा करने का जोखिम होता है जो शायद एक धोखाधड़ी है।

साइबर क्राइम का शिकार होने से बचने का एक और तरीका है कि आम धोखाधड़ी के लिए अतिसंवेदनशील होने से बचा जाए, जैसे इनहेरिटेंस लेटर, लेटर जिसमें विदेशी बैंक खातों, विदेशी लॉटरी और फॉनी स्वीपस्टेक में बड़ी रकम रखने में मदद मांगी जाती है। इन उल्लिखित गतिविधियों में साइबर अपराधियों द्वारा व्यक्तिगत जानकारी और धन प्राप्त करने के लिए उपयोग की जाने वाली सभी विधियाँ हैं। अगर यह सच होने के लिए बहुत अच्छा लगता है, तो यह शायद है।

बच्चों को कंप्यूटर और इंटरनेट के उचित उपयोग के बारे में शिक्षित करें और घर और स्कूल में समान रूप से उनकी ऑनलाइन गतिविधियों की निगरानी करना सुनिश्चित करें। उन्हें केवल आपके घर के मध्य क्षेत्र में स्थित कंप्यूटर तक पहुंच होनी चाहिए और आपको नियमित रूप से सभी ब्राउज़र और ईमेल गतिविधि की जांच करनी चाहिए। माता-पिता के नियंत्रण सॉफ़्टवेयर का उपयोग करना बुद्धिमानी है जिससे कि उपयोगकर्ता उन साइटों के प्रकार को सीमित कर सकता है, जिनका उपयोग किया जा सकता है। स्कूलों में, प्रतिबंधित वेबसाइट और अन्य उपयोगकर्ता प्रतिबंध होने चाहिए जो उपयोगकर्ता और संस्था को साइबर अपराध से बचाने में मदद करेंगे। इसी तरह, कंपनियों को शिक्षित होना चाहिए और वर्कप्लेस पीसी को नियंत्रित करने वाली नीतियों को लिखना चाहिए और कंपनी के खिलाफ साइबर अपराध के जोखिम को कम करने के लिए इसके नेटवर्क का उपयोग करना चाहिए। यह सुनिश्चित करने का एक निश्चित तरीका है कि आप साइबर अपराधों के शिकार न हों, कंप्यूटर को पूरी तरह से इंटरनेट से अलग करना है। यदि कोई नेटवर्क नहीं है, तो किसी भी साइबर हमले के बारे में चिंता करने की ज़रूरत नहीं है। हालाँकि, यह विकल्प हमारे परस्पर समाज में सबसे व्यवहार्य नहीं है। सच्चाई यह है कि संभावित साइबर अपराधों से बचने के लिए आवश्यक सावधानी बरतना आपके ऊपर है।

10.10 शब्दावली

साइबर कानून: साइबर कानून एक सामान्य शब्द है जो इंटरनेट और वर्ल्ड वाइड वेब के सभी कानूनी और नियामक पहलुओं को संदर्भित करता है। किसी भी कानूनी पहलुओं से संबंधित साइबरस्पेस के विषय में से संबंधित के साथ या संबंधित कुछ भी साइबर कानून के दायरे में आता है।

साइबर सुरक्षा: साइबर सुरक्षा कंप्यूटर सिस्टम की चोरी या क्षति से उनके हार्डवेयर, सॉफ्टवेयर या इलेक्ट्रॉनिक डेटा की सुरक्षा के साथ-साथ उनके द्वारा प्रदान की जाने वाली सेवाओं के विघटन या गलत व्यवहार से सुरक्षा है। साइबर सुरक्षा का मुख्य उद्देश्य व्यवसाय को अधिक सफल बनाने में मदद करना है।

साइबर स्पेस: साइबरस्पेस एक संवादात्मक डोमेन है जो डिजिटल नेटवर्क से बना होता है जिसका उपयोग सूचनाओं को संग्रहीत, संशोधित और संचार करने के लिए किया जाता है। इसमें इंटरनेट भी शामिल है, लेकिन हमारी कंपनियों, बुनियादी ढांचे और सेवाओं का समर्थन करने वाली अन्य सूचना प्रणालियाँ भी शामिल हैं।

साइबर क्राइम: साइबर क्राइम एक व्यक्ति की पहचान को चुराने के लिए कंप्यूटर और इंटरनेट का उपयोग करने वाले अपराध होते हैं या किसी व्यक्ति की पहचान को बेचने या चोरी करने या पीड़ितों को बेचने या द्वेषपूर्ण कार्यक्रमों के साथ संचालन को बाधित करने के लिए होते हैं। साइबर क्राइम कानून प्रवर्तन ब्यूरो के लिए एक बहुत बड़ा काम है क्योंकि वे बेहद तकनीकी अपराध हैं

हैकिंग: हैकिंग किसी भी कंप्यूटर सिस्टम या नेटवर्क तक अनधिकृत पहुंच है। यह विधि तब हो सकती है जब कंप्यूटर हार्डवेयर और सॉफ़्टवेयर में कोई कमज़ोरी हो, जिसे घुसपैठ किया

जा सकता है यदि ऐसे हार्डवेयर या सॉफ़्टवेयर में पैचिंग, सुरक्षा नियंत्रण, कॉन्फ़िगरेशन या खराब पासवर्ड विकल्प की कमी है।

पहचान की चोरी: पहचान की चोरी तब होती है जब कोई व्यक्ति चोरी या धोखाधड़ी करने के लिए अपनी जागरूकता के बिना किसी अन्य व्यक्ति की व्यक्तिगत जानकारी को जब्त कर लेता है। आमतौर पर, पीड़ित को यह विश्वास करने के लिए प्रेरित किया जाता है कि वे एक वास्तविक व्यवसाय के लिए संवेदनशील निजी डेटा का खुलासा कर रहे हैं, कभी-कभी यह बिलिंग या सदस्यता जानकारी आदि के आधुनिकीकरण के लिए ई-मेल की प्रतिक्रिया के रूप में होता है।

सूचना सुरक्षा: सूचना सुरक्षा जिसे इन्फोसेक के रूप में भी जाना जाता है, जानकारी की सुरक्षा के बारे में है, जो आम तौर पर सूचना की गोपनीयता, अखंडता, उपलब्धता (सीआईए) पर केंद्रित है। यह सुनिश्चित करता है कि भौतिक और डिजिटल दोनों डेटा अनधिकृत पहुँच, उपयोग, प्रकटीकरण, व्यवधान, संशोधन, निरीक्षण, रिकॉर्डिंग या विनाश से सुरक्षित हैं।

लॉजिक बॉम्ब: वे मूल रूप से निर्देशों का एक समूह हैं जहां गुप्त रूप से एक कार्यक्रम में निष्पादित किया जा सकता है जहां यदि कोई विशेष स्थिति सच है तो अंतिम परिणाम आमतौर पर हानिकारक प्रभावों के साथ समाप्त होता है।

वायरस / वार्म अटैक: वायरस ऐसे प्रोग्राम हैं जो किसी भी फाइल में खुद को एम्बेड कर सकते हैं। कार्यक्रम तब खुद को कॉपी करता है और एक नेटवर्क पर अन्य कंप्यूटरों में फैलता है जो वे उन पर कुछ भी प्रभावित करते हैं, या तो इसे बदलकर या नष्ट कर के।

वेब जैकिंग: यह वह जगह है जहां हैकर पहुंच प्राप्त करता है और किसी अन्य व्यक्ति की वेब साइट को नियंत्रित कर सकता है, जहां वह साइट पर जानकारी को नष्ट या बदल सकता है, क्योंकि वे उनके लिए उपयुक्त हैं। साइबर क्राइम का यह तरीका राजनीतिक एजेंडा को संतुष्ट करने या विशुद्ध मौद्रिक साधनों के लिए किया जाता है।

10.12 बोध प्रश्नो के उत्तर

बोध प्रश्न क:

4. i) डेटा सुरक्षा ii) इंटरनेट iii) भेद्यता iv) इंटरएक्टिव v) नेटवर्क

10.13 स्वपरख प्रश्न

1) इंटरनेट और डब्ल्यू डब्ल्यू डब्ल्यू के बीच अंतर बताइए।

2) सूचना सुरक्षा और साइबर सुरक्षा के बीच अंतर बताइए।

3) साइबर सुरक्षा क्या है? आज के डिजिटल रूप से जुड़े विश्व में इसका महत्व बताएं।

4) साइबर खतरों से आप क्या समझते हैं? इसके विभिन्न प्रकारों की व्याख्या कीजिए।

5) साइबर अपराध के विभिन्न रूप क्या हैं?

6) कंपनियों द्वारा किन विभिन्न सुरक्षा बाधाओं का सामना क्या किया जाता है? एम एस एस पी कैसे उन्हें हल करने में मदद कर सकते हैं?

7) चोरी के अपराध कितने प्रकार के होते हैं?

 **नोट**	ये प्रश्न इस इकाई को समझने में सहायक हैं। इन प्रश्नों के उत्तर लिखने के लिए प्रयास करें लेकिन अपना उत्तर विश्वविद्यालय को न भेजें। यह केवल आपके अभ्यास के लिए है।

ignou
THE PEOPLE'S
UNIVERSITY