भारत में साइबर अपराध

डॉ0 दिलीप कुमार मौर्य

[1] असिस्टेंट प्रोफेसर, श्याम प्रसाद मुखर्जी राजकीय महाविद्यालय, फाफामऊ, प्रयागराज, भारत

Correspondence Author: डॉ0 दिलीप कुमार मौर्य

Received 14 Dec 2022; Accepted 25 Jan 2023; Published 4 Feb 2023

सारांश

ग्लोबल विलेज के लिए इंटरनेट टाउन स्क्वायर बनता जा रहा है। हम सभी जब इंटरनेट से जुड़े हुए हैं, जैसे कि एक विशाल मस्तिष्क में न्यूरॉन्स वास्तव में आज इंटरनेट लोगों के लिए वरदान और अभिशाप बन गया हे। इसके अलावा, इंटरनेट की बढ़ती आवश्यकता के साथ हमारी जानकारी और डेटा की सुरक्षा भी एक चुनौती बन गई है। चाहे आप एक कंपनी के मालिक हों या यदि आप केवल इंटरनेट के अभ्यस्त उपयोगकर्ता हैं, तो आपका इस बात की जानकारी होनी चाहिए कि खतरा, जोखिम और साइबर अपराध को कैसे कम किया जाए।

प्रौद्योगिकी की प्रगति ने मनुष्य को अपनी सभी जरूरतों क लिए इंटरनेट पर निर्भर बना दिया है। इंटरनेट ने मनुष्य को एक ही स्थान पर बैठकर सब कुछ आसानी से उपलब्ध करा दिया है। सोशल नेटवर्किंग, ऑनलाइन शार्पिंग, डाटा स्टोर करना, गेमिंग, ऑनलाइन पढ़ाई, ऑनलाइन जॉब, हर वो संभव काम जो मनुष्य सोच सकता है, इंटरनेट के माध्यम से किया जा सकता है। इंटरनेट का उपयोग लगभग हर क्षेत्र में किया जाता है। इंटरनेट के विकास और इससे संबंधित लाभों के साथ साइबर अपराध की अवधारणा भी विकसित हुई। साइबर अपराध विभिन्न रूपों में किये जाते हैं। कुछ साल पहले, इंटरनेट के माध्यम से होने वाले अपराधों के बारे में जागरूकता की कमी थी। साइबर अपराधों के मामले में भारत भी अन्य देशों से पीछे नहीं है, जहाँ साइबर अपराध की घटनायें दिन–ब–दिन बढ़ती जा रही है।

मूलशब्द: साइबर सुरक्षा, इंटरनेट

परिचय

साइबर अपराध अपराधिक गतिविधि है जो या तो कम्प्यूटर, कम्प्यूटर नेटवर्क या नेटवर्क डिवाइस को उपयोग करता है। अधिकांश साइबर अपराध साइबर अपराधियों या हैकरों द्वारा किये जाते हैं जो पैसा कमाना चाहते हैं। साइबर अपराध व्यक्तियों या संगठनों द्वारा किया जाता है। कुछ साइबर अपराधी संगठित होते हैं, उन्नत तकनीकों का उपयोग करते हैं और अत्यधिक तकनीकी रूप से कुशल होते हैं। साइबर अपराध का उद्देश्य लाभ के अलावा अन्य कारणों से कम्प्यूटर को नुकसान पहुँचाना होता है। ये राजनीतिक या व्यक्तिगत हो सकते हैं। साइबर अपराध कम्प्यूटर या डिजिटल उपकरणों से जुड़ा एक खतरनाक अपराध है, जिसमें कम्प्यूटर या तो अपराध का लक्ष्य हो सकता है या अपराध का सबूत हो सकता है। साइबर अपराध को मूल रूप से इंटरनेट पर होने वाली किसी भी आपराधिक गतिविधि के रूप में परिभाषित किया गया है। धोखाधड़ी, मैलवेयर जैसे वायरस, पहचान की चोरी और साइबर स्टॉकिंग जैसे कई उदाहरण है। वर्तमान परिवेश में, चूँकि अधिकांश सूचना प्रसंस्करण सूचना प्रौद्योगिकी के उपयोग पर निर्भर करता है, इसलिए साइबर गतिविधियों का नियंत्रण, रोकथाम और जांच संगठनों, सरकर की एजेंसियों और व्यक्तियों की सफलता के लिए महत्वपूर्ण है। सरकार और व्यावसायिक उद्यमों द्वारा अत्यधिक कौशल वाले साइबर अपराध विशेषज्ञ की खरीद और रख–रखाव को बढ़ा–चढ़ा कर नहीं किया जा सकता है। इससे पहले, साइबर अपराध मुख्य रूप से व्यक्तियों या छोटे समूहों द्वारा किया जाता था। वर्तमान में, यह देखा गया है कि अत्यधिक जटिल साइबर अपराधी नेटवर्क वैश्विक स्तर पर व्यक्तियों को वास्तविक समय में अपराध करने के लिए एक साथ लाते हैं। आज साइबर अपराध करने वाले अपराधी अहंकार या विशेषज्ञता से प्रेरित नहीं होते हैं। इसके बजाय, वे तुरंत लाभ हासिल करने के लिए अपने ज्ञान का उपयोग करना चाहते हैं। वे अपनी क्षमता का उपयोग लोगों को छीनने, धोखा देने और उनका शोषण करने के लिए कर रहे हैं, क्योंकि उन्हें बिना मेहनत किए पैसा कमाना आसान लगता है। साइबर क्राइम आज एक बड़ा खतरा बन गया है।

साइबर अपराध के प्रकार

1. फ़िशिंग घोटाले

फ़िशिंग स्कैम स्कैमर्स द्वारा आपकी व्यक्तिगत जानकारी जैसे बैंक खाता नंबर, पासवर्ड और क्रेडिट कार्ड नंबर देने के लिए आपको बरगलाने का प्रयास है। ये स्कैमर आपके बैंक, टेलीफोन कम्पनी या यहाँ तक कि इंटरनेट प्रदाता जैसे वैध व्यवसाय होने का नाटक करते हुए, ई–मेल, टेक्स्ट संदेश, फोन कॉल या यहाँ तक कि सोशल मीडिया के माध्यम से आपसे सीधे सम्पर्क करेंगे। स्कैमर आपसे उन्हें अपने विवरण पर अपडेट करने के लिए कह सकता है ताकि वे अपने सिस्टम को रिफ्रेश कर सकें, वे आपसे एक सर्वेक्षण भरने के लिए भी कह सकते हैं क्योंकि आपके पास अंत में पुरस्कार जीतने का मौका है। लेकिन यह वह जगह है जहाँ स्कैमर आपके ई–मेल पते, फोन नंबर और अधिक तक पहुँच प्राप्त कर सकता है। एक और तरीका है कि ये स्कैमर्स आपकी जानकारी को पकड़ लेते हैं, आपको यह बताना है कि 'आपके खाते पर अनाधिकृत या संदिग्ध गतिविधि हो रही है', और फिर ये आपसे आपकी जानकारी मागेंगे ताकि वे इसे 'सॉर्ट' कर सकें। वास्तव में वे आपके पैसे चोरी करने जा रहे हैं। फ़िशिंग हमले धोखाधड़ी वाले फ़ोन कॉलों की तरह काम करते हैं जिनके बारे में लोगों को शिक्षित किया जा रहा है।

2. ऑनलाइन घोटाले

ऑनलाइन घोटाले मूल रूप से ऑनलाइन होने वाले घोटाले होते हैं। क्या यह आपको एक विज्ञान पॉपअप करके व्यक्तिगत विवरण ऑनलाइन देने के लिए छल कर रहा है कि आपने कुछ जीता है और शिपिंग के लिए भुगतान करने के लिए आपके कार्ड का विवरण मांग रहा है। अफसोस की बात है कि आपको कुछ भी प्राप्त नहीं होगा लेकिन आप अपने बैंक खाते में आने वाले अजीब लेन–देन को देखन शुरू कर देंगे।

3. मैलवेयर

मैलवेयर आपके सिस्टम पर दुर्भावनापूर्ण सॉफ्टवेयर का संकुचन है।

यह डेटा और उपकरणों को नुकसान पहुंचाने के इरादे से लिखा गया सॉफ्टवेयर का एक टुका है। मैलवेयर विभिन्न प्रकार के वायरस जैसे 'ट्रोजन' और 'स्पाइवेयर' का व्यापक नाम हे। मैलवेयर अक्सर कई प्रकार के वायरस के माध्यम से किया जाता है जो आपके कम्प्यूटर, टैबलेट, फोन को नुकसान पहुँचाकर आपके कम्प्यूटर में घुसकर कहर बरपा सकता है, ताकि अपराधी क्रेडिट कार्ड के विवरण और अन्य व्यक्तिगत जानकारी चुरा सकें।

4. ईमेल बमबारी

एक ईमेल बम अधिक इंटरनेट दुरूपयोग का एक रूप है। ईमेल बमबारी एक ईमेल पते पर निर्देशित ईमेल का एक अधिभार है, इससे ईमेल सर्वर प्राप्त करने वाला व्यक्ति सुस्त हो जाएगा या क्रैश भी हो सकता है। जरूरी नहीं कि वे आपसे कुछ भी चुरा रहे हों, लेकिन एक सुस्त सर्वर होना एक वास्तविक दर्द, और इसे ठीक करने के लिए कड़ी मेहनत हो सकती है।

5. वायरस प्रसारयह

साइबर क्राइम का विशेष रूप से डरपोक रूप है। यह न केवल पीड़ित के सिस्टम के एक हिस्से पर मैलवेयर (किसी प्रकार का वायरस) का एक टुकड़ा प्राप्त करता है, बल्कि यह सॉफ्टवेयर के अन्य टुकड़ों में फैल जाता है।

एक पूर्ण और उचित संगरोध प्रक्रिया और सुरक्षित वातावरण के बिना (एक सैंडबॉक्स) मे परीक्षण करने के लिए, अगली बार जब आप बिना निदान–संक्रमित सॉफ्टवेयर का एक टुकड़ा खोलते हैं, ते प्रक्रिया फिर से शुरू हो जाती है।

6. चोरी

इंटरनेट पर होने वाली किसी भी प्रकार की चोरी के लिए इंटरनेट की चोरी व्यापक शब्द है, यह कई तरह से किया जा सकता है जैसे कि नकली विज्ञापन, नकली ईमेल, वायरस और जासूसी। इंटरनेट चोरी का उद्देश्य आपकी व्यक्तिगत जानकारी को चुराना और उसका उपयोग अपने बैंक खाते से पैसे चुराना या आपके विवरण का उपयोग करके खरीदारी करना है।

7. सोशल मीडिया हैक और स्पैमिंग

सोशल मीडिया हैकिंग को अक्सर मजाक के रूप में किया जाता है, जैसे बर्गर किंग के ट्विटर अकाउंट को हैक करने वाले लोगों द्वारा किया गया हमला और कई हस्तियाँ जिन्हें हैक किया गया है, वे उन लोगों का अनुसरण कर सकते हैं जो वे आमतौर पर नहीं करते हैं या यादृच्छिक स्थिति नहीं डालते हैं। भले ही औसत जो के लिए किसी सेलिब्रिटी या ब्रांड पोस्ट को अजीब चीजें देखना मनोरंजक हो सकता है, यह गोपनीयता का आक्रमण है। हालांकि एक हैकर अनुचित सामग्री भी फैला सकता है जो इस सामग्री को देखने वाले लोगों के लिए कष्टदायक हो सकता है, यह आपके खाते की रिपोर्ट और बंद होने का कारण भी बन सकता है। सोशल मीडिया स्पैमिंग तब आती है जब कोई व्यक्ति नकली खाता बनाता है और दोस्त बन जाता है या औसत व्यक्ति द्वारा उसका अनुसरण किया जाता है। यह तब नकली खाते को बल्क मैसेजिंग के साथ इनबॉक्स को स्पैम करने की स्वतंत्रता देता है, यह मैलवेयर फैलाने के लिए किया जा सकता है। स्पैमिंग किसी उपयोगकर्ता या उनके डिवाइस को नुकसान पहुंचाने, गुमराह करने या क्षति पहुंचाने के इरादे से बनाए गए दुर्भावनापूर्ण लिंग भी फैल सकती है। दुर्भावनापूर्ण लिंक पर क्लिक करना, जो एक नए आईफोन या वजन घटाने का उपचार का विज्ञापन कर सकता है, इसका मतलब है कि आप मलवेयर डाउनलोड कर रहे हैं जिससे व्यक्तिगत जानकारी की चोरी हो सकती है सोशल मीडिया का एक और पक्ष यह है कि दुर्भावनापूर्ण खाते लगातार नकारात्मक संदेशों का जवाब देकर आपके आउटपुट को स्पैम कर सकते हैं। जबकि आप सोशल मीडिया प्लेटफॉर्म पर इस तरह के व्यवहार की आसानी से रिपार्ट कर सकते हैं और उन्हें उपयोगकर्ता को हटा देना चाहिए, या आप उन्हें आपनी सामग्री देखने से रोक सकते हैं, लोगों के लिए मिनटों में नए बॉट खाते सेट करना और अपना हमला फिर से शुरू करना आसान है। कुछ लोगो के साथ में बहुत अधिक समय होता है।

8. इलेक्ट्रॉनिक मनी लॉन्ड्रिंग

बड़ी मात्रा में अवैध रूप से उत्पन्न धन को खर्च करने या निवेश करने से पहले उसे धोखा देना चाहिए। मनी लॉन्ड्रिंग का एक तरीका यह है कि इसे बैंकों के बीच संदेशों के माध्यम से इलेक्ट्रॉनिक रूप से किया जाए जिसे 'वायर ट्रांसफर' के रूप में जाना जाता है। पहले वायर ट्रांसफर की निगरानी करना या स्क्रीन करना असम्भव लग रहा था क्योंकि वे दिन–प्रतिदिन के लेन–देन पर भारी मात्रा में होने के कारण होते है, हालांकि बैंक इस मुद्दे पर सख्ती कर रहे हैं और किसी भी संदिग्ध गतिविधि को दर्ज कर रहे हैं।

9. बिक्री और निवेश धोखाधड़ी

बचत या निवेश खाताधारकों के लिए सम्पर्क विवरण और उपलब्ध खाते की जानकारी प्राप्त करके, धोखेबाते एक निवेश दलाल के व्यक्तित्व को अपना सकते हैं। फिर वे लाभदायक अवसरों के साथ उन्हें लुभाने के लिए ग्राहकों से सम्पर्क करेंगे, लेकिन वे बहुत अधिक भरोसेमंद लगते हैं क्योंकि वे उन खातो के बारे में बात करते है जो आपके पास पहले से हैं और वास्तविक परिणाम हैं। इसे अधिक गहन फिशिंग घोटाले के रूप में सोचें।

10. सॉफ्टवेयर पायरेसी

आजकल, इंटरनेट के लिए धन्यवाद, आप लगभग कोई भी फिल्म, गीत या सॉफ्टवेयर मुफ्त में ऑनलाइन पा सकते हैं। सॉफ्टवेयर पायरेसी कम्प्यूटर सॉफ्टवेयर का अनाधिकृत उपयोग और विवरण है। भले ही पायरेटेड सामग्री का उपयोग करना अच्छा लग सकता है क्योंकि यह मुफ्त है, यह कई प्रकार के जोखिमों के साथ आता है। इन जोखिम में शामिल हैः ट्रोजन, वायरस, वर्म्स और मैलवेयर के अन्य रूप। लेकिन यह चोरी भी करता है, क्योंकि सामग्री के निर्माताओं के पास कोई आय नहीं जाती है।

11. डेटा डिडलिंग

इस सूची में अन्य साइबर अपराधों की तुलना में विनोदी नाम और प्रतीत होता है कि अहानिकर कार्रवाई के बावजूद, डेटा डिडलिंग उपयोगकर्ता के सिस्टम में डेटा प्रविष्टियों को तिरछा करने की क्रिया है। परिणाम बहुत बड़ा हो सकता है, हालांकि उनमें वित्तीय आंकड़ों को थोड़ा ऊपर या नीचे समायोजित करना शामिल हो सकता है, या यह अधिक जटिल हो सकता है और पूरी प्रणाली को अनुपयोगी बना सकता है।

12. हैकिंग

सरल शब्दों में, एक हैकर एक घुसपैठिया है जो आपकी अनुमति के बिना आपके कम्प्यूटर सिस्टम तक पहुँचता है। हैकर्स ऐसे कई कारणों से करते हैं, चाहे वह लालच, प्रसिद्धि या शक्ति के लिए हो, क्योंकि यह लोगों को दिखाता है कि वे उस चीज़ में जाने के लिए पर्याप्त चतुर है जो उनके पास नहीं होनी चाहिए। हालांकि, कुछ सिस्टम में सेध लगाने और व्यक्तिगत बैंकिंग जानकारी और निगम वित्तीय डेटा चोरी करने में सक्षम होंगे। हैकर्स आमतौर पर कम्प्यूटर प्रोग्रामर होते हैं और उन्हें कम्प्यूटर में उन्नत समझ होती है।

13. साइबर स्टाकिंग

दुनिया भर में साइबर स्टाकिंग के कई मामले हैं और यह विशेष रूप से किशोरों और युवा वयस्कों के साथ आम हैं। आमतौर पर पीड़ित और पीछा करने वाला एक दूसरे को जानते हैं। पीड़िता को आमतौर पर ऑनलाइन संदेशों और ईमेल के बैराज के रूप में ऑनलाइन उत्पीड़न का शिकार होना पड़ता है। ऑनलाइन पीछा करने का उद्देश्य पीड़ित को दुखी करना या सामान्य पीछा करने की तरह पीड़ित के सम्पर्क में रहने के विकृत तरीकों के रूप में नियंत्रण करना

है।

14. साइबर बुलिंग

साइबर बुलिंग साइबर स्टॉकिंग के समान है, हालांकि, संदेशो का बैराज हानिकारक, अपमानजनक और पूरी तरह से आक्रामक हो सकता है। साइबर बुलिंग को छवियों और वीडियो को ऑनलाइन पोस्ट करके भी किया जा सकता है जो पीड़ितों को अपमानित करेगा। यह ऑनलाइन लोगों को बाहर करना, हानिकारक या परेशान करने वाली सामग्री पोस्ट करने के लिए नकली खाते बनाना और फिर से अपमानजनक संदेश भेजना भी हो सकता है। कुल मिलाकर यह बदमाशी है लेकिन आमतौर पर सोशल मीडिया चैनलों के माध्यमों से ऑनलाइन होती है।

15. पहचान की चोरी

पहचान की चोरी सइबर अपराध के सबसे आम प्रकारों में से एक है। पहचान की चोरी होने का मुख्य कारण वित्तीय लाभ के लिए धोखाधड़ी पैदा करना है। अपराधी आमतौर पर दूसरों की पहचन की जानकारी जैसे क्रेडिट कार्ड की जानकारी, पते, ईमेल पते और बहुत कुछ चुरा लेते हैं। इस जानकारी से वे किसी और के होने का दिखावा कर सकते हैं और नए बैंक खाते बना सकते हैं।

16. बाल याचना और दुर्व्यहार

ऑनलाइन बच्चों की याचना और दुर्व्यवहार एक प्रकार का साइबर अपराध है जहाँ अपराध पोर्नोग्राफी के उद्देश्य से चैट रूम के माध्यम से बच्चों की याचना करते हैं। इस सामग्री के रूप में भी आ सकती है जो बच्चों के प्रति यौन शोषण को दर्शाती है या उसका वर्णन करती है। एक बच्चे को 16 वर्ष से कम उम्र के व्यक्ति में रूप में माना जाता है। इस प्रकार के साइबर अपराध पर पुलिस द्वारा भारी निगरानी रखी जाती है। यह कम्पनियों के साथ–साथ व्यक्तियों के लिए भी खतरा हो सकता है क्योंकि अपराधी किसी अन्य व्यक्ति को ऑनलाइन अपनाने की तलाश में हो सकते हैं।

17. फिरौती का समान

रैनसम वेयर ने कई कम्पनियों को प्रभावित किया है और हाल ही में पूरी दुनिया में एनएचएस और अन्य बड़े नियमों को प्रभावित किया है। रैनसम वेयर आपके कम्प्यूटर नेटवर्क में प्रवेश करता है जिससे वे और फाइलों को एन्क्रिप्ट करता है, जिसका अर्थ है कि आपके पास उन तक कोई पहुँच नहीं है। हमलावर आपको एक सूचना भेजेगा जिसमें आपसे बड़ी रकम की मांग की जायेगी ताकि आप अपना डेटा वापस पा सकें।

अपराधियों का उद्देश्य यह है कि उन्हें जल्दी पैसा पाने के लिए पर्याप्त लोगों को फिरौती शुल्क भुगतान करना होगा। आपको अपनी रक्षा करने की आवश्यकता क्यो है?

साइबर अपराधी बाहर हैं और पैसा बनाने और उपयोगी जानकारी चुराने के लिए कुछ भी करेंगे। जैसे–जैसे हम अधिक डिजिटल होते जा रहे हैं, हम अपने आप को अधिक से अधिक प्रकार के साइबर अपराध के लिए खोल रहे हैं। साइबर हमलों में खुद को बचाने के कई तरीके हैं।

18. छिपकर बातें सुनना और निगरानी करना

पक्षों की सहमति के बिना सुनना एक अपराध है और इसे ऑनलाइन या फोन पर किया जा सकता है। छिपकर बात सुनने का सबसे आम तरीका वायरटैप है, जो सुनने वाले उपकरण को आमतौर पर एक टेलीफोन लाइन से जोड़ने की प्रथा है, जो अपराधी को गुप्त रूप से बातचीत की निगरानी करने की अनुमति देता है। जैसे–जैसे कई तकनीकें पेश की जाती है, कम्प्यूटर को अब छिपकर सुनने और निगरानी के लिए हैक किया जा सकता है। एक यादृच्छिक टिप के रूप में फेसबुक हेड मैन, मार्क जुकरबर्ग की दर्दनाक सरल रक्षा पर एक नज़र डालें, जो कि वेबकैम वॉयर्स होंगे।

रोकथाम

हो सकता है कि आप सीखना चाहें कि साइबर अपराध को कैसे रोक जाए, लेकिन यहाँ एक बात हैः आप नहीं कर सकते। हालाकि, आप इससे बचाव में मदद करने के लिए सावधानी बरत सकते हैं। साइबर अपराध से खुद को कैसे बचाएं इंटरनेट का उपयोग करने वाले किसी भी व्यक्ति को कुछ बुनियादी सावधानियों बरतनी चाहिए। यहाँ 11 युक्तियां दी गई हैं जिनका उपयोग आप साइबर अपराधों की सीमा से खुद को बचाने में मदद के लिए कर सकते हैं।

1. एक पूर्ण–सेवा इंटरनेट सुरक्षा सूट का उपयोग करें उदाहरण के लिए, नॉर्टन सिक्योरिटी रैंसम वेयर और वायरस सहित मौजूदा और उभरते मैलवेयर के खिलाफ रीयल–टाइम सुरक्षा प्रदान करती है, और जब आप ऑनलाइन जाते हैं तो आपकी निजी और वित्तीय जानकारी को सुरक्षित रखने में मदद करता है।
2. मजबूत पासवर्ड का उपयोग करें अपने पासवर्ड को अलग–अलग साइटों पर न दोहराएं और अपने पासवर्ड को नियमित रूप से बदलें उन्हें जटिल बनायें। इसका मतलब है कि कम से कम 10 अक्षरों, संख्याओं और प्रतीकों के संयोजन का उपयोग करना। पासवर्ड प्रबंधन एप्लिकेशन आपके पासवर्ड के लॉक रखने में आपकी मदद कर सकता है।
3. अपने सॉफ्टवेयर को अपडेट रखें यह आपके ऑपरेटिंग सिस्टम और इंटरनेट सुरक्षा सॉफ्टवेयर के लिए विशेष रूप से महत्वपूर्ण है। साइबर अपराधी आपके सिस्टम तक पहुंच प्राप्त करने के लिए आपके सॉफ्टवेयर में अक्सर ज्ञात कारनामों, या खामियों का उपयोग करते हैं। उन कारनामों और खामियों को दूर करने से यह सम्भावना कम हो सकती है कि आप साइबर अपराध का लक्ष्य बन जाऐंगे।
4. अपनी सोशल मीडिया सेटिंग प्रबंधित करें अपनी निजी और निजी जानकारी केवल कुछ डेटा बिंदुओं के साथ प्राप्त कर सकते हैं, इसलिए जितना कम आप सार्वजनिक रूप से साझा करेंगे, उतना ही बेहतर होगा। उदाहरण के लिए, यदि आप अपने पालतू जानवर का नाम पोस्ट करते हैं या अपनी मां के पहले नाम का खुलासा करते हैं, तो आप दो सामान्य सुरक्षा प्रश्नों के उत्तर उजागर कर सकते हैं।
5. अपने घरेलू नेटवर्क को मजबूत करें, एक मजबूत एन्क्रिप्शन पासवर्ड के साथ–साथ वर्चुअल प्राइवेट नेटवर्क के साथ शुरूआत करना एक अच्छा विचार है। एक वीपीएन आपके डिवाइस को छोड़ने वाले सभी ट्रैफ़िक को एन्क्रिप्ट करेगा जब तक कि वह अपने गंतव्य पर नहीं पहुंच जाता। यदि साइबर अपराधी आपकी संचार लाइन को हैक करने का प्रबंधन करते हैं, तो वे एन्क्रिप्टेड डेटा के अलावा कुछ भी इंटरसेप्ट नहीं करेंगे। जब भी आप सार्वजनिक वाई–फाई नेटवर्क में हों, चाहे वह पुस्तकालय, कैफे, होटल या हवाई अड्डे में हो, वीपीएन का उपयोग करना एक अच्छा विचार है।
6. प्रमुख सुरक्षा उल्लंघनों पर अद्यतित रहें यदि आप किसी व्यापारी के साथ व्यापार करते हैं या किसी सुरक्षा उल्लंघन से प्रभावित वेबसाइट पर आपका खाता है, तो पता करें कि हैकर्स ने कौन सी जानकारी एक्सेस की और तुरंत अपना पासवर्ड बदल दें।
7. बच्चों पर रखें नजर जैसे आप अपने बच्चों से इंटरनेट के बारे में बात करना चाहते हैं, वैसे ही आप उन्हें पहचान की चोरी से बचाने में भी मदद करना चाहेंगे। पहचान चोर अक्सर बच्चों को निशाना बनाते हैं क्योंकि उनकी सामाजिक सुरक्षा संख्या और क्रेडिट इतिहास अक्सर एक साफ स्लेट का प्रतिनिधित्व करते हैं। आप अपने बच्चे की व्यक्तिगत जानकारी साझा करते समय सावधानी बरतकर पहचान की चारी में बचाव में मदद कर सकते हैं। यह जानना भी स्मार्ट है कि क्या देखना है, यह सुझाव दे सकता है कि आपके बच्चे की पहचान में समझौता किया गया है। ये सभी युक्तियों का पालन करके आप कैसे मदद कर सकते हैं एक तरह से साइबर क्राइम से लड़ना हर किसी का काम है।

8. साइबर अपराध के खिलाफ लड़ाई में अपनी भूमिका निभाने के लिए इसे एक दायित्व के रूप में सोचें। अधिकांश लोगों के लिए इसका अर्थ है अपने आपको और अपने परिवार को सुरक्षित रखने के लिए कुछ सरल, सामान्य ज्ञान के चरणों का पालन करना। इसका अर्थ उचित समय पर संबंधित अधिकारियों को साइबर अपराध की सूचना देना भी है। जब आप ऐसा करते हैं, तो आप साइबर अपराध से लड़ने में मदद कर रहे होते हैं। सिफारिशों साइबर अपराध एक गंभीर और बढ़ता हुआ खतरा है। इसलिए इस शोध पत्र में मैं सरकार की डिजिटल सुरक्षा को मजबूत करने के लिए रूपरेखा तैयार कर रहा हूँ।

निष्कर्ष

इंटरनेट बहुत शक्तिशाली उपकरण और संचार का प्रभावी साधन है लेकिन यह किसी भी चीज़ की तरह ही असुरक्षित है। साइबर अपराधों से बचाव के लिए, घुसपैठ का पता लगाने की तकनीकों को डिजाइन, कार्यान्वित और प्रशासित किया जाना चाहिए। अभी के लिए इसे बचाने का तरीका यह है कि सभी लोग स्मार्ट हों और निवारक उपायों का पालन करें, व्यक्तियों, संस्थानों और सरकार को समान रूप से इन उपायों का पालन करना चाहिए। साइबर हमले सरकारों, निगमों और व्यक्तियों को दैनिक आधार पर नकारात्मक रूप से प्रभावित करते हैं। हमारी चल रही भेद्यता के कई कारणों में से एक यह है कि साइबर खतरों के खिलाफ भारतीय हितों की रक्षा के लिए हमारे पास एक समेकित दृष्टिकोण की कमी है। यह दर्दनाक रूप से स्पष्ट हो गया है कि न तो सरकार और न ही निजी क्षेत्र इस समस्या को अपने आप हल कर सकते हैं। साइबर सुरक्षा के मामले में हमारे देश के राष्ट्रीय हितों की रक्षा के लिए एक संयुक्त प्रयास होना चाहिए।

संदर्भ

1. Cyber Crime @Coe Update on Council of Europe activities o4 Cyber Crime, 2017.
2. Details of Treaty No. 185 Convention Cyber Crime (Online). Available: http:/www.coe.int/cn/web/convention/full-list/convenction/treats/185 (Accessed 27 Aug. 2017).
3. Internet Security Threat Report (ISTR), Symantec Corporation World Headquarters 350 Ellies Streat Mountain View, CA94043 United Stated of America, 2017.
4. Cyber Crime and Punishment? Archaic Law Threaten Global Information, Mc. Connect International, 2000.
5. Chethan-one Cyber Crime in India every 10 Hindu's-Times of India, 2021.
6. Naidu JS. -10,000 Cyber Crime Cases, only 34 Conviction in Maharashtra between 2012 and 2017, 2017. http://www.hindustantimes.com.
7. A Seger- India and the Budapest Convention Why not?
8. D.A. Kovacs- India and the Budapest Convention.
9. Zee News, April 29, 2022.
10. Mnistry of Electronics and Information Technology.
11. Cyber lawsindia.net.
12. Computer Crime- Final Law available at:- https:/criminal-Findlaw.com (visited on 27 Nov. 2020).