Quest Journals
Journal of Research in Humanities and Social Science
Volume 12 ~ Issue 6 (2024) pp: 188-201
ISSN(Online):2321-9467
www.questjournals.org

Research Paper

साइबर अपराध एक चुनौती

Ravina Ningawal
Institute of law & legal studies
Sage University Indore

***R**eceived 14 June, 2024; **R**evised 25 June, 2024; **A**ccepted 27 June, 2024 © The author(s) 2024.*
P**ublished with open access at **www.questjournals.org

अमूर्त

इंटरनेट सब कुछ बदल देता है. चीजें कैसी होनी चाहिए, देशों पर कैसे शासन किया जाना चाहिए, कंपनियों को कैसे चलाया जाना चाहिए, शिक्षक कैसे पढ़ाते हैं और बच्चे कैसे सीखते हैं, और यहा तक कि गृहिणियां नए व्यंजन कैसे बनाती हैं, इस बारे में हमारी धारणाएं खराब हो गई हैं। यह हमारे वैचारिक हाँचे को मिधित करता है कि हम दुनिया के बारे में, एक-दूसरे के बारे में और अपने बारे में क्या सोचते हैं। यह एक ही समय में मुक्तिदायक, रोमांचक, चुनौतीपूर्ण और भयानक है.. अधिकांश लोगों के लिए, इंटरनेट रहस्यमय, निषिद्ध, समझ से बाहर और डरावना बना हुआ है यह पेपर साइबर अपराधों साइबर अपराध करने वालों और उनकी प्रेरणाओं का अवलोकन करता है। मैं विभिन्न साइबर अपराधों और रोकथाम, पता लगाने और जांच के दौरान आने बाली अनूठी चुनौतियों और प्रतिक्रिया मुद्दों पर भी विस्तार से चर्चा करना चाहता हूं और इसकी रूपरेखा भी प्रस्तुत करता हूं। भारत के आईटी अधिनियम 2000 की विभिन्न धाराओं ने भी आईटी अधिनियम 2000 में नए प्रावधान का प्रस्ताव रखा।

कीवर्ड

साइवर अपराध, हैकर्स, क्रैकर्स, चाइल्ड पोर्नोग्राफी, वायरस, वॉर्म्स, ट्रोजन, साइबरस्टॉकिंग, साइबर मानहानि, साइबर कानून, भारत, आईटी अधिनियम 2000।

1 परिचय

हम जितनी तेज़ी से डिजिटल दुनिया की ओर बढ़ रहे हैं, ठीक उतनी ही तेज़ी से साइबर अपराध की संख्या में भी वृद्धि हो रही है। जिस गति से तकनीक ने उन्नति की है, उसी गति से मनुष्य की इंटरनेट पर निर्भरता भी बढ़ी है। एक ही जगह पर बैठकर इंटरनेट के ज़रिये मनुष्य की पहुँच, विश्व के हर कोने तक आसान हुई है। आज के समय में हर वो चीज़ जिसके विषय में इंसान सोच सकता है, उस तक उसकी पहुँच इंटरनेट के माध्यम से हो सकती है, जैसे कि सोशल नेटवर्किंग,

ऑनलाइन शॉपिंग, डेटा स्टोर करना, गेमिंग, ऑनलाइन स्टडी, ऑनलाइन जॉब इत्यादि। आज के समय में इंटरनेट का उपयोग लगभग हर क्षेत्र में किया जाता
है। इंटरनेट के विकास और इसके संबंधित लाभों के साथ साइबर अपराधों की अवधारणा भी विकसित हुई है।
वर्तमान में भारत की बड़ी आबादी सोशल नेटवर्किंग साइट्स का उपयोग करती है। भारत में सोशल नेटवर्किंग साइट्स के उपयोग के प्रति लोगों में जानकारी का अभाव है। इसके साथ ही अधिकतर सोशल नेटवर्किंग साइट्स के सर्वर विदेश में हैं, जिससे भारत में साइबर अपराध घटित होने की स्थिति में इनकी जड़ तक पहुँच पाना कठिन होता है।

2.पृष्ठभूमि

साइबर क्राइम क्या है? कुछ विशेषज्ञों का मानना है कि साइबर अपराध उच्च तकनीक वाले कंप्यूटरों द्वारा किए गए सामान्य अपराध से ज्यादा कुछ नहीं है, जहां कंप्यूटर या तो एक उपकरण या लक्ष्य या दोनों है और अन्य विशेषज्ञों का मानना है कि साइवर अपराध अपराध की एक नई श्रेणी है जिसे संबोधित करने के लिए एक व्यापक नए कानूनी ढांचे की आवश्यकता है। उभरती प्रौद्योगिकियों की एक अनूठी प्रकृति और चुनौतियों का एक अनूठा सेट जो पारंपरिक अपराध से निपट नहीं पाता है जैसे कि अधिकार क्षेत्र, अंतर्राष्ट्रीय महयोग, इरादा और अपराधी की पहचान करने में कठिनाई।

2.1 अपराधी हैकर्स और कैकर्स

2.1.1हैकर

एक शब्द है जो आमतौर पर "कंप्यूटर उपयोग करने वालों के लिए प्रयोग किया जाता है जो कंप्यूटर सिस्टम में अनधिकृत पहुंच प्राप्त करने का इरादा रखता है।" आईटी अधिनियम 2000 की धारा 66 के अनुसार कोई भी व्यक्ति जनता या किसी अन्य व्यक्ति को गलत तरीके से हानि या क्षति पहुंचाने के इरादे से या यह जानते हुए कि वह किसी कंप्यूटर संसाधन में मौजूद किसी भी जानकारी को नष्ट कर देता है या हटा देता है या बदल देता है या उसका मूल्य कम कर देता है या उपयोगिता या किसी भी माध्यम से इसे अशुभ रूप से प्रभावित करने वाला हैकर है।

2.1.2 पटाखे

क्रैकर" आपराधिक इरादे वाला एक हैकर है। जार्गन डिक्शनरी के अनुसार इस शब्द का उपयोग "सौम्य" हैकर्स को दुर्भावनापूर्ण हैकर्स से अलग करने के लिए किया जाता है लक्षित कंप्यूटरों को नुकसान पहुंचाएँ। बैंकर दुर्भावनापूर्वक कंप्यूटरों को नुकसान पहुंचाते हैं, सुरक्षित कंप्यूटरों पर मौजूद जानकारी चुराए और उसमें व्यवधान पैदा करें व्यक्तिगत या राजनीतिक उद्देश्यों के लिए नेटवर्क।

3 लोग हैक क्यों करते हैं?

साइबर अपराध को "व्यवसाय के नए रूप" के रूप में प्रस्तुत किया गया है, इसकी विशेषता अपराध के नए रूप, अपराध और उत्पीड़न का व्यापक दायरा और पैमाना, अधिक समय पर प्रतिक्रिया देने की आवश्यकता और चुनौतीपूर्ण तकनीकी और कानूनी जटिलताएँ होंगी। इसलिए हैकिंग में अलग-अलग व्यक्तिगत, राजनीतिक या व्यावसायिक उद्देश्य शामिल होते हैं।

3.1 सक्रियतावाद

हाल के वर्षों में यह देखा गया है कि हैक्टिविस्ट सार्वजनिक वेब पेजों या ई- मेल सर्वरों पर व्यवसाय प्रेरित हमले शुरू करते हैं। हैकिंग समूह और व्यक्ति, या हैसिटिविस्ट एक पते पर भारी मात्रा में ई-मेल भेजकर ईमेल सर्वर को ओवरलोड करते हैं और पेशेवर या व्यावसायिक संदेश भेजने के लिए बेबसाइटों को हैक करते हैं।

3.2 कर्मचारी

एक अध्ययन में पाया गया है कि असंतुष्ट कर्मचारी कंप्यूटर सुरक्षा के लिए सबसे बड़ा खतरा है। कर्मचारी वित्तीय लाभ के लिए गोपनीय जानकारी और व्यापार रहस्य चुराते हैं। सीबीआई (साइबर क्राइम सेल) के अनुसार असंतुष्ट अंदरूनी लोग कंप्यूटर अपराधों का एक प्रमुख योत हैं। अंदरूनी लोगों को अपने लक्षित कंप्यूटरों के बारे में बहुत अधिक ज्ञान की आवश्यकता नहीं है, क्योंकि पीड़ित के सिस्टम के बारे में उनका आंतरिक ज्ञान उन्हें सिस्टम को नुकसान पहुंचाने या सिस्टम डेटा चुराने के लिए अप्रतिबंधित पहुंच की
अनुमति देता है।

3.3 मनोरंजक हैकर्स

"मनोरंजक हैकर्स" चुनौती के रोमांच के लिए या हैकिंग समुदाय में अपने अधिकारों का दावा करने के लिए कंप्यूटर नेटवर्क में सेंध लगाते हैं। मनोरंजक हैकर केवल इंटरनेट से हमले की स्क्रिप्ट और प्रोटोकॉल डाउनलोड करते हैं और उन्हें पीड़ित साइटों के खिलाफ लॉन्च करते हैं, जिनके सिस्टम पर वे हमला कर रहे हैं, उनके बारे में कम जानकारी होती है।

3.4 वेब साइट प्रशासक और वेब पेज।

बेबसाइटें उपयोगकर्ता से बहुत सारी
छिपी हुई पृष्ठभूमि जानकारी भी हासिल करती हैं। दूरस्थ वेवसाइट के बारे में निम्नलिखित महत्वपूर्ण जानकारी निर्धारित कर सकती है।
आगंतुक
एक वह आईपी पता जिससे उपयोगकर्ता वेव साइट तक पहुंच रहा है।
बी। वेब साइट पर पूर्व विज़िट की संख्या, और तारीखें;

सी। उस पृष्ठ का यूआरएल जिसमें उपयोगकर्ता को वेब साइट पर लाने के लिए लिंक था;
डी। उपयोगकर्ता का ब्राउज़र प्रकार और ऑपरेटिंग सिस्टम और संस्करणः
इ) उपयोगकर्ता का स्त्रीन रिज़ॉल्यूशनः
एफा क्या उपयोगकर्ता के कंप्यूटर पर जावास्क्रिप्ट और बीबीस्क्रिप्ट
सक्षम हैं; जी। वर्तमान सत्र में उपयोगकर्ता ने कितने वेव पेज देखे हैं। एन। स्थानीय समय और तारीख और
मै। एफटीपी उपयोगकर्ता नाम और पासवर्ड, यदि कोई हो।

4. साइबर अपराध के प्रकार

लगभग सभी साइबर अपराधों के लिए कंप्यूटर एक अनिवार्य उपकरण है। हालाँकि, जितना अधिक उपकरण इंटरनेट के साथ संचार करने में सक्षम हैं, हैकर्स के पास उपकरणों का शब्वामार है बहुगुणित होने की संभावना
एक कंप्यूटर अक्षरण अपराध में विज्ञापक म्प्यूटर परिणाम देगा है

कंप्यूटर को लक्षित करने वाले अपराधों के सामान्य रूप। अपराधी किशोर, छात्र, पेशेवर या आतंकवादी हो सकते हैं।
कंप्यूटर भी अपराध का उपकरण हो सकता है. साइबर अपराधी पारंपरिक अपराध करने के लिए कंप्यूटर का उपयोग करते हैं। जैसे कि उन्नत रंगीन प्रिंटर का उपयोग करके नकली मुद्रा छापना। कंप्यूटर भी अपराध के लिए आकस्मिक हो सकते हैं, लेकिन फिर भी महत्वपूर्ण हैं क्योंकि उनमें अपराध के सबूत होते हैं। उदाहरण के लिए, बाल पोर्नोग्राफ़र के कंप्यूटर में उत्पादित, स्वामित्व बाली, प्राप्त और/या वितरित बाल पोर्नोग्राफ़ी शामिल हो सकती है। मनी लॉन्ड्रर्स, कागजी लेखांकन रिकॉर्ड पर भरोसा करने के बजाय अपने लॉन्ड्रिग ऑपरेशन का विवरण संग्रहीत करने के लिए कंप्यूटर का उपयोग कर सकते हैं।

4.1 दुर्भावनापूर्ण कोड वायरस, वॉर्म और ट्रोजन

4.1.1 वायरस

वायरस एक प्रोग्राम है जो अन्य कंप्यूटर प्रोग्राम को संशोधित करता है। ये संशोधन सुनिश्चित करते हैं कि संक्रमित प्रोग्राम वायरस की प्रतिकृति बनाता है। सभी वायरस अपने होस्ट को नुकसान नहीं पहुंचाते। वायरस आम तौर पर ई-मेल या संक्रमित डिस्क द्वारा एक कंप्यूटर से दूसरे कंप्यूटर में फैलता है। हालाँकि कोई वायरस किसी अन्य कंप्यूटर को तब तक संक्रमित नहीं कर सकता जब तक प्रोग्राम निष्पादित न हो जाए। वायरस निष्पादन का एक सामान्य तरीका यह है कि जब एक कंप्यूटर उपयोगकर्ता को ई-मेल पर हमला की गई फाइल खोलने के लिए धोखा दिया जाता है, यह सोचकर कि फ़ाइल एक मित्रवत स्रोत से आने वाला एक हानिरहित प्रोग्राम है। वायरस का

सबसे लोकप्रिय उदाहरण मेलिसा बागरस है जिसे मार्च 1999 में लॉन्च किया गया था। मलिसा वायरस माइक्रोसॉफ्ट वर्ड अटैचमेंट में छिपा हुआ था जो प्राप्तकर्ता को किसी परिचित व्यक्ति से आया हुआ प्रतीत होता था। प्रोग्राम ने एक मैक्रो को सक्रिय किया जो माइक्रोसॉफ्ट आउटलुक ई-मेल प्रोग्राम में स्थित पहले पचास ई-मेल पतों को पड़ता है और खुद को पचास पतों पर ई-
मेल करता है। अनुमान लगाया गया था कि इस वायरस में 80 मिलियन डॉलर का नुकसान हुआ है।

4.1.2 वर्म

वर्म एक अकेला प्रोग्राम है जो स्वयं की प्रतिकृति बनाता है। बायरस के विपरीत, एक वर्म किसी फाइल से जुड़े होने की आवश्यकता के बिना पूरे नेटवर्क सिस्टम में अपना रास्ता बता मकता है। उदाहरण के लिए 2001 में आई लव यू वर्म में 10.7 बिलियन अमेरिकी डॉलर का नुकसान होने का अनुमान स्वाया गया था।

4.1.3 ट्रोजन हॉर्स

ट्रोजन हॉर्स एक मासूम दिखने वाला कंप्यूटर प्रोग्राम है जिसमें छिपे हुए कार्य होते हैं। उन्होंने नियमित प्रोग्राम के साथ एक निष्पादित प्रोग्राम को कंप्यूटर की हार्ड ड्राइव पर लोड किया। हालांकि, इनोसेंट प्रोग्राम में एक उप-प्रोग्राम छिपा हुआ है जो एक अनधिकृत कार्य करेगा। ट्रोजन हॉर्स कंप्यूटर सिस्टम में बायरस लाने का सबसे आम तरीका है। उदाहरण के लिए बैंक ऑरिफिस 2000 एक प्रोग्राम है जो किसी अन्य कंप्यूटर के दुरुपयोग और हमले के लिए डिज़ाइन किया गया है

4.2 सेवा से इनकार

सेवा से इनकार ("DoS") एक हमला या घुसपैठ है जिसके विरुद्ध उपयोग के लिए डिज़ाइन किया गया है इंटरनेट से जुड़े कंप्यूटर जिससे एक उपयोगकर्ता दूसरे को सेवा देने से इनकार कर सकता है वैध उपयोगकर्ताओं को बस साइट पर इतना अधिक ट्रैफिक भरकर लाना होगा जितना किसी अन्य को नहीं ऐसा ट्रैफिक जिसमें कोई अन्य ट्रैफिक नहीं जा सकता या बाहर नहीं जा सकता। हैकर नहीं है अनिवार्य रूप से सिस्टम में सेंध लगाने या डेटा डेटा चुराने की कोशिश करना, बल्कि बस केवल हैकर के कारणों से उपयोगकर्ताओं को अपने नेटवर्क तक पहुंचने से रोकें जानता है: बदला, आर्थिक या राजनीतिक लाभ, या सिर्फ सादा गंदापन। उदाहरण के लिए फरवरी 2000 में, एक पंद्रह वर्षीय कनाडाई लड़के को कथित तौर पर "माफियाबॉय" के नाम से जाना जाता था Yahoo, Amazon.com जैसी लोकप्रिय रुचि वाली साइटों को बंद करने के लिए DoS हमला Buy.com और अन्य।

4.3 साइबरस्टॉर्निंग

साइबर स्टॉकिंग तब होती है जब किसी व्यक्ति का ऑनलाइन पीछा किया जाता है। उनकी निजता पर हमला किया जाता है, उनकी हर हरकत पर नजर रखी जाती है। यह उत्पीड़न का एक रूप है. और पीडित के जीवन को बाधित कर सकता है और उन्हें बहुत डरा हुआ और धमकी भरा महसूस करा सकता है। पीछा करना या 'पीछा किया जाना' ऐसी समस्याएं हैं जिनसे बहुत से लोग, विशेषकर महिलाएं परिचित हैं। कभी-कभी ये समस्याएं (उत्पीड़न और पीछा करना) इंटरनेट पर हो सकती हैं। इसे साइवर स्टॉकिंग के नाम से जाना जाता है। इंटरनेट वास्तविक दुनिया को प्रतिबिंबित करता है। इसका मतलब है कि यह वास्तविक जीवन और बास्तविक समस्याओं वाले वास्तविक लोगों को भी दर्शाता है। हालाँकि यह दुर्लभ है, साइबर स्टॉकिंग के मामले सामने आते हैं। साइबर स्टॉकिंग जाम तौर पर उन महिलाओं के साथ होती है, जिनका पुरुष पीछा करते हैं, या बच्चे जिनका पीछा वयस्क शिकारी या पीडोफाइल करते हैं। एक साइबर स्टॉकर को अपने लक्ष्य को खोजने या परेशान करने के लिए अपना घर छोड़ने की ज़रूरत नहीं है, और उसे शारीरिक हिंसा का कोई डर नहीं है क्योंकि उसका मानना है कि साइवरस्पेस में उसे शारीरिक रूप से नहीं हुआ जा सकता है। वह शायद पृथ्वी के दूसरी ओर या पड़ोसी या रिश्तेदार भी हो एकता है। बऔर पीछा करने बाना किसी भी लिंग का हो सकता है।

आमतौर पर, साइबर स्टॉकर का शिकार वेब पर नया होता है, और नेटिकेट और इंटरनेट सुरक्षा के नियमों के बारे में अनुभवहीन होता है। उनका मुख्य लक्ष्य ज्यादातर महिलाएं, बच्चे, भावनात्मक रूप से कमजोर या अस्थिर आदि होते हैं। ऐसा माना जाता है कि 75% से अधिक पीड़ित महिलाएं हैं, लेकिन कभी-कभी पुरुयों का भी पीछा किया जाता है। आँकड़े कल्पित आधार पर है और वास्तविक आँकड़े वास्तव में कभी भी ज्ञात नहीं हो सकते क्योंकि ऐसी प्रकृति के अधिकांश अपराध दर्ज ही नहीं किए जाते हैं।

4.4 वित्तीय अपराध

इसमें धोखाधड़ी, क्रेडिट कार्ड धोखाधड़ी, मनी लॉन्ड्रिंग आदि शामिल होंगे।

एक हालिया मामले का हवाला देते हुए, एक वेबसाइट ने अल्फांसो आम को बहुत कम कीमत पर बेचने की पेशकश की। इस तरह के लेन-देन पर अविश्वास करते हुए, बहुत कम लोगों ने जवाब दिया या वेबसाइट को अपने क्रेडिट कार्ड नंबर उपलब्ध कराए। दरअसल इन लोगों को अल्फांसो आम भेजा गया था. इस वेबसाइट के बारे में बात अब जंगल की आग की तरह फैल गई। देश भर से हजारों लोगों ने प्रतिक्रिया दी और अपने क्रेडिट कार्ड नंबर प्रदान करके आम का ऑर्डर दिया। जो बाद में फर्जी वेबसाइट सावित हुई, उसके मालिक कई क्रेडिट कार्ड नंबर लेकर भाग गए और कार्ड मालिकों को परेशान करते हुए भारी मात्रा में पैसा खर्च करने लगे।

4.5 साइबर पोर्नोग्राफ़ी

इसमें अश्लील वेबसाइटें शामिल होंगी: कंप्यूटर (सामग्री को प्रकाशित करने और प्रिंट करने के लिए) और इंटरनेट (अल्लील चित्र, फोटो, लेख फोटो, लेख आदि को डाउनलोड करने और प्रसारित करने के लिए) का उपयोग करके अधील पत्रिकाएँ तैयार की जाती हैं। साइबर पोर्नोग्राफ़ी से जुड़ी हालिया भारतीय घटनाओं में वायु सेना बालभारती स्कूल मामला शामिल है। दिल्ली के एयर फ़ोर्स बालभारती स्कूल के एक छात्र को उसके सभी सहपाठी उसके चिड़चिड़े चेहरे के कारण चिढ़ाते थे। क्रूर चुटकुलों से तंग आकर, उसने अपने उत्पीड़कों से वापस मिलने का फैसला किया। उसने अपने सहपाठियों और शिक्षकों की तस्वीरें स्कैन कीं, उन्हें नग्न तस्वीरों के साथ रूपांतरित किया और उन्हें एक बेवसाइट पर डाल दिया, जिसे उसने एक मुफ्त वेव होस्टिंग सेवा पर अपलोड किया। ऐसा तब हुआ जब वेवसाइट पर प्रदर्शित कक्षा की लड़कियों में से एक के पिता ने आपत्ति जताई और शिकायत दर्ज कराई पुलिस ने कोई कार्रवाई की.

एक अन्य घटना में, मुंबई में एक स्विस जोड़ा झुग्गी-झोपड़ी के बच्चों को इकट्ठा करता था और फिर उन्हें अलील तस्वीरें दिखाने के लिए मजबूर करता था। फिर वे इन तस्वीरों को विशेष रूप से पीडोफाइल के लिए डिज़ाइन की गई बेबसाइटों पर अपलोड करेंगे। मुंबई पुलिस ने इस जोड़े को पोर्नोग्राफी के आरोप में गिरफ्तार किया है.

4.6 अवैध वस्तुओं की विक्री

इसमें वेबसाइटों, नीलामी वेबसाइटों और बुलेटिन बोर्डों पर जानकारी पोस्ट करके या केवल ईमेल संचार का उपयोग करके 167 पर नशीले पदार्थों, हथियारों और वन्यजीवों आदि की बिक्री शामिल होगी। जैसे ऐसा माना जाता है कि भारत में भी कई नीलामी स्थल शहद के नाम पर कोकीन बेच रहे हैं।

4.7 ऑनलाइन जुआ

लाखों वेबसाइटें हैं; सभी विदेशी सर्वरों पर होस्ट किए गए हैं, जो ऑनलाइन जुए की पेशकश करते हैं। वास्तव में, ऐसा माना जाता है कि इनमें से कई वेबसाइटें वास्तव में मनी लॉन्ड्रिंग का मुखौटा हैं।

4.8 बौद्धिक संपदा अपराध

इनमें सॉफ्टवेयर चोरी, कॉपीराइट उल्लंघन, ट्रेडमार्क उल्लंघन शामिल हैं। कंप्यूटर मोर्न कोड आदि की चोरी

4.9 ईमेल स्पूफिंग

नकली ईमेल वह होती है जो एक स्रोत से उत्पन्न होती प्रतीत होती है लेकिन वास्तव में किसी अन्य स्रोत से भेजी गई होती है। जैसे पूजा का ई-मेल पता pooja@asianlaws.org है। उसका दुश्मन, समीर ने उसके ई-मेल को धोखा दिया और उसके सभी परिचितों को अश्लील संदेश भेजे। चूंकि ई-मेल पूजा की ओर से आए प्रतीत होते हैं, इसलिए उसके दोस्त नाराज हो सकते हैं और जीवन भर के लिए रिश्ते खराब हो सकते

ईमेल स्पूफिंग से आर्थिक नुकसान भी हो सकता है. एक अमेरिकी मामले में, एक किशोर ने कुछ कंपनियों के बारे में गलत जानकारी फैलाकर लाखों डॉलर कमाए, जिनके शेयर उसने कम बेचे थे। यह गलत सूचना शेयर दलालों और निवेशकों को कथित तौर पर रॉयटर्स जैसी समाचार एजेंसियों से फर्जी ईमेल भेजकर फैलाई गई थी, जिन्हें सूचित किया गया था कि कंपनियां बहुत खराब प्रदर्शन कर रही थीं। सज्जाई सामने आने के बाद भी शेयरों की कीमत पहले के स्तर पर नहीं लौटी और हजारों निवेशकों का काफी पैसा डूब गया।

4.10 जालसाजी

नकली मुद्रा नोट, डाक और राजस्व टिकट, मार्कशीट आदि को परिष्कृत कंप्यूटर, प्रिंटर और स्कैनर का उपयोग करके जाली बनाया जा सकता है। भारत भर में कई कॉलेजों के बाहर, दलाल नकली मार्कशीट या यहां तक कि प्रमाणपत्रों की बिक्री का अनुरोध करते हुए पाए जाते हैं। इन्हें कंप्यूटर और उच्च गुणवत्ता वाले स्कैनर और प्रिंटर का उपयोग करके बताया जाता है। वास्तव में, यह एक फलता-फूलता व्यवसाय बनता जा रहा है जिसमें इन फर्जी लेकिन प्रामाणिक दिखने वाले प्रमाणपत्रों के बदले छात्र गिरोहों को हजारों रुपये दिए जाते हैं।

4.11 साइबर मानहानि

ऐसा तब होता है जब कंप्यूटर और/या इंटरनेट की मदद से मानहानि की जाती है। जैसे कोई व्यक्ति किसी वेबसाइट पर किसी के बारे में मानहानिकारक बात् प्रकाशित करता है या उस व्यक्ति के सभी दोस्तों को मानहानिकारक जानकारी वाले ई-मेल भेजता है। हाल ही की एक घटना में. सुरेखा (लोगों के नाम बदल दिए गए हैं) नाम की एक जवान लड़की की शादी सूरज से होने वाली थी। वह बहुत खुश थी क्योंकि अरेंज मैरिज होने के बावजूद उसे लड़का पसंद आ गया था। वह खुले विचारों वाला और खुशमिजाज़ लग रहा था। फिर, एक दिन जब वह सूरज से मिली तो वह चिंतित और थोड़ा

परेशान भी लग रहा था। उसे वास्तव में उससे बात करने में कोई दिलचस्पी नहीं थी। पूछने पर उन्होंने बताया कि, उनके परिवार के सदस्यों को ई-मेल मिल रहे थे जिनमें सुरेखा के चरित्र के बारे में दुर्भावनापूर्ण बातें थीं। उनमें से कुछ ने उन मामलों के बारे में बात की, जो उसके अतीत में थे। उसने उसे बताया 168 कि, उसके माता-पिता उचित रूप से बहुत अच्छे थे परेशान थे और सगाई तोड़ने पर भी विचार कर रहे थे। सौभाग्य से, सूरज वह अपने माता-पिता और अपने घर के अन्य बुजुर्गों से संपर्क करने में सक्षम था
पुलिस ने मेल में लिखी बातों पर आंख मूंदकर विश्वास करने के बजाय। जांच में पता चला कि वो ई-मेल भेजने वाला कोई और नहीं बल्कि सुरेखा का सौतेला पिता था. ये ई-मेल उसने शादी तोड़ने के लिए भेजे थे. लड़की की शादी के कारण वह उसकी संपत्ति पर नियंत्रण खो देता, जिसका वह शादी होने तक संरक्षक था। साइबर मानहानि का एक और चर्चित मामला अमेरिका में हुआ. एक महिला के सभी दोस्त और रिश्तेदार उसके खाते से आने बाले अश्लील ई-मेल संदेशों से परेशान थे। ये मेल संबंधित महिला को उनके दोन्तों के बीच बदनाम कर रहे थे। महिला पोर्नोग्राफी के खिलाफ एक कार्यकर्ता थी। हकीकत में, उनके विचारों से नाखुश और उनके विरोध करने से नाराज लोगों के एक समूह ने इस तरह के गुप्त तरीकों का इस्तेमाल करके उन पर पलटवार करने का फैसला किया था। नकली अश्लील ई-मेल भेजने के अलावा उन्होंने उसके बारे में वेबसाइटें भी डालीं, जो मूल रूप से उसके चरित्र को बदनाम करती थीं और उसके परिवार और दोस्तों को ई-मेल भेजती थीं जिनमें उसे बदनाम करने वाली बातें थी।

4.12 डीप फेक टेक्नोलॉजी

गहरे नकली खतरों को सामाजिक, कानूनी, व्यक्तिगत और पारंपरिक साइबर सुरक्षा में वर्गीकृत किया जा सकता है। डीप फेक के कारण होने वाली समस्याओं के समाधान के लिए आम तौर पर दो समाधान प्रस्तावित किए गए हैं: या तो नकली वीडियो की पहचान करने के लिए प्रौद्योगिकी का उपयोग करें या मीडिया साक्षरता बढ़ाएं।

4.13 उभरते 5जी अनुप्रयोग

5जी नेटवर्क की विशेषताओं से साइबर सुरक्षा का खतरा और भी बदतर हो गया है। 5G को अपनाने का प्रयास कर रहे देश भर के उपभोक्ता, व्यवसाय और कस्बे इसके खतरों का मूल्यांकन करने और उनसे निपटने के लिए अपर्याप्त रूप से सुसज्जित हैं।

एक समाधान के रूप में, उपयोगकर्ताओं के डेटा तक अवैध पहुंच प्राप्त करने और जिन फर्मों के साथ वे काम कर रहे हैं, उनमें उनकी गोपनीयता और विश्वास का दुरुपयोग करने की निरंतर प्रक्रिया में लगे तीसरे पक्ष के हमलावरों की पहचान निर्धारित करना महत्वपूर्ण है।

5. अनोखी चुनौतियों

चूँकि पारंपरिक अपराधी कंप्यूटर प्रौद्योगिकी का उपयोग करेंगे, साइबर अपराध की प्रकृति और विशेषताएं भारत सरकार और नीति निर्माताओं के लिए नई चुनौतियों

* महत्त्वपूर्ण बुनियादी ढाँचे की भेद्यता:

* पावर ग्रिड, परिवहन प्रणाली तथा संचार नेटवर्क साइबर हमलों के प्रति संवेदनशील हैं जो आवश्यक सेवाओं एवं राष्ट्रीय सुरक्षा के लिये खतरा उत्पन्न करते हैं।

* उदाहरणार्थ अक्तूबर 2019 में कुडनकुलम परमाणु ऊर्जा संयंत्र पर साइबर हमले का प्रयास किया गया था जो महत्त्वपूर्ण सूचना बुनियादी ढाँचे के लिये संभावित जोखिमों को उजागर करता है।

* वित्तीय क्षेत्र को खतरा:

* वित्तीय क्षेत्र को साइबर हमलों के उच्च जोखिम का सामना करना पड़ता है, साइबर अपराधी को बैंकों, वित्तीय संस्थानों एवं ऑनलाइन भुगतान प्रणालियों को निशाना बना रहे हैं।

* मार्च 2020 में सिटी यूनियन बैंक के स्विफ्ट सिस्टम (SWIFT System) पर हुए मैलवेयर हमलों के परिणामस्वरूप वित्तीय क्षति, पहचान की चोरी व वित्तीय प्रणाली में लोगों का विश्वास कम हो सकता है।

डेटा उल्लंघन तथा गोपनीयता संबंधी चिंताएँ:

* भारत द्वारा डिजिटल अर्थव्यवस्था में परिवर्तित होने के साथ वैयक्तिक तथा सरकारी डेटा के ऑनलाइन भंडारण में वृद्धि से डेटा उल्लंघन का खतरा बढ़ जाता है।

* मई 2021 में कॉमन एडमिशन टेस्ट (CAT) डेटा लीक जैसे संवेदनशील डेटा उल्लंघनों का सुरक्षा और गोपनीयता पर हानिकारक प्रभाव पड़ सकता है।

* साइबर जासूसी:

* भारत को साइबर जासूसी/गुप्तचरी संबंधी गतिविधियों का सामना करना पड़ता है जिसका उद्देश्य गोपनीय जानकारी चुराना एवं रणनीतिक लाभ हासिल करना है।

* उदाहरणार्थ वर्ष 2020 में घटित ऑपरेशन साइडकॉपी, जहाँ एक पाकिस्तानी थ्रेट एक्टर ने मैलवेयर और फिशिंग ईमेल के माध्यम से भारतीय सैन्य एवं राजनयिक कर्मियों को लक्षित किया था।

* एडवांस्ड परसिस्टेंट थ्रेट्स-APTs:

* APTS का आशय जटिल एवं दीर्घकालिक साइबर हमलों से है जो एक चुनौती पेश करते हैं क्योंकि उनका पता लगाना एवं उनका मुकाबला करना मुश्किल होता है।

* आपूर्ति शृंखला की कमज़ोरियाँः

* सरकार एवं व्यवसायों द्वारा उपयोग किये जाने वाले सॉफ्टवेयर अथवा हार्डवेयर घटकों में कमज़ोरियाँ आपूर्ति शृंखला में कमज़ोरियों को जन्म देती हैं।

* दिसंबर 2020 में सोलरविंड्स पर वैश्विक साइबर हमले ने राष्ट्रीय सूचना विज्ञान केंद्र (NIC) एवं इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY) सहित भारतीय संगठनों को प्रभावित किया।

6. भारत में साइबर कानून

मई 2000 में, भारतीय संसद के दोनों सदनों ने सूचना प्रौद्योगिकी विधेयक पारित किया। विधेयक को अगस्त 2000 में राष्ट्रपति की सहमति प्राप्त हुई और इसे सूचना प्रौद्योगिकी अधिनियम, 2000 के रूप में जाना गया। साइबर कानून आईटी अधिनियम, 2000 में निहित हैं। इस अधिनियम का उद्देश्य भारत में ई-कॉमर्स के लिए कानूनी बुनियादी ढांचा प्रदान करना है।

और साइबर कानूनों का भारत में ई-व्यवसायों और नई अर्थव्यवस्था पर बड़ा प्रभाव पड़ता है। इसलिए, यह समझना महत्वपूर्ण है कि आईटी अधिनियम, 2000 के विभिन्न दृष्टिकोण क्या हैं और यह क्या प्रदान करता है।

सूचना प्रौद्योगिकी अधिनियम, 2000 का उद्देश्य कानूनी ढांचा प्रदान करना भी है ताकि सभी इलेक्ट्रॉनिक रिकॉर्ड और इलेक्ट्रॉनिक माध्यमों से की जाने वाली अन्य गतिविधियों को कानूनी पवित्रता प्रदान की जा सके। अधिनियम में कहा गया है कि जब तक अन्यथा सहमति न हो, अनुबंध की स्वीकृति संचार के इलेक्ट्रॉनिक माध्यमों द्वारा व्यक्त की जा सकती है और इसकी कानूनी वैधता और प्रवर्तनीयता होगी। अधिनियम की कुछ मुख्य बातें नीचे सूचीबद्ध हैं:

* **अधिनियम का अध्याय** ।। विशेष रूप से निर्धारित करता है कि कोई भी ग्राहक अपने डिजिटल हस्ताक्षर लगाकर इलेक्ट्रॉनिक रिकॉर्ड को प्रमाणित कर सकता है। इसमें आगे कहा गया है कि कोई भी व्यक्ति ग्राहक की सार्वजनिक कुंजी का उपयोग करके इलेक्ट्रॉनिक रिकॉर्ड को सापापित कर सकता है।

अधिनियम का अध्याय-III इलेक्ट्रॉनिक गवर्नेंस के बारे में विवरण देता है और अन्य बातों के साथ-साथ यह भी प्रदान करता है कि जहां कोई भी कानून यह प्रदान करता है कि जानकारी या कोई अन्य मामला लिखित या टाइप किए गए या मुद्रित रूप में होगा, तो, ऐसे कानून में किसी बात के होते हुए भी, ऐसी आवश्यकता होगी पछि ऐसी जानकारी वा मागता है तो संतुर माना जाएगा

इलेक्ट्रॉनिक रूप में प्रस्तुत या उपलब्ध कराया गया,

* सुलभ ताकि वाद के संदर्भ के लिए उपयोग किया जा सके उक्त अध्याय में डिजिटल हस्ताक्षर की कानूनी मान्यता का भी विवरण दिया गया है।

उक्त अधिनियम का अध्याय-IV प्रमाणन प्राधिकारियों के विनियमन के लिए एक योजना देता है। अधिनियम में प्रमाणन प्राधिकारियों के एक नियंत्रक की परिकल्पना की गई है जो प्रमाणन प्राधिकारियों की गतिविधियों पर पर्यवेक्षण का कार्य करेगा, साथ ही प्रमाणन प्राधिकारियों को नियंत्रित करने वाले मानकों और शर्तों को निर्धारित करेगा और साथ ही डिजिटल हस्ताक्षर प्रमाणपत्रों के विभिन्न रूपों और सामग्री को निर्दिष्ट करेगा। अधिनियम विदेशी प्रमाणन प्राधिकारियों को मान्यता देने की आवश्यकता को पहचानता है और यह डिजिटल हस्ताक्षर प्रमाणपत्र जारी करने के लिए लाइसेंस जारी करने के विभिन्न प्रावधानों का विवरण देता है।

अधिनियम का अध्याय-V सुरक्षित इलेक्ट्रॉनिक रिकॉर्ड और सुरक्षित डिजिटल हस्ताक्षर का विचार देता है

अधिनियम का अध्याय-VI प्रमाणन प्राधिकारियों के नियम, विनियम, कार्य और प्रक्रिया देता है

अधिनियम का अध्याय-VII डिजिटल हस्ताक्षर प्रमाणपत्रों से संबंधित चीजों की योजना के बारे में विवरण देता है। उक्त अधिनियम में अभिदात्ताओं के कर्तव्य भी निहित

- अधिनियम का अध्याय-VIII ग्राहकों के कर्तव्यों के बारे में बात करता है।

* **उक्त अधिनियम का अध्याय-IX** विभिन्न अपराधों के लिए दंड और न्यायनिर्णयन के बारे में बात करता है। कंप्यूटर, कंप्यूटर सिस्टम आदि को नुकसान पहुंचाने पर जुर्माने के तौर पर मुआवजे के रूप में अधिकतम 500 रुपये तक का जुर्माना तय किया गया है। प्रभावित व्यक्तियों को 1,00,00,000 रु. यह अधिनियम किसी ऐसे अधिकारी की नियुक्ति की बात करता है जो भारत सरकार के निदेशक या राज्य सरकार के समकक्ष अधिकारी के रैंक से नीचे का न हो, एक न्यायनिर्णयन अधिकारी के रूप में जो निर्णय करेगा कि क्या किसी व्यक्ति ने उक्त अधिनियम के किसी भी प्रावधान का उल्लंघन किया है। या उसके तहत बनाए गए नियम। उक्त न्यायनिर्णायक अधिकारी को सिविल न्यायालय की शक्तियां प्रदान की गई हैं।

अधिनियम का अध्याय-X साइवर रेगुलेशन अपीलीय न्यायाधिकरण की स्थापना की बात करता है, जो एक अपीलीय निकाय होगा जहां निर्णय अधिकारियों

द्वारा पारित आदेशों के खिलाफ अपील को प्राथमिकता दी जाएगी। अधिनियम का अध्याय-XI विभिन्न अपराधों के बारे में बात करता है और उक्त

अपराधों की जांच केवल एक पुलिस अधिकारी द्वारा की जाएगी जो पुलिम उपाधीक्षक के पद से नीचे का न हो। इन अपराधों में कंप्यूटर स्रोत दस्तावेजों के साथ छेड़छाड़, इलेक्ट्रॉनिक रूप में अलील जानकारी का प्रकाशन और हैकिंग शामिल है।

* अधिनियम साइबर विनियम सलाहकार समिति के गठन का भी प्रावधान करता है, जो सरकार को किसी भी नियम के संबंध में, या उक्त अधिनियम से जुड़े किसी अन्य उद्देश्य के लिए सलाह देगी। उक्त अधिनियम में भारतीय दंड संहिता, 1860, भारतीय साक्ष्य अधिनियम, 1872, वैकर्स बुक्स साक्ष्य अधिनियम, 1891, भारतीय रिजर्व बैंक अधिनियम, 1934 में संशोधन का भी प्रस्ताव है ताकि उन्हें आईटी अधिनियम के प्रावधानों के अनुरूप बनाया जा सके।

7. साइबर कानून के फायदे

आईटी अधिनियम 2000 पुराने कानूनों को बदलने का प्रयास करता है और इससे निपटने के तरीके प्रदान करता है साइबर अपराध। हमें ऐसे कानूनों की जरूरत है ताकि लोग खरीद-फरोख्त कर सकें दुरुपयोग के डर के बिना क्रेडिट कार्ड के माध्यम से नेट पर। अधिनियम बहुत कुछ प्रदान करता है- कानूनी हांचे की आवश्यकता है ताकि जानकारी कानूनी प्रभाव, वैधता या से बंचित न हो प्रवर्तनीयता, केवल इस आधार पर कि यह इलेक्ट्रॉनिक रिकॉर्ड के रूप में है।

इलेक्ट्रॉनिक रिकॉर्ड के माध्यम से किए गए लेनदेन और संचार में वृद्धि को देखते हुए, अधिनियम सरकारी विभागों को डिजिटल प्रारूप में आधिकारिक दस्तावेजों को दाखिल करने, बनाने और बनाए रखने को स्वीकार करने के लिए सशक्त बनाने का प्रयास करता है। अधिनियम ने डिजिटल हस्ताक्षर के माध्यम से इलेक्ट्रॉनिक रिकॉर्ड/संचार के प्रमाणीकरण और उत्पत्ति के लिए एक कानूनी ढांचा भी प्रस्तावित किया है।

* भारत में ई-कॉमर्स के दृष्टिकोण से, आईटी अधिनियम 2000 और इसके प्रावधानों में कई सकारात्मक पहलू शामिल हैं। सबसे पहले, ई-व्यवसायों के लिए इन प्रावधानों का निहितार्थ यह होगा कि ईमेल अब हमारे देश में संचार का एक वैध और कानूनी रूप होगा जिसे अदालत में विधिवत प्रस्तुत और अनुमोदित किया जा सकता है।

* कंपनियां अब अधिनियम द्वारा प्रदान किए गए गए कानूनी बुनियादी ढांचे का उपयोग करके इलेक्ट्रॉनिक वाणिज्य करने में सक्षम होंगी।

* अधिनियम में डिजिटल हस्ताक्षर को कानूनी वैधता और मंजूरी दी गई है।

* यह अधिनियम डिजिटल हस्ताक्षर प्रमाणपत्र जारी करने के लिए प्रमाणन प्राधिकारी बनने के व्यवसाय में कॉर्पोरेट कंपनियों के प्रवेश के लिए दरवाजे खोलता है।

अधिनियम अब गरकार की बेय पर जधिसूचना जारी करने की अनुमति देता है जिसने है- गवर्नेंस की शुरुआत होती है।

- अधिनियम कंपनियों को उपयुक्त सरकार के स्वामित्व या नियंत्रण वाले किसी भी कार्यालय, प्राधिकरण, निकाय या एजेंसी के साथ इलेक्ट्रॉनिक रूप में किसी भी फॉर्म, आवेदन या किसी अन्य दस्तावेज़ को ऐसे इलेक्ट्रॉनिक फॉर्म के माध्यम से दाखिल करने में सक्षम बनाता है जो उपयुक्त सरकार द्वारा निर्धारित किया जा सकता है।

* आईटी अधिनियम सुरक्षा के महत्वपूर्ण मुद्दों को भी संबोधित करता है. जो इलेक्ट्रॉनिक लेनदेन की सफलता के लिए बहुत महत्वपूर्ण हैं। अधिनियम ने सुरक्षित डिजिटल हस्ताक्षर की अवधारणा को एक कानूनी परिभाषा दी है जिसे बाद की तारीख में सरकार द्वारा निर्धारित सुरक्षा प्रक्रिया की एक प्रणाली के माध्यम से पारित करना आवश्यक होगा।

आईटी अधिनियम, 2000 के तहत, अब कॉरपोरेट्स के लिए वैधानिक उपाय करना संभव होगा यदि कोई उनके कंप्यूटर सिस्टम या नेटवर्क में सेंध लगाता है और नुकसान पहुंचाता है या डेटा कॉपी करता है। अधिनियम द्वारा प्रदान किया गया उपाय मौद्रिक क्षति के रूप में है, जो रुपये से अधिक नहीं

8. आईटी एक्ट 2000 में प्रस्तावित बदलाव

यह पाया गया कि निम्नलिखित के लिए प्रावधान होना चाहिए -

एक। ट्रैप और ट्रेस आदेश. नए आईटी अधिनियम में ऐसा कानून बनाया जाना चाहिए जिससे साइबर जांचकर्ताओं के लिए "ट्रैप एंड ट्रेस" बॉर्डर प्राप्त करना आसान हो जाए। "पैकेट की पहचान करने के लिए आने वाले आईपी पैकेट को पकड़ने के लिए ट्रैप और ट्रेस डिवाइस का उपयोग किया जाता है उत्तात्ति जिस आसानी से हैकर्स अपने वास्तविक मूल को "स्यूफ" करने में सक्षम होते हैं, वायरस, DoS या हैकिंग हमले के पथ को फिर से बनाने का सबसे प्रभावी तरीका ट्रैपिंग उपकरणों की एक श्रृंखला का पालन करना है जो मूल दुर्भावनापूर्ण पैकेटों को आते ही लॉग कर लेते हैं। प्रत्येक व्यक्तिगत राउटर या सर्वर पर। एक मामले में एकल टेलीफोन कंपनी के मामले में, जांचकर्ताओं के लिए यह अपेक्षाकृत आसान हो गया है ट्रैप और ट्रेस ऑर्डर प्राप्त करें लेकिन आज एक संचार किया जा रहा है

कई अलग-अलग (आईएसपी), एक या अधिक टेलीफोन कंपनी या एक या अधिक सेल कंपनी द्वारा और बहुत जल्द एक या अधिक उपग्रह कंपनी द्वारा। एक बार जब मार्ग का खंड अदालत के अधिकार क्षेत्र से बाहर चला जाता है, तो जांचकर्ताओं को अगले क्षेत्राधिकार में जाना होगा और अगले खंड के लिए जाल और ट्रेस आदेश के लिए अनुरोध दायर करना होगा। नया कानून किसी ऑनलाइन संचार को शुरू से अंत तक पूरी तरह से ट्रैक करने के लिए एकल आदेश जारी

करने को अधिकृत करेगा। बी। हमने नए कानून का प्रस्ताव रखा है जो पंद्रह वर्ष और उससे अधिक उम्र के युवा अपराधियों को गंभीर कंप्यूटर अपराध में अपराध के लिए पात्र बनाता है। सी। साइबर कैफे, कंप्यूटर प्रशिक्षण केंद्र और अन्य संस्थान जहां कंप्यूटर प्रशिक्षण का माध्यम है, उन्हें किसी अधिनियम के तहत शामिल किया जाना चाहिए।

निष्कर्ष - भारत इंटरनेट का तीसरा सबसे बड़ा उपयोगकर्ता है और हाल के वर्षों में साइबर अपराध कई गुना बढ़ गए हैं। साइबर सुरक्षा उपलब्ध कराने के लिये सरकार की ओर से कई कदम उठाए गए हैं। कैशलेस अर्थव्यवस्था को अपनाने की दिशा में बढ़ने के कारण भारत में साइबर सुरक्षा सुनिश्चित करना आवश्यक है। डिजिटल भारत कार्यक्रम की सफलता काफी हद तक साइबर सुरक्षा पर निर्भर करेगी अतः भारत को इस क्षेत्र में तीव्र गति से कार्य करना होगा। वहीं दूसरी ओर सोशल मीडिया ने अभिव्यक्ति की स्वतंत्रता के अधिकार को नया आयाम दिया है, आज प्रत्येक व्यक्ति बिना किसी डर के सोशल मीडिया के माध्यम से अपने विचार रख सकता है और उसे हज़ारों लोगों तक पहुँचा सकता है, परंतु सोशल मीडिया का सावधानीपूर्वक उपयोग ही हमें ऑनलाइन ठगी तथा साइबर अपराध के गंभीर खतरों से बचा सकता है।

प्रश्न- साइबर अपराध से आप क्या समझते हैं? साइबर अपराध को रोकने में सरकार के द्वारा किये जा रहे प्रयासों का विश्लेषण कीजिये।

1. एटर, बी. (2001), ई-क्राइम की फोरेंसिक चुनौतियों, करंट कमेंटरी नंबर 3 ऑस्ट्रेलेशियन सेंटर फॉर पुलिसिंग रिमर्च, एडिलेड।

2. एटर बी. (2002), पुलिसिंग साइबरस्पेस की चुनौतियाँ, नेटसेफ में प्रस्तुतः 2 समाज, सुरक्षा और इंटरनेट सम्मेलन, ऑकलैंड, न्यूज़ीलैंड। 3. एरिक जे. सिनरोड और विलियम पी रेली, साइबर क्राइम्स (2000), ए प्रैक्टिकल अप्रोच संघीय कंप्यूटर अपराध कानूनों के अनुप्रयोग के लिए, सांता क्लारा विश्वविद्यालय।

खंड 16. संख्या

2.4. गैंगलर, वी. (2001), वायरस कॉस्ट हिट $20 बिलियन, द ऑस्ट्रेलियन, 11 सितंबर पृष्ठ 36। 5. आईटी अधिनियम 2000.

6. साइवर स्टॉकिंग इंडिया, www. Indianchild.comi

7. साइबर अपराध सीबीआई के लिए एक नई चुनौती, www.rediff.com, 12 मार्च, 2003 12:27 IST

8. रिचर्ड रेज़मैन और पीटर ब्राउन (1999), वाइरस वर्क्स, और अन्य विनाशकारी कर एन, बाई. गुन. जे.