अध्याय–6
साइबर अपराध और साइबर कानून का परिचय

साइबर अपराध एक आपराधिक घटना हैं जिसमे कंप्यूटर और नेटवर्क भी शामिल हैं। इसके साथ ही, साइबर अपराध इंटरनेट के माध्यम से आयोजित पारंपरिक अपराध है। उदाहरण के लिए जैसे नफरत अपराध, टेलीमार्केटिंग और इंटरनेट धोखाधड़ी, पहचान की चोरी, और क्रेडिट कार्ड खाता चोरी। जब अवैध गतिविधियां एक कंप्यूटर और इंटरनेट के उपयोग के माध्यम से की जाती है साइबर अपराध माना जाता है। साइबर अपराधों के पारंपरिक रूप हैं जैसे कि चोरी, धोखाधड़ी, जालसाजी, मानहानि और शरारत, आपराधिक गतिविधियों जो सभी भारतीय दंड संहिता के अधीन हैं। कंप्यूटर का दुरुपयोग भी सूचना प्रौद्योगिकी अधिनियम, 2000 से हैं जिसमे नए अपराधों को सम्मिलित कर दिया है।

6.1 साइबर कानून

साइबर कानून कानूनी मान्यता के लिए इलेक्ट्रॉनिक दस्तावेजों और ई–फाइलिंग और ई–कॉमर्स लेन–देन का समर्थन करने के लिए एक रूपरेखा प्रदान करता है और साइबर अपराधों की जांच करने के लिए एक कानूनी रूपरेखा प्रदान करता है। हम दो तरीकों से साइबर अपराधों को वर्गीकृत कर सकते हैं:

एक लक्ष्य के रूप में कंप्यूटर – एक कंप्यूटर का उपयोग करके अन्य कंप्यूटर्स. पर हमला करने के लिए। उदाहरण के लिए जैसे हैकिंग, वायरस हमले, DoS हमले आदि।

एक हथियार के रूप में कंप्यूटर–एक कंप्यूटर के द्वारा दुनिया में अपराध को अंजाम देना। जैसे साइबर आतंकवाद, बौद्धिक संपदा अधिकारों के उल्लंघन, क्रेडिट कार्ड धोखाधड़ी, ईएफटी धोखाधड़ी, अश्लीलता आदि।

6.2 साइबर अपराध के तकनीकी पहलू

(i) अनाधिकृत एक्सेस और हैकिंग

एक्सेस का मतलब कंप्यूटर सिस्टम या कंप्यूटर नेटवर्क के संसाधनों के साथ कम्युनिकेशन करना होता है। व्यक्ति की अनुमति के बिना कंप्यूटर और नेटवर्क उपयोग अनधिकृत एक्सेस कहलाता है। हैकिंग कंप्यूटर और नेटवर्क के अनधिकृत एक्सेस को कहते है। हैकर्स कंप्यूटर पर हमला करने के लिए पहले से तैयार कंप्यूटर प्रोग्राम का उपयोग करते हैं। कुछ हैकर्स व्यक्तिगत मौद्रिक लाभ के

लिए, जैसे क्रेडिट कार्ड की जानकारी चोरी करके विभिन्न बैंक खातों से अपने खाते में पैसे स्थानांतरित करने के उद्देश्य से हैकिंग के कार्य को अंजाम देते हैं।

(ii) वायरस और वर्म हमला

अन्य प्रोग्राम्स को संक्रमित और स्वयं की प्रतियाँ बनाने और अन्य प्रोग्राम्स में फैलने की क्षमता वाले प्रोग्राम को वायरस कहा जाता है। वॉर्म भी एक प्रोग्राम है जो कि वायरस की तरह एक कंप्यूटर से दुसरे कंप्यूटर में फैलने की क्षमता रखता हैं।

(iii) ई–मेल से संबंधित अपराध

ई–मेल स्पूफिंग

ई–मेल स्पूफिंग, संदर्भित करता है कि यह ईमेल है जो एक स्रोत से उत्पन्न किया गया है जबकि यह वास्तव में किसी अन्य स्रोत से भेजा गया था।

ई–मेल स्पैमिंग

ई–मेल स्पैमिंग उपयोगकर्ता – इसी तरह के हजारों ईमेल भेजने के लिए संदर्भित करता है। ईमेल के माध्यम से दुर्भावनापूर्ण कोड भेज जाता हैं। वायरस, आदि एक लिंक भेजकर या किसी अनुलग्नक (अटैचमेंट) के रूप में ईमेल के माध्यम से भेजने के लिए उपयोग किया जाता है।जो डाउनलोड करने पर सिस्टम तो नुकसान पहुँचाता है।

ईमेल बम

ई–मेल बमबारी से मतलब एक विशेष पते पर बार–बार एक समान ईमेल संदेश भेजना होता है।

(iv) एक्सप्लोइट

एक्सप्लोइट सॉफ्टवेयर का एक भाग है जो डेटा का हिस्सा, या एक अनुक्रम का लाभ लेता है। यह कंप्यूटर सॉफ्टवेयर, हार्डवेयर के लिए अनायास ही या अप्रत्याशित व्यवहार जोखिम का कारण बनता है। ऐसे व्यवहार अक्सर एक कंप्यूटर सिस्टम का नियंत्रण प्राप्त कर प्रीविलेज वृद्धि, या डोस (DoS) or डी डोस (DDoS) हमले की इजाजत देता है।

डिनायल ऑफ सर्विस अटैक्स

एक कंप्यूटर संसाधन का लिमिट से अधिक अनुरोध जो कि अधिकृत उपयोगकर्ताओं के लिए सेवा का उपयोग करने से इनकार (डिनायल ऑफ सर्विस अटैक्स) का कारण बनता है। उदाहरण के लिए

1. जिससे वैध नेटवर्क ट्रैफिक की रोकथाम, का प्रयास करता है।
2. दो मशीनों, के बीच कनेक्शन को बाधित करने का प्रयास करता है। जिससे मशीनों की सेवा बाधित होती हैं।
3. किसी खास व्यक्ति के एक सेवा तक पहुँचने से रोकने के लिए प्रयास करता है।
4. सेवा को एक विशिष्ट सिस्टम या व्यक्ति को बाधित करने का प्रयास करता है।

डॉस हमलो के प्रकार

डॉस हमले के तीन बुनियादी प्रकार हैं।

1. सीमित संसाधनों की खपत नेटवर्क बैंडविड्थ (Network Bandwidth), रैम (RAM), सी पी यू टाइम (CPU time) इत्यादि है।
2. विनाश या कॉन्फिगरेशन जानकारी का परिवर्तन करना।
3. भौतिक विनाश या नेटवर्क घटकों का परिवर्तन करना।

डी डोस (DDoS)

डिस्ट्रीब्यूटेड डिनायल ऑफ सर्विस डी डोस (DDoS) आक्रमण इंटरनेट का उपयोग करके कंप्यूटर और उन्हें एक नेटवर्क पर हमला करने के लिए उपयोग में इस्तेमाल किया जा सकता है। इंटरनेट से सैकड़ों या हजारों कंप्यूटर सिस्टम जॉम्बीज में बदलकर और किसी अन्य सिस्टम या वेबसाइट पर हमला करने के लिए इस्तेमाल किया जा सकता है।

(v) अश्लील साहित्य

अश्लील साहित्य का वर्णन यौन उत्तेजना पैदा करने के लिए यौन कार्य पुस्तकों, फिल्मों, आदि के माध्यम से होता हैं। यह इंटरनेट के उपयोग से अश्लील वेबसाइटों, अश्लील वीडियो, चित्र, तस्वीरें, लेखन अश्लील सामग्री डाउनलोड और संचारित की जाती हैं।

(vi) साइबर आतंकवाद

इंटरनेट के उपयोग से लक्षित हमलों सबसे अधिक इन पर जैसे सैन्य प्रतिष्ठानों, विद्युत संयंत्रों, वायु यातायात नियंत्रण, बैंकों, निशान यातायात नियंत्रण, दूरसंचार नेटवर्क, पुलिस, चिकित्सा, आग और बचाव प्रणाली इत्यादि पर किये जाते हैं।

साइबर आतंकवाद कई कारणों के लिए नीचे दिए गए आधुनिक आतंकवादियों के लिए एक आकर्षक विकल्प है।

1. यह पारंपरिक आतंकवादी तरीकों से सस्ता है।
2. साइबर आतंकवाद अधिक पारंपरिक आतंकवादी तरीकों से अनाम है।
3. विविधता और लक्ष्य की संख्या ज्यादा हैं।
4. साइबर आतंकवाद दूरस्थ रुप से किया जा सकता, यह फीचर आतंकवादियों को अपील करता है।
5. साइबर आतंकवाद मे एक बड़ी संख्या में लोगों को सीधे ही प्रभावित करने की क्षमता है।

(vii) बैंकिंग/क्रेडिट कार्ड संबंधित अपराधों

कॉर्पोरेट दुनिया में, इंटरनेट हैकर्स लगातार बैंकिंग और गोपनीय वित्तीय जानकारी तक पहुँच के लिए कंपनी की सुरक्षा से समझौता करने के लिए अवसरों को देख रहे हैं। चोरी, कार्ड जानकारी या नकली क्रेडिट/डेबिट कार्ड का उपयोग आम हैं।

(viii) ई–कॉमर्स / निवेश धोखाधड़ी

बिक्री और निवेश धोखाधड़ी। यह निवेश या ऋण विनती करने के लिए झूठे या छलपूर्ण दावा करता है, या खरीद, उपयोग, या जाली या नकली प्रतिभूतियों को व्यापार के लिए प्रदान करता है। ऑनलाइन व्यक्तियों द्वारा खरीदा माल या सेवाओं को कभी नहीं दिया जाता है। निवेशकों द्वारा असामान्य रूप से उच्च लाभ के वादे इस धोखाधड़ी की योजना में निवेश करने के लिए मोहित करते हैं।

(ix) मानहानि

मानहानि को किसी अन्य व्यक्ति के अधिकार को उसके अच्छा नाम को जानबूझकर अपमानित करने के रूप में समझा जा सकता है। साइबर मानहानि कंप्यूटर और इंटरनेट की मदद से होती है। जैसे किसी अपमानजनक मामले के बारे में किसी वेबसाइट पर प्रकाशित करना या उस व्यक्ति के दोस्तों को अपमानजनक जानकारी युक्त ई–मेल भेजता है।

(x) पहचान की चोरी

पहचान की चोरी तब होती है जब किसी दूसरे की व्यक्तिगत जानकारी की चोरी या धोखाधड़ी, उसके ज्ञान के बिना की जाती है।

(xi) गोपनीयता और गोपनीयता का उल्लंघन

गोपनीयता कब, कैसे और किस हद तक अपने या अपने व्यक्तिगत डेटा को दूसरों के साथ साझा किए जाने को संदर्भित करता है। गोपनीयता के उल्लंघन के अनाधिकृत उपयोग या वितरण जैसी व्यक्तिगत जानकारी मेडिकल रिकॉर्ड, यौन वरीयताओं, वित्तीय स्थिति आदि है।

6.3 कंप्यूटर वायरस

कंप्यूटर वायरस कंप्यूटर कार्यक्रम है जो कि, खुद की प्रतिलिपियाँ उपयोगकर्ता सहमति के बिना अन्य कंप्यूटरों की हार्ड ड्राइव में डालता हैं। कंप्यूटर वायरस बनाना और प्रसार करना एक साइबर अपराध है। वायरस डिस्क स्थान चोरी हो सकता है, व्यक्तिगत जानकारी का उपयोग, कंप्यूटर पर डेटा को बर्बाद या अन्य कंप्यूटर उपयोगकर्ता के लिए व्यक्तिगत संपर्क जानकारी बाहर भेजने के काम आता है। किसी ई–मेल अनुलग्नक के माध्यम से एक कंप्यूटर को संक्रमित करने के लिए वायरस के लिए सबसे आम तरीका है। एक उदाहरण यदि आप किसी अनुलग्नक के साथ एक ईमेल प्राप्त होगा। आप इस अनुलग्नक को खोलें, और वायरस तुरंत आपके कंप्यूटर सिस्टम के माध्यम से फैलता है।

6.4 सामाजिक इंजीनियरिंग

सामाजिक इंजीनियरिंग लोगों में हेर–फेर की कला है जिससे गोपनीय जानकारी पायी जा सकती है। अपराधी सोशल इंजीनियरिंग के माध्यम से व्यक्तियों के बैंक पासवर्ड और बैंक की इनफार्मेशन एक्सेस कर उसके कंप्यूटर पर कन्ट्रोल कर लेते हैं जो की बहुत ही घातक होता हैं। हमें अपनी कोई भी निजी जानकारी और गोपनीय इनफार्मेशन सोशल मीडिया या बैंक की जानकारी फोन पर नहीं देनी चाहिए इसके लिए सबको जागरूक होना आवश्यक हैं।

6.5 फिशिंग

फिशिंग द्वारा इन्टरनेट पर नकली वेबसाइट या ईमेल के माध्यम से इन्टरनेट यूजर्स के साथ की गयी धोखेबाजी को कहते हैं जिसमें आपकी निजी जानकारी को धोखे से चुरा लिया जाता हैं और उसका कही गलत उपयोग किया जा सकता है। अपराधी फिशिंग के माध्यम से नकली ईमेल या सन्देश भेजते है जो किसी रेपुटेड कंपनी, आपकी बैंक, आपकी क्रेडिट कार्ड कंपनी और ऑनलाइन शॉपिंग वेबसाइट्स की तरह मिलते जुलते होते हैं। अगर आप सतर्क नहीं रहते हैं तो आप उसके झांसे में आकर आपकी निजी जानकारिया जैसे आपका नाम, मोबाइल नंबर, क्रेडिट कार्ड नम्वर, बैंक पासवर्ड, बैंक अकाउंट नंबर इत्यादि खो देते हैं।

6.6 सॉफ्टवेयर पायरेसी

सॉफ्टवेयर पायरेसी अनधिकृत नकल, रिप्रोडक्शन, उपयोग, या सॉफ्टवेयर उत्पादों का विनिर्माण है। औसतन हर कंप्यूटर सॉफ्टवेयर के प्रयोग में आने वाली अधिकृत प्रति के लिए, कम से कम एक अनधिकृत प्रतिलिपि उपलब्ध है। सॉफ्टवेयर चोरी सॉफ्टवेयर सहित आप और अंत उपयोगकर्ता समुदाय में सभी को हानि पहुँचाता हैं। चोरी की वजह से विधिवत लाइसेंस उपयोगकर्ताओं के लिए उच्च कीमतों में परिणाम, कम स्तर का समर्थन, और धन और नए उत्पादों के विकास में देरी होती हैं। चोरी सभी सॉफ्टवेयर प्रकाशकों, उनके आकार की परवाह किए बिना हानि पहुँचाता है। सॉफ्टवेयर प्रकाशकों के सॉफ्टवेयर विकास का उपयोग जनता के लिए करने के लिए कई वर्ष खर्च करते हैं।

सॉफ्टवेयर चोरी भी स्थानीय और राष्ट्रीय अर्थव्यवस्थाओं को हानि पहुँचाता हैं। कम राजस्व और कम रोजगार वैध सॉफ्टवेयर की कम बिक्री का परिणाम होता हैं। सॉफ्टवेयर चोरी स्थानीय

सॉफ्टवेयर समुदायों के विकास में अड़चन डालता हैं। कोई सॉफ्टवेयर प्रकाशक बाजार में प्रवेश नहीं करेगा क्योंकि जहां चोरी की दर बहुत अधिक हैं, वहॉ वे उनके विकास की लागत की वसूली नहीं कर सकेंगे।

सॉफ्टवेयर चोरी के प्रकार

ऐसा लगता है कि अवैध सॉफ्टवेयर किसी भी समय कहीं भी, किसी को भी करने के लिए, उपलब्ध है। निम्न कुछ तरीके जिसके द्वारा अवैध प्रतियाँ सॉफ्टवेयर कंप्यूटर उपयोगकर्ताओं के बीच प्रसारित की जाती हैं।

सॉफ्टलिफ्टिंग

सॉफ्टलिफ्टिंग (softloading भी कहा जाता है), चोरी का सबसे सामान्य प्रकार का है जिसमे इसके उपयोग करने के लिए लायसेंस एग्रीमेंट द्वारा अधिकृत नहीं है। सॉफ्टलिफ्टिंग का एक आम रूप है सॉफ्टवेयर की एक प्रतिलिपि लाइसेंस खरीदकर और फिर लायसेंसिंग शर्तों के उल्लंघन में कई कंप्यूटरों पर सॉफ्टवेयर लोड करना शामिल है। कॉलेज परिसरों पर, एक सॉफ्टवेयर प्रोग्राम खोजना दुर्लभ है जो यह सॉफ्टलॉडेड (softloaded) नहीं किया गया है। सॉफ्टलिफ्टिंग व्यवसायों और घरों दोनों में आम है।

हार्ड डिस्क लोडिंग

अक्सर हार्डवेयर डीलरों द्वारा की गई, चोरी के इस फार्म को अंत उपयोगकर्ता के लिए एक कंप्यूटर पर सॉफ्टवेयर की एक अनधिकृत प्रतिलिपि लोड करना शामिल है। यह सौदा खरीदार के लिए आकर्षक होता है, क्योकि डीलर को इसके लिए कोई कीमत देनी नहीं पड़ती हैं। व्यापारी आमतौर पर खरीदार को सॉफ्टवेयर मैनुअल या CD के साथ प्रदान नहीं करता हैं।

किराये पर लेना

सॉफ्टवेयर की एक प्रति अस्थायी उपयोग के लिए किसी कॉपीराइट धारक की अनुमति के बिना, बाहर किराये पर लिया जाना शामिल है। एक वीडियो फिल्म और सॉफ्टवेयर किराये पर लेना लायसेंस एग्रीमेंट का उल्लंघन होता है।

ओ इ एम अनबंडलिंग (OEM unbundling)

किसी प्रोडक्ट के साथ आने वाले सॉफ्टवेर को अलग से बेचना ओ इ एम अनबंडलिंग होता है। चोरी के इस रूप का एक उदाहरण किसी प्राधिकरण के बिना प्रिंटर के लिए ड्रायवर प्रदान करना होता है।

जालसाजी

जालसाजी, एक सॉफ्टवेयर की नकली प्रतियां उत्पादन करना होता हैं जो की ओरिजिनल के समान प्रतीत होती हैं बॉक्स डिजाइन, सीडी, और मैनुअल, सभी के रूप मूल उत्पाद के समान प्रतीत होती हैं। बड़े पैमाने पर माइक्रोसॉफ्ट ऑपरेटिंग सिस्टम के प्रोडक्ट जालसाजी में आते हैं जो बहुतायत से यूज होते हैं। सबसे अधिक, एक सीडी की एक प्रति एक सीडी बर्नर के साथ किया जाता है, और मैनुअल की फोटोकॉपी बनाता है। नकली सॉफ्टवेयर वास्तविक खुदरा मूल्य से कम मूल्य पर बेचा जाता है।

ऑनलाइन चोरी

इंटरनेट चोरी, चोरी के सबसे तेजी से बढ़ता रूप है। ऑनलाइन उपयोगकर्ताओं की बढ़ती संख्या के साथ, और तेजी से बढ़ती कनेक्शन की गति के साथ, इंटरनेट पर सॉफ्टवेयर के आदान प्रदान को व्यापक तौर पर आकर्षित किया है।

6.7 बौद्धिक संपदा

बौद्धिक संपदा (आईपी) मन के विचार, जैसे आविष्कार, साहित्यिक और कलात्मक काम करता है, डिजाइन और प्रतीक, नाम और वाणिज्य में उपयोग किए गए छवि की रचना को संदर्भित करता है। बौद्धिक संपदा सुरक्षित विधि द्वारा, उदाहरण के लिए, जो लोग पहचान या आविष्कार या वित्तीय लाभ कमाने के लिए सक्षम पेटेंट, कॉपीराइट और ट्रेडमार्क उपलब्ध करवाते हैं। नवीन आविष्कारों के हित और जनता के व्यापक हित के बीच सही संतुलन द्वारा, बौद्धिक संपदा प्रणाली का उद्देश्य एक परिवेश में जो रचनात्मकता और नवीनता को बढ़ावा दे जिससे की वो पनप सकते हैं।

बौद्धिक संपदा के प्रकार

कॉपीराइट

कॉपीराइट एक कानूनी शब्द है जो कि रचनाकारों के अधिकारों का वर्णन करने के लिए प्रयोग किया जाता है। कॉपीराइट के अंतर्गत किताबें, संगीत, पेंटिंग, मूर्तिकला और फिल्मों, कंप्यूटर प्रोग्राम, डेटाबेस, विज्ञापन, मैप्स और तकनीकी चित्र द्वारा कवर किया गया हैं।

पेटेंट

पेटेंट एक अनन्य अधिकार है आविष्कार के लिए दी एक पेटेंट मालिक कैसे – या चाहे – आविष्कार दूसरों द्वारा इस्तेमाल किया जा सकता, यह तय करने का अधिकार प्रदान करता है। इस अधिकार के बदले में, पेटेंट स्वामी आविष्कार के बारे में तकनीकी जानकारी प्रकाशित पेटेंट दस्तावेज में सार्वजनिक रूप से उपलब्ध बनाता है।

ट्रेडमार्क

ट्रेडमार्क एक साइन है जो एक उद्यम को अन्य उद्यमों से वस्तुओं या सेवाओं के द्वारा भेद करने में सक्षम होता है। प्राचीन काल मे ट्रेडमार्क जब कारीगरों अपने हस्ताक्षर या मार्क पर अपने उत्पादों डाल करने के लिए उपयोग करते थे।

औद्योगिक डिजाइन

औद्योगिक डिजाइन एक लेख के सजावटी या सौंदर्य पहलू को बताता हैं। एक डिजाइन तीन आयामी सुविधाओं, जैसे आकार, या एक लेख, या द्वि–आयामी सुविधाओं की सतह, जैसे कि पैटर्न, लाइनों, या रंग से मिलकर कर सकते हैं।

भौगोलिक संकेत

भौगोलिक संकेत किसी उत्पाद के ओरिजिन की ओर इंगित करता हैं साथ में उस उत्पाद की विशेषता उसके स्थान से जुडी होती हैं। एक भौगोलिक संकेत मे माल के मूल की जगह का नाम भी शामिल है।

6.8 मेल बम

मेल बम एक विशाल संख्या में एक विशिष्ट व्यक्ति या प्रणाली के लिए भेजे जाने वाला ई–मेल है। मेल की एक बड़ी संख्या प्राप्तकर्ता के सर्वर पर डिस्क स्थान को भरने में कर सकते हैं या, कुछ मामलों में, सर्वर कार्य को रोकने के लिए हो सकता है। मेल बम ना केवल लक्षित लक्ष्य को असुविधा करता हैं बल्कि ये उन सभी को असुविधा प्रदान करता हैं जो सर्वर यूज करते हैं। प्रेषक मेल बम के परस्पर मेल बम या कानूनी कार्रवाई के लिए खुद को उजागर का एक चिंता का विषय होना चाहिए।

महत्वपूर्ण बिंदु

- साइबर अपराध सूचना प्रौद्योगिकी अधिनियम, 2000 के द्वारा संबोधित करते हैं।
- साइबर अपराध एक आपराधिक घटना हैं जिसमे कंप्यूटर और नेटवर्क भी शामिल हैं।
- साइबर अपराधों दो प्रकार के होते है। (i) एक लक्ष्य के रूप में कंप्यूटर (ii) एक हथियार के रूप में कंप्यूटर।
- डिस्ट्रीब्यूटेड डिनायल ऑफ सर्विस (DDoS) आक्रमण इंटरनेट का उपयोग करके कंप्यूटर और उन्हें एक नेटवर्क पर हमला करने के लिए उपयोग में इस्तेमाल किया जा सकता है।
- कंप्यूटर वायरस कंप्यूटर कार्यक्रम है जो कि, खुद की प्रतिलिपियाँ उपयोगकर्ता की सहमति के बिना अन्य कंप्यूटरों की हार्ड ड्राइव में डालता हैं।
- सामाजिक इंजीनियरिंग लोगों में हेर–फेर की कला है जिससे गोपनीय जानकारी पायी जा सकती है।
- फिशिंग द्वारा इन्टरनेट पर नकली वेबसाइट या ईमेल के माध्यम से इन्टरनेट यूजर्स के साथ की गयी धोखेबाजी को कहते हैं जिसमें आपकी निजी जानकारी को धोखे से चुरा लिया जाता हैं।
- सॉफ्टवेयर पायरेसी अनधिकृत नकल, रिप्रोडक्शन, उपयोग, या सॉफ्टवेयर उत्पादों का विनिर्माण है।
- मेल बम एक विशाल संख्या में एक विशिष्ट व्यक्ति या प्रणाली के लिए भेजे जाने वाला ई–मेल है।

अभ्यासार्थ प्रश्न

वस्तुनिष्ठ प्रश्नः

प्रश्न 1. सबसे पहले साइबर अपराध सूचना प्रौद्योगिकी अधिनियम किस वर्ष से जुड़े

अ 1999   ब 2000

स 2001   द 1998

प्रश्न 2. सॉफ्टवेयर चोरी की विधि क्या हैं

अ सॉफ्टलिफ्टिंग   ब हार्ड डिस्क लोडिंग

स जालसाजी   द उपरोक्त सभी

प्रश्न 3. डोस (DoS) का मतलब है

अ सेवा का वितरित इनकार   ब सेवा की अस्वीकृति

स सेवा से वंचित इनकार   द इनमें से कोई नहीं

प्रश्न 4. कंप्यूटर वायरस संक्रमित करता है

अ) मनुष्य   ब) जानवरों

स) कंप्यूटर   द) इनमे से कोई नहीं

अति लघुत्तरात्मक प्रश्न

प्रश्न 1. डी डोस (DDoS) की फुल फॉर्म बताइये।

प्रश्न 2. कॉपीराइट को परिभाषित कीजिये।
प्रश्न 3. सॉफ्टलिफ्टिंग को परिभाषित कीजिये।
प्रश्न 4. पहचान की चोरी को परिभाषित कीजिये।
प्रश्न 5. एक्सप्लोइट को परिभाषित कीजिये।

लघुत्तरात्मक प्रश्न

प्रश्न 1. साइबर अपराध क्या है?
प्रश्न 2. वायरस को परिभाषित कीजिये।
प्रश्न 3. कुछ एंटीवायरस सॉफ्टवेयर का नाम बताइये।
प्रश्न 4. बौद्धिक संपत्ति क्या है?
प्रश्न 5. पेटेंट क्या है?
प्रश्न 6. ऑनलाइन चोरी क्या है?
प्रश्न 7. साइबर आतंकवाद क्या है?
प्रश्न 8. सेवा की अस्वीकृति (DoS) अटैक क्या है?

निबन्धात्मक प्रश्न

प्रश्न 1. फिशिंग विस्तार में समझाइये।
प्रश्न 2. सॉफ्टवेयर चोरी के विभिन्न प्रकार समझाइये।
प्रश्न 3. बौद्धिक संपदा के विभिन्न प्रकार समझाइये।

उत्तरमाला

उत्तर 1: ब　　**उत्तर** 2: द
उत्तर 3: ब　　**उत्तर** 4: स