खंड 4
साइबर सुरक्षा और आई टी अधिनियम

खंड 4 साइबर सुरक्षा और आई.टी. अधिनियम

यह पाठ्यक्रम "ई-कॉमर्स" का चौथा खंड है। यह खंड शिक्षार्थियों को साइबर सुरक्षा, साइबर सुरक्षा के विभिन्न उपायों, विभिन्न प्रकार के साइबर अपराधों और खतरों के साथ-साथ आई टी अधिनियम की विभिन्न विशेषताओं से परिचित कराता है। इस खंड को साइबर शब्द से संबंधित विभिन्न शब्दावली की व्याख्या करने और जरूरत पड़ने पर उनकी सहायता के लिए आई टी अधिनियम के तहत दिए गए विभिन्न प्रावधानों को समझने के लिए सरंचित किया गया है । "साइबर सुरक्षा और आई टी अधिनियम" विषय पर खंड में तीन इकाइयाँ शामिल हैं, जिनका विवरण नीचे दिया गया है:

- **इकाई -10:** यह इकाई शिक्षार्थियों को साइबर दुनिया की बुनियादी शब्दावली को समझने में मदद करती है। इकाई साइबर सुरक्षा के अवलोकन के बारे में संक्षेप में बताती है कि यह सूचना सुरक्षा से कैसे भिन्न है। इकाई का बाद का हिस्सा विभिन्न प्रकार के प्रचलित साइबर खतरों, साइबर अपराधों, साइबर कानूनों और सुरक्षा बाधाओं पर केंद्रित है।
- **इकाई -11:** यह इकाई इंटरनेट पर विभिन्न कमजोर जानकारी जैसे कि दुर्भावनापूर्ण सॉफ़्टवेयर, वायरलेस सुरक्षा चुनौतियों, हैकर्स और कंप्यूटर अपराधों आदि के बारे में शिक्षार्थियों को बताती है। इकाई का बाद का हिस्सा व्यवसाय को सुरक्षित करने के विभिन्न उपायों या प्रवर्तन के अपने विभिन्न तरीकों के साथ नेटवर्क लेनदेन पर संक्षिप्त जानकारी देता है।
- **इकाई -12:** यह इकाई समय के साथ अपने विभिन्न संशोधनों और प्रावधानों के साथ शिक्षार्थियों को आई टी अधिनियम 2000 से अवगत कराती है। इस इकाई के अध्ययन के बाद शिक्षार्थी डिजिटल हस्ताक्षर, उनकी प्रक्रिया, कार्य और कानूनी स्थिति, साइबर अपराधों, अपीलीय न्यायाधिकरण, एन्क्रिप्शन आदि के बारे में भी समझ सकेंगे।

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

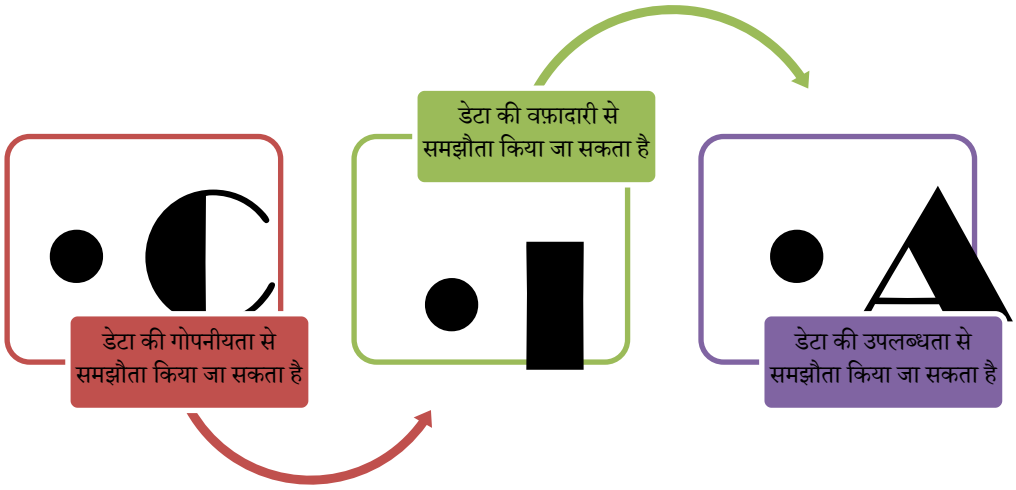
साइबर खतरे एक वैश्विक जोखिम है जिससे सरकारों, निजी क्षेत्र, गैर-सरकारी संगठनों - और वैश्विक समुदाय को समग्र रूप से निपटना चाहिए। कंप्यूटर सुरक्षा, साइबर सुरक्षा या सूचना

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:

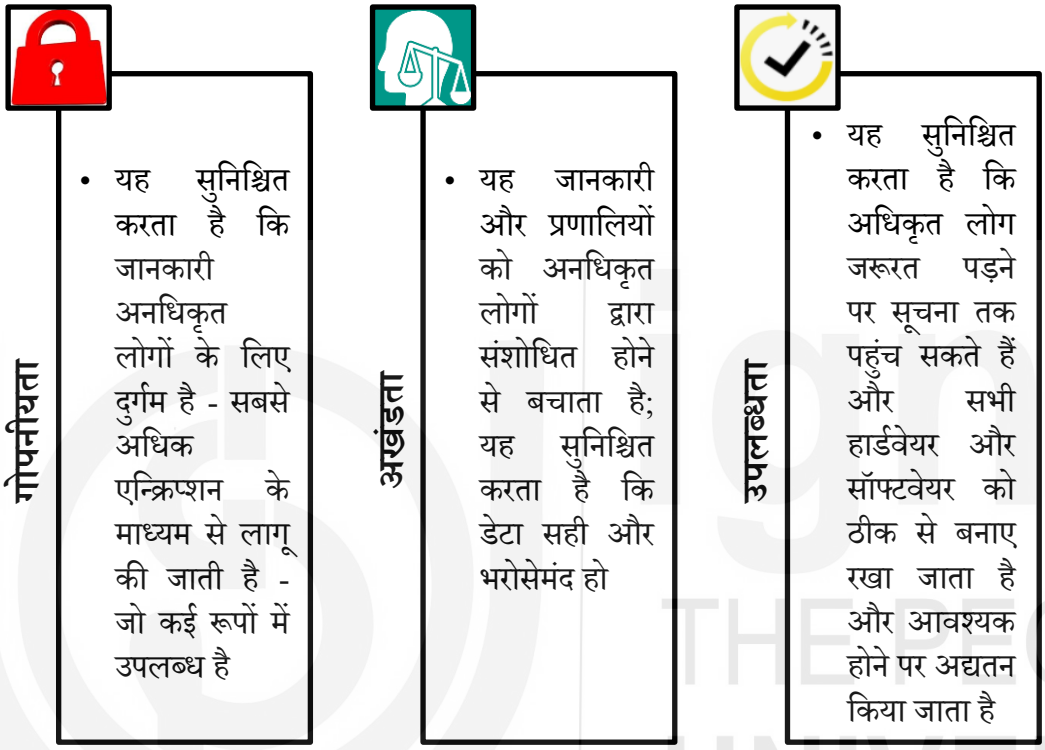
- इंटरनेट से जुड़ी सेवाओं, स्मार्ट उपकरणों और संचार प्रणालियों के सुरक्षित उपयोग को सक्षम करना।
- सभी आईटी नियंत्रित व्यावसायिक कार्यों, महत्वपूर्ण राष्ट्रीय अवसंरचनाओं के सुरक्षित उपयोग को सक्षम करना।
- अनधिकृत पहुंच का पता लगाना और उसकी रोकथाम करना।
- आईटी सिस्टम और क्लाउड सेवाओं की उपलब्धता।
- ग्राहकों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

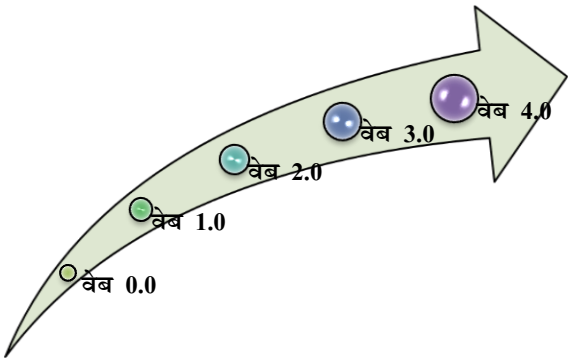
वर्ल्ड वाइड वेब (डब्ल्यू.डब्ल्यू.डब्ल्यू): जीवन के दौरान, जब लोग "इंटरनेट" कहते हैं, तो अधिकांश समय वे वास्तव में वर्ल्ड वाइड वेब या डब्ल्यू.डब्ल्यू.डब्ल्यू का उल्लेख करते हैं। डब्ल्यू.डब्ल्यू.डब्ल्यू इंटरनेट में उपलब्ध सभी सूचनाओं का संग्रह है। तो, सभी पाठ, चित्र, ऑडियो, वीडियो ऑनलाइन डब्ल्यू.डब्ल्यू.डब्ल्यू 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।

इकाई 11 साइबर सुरक्षा उपाय

इकाई की रूपरेखा

11.0 उद्देश्य

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

- विभिन्न साइबर सुरक्षा उपायों को समझ सकें;
- इंटरनेट पर कमजोर जानकारी के बारे में बता सकें ;
- साइबर फोरेंसिक विधियों की व्याख्या कर सकें;
- इंटरनेट पर विभिन्न प्रकार के खतरों को समझ सकें ;
- इंटरनेट पर व्यापार लेनदेन को सुरक्षित करना समझ सकें; तथा
- विभिन्न प्रकार के सुरक्षा उपायों और प्रवर्तन के बारे में बता सकें।

11.1 प्रस्तावना

पूरी दुनिया इस समस्या का सामना कर रही है कि साइबर क्राइम से कैसे लड़ा जाए और नागरिकों और संगठनों को सुरक्षा को प्रभावी ढंग से कैसे बढ़ावा दिया जाए। यदि हम एक पृष्ठभूमि में जाते हैं, तो हम जल्दी से समझेंगे कि साइबर अपराध, जिसे कंप्यूटर अपराध भी कहा जाता है, मूल रूप से अवैध अंत करने के लिए एक उपकरण के रूप में एक कंप्यूटर का उपयोग है, जैसे कि धोखाधड़ी करना, बाल पोर्नोग्राफी और बौद्धिक संपदा की तस्करी, अस्तित्व को नष्ट करना, या गोपनीयता का उल्लंघन करना आदि।

इन उभरते अपराधों से निपटने के लिए समस्या की समन्वित वैश्विक प्रतिक्रिया की आवश्यकता है। साइबर अपराध बड़े पैमाने पर बढ़ रहा है और साइबर अपराध से निपटने के लिए वर्तमान तकनीकी मॉडल अव्यवस्थित हैं। यह इंगित करता है कि साइबर अपराध को कम करने के लिए आगे निवारक रणनीतियों की आवश्यकता है। आगे के खण्डों में यह इकाई साइबर अपराधों से सम्बंधित विभिन्न सुरक्षा उपाय और विभिन्न पहलुओं पर प्रकाश डालती है।

11.2 साइबर सुरक्षा उपाय

जैसा कि हम जानते हैं कि इंटरनेट ने व्यवसाय, शिक्षा, सरकार, स्वास्थ्य सेवा और यहां तक कि हमारे प्रियजनों के साथ बातचीत करने के तरीकों को बदल दिया है - यह सामाजिक विकास के प्रमुख पहलुओं में से एक बन गया है। यह एक मुख्य कारण है कि दुर्भावनापूर्ण लिंक, ट्रोजन और वायरस इंटरनेट के माध्यम से प्रवेश कर रहे हैं। डाटा , उल्लंघन लगातार अधिक हो रहे हैं, अनपेक्षित उपयोगकर्ता पहले से कही अधिक निर्भर हो रहे हैं। जब एक क्लिक में हजारों, और यहां तक कि लाखों निकल सकते हैं, तो उपयोगकर्ताओं को ऐसा करने के लिए कार्रवाई करने की आवश्यकता होती है जो उन्हें चौकस और सुरक्षित ऑनलाइन रहने के लिए सुविधा प्रदान कर सकता है। साइबर अपराध, पारंपरिक अपराधों के विपरीत, जो एक

भौगोलिक स्थान में किए जाते हैं, ऑनलाइन प्रतिबद्ध होते हैं और यह अक्सर किसी भी भौगोलिक स्थान से स्पष्ट रूप से जुड़ा नहीं होता है, जिसका अर्थ है कि यह अधिकार क्षेत्र केंद्रित नहीं है। कंप्यूटर सुरक्षा, साइबर सुरक्षा या सूचना प्रौद्योगिकी सुरक्षा कंप्यूटर, सर्वर, मोबाइल डिवाइस, इलेक्ट्रॉनिक सिस्टम, नेटवर्क और दुर्भावनापूर्ण हमलों से डाटा का बचाव करने का अभ्यास है।

11.2.1 साइबर सुरक्षा विश्लेषकों की भूमिका

सूचना सुरक्षा या साइबर सुरक्षा विश्लेषक के दैनिक कार्य में उनके काम करने के स्थान के आधार पर उतार चढाव होता है। लेकिन सामान्य तौर पर इसका कार्य सुरक्षा पहुंच कि निगरानी करना है । सुरक्षा विश्लेषक पासवर्ड, बैज, लॉग-इन और अधिक का आकलन करते है क्योंकि वे किसी साइट या सिस्टम को सुरक्षित रखने के लिए काम करते हैं। साइबर सुरक्षा विश्लेषक (जिसे सूचना सुरक्षा विश्लेषक भी कहा जाता है) कंपनी के कंप्यूटर नेटवर्क और सिस्टम की देखभाल के लिए सुरक्षा उपाय करते हैं। वे खतरों पर लगातार नज़र रखते हैं और सुरक्षा में किसी भी उल्लंघन के लिए अपने संगठन के नेटवर्क की निगरानी करते हैं। दूसरी ओर जिम्मेदारियां बहुत व्यापक हैं, सुरक्षा विश्लेषक की कुछ प्रमुख भूमिकाएँ हैं:

- उपयोक्ता अभिगम नियंत्रण और विशिष्टता तथा अभिगम प्रबंधन प्रणालियों को सेट और कार्यान्वित करना।
- एक तरफ़ा गतिविधि को वर्गीकृत करने के लिए नटवर्क और एप्लीकेशन के प्रदर्शन की निगरानी करना।
- सेट और उपयोगकर्ता अभिगम नियंत्रण और विशिष्टता और प्रबंधन प्रणाली का उपयोग लागू करना।
- सुरक्षा अभ्यास सुनिश्चित करने के लिए नियमित ऑडिट करना।

11.2.2 आवश्यक साइबर सुरक्षा उपाय

विभिन्न आवश्यक साइबर सुरक्षा उपाय नीचे दिए गए हैं:

- मजबूत पासवर्ड का उपयोग करना
- नियंत्रण का उपयोग
- फ़ायरवॉल
- सुरक्षा सॉफ्टवेयर का उपयोग
- अद्यतन कार्यक्रमों और प्रणालियों को नियमित रूप से जाँचना
- घुसपैठ के लिए निगरानी
- जागरूकता बढ़ाना

आगे के खंडों में इकाई ने विभिन्न मजबूत साइबर सुरक्षा उपायों पर विस्तार से चर्चा की है।

11.2.3 उद्यमों द्वारा लिए जाने वाले एहतियाती साइबर-सुरक्षा उपाय

जैसा कि हम जानते हैं कि हर व्यवसाय ऑनलाइन बढ़ रहा है। साइबर-सुरक्षा मूल बातें समझने के लिए नीचे दर्शाई कुछ बातों पर ध्यान दिया जाना चाहिए:

- **एक एकीकृत खतरा प्रबंधन (UTM) प्रणाली:** सुरक्षा उपकरणों का एक संयोजन होना चाहिए जो इंटरनेट के प्रवेश द्वार के रूप में कार्य करता है।

- **एक स्पैम फ़िल्टर:** एक स्पैम फ़िल्टर एक प्रोग्राम है जिसका उपयोग अवांछित और अवांछित ईमेल का पता लगाने और उन संदेशों को उपयोगकर्ता के इनबॉक्स में जाने से रोकने के लिए किया जाता है। अन्य प्रकार के फ़िल्टरिंग कार्यक्रमों की तरह, एक स्पैम फ़िल्टर निश्चित मानदंड की तलाश करता है, जिस पर वह निर्णय लेता है। दूसरी ओर यह संभावित रूप से दुर्भावनापूर्ण फ़ाइलों को ईमेल के माध्यम से नेटवर्क में प्रवेश करने से रोकता है।

- **एंटीवायरस / एंटी-मैलवेयर सॉफ़्टवेयर:** एंटीवायरस सॉफ़्टवेयर मूल रूप से कंप्यूटर वायरस का पता लगाने और हटाने के लिए विकसित किया गया था, इसे एंटी-मैलवेयर के रूप में भी जाना जाता है, जोकि एक कंप्यूटर प्रोग्राम है, जिसका उपयोग मैलवेयर को रोकने, पता लगाने और हटाने के लिए किया जाता है। ये ऐसे एप्लिकेशन हैं जो सर्वर, लैपटॉप और अन्य उपकरणों को मैलवेयर से बचाते हैं।

- **पैच प्रबंधन सिस्टम:** यह सुरक्षा स्वामियों को हटाने के लिए सॉफ्टवेयर अपडेट की स्थापना का प्रबंधन करता है।

- **2-कारक प्रमाणीकरण:** यह अनधिकृत साइन-इन को रोकने के लिए प्रमाणीकरण का दूसरा स्तर देता है।

- **डिवाइस एन्क्रिप्शन:** यह मशीन पर संग्रहीत किसी भी डाटा को अपराधियों के लिए बेकार कर देता है और डाटा को गुप्त रखता है।

- **रूटीन डाटा बैकअप:** मूल खो जाने कि स्थिति में यह व्यावसायिक डाटा कि एक प्रति सुरक्षित ऑफ़साइट स्थान पर रखता है।

- **सामग्री फ़िल्टरिंग:** यह खतरनाक या निषिद्ध वेबसाइटों तक पहुंच को रोकता है जो संक्रमण के जोखिम को कम करता है।

- **डिजास्टर रिकवरी प्लान:** यह निर्धारित करता है कि साइबर हमले जैसी सहज घटना से कैसे उभर सकते है ।

11.3 आई ओ टी और इसके प्रभाव

आई ओ टी (IoT) इंटरनेट ऑफ थिंग्स के लिए उपयोग किया जाने वाला एक संक्षिप्त नाम है; यह मूल रूप से कई उपकरणों का एक नेटवर्क है जो किसी भी प्रकार की सूचनाओं के आदान-

प्रदान और संकलन के उद्देश्य से विविध सॉफ्टवेयर, इलेक्ट्रॉनिक्स और अलग-अलग प्रकार के नेटवर्क कनेक्टिविटी के साथ जुड़ा हुआ है। आई ओ टी उपकरण बहुत विशाल डाटा रख सकते हैं वह बहुत विशाल है। आई ओ टी में कनेक्टेड उपकरणो के विशाल प्रसार ने दुनिया भर में लाखों या शायद लाखों कनेक्टेड डिवाइसों और सेवाओं की बढ़ती मांग के जवाब में मजबूत सुरक्षा की भारी मांग पैदा की है।

चूँकि आई ओ टी उपकरण हर समय इंटरनेट से जुड़े होते है, यह सुरक्षा, उनके प्लेटफार्मों और ऑपरेटिंग सिस्टम, उनके संचार और उन सिस्टमों से सवाल करता है जिनसे वे जुड़े हुए हैं। इस तरह की सुरक्षा चुनौतियों को दूर करने के लिए, इन उपकरणों और प्लेटफार्मों को सूचना हमलों और शारीरिक हानि दोनों से बचाने के लिए उपकरणों के एक नए सेट की आवश्यकता है । इसके अलावा, उपकरणों के बीच लेनदेन को एन्क्रिप्ट करने की आवश्यकता है। कुछ उपकरणों में बहुत ही सरल प्रोसेसर एवं ऑपरेटिंग सिस्टम है, जोकि परिष्कृत सुरक्षा प्रणालियों का समर्थन करने में असमर्थ है।

हम उपरोक्त पाराग्राफ से जानते है और दर्शाते है कि आई ओ टी सुरक्षा आई ओ टी से जुड़े उपकरणो और नेटवर्क की सुरक्षा के साथ आशंकित प्रौद्योगिकी क्षेत्र है। इंटरनेट से कनेक्ट करने की अनुमति देने से वे कई गंभीर कमज़ोरियों के लिए खुल जाते है अगर वे उचित रूप से संरक्षित नहीं हैं। आई ओ टी (IoT) सुरक्षा आई ओ टी उपकरण और उनसे जुड़े नेटवर्क को सुरक्षित करने का कार्य है। व्यवसाय आई ओ टी उपकरणों में औद्योगिक मशीनें, स्मार्ट ऊर्जा ग्रिड, बिल्डिंग ऑटोमेशन, और जो भी व्यक्तिगत डिवाइस कर्मचारी काम करते हैं, शामिल हैं।

आई औ टी उपकरणों का प्रयोग करते समय निम्न पहलुओं का ध्यान रखना चाहिए:

- फ़ायरवॉल के पीछे किसी प्रोग्राम को ब्लॉक करना या सॉफ़्टवेयर की केवल कुछ विशेषताओं के उपयोग को प्रतिबंधित करना, महत्वपूर्ण डाटा को लीक होने से बचाना आदि को । नेटवर्क से जुड़े सभी उपकरणों को नवीनतम सॉफ़्टवेयर में अपडेट किया जाना चाहिए।

- हार्डवेयर, सॉफ्टवेयर और कनेक्टिविटी सभी को प्रभावी ढंग से काम करने के लिए आई ओ टी (IoT) के लिए सुरक्षित होने की आवश्यकता होती है । सुरक्षा के बिना, रेफ्रिजरेटर से निर्माण बॉट्स तक, किसी भी जुड़े उपकारों को हैक किया जा सकता है। एक बार जब हैकर्स व्यवस्थित हो जाते हैं, तो वे उपकरण की कार्यक्षमता को संभाल सकते हैं और उपयोगकर्ता के डिजिटल डाटा को चुरा सकते हैं।

11.4 इंटरनेट पर व्यवहार्य जानकारी

जब कोई फसल खराब हो जाती है, तो किसी खतरे से बचाव या प्रतिक्रिया के लिए कार्य करने में अक्षमता होती है। उदाहरण के लिए, जो लोग मैदानी इलाकों में घूमते रहते हैं, वे बाढ़ की चपेट में आने वाले लोगों की तुलना में अधिक कमजोर होते हैं। इसे ही हम आर्थिक भेद्यता कहते हैं। यदि हम एक तकनीकी परिप्रेक्ष्य में बात करते हैं, तो कंप्यूटर भेद्यता एक साइबर-सुरक्षा अभिव्यक्ति है जो एक प्रणाली में कमी को संदर्भित करती है जो इसे हमले के लिए खुला छोड़ सकती है। यह भेद्यता किसी भी प्रकार की कमजोरी का उल्लेख कंप्यूटर में, प्रक्रियाओं के

एक समूह में, या ऐसी किसी भी चीज़ में हो सकती है जो सूचना सुरक्षा को किसी खतरे के संपर्क में लाने की अनुमति देती है।

चित्र 11.1: साइबर दुनिया में विभिन्न संवेदनशील शब्द

अब, लगभग हर व्यवसाय में डाटा चालित प्रक्रियाएं होती हैं। यदि कोई मशीन या कंप्यूटर व्यवसाय लेनदेन को चलाना शुरू कर देता है, तो व्यवसायी व्यक्ति ग्राहकों को बेचने या मशीन के क्रम में नहीं होने पर आपूर्तिकर्ताओं के साथ ऑर्डर करने के लिए दक्ष नहीं हो सकता है। यह कभी भी हो सकता है कि एक अतिचारक कंप्यूटर सिस्टम में भी प्रवेश करने की करें और ग्राहकों के गोपनीय डाटा विवरण को नष्ट कर दे। ऐसे परिदृश्य में, कोई भी व्यवसाय कभी भी संचालित नहीं हो सकता है। तदनुसार, किसी भी व्यवसाय की सफलता के लिए, डाटा सुरक्षा एक शीर्ष वरीयता पर होनी चाहिए। सूचना संगठनों में अनधिकृत पहुंच, परिवर्तन, चोरी या किसी भी प्रकार की शारीरिक क्षति को रोकने के लिए व्यापारिक संगठनों में नीतियां, प्रक्रियाएं और तकनीकी उपाय होने चाहिए।

11.4.1 सिस्टम की कमजोरियाँ

जब बड़ी मात्रा में डिजिटल जानकारी संग्रहीत की जाती है, तो यह कई अन्य प्रकार के खतरों की चपेट में आ सकती है । सूचना प्रणालियों को कंप्यूटर नेटवर्क के माध्यम से कई स्थानों पर परस्पर जोड़ा जा सकता है। और इसलिए, घुसपैठियों के हमले या अनधिकृत पहुंच कभी भी कंप्यूटर नेटवर्क के किसी भी पहुंच बिंदु पर हो सकती है, जो पूरे नेटवर्क को नष्ट कर सकती है।

उसी तरह, मल्टी-लेयर क्लाइंट / सर्वर कंप्यूटिंग वातावरण भी प्रत्येक परत पर असुरक्षित है। डाटा ट्रांसमिशन के दौरान अनधिकृत व्यक्ति के लिए नेटवर्क पर संगठन के मूल्यवान डाटा को चुराना या बदलना हमेशा संभव होता है। घुसपैठिये सेवा को बाधित करने के लिए हमलों या दुर्भावपूर्ण सॉफ्टवेयर का उपयोग कर सकते है।

11.4.2 इंटरनेट कमजोरियाँ

कंप्यूटर नेटवर्क के बजाय, इंटरनेट के माध्यम से जुड़े सिस्टम अधिक असुरक्षित हैं क्योंकि वे पूरी दुनिया में किसी के लिए भी खुले हैं। इंटरनेट इतना बड़ा है कि इसका दुरुपयोग होने पर इसका व्यापक प्रभाव हो सकता है। जब हमारे कॉर्पोरेट नेटवर्क में इंटरनेट का उपयोग किया जाता है, तो हम उद्योग के सूचना नेटवर्क में बाहरी संचालन के लिए अधिक संवेदनशील होते हैं। कंप्यूटर सिस्टम जो स्थायी रूप से इंटरनेट से जुड़े होते हैं, बाहरी व्यक्तियों के प्रवेश के लिए अधिक असुरक्षित होते हैं क्योंकि वे निश्चित आई पी पते के साथ जल्दी से पंजीकरण कर सकते हैं।

चित्र 11.2 (क): इंटरनेट कमजोरियाँ

चित्र -11.2 (ख): कमजोरियाँ को इंटरनेट के द्वारा सही करना

एक निश्चित आई पी अड्रेस हैकर्स को एक निश्चित लक्ष्य प्रदान करता है । यदि टेलीफोन सेवा सुरक्षित व्यक्तिगत इंटरनेट नेटवर्क से जुड़ी नहीं है, तो स्विच किया जाने वाला इंटरनेट बुनियादी ढांचा सबसे कमजोर है। अधिकांश सार्वजनिक इंटरनेट (वी ओ आई पी) ट्रैफ़िक को एन्क्रिप्ट नहीं किया गया है, ताकि जिस किसी के पास नेटवर्क है वह बात सुन सके। वी ओ आई पी सहायक सर्वरों से, हैकर्स या आवाज सेवाओं को बंद करके बातचीत को रोका जा सकता है। आजकल मेल, इंस्टेंट मैसेजिंग (आई एम) और पीयर टू पीयर फाइल-शेयरिंग सेवाओं की भेद्यता भी बढ़ गई है। कर्मचारियों के लिए ईमेल का उपयोग कर मूलयवान कम्पनी रहस्यों, वित्तीय देता या संवेदनशील जानकारी को अनधिकृत प्राप्तकर्ताओं तक पहुँचाना संभव है। लोकप्रिय आई एम एप्लीकेशन उपयोगकर्ताओं को सार्वजानिक इंटरनेट ट्रांसमिट करते समय इसे समझने और पढ़ने की अनुमति देने के लिए सुरक्षित तरीकों का उपयोग नहीं करते। कुछ मामलों में इंटरनेट द्वारा इंस्टेंट मेसेजिंग को सुरक्षित नेटवर्क के ठोस रूप में इस्तेमाल किया जाता है। पी पी फाइलों में साँझा करके से किसी भी व्यक्तिगत या कॉर्पोरेट जानकारी का खुलासा या कोई दुर्भावनापूर्ण सॉफ्टवेयर भी फ़ैल सकता है।

11.4.3 वायरलेस सुरक्षा चुनौतियां

वायरलेस नेटवर्किंग कई फायदे प्रदान करता है, लेकिन यह विभिन्न सुरक्षा खतरों के साथ भी जुड़ा हुआ है। वायरलेस सुरक्षा खतरों और कमजोरियों के लिए तकनीकी समाधान का कार्यान्वयन, और वायरलेस सुरक्षा संगठन की प्राथमिक आवश्यकता है। सार्वजनिक स्थान पर एक वायरलेस नेटवर्क का उपयोग करना सुरक्षित जैसे, एक हवाई अड्डा, पुस्तकालय, शॉपिंग मॉल में एक वायरलेस नेटवर्क का उपोयग सुरक्षित नहीं है। वास्तव में, घर पर वायरलेस नेटवर्क सुरक्षित नहीं है क्योंकि कभी भी रेडियो आवृत्ति बैंड आसानी से स्कैन किए जा सकते हैं। इसलिए लैन, ब्लूटूथ, वाई-फाई नेटवर्क आदि सभी आसानी से हैकिंग की चपेट में हैं। वायरलेस नेटवर्क में चार निम्न उल्लेखित बुनियादी घटक हैं:

- रेडियो आवृत्तियों का उपयोग करके डाटा का संचरण
- एक्सेस पॉइंट, जो संगठनात्मक नेटवर्क के लिए एक कनेक्शन प्रदान करते हैं
- उपकरण - लैपटॉप, पीडीए आदि, एवं
- उपयोगकर्ता

ये घटक हमले का स्रोत बन सकते हैं जिसके कारण संगठन को डाटा से समझौता करना पड़ता है। इसके अलावा, एक वाई-फाई नेटवर्क में, घुसपैठिए आसानी से पहचान सेवा सेट पहचानकर्ता (एस एस आई डी) एकत्र कर सकते हैं, जो पहुंच बिंदुओं को चिह्नित करते हैं, कई बार संचारित करते हैं। वाई-फाई नेटवर्क में आमतौर पर मूलभूत सुरक्षा उपाय नहीं होते हैं, जो अनधिकृत उपयोगकर्ताओं को आसपास की इमारतों या साइट के बाहर नेटवर्क तक पहुंचने की अनुमति देते हैं। एक हमलावर जिसके पास सही एस एस आई डी के साथ एक पहुंच बिंदु है, अन्य नेटवर्क संसाधनों तक पहुंच सकता है। इसके अलावा, घुसपैठिए वेबसाइट के पास एक अलग रेडियो चैनल में उपयोगकर्ता के रेडियो नेटवर्क इंटरफ़ेस नियंत्रक (एन आई सी) के लिए अनधिकृत पहुंच बिंदुओं को स्थापित करने के लिए एकत्रित जानकारी का उपयोग कर सकते हैं। दुष्ट अभिगम बिंदु का उपयोग करने वाले हैकर इस एसोसिएशन के बन जाने के बाद उपयोगकर्ताओं के लॉगिन क्रेडेंशियल्स को एकत्रित करते है।

11.4.4 दुर्भावनापूर्ण सॉफ़्टवेयर

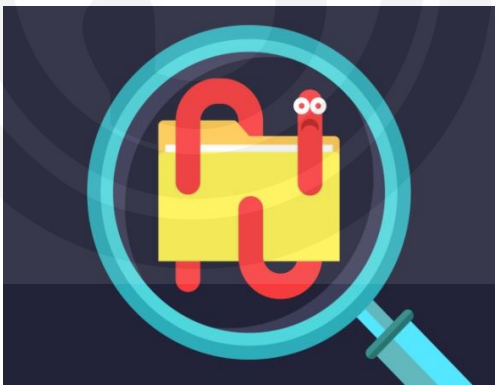
दुर्भावनापूर्ण सॉफ्टवेयर को मैलवेयर जिसमें कई खतरे जैसे- कंप्यूटर वायरस, वॉर्म और ट्रोजन हॉर्स आदि शामिल है, के रूप से भी लाना जाता है।

- **कंप्यूटर वायरस:** कंप्यूटर वायरस एक सॉफ्टवेयर प्रोग्राम है जो निष्पादित होने के लिए खुद को अन्य सॉफ्टवेयर प्रोग्राम या डाटा फाइलों में संलग्न करता है। यह कार्यक्रम के निष्पादन से पहले उपयोगकर्ता की कोई अनुमति नहीं लेता।


चित्र 11.3: कंप्यूटर वायरस

वायरस अत्यधिक विनाशकारी हो सकता है जो संगठन के डाटा को पूरी तरह से नष्ट कर सकता है, कंप्यूटर मेमोरी को ब्लॉक कर सकता है, कंप्यूटर की हार्ड ड्राइव को मिटा सकता है या प्रोग्राम को अनुचित तरीके से चलाने का कारण बन सकता है। वायरस मशीन से मशीन तक फैल सकता है, उदाहरण के लिए, ई-मेल अटैचमेंट या संक्रमित फ़ाइल के माध्यम से।

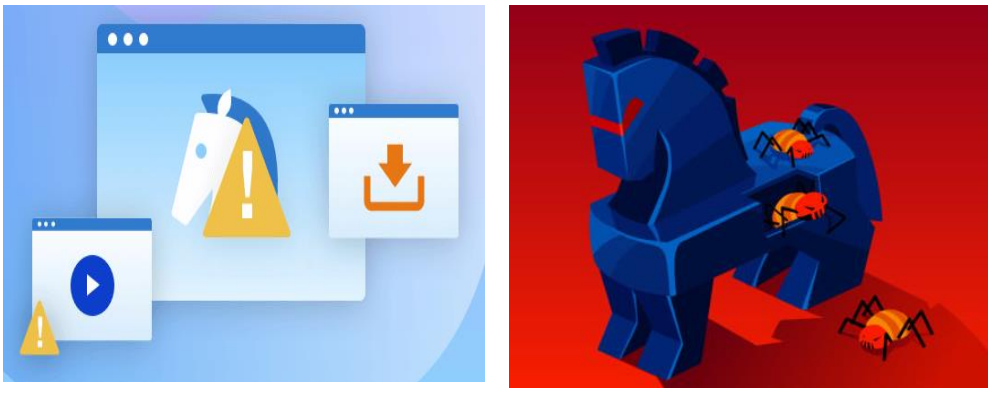
- **वॉर्म:** वॉर्म स्वतंत्र कंप्यूटर प्रोग्राम हैं जो एक कंप्यूटर से दूसरे कंप्यूटर में खुद को कॉपी करने के लिए एक कंप्यूटर नेटवर्क का उपयोग करते हैं। ये किसी भी मानवीय हस्तक्षेप के बिना अपने दम पर काम कर सकते हैं और इसे किसी भी कंप्यूटर प्रोग्राम फाइलों में संलग्न करने की आवश्यकता नहीं है।




चित्र 11.4: कंप्यूटर वर्म्स

वार्म कंप्यूटर कंप्यूटर वायरस की तुलना में बहुत अधिक तेजी से फैलते हैं। वार्म डाटा और कार्यक्रमों के लिए बहुत हानिकारक हैं। ये पूरे कंप्यूटर नेटवर्क को हिला कर सकते हैं।

- **ट्रोजन हॉर्स:** एक अन्य मैलवेयर ट्रोजन हॉर्स है जो डाटा पर चुपचाप हमला करता है। ट्रोजन हॉर्स स्वयं एक वायरस नहीं है, लेकिन यह सिस्टम में प्रवेश करने के लिए वायरस को एक रास्ता देता है। उदाहरण के लिए, ZeuS (Zot) ट्रोजन जिसने पिछले वर्षों में 3.6 मिलियन से अधिक कंप्यूटरों को संक्रमित किया और अभी भी खतरा बना हुआ है। इस सॉफ्टवेयर ने अनधिकृत व्यक्ति को कंप्यूटर में उपोग किया जाने वाले की स्ट्रोक्स को पकड़कर गुप्त रूप से ग्राहकों की बैंक लॉगिन जानकारियों की चोरी करने में मदद की। यह वायरस फिशिंग के माध्यम से फैला है।

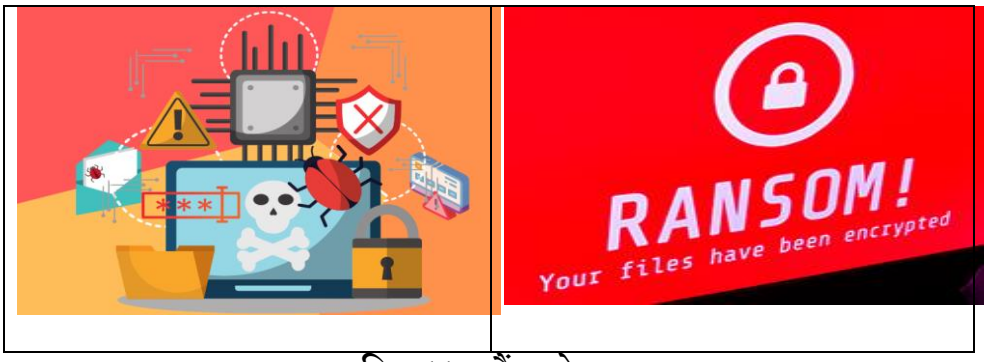


चित्र 11.5: ट्रोजन हॉर्स

- **एस क्यू एल इंजेक्शन हमले:** एस क्यू एल इंजेक्शन हमले वेब एप्लिकेशन सॉफ्टवेयर के कमजोर बिंदुओं का लाभ उठाते हैं जो सुरक्षा जांच के मामले में मजबूत नहीं होते हैं या जिनके पास डाटा सुरक्षा के लिए पर्याप्त कोड नहीं होता का लाभ उठाते है। इस तरह के हमले सिस्टम के दुर्भावनापूर्ण कार्यक्रमों और संगठनों के नेटवर्क का परिचय देते हैं।

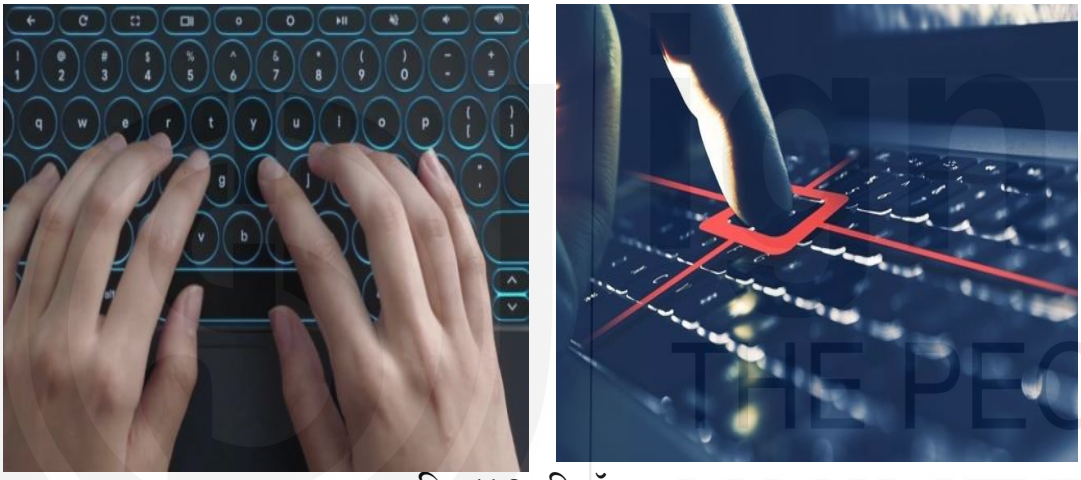
चित्र 11.6: एस क्यू एल इंजेक्शन

- **रैंसमवेयर:** रैंसमवेयर को एक मैलवेयर के रूप में जाना जाता है जो फाइलों तक पहुंच को अवरुद्ध करता है पॉप-अप संदेशों को प्रदर्शित करता है और अपने सिस्टम का नियंत्रण लेकर उपयोगकर्ताओं से पैसे निकालता है। उदाहरण के लिए, WannaCry, एक रेसंमवेयर है जिसने पिछले वर्षों में 150 से अधिक देशों में कंप्यूटरों पर हमला किया। इसने सिस्टम की फाइलों को एन्क्रिप्ट किया और फिर उपयोगकर्ताओं से एक्सेस के लिए बहुत सारे पैसे देने को कहा। रैंसमवेयर अनधिकृत ईमेल के अनुलग्नकों को डाउनलोड करके या असुरक्षित लिंक से फ़ाइल डाउनलोड करके सिस्टम में प्रवेश कर सकता है। कुछ मैलवेयर स्पाईवायर होते हैं। उपयोगकर्ताओं की गतिविधियों को देखने के लिए स्पाइवेयर खुद को गुप्त रूप से सिस्टम में स्थापित करते हैं। आजकल कई प्रकार के स्पायवेयर मौजूद हैं जो उपयोगकर्ताओं की गोपनीयता को भंग करने की कोशिश करते हैं ।



चित्र 11.7: रैंसमवेयर

- **की लॉगर:** एक की लॉगर जो उपयोगकर्ता के डाटा पर हमला करने, ईमेल खातों या पासवर्ड तक पहुंच प्राप्त करने या क्रेडिट प्राप्त करने के लिए कंप्यूटर या मोबाइल फोन पर किए गए प्रत्येक कीस्ट्रोक के सीरियल नंबर या सॉफ़्टवेयर के अन्य कोड को रिकॉर्ड करता है। कुछ स्पाईवेयर वेब ब्राउजर के होम पेज को रिसेट करते है, या धीमी गति से प्रदर्शन को पुनर्निर्देशित करते है।



चित्र 11.8: की लॉगर

11.4.5 हैकर्स और कंप्यूटर अपराध

एक हैकर एक बुद्धिमान कोडर है जिसका उद्देश्य किसी अन्य उपयोगकर्ता के कंप्यूटर सिस्टम तक पहुंच प्राप्त करना है। वे किसी भी मानवीय हस्तक्षेप के बिना दुर्भावनापूर्ण फ़ाइलों का अनुरोध कर सकते हैं, उपयोगी डाटा को नष्ट कर सकते हैं, डाटा संचारित कर सकते हैं और उपयोगकर्ता कार्यों की निगरानी के लिए पृष्ठभूमि में छिपे हुए प्रोग्राम को स्थापित कर सकते हैं। ये विशेषज्ञ हैं और वेब साइटों और कंप्यूटर सिस्टम द्वारा नियोजित सुरक्षा सुरक्षा में खामियों को खोजने के द्वारा अनधिकृत पहुंच प्राप्त करने के तरीकों को जानते हैं। किसी सिस्टम को हैक करने का उद्देश्य डाटा को चोरी करना या जानकारी को नुकसान पहुंचाना, सिस्टम को नुकसान पहुंचाना, खराब करना, किसी वेब साइट या कॉर्पोरेट सूचना प्रणाली को नष्ट करना आदि है। जिस मोबाइल प्लेटफॉर्म का सबसे ज्यादा हैकर्स इस्तेमाल करते हैं वह है, दुनिया का प्रमुख मोबाइल ऑपरेटिंग सिस्टम। मोबाइल उपकरणों पर वायरस कंपनी कंप्यूटिंग के लिए गंभीर खतरा पैदा करते हैं क्योंकि कई सेलुलर डिवाइस अब कॉर्पोरेट सूचना प्रणालियों से संबंधित हैं। सोशल नेटवर्किंग साइट्स जैसे फेसबुक, ब्लॉग साइट्स आदि भी मैलवेयर या स्पाईवेयर का स्रोत बन गए हैं। लोगों को उन संदेशों पर भरोसा करने की अधिक संभावना है जो उन्हें मित्रों से

प्राप्त होते हैं, भले ही यह संचार प्रामाणिक न हो। हैकर्स द्वारा विभिन्न प्रकार के कंप्यूटर अपराधों के बारे में नीचे चर्चा की गई है:

- **स्पूफिंग और स्निफिंग:** उपयोगकर्ताओं की संवेदनशील जानकारी तक पहुँच प्राप्त करने के लिए, हैकर्स आमतौर पर उनके जानकार का दिखावा करते हैं, इसे स्पूफिंग कहा जाता है। कभी-कभी, हैकर उन उपयोगकर्ताओं के साथ एक वेब लिंक भी साझा करता है जो मूल वेबसाइट से पूरी तरह से अलग होते हैं । इस तरीके से, हैकर प्रभावी रूप से व्यवसाय को चुराने के साथ-साथ मूल साइट से संवेदनशील ग्राहक जानकारी को एकत्र और संसाधित कर सकता है।

  स्निफिंग वह तंत्र है जिसके द्वारा डाटा पैकेट कंप्यूटर के एक नेटवर्क के माध्यम से चलते हैं जिससे स्निफ़र्स पर नज़र रखी जा सकती है और उन्हें कैद किया जा सकता है। नेटवर्क व्यवस्थापक अपने नेटवर्क के माध्यम से डाटा ट्रैफ़िक की निगरानी के लिए पैकेट स्निफ़र्स का उपयोग करते हैं। इन्हें नेटवर्क प्रोटोकॉल का विश्लेषक कहा जाता है। स्निफर्स नेटवर्क पर संभावित नेटवर्क भेद्यता या अवैध गतिविधियों की पहचान कर सकते हैं, लेकिन अगर इसका उपयोग नकारात्मक रूप से किया जाए तो यह खतरनाक और बहुत मुश्किल हो सकता है। नेटवर्क के किसी भी हिस्से से संवेदनशील जानकारी चुराने के लिए स्नाइपर ईमेल, कंपनी फाइलों और गोपनीय रिपोर्टों सहित हैकर्स को अनुमति देते हैं।

- **डिनायल-ऑफ-सर्विस (DoS):** जब कोई हैकर ऐसी गतिविधि करता है, जिसके कारण किसी संगठन के सर्वर को कुछ सेवा के लिए भारी अनुरोध प्राप्त होने लगते हैं, तो सर्वर नेटवर्क की भीड़ या दुर्घटना के कारण वास्तविक अनुरोधों का जवाब देना बंद कर देता है। इसे डिस्ट्रिब्यूटेड डिनायल ऑफ़ सर्विस (DDoS) हमला कहा जाता है। हालाँकि, डी ओ एस (DoS) हमले किसी कंपनी की सूचना प्रणालियों के प्रतिबंधित क्षेत्रों की सूचना या पहुँच को नष्ट नहीं करते, वे अक्सर एक वेब साइट को बंद करने का कारण बनते हैं, जिससे वास्तविक उपयोगकर्ताओं के लिए साइट का उपयोग करना असंभव हो जाता है। ये हमले ई-कॉमर्स साइटों के लिए बहुत खतरनाक हैं जो साइट को बंद कर देते हैं क्योंकि यह ग्राहकों के लिए दुर्गम है।

  डी डी ओ एस के हमलों में हजारों "ज़ोंबी" पीसी का भी उपयोग होता है, जो दुर्भावनापूर्ण सॉफ़्टवेयर से संक्रमित होकर बॉटनेट नहीं बनते हैं। बॉटनेट हैकर्स द्वारा बनाए जाते हैं जो दूसरे लोगों के कंप्यूटरों को बॉट मालवेयर से संक्रमित करते हैं, और घुसपैठिए से ऑर्डर भेजने के लिए एक पिछला दरवाजा खोलते हैं। एक गुलाम या ज़ोंबी संक्रमित मशीन में तब्दील हो जाता है जो मास्टर कंप्यूटर का काम करता है। जब तक वे पर्याप्त कंप्यूटरों को संक्रमित नहीं करते, हैकर्स डी डी ओ एस, फ़िशिंग अभियानों या अचयनित "स्पैम" ई-मेल पर हमले करने के लिए बॉटनेट के संचित संसाधनों का उपयोग करते है

11.4.6 साइबर अपराध

किसी भी आपराधिक गतिविधि या डाटा की चोरी जो इंटरनेट का उपयोग करके की जाती है, साइबर अपराध कहलाती है। विभिन्न प्रकार के साइबर अपराधों के बारे में नीचे विस्तार से बताया गया है:

- **पहचान की चोरी:** जैसे-जैसे अधिक से अधिक लोग इंटरनेट का उपयोग करने लगे हैं और ऑनलाइन लेनदेन कर रहे हैं, पहचान की चोरी की समस्या दिन-प्रतिदिन बढ़ती जा रही है। यह साइबर अपराधों में से एक है जिसमें उपयोगकर्ता को नुकसान पहुंचाने के लिए इंटरनेट पर कुछ अनधिकृत व्यक्तियों द्वारा व्यक्तिगत या वित्तीय जानकारी हासिल की जाती है। इस जानकारी का उपयोग खाताधारक के बैंक से पैसे चुराने या पीड़ित के नाम पर क्रेडिट कार्ड का उपयोग करके या झूठी जानकारियों के साथ चोर को प्रदान करने के लिए बहुत सारी चीजें, माल, या सेवाओं की खरीद के लिए किया जा सकता है।

  इंटरनेट पर पहचान की धोखाधड़ी वेबसाइट हैकरों का एक बड़ा लक्ष्य रहा है। अक्सर, विभिन्न प्रकार के ई-कॉमर्स साइट एक अपराध की उत्पत्ति में से एक हैं, जिसमें साइबर अपराधी उपभोक्ता धोखाधड़ी को प्रस्तुत करने के लिए अपने उपयोगकर्ताओं से व्यक्तिगत जानकारी एकत्र करते हैं।

- **फ़िशिंग:** पहचान की चोरी के लिए एक तेजी से लोकप्रिय रणनीति को फ़िशिंग कहा जाता है जिसमें नकली वेब साइट्स स्थापित करना शामिल है जो उपयोगकर्ताओं को उनके व्यक्तिगत या वित्तीय डाटा के लिए पूछने के लिए वास्तविक वेबसाइटों की तरह दिखता है। कभी-कभी पीड़ितों को फर्जी वेबसाइटों के लिंक के साथ ई मेल भी भेजे जाते हैं जो उनके बैंक की वेबसाइट के मुख पृष्ठ से मिलता जुलता है। फिशिंग को एक अधिक लक्षित रूप में स्पीयर फिशिंग कहा जाता है यह एक विश्वनीय स्रोत से या सोशल मीडिया संदेशों के रूप में उपयोगकर्ताओं के पास आता है तथा उन्हें बेवकूफ बनाता है। फ़िशिंग को दो तरीकों से वर्गीकृत किया जा सकता है, जिसे ईविल ट्विन्स और फ़ार्मिंग के रूप में जाना जाता है जिन्हें पहचानना और भी मुश्किल है।

  i) **ईविल ट्विन्स:** ये हवाई अड्डों या शॉपिंग माल में आने वाले वायरलेस नेटवर्क हैं जो इंटरनेट को भरोसेमंद वाई-फाई कनेक्शन देने का नाटक करते हैं। ये नकली नेटवर्क एक प्रामाणिक सार्वजनिक नेटवर्क के समान दिखते है। नेटवर्क पर लॉग ऑन करते ही साइबर अपराधियों द्वारा निर्दोष उपयोगकर्ताओं के पासवर्ड या क्रेडिट कार्ड नंबर पर कब्जा कर लिया जाता है।

  ii) **फार्मिंग:** फार्मिंग वेबसाइट के सही यू आर एल को टाइप करने के बाद भी, उपयोगकर्ताओं को एक फर्जी वेब पेज पर पुनर्निर्देशित करता है। इसे "द फिशिंग विदाउट ए लॉअर" भी कहा जाता है। फ़िशिंग का साइबर अपराध सूचना प्रौद्योगिकी अधिनियम, 2000 के कई दंडात्मक प्रावधानों को उल्लेखित करता है।

- **पे-पर-क्लिक फ्रॉड:** किसी सर्च इंजन द्वारा प्रदर्शित सभी प्रकार के प्रायोजित खोज परिणामों के लिए, विज्ञापनदाता प्रत्येक प्राप्त उत्पादों के लिए संभावित खरीदारों के परिणामस्वरूप प्राप्त होने वाले प्रत्येक क्लिक के लिए शुल्क का भुगतान करता है। क्लिक धोखाधड़ी तब होती है जब कोई व्यक्ति या कंप्यूटर प्रोग्राम धोखे से ऑनलाइन विज्ञापन पर क्लिक करता है । गूगल और अन्य वेब साइटों पर क्लिक धोखाधड़ी एक गंभीर समस्या बन गई है, जिसमें पे-पर-क्लिक ऑनलाइन विज्ञापन की सुविधा है। कंपनियों के बीच प्रतिस्पर्धा के कारण, कुछ कंपनियां विपणन व्यय द्वारा अपने प्रदर्शन को तेज करने

के लिए प्रतियोगी से विज्ञापन पर क्लिक करने के लिए तीसरे पक्ष को नियुक्त करती हैं। यह धोखाधड़ी सॉफ्टवेयर प्रोग्राम पर क्लिक करने के साथ भी की जा सकती है, जिसके लिए आमतौर पर बॉटनेट का उपयोग किया जाता है। गूगल जैसे खोज इंजन इस धोखाधड़ी को ट्रैक करने का प्रयास कर रहे हैं, लेकिन अपने प्रयासों को प्रचारित करने में अनिच्छुक हैं।

11.4.7 वैश्विक खतरे: साइबर आतंकवाद और साइबर युद्ध

अब तक चर्चा में रहे सभी साइबर अपराध सीमा रहित हैं क्योंकि इनका यात्रा का माध्यम इंटरनेट है। साइबर अपराध हर देश में हर जगह यात्रा कर सकते है और दुनिया में कहीं भी नुकसान पहुंचा सकते है। चीन, संयुक्त राज्य अमेरिका, दक्षिण कोरिया, रूस और ताइवान वर्तमान में दुनिया के अधिकांश मैलवेयर के स्रोत हैं वास्तव में, जो देश अपने प्रतिद्वंद्वियों की अर्थव्यवस्था को नुकसान पहुंचाने की कोशिश करते है, वे, ऐसी साइबर गतिविधियों का उपयोग करके उनकी जासूसी करते हैं। "साइबर युद्ध" एक राज्य-प्रायोजित गतिविधि है जिसका उद्देश्य अपने कंप्यूटर या नेटवर्क पर घुसपैठ के माध्यम से किसी राज्य या राष्ट्र को नुकसान पहुंचाने, भड़काने और नुकसान पहुंचाना है।

सामान्यतया, साइबर युद्ध के हमले अधिक सामान्य, परिष्कृत और संभावित विनाशकारी होते जा रहे हैं। वर्षों के दौरान, हैकर्स ने मिसाइल ट्रैकिंग सिस्टम, उपग्रह नेविगेशन उपकरण, रक्षा ड्रोन और उन्नत जेट लड़ाकू विमानों की योजनाएं लूट ली हैं। चूंकि उनके प्रमुख वित्तीय, स्वास्थ्य, सरकार और औद्योगिक संस्थान अपने दिन-प्रतिदिन के संचालन के लिए इंटरनेट पर निर्भर हैं, साइबर युद्ध आधुनिक समाज के बुनियादी ढांचे के लिए एक गंभीर खतरा है। इसमें ऐसे हमलों के खिलाफ साइबर युद्ध का बचाव करना भी शामिल है।

11.5 साइबर फोरेंसिक

साइबर फोरेंसिक कंप्यूटर और डिजिटल स्टोरेज मीडिया में डिजिटल साइंस की एक शाखा है जिसमें तथ्य हैं। कानूनी कार्रवाई का जवाब देने के लिए, डाटा सुरक्षा और नियंत्रण प्रबंधन अत्यंत आवश्यक हो गया है। आज, इन्वेंट्री फ्रॉड, हेराफेरी, व्यापार गुप्त डाटा की चोरी, साइबर अपराध और कई सिविल मामलों के लिए बहुत सारे साक्ष्य डिजिटल रूप में उपलब्ध हैं। मुद्रित और टाइप-लिखित पृष्ठों के तथ्यों के अलावा, कानूनी मामले आज मोबाइल स्टोरेज डिवाइस, सी डी और हार्ड डिस्क मशीनों और इंटरनेट ईमेल, त्वरित संदेशों और ई-कॉमर्स पर संग्रहीत डिजिटल डाटा के रूप में चित्रित साक्ष्य पर निर्भर करते हैं। आजकल इलेक्ट्रॉनिक प्रूफ का सबसे लोकप्रिय रूप ई-मेल है।

कानूनी कार्रवाई में, एक फर्म को सबूत के रूप में उपयोग की जा सकने वाली जानकारी तक पहुंच के लिए एक खोज अनुरोध का जवाब देना पड़ता है, और कंपनी को आवश्यक डाटा का उत्पादन करने के लिए कानून की आवश्यकता होती है। यदि कम्पनी को अनावश्यक डाटा प्रदर्शित करने में परेशानी होती है, या डाटा दूषित या नष्ट हो गया है, तो खोज अनुरोध का जवाब देने कि कम्पनी के लिए लागत बहुत बड़ी हो सकती है। न्यायालय अब इलेक्ट्रॉनिक दस्तावेजों के अनुचित विनाश के लिए गंभीर वित्तीय और यहां तक कि आपराधिक दंड भी लगाते हैं।

इलेक्ट्रॉनिक प्रलेखन के संरक्षण के लिए एक विशेष नीति यह सुनिश्चित करती है कि फाइलें, ई-मेल और अन्य रिकॉर्ड अच्छी तरह से, सुलभ और न ही बहुत लंबे समय तक व्यवस्थित रहें और न ही बहुत जल्द रखे जाएं। यह इस बात की समझ का भी प्रतिनिधित्व करता है कि डिजिटल फोरेंसिक को कैसे बनाए रखा जा सकता है। कंप्यूटर फोरेंसिक में, वैज्ञानिक डाटा प्रोसेसिंग, अध्ययन, प्रमाणीकरण, संरक्षण और विश्लेषण का उपयोग इस तरह से किया जाता है कि जानकारी का उपयोग कानून की अदालत में सबूत के रूप में किया जा सकें, जिसे कंप्यूटर स्टोरेज मीडिया से संरक्षित या पुनर्प्राप्त किया जा सकता है। जैसे कि:

- सबूत की विश्वसनीयता सुनिश्चित करते हुए कंप्यूटर डाटा पुनर्प्राप्त करना
- सुरक्षित इलेक्ट्रॉनिक डाटा भंडारण और हैंडलिंग
- आवश्यक विवरणों के लिए इलेक्ट्रॉनिक डाटा की विशाल मात्रा का पता लगाना
- कानून की एक अदालत में विवरण प्रस्तुत करना

इलेक्ट्रॉनिक सबूत जो एक नियमित व्यक्ति के लिए स्पष्ट नहीं होते, कंप्यूटर स्टोरेज मीडिया पर डाटा के रूप में पाए जा सकते है। इसका एक उदाहरण एक फ़ाइल है जिसे पीसी हार्ड ड्राइव पर हटा दिया गया है। विभिन्न तकनीकों द्वारा कंप्यूटर स्टोरेज मीडिया पर एक उपयोगकर्ता द्वारा डाटा हटाया जा सकता है। सॉफ्टवेयर फोरेंसिक विशेषज्ञ दिखाने के लिए गोपनीय डाटा को पुनः प्राप्त करने का प्रयास करते हैं। सॉफ्टवेयर फोरेंसिक जागरूकता को किसी भी व्यवसाय की आकस्मिक योजना चरण में एकीकृत किया जाना चाहिए। सी आई ओ, सुरक्षा पेशेवरों, सूचना प्रौद्योगिकी कर्मियों और कॉर्पोरेट सलाहकार को एक रणनीति को लागू करने के लिए मिलकर काम करना चाहिए, यदि कानूनी आवश्यकताएं होती हैं, तो इसे लागू किया जा सकता है।

बोध प्रश्न क:

1) स्पूफिंग और स्निफिंग के बीच अंतर बताइए।

……

……

……

……

……

2) साइबर आतंकवाद के विभिन्न वैश्विक खतरे क्या हैं?

……

……

……

……

……

3) पे-पर-क्लिक धोखाधड़ी कैसे होती है?

.....

.....

.....

.....

.....

4) कंप्यूटर अपराधों को हैकर्स कैसे अंजाम देते हैं?

.....

.....

.....

.....

.....

11.6 इंटरनेट पर कारोबार की सुरक्षा

नई प्रौद्योगिकियों की निरंतर धारा के साथ, कंपनियां अपने प्रतिद्वंद्वियों से एक कदम आगे रखने के लिए तेजी से अपने आई टी वातावरण को बदल रही हैं। हालांकि, ई-व्यावसायिक अनुप्रयोगों को लागू करना एक सुसंगत, ई-व्यावसायिक सुरक्षा दृष्टिकोण के बिना असंभव हो सकता है। बाहरी और आंतरिक घुसपैठियों से सूचना परिसंपत्तियों की रक्षा करने में विफलता से सार्वजनिक जोखिम, ग्राहकों के विश्वास की हानि और वित्तीय नुकसान हो सकता है। खुद की सुरक्षा के लिए कंपनी का निर्णय केवल एक प्रौद्योगिकी निर्णय नहीं है, यह एक व्यावसायिक निर्णय है।

कॉरपोरेट परिसंपत्तियों की सुरक्षा सुनिश्चित करना एक निरंतर और गतिशील प्रक्रिया है । समाधान का खुलापन और विस्तारशीलता एक वैश्विक संचार कंपनी को मौजूदा प्रौद्योगिकियों का लाभ उठाने और अपने ई-व्यवसायों के रूप में नए को अपनाने के लिए लचीलापन देती है।

- **सूचना संसाधनों की सुरक्षा के लिए प्रौद्योगिकी और उपकरण:** कंपनियों के पास विभिन्न प्रकार के सूचना संसाधन सुरक्षा प्रौद्योगिकियां हैं। इनमें उपयोगकर्ता पहचान को प्रबंधित करने, सिस्टम और डाटा तक अनधिकृत पहुंच को रोकने, उपलब्ध रूपरेखा सुनिश्चित करने और सॉफ्टवेयर की गुणवत्ता की गारंटी देने इत्यादि के लिए उपकरण शामिल हैं।

- **पहचान प्रबंधन और प्रमाणीकरण:** मध्यम आकार और बड़े व्यवसायों में कई अलग-अलग आई टी अवसंरचनाएं और प्रक्रियाएं हैं, जिनमें प्रत्येक में उपयोगकर्ता समुदाय होते हैं। पहचान सॉफ्टवेयर इन सभी उपयोगकर्ताओं के उपकरण अधिकारों की निगरानी की

प्रक्रिया को स्वचालित करता है तथा, प्रत्येक उपयोगकर्ता को सिस्टम तक पहुंचने के लिए एक अद्वितीय डिजिटल पहचान प्रदान करता है। यह उपयोगकर्ता प्रमाणीकरण, उपयोगकर्ता पहचान सुरक्षा और उपकरण अभिगम नियंत्रण के लिए भी उपकरण प्रदान करता है।

किसी सिस्टम तक पहुँचने के लिए, उपयोगकर्ता का प्रमाणिकरण होना चाहिए । प्रमाणीकरण का मतलब यह जानने की क्षमता है कि एक व्यक्ति है जो केवल अधिकृत उपयोगकर्ता को ज्ञात उपयोगकर्ता नाम और पासवर्ड का उपयोग करके स्थापित किया गया है, वह एक्सेस कर रहा है । लेकिन उपयोगकर्ता पासवर्ड की भी खामिया होती है, प्राय उन्हें साझा किया जाता है और कमजोर पासवर्ड चुना जाता है। अत्यधिक कठिन लॉगिन योजनाएं कर्मचारी दक्षता में बाधा डालती हैं। उपयोगकर्ता आमतौर पर आसान पासवर्ड पसंद करते हैं जो जटिल पासवर्ड को स्थानांतरित करने में सक्षम बनाते हैं, और कुछ उपयोगकर्ता आसानी से उपलब्ध कार्यस्थानों के पास अपने पासवर्ड भी लिखते या पकड़ते हैं। नेटवर्क पर भेजे गए सोशल इंजीनियरिंग तरीकें पासवर्ड भी लूट सकते हैं।

इनमें से कोई भी समस्या आधुनिक प्रमाणीकरण विधियों जैसे कि की, इंटेलिजेंट कार्ड और बायोमेट्रिक प्रमाणीकरण द्वारा हल की जाती है। एक टोकन एक भौतिक उपकरण है, जो एक उपयोगकर्ता की पहचान को साबित करने के लिए बनाए किए गए आई डी कार्ड के समान होता है। टोकन छोटे उपकरण हैं जो आम तौर पर की के छल्ले पर फिट होते हैं और अक्सर पास कोड बदलते हैं।

11.7 सुरक्षित नेटवर्क लेनदेन

नेटवर्क लेनदेन को सुरक्षित करने के विभिन्न तरीकों की चर्चा नीचे दी गई है:

- **वायरलेस नेटवर्क को सुरक्षित करना:** वाई-फाई के लिए विकसित प्रारंभिक सुरक्षा मानक, वायर्ड इक्विवेलेंट प्राइवेसी (WEP) बहुत सफल नहीं है, क्योंकि एन्क्रिप्शन की को क्रैक करना आसान है। हालांकि, यदि उपयोगकर्ता इसे अनुमति देना याद करते हैं, तो WEP सुरक्षा के कुछ मार्जिन प्रदान करता है। आंतरिक कॉर्पोरेट डाटा तक पहुंच में वर्चुअल प्राइवेट नेटवर्क (वीपीएन) तकनीक का उपयोग वाई-फाई सुरक्षा को और बढ़ाएगा। यह केंद्रीय प्रमाणीकरण सर्वर के साथ एक एन्क्रिप्टेड प्रमाणीकरण योजना भी संचालित करता है ताकि यह सुनिश्चित हो सके कि नेटवर्क केवल स्वीकृत उपयोगकर्ताओं के साथ ही एक्सेस हो।

- **एन्क्रिप्शन और सार्वजनिक की बुनियादी ढांचा:** इंटरनेट पर संगठनों द्वारा संग्रहीत या साझा की गई डिजिटल जानकारी की सुरक्षा के लिए एन्क्रिप्शन सबसे आम तरीकों में से एक है। यह सादे पाठ या डाटा को एन्क्रिप्टेड डाटा में बदलने की प्रक्रिया है, जिसे सिफर टेक्स्ट कहा जाता है ताकि कोई अनधिकृत व्यक्ति इसे न पढ़ सके। इसे केवल प्राप्तकर्ता और प्रेषक द्वारा पढ़ा जा सकता है। एक गुप्त संख्यात्मक कोड, जिसे एन्क्रिप्शन की कहा जाता है, का उपयोग सादे डाटा को सिफर टेक्स्ट में बदलने के लिए किया जाता है। प्राप्तकर्ता द्वारा संदेश डिक्रिप्ट किया जाना चाहिए। प्राप्तकर्ता को दूसरी की या उसी की

का उपयोग करके डाटा को डिक्रिप्ट किया जाना चाहिए। वेब पर नेटवर्क ट्रैफ़िक को एन्क्रिप्ट करने के विभिन्न तरीकों पर चर्चा नीचे की गई:

- **सिक्योर सॉकेट्स लेयर (एस एस एल):** एस एस एल एक प्रोटोकॉल है जो इंटरनेट पर आने वाले डाटा को एन्क्रिप्ट करने के लिए उपयोग किया जाता है। ट्रांसपोर्ट लेयर सिक्योरिटी (टी एल एस) के साथ-साथ टी एल एस क्लाइंट और सर्वर कंप्यूटरों को एन्क्रिप्शन और डिक्रिप्शन गतिविधियों को प्रबंधित करने में सक्षम बनाते हैं क्योंकि वे सुरक्षित सत्र के दौरान एक-दूसरे के साथ संवाद करते हैं। एस एस एल और टी एल एस को दो कंप्यूटरों के बीच एक सुरक्षित कनेक्शन स्थापित करने के लिए डिज़ाइन किया गया है।

- **सिक्योर हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल (एस-एच टी टी पी):** यह इंटरनेट पर आने वाले डाटा को एन्क्रिप्ट करने के लिए इस्तेमाल किया जाने वाला एक अन्य प्रोटोकॉल है, लेकिन यह व्यक्तिगत संदेशों तक सीमित है। इंटरनेट क्लाइंट ब्राउज़र सॉफ़्टवेयर और सर्वर सुरक्षित सत्र उत्पन्न करते हैं। क्लाइंट और सर्वर चर्चा करते हैं कि किस की और किस स्तर की सुरक्षा का उपयोग करना आवश्यक है। क्लाइंट और सर्वर के बीच सुरक्षित सत्र स्थापित हो जाने के बाद, उस सत्र के सभी संदेश एन्क्रिप्ट किए जाते हैं।

- **की एन्क्रिप्शन:** सममित की एन्क्रिप्शन में, प्रेषक और प्राप्तकर्ता एक एकल एन्क्रिप्शन की बनाकर और इसे प्राप्तकर्ता को भेजकर एक सुरक्षित इंटरनेट सत्र बनाते हैं, परिणामस्वरूप, प्रेषक और प्राप्तकर्ता दोनों एक ही की साझा करते हैं। एन्क्रिप्शन की की ताकत इसकी बिट लंबाई द्वारा मापी जाती है। आज, एक विशिष्ट की 128 बिट लंबी (128 बाइनरी अंकों की एक स्ट्रिंग) होगी। सममित एन्क्रिप्शन की के साथ एक खामी है कि की को स्वयं प्रेषकों और प्राप्तकर्ता के बीच साझा किया जाना चाहिए, जो बाहरी लोगों की की को उजागर करता है, जो सिर्फ होना चाहिए की को पकड़ने और डिक्रिप्ट करने में सक्षम होना चाहिए।

- **सार्वजनिक की एन्क्रिप्शन:** यह एन्क्रिप्शन का अधिक सुरक्षित रूप है जो दो की का उपयोग करता है-

  - **सार्वजानिक:** ये प्रेषक के स्वामित्व में होती है, तथा संदेशों को एन्क्रिप्ट करती है।

  - **निजी:** यह प्राप्तकर्ता के स्वामित्व में होती है, तथा संदेशों को डिक्रिप्ट करती है।

संदेश भेजने और प्राप्त करने के लिए, संचारक पहले निजी और सार्वजनिक की के अलग-अलग जोड़े बनाते हैं। सार्वजनिक की को एक निर्देशिका में रखा जाता है और निजी की को गुप्त रखा जाता है । प्रेषक प्राप्तकर्ता की सार्वजनिक की के साथ एक संदेश भेजता है। संदेश प्राप्त करने पर, प्राप्तकर्ता इसे डिक्रिप्ट करने के लिए अपनी निजी की का उपयोग करता है।

- **डिजिटल प्रमाणपत्र:** ये ऑनलाइन लेनदेन उपयोगकर्ताओं और इलेक्ट्रॉनिक गुणों की पहचान के लिए डाटा फाइलें हैं। प्रमाणपत्रों की एक डिजिटल प्रणाली किसी उपयोगकर्ता

की पहचान को सत्यापित करने के लिए प्रमाणपत्र प्राधिकरण नामक एक भरोसेमंद तृतीय पक्ष का उपयोग करती है। सिमेंटेक, गो-डैडी और कोमोडो सहित कई प्रमाणपत्र प्राधिकरण, संयुक्त राज्य अमेरिका और दुनिया भर में उपलब्ध हैं। जब प्रमाणीकरण अधिकार ऑफ़लाइन उपयोगकर्ता के डिजिटल प्रमाण पत्र की पुष्टि करता है, तो एक डिजिटल एन्क्रिप्टेड प्रमाण पत्र जिसमें मालिक की पहचान की जानकारी होती है और मालिक की सार्वजनिक की की एक प्रति प्रमाणपत्र प्राधिकरण सर्वर से उत्पन्न होती है।

प्रमाण पत्र सुनिश्चित करता है कि नियुक्त मालिक के पास सार्वजनिक की है। प्रमाणपत्र प्राधिकरण प्रिंट में वेब पर अपनी सार्वजनिक की प्रदान करता है। एक एन्क्रिप्टेड संदेश का प्राप्तकर्ता संदेश से जुड़े डिजिटल प्रमाण पत्र को समझने और मान्य करने के लिए प्रमाणपत्र प्राधिकरण की सार्वजनिक की का उपयोग करता है और फिर प्रमाण पत्र में मिली सार्वजनिक की जानकारी और पहचान विवरण प्राप्त करता है। प्राप्तकर्ता इस जानकारी का उपयोग करके एक एन्क्रिप्टेड प्रतिक्रिया प्रस्तुत कर सकता है। एक क्रेडिट कार्ड उपभोक्ता और एक व्यापारी एक स्वीकृत और विश्वसनीय व्यक्ति से डाटा का आदान-प्रदान करने से पहले डिजिटल हस्ताक्षर का उपयोग करके अपने डिजिटल प्रमाणपत्रों का सत्यापन कर सकते हैं। इलेक्ट्रॉनिक कॉमर्स में, सार्वजनिक की अवसंरचना का उपयोग आमतौर पर सार्वजनिक की क्रिप्टोग्राफी के उपयोग में किया जाता है जो कि प्रमाणपत्र प्राधिकरण के साथ संचालित होता है।

- **ब्लॉकचेन के साथ लेनदेन को सुरक्षित करना:** यह लेनदेन को सुरक्षित करने और कई दलों के बीच विश्वास स्थापित करने के लिए एक वैकल्पिक तरीका है। एक ब्लॉकचेन कई ब्लॉकों की एक श्रृंखला है जिसमें लेनदेन के रिकॉर्ड होते हैं। प्रत्येक ब्लॉक इससे पहले और बाद में सभी ब्लॉकों से जुड़ा हुआ है और ब्लॉक चेन को लगातार अपडेट किया जाता है और एक तादत्म्यता में रखा जाता है। इससे एकल रिकॉर्ड के साथ छेड़छाड़ करना मुश्किल हो जाता है क्योंकि किसी व्यक्ति को उस रिकॉर्ड के साथ ब्लॉक को बदलना होगा और साथ ही इससे जुड़े लोगों का पता लगाने से बचना होगा।

  एक बार दर्ज होने के बाद, ब्लॉकचेन लेनदेन को बदला नहीं जा सकता है। ब्लॉकचेन में सभी रिकॉर्ड क्रिप्टोग्राफी के माध्यम से सुरक्षित होते हैं और सभी लेनदेन एन्क्रिप्टेड हैं। ब्लॉकचेन नेटवर्क प्रतिभागियों की अपनी निजी की होती हैं, जो उनके द्वारा बनाए गए लेनदेन को सौंपी जाती हैं और व्यक्तिगत डिजिटल हस्ताक्षर के रूप में कार्य करती हैं। यदि कोई रिकॉर्ड बदल दिया जाता है, तो हस्ताक्षर अमान्य हो जाता है और ब्लॉकचेन नेटवर्क को तुरंत पता चल जाएगा कि कुछ अनुचित है। क्योंकि ब्लॉकचैन को एक केंद्रीय स्थान पर नहीं रखा जाता है, इसलिए उनके पास विफलता का एक भी बिट्टू नहीं है और न ही उन्हें एक कंप्यूटर से बदला जा सकता है। ब्लॉकचेन उच्च सुरक्षा आवश्यकताओं और पारस्परिक रूप से अज्ञात अभिनेताओं के साथ वातावरण के लिए उपयुक्त है।

- **दोष-सहिष्णु कंप्यूटर सिस्टम:** दोष-सहिष्णु कंप्यूटर सिस्टम में अनावश्यक हार्डवेयर, सॉफ्टवेयर और बिजली आपूर्ति घटक होते हैं जो एक ऐसा वातावरण बनाते हैं जो निरंतर, निर्बाध सेवा प्रदान करता है। दोष-सहिष्णु कंप्यूटर हार्डवेयर विफलता का पता लगाने और स्वचालित रूप से एक बैकअप डिवाइस पर स्विच करने के लिए अपने सर्किट्री में निर्मित विशेष सॉफ्टवेयर दिनचर्या या स्वयं-जाँच तर्क का उपयोग करते हैं। ये विशेष प्रणालियाँ है,

जिनसे इन कम्प्यूटरों से अलग अलग हिस्सों को हटाया जा सकता है और कम्प्यूटरों सिस्टम की बिना किसी गड़बड़ी के मरम्मत की जा सकती है।

- **उच्च उपलब्धता कंप्यूटिंग वातावरण:** उच्च उपलब्धता कंप्यूटिंग वातावरण आमतौर पर ई-कॉमर्स अनुप्रयोगों के लिए उपयोग किया जाता है जिसमें भारी ई-कॉमर्स प्रसंस्करण के लिए बहुत कम आवश्यकता होती है जहां संगठन अपने आंतरिक संचालन के लिए डिजिटल नेटवर्क पर निर्भर करते हैं। उच्च उपलब्धता प्रणाली के अच्छे निष्पादन के लिए बैकअप सर्वर कई सर्वरों में प्रसंस्करण का वितरण, उच्च क्षमता भण्डारण और अच्छी आपदा वसूली और व्यापार निंरतरता योजनाओं की आवश्यकता है। इसके अलावा, इसे ठीक से काम करने के लिए स्केलेबल प्रोसेसिंग पावर, स्टोरेज और बैंडविड्थ के साथ बेहद मजबूत कंप्यूटिंग प्लेटफॉर्म की आवश्यकता होती है। दोनों दोष सहिष्णुता और उच्च उपलब्धता कंप्यूटिंग का उपयोग डाउनटाइम को कम करने के लिए किया जाता है। डाउनटाइम उस समय की अवधि है जिसमें एक सिस्टम प्रदर्शन करने में सक्षम नहीं है। तुलनात्मक रूप से, उच्च उपलब्धता कंप्यूटिंग कंपनियों को फॉल्ट टॉलरेंस सिस्टम की तुलना में सिस्टम क्रैश से जल्दी ठीक होने में मदद करता है।

- **डीप पैकेट निरीक्षण (डी पी आई):** कभी-कभी देखा जा सकता है कि परिसर में विश्वविद्यालय का नेटवर्क बहुत सुस्त होता है। ऐसा तब हो सकता है जब कोई भी संगीत डाउनलोड करने या यु ट्यूब (YouTube) देखने के लिए नेटवर्क का उपयोग करता है, क्योकि ऐसे करने से एप्लिकेशन की बैंडविड्थ का भारी उपयोग होता है जिससे कैंपस नेटवर्क धीमा हो जाता है। डीप पैकेट निरीक्षण (डी पी आई) तकनीक ने इस समस्या को हल कर दिया। डी पी आई डाटा फ़ाइलों की जाँच करता है और व्यावसायिक-महत्वपूर्ण फ़ाइलों को उच्च प्राथमिकता प्रदान करते हुए निम्न-प्राथमिकता वाली ऑनलाइन सामग्री को सॉर्ट करता है। नेटवर्क संचालकों द्वारा स्थापित प्राथमिकताओं के आधार पर, यह तय करता है कि एक विशिष्ट डाटा पैकेट अपने गंतव्य तक जारी रह सकता है या अधिक महत्वपूर्ण ट्रैफ़िक कार्यवाही के दौरान अवरुद्ध या विलंबित होना चाहिए।

- **सुरक्षा आउटसोर्सिंग:** कई ऐसे संगठन हैं जो अपने कार्यबल को एक सुरक्षित उच्च उपलब्धता कंप्यूटिंग वातावरण प्रदान करने के लिए सुरक्षा उपायों और संसाधनों को हासिल करने में असमर्थ हैं। आम तौर पर, यह मध्य-स्तर या छोटे स्तर के उद्योगों के साथ होता है। ऐसी संस्थाएँ नेटवर्क गतिविधियों की निगरानी और भेद्यता परीक्षण और घुसपैठ का पता लगाने के लिए प्रबंधित सुरक्षा सेवा प्रदाताओं (MSSP) से अपनी सुरक्षा सेवाओं का प्रबंधन करने के लिए कई सुरक्षा कार्यों को आउटसोर्स कर सकती हैं। सिक्योर वर्क्स बी टी प्रतिबंधित सुरक्षा समाधान समूह, आई बी एम, वेरिजोंन, एंटी एन्ड टी और सिमेंटेक एम एस एस पी सेवाओं के प्रमुख प्रदाता है।

- **क्लाउड कंप्यूटिंग और मोबाइल डिजिटल प्लेटफ़ॉर्म के लिए सुरक्षा मुद्दे:** क्लाउड कंप्यूटिंग और मोबाइल डिजिटल प्लेटफ़ॉर्म डाटा संग्रह, विश्लेषण और फिर भविष्यवाणियों की रीढ़ बन गए हैं। ये प्रौद्योगिकियां शक्तिशाली लाभ पहुंचाने की क्षमता रखती हैं। लेकिन साथ ही, इन प्रौद्योगिकियों ने सिस्टम सुरक्षा और विश्वसनीयता के लिए कुछ चुनौतियां दी हैं। अब हम इनमें से कुछ चुनौतियों का वर्णन नीचे किया गया है।

1) **क्लाउड में सुरक्षा:** वेब-आधारित फर्में जो बहुत परिष्कृत हैं और क्लाउड सेवा का उपयोग करती हैं, सुरक्षा गड़बड़ी का अनुभव कर सकती हैं। संवेदनशील डाटा की सुक्षा के लिए जवाबदेही और जिम्मेदारी स्वामित्व संगठन की है। यह समझना थोड़ा जटिल है कि क्लाउड कंप्यूटिंग प्रदाता अपनी सेवाओं को व्यवस्थित और डाटा का प्रबंधन कैसे करता है।

क्लाउड कंप्यूटिंग सेवाओं को वितरित किया जा सकता है। क्लाउड सिस्टम बड़े दूरस्थ डाटा केंद्रों और सर्वर फ़ार्म में रहते हैं जो उद्यम और डाटा प्रबंधन के साथ मल्टी-कंपनी क्लाइंट प्रदान करते हैं। क्लाउड प्रदाता संसाधनों को बचाने और लागत को कम रखने के लिए दुनिया भर के डाटा केंद्रों को काम भी सौंपते हैं। क्लाउड का उपयोग करते समय, यह कोई नहीं जानता कि डाटा कहां स्थित होता है।

हालांकि, नकारात्मक पक्ष यह है कि क्लाउड कंप्यूटिंग के वितरित अस्तित्व के कारण अवैध गतिविधि पर नजर रखना मुश्किल है। लगभग सभी क्लाउड प्रदाता डाटा को सुरक्षित रखने के लिए एन्क्रिप्शन का उपयोग करते हैं, जो डाटा को प्रसारित करते समय नियंत्रित करते हैं। उदाहरण के लिए, सिक्योर सॉकेट्स लेयर (एस एस एल) के साथ। यदि डाटा उन उपकरणों द्वारा संग्रहित किया जाता है, जो अन्य कंपनियों का भी डाटा संग्रहित करते है, तो ये सुनिश्चित करना महतवपूर्ण है कि डाटा एन्क्रिप्ट किया जाए।

कंपनियां उम्मीद करती है कि उनके सिस्टम दिन-रात लगातार चलें, लेकिन क्लाउड प्रदाता हमेशा इस तरह की सेवा प्रदान करने में सक्षम नहीं होते हैं। पिछले कुछ वर्षों में, Amazon.com और Salesforce.com की क्लाउड सेवाओं ने ऐसे अनुभव किए हैं जो लाखों उपयोगकर्ताओं के लिए व्यावसायिक कार्यों को बाधित करते हैं।

भले ही डाटा कही भी सहेजा गया हो, क्लाउड उपयोगकर्ताओं को यह सुनिश्चित करना चाहिए कि वे उस स्तर पर सुरक्षित हैं जो उनकी व्यावसायिक आवश्यकताओं को पूरा करें, क्लाउड प्रदाता कुछ न्यायालयों में कुछ विशेष न्यायालयों के डाटा सुरक्षा कानूनों के तहत डाटा दर्ज और संसाधित कर सकता है। क्लाउड ग्राहकों को यह पता लगाना चाहिए कि क्लाउड प्रदाता द्वारा उनकी कंपनी के डाटा को अन्य कंपनियों से कैसे अलग किया जाता है और एक ध्वनि एन्क्रिप्शन प्रक्रिया का प्रमाण प्राप्त होना चाहिए। यह जानना भी महत्वपूर्ण है कि आपदा की स्थिति में क्लाउड प्रदाता कैसे प्रतिक्रिया देगा, क्या प्रदाता आपके डाटा को पूरी तरह से पुनर्प्राप्त करेगा और कब तक। क्लाउड में उपयोगकर्ताओं को यह भी पूछताछ करनी चाहिए कि क्या क्लाउड सेवाएँ बाहरी ऑडिट और सुरक्षा अनुमोदन के अधीन होंगी। क्लाउड प्रदाता के हस्ताक्षर करने से पहले इस तरह की समीक्षाओं को एस एल ए समझौते में लिखा जा सकता है।

2) **मोबाइल प्लेटफ़ॉर्म सुरक्षित करना:** यदि मोबाइल डिवाइस कंप्यूटर के कई कार्य करते हैं, तो उन्हें मालवेयर, चोरी, आकस्मिक हानि, अनधिकृत प्रवेश और हैकिंग, जैसे डेस्कटॉप और लैपटॉप से सुरक्षित रखने कि आवश्यकत है। मोबाइल उपकरणों के लिए विशेष सुरक्षा की आवश्यकता होती है जो कंपनी सिस्टम और डाटा तक पहुंचते हैं। कंपनियों को यह सुनिश्चित करना चाहिए कि उनकी कॉर्पोरेट सुरक्षा रणनीति में मोबाइल डिवाइस और मोबाइल उपकरणों का समर्थन, सुरक्षित और उपयोग करने की बारीकियों को शामिल किया जाए। मोबाइल प्रबंधन उपकरण उपयोग में आने वाले सभी उपकरणो

को स्वीकृत करने के लिए आवश्यक है। ये सभी मोबाइल उपकरण।, उपयोगकर्ताओं और ऐप्स पर सही इवेंटरी डाटा रखते है और उन्हें अपडेट करते रहते है। साथ ही ये खोये या चोरी हुए उपकरणो का लॉक हटाने में सक्षम है, जिससे उनका दुरूपयोग नहीं हो पाता। लाइसेंस प्राप्त मोबाइल प्लेटफॉर्म और सॉफ्टवेयर एप्लिकेशन के साथ-साथ आवश्यक सॉफ्टवेयर और कंपनी सिस्टम की रिमोट एक्सेस प्रक्रियाओं के लिए कॉर्पोरेट दिशानिर्देश व्यवसायों द्वारा स्थापित किए जाने चाहिए।

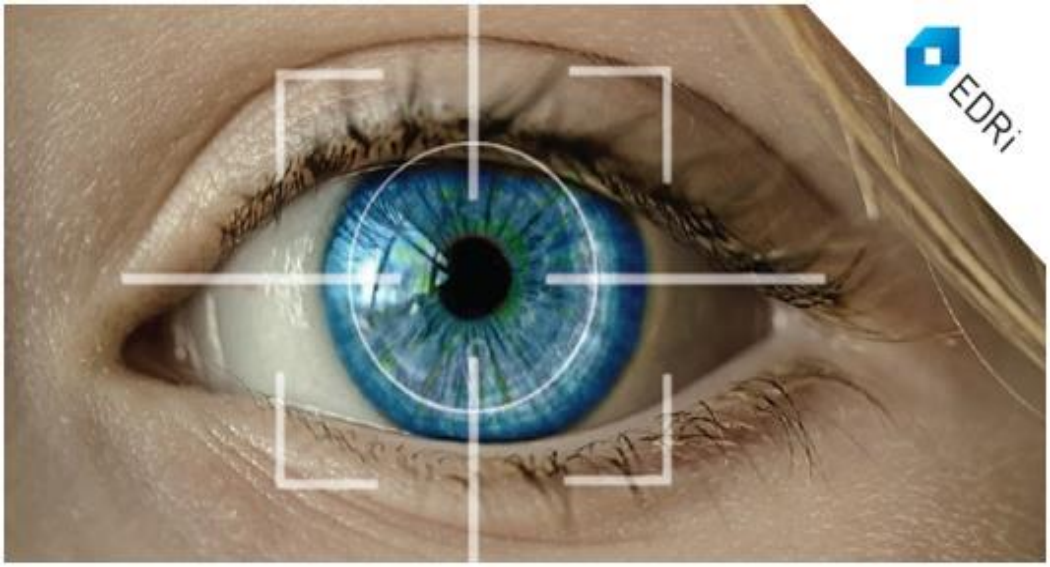
कंपनियां, जहां भी आवश्यक हो, संपर्क को एन्क्रिप्ट कर सकती हैं। प्रत्येक स्मार्टफ़ोन पर पाया जाने वाला पासवर्ड फीचर सभी मोबाइल डिवाइस उपयोगकर्ताओं के लिए आवश्यक होना चाहिए। कुछ व्यवसायों की मांग है कि कर्मचारी केवल कंपनी से स्मार्टफोन का उपयोग करते हैं। चूंकि ब्लैकबेरी डिवाइस अपने स्वयं के सुरक्षित सिस्टम पर चलते हैं, इसलिए उन्हें सबसे सुरक्षित माना जाता है। लेकिन अधिक से अधिक व्यवसाय अपने स्वयं के उपकरणों पर कर्मचारियों को अधिक सुलभ और कुशल बनाने के लिए कर्मचारियों को सशक्त बना रहे हैं, जिनमें आईफ़ोन और एंड्रॉइड फोन शामिल हैं। अपनी निजी जानकारी से निजी मोबाइल उपकरणों में संग्रहीत कॉर्पोरेट डाटा के अलगाव के लिए, गुड टेक्नोलॉजी टूल्स जैसे सॉफ़्टवेयर उत्पादों की सुरक्षा अब उपलब्ध है।

11.8 सुरक्षा उपाय और प्रवर्तन

सूचना सुरक्षा हर व्यवसाय और व्यक्ति के लिए सबसे महत्वपूर्ण क्षेत्रों में से एक है एवं जानकारी का ध्यान एवं संरक्षण रखना एक संगठन कि सबसे कीमती सम्पति है। बड़े पैमाने पर देखते हुए, लगभग 86% वेबसाइटों में एक गंभीर भेद्यता थी जो अतीत में और वर्तमान में भी एक अवलोकन ओमनी प्रस्तुत करती है।

11.8.1 बॉयोमीट्रिक सुरक्षा उपाय

प्रविष्टि देने या अस्वीकार करने के लिए, बायोमेट्रिक प्रमाणीकरण उन उपकरणों का उपयोग करता है जो व्यक्तिगत मानव लक्षणों, जैसे कि उंगलियों के निशान, रेटिना और आवाज़ को पढ़ते हैं और व्याख्या करते हैं। बॉयोमीट्रिक प्रमाणीकरण एक भौतिक या व्यवहार संबंधी विशेषता माप पर आधारित है, जो प्रत्येक व्यक्ति के लिए विशिष्ट है। यह एक व्यक्ति की अद्वितीय विशेषताओं की तुलना करता है, जैसे कि उंगलियों के निशान, चेहरे या रेटिना की छवियों की तुलना एक संग्रहीत प्रोफ़ाइल से, यह देखने के लिए करता है कि क्या उनके बीच कोई भिन्नता मौजूद है दो प्रोफाइलों के मेल खाने पर संग्रहित प्रोफाइल पहुंचा दी जाती है। फ़िंगर प्रिंटिंग और फेस रिकग्निशन टेक्नोलॉजी अभी हाल ही में फ़िंगरप्रिंट ऑथेंटिकेशन सिस्टम के साथ कई लैपटॉप में इस्तेमाल होने लगी हैं, साथ ही बिल्ट-इन वेबकैम और फेस रिकग्निशन ऐप के साथ और सिक्योरिटी एप्लिकेशन के लिए कई मॉडल हैं। मोहरा और फिडेलिटी जैसी वित्तीय सेवा फर्मों ने अपने ग्राहकों के लिए वॉयस ऑथेंटिकेशन सिस्टम लागू किया है।



*स्रोत: edri.org

चित्र 11.9: बायोमेट्रिक

11.8.2 गैर-बॉयोमीट्रिक सुरक्षा उपाय

मैलवेयर और घुसपैठियों से सुरक्षा के बिना इंटरनेट से जुड़ना बहुत जोखिम भरा होगा। आवश्यक व्यावसायिक उपकरण फ़ायरवॉल, घुसपैठ का पता लगाने वाले सिस्टम और एंटीवायरस सॉफ़्टवेयर हैं। इन्हें नीचे विस्तार से बताया गया है:

- **फ़ायरवॉल:** बिना लाइसेंस के उपयोगकर्ता फ़ायरवॉल के साथ निजी नेटवर्क तक नहीं पहुँच सकते। फ़ायरवॉल एक हार्डवेयर-से-सॉफ़्टवेयर संयोजन है जो ट्रैफ़िक इनपुट और आउटपुट को नियंत्रित करता है। यह आमतौर पर निजी आंतरिक नेटवर्क और इंटरनेट जैसे अविश्वासपूर्ण बाहरी नेटवर्क के बीच स्थित होता है, हालांकि कंपनी के नेटवर्क के एक हिस्से को नेटवर्क के शेष हिस्सों से फायरवॉल द्वारा भी परिरक्षित किया जा सकता है।

  फ़ायरवॉल एक कुली के रूप में कार्य करता है जो नेटवर्क एक्सेस प्रदान करने से पहले प्रत्येक उपयोगकर्ता की साख की जाँच करता है। यह इनपुट ट्रैफिक नाम, आई पी एड्रेस, एप्लिकेशन और अन्य सुविधाओं को परिभाषित करता है। यह जानकारी नेटवर्क व्यवस्थापक द्वारा प्रबंधित नियमों तक पहुँच नियमों के विरुद्ध है। फ़ायरवॉल नेटवर्क में और उसके बाहर अवांछित संपर्क को प्रतिबंधित करता है और बड़े संगठनों में विशेष रूप से नामित डिवाइस, जो बाकी नेटवर्क से अलग है पर स्थित होता है, ताकि किसी भी आने वाले अनुरोध की निजी नेटवर्क संसाधनों तक सीधी पहुंच न हो। स्थिर पैकेट फ़िल्टरिंग, अत्याधुनिक निरीक्षण, नेटवर्क एड्रेस अनुवाद और प्रॉक्सी फ़िल्टरिंग सहित फ़ायरवॉल स्क्रीनिंग के लिए कई प्रौद्योगिकियाँ हैं। उनका उपयोग फ़ायरवॉल सुरक्षा मिश्रण के रूप में भी किया जाता है।

  पैकेट फ़िल्टर डाटा पैकेट हेडर के चयनित क्षेत्रों का विश्लेषण करता है, जो विश्वसनीय नेटवर्क और इंटरनेट के बीच अलग-अलग पैकेट को स्कैन करता है। यह फ़िल्टरिंग तकनीक कई प्रकार के हमलों को छोड़ सकती है। पूर्ण निरीक्षण यह आकलन करके कि शिपमेंट प्रेषक और प्राप्तकर्ता के बीच चल रही बातचीत का हिस्सा है या नहीं अधिक सुरक्षा प्रदान करता है । यह कई शिपमेंट में ट्रैकिंग जानकारी के लिए तालिका बनाता है।

अनुमत चर्चा के लिए अनुमति प्राप्त चर्चा या प्रयास करने के उद्देश्य से पैक्स की अनुमति या अस्वीकार कर दिया जाता है। जब स्थिर पैकेट फ़िल्टरिंग और निरीक्षण किए जाते हैं, तो नेटवर्क एड्रेस ट्रांसलेशन (NAT) अतिरिक्त परत सुरक्षा प्रदान कर सकता है। NAT, कंपनी के आंतरिक होस्ट कंप्यूटर के आई पी एड्रेस को फ़ायरवॉल के बाहर स्निफर प्रोग्राम से बचाने के लिए और आंतरिक सिस्टम में घुसपैठ करने के लिए उस जानकारी का उपयोग करने के लिए मास्क करता है।

एप्लिकेशन प्रॉक्सी को फ़िल्टर करना पैकेट एप्लिकेशन सामग्री की जांच करता है। एक प्रॉक्सी सर्वर कंपनी के बाहर उत्पन्न होने वाले फ़ायरवॉल डाटा पैकेट के दूसरी ओर एक प्रॉक्सी को रोकता है, उसका निरीक्षण करता है तथा स्थानांतरित करता है। यदि कंपनी के बाहर का उपयोगकर्ता कंपनी के अंदर के उपयोगकर्ता से जुड़ना चाहता है, तो बाहरी उपयोगकर्ता पहले प्रॉक्सी एप्लिकेशन से बात करता है और प्रॉक्सी एप्लिकेशन कंपनी के आंतरिक उपकरण से संपर्क करता है। इसी तरह, कंपनी में एक कंप्यूटर उपयोगकर्ता बाहरी मशीनों के साथ प्रॉक्सी करने के लिए चलता है। एक सफल फ़ायरवॉल बनाने के लिए, एक व्यवस्थापक को विस्तृत आंतरिक नियमों को बनाए रखना चाहिए जो अधिकृत या अस्वीकृत व्यक्तियों, अनुप्रयोगों या पते को परिभाषित करता है। फायरवॉल बाह्य उपकरणों द्वारा नेटवर्क के प्रवेश को बाधित कर सकते हैं, लेकिन वे उन्हें ऐसा करने से पूरी तरह से रोक नहीं सकते हैं।

- **घुसपैठ का पता लगाने वाले सिस्टम:** वाणिज्यिक सुरक्षा विक्रेता संदिग्ध नेटवर्क ट्रैफ़िक के खिलाफ घुसपैठ का पता लगाने और फ़ायरवॉल के अलावा फ़ाइलों और डाटा बेस तक पहुंचने का प्रयास करने के लिए सॉफ़्टवेयर और सेवाएं भी प्रदान करते हैं। पता लगाने और बंद करने वाले घुसपैठियों के लिए पूर्णकालिक निगरानी उपकरण व्यापार नेटवर्क के सबसे कमजोर बिंदुओं या "हॉट स्पॉट" में घुसपैठ का पता लगाने वाले सिस्टम में शामिल हैं। यदि कोई संदेहास्पद या विसंगतिपूर्ण घटना होती है, तो उपकरण अलर्ट को ट्रिगर कर सकता है। स्कैनिंग सॉफ्टवेयर उन रुझानों के लिए खोज करता है जो हमलावर मशीन के ज्ञात तरीकों को इंगित करता है, जैसे कि खराब पासवर्ड । जब सुरक्षा हमलों का पता लगाया जाता है। तो कंप्यूटर निगरानी उन घटाओं की जांच करती है यदि कोई अवांछित ट्रैफ़िक प्राप्त होता है, तो नेटवर्क के विशेष रूप से संवेदनशील भाग को बंद करने के लिए घुसपैठ का पता लगाने वाले उपकरण को भी संशोधित किया जा सकता है।

- **एंटीवायरस और एंटीस्पायवेयर सॉफ्टवेयर:** रक्षा सुरक्षा योजनाओं को मैलवेयर से व्यक्तियों और कंपनियों दोनों के लिए सभी उपकरणों की रक्षा करने की आवश्यकता है। कंप्यूटर वायरस, कंप्यूटर वार्म, ट्रॉपिकल हॉर्स, स्पाइवेयर और एडवेयर जैसे मैलवेयर को एंटीवायरल द्वारा रोका और पहचाना जाता है। अधिकांश एंटीवायरस सॉफ़्टवेयर केवल तभी प्रभावी होते हैं जब यह पहले से ज्ञात मालवेयर के विरुद्ध लिखा जाता है।

- **एकीकृत खतरा प्रबंधन प्रणाली (यू टी एम):** चूंकि इस तरह की सुरक्षा सेवाओं का लाभ उठाने के लिए एक बड़ी लागत लागू की जाती है और छोटे और मध्यम व्यापारिक संगठनों द्वारा ऐसी सुविधाओं तक पहुंच बनाना आसान नहीं होता है, इसलिए बाजार में कम लागत और बेहतर प्रबंधन के साथ सुरक्षा उत्पादों को बाजार में पेश किया जाता है

जिसमें एक ही उपकरण में संयुक्त सुरक्षा विधियां और फायरवाल, वर्चुअल प्राइवेट नेटवर्क, घुसपैठ का पता लगाने वाले सिस्टम, वेब सिस्टम, वेब कंटेंट फ़िल्टरिंग और एंटी स्पेम सॉफ्टवेयर इत्यादि शामिल होते है। इन व्यापक सुरक्षा प्रबंधन उत्पादों को एकीकृत खतरा प्रबंधन (यू टी एम) सिस्टम कहा जाता है। हालांकि शुरू में छोटे और मध्यम आकार के व्यवसायों के उद्देश्य से, यू टी एम उत्पाद सभी प्रकार के नेटवर्क के लिए उपलब्ध हैं। बाजार में यू टी एम के प्रमुख खिलाड़ी क्रॉसबीम, फोर्टिनेंट और चेक प्वाइंट हैं, और सिस्को सिस्टम्स और जुनिपर नेटवर्क जैसे नेटवर्किंग विक्रेता अपने उपकरणों में कुछ यू टी एम क्षमताएं प्रदान करते हैं।

11.8.3 साइबर-भौतिक सुरक्षा प्रणाली

साइबर-फिजिकल सिक्योरिटी सिस्टम (सी पी एस एस) उपकरण संगठनों की सुरक्षा को बढ़ाने में महत्वपूर्ण भूमिका निभा सकते हैं। हालांकि, उन्हें अलगाव में तैनात नहीं किया जाना चाहिए। साइबर भौतिक सुरक्षा प्रणाली प्रौद्योगिकियां केवल समग्र सुरक्षा योजनाओं, प्रक्रियाओं और उनके द्वारा समर्थित प्रक्रियाओं के रूप में प्रभावी हैं। सी पी एस एस को संगठन के एक बड़े, समन्वित सुरक्षा रणनीति के हिस्से के रूप में लागू किया जाना चाहिए जो नेटवर्क, सुरक्षा कर्मियों और कर्मचारियों पर प्रभाव को ध्यान में रखता है। साइबर भौतिक सुरक्षा प्रणाली के विभिन्न प्रकार हैं:

- **निष्क्रिय:** वीडियो कैमरे अपराध को रोक सकते हैं, परिसर के आगंतुकों की पहचान कर सकते हैं, और सक्रिय खतरे की स्थिति के दौरान वास्तविक समय की जानकारी प्रदान कर सकते हैं। निष्क्रिय निगरानी रिकॉर्डेड डाटा को संदर्भित करता है जिसका, आमतौर पर एक घटना जांच के हिस्से के रूप में विश्लेषण किया जाता है । एक्टिव मॉनिटरिंग में लाइव वीडियो फीड देखने वाले कर्मी शामिल होते हैं। कुछ जिलों में कानून प्रवर्तन के साथ एक सुरक्षा घटना के दौरान वास्तविक समय वीडियो फ़ीड पहुंच प्रदान करने के लिए समझौते हैं।

- **संचार उपकरण और प्लेटफॉर्म:** वायर्ड और वायरलेस संचार प्रौद्योगिकियाँ, जैसे इंटरकॉम सिस्टम, स्थानीय अलार्म एन्यूकेटर, फ़ोन सिस्टम और दो तरह से रेडियो का उपयोग स्कूल के अधिकारियों और आपातकालीन कर्मियों द्वारा आपात स्थिति के दौरान किया जाता है। उन्नत 911 (E911) और अन्य स्थान-आधारित संचार उस स्थान की पहचान करते हैं जहां से कॉल या संदेश भेजे जाते हैं। उपस्थिति और चेक-इन एप्लिकेशन का उपयोग कैंपस में छात्र की उपस्थिति को ट्रैक करने के लिए किया जा सकता है और किसी आपातकालीन घटना के दौरान स्कूल के कर्मचारियों को छात्रों के लिए खाते की अनुमति दे सकता है।

- **सेंसर और अलार्म:** सेंसर और अलार्म का इस्तेमाल कैंपस में चालू और बंद होने वाले कर्मियों को सूचित करने के लिए किया जा सकता है। मानचित्रण और सत्यापन समाधान कर्मियों को आपातकाल के सटीक स्थान की मदद कर सकते हैं और ऑडियो / या वीडियो इनपुट प्रदान कर सकते हैं जो खतरे की प्रकृति का निर्धारण करते हैं।

- **ड्यूरेस अलार्म (पैनिक बटन):** ये वायर्ड या वायरलेस डिवाइस होते हैं जिनका उपयोग स्कूल के अधिकारियों और आपातकालीन कर्मियों को किसी आपात स्थिति के बारे में सूचित करने के लिए किया जा सकता है। कुछ उपकरण स्थान के अलावा प्रेषक की पहचान भी प्रसारित करते हैं। दरवाजे और खिड़की के सेंसर जब दरवाजे और खिड़कियां टूट गई हैं उन्हें अलार्म को अलर्ट या ट्रिगर भेज सकते है। गनशॉट डिटेक्टर एक बंदूक की गोली के स्थान और कैलिबर की पहचान कर सकते हैं। इन्हें व्यापक सुरक्षा प्रणालियों के साथ एकीकृत किया जा सकता है जो अधिकारियों को प्रभावित क्षेत्र पर कैमरे को इंगित कर सकते हैं, और दरवाजे बंद कर सकते हैं।

- **रोबोट:** रोबोट चेहरे और वस्तु की पहचान और स्ट्रीमिंग वीडियो सहित कई सुरक्षा सुविधाओं को एकीकृत करते हैं, जो उत्तरदाताओं के लिए आंखों और कानों के रूप में काम कर सकते हैं।

- **प्रकाश व्यवस्था:** यह आपात स्थिति में सुरक्षित मार्ग प्रदान करने और समग्र परिसर सुरक्षा में सुधार करने के लिए प्रकाश व्यवस्था पर विचार किया जाना चाहिए । आपातकालीन निकास मार्गों को हाइलाइट करने के अलावा, संचार के लिए प्रकाश व्यवस्था का उपयोग किया जा सकता है, जैसे कानून प्रवर्तन को उन स्थानों की पहचान करने की अनुमति देना जो एक सुरक्षा घटना के दौरान साफ किए गए हैं।

- **फॉगिंग और काली मिर्च स्प्रे सिस्टम:** यह एक स्मोकेनस्क्रीन बनाता है या रासायनिक अवक्षेप को तैनात करता है और अक्सर वेस्टिब्यूल में डाल दिया जाता है। हालांकि, ये ऑपरेशन में बाधा उत्पन्न करने का जोखिम रखते हैं और इनका या दुरुपयोग किया जा सकता है।

11.8.4 अभिगम नियंत्रण

अभिगम नियंत्रण स्थानों या अन्य संसाधनों तक पहुंच का चयनात्मक प्रतिबंध है। मानव संसाधन (जैसे सुरक्षा गार्ड), यांत्रिक साधन (जैसे ताले और गेट) या एक तकनीकी समाधान (जैसे आई डी कार्ड स्वाइप करना) का उपयोग करके अभिगम नियंत्रण पूरा किया जा सकता है। अभिगम नियंत्रण समाधान के उदाहरणों में शामिल हैं:

- **ताले, गेट्स, और वेस्टिब्यूल्स:** विशेषज्ञों का सुझाव है कि विश्वविद्यालय के परिसरों को केवल एक प्रवेश बिंदु और सॉफ्टवेयर सक्षम कैमरों के साथ काम करने के दौरान बंद कर दिया जाए। कार्यालय कर्मी बाहरी लोगों को एक सुरक्षित वेस्टिब्यूल के माध्यम से प्रवेश करने के लिए स्पष्ट कर सकते हैं, जो बुलेट-प्रूफ ग्लास से बना हो सकता है या एक सॉफ्टवेयर सक्षम कैमरे के साथ एक टूट-प्रूफिंग फिल्म से सुसज्जित होता है।

- **मेटल डिटेक्टर:** विश्वविद्यालय परिसर में छात्रों, कर्मचारियों या आगंतुकों को बंदूक या अन्य हथियार लाने से रोकने के लिए कुछ विश्वविद्यालय मेटल डिटेक्टर का उपयोग करते हैं।

- **डोर बैरियर:** ये सुरक्षा उपकरण एक हमलावर को पहुंच प्राप्त करने से रोकने में मदद करने के लिए दरवाजे को बैरिकेड में बदल देते हैं। हालांकि इन उत्पादों का स्थानीय फायर कोड के साथ विरोध हो सकता है।

- **एंट्री कार्ड्स:** एंट्री कार्ड्स का इस्तेमाल एम्बेडेड तकनीक के साथ या बिना किया जा सकता है। आई डी कार्ड एक व्यक्ति के विश्वविद्यालय परिसर में प्रवेश करने का अधिकृत संकेत है। कुछ विश्वविद्यालय प्रणाली छात्रों, शिक्षकों और कर्मचारियों को आई डी कार्ड जारी करती हैं। आगंतुक अतिथि बैज या चिपकने वाले स्टिकर प्राप्त कर सकते हैं। स्मार्ट आई डी कार्ड में एक चिप शामिल होती है जिसका उपयोग आपातकालीन स्थिति के दौरान छात्र के स्थानों की पहचान करने के लिए किया जा सकता है या स्कूल के कर्मचारियों को दरवाजे खोलने की अनुमति देता है। बायोमेट्रिक रीडर जैसे कि फिंगरप्रिंट स्कैनर का उपयोग समान उद्देश्यों के लिए किया जा सकता है।

- **एक्सेस सॉफ्टवेयर:** यह एक विशेष सॉफ्टवेयर है, जो अक्सर स्कूल कार्यालयों या अन्य परिसर में प्रवेश बिंदुओं में उपयोग किया जाता है, यह आगंतुक इतिहास को ट्रैक कर सकता है, अस्थायी बैज प्रिंट कर सकता है, और पंजीकृत यौन अपराधियों के लिए डाटा बेस की जांच कर सकता है। एक व्यक्ति को किसी इमारत में प्रवेश करने से रोकने, आपराधिक डाटा बेस के खिलाफ आगंतुकों से मेल खाने या छात्रों को सही बस में चढ़ाने में मदद करने के लिए चेहरे की पहचान सॉफ्टवेयर का उपयोग किया जा सकता है। यह सॉफ्टवेयर अपनी प्रारंभिक अवस्था में है इसमें अभी सटीकता और छात्र की गोपनीयता के बारे में चिंताएं व्यक्त की गई हैं। उसी तर्ज पर, ऑब्जेक्ट मान्यता प्रौद्योगिकी का उपयोग हथियारों या अन्य निषिद्ध वस्तुओं की पहचान करने के लिए किया जा सकता है।

11.8.5 सॉफ्टवेयर की गुणवत्ता सुनिश्चित करना

कंपनियां सॉफ्टवेयर उपायों और कठोर सॉफ्टवेयर परीक्षण के उपयोग के साथ-साथ प्रभावी सुरक्षा और नियंत्रणों को लागू करने के माध्यम से सिस्टम की गुणवत्ता और विश्वसनीयता में सुधार कर सकती हैं। सॉफ्टवेयर मेट्रिक्स गणना किए गए परिमाण के रूप में मशीन उद्देश्य मूल्यांकन हैं। मेट्रिक्स के उपयोग से आई टी और अंतिम उपयोगकर्ताओं को सामूहिक रूप से मूल्यांकन करने में मदद मिलती है कि वे आउटपुट हैं और समस्या उत्पन्न होने पर उनका पता लगा सकते हैं। सॉफ्टवेयर मेट्रिक्स इस बात के उदाहरण हैं कि किसी दी गई इकाई में कितने लेन-देन किए जा सकते हैं, ऑनलाइन उत्तर देने का समय कितना है, हर घंटे कितने भुगतान किए गए चेक दिखाए जाते हैं और कार्यक्रम कोड की 100 लाइनों के अनुसार कितनी त्रुटियां ज्ञात होती हैं। कुशल होने के लिए मेट्रिक्स की योजना, औपचारिकता, उद्देश्य और नियमित रूप से उपयोग किया जाना चाहिए।

प्रारंभिक, विश्वसनीय और व्यापक परीक्षण प्रणाली की स्थिरता में बहुत योगदान कर सकते हैं। कई लोग अपने काम की शुद्धता को प्रदर्शित करने के तरीके के रूप में जाँच करते हैं। वास्तव में हम जानते हैं,कि सभी बड़े सॉफ़्टवेयर में त्रुटियाँ हैं और हमें इन त्रुटियों का पता लगाने के लिए परीक्षण करना होगा।

एक सॉफ्टवेयर एप्लीकेशन से पहले अच्छा परीक्षण शुरू होता है। यह लोगों के एक छोटे समूह के व्यवस्थित विश्लेषण का भी उपयोग करता है, जिन्होंने परीक्षण के लिए विशेष लक्ष्यों के लिए आवश्यक विशेषज्ञता को ध्यान से चुना है। जब डेवलपर्स प्रोग्राम लिखना शुरू करते हैं, तो वे कोड को फिर से लिखने के लिए कोडिंग का उपयोग भी कर सकते हैं। हालाँकि, प्रोग्राम चलाकर कोड की जाँच की जानी चाहिए। यदि गलतियाँ पाई जाती हैं, तो डिबगिंग नामक एक प्रक्रिया स्रोत को खोज लेगी और हटा देगी।

बोध प्रश्न ख:

1) वेब पर नेटवर्क ट्रैफ़िक को एन्क्रिप्ट करने के तरीके क्या हैं?

.....

.....

.....

.....

2) साइबर-भौतिक सुरक्षा सुनिश्चित करने में सेंसर और अलार्म कैसे मदद करते हैं?

.....

.....

.....

3) सुरक्षा आउटसोर्सिंग से आप क्या समझते हैं?

.....

.....

.....

.....

4) बायोमेट्रिक सुरक्षा उपाय क्या हैं?

.....

.....

.....

.....

11.9 सारांश

अब, लगभग हर व्यवसाय में डाटा चालित प्रक्रियाएं होती हैं। यदि कोई मशीन या कंप्यूटर व्यवसाय लेनदेन करना शुरू कर देता है, तो व्यवसायिक व्यक्ति ग्राहकों को बेचने में सक्षम नहीं

हो सकता है। या कभी-कभी ऐसा भी हो सकता है कि कोई घुसपैठिया कंप्यूटर सिस्टम में घुसने की कोशिश करता है और ग्राहकों के गोपनीय डाटा विवरण को चुरा लेता है या नष्ट कर देता है।

जब बड़ी मात्रा में डिजिटल जानकारी संग्रहीत की जाती है, तो यह कई अन्य प्रकार के खतरों की चपेट में है। सूचना प्रणाली को कंप्यूटर नेटवर्क के माध्यम से कई स्थानों पर परस्पर जोड़ा जा सकता है। और इसलिए, घुसपैठियों के हमले या अनधिकृत पहुंच कभी भी कंप्यूटर नेटवर्क के किसी भी एक्सेस बिंदु पर हो सकती है, जो पूरे नेटवर्क को नष्ट कर सकती है। कंप्यूटर नेटवर्क के बजाय, इंटरनेट के माध्यम से जुड़े सिस्टम अधिक असुरक्षित हैं क्योंकि वे पूरी दुनिया में किसी के लिए भी खुले हैं। इंटरनेट इतना बड़ा है कि इसका दुरुपयोग होने पर इसका व्यापक प्रभाव हो सकता है। वायरलेस नेटवर्किंग कई फायदे प्रदान करता है, लेकिन यह विभिन्न सुरक्षा खतरों के साथ भी जुड़ा हुआ है। वायरलेस सुरक्षा खतरों और कमजोरियों के लिए तकनीकी समाधान का कार्यान्वयन, वायरलेस सुरक्षा एक संगठन की प्राथमिक आवश्यकता है।

एक हैकर एक बुद्धिमान कोडर है जिसका उद्देश्य किसी अन्य उपयोगकर्ता के कंप्यूटर सिस्टम तक पहुंच प्राप्त करना है। वे किसी भी मानवीय हस्तक्षेप के बिना दुर्भावनापूर्ण फ़ाइलों का अनुरोध कर सकते हैं, उपयोगी डाटा को नष्ट कर सकते हैं, डाटा संचारित कर सकते हैं और उपयोगकर्ता कार्यों की निगरानी के लिए पृष्ठभूमि में छिपे हुए प्रोग्राम को स्थापित कर सकते हैं। ये विशेषज्ञ हैं और वेब साइटों और कंप्यूटर सिस्टम द्वारा नियोजित सुरक्षा सुरक्षा में खामियों को खोजने के द्वारा अनधिकृत पहुंच प्राप्त करने के तरीकों को जानते हैं। किसी सिस्टम को हैक करने का उद्देश्य डाटा चोरी करना या जानकारी को नुकसान पहुंचाना, सिस्टम को नुकसान पहुंचाना, ख़राब करना, किसी वेब साइट का नष्ट होना या कॉर्पोरेट सूचना प्रणाली आदि होता है।

साइबर फोरेंसिक कंप्यूटर और डिजिटल स्टोरेज मीडिया में डिजिटल साइंस की एक शाखा है जिसमें तथ्य हैं। कानूनी कार्रवाई का जवाब देने के लिए, डाटा सुरक्षा और नियंत्रण प्रबंधन अत्यंत आवश्यक हो गया है। आज के समय में, इन्वेंट्री फ्रॉड, हेराफेरी, व्यापार गुप्त डाटा की चोरी, साइबर अपराध और कई सिविल मामलों के लिए बहुत सारे साक्ष्य डिजिटल रूप में उपलब्ध हैं।

इंटरनेट पर संगठनों द्वारा संग्रहीत या साझा की गई डिजिटल जानकारी की सुरक्षा के लिए एन्क्रिप्शन सबसे आम तरीकों में से एक है। यह सादे पाठ या डाटा को एन्क्रिप्टेड डाटा में बदलने की प्रक्रिया है, जिसे सिफर टेक्स्ट कहा जाता है ताकि कोई अनधिकृत व्यक्ति इसे न पढ़ सके। इसे केवल प्राप्तकर्ता और प्रेषक द्वारा पढ़ा जा सकता है। एक गुप्त संख्यात्मक कोड, जिसे एन्क्रिप्शन की कहा जाता है, का उपयोग सादे डाटा को सिफर टेक्स्ट में बदलने के लिए किया जाता है। संदेश को प्राप्तकर्ता द्वारा डिक्रिप्ट किया जाना चाहिए।

बायोमेट्रिक प्रमाणीकरण उन उपकरणों का उपयोग करता है जो व्यक्तिगत मानव लक्षणों को पढ़ते हैं और उनकी व्याख्या करते हैं, जैसे कि उंगलियों के निशान, रेटिना और आवाज। बॉयोमीट्रिक प्रमाणीकरण एक भौतिक या व्यवहार संबंधी विशेषता माप पर आधारित है, जो प्रत्येक व्यक्ति के लिए विशिष्ट है। मैलवेयर और घुसपैठियों से सुरक्षा के बिना इंटरनेट से जुड़ना बहुत जोखिम भरा होगा। गैर-बायोमेट्रिक सुरक्षा उपायों के लिए आवश्यक व्यवसाय उपकरण

फ़ायरवॉल, घुसपैठ का पता लगाने वाले सिस्टम और एंटीवायरस सॉफ़्टवेयर आदि उपलब्ध हैं।

संगठनों की सुरक्षा बढ़ाने में साइबर- भौतिक सुरक्षा सिस्टम उपकरण महत्वपूर्ण भूमिका निभा सकते हैं। हालांकि, उन्हें अलगाव में तैनात नहीं किया जाना चाहिए। साइबर भौतिक सुरक्षा प्रणाली प्रौद्योगिकियां केवल समग्र सुरक्षा योजनाओं, प्रक्रियाओं और उनके द्वारा समर्थित प्रक्रियाओं के रूप में प्रभावी हैं। इसे संगठन के एक बड़े, समन्वित सुरक्षा रणनीति के हिस्से के रूप में लागू किया जाना चाहिए जो नेटवर्क, सुरक्षा कर्मियों और कर्मचारियों पर प्रभाव को ध्यान में रखता है।

अभिगम नियंत्रण स्थानों या अन्य संसाधनों तक पहुंच का चयनात्मक प्रतिबंध है। मानव संसाधन (जैसे सुरक्षा गार्ड), यांत्रिक साधन (जैसे ताले और गेट) या एक तकनीकी समाधान (जैसे आईडी कार्ड स्वाइप करना) का उपयोग करके अभिगम नियंत्रण पूरा किया जा सकता है। अभिगम नियंत्रण समाधान के उदाहरणों में ताले, द्वार और वेस्टिब्यूल, मेटल डिटेक्टर, डोर बैरियर, प्रवेश पत्र, एक्सेस कार्ड आदि शामिल हैं।

11.10 शब्दावली

साइबर फोरेंसिक: साइबर फोरेंसिक कंप्यूटर और डिजिटल स्टोरेज मीडिया में डिजिटल साइंस की एक शाखा है जिसमें तथ्य हैं। इसका लक्ष्य डिजिटल जानकारी के बारे में तथ्यों और विचारों को पहचानने, संरक्षित करने, पुनर्प्राप्त करने, विश्लेषण करने और प्रस्तुत करने के उद्देश्य से डिजिटल मीडिया की जांच करना है।

डीप पैकेट निरीक्षण (डी पी आई): डी पी आई डाटा फ़ाइलों की जांच करता है और व्यावसायिक-महत्वपूर्ण फ़ाइलों को उच्च प्राथमिकता प्रदान करते हुए निम्न-प्राथमिकता वाली ऑनलाइन सामग्री को सॉर्ट करता है। नेटवर्क के संचालकों द्वारा स्थापित प्राथमिकताओं के आधार पर, यह तय करता है कि एक विशिष्ट डाटा पैकेट अपने गंतव्य तक जारी रह सकता है या अधिक महत्वपूर्ण ट्रैफ़िक कार्यवाही के दौरान अवरुद्ध या विलंबित होना चाहिए।

डोर बैरियर: डोर बैरियर सुरक्षा उपकरण हमलावर को पहुंच हासिल करने से रोकने में मदद के लिए कक्षा के दरवाजे को एक बैरिकेड में बदल देते हैं। इन उत्पादों का स्थानीय फायर कोड के साथ विरोध भी हो सकता है।

ड्यूरस अलार्म (पैनिक बटन): ये वायर्ड या वायरलेस डिवाइस होते हैं जिनका उपयोग स्कूल के अधिकारियों और आपातकालीन कर्मियों को आपातकाल के बारे में सूचित करने के लिए किया जा सकता है। कुछ उपकरण स्थान के अलावा प्रेषक की पहचान भी प्रसारित करते हैं। दरवाजे और खिड़की के सेंसर जब दरवाजे और खिड़कियां टूट गई हैं उन्हें अलर्ट भेज सकते है या अलार्म को ट्रिगर कर सकते है। ।

पे- प्रति- क्लिक फ्रॉड: क्लिक फ्रॉड तब होता है, जब कोई व्यक्ति या कंप्यूटर प्रोग्राम धोखे से ऑनलाइन विज्ञापन पर क्लिक करता है, ताकि उसे खरीदने के लिए विज्ञापन में प्रदर्शित उत्पादों के बारे में अधिक जानने का कोई इरादा न हो। गूगल और अन्य वेब साइटों पर क्लिक

धोखाधड़ी एक गंभीर समस्या बन गई है जिसमें पे-पर-क्लिक ऑनलाइन विज्ञापन की सुविधा है।

रिकवरी-ओरिएंटेड कम्प्यूटिंग: इसमें क्विक-रिकवरी सिस्टम का डिज़ाइन और मल्टी-कंपोनेंट्स सिस्टम में त्रुटि स्रोतों का पता लगाने और जल्दी से उपाय करने के लिए ऑपरेटरों के कौशल और उपकरणों के कार्यान्वयन शामिल हैं।

एस क्यू एल इंजेक्शन अटैक: एस क्यू एल इंजेक्शन हमले वेब एप्लिकेशन सॉफ्टवेयर के कमजोर बिंदुओं का लाभ उठाते हैं जो सुरक्षा जांच के मामले में मजबूत नहीं होते हैं या जिनके पास डाटा सुरक्षा के लिए पर्याप्त कोड नहीं होता है।

11.11 स्वपरख प्रश्न

1) विभिन्न प्रकार के दुर्भाग्यपूर्ण सॉफ्टवेयर / मैलवेयर क्या है, जो साइबर अपराधों को प्रेरित करते है ?

2) साइबर अपराध क्या हैं? इन दिनों विभिन्न के हो रहे साइबर अपराधों का उल्लेख कीजिए।

3) साइबर फोरेंसिक क्या है?

4) नेटवर्क लेनदेन को सुरक्षित करने के विभिन्न तरीके क्या हैं?

5) इंटरनेट पर व्यवसाय को सुरक्षित करने के विभिन्न तरीके क्या हैं?

6) विभिन्न गैर-बायोमेट्रिक सुरक्षा उपाय क्या हैं?

7) साइबर भौतिक सुरक्षा प्रणाली के विभिन्न प्रकार क्या हैं?

8) विभिन्न अभिगम नियंत्रण समाधान बताइए।

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।

इकाई 12 आई टी अधिनियम 2000

इकाई की रूपरेखा

12.0 उद्देश्य

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

- सूचना प्रौद्योगिकी अधिनियम के अर्थ और महत्व को समझ सकें;
- आई टी संशोधन अधिनियम 2008 कैसे लागू हुआ यह स्पष्ट कर सकें;
- अधिनियम के विभिन्न प्रावधानों का वर्णन कर सकें; तथा
- साइबर अपराध और विभिन्न अपराधों के अर्थ को पहचान सकें।

12.1 प्रस्तावना

सूचना प्रौद्योगिकी अधिनियम को आई टी क्षेत्र के विकास, ई-कॉमर्स और ई-गवर्नेंस को सुविधाजनक बनाने और साइबर अपराधों को नियंत्रित करने के लिए प्रतिक्रिया के रूप में पारित किया गया था। आज इंटरनेट एक आवश्यकता बन गया है और इसकी बढ़ी हुई पैठ के साथ, डोमेन में स्पष्टता की आवश्यकता थी, आई टी एक्ट बहुत आवश्यक स्पष्टता और दिशा प्रदान करने का एक प्रयास था। यह इकाई आई टी अधिनियम 2000 और आई टी संशोधन अधिनियम 2008 के विभिन्न पहलुओं पर चर्चा करती है।

12.2 परिभाषा

सूचना प्रौद्योगिकी अधिनियम, 2000 सूचना प्रौद्योगिकी से संबंधित कानून है। आई टी अधिनियम, 2000 संसद के दोनों सदनों द्वारा आई टी विधेयक को पारित करने का परिणाम था। यह अधिनियम संयुक्त राष्ट्र आयोग द्वारा अंतर्राष्ट्रीय व्यापार कानून (UNCITRAL) पर आधारित है। यह ई-कॉमर्स और साइबर क्राइम से संबंधित है। यह, "इलेक्ट्रॉनिक डेटा इंटरचेंज और इलेक्ट्रॉनिक संचार के अन्य साधनों द्वारा आमतौर पर इलेक्ट्रॉनिक कॉमर्स के रूप में संदर्भित लेनदेन के लिए कानूनी मान्यता प्रदान करने के लिए एक अधिनियम है।" अधिनियम 17.10 2000 को लागू हुआ।

12.3 आई टी अधिनियम 2000 का गठन

इंटरनेट के आगमन और फिर इंटरनेट आधारित व्यापार लेनदेन में वृद्धि ने क्षेत्र को विनियमित करने के लिए कानून के निर्माण और कार्यान्वयन को आवश्यक बना दिया । डिजिटल तकनीक ने हमारे जीवन को बदल दिया है, अधिक से अधिक व्यक्ति और व्यवसाय इसे अपना रहे हैं और इसकी मदद से कई गतिविधियों का संचालन कर रहे हैं। आई टी अधिनियम 2000 के निर्माण से पहले, समग्र वातावरण आशंका का था। व्यक्तियों और व्यवसायों को इस डिजिटलकरण के साथ होने वाले फायदों के बारे में पता था, लेकिन साथ ही वे गतिविधियों का संचालन करने में संकोच कर रहे थे, विशेषकर मौद्रिक लेनदेन कानूनी ढांचे की कमी के कारण थे जो उन्हें कुछ अप्रिय घटनाओं से बचाएंगे। डिजिटल दुनिया में उठाए जा रहे कदमों से मेल खाने के लिए, UNCITRAL ने वर्ष 1996 में इलेक्ट्रॉनिक कॉमर्स पर मॉडल कानून को अपनाया। भारत भी इसके लिए एक हस्ताक्षरकर्ता था और इसलिए मॉडल कानून के अनुसार कानूनों को लागू करने की अपेक्षा की गई थी। इन कारकों को ध्यान में रखते हुए, ई-कॉमर्स और ई-गवर्नेंस की सुविधा के लिए इन बिलों को पेश किया गया था।

वर्ष 1998 में आई टी बिल का मसौदा तैयार किया गया था। तब बिल को संसदीय स्थायी समिति के सामने रखा गया था, जिसमें कुछ संशोधनों का सुझाव दिया गया था। अंत में, आई टी मंत्रालय ने कुछ बदलावों का सुझाव दिया और अनुमोदित संशोधनों को बिल में बनाए रखा गया और बाकी को छोड़ दिया गया। बिल को केंद्रीय कैबिनेट और फिर संसद के दोनों सदनों द्वारा अनुमोदित किया गया था। भारत के राष्ट्रपति ने भी विधेयक के लिए अपनी सहमति प्रदान की और यह 17 अक्टूबर, 2000 को लागू हुआ एक अधिनियम बन गया। आई टी

अधिनियम, 2000 भारतीय दंड संहिता 1860, भारतीय साक्ष्य अधिनियम 1872, बैंकर्स बुक संज्ञान में संशोधन लाया गया। अधिनियम 1891 और भारतीय रिजर्व बैंक अधिनियम 1934, जिसमें इलेक्ट्रॉनिक मोड पर आधारित अपराधों और सबूतों से संबंधित मुद्दों को शामिल करना और धन के इलेक्ट्रॉनिक हस्तांतरण से संबंधित विनियमों की आवश्यकता को संबोधित करना शामिल है।

12.4 आई टी अधिनियम 2000 में संशोधन

डिजिटलीकरण और ई-कॉमर्स लेन-देन के विकास के लिए आवश्यक बदलाव लाने और ऐसे लेनदेन की बचाव और सुरक्षा सुनिश्चित करने के लिए वर्ष 2000 में सूचना प्रौद्योगिकी अधिनियम बनाया गया, जिससे अपराधों को रोका जा सके। तब अधिनियम को डोमेन के विकास के लिए संशोधित किया गया था, ये संशोधन 2008 में संसद के दोनों सदनों द्वारा पारित किए गए थे और 5 फरवरी, 2009 को राष्ट्रपति की सहमति प्राप्त की, इस प्रकार संशोधन अधिनियम बन गया। इसने विभिन्न सकारात्मक घटनाक्रम पेश किए। इसे भारत सरकार द्वारा एक ऐसी नीति बनाने के प्रयास के रूप में देखा गया, जो विकसित हो रही प्रौद्योगिकी के साथ तालमेल बनाए रखने में सक्षम है। भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (CERT-In) अधिनियम के प्रशासन के लिए जिम्मेदार है। संशोधन ने पहले के अधिनियम द्वारा छोड़े गए अंतराल को भरने और सुरक्षा चिंताओं को दूर करने का प्रयास किया।

बढ़ते डिजिटलकरण, डिजिटल स्पेस में अपराधों या डिजिटल एड्स की मदद से इस अधिनियम को समय की जरूरत थी। आपत्तिजनक सामग्री भेजना / साझा करना, फ़िशिंग, पहचान की चोरी, धोखाधड़ी आदि ऐसे अपराध थे जिन्हें दंडात्मक प्रावधानों के दायरे में लाया जाना था। इन सभी कारकों ने आई टी अधिनियम 2000 में संशोधन किया, इस प्रकार आई टी अधिनियम 2008 के लिए मार्ग प्रशस्त हुआ। आई टी अधिनियम 2008 ने राष्ट्र के साइबर कानून ढांचे में क्रांति ला दी। अधिनियम में विभिन्न मुद्दों जैसे इलेक्ट्रॉनिक हस्ताक्षर को शामिल करना, साइबर अपराधों की अधिक संख्या को शामिल करना, डेटा सुरक्षा, गोपनीयता से संबंधित चिंताओं को संबोधित करना, और आतंकवाद के लिए डिजिटल / साइबर माध्यम के उपयोग से संबंधित मुद्दों से भी निपटा गया।

12.4.1 संशोधन अधिनियम, 2008 आई टी अधिनियम 2008

संशोधन अधिनियम 2008 के महत्वपूर्ण योगदान इस प्रकार हैं:

- अधिनियम ने अधिक स्पष्टता लाने और इसे अधिक समावेशी बनाने के लिए कई परिभाषाएँ प्रस्तुत की हैं:
  - **i)** इलेक्ट्रॉनिक हस्ताक्षर "का अर्थ है कि दूसरी अनुसूची में निर्दिष्ट इलेक्ट्रॉनिक तकनीक के माध्यम से एक ग्राहक द्वारा किसी भी इलेक्ट्रॉनिक रिकॉर्ड का प्रमाणीकरण और डिजिटल हस्ताक्षर शामिल हैं"
  - **ii)** संचार उपकरण "सेल फोन, व्यक्तिगत डिजिटल सहायता (सिसिली), या किसी भी पाठ, वीडियो, ऑडियो, या छवि को संचार भेजने या संचार करने के लिए उपयोग किए जाने वाले दोनों या किसी अन्य उपकरण के संयोजन का मतलब है।"

iii) साइबर कैफ़े का अर्थ है "किसी भी सुविधा से जहां इंटरनेट का उपयोग किसी भी व्यक्ति द्वारा व्यवसाय के साधारण पाठ्यक्रम में जनता के लिए पेश किया जाता है।"

iv) साइबर सुरक्षा "का अर्थ है अनधिकृत पहुंच, उपयोग, प्रकटीकरण, व्यवधान, संशोधन या विनाश से उसमें संग्रहीत सूचना, उपकरण, कंप्यूटर, कंप्यूटर संसाधन, संचार उपकरण और जानकारी की रक्षा करना।"

v) अधिनियम ने "किसी विशेष इलेक्ट्रॉनिक रिकॉर्ड के संबंध में मध्यस्थता" की परिभाषा को भी संशोधित किया, इसका मतलब है कि कोई भी व्यक्ति जो किसी अन्य व्यक्ति की ओर से उस रिकॉर्ड को प्राप्त करता है, संग्रहीत करता है या प्रसारित करता है या उस रिकॉर्ड के संबंध में कोई सेवा प्रदान करता है और इसमें दूरसंचार सेवा प्रदाता शामिल हैं, नेटवर्क सेवा प्रदाताओं, इंटरनेट सेवा प्रदाताओं, वेब होस्टिंग सेवा प्रदाताओं, खोज इंजन, ऑनलाइन भुगतान साइटों, ऑनलाइन-नीलामी साइटों, ऑनलाइन बाजार स्थानों और साइबर कैफे।

- कंप्यूटर, कंप्यूटर सिस्टम, आदि के नुकसान और क्षतिपूर्ति को संबोधित करते हुए अधिनियम में भी बदलाव लाया गया है, यदि कोई व्यक्ति किसी कंप्यूटर संसाधन में रहने वाली किसी सूचना को नष्ट या मिटा देता है या उसका मूल्य या उपयोगिता कम कर देता है या उसे नुकसान पहुंचाता है किसी भी तरह; किसी भी व्यक्ति को नुकसान पहुंचाने के इरादे से कंप्यूटर संसाधन के लिए उपयोग किए जाने वाले किसी भी कंप्यूटर स्रोत कोड को चोरी करना, छिपाना, नष्ट करना या बदलना या उसे नष्ट या परिवर्तित करना; वह इतने प्रभावित व्यक्ति को रूप में नुक्सान का भुगतान करके के लिए उत्तरदायी होगा जो अधिक नहीं होगा एक करोड़ रूपये से।
- कंप्यूटर से संबंधित अपराधों में "संचार सेवाओं के माध्यम से आपत्तिजनक संदेश भेजने के लिए दंड" से संबंधित अनुभाग शामिल हैं। इसमें आगे कहा गया है, "इस तरह के संदेशों की उत्पत्ति के बारे में किसी भी इलेक्ट्रॉनिक मेल या इलेक्ट्रॉनिक मेल संदेश में झुंझलाहट या असुविधा या धोखा देने या पता लगाने वाले या प्राप्तकर्ता को भ्रमित करने के उद्देश्य से (आईटीएएस 2008 के विचाराधीन) कैद की सजा दी जाएगी।

कई अन्य बदलाव भी पेश किए गए। इन प्रमुख परिवर्तनों की चर्चा आगामी वर्गों में की गई है।

बोध प्रश्न क:

1) आई टी अधिनियम 2000 की क्या आवश्यकता थी?

……

……

……

……

……

……

……

2) आई टी अधिनियम, 2000 में संशोधन में क्या प्रेरित किया?

……

……

……

……

……

3) रिक्त स्थान भरें:

i) आई टी अधिनियम _____ पर लागू हुआ।

ii) _____आई टी अधिनियम 2000 में संशोधन किया गया।

iii) अधिनियम के प्रशासन के लिए _____ जिम्मेदार है।

iv) _____सेल फ़ोन, व्यक्तिगत डिजिटल सहायता (सिसिली), या किसी भी पाठ, वीडियो, ऑडियो, या छवि को संचार करने, भेजने या प्रसारित करने के लिए उपयोग किए जाने वाले दोनों या किसी भी अन्य डिवाइस का संयोजन

12.5 डिजिटल हस्ताक्षर और एन्क्रिप्शन

आई टी अधिनियम 2000 के प्रावधानों के तहत, इलेक्ट्रॉनिक रिकॉर्ड के प्रमाणीकरण के उद्देश्य से किसी भी ग्राहक द्वारा डिजिटल हस्ताक्षर का उपयोग किया जा सकता है। इलेक्ट्रॉनिक रिकॉर्ड को "असममित क्रिप्टो प्रणाली और हैश फ़ंक्शन की सहायता से प्रमाणित किया जाता है जो प्रारंभिक इलेक्ट्रॉनिक रिकॉर्ड को एक और इलेक्ट्रॉनिक रिकॉर्ड में परिवर्तित करता है। (सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 2 (1) (पी)) ”

परंपरागत रूप से, किसी भी दस्तावेज़ पर एक व्यक्ति द्वारा हस्ताक्षर दस्तावेज़ के प्रमाणीकरण में मदद करता है और इसकी विश्वसनीयता के बारे में प्राप्तकर्ता को आश्वासन देता है। कागज़-आधारित दस्तावेज़ के मामले में यह संभव है, लेकिन इलेक्ट्रॉनिक दस्तावेज़ के मामले में, दस्तावेज़ या ईमेल के अंत में नाम का उल्लेख करने से इसकी प्रामाणिकता के बारे में लगभग कोई आश्वासन नहीं मिलता है। आई टी अधिनियम, 2000 इलेक्ट्रॉनिक दस्तावेजों की सुरक्षा के लिए सार्वजनिक कुंजी क्रिप्टोग्राफी को मान्यता देता है। अधिनियम की धारा 3 आगे एक उपयोगकर्ता को अपने डिजिटल हस्ताक्षर को चिपकाकर एक इलेक्ट्रॉनिक रिकॉर्ड के प्रमाणीकरण के लिए शक्ति प्रदान करती है। प्रमाणीकरण प्रक्रिया "असममित क्रिप्टो प्रणाली और हैश फ़ंक्शन को लागू करेगी जो प्रारंभिक इलेक्ट्रॉनिक रिकॉर्ड को अन्य रिकॉर्ड में बदल देती है"। इलेक्ट्रॉनिक रिकॉर्ड को किसी अन्य व्यक्ति द्वारा सत्यापित किया जा सकता है जो सार्वजनिक कुंजी के कब्जे में है। इसके अलावा, प्रत्येक ग्राहक के पास एक निजी और साथ ही एक सार्वजनिक कुंजी होती है जो उसके लिए विशिष्ट होती है और जो एक कामकाजी कुंजी जोड़ी का गठन करती है। डिजिटल हस्ताक्षर के निर्माण के लिए विशिष्ट जानकारी के लिए एन्क्रिप्शन के आवेदन की आवश्यकता होती है। प्रक्रिया में निम्नलिखित चरण शामिल हैं:

- डिजिटल हस्ताक्षर का उपयोग करके हस्ताक्षर किए जाने वाले संदेश को रेखांकित किया गया है, और फिर हैश फ़ंक्शन नामक एल्गोरिथ्म की मदद से संसाधित किया गया है। इस प्रकार प्राप्त संसाधित उत्पादन को हैश परिणाम कहा जाता है जो संदेश के लिए अद्वितीय है।
- इस हैश परिणाम का उत्पादन प्रेषक की निजी कुंजी का उपयोग करके एन्क्रिप्ट किया गया है। यह डिजिटल सिग्नेचर है।
- डिजिटल सिग्नेचर को उस संदेश से जोड़ा जाता है, जिसे बाद में इंटरनेट के माध्यम से प्राप्तकर्ता को भेज दिया जाता है।
- प्राप्तकर्ता के अंत में संदेश प्राप्त होने के बाद, वह संदेश को डिक्रिप्ट करने के लिए प्रेषक की सार्वजनिक कुंजी का उपयोग करता है। यदि प्रेषक के संदेश को उसकी सार्वजनिक कुंजी का उपयोग करके सफलतापूर्वक डिक्रिप्ट किया जाता है और हैश परिणाम की गणना की जाती है और डिजिटल हस्ताक्षर के आउटपुट के साथ तुलना की जाती है, तो प्राप्तकर्ता को संदेश की प्रामाणिकता और अखंडता का आश्वासन दिया जाता है।

12.6 आरोपण

इलेक्ट्रॉनिक माध्यम से होने वाले संचार में कोई ठोस घटक नहीं होता है। इसलिए, जिम्मेदारियों की पुष्टि करना और संघों को परिभाषित करना मुश्किल हो जाता है। एट्रिब्यूशन शब्द का अर्थ है "किसी लेखक, कलाकार या व्यक्ति को किसी कार्य या टिप्पणी को बताने की क्रिया।" आई टी अधिनियम 2000 (धारा 11) दिशानिर्देशों के बारे में बताता है कि इलेक्ट्रॉनिक दस्तावेज़ को उस व्यक्ति को कैसे जिम्मेदार ठहराया जा सकता है, जिससे यह उत्पन्न हुआ है। यह कहता है कि इलेक्ट्रॉनिक दस्तावेज़ को निम्नलिखित स्थितियों में प्रवर्तक के लिए जिम्मेदार ठहराया जाएगा:

- यदि प्रवर्तक ने स्वयं इलेक्ट्रॉनिक रिकॉर्ड भेजा है
- यदि किसी व्यक्ति को जिसे उस विशेष इलेक्ट्रॉनिक रिकॉर्ड के संबंध में उसकी ओर से कार्रवाई करने के लिए प्रवर्तक द्वारा अधिकार दिया गया था, तो उसने भेजा है।
- यदि यह सूचना प्रणाली का उपयोग करके भेजा गया था, जो स्वयं या उसकी ओर से प्रोग्रामर द्वारा स्वचालित रूप से इलेक्ट्रॉनिक रिकॉर्ड भेजने के लिए प्रोग्राम किया गया था।
- उदाहरण के लिए, यदि A से B को कोई ईमेल भेजा गया था, तो A इलेक्ट्रॉनिक रिकॉर्ड का प्रवर्तक होगा और B इस मामले में पताका होगा।

12.7 इलेक्ट्रॉनिक रिकॉर्ड की प्राप्ति और प्रेषण

आई टी अधिनियम की धारा 12 उन शिष्टाचार से संबंधित है जिसमें इलेक्ट्रॉनिक रिकॉर्ड की प्राप्ति की पावती दी जा सकती है और आई टी अधिनियम की धारा 13 में इलेक्ट्रॉनिक रिकॉर्ड की प्राप्ति के समय की चर्चा की गई है।

यदि इलेक्ट्रॉनिक रिकॉर्ड के प्रवर्तक ने रिकॉर्ड की प्राप्ति के बारे में रिसीवर द्वारा दी जाने वाली पावती के किसी विशेष मोड को निर्दिष्ट नहीं किया है, तो पावती "पतेदार द्वारा किसी भी संचार, स्वचालित या अन्यथा" या "किसी भी आचरण" द्वारा दी जा सकती है। यह पता लगाने के लिए पर्याप्त है कि प्रवर्तक को इलेक्ट्रॉनिक रिकॉर्ड प्राप्त हुआ है। " उदाहरण के लिए, यदि कोई व्यक्ति किसी मीटिंग के लिए मेल प्राप्त करता है, तो व्यक्ति प्रेषक को एक मेल भेजकर कह सकता है कि जानकारी के लिए धन्यवाद, या एक स्वचालित प्रतिक्रिया भेजें या मीटिंग में शामिल होकर रुचि दिखाता है। ये गतिविधियाँ रिसीवर के छोर से पावती दिखाती हैं।

इसके अलावा, ऐसे मामलों में जहां इलेक्ट्रॉनिक रिकॉर्ड के प्रवर्तक ने यह निर्धारित किया है कि इलेक्ट्रॉनिक रिकॉर्ड केवल उसके द्वारा ऐसे इलेक्ट्रॉनिक रिकॉर्ड की पावती प्राप्त करने पर बाध्यकारी होगा, तब तक जब तक कि स्वीकृति प्राप्त नहीं हुई है, इलेक्ट्रॉनिक रिकॉर्ड को माना जाएगा प्रवर्तक द्वारा कभी नहीं भेजा गया। " लेकिन उन मामलों में जहां प्रवर्तक ने यह निर्दिष्ट नहीं किया है कि इलेक्ट्रॉनिक रिकॉर्ड केवल पावती की प्राप्ति पर बाध्यकारी होगा और पावती को निर्दिष्ट या सहमत होने के समय के भीतर प्रवर्तक द्वारा प्राप्त नहीं किया गया है या, यदि कोई समय निर्दिष्ट नहीं किया गया है या भीतर सहमत नहीं है एक उचित समय, तब प्रवर्तक को यह कहते हुए नोटिस दिया जा सकता है कि उसके द्वारा कोई पावती प्राप्त नहीं हुई है और एक उचित समय निर्दिष्ट करके जिसके द्वारा पावती उसके द्वारा प्राप्त की जानी चाहिए और यदि कोई पावती उक्त समय सीमा के भीतर प्राप्त नहीं हुई है, पता करने वाले को नोटिस देते हुए, इलेक्ट्रॉनिक रिकॉर्ड के साथ ऐसा व्यवहार करें जैसे कि इसे कभी नहीं भेजा गया हो। "

आई टी अधिनियम की धारा 13 इलेक्ट्रॉनिक रिकॉर्ड को भेजने की बात करती है। यह कहा जाता है कि, जिस समय कोई व्यक्ति इलेक्ट्रॉनिक रिकॉर्ड भेजता है और यह प्रेषक के नियंत्रण के दायरे के बाहर एक कंप्यूटर में प्रवेश करता है, प्रेषण का समय है। इसके अलावा, प्रेषण की उत्पत्ति का स्थान प्रेषक के व्यवसाय का स्थान है और रसीद का स्थान रिसीवर के व्यवसाय का स्थान है।

12.8 प्राधिकरण प्रमाणित करने का विनियमन

सूचना प्रौद्योगिकी अधिनियम यह निर्दिष्ट करता है कि "प्रमाणीकरण प्राधिकारी के नियंत्रक" को केंद्र सरकार द्वारा नियुक्त किया जा सकता है। प्रमाणित करने वाले अधिकारियों के नियंत्रक के पास प्राधिकारी को प्रमाणित करने के विनियमन के संबंध में अधिकार होता है। केंद्र में सरकार उप-नियंत्रक, सहायक नियंत्रक, अन्य अधिकारियों और कर्मचारियों को नियुक्त कर सकती है जैसा वे उचित समझे।

उप नियंत्रक और सहायक नियंत्रकों को कार्य नियंत्रक को कार्य सौंपने की आवश्यकता होती है। नियंत्रक के कार्यों में शामिल हैं: प्रमाणित अधिकारियों की गतिविधियों की निगरानी करना, उनके कर्तव्यों को निर्दिष्ट करना, उनकी चाबियों को प्रमाणित करना, उनके लिए मानक रखना, वांछित योग्यता से संबंधित आवश्यकताओं के संबंध में निर्णय लेना और प्रमाणित करने वाले अधिकारियों के प्रासंगिक अनुभव आदि। प्रमाणित प्राधिकरणों की सार्वजनिक कुंजी को प्रमाणित करने के लिए और उनके और ग्राहकों के बीच हितों के टकराव को भी हल करना होगा।

नियंत्रक के पास विदेशी प्रमाणन प्राधिकरण की मान्यता के लिए प्राधिकारी है, जो केंद्र सरकार की पूर्व स्वीकृति के साथ एक प्रमाणित प्राधिकारी है, नियंत्रक इस मान्यता को रद्द कर सकता है यदि वह संतुष्ट हो "कि किसी भी प्रमाणन प्राधिकरण ने शर्तों और प्रतिबंधों में से कोई भी उल्लंघन किया हो जिसके लिए इसे मान्यता दी गई थी "। अधिनियम यह भी प्रदान करता है कि कोई भी व्यक्ति भारत में इलेक्ट्रॉनिक हस्ताक्षर प्रमाणपत्र जारी करने के उद्देश्य से नियंत्रक के लिए लाइसेंस के लिए आवेदन कर सकता है। लाइसेंस जारी किया जा सकता है यदि संबंधित व्यक्ति केंद्र सरकार द्वारा निर्धारित आवश्यकताओं को पूरा करता है और केवल केंद्र सरकार द्वारा निर्धारित अवधि के लिए वैध है। लाइसेंस के नवीनीकरण के लिए, आवेदन को निर्धारित शुल्क के साथ करना होगा और मौजूदा लाइसेंस की समाप्ति की तारीख से पैंतालीस दिन पहले आवेदन करना होगा। लाइसेंस के लिए आवेदन को मामले की योग्यता और आवेदन के साथ दस्तावेजों के आधार पर अनुमोदित या अस्वीकार किया जा सकता है। नियंत्रक के पास लाइसेंस निलंबित करने का अधिकार है, अगर वह एक जांच के बाद संतुष्ट हो जाता है कि प्रमाणित प्राधिकारी द्वारा गलत और गलत बयान दिए गए हैं और जिन शर्तों के तहत लाइसेंस जारी किया गया था, उनका अनुपालन नहीं किया गया है, लेकिन निरस्त करने से पहले प्रमाणन प्राधिकरण सुना होने का एक उचित मौका दिया जाना चाहिए।

नियंत्रक के पास अपनी किसी भी शक्ति के प्रतिनिधिमंडल के लिए उप नियंत्रक, सहायक नियंत्रक या किसी अन्य अधिकारी के पास भी शक्ति है। नियंत्रक या कोई अन्य अधिकारी, जिसे उसके द्वारा अधिकृत किया गया है, के पास आई टी अधिनियम, किसी भी अन्य नियमों या विनियमों के उल्लंघन के संबंध में जांच / पूछताछ शुरू करने का अधिकार है। उनके पास भी पहुंच होगी: "किसी भी कंप्यूटर सिस्टम, किसी भी तंत्र, डेटा या ऐसी प्रणाली से जुड़े किसी भी अन्य सामग्री" की जानकारी के उद्देश्य से। इसके अलावा, "नियंत्रक या उनके द्वारा अधिकृत कोई भी अधिकारी इस तरह की शक्तियों का प्रयोग करेगा, जो आयकर अधिनियम, 1961 (1961 के 43 वें अध्याय) के अध्याय XIII के तहत आयकर अधिकारियों को दिए गए हैं, और ऐसी शक्तियों का प्रयोग करेंगे, उस अधिनियम के तहत निर्धारित ऐसी सीमाओं के अधीन। "

प्रमाणित अधिकारियों के मामले में, उन्हें यह सुनिश्चित करना होगा कि वे अधिनियम द्वारा निर्धारित प्रक्रियाओं और प्रोटोकॉल का पालन कर रहे हैं और उन्हें यह भी सुनिश्चित करना होगा कि उनके कर्मचारी भी प्रक्रियाओं और प्रोटोकॉल का पालन करते हैं। उनसे सुरक्षा प्रोटोकॉल का पालन करने और संसाधनों का उपयोग करने की अपेक्षा की जाती है जो दुर्भावनापूर्ण हमलों से सुरक्षित हैं। उन्हें अपने परिसर के भीतर एक विशिष्ट स्थान पर लाइसेंस प्रदर्शित करना होगा और यदि लाइसेंस निलंबित या निरस्त किया गया हो; उनसे अपेक्षा की जाती है कि वे इसे तुरंत प्रस्तुत करेंगे। यह प्रकटीकरण मानदंडों का भी पालन करना है ताकि प्रक्रिया की पवित्रता बनाए रखी जा सके और ऐसी स्थिति में जहां उनके कंप्यूटर सिस्टम की अखंडता प्रभावित हो सकती है; उन्हें संबंधित हितधारकों को सूचित करना चाहिए।

12.9 डिजिटल हस्ताक्षर प्रमाणपत्र

आई टी अधिनियम 2000 डिजिटल हस्ताक्षर प्रमाणपत्रों के बारे में बात करता है जो एक डिजिटल कुंजी है जो इसे धारण करने वाले व्यक्ति की पहचान को प्रमाणित करता है, और

प्रमाणित एजेंसियों द्वारा जारी किया जाता है। डिजिटल हस्ताक्षर प्रमाणपत्र इलेक्ट्रॉनिक रिकॉर्ड की प्रामाणिकता की पुष्टि करता है और यह सुनिश्चित करता है कि इसे पारगमन के दौरान नहीं बदला गया है। डिजिटल हस्ताक्षर प्रमाणपत्र की महत्वपूर्ण विशेषताएं हैं:

- ये प्रमाण पत्र संदेश स्रोत के प्रमाणीकरण में मदद करते हैं क्योंकि स्वामित्व एक विशिष्ट उपयोगकर्ता के लिए बाध्य है।
- वे एक आश्वासन प्रदान करने में मदद करते हैं कि संदेश पारगमन के दौरान बदल नहीं गया था।
- गैर-परित्याग सुनिश्चित किया जाता है क्योंकि प्रेषक अपने डिजिटल हस्ताक्षर को प्रभावित करने वाले संदेश भेजने से इनकार नहीं कर सकता है।

कोई भी व्यक्ति फॉर्म भरने और शुल्क की आवश्यक राशि जमा करने पर (INR 25,000 से अधिक नहीं) जमा करके डिजिटल हस्ताक्षर प्रमाणपत्र जारी करने के लिए आवेदन कर सकता है। प्रमाणन प्राधिकारी प्रमाण पत्र जारी कर सकता है यदि यह आवश्यक आदेश में आवेदन पाता है। ये प्रमाणपत्र केवल प्राधिकारी को प्रमाणित करके जारी किए जा सकते हैं।

12.10 सब्सक्राइबर्स की डयूटी

डिजिटल सिग्नेचर सर्टिफिकेट जारी होने के बाद, सब्सक्राइबर्स से अधिनियम द्वारा निर्धारित कुछ कर्तव्यों को पूरा करने की उम्मीद की जाती है। डिजिटल हस्ताक्षर प्रमाणपत्र में सूचीबद्ध सार्वजनिक कुंजी से मेल खाती निजी कुंजी का नियंत्रण रखने के लिए ग्राहक को अत्यंत सावधानी बरतनी होती है। यह महत्वपूर्ण है कि वह निजी कुंजी के रिसाव से बचने के लिए सभी आवश्यक सावधानी बरतता है, और यदि निजी कुंजी से समझौता हो जाता है, तो उसे तुरंत प्रमाणीकरण प्राधिकारी को सूचित करना चाहिए। ग्राहक को उस समय तक उत्तरदायी माना जाएगा जब तक कि उल्लंघन के संबंध में प्रमाणित प्राधिकारी को सूचित नहीं किया गया हो।

12.11 दंड और न्यायनिर्णय

सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 ने साइबर स्पेस से संबंधित कई अपराधों को जोड़ा और ऐसे अपराधों के नियंत्रण के लिए दंड का भी परिचय दिया। डिजिटलाइजेशन की बढ़ती पहुंच के साथ, सूचना का प्रवाह रूपांतरित हो गया है। जबकि डिजिटल मीडिया के उपयोग के लाभों के असंख्य हैं, यह बढ़ते अपराधों से अछूता नहीं है। साइबरस्पेस ने भूगोल की बाधाओं को हटा दिया है और ज्ञान / सूचना को अस्थिर बना दिया है। सूचना के दुरुपयोग को रोकने के लिए और इस प्रकार इससे होने वाले नुकसान को रोकने के लिए, आई टी अधिनियम ने दंड लागू किया। आई टी एक्ट के चैप्टर IX में दंड मुआवजा और न्याय निर्णयन चर्चा की गई है।

विभिन्न अपराधों के लिए दंड इस प्रकार हैं:

- **धारा 43:** "कंप्यूटर, कंप्यूटर सिस्टम आदि को नुकसान के लिए जुर्माना और क्षतिपूर्ति (आई टी ए ए -2008 में संशोधित वीडियोग्राफी)"। यह खंड कहता है, अगर कोई भी

व्यक्ति जो किसी कंप्यूटर, कंप्यूटर सिस्टम या कंप्यूटर नेटवर्क का उपयोग / उपयोग करने के लिए अधिकृत नहीं है, या किसी भी रूप में उससे डेटा निकालता है, उसमें वायरस का परिचय देता है या वायरस के हमले में कुछ कार्रवाई के लिए जिम्मेदार है, इसे बाधित करता है, इसे प्रभावित करता है या प्रभावित लोगों को मुआवजे के तरीके से क्षति के भुगतान के लिए जिम्मेदार किसी भी जानकारी को नष्ट कर देता है या बदल देता है। । मुआवजा एक करोड़ रुपये से अधिक नहीं होना चाहिए। यह उन मामलों में भी लागू होता है, जिसमें वह अधिकृत व्यक्ति तक पहुंच से इनकार करता है, दुर्भावनापूर्ण गतिविधियों के लिए अन्य को सहायता प्रदान करता है, या नुकसान का कारण बनने के इरादे से कंप्यूटर संसाधन के स्रोत कोड को चुराता है, छिपाता है या नष्ट करता है।

- **धारा 43 ए:** "डाटा की सुरक्षा में विफलता के लिए मुआवजा (आई टी ए ए 2006 में सम्मिलित वी डी ए, आई टी ए ए 2008 को बदलें)"। यह अनुभाग लापरवाही के मामलों से संबंधित है, और कहता है "जहां एक संवेदनशील शारीरिक व्यक्तिगत डेटा को रखने, निपटने या निपटने के लिए एक निगम निकाय के पास है। या एक कंप्यूटर संसाधन में जानकारी जो इसका मालिक है, नियंत्रित करता है या संचालित करता है, उचित सुरक्षा प्रथाओं और प्रक्रियाओं को लागू करने और बनाए रखने में लापरवाही करता है और जिससे किसी भी व्यक्ति को गलत नुकसान या गलत लाभ होता है, ऐसे निगम निकाय क्षतिपूर्ति के माध्यम से नुकसान का भुगतान करने के लिए उत्तरदायी होंगे इतना प्रभावित व्यक्ति को पांच करोड़ रुपये से अधिक नहीं।
- **धारा 44:** "जानकारी प्रस्तुत करने में विफलता के लिए दंड, वापसी, आदि" यह खंड जानकारी प्रस्तुत करने में विफलता, या रिकॉर्ड, फ़ाइल वापसी, खाते या रिकॉर्ड की पुस्तकों को बनाए रखने के परिणामस्वरूप दंड पर चर्चा करता है। यदि कोई व्यक्ति जिसे अधिनियम द्वारा सूचना या रिटर्न या रिपोर्ट प्रदान करने या प्राधिकारी को प्रमाणित करने के लिए आवश्यक है, तो आवश्यकता को पूरा करने में विफल रहता है, वह आयोजित किया जाएगा, "ऐसी विफलता के लिए एक लाख और पचास हजार रुपये से अधिक के दंड के लिए उत्तरदायी नहीं "। यदि वह "रिटर्न दाखिल करने या किसी भी जानकारी, पुस्तकों या अन्य दस्तावेजों को दर्ज करने में विफल रहता है, इसलिए निर्दिष्ट समय में नियमों में रिटर्न फाइल करने या उसे प्रस्तुत करने में विफल रहता है तो, वह दंड के लिए उत्तरदायी नहीं होगा इस तरह की विफलता के दौरान हर दिन पांच हजार रुपये से अधिक की "और अगर वह खाते की पुस्तक को बनाए रखने या कुछ रिकॉर्ड बनाए रखने के लिए अधिनियम द्वारा आवश्यक है, तो ऐसा करने में विफल रहता है," वह एक दंड के लिए उत्तरदायी होगा जो दस हजार रुपये से अधिक नहीं है हर दिन जिसके दौरान विफलता जारी है।
- **धारा 45: "अवशिष्ट दंड":** यदि कोई व्यक्ति आई टी अधिनियम द्वारा निर्धारित किसी नियम और विनियमन के विरोध में कार्य करता है, जिसके लिए अधिनियम में किसी विशिष्ट दंड का उल्लेख नहीं किया गया है, तो उसे 25000 से अधिक नहीं होने वाली राशि के मुआवजे के भुगतान के लिए उत्तरदायी ठहराया जाएगा। उस व्यक्ति को रुपए जो कार्रवाई से प्रभावित हो जाता है या राशि का जुर्माना 25000 रुपये से अधिक नहीं होता है।

न्यायिक निर्णय

अध्याय में चर्चा किए गए मामलों से संबंधित अधिनिर्णय के लिए, केंद्र सरकार के पास एक न्यायनिर्णायक अधिकारी नियुक्त करने की शक्ति है। " न्यायनिर्णायक अधिकारी को भारत सरकार के निदेशक या राज्य के समकक्ष अधिकारी के पद से नीचे नहीं होना चाहिए"। किसी व्यक्ति को तभी न्यायनिर्णायक अधिकारी नियुक्त किया जाना चाहिए, जब उसके पास "आई टी के क्षेत्र में अनुभव और केंद्र सरकार द्वारा निर्धारित कानूनी या न्यायिक अनुभव" हो। जुर्माना लगाने या मुआवजा देने के दौरान, न्यायनिर्णायक अधिकारी प्रतिनिधित्व के लिए उचित अवसर देगा और मुआवजा देने या केवल जब वह पूरी तरह से संतुष्ट है दंडित करना चाहिए। न्यायनिर्णायक अधिकारी के पास "सिविल न्यायालय की शक्तियां होंगी जो धारा 58 की उप-धारा (2) के तहत साइबर अपीलीय न्यायाधिकरण में दी गई हैं।" अधिनियम की धारा 47 उन कारकों पर चर्चा करती है जिन्हें मुआवजे का पुरस्कार देते समय न्यायनिर्णायक अधिकारी द्वारा विचार किया जाना चाहिए। इसमें कहा गया है कि अधिकारी को अनुचित लाभ के लाभों के प्रति सचेत होना चाहिए जो कि डिफ़ॉल्ट के परिणामस्वरूप हुआ, "डिफ़ॉल्ट के परिणामस्वरूप पीड़ित पक्ष को हुई हानि की मात्रा, और डिफ़ॉल्ट की दोहरावदार प्रकृति।"

बोध प्रश्न ख:

1) डिजिटल हस्ताक्षर प्रमाण पत्र क्या हैं?

.....

.....

.....

.....

2) आरोपण से आपका क्या मतलब है?

.....

.....

.....

.....

.....

3) रिक्त स्थान भरें:
   i) आई टी अधिनियम, 2000 इलेक्ट्रॉनिक दस्तावेजों की सुरक्षा के लिए _____ कूटलेखन को मान्यता देता है।
   ii) आई टी अधिनियम की धारा _____ में कंप्यूटर, कंप्यूटर सिस्टम आदि को नुकसान के लिए दंड और क्षतिपूर्ति पर चर्चा की गई है।
   iii) आई टी अधिनियम की धारा _____ में अवशिष्ट पेनल्टी पर चर्चा की गई।
   iv) ग्राहक को उस समय तक उत्तरदायी माना जाएगा जब तक कि उल्लंघन के संबंध में प्रमाणित प्राधिकारी को सूचित नहीं किया गया हो। (सही गलत)

12.12 डिजिटल हस्ताक्षर में प्रक्रिया, कार्य और कानूनी स्थिति

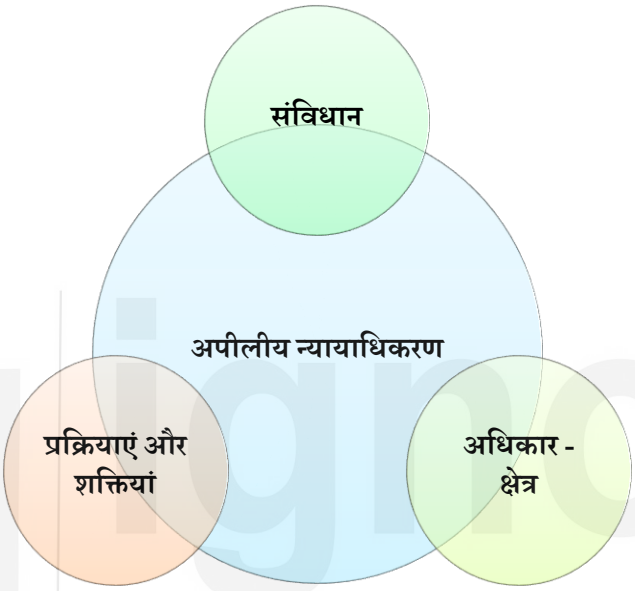
डिजिटल हस्ताक्षरों को भारतीय कानून प्रणाली द्वारा आई टी अधिनियम 2000 द्वारा जारी दिशा-निर्देशों के तहत मान्यता दी गई है। यह अधिनियम भारत में व्यापार करने में आसानी को बेहतर बनाने और डिजिटल लेनदेन को सुविधाजनक बनाने के लिए आवश्यक परिवर्तनों को लाने पर केंद्रित फोकस का परिणाम था। डिजिटल हस्ताक्षर सुनिश्चित करता है कि इलेक्ट्रॉनिक रिकॉर्ड प्रामाणिक है और सामग्री / संदेश के साथ छेड़छाड़ नहीं की गई है। आई टी अधिनियम 2000 डिजिटल सिग्नेचर के बारे में बात करता है, जबकि आई टी ए ए 2008 में इलेक्ट्रॉनिक हस्ताक्षर का उल्लेख किया गया है। डिजिटल सिग्नेचर को "इलेक्ट्रॉनिक रिकॉर्ड के प्रमाणीकरण" के रूप में परिभाषित किया गया है, जो अधिनियम द्वारा निर्धारित प्रक्रियाओं के अनुसार होता है। लेकिन 2000 के आई टी अधिनियम में "असममित क्रिप्टो प्रणाली, सार्वजनिक कुंजी अवसंरचना और हैश फ़ंक्शन" का उपयोग शामिल है, इस प्रकार यह केवल सीमित बुनियादी ढांचे पर निर्भर करता है। आई टी अधिनियम, 2008 में इलेक्ट्रॉनिक हस्ताक्षर की शुरूआत; तकनीकी तटस्थता में लाया गया और डिजिटल हस्ताक्षर के साथ-साथ बॉयोमीट्रिक जैसे अन्य रूपों को कवर करके महत्वाकांक्षी को व्यापक बनाया। इसके अलावा, यह समझना महत्वपूर्ण है कि डिजिटल (या इलेक्ट्रॉनिक) हस्ताक्षर हस्ताक्षर की स्कैन कॉपी या डिजिटाइज्ड कॉपी, या हस्ताक्षर के किसी अन्य पारंपरिक रूप के समान नहीं है, यह इलेक्ट्रॉनिक रिकॉर्ड के प्रमाणीकरण से संबंधित प्रक्रियाओं के अनुसार है आई टी आई टी ए ए की धारा 3।

डिजिटल हस्ताक्षर सार्वजनिक कुंजी अवसंरचना का उपयोग करते हैं और इसकी सहायता से बनाए और सत्यापित किए जाते हैं। इन हस्ताक्षरों को एन्क्रिप्ट और डिक्रिप्ट करने के लिए, दो कुंजी की आवश्यकता होती है: सार्वजनिक कुंजी और निजी कुंजी। सार्वजनिक कुंजी को डेटा को एन्क्रिप्ट करने की आवश्यकता होती है जिसे बाद में निजी कुंजी की मदद से डिक्रिप्ट किया जाता है। सार्वजनिक कुंजी साझा की जाती है, लेकिन डिक्रिप्टिंग के लिए उपयोग की जाने वाली निजी कुंजी केवल कुंजी के स्वामी के लिए जानी जाती है। सिस्टम क्रिप्टोग्राफी पर आधारित है।

किसी व्यक्ति के हस्ताक्षर उसकी पहचान का प्रतिनिधित्व करते हैं। यह एक महत्वपूर्ण कानूनी स्थिति रखता है और संबंधित व्यक्ति के इरादे के साथ-साथ पहचान का प्रतिनिधित्व करता है। आई टी अधिनियम ने हाथ से लिखे हस्ताक्षर के समान डिजिटल / इलेक्ट्रॉनिक हस्ताक्षर को वैधानिक दर्जा प्रदान किया। अवधारणा इलेक्ट्रॉनिक हस्ताक्षर, 2001 पर UNCITRAL मॉडल कानून पर आधारित है। ये हस्ताक्षर पारंपरिक हस्ताक्षर के रूप में एक ही उद्देश्य की सेवा करते हैं। डिजिटल दुनिया में, जहाँ इलेक्ट्रॉनिक रिकॉर्ड्स को प्रेषित किया जा रहा है, डिजिटल हस्ताक्षर इलेक्ट्रॉनिक रिकॉर्ड की प्रामाणिकता और वैधता सुनिश्चित करता है। वे पारंपरिक हस्ताक्षर की तुलना में सुरक्षित हैं और जाली नहीं हो सकते। डिजिटल हस्ताक्षर का उपयोग करना कहीं अधिक सुविधाजनक है।

12.13 अपीलीय न्यायाधिकरण

आई टी अधिनियम 2000 साइबर अपीलीय न्यायाधिकरण की स्थापना के लिए प्रदान करता है। अधिनियम में कहा गया है: "केंद्र सरकार, अधिसूचना द्वारा, साइबर विनियम अपीलीय न्यायाधिकरण के रूप में जाने के लिए एक या अधिक अपीलीय न्यायाधिकरणों की स्थापना करेगी।" केंद्र सरकार के पास मामलों और स्थानों को निर्दिष्ट करने की शक्ति भी है। जो न्यायाधिकरण अपने अधिकार क्षेत्र का प्रयोग कर सकता है।



चित्र 12.1: अपीलीय न्यायाधिकरण

- **संविधान:** ट्रिब्यूनल में केवल एक व्यक्ति शामिल होगा: साइबर अपीलीय न्यायाधिकरण के पीठासीन अधिकारी। पीठासीन अधिकारी केंद्र सरकार द्वारा नियुक्त किया जाता है, और उसी के लिए आवश्यक योग्यताएं हैं: वह नियुक्ति के लिए तभी योग्य होगा जब वह "है, या रहा है, या उच्च न्यायालय का न्यायाधीश है; या भारतीय विधिक सेवा का सदस्य है या रहा है और कम से कम कम से कम तीन वर्षों तक उस सेवा के ग्रेड I में पद पर है या रहा है। " पीठासीन अधिकारी 5 वर्ष या जब तक वह 65 वर्ष की आयु (जो भी पहले हो) के लिए पद धारण करेगा। भारत के मुख्य न्यायाधीश के परामर्श से केंद्र सरकार, ट्रिब्यूनल के अध्यक्ष और सदस्यों के चयन के लिए जिम्मेदार होगी। इसके अलावा, "केंद्र सरकार साइबर अपीलीय न्यायाधिकरण को ऐसे अधिकारियों और कर्मचारियों के साथ प्रदान करेगी, जैसा कि सरकार उचित समझ सकती है" और ये लोग पीठासीन अधिकारी के अधीक्षण के तहत काम करेंगे।

- **अधिकार क्षेत्र:** कोई भी पीड़ित व्यक्ति जो नियंत्रक या एक न्यायनिर्णयक अधिकारी के आदेशों से संबंधित है, साइबर अपीलीय न्यायाधिकरण में अपील कर सकता है। संबंधित व्यक्ति द्वारा आदेश प्राप्त होने की तिथि से 45 दिनों के भीतर अपील दायर की जानी है। यदि पीड़ित व्यक्ति ट्रिब्यूनल के फैसले से संतुष्ट नहीं है, तो वह उच्च न्यायालय में अपील दायर कर सकता है।

- **प्रक्रियाएं और शक्तियां:** अधिनियम में कहा गया है कि, "साइबर अपीलीय न्यायाधिकरण सिविल प्रक्रिया संहिता, 1908 द्वारा निर्धारित प्रक्रिया से बाध्य नहीं होगा, लेकिन प्राकृतिक न्याय के सिद्धांतों द्वारा निर्देशित किया जाएगा और, अन्य प्रावधानों के अधीन यह अधिनियम और किसी भी नियम की, साइबर अपीलीय न्यायाधिकरण के पास अपनी प्रक्रिया को विनियमित करने की शक्तियां होंगी, जिसमें उस स्थान पर अपनी बैठकें शामिल होंगी। " ट्रिब्यूनल के पास सिविल कोर्ट के समान शक्ति होगी (जैसा कि सिविल प्रक्रिया संहिता, 1908 के तहत निहित है) जैसे मामलों में अपने कार्यों को पूरा करने के उद्देश्य से: उपस्थिति को बुलाना और लागू करना, रिकॉर्ड की खोज और उत्पादन की आवश्यकता, सबूत प्राप्त करना, समीक्षा करना फैसले, आदि। न्यायाधिकरण के समक्ष कार्यवाही "धारा 193 228 के अर्थ के भीतर एक न्यायिक कार्यवाही होने के लिए, और भारतीय दंड संहिता की धारा 196 और साइबर अपीलीय न्यायाधिकरण के प्रयोजनों के लिए एक समझा जाएगा दंड प्रक्रिया संहिता 1973 की धारा 195 और अध्याय XXVI के प्रयोजनों के लिए दीवानी अदालत। "

12.14 अपराध और साइबर अपराध

दिन प्रतिदिन साइबर अपराधों की संख्या बढ रही है। ऐसी दुर्भावनापूर्ण गतिविधियों को नियंत्रित करने और उपद्रवियों को रोकने के लिए इन मुद्दों को संबोधित करने के प्रावधानों के साथ आई टी अधिनियम पेश किया गया था। आई टी अधिनियम का चैप्टर XI आपराधिक अपराधों पर चर्चा करता है जो जुर्माना या कारावास या दोनों से दंडनीय हैं।

साइबर अपराध एक शब्द है जिसमें कंप्यूटर / इंटरनेट / साइबरस्पेस से जुड़ी आपराधिक गतिविधियां शामिल हैं। यह मूल रूप से कंप्यूटर और / या इंटरनेट का आपराधिक शोषण है। ये अपराध परिष्कृत प्रकृति के हैं और इन अपराधों में कंप्यूटर आमतौर पर उपकरण या लक्ष्य या दोनों होते हैं। इसमें शामिल है:

चित्र 12.2: साइबर अपराध

भारतीय कानून साइबर अपराध की कोई विशेष परिभाषा प्रदान नहीं करता है, लेकिन साइबर सुरक्षा शब्द को परिभाषित किया गया है, इसका अर्थ है "सूचना, उपकरण, कंप्यूटर, कंप्यूटर संसाधन, संचार उपकरण और अनधिकृत पहुंच, उपयोग, प्रकटीकरण से संग्रहीत जानकारी की रक्षा करना, विघटन, संशोधन या विनाश। " भले ही साइबर अपराध को आई टी अधिनियम में परिभाषित नहीं किया गया है, लेकिन कंप्यूटर और साइबरस्पेस से संबंधित अपराधों और अपराधों को आई टी अधिनियम में विस्तार से निपटाया गया है। आई टी अधिनियम में निम्नलिखित अपराधों को शामिल किया गया है:

तालिका 12.1: अपराध और उनकी सजा

अनुभाग	अपराध	सज़ा
धारा 65	कंप्यूटर स्रोत दस्तावेजों के साथ छेड़छाड़	तीन साल तक कारावास, या जुर्माना जो दो लाख रुपये तक हो सकता है, या दोनों के साथ।
धारा 66	कंप्यूटर से संबंधित अपराध	ऐसे शब्द के लिए कारावास जो तीन साल तक या जुर्माना हो सकता है जो पांच लाख रुपये या दोनों के साथ हो सकता है।
धारा 66 बी	बेईमानी से चोरी हुए कंप्यूटर संसाधन या संचार उपकरण प्राप्त करने की सजा	किसी एक अवधि के लिए कारावास जो तीन साल तक या जुर्माना के साथ विस्तारित हो सकती है जो एक लाख रुपये या दोनों के साथ हो सकती है।
धारा 66 सी	पहचान की चोरी के लिए सजा	किसी एक अवधि के लिए कारावास की अवधि जो तीन साल तक बढ़ सकती है और जुर्माना के लिए भी उत्तरदायी होगी जो एक लाख रुपये तक हो सकती है।
धारा 66 डी	कंप्यूटर संसाधन का उपयोग करके प्रतिरूपण द्वारा धोखा देने की सजा	किसी भी एक अवधि के लिए कारावास की अवधि जो तीन साल तक बढ़ सकती है और जुर्माना भी देय होगा जो एक लाख रुपये तक हो सकता है।
धारा 66 ई	निजता के उल्लंघन के लिए सजा	कारावास जो तीन साल तक या जुर्माना दो लाख रुपये से अधिक या दोनों के साथ नहीं हो सकता है।
धारा 66 एफ	साइबर आतंकवाद के लिए सजा	कारावास जो आजीवन कारावास तक हो सकता है
धारा 67	इलेक्ट्रॉनिक रूप में अश्लील सामग्री को प्रकाशित या प्रसारित करने की सजा	दोनों में से किसी एक अवधि के लिए कारावास जो पांच साल तक बढ़ सकती है और जुर्माने के साथ जो दस लाख रुपये तक हो सकती है।

धारा 67 ए	इलेक्ट्रॉनिक रूप में यौन रूप से स्पष्ट कृत्य, आदि युक्त सामग्री के प्रकाशन या प्रसारण के लिए सजा	दोनों में से किसी एक अवधि के लिए कारावास जो सात साल तक बढ़ सकती है और जुर्माने के साथ जो दस लाख रुपये तक हो सकती है।
धारा 67 बी	इलेक्ट्रॉनिक रूप में बच्चों को यौन रूप से स्पष्ट कृत्य आदि में दर्शाती सामग्री को प्रकाशित या प्रसारित करने की सजा	किसी पद के लिए या तो विवरण के कारावास के साथ पहली सजा पर दंडित किया जा सकता है, जो पांच साल तक और जुर्माना जो दस लाख रुपये तक हो सकता है और दूसरे या बाद में दोषी ठहराए जाने की स्थिति में या तो दोनों में से किसी एक के लिए कारावास के साथ जो सात साल तक बढ़ सकता है और जुर्माने के साथ जो कि दस लाख रुपये तक हो सकता है।
धारा 67 सी	बिचौलियों द्वारा सूचना का संरक्षण और प्रतिधारण	एक अवधि के लिए कारावास की सजा जो तीन साल तक बढ़ सकती है और जुर्माना भी हो सकता है।
धारा 68	दिशा-निर्देश देने के लिए नियंत्रक की शक्ति	दो साल से अधिक की अवधि के लिए कारावास या एक लाख रुपये से अधिक का जुर्माना या दोनों नहीं।
धारा 69	किसी भी कंप्यूटर संसाधन के माध्यम से किसी सूचना के अवरोधन या निगरानी या डिक्रिप्शन के लिए निर्देश जारी करने की शक्ति	एक अवधि के लिए कारावास जो सात साल तक बढ़ सकता है और जुर्माना के लिए भी उत्तरदायी होगा।
धारा 69 ए	किसी भी कंप्यूटर संसाधन के माध्यम से किसी भी जानकारी के सार्वजनिक उपयोग के लिए अवरुद्ध करने के लिए निर्देश जारी करने की शक्ति	एक अवधि के लिए कारावास जो सात साल तक बढ़ सकता है और जुर्माना के लिए भी उत्तरदायी हो सकता है।
धारा 69 बी	साइबर सुरक्षा के लिए किसी भी कंप्यूटर संसाधन के माध्यम से ट्रैफ़िक डेटा या जानकारी की निगरानी और एकत्र करने के लिए अधिकृत	एक अवधि के लिए कारावास जो किसी भी अवधि में तीन साल तक बढ़ जाता है और जुर्माना के लिए भी उत्तरदायी होगा।

	करने की शक्ति	
धारा 70	संरक्षित प्रणाली: कोई भी व्यक्ति जो पहुंच को सुरक्षित करता है या धारा 70 के प्रावधान के उल्लंघन में संरक्षित प्रणाली तक सुरक्षित पहुंच का प्रयास करता है।	किसी एक अवधि के लिए किसी भी प्रकार का कारावास जो १० वर्ष तक बढ़ाया जा सकता है और जुर्माना के लिए भी उत्तरदायी होगी।
धारा 70 बी	घटना प्रतिक्रिया के लिए भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल राष्ट्रीय एजेंसी के रूप में कार्य करेगा	एक अवधि के लिए कारावास जो एक वर्ष तक या जुर्माना हो सकता है, जो एक लाख रुपये या दोनों के साथ हो सकता है।
धारा 71	गलत बयानी के लिए जुर्माना	एक अवधि के लिए कारावास जो दो साल तक का हो सकता है, या जुर्माना जो एक लाख रुपये तक हो सकता है, या दोनों के साथ हो सकता है।
धारा 72	गोपनीयता और गोपनीयता के उल्लंघन के लिए दंड	एक अवधि के लिए कारावास जो दो साल तक का हो सकता है, या जुर्माना जो एक लाख रुपये तक हो सकता है, या दोनों के साथ हो सकता है।
धारा 72 ए	कानूनी अनुबंध के उल्लंघन में सूचना के प्रकटीकरण के लिए सजा	एक अवधि के लिए कारावास जो तीन साल तक का हो सकता है, या जुर्माना जो पांच लाख रुपये तक हो सकता है, या दोनों के साथ।
धारा 73	प्रकाशन के लिए जुर्माना [इलेक्ट्रॉनिक हस्ताक्षर] कुछ विशेष वितरण में गलत प्रमाण पत्र	एक अवधि के लिए कारावास जो दो साल तक का हो सकता है, या जुर्माना जो एक लाख रुपये तक हो सकता है, या दोनों के साथ हो सकता है।
धारा 74	कपटपूर्ण प्रयोजन के लिए प्रकाशन	एक अवधि के लिए कारावास जो दो साल तक का हो सकता है, या जुर्माना जो एक लाख रुपये तक हो सकता है, या दोनों के साथ हो सकता है

यह अधिनियम भारत के बाहर किये गए उललंघनों पर भी लागू होगा यदि इसमें भारत से बाहर कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क शामिल है।

12.15 ई-हस्ताक्षर और डिजिटल हस्ताक्षर

भारत का आई टी अधिनियम दो प्रकार के हस्ताक्षरों पर चर्चा करता है:

- इलेक्ट्रॉनिक हस्ताक्षर, और
- डिजिटल हस्ताक्षर

तुलना के लिए महत्वपूर्ण बिंदुओं को संक्षेप में प्रस्तुत किया गया है:

- आई टी अधिनियम 2008 की धारा 2 (1) (टी ए) इलेक्ट्रॉनिक सिग्नेचर को परिभाषित करती है: "इलेक्ट्रॉनिक हस्ताक्षर का अर्थ है कि किसी ग्राहक द्वारा किसी इलेक्ट्रॉनिक रिकॉर्ड का प्रमाणीकरण दूसरी अनुसूची में निर्दिष्ट इलेक्ट्रॉनिक तकनीक के माध्यम से और डिजिटल हस्ताक्षर शामिल हैं"। आई टी अधिनियम 2000 की धारा 2 (1) (पी) डिजिटल हस्ताक्षरों के बारे में बात करती है और इसे "डिजिटल हस्ताक्षर का अर्थ है कि किसी उपभोक्ता द्वारा इलेक्ट्रॉनिक तरीके या प्रक्रिया के माध्यम से सुचना प्रौद्योगिकी अधिनियम के प्रावधानों के अनुसार किसी भी इलेक्ट्रॉनिक रिकॉर्ड का प्रमाणीकरण।
- इलेक्ट्रॉनिक हस्ताक्षर तकनीकी रूप से तटस्थ हैं और अधिनियम इलेक्ट्रॉनिक हस्ताक्षर के निर्माण के लिए किसी विशेष तकनीक को निर्दिष्ट नहीं करता है जबकि डिजिटल हस्ताक्षर विशिष्ट प्रौद्योगिकी-आधारित दृष्टिकोण का अनुसरण करता है। उदाहरण के लिए, हैश फ़ंक्शन का उपयोग, सार्वजनिक कुंजी प्रणाली का उपयोग, आदि।
- इलेक्ट्रॉनिक हस्ताक्षर बायोमेट्रिक हो सकता है, मेल के अंत में टाइप किया गया नाम, पारंपरिक हस्ताक्षर का डिजिटल संस्करण। डिजिटल हस्ताक्षर एन्क्रिप्शन और डिक्रिप्शन के साथ दो-तरह से सुरक्षा प्रणाली का उपयोग करता है।
- डिजिटल हस्ताक्षर इलेक्ट्रॉनिक हस्ताक्षर की तुलना में अधिक प्रामाणिक हैं।
- इलेक्ट्रॉनिक हस्ताक्षर दस्तावेज़ के सत्यापन के उद्देश्य से उपयोग किए जाते हैं जबकि डिजिटल हस्ताक्षर दस्तावेज़ को सुरक्षित करने के लिए उपयोग किए जाते हैं।
- डिजिटल हस्ताक्षरों में अधिकतम तीन वर्षों की वैधता है, जबकि इलेक्ट्रॉनिक हस्ताक्षरों की वैधता पर ऐसी कोई सीमा नहीं है।

12.16 एन्क्रिप्शन

इलेक्ट्रॉनिक रिकॉर्ड के प्रमाणीकरण के लिए डिजिटल हस्ताक्षर का उपयोग किया जाता है। ये हस्ताक्षर की मदद से बनाए और सत्यापित किए जाते हैं। प्रमाणीकरण प्रक्रिया में दो अन्य प्रक्रियाएँ शामिल हैं: एन्क्रिप्शन और डिक्रिप्शन।

एन्क्रिप्शन में सरल संदेशों को सिफर टेक्स्ट में बदलना शामिल है जबकि डिक्रिप्शन की प्रक्रिया कोडेड टेक्स्ट को वास्तविक सरल संदेश में बदल देती है।

एन्क्रिप्शन-डिक्रिप्शन के दो रूप हैं:

- **सममित एन्क्रिप्शन:** यह एन्क्रिप्शन का सबसे बुनियादी प्रकार है जिसमें एन्क्रिप्शन और सूचना के डिक्रिप्शन के उद्देश्य के लिए केवल एक गुप्त कुंजी शामिल है। कुंजी को दोनों के लिए जाना जाता है: प्रेषक और साथ ही संदेश का प्राप्तकर्ता।
- **असममित एन्क्रिप्शन:** संदेश को एन्क्रिप्ट / डिक्रिप्ट करने के लिए इस मामले में दो कुंजी शामिल हैं: सार्वजनिक कुंजी और निजी कुंजी या गुप्त कुंजी। सूचना प्रौद्योगिकी अधिनियम 2000 की धारा 2 (1) (एफ) इस तरह के एन्क्रिप्शन के बारे में बात करती है। एन्क्रिप्शन सार्वजनिक कुंजी का उपयोग करके किया जाता है जो कई के लिए जाना जाता है, लेकिन डिक्रिप्शन केवल उस व्यक्ति द्वारा किया जा सकता है जिसके पास निजी कुंजी है जो केवल प्राप्तकर्ता को ज्ञात है। यह डिजिटल हस्ताक्षर को जालसाजी से बचाने में मदद करता है। असममित एन्क्रिप्शन एक अपेक्षाकृत आधुनिक तरीका है।

बोध प्रश्न ग:

1) एन्क्रिप्शन के विभिन्न प्रकार क्या हैं?

   .....

   .....

   .....

   .....

2) साइबर अपीलीय न्यायाधिकरण के संविधान और अधिकार क्षेत्र की व्याख्या करें।

   .....

   .....

   .....

   .....

3) **रिक्त स्थान भरें:**

   i) डिजिटल हस्ताक्षरों को ..... द्वारा जारी दिशानिर्देशों के तहत भारतीय कानूनी प्रणाली द्वारा मान्यता दी गई है।

   ii) ..... एन्क्रिप्शन का सबसे बुनियादी प्रकार है जिसमें सूचना के एन्क्रिप्शन और डिक्रिप्शन के उद्देश्य के लिए केवल एक गुप्त कुंजी शामिल है।

   iii) ..... संदेशों को एन्क्रिप्ट / डिक्रिप्ट करने के मामले में दो कुंजी शामिल हैं: सार्वजनिक कुंजी और निजी कुंजी या गुप्त कुंजी।

   iv) न्यायधिकरण में केवल एक व्यक्ति शामिल होगा: साइबर अपीलीय ट्रिब्यूनल .....।

12.17 सारांश

सूचना प्रौद्योगिकी अधिनियम, 2000 सूचना प्रौद्योगिकी से संबंधित कानून है। आई टी अधिनियम, 2000 संसद के दोनों सदनों द्वारा आई टी विधेयक को पारित करने का परिणाम

था। यह अधिनियम संयुक्त राष्ट्र आयोग द्वारा अंतर्राष्ट्रीय व्यापार कानून (UNCITRAL) पर आधारित है। यह ई-कॉमर्स और साइबर क्राइम से संबंधित है।

आई टी अधिनियम 2000 के प्रावधानों के तहत, इलेक्ट्रॉनिक रिकॉर्ड के प्रमाणीकरण के उद्देश्य से किसी भी ग्राहक द्वारा डिजिटल हस्ताक्षर का उपयोग किया जा सकता है। इलेक्ट्रॉनिक रिकॉर्ड को "असममित क्रिप्टो प्रणाली और हैश फ़ंक्शन की सहायता से प्रमाणित किया जाता है जो प्रारंभिक इलेक्ट्रॉनिक रिकॉर्ड को एक और इलेक्ट्रॉनिक रिकॉर्ड में परिवर्तित करता है। (सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 2 (1) (पी)) ”

इलेक्ट्रॉनिक माध्यम से होने वाले संचार में कोई ठोस घटक नहीं होता है। इसलिए, जिम्मेदारियों की पुष्टि करना और संघों को परिभाषित करना मुश्किल हो जाता है। आरोपण शब्द का अर्थ है "किसी लेखक, कलाकार या व्यक्ति को किसी कार्य या टिप्पणी को बताने की क्रिया।" आई टी अधिनियम 2000 (धारा 11) दिशानिर्देशों के बारे में बताता है कि इलेक्ट्रॉनिक दस्तावेज़ को उस व्यक्ति को कैसे जिम्मेदार ठहराया जा सकता है, जिनसे यह उत्पन्न हुआ है।

यदि इलेक्ट्रॉनिक रिकॉर्ड के प्रवर्तक ने रिसीवर की ओर से दिए जाने वाले पावती के किसी विशेष मोड को रिकॉर्ड की प्राप्ति के बारे में निर्दिष्ट नहीं किया है, तो पावती दी जा सकती है: "किसी भी संचारक द्वारा पता, स्वचालित या अन्यथा" या "कोई आचरण" पतेदार के लिए, यह इंगित करने के लिए पर्याप्त है कि प्रवर्तक को इलेक्ट्रॉनिक रिकॉर्ड प्राप्त हुआ है। ” उदाहरण के लिए, यदि कोई व्यक्ति किसी मीटिंग के लिए मेल प्राप्त करता है, तो व्यक्ति प्रेषक को एक मेल भेजकर कह सकता है कि जानकारी के लिए धन्यवाद, या एक स्वचालित प्रतिक्रिया भेजें या मीटिंग में शामिल होकर रुचि दिखाता है। ये गतिविधियाँ रिसीवर के छोर से पावती दिखाती हैं।

आई टी अधिनियम 2000 डिजिटल हस्ताक्षर प्रमाणपत्रों के बारे में बात करता है जो एक डिजिटल कुंजी है जो इसे धारण करने वाले व्यक्ति की पहचान को प्रमाणित करता है और प्रमाणित करता है, और प्रमाणित एजेंसियों द्वारा जारी किया जाता है। डिजिटल हस्ताक्षर प्रमाणपत्र इलेक्ट्रॉनिक रिकॉर्ड की प्रामाणिकता की पुष्टि करता है और यह सुनिश्चित करता है कि इसे पारगमन के दौरान नहीं बदला गया है।

12.18 शब्दावली

आरोपण: किसी लेखक, कलाकार या व्यक्ति को किसी कार्य या टिप्पणी को बताने की क्रिया।

डिजिटल हस्ताक्षर: डिजिटल हस्ताक्षर का अर्थ है कि किसी उपभोक्ता द्वारा किसी इलेक्ट्रॉनिक तरीके या प्रक्रिया के अनुसार धारा ३ के प्रावधानों के अनुसार किसी इलेक्ट्रॉनिक रिकॉर्ड का प्रमाणीकरण।

डिजिटल हस्ताक्षर प्रमाणपत्र: डिजिटल हस्ताक्षर प्रमाणपत्र इलेक्ट्रॉनिक रिकॉर्ड की सत्यता की पुष्टि करता है और यह सुनिश्चित करता है कि इसे ट्रांजिट के दौरान बदला नहीं गया है।

इलेक्ट्रॉनिक हस्ताक्षर: किसी ग्राहक द्वारा किसी इलेक्ट्रॉनिक रिकॉर्ड के प्रमाणीकरण को दूसरी अनुसूची में निर्दिष्ट इलेक्ट्रॉनिक तकनीक के माध्यम से और डिजिटल हस्ताक्षर शामिल हैं।

एन्क्रिप्शन: एन्क्रिप्शन में सरल संदेशों को सिफर टेक्स्ट में बदलना शामिल है जबकि डिक्रिप्शन की प्रक्रिया कोडेड टेक्स्ट को वास्तविक सरल संदेश में बदल देती है।

आई टी अधिनियम: इलेक्ट्रॉनिक डेटा इंटरचेंज और इलेक्ट्रॉनिक संचार के अन्य साधनों द्वारा आमतौर पर इलेक्ट्रॉनिक कॉमर्स के रूप में संदर्भित लेनदेन के लिए कानूनी मान्यता प्रदान करने के लिए एक अधिनियम।

12.19 बोध प्रश्नों के उत्तर

क) i) 17.10. 2000 ii) 2008 iii) भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (CERT-In) iv) संचार उपकरण

ख) i. सार्वजनिक कुंजी ii. 43 iii. 45 iv. सत्य

ग) i. आई टी एक्ट 2000 ii. सममित एन्क्रिप्शन iii. असममित एन्क्रिप्शन iv. अधिष्ठाता

12.20 स्वपरख प्रश्न

1. निम्नलिखित पर संक्षिप्त रूप में व्याख्या कीजिए:

i) प्राधिकारी को प्रमाणित करना

ii) अभिदाता के कर्तव्य

iii) अपीलीय न्यायाधिकरण

iv) एन्क्रिप्शन

2. निम्नलिखित में अंतर करें:

i) डिजिटल हस्ताक्षर और इलेक्ट्रॉनिक हस्ताक्षर

ii) आई टी अधिनियम 2000 और आई टी (संशोधन) अधिनियम 2008

3. डिजिटल हस्ताक्षर में एन्क्रिप्शन की प्रक्रिया को समझाइए।

4. इलेक्ट्रॉनिक अभिलेखों की प्राप्ति और प्रेषण से संबंधित प्रक्रिया को समझाएं।

5. साइबर अपराध क्या 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।