PRAKASH CHANDRA UPADHYAY
GHSS KHOONABORA,CHAMPAWAT

साइबर सुरक्षा : व्यक्तिगत डेटा को सुरक्षित रखना–

प्रतिदिन की तरह प्रिया आज भी सुबह–सुबह स्कूल जाने के लिए तैयार ही हो रही थी कि अचानक उसके मोबाइल में एक मैसेज आया,जिसमें उसके कुछ फोटो और एक वीडियो था। जब प्रिया ने उस मैसेज को ओपन किया तो प्रिया ने देखा कि उसमें उसके व्यक्तिगत फोटो को एआई की मदद से वीडियो में कनवर्ट कर आपत्तिजनक अवस्था में दिखाया गया था। प्रिया को समझ ही नहीं आया कि ये फोटो तो मैंने अपनी सहेलियों के साथ पिछली बार की पिकनिक में खिंचवाये थे, लेकिन मेरे इन फोटो में मेरे साथ दिखाया गया ये अनजान शख्स कौन है। मैं तो इस व्यक्ति को जानती भी नहीं हूँ।

प्रिया का मन बेचैन हो उठा और किसी अनहोनी की आशंका से भयभीत हो गया। प्रिया किसी–न–किसी प्रकार विद्यालय पहुंच गई और अपनी कक्षा में विचारमग्न बैठ गई और उसका पढ़ाई में भी मन नहीं लग रहा था। कक्षा में कंम्प्यूटर विषय को पढाने वाली प्रिया की प्रिय शिक्षिका रजनी मैडम आई और प्रिया को उदास बैठे देखा तो अनायास ही प्रिया से पूछ बैठी कि तुम इतनी उदास और बेचैन क्यों लग रही हो?

प्रिया पहले तो सकुचाई लेकिन फिर उसने अपनी फैवरेट मैडम के अपनत्व भरे व्यवहार को देखकर सारी बात बेहिचक बता दी। रजनी मैडम ने ध्यानपूर्वक प्रिया की बात सुनी और प्रिया को पहले तो सांत्वना दी कि तुम घबराओ मत। उन्होंने प्रिया को बताया कि वर्तमान समय में इस प्रकार की साइबर संबंधी अनेक घटनाएं बहुत से लोगों के साथ दिन–प्रतिदिन हो रही हैं। रजनी मैडम ने प्रिया को कहा कि पहले तो तुम डरना बंद करो और हम मिलकर इस बारे में विस्तारपूर्वक बात करते हैं।

इसके उपरांत रजनी मैडम ने साइबर सुरक्षा की आधारभूत जानकारी देने के साथ ही साइबर फ्राड,साइबर सिक्योरिटी तथा व्यक्तिगत डाटा को सुरक्षित रखने

के बारे में प्रिया को गहन जानकारी प्रदान की। साइबर की दुनिया की जानकारी देने के साथ ही रजनी मैडम ने इस प्रकार की घटनाओं की शिकायत संबंधी टोल फ्री नंबर तथा पोर्टल की भी जानकारी दी, जिसमें शिकायत करने पर इस प्रकार की घटनाओं के संबंध में सहायता दी जाती है।

साइबर सुरक्षा की मूल अवधारणाः– वर्तमान समय में दिन–प्रतिदिन परिवर्तित हो रही दुनिया में तकनीकी के प्रयोग के बिना जीवन निर्वहन अत्यधिक दुरूह हो जाएगा। तकनीकी का प्रयोग करते समय साइबर सुरक्षा व्यक्तिगत रूप से तथा सांगठनिक रूप से सभी के लिए अत्यधिक महत्वपूर्ण है। साइबर अपराध की दर सम्पूर्ण विश्व में लगातार बढ़ रही है। साइबर अपराधी सुरक्षा कदमों से भी सदैव आगे चल रहे हैं। दिन–प्रतिदिन हो रहे साइबर हमलों के कारण वर्तमान समय में प्रत्येक व्यक्ति के लिए साइबर सुरक्षा और व्यक्तिगत डेटा को सुरक्षित रखना अत्यधिक महत्वपूर्ण हो गया है। साइबर सुरक्षा तथा व्यक्तिगत डेटा को सुरक्षित रखने के और साइबर दुनिया संबंधी जोखिमों को कम करने के लिए साइबर सुरक्षा संबंधी मूलभूत अवधारणाओं तथा नियमों व कानूनों को जानना आवश्यक है।

साइबर सुरक्षा का अर्थः– साइबर सुरक्षा का अर्थ है, किसी व्यक्ति अथवा संगठन को साइबर हमलों से बचाने के लिए उपयोगी प्रौद्योगिकी तथा प्रक्रियाओं का इस्तेमाल करना। यह इंटरनेट से जुड़ी इकाइयों से संबंधित एक तरह की सुरक्षा है। साइबर सुरक्षा कंप्यूटर,मोबाइल,नेटवर्क और व्यक्तिगत डेटा को दुर्भावनापूर्ण हमलों से बचाने का एक पूर्वाभ्यास है। साइबर सुरक्षा में कंम्प्यूटर,मोबाइल,नेटवर्क और डेटा को चोरी,क्षति या अनधिकृत पहुंच से बचाना सम्मिलित है। बढ़ते साइबर खतरों के कारण हमें दिन–प्रतिदिन अपनी रणनीतियां भी विकसित करनी होंगी और उनको समय–समय पर अद्यतन भी करना होगा।

साइबर सुरक्षा हेतु महत्वपूर्ण उपायः–

1.मजबूत पासवर्ड– मजबूत और विशेष पासवर्ड व्यक्तिगत उपकरणों तथा डिवाइस के लिए अत्यधिक प्रभावी उपाय है। मजबूत पासवर्ड के कुछ आवश्यक बिन्दु–

अ. पासवर्ड कम से कम 12 वर्ण का होना चाहिए।

ब. अपरकेस और लोअरकेस के अक्षर पासवर्ड में सम्मिलित होने चाहिए।

स. संख्याओं और विशेष प्रतीक चिन्हों का मिश्रण पासवर्ड में सम्मिलित होना चाहिए।

2.मल्टी फैक्टर ऑथेंटिकेशन– मल्टी फैक्टर ऑथेंटिकेशन अतिरिक्त सुरक्षा को सुनिश्चित करता है। बहुकारक प्रमाणीकरण हमारे पासवर्ड को और अधिक सुरक्षित तथा अतिरिक्त परत जोड़ने का कार्य करता है। एमएफए दो स्तर पर सत्यापन करता है।

3. नियमित सॉफ्टवेयर अपडेट– अपने सॉफ्टवेयर और ऑपरेटिंग सिस्टम को नियमित रूप से अपडेट करते रहें, जिससे एक अतिरिक्त सुरक्षा सुनिश्चत होगी। अपनी डिवाइसों को समय–समय पर अपडेट करना अत्यधिक महत्वपूर्ण है क्योंकि सॉफटवेयर डेवलपर्स नियमित रूप से कमजोरियों को पैच करने के लिए अपडेट जारी करते हैं।

4. फिशिंग हमलों से सतर्कता– अक्सर भ्रामक ईमेल या वेबसाइटों के माध्यम से फिशिंक हमलों द्वारा लोगों से संवदेनशील तथा उनकी गोपनीय जानकारी प्राप्त कर धोखा दिया जाता है। इस प्रकार के फिशिंग हमलों से सतर्कता एवं सावधानी रखना आवश्यक है।

5. वाई–फाई नेटवर्क को सुरक्षित रखना– वाई–फाई के माध्यम से साइबर अपराधी बहुत ही आसानी से आपकी डिवाइस में प्रवेश कर सकते हैं। इसके साथ ही ब्लूटुथ आदि माध्यमों से अन्य उपकरणों को जोडना भी अत्यधिक घातक हो सकता है। इस प्रकार कनेक्टिविटी के समय सतर्कता रखना अत्यावश्यक है।

6. व्यक्तिगत डेटा बैकअप– किसी भी संभावित खतरों से बचाव हेतु नियमित रूप से अपने डेटा का बैकअल लेना आवश्यक है। डेटा के बैकअप के लिए बाहरी हार्ड ड्राइव या क्लाउड स्टोरेज आदि का उपयोग करना उपयोगी साबित होगा।

आर्टिफिशियल इंटेजिलेंस और साइबर सुरक्षाः– साइबर सुरक्षा में आर्टिफिश्झियल इंटेलिजेंस अत्यधिक उपयोगी सिद्ध हो सकता है। आर्टिफिशियल इंटेलिजेंस से साइबर खतरों का पता आसानी से लगाया जा सकता है। इसके माध्यम से जोखिम को कम किया जा सकता है। साइबर सुरक्षा में एआई का उपयोग निम्नलिखित तरीकों से किया जा सकता है–

1.खतरे का पता लगाना और रोकथाम करना– एआई के माध्यम से किसी भी सिस्टम या नेटवर्क की गतिविधियों आदि पर नजर रखकर उनका विश्लेषण किया जा सकता है। एआई संभावित खतरों को चिन्हित कर सकता है। एआई के माध्यम

से मशीन लर्निंग मॉडल को बड़ी मात्रा में डेटा के विश्लेषण करने तथा संभावित खतरों को पहचानने के लिए प्रशिक्षित किया जा सकता है।

2.स्वचालित प्रतिक्रिया– एआई स्वचालित रूप से संभावित खतरों को स्वयं जानकर काफी हद तक उनका निदान भी कर सकता है। एआई गलत आईपी एड्रेस को ज्ञातकर उसे ब्लॉक कर सकता है। इसके साथ ही एआई संक्रमित फाइलों को भी ब्लॉक कर सकता है। उदाहरण के रूप में सिक्योरिटी ऑर्केस्ट्रेशन,ऑटोमेशन आदि।

3.फिशिंग डिटेक्शन– एआई को ईमेल,वेबसाइटों और यूआरएल में पैटर्न को पहचानने के लिए आसानी से प्रशिक्षित किया जा सकता है,जिनके माध्यम से फिशिंग हमलों को रोका जा सकता है। उदाहरण के लिए एआई फिशिंग के संकेतों के लिए ईमेल हेडर सामग्री और अटैचमेंट का विश्लेषण कर सकता है।

4. उपयोगकर्ता के व्यवहार का विश्लेषण–एआई उपयोगकर्ता के व्यवहार की निगरानी कर सकता है, व्यक्तिगत प्रोफाइल बना सकता है और असामान्य गतिविधियों का भी विश्लेषण कर सकता है। इसके माध्यम से साइबर हमलों का भी पता लगाया जा सकता है।

साइबर सुरक्षा तथा व्यक्तिगत डेटा को सुरक्षित रखने के लिए अनेक उपाय किए जा सकते हैं। सर्वप्रथम हमें जागरूक होना होगा तथा अपनी सभी डिवाइसों को सुरक्षित करने के भी उपाय करने होंगे। डिवाइस को अनेक प्रकार से सुरक्षित किया जा सकता है, जिसके दो उदाहरण नीचे दिए जा रहे हैं–

कीलौगर सॉफ्टवेयरः– कीलोंगर एक सर्विलांस सॉफ्टवेयर है, जिसको किसी भी डिवाइस में यदि इंस्टॉल किया जाए तो वह उस सिस्टम में प्रत्येक कीस्टोक को रिकार्ड कर लेता है। यह प्रोग्राम रिकार्ड की गई फाइल को एक लौग फाइल के रूप में सहेज कर रखता है।

Fig 1- keylogger software

इंटीग्रीटी चेकरः– इंटीग्रीटी चेकर एक ऐसा उपकरण है जो ऑपरेटिंग सिस्टम की सुरक्षा को सुनिश्चित करता है। इस टूल के माध्यम से सभी सिस्टम फाइलों की सत्यनिष्ठता तथा सुरक्षा सुनिश्चित हो जाती है। यह नियमित रूप से ऑपरेटिंग सिस्टम की जॉच करता है और एक भरोसेमंद डेटाबेस के साथ तुलना कर निरंतर अपडेट देता रहता है। इंटीग्रीटी चेकर के माध्यम से यह वास्तविक समय में तुरंत अलर्ट और नोटिफिकेशन भेजता है।

Fig 2- Integrity checker

निष्कर्ष– साइबर सुरक्षा प्रत्येक व्यक्ति के लिए अत्यधिक महत्वपूर्ण है। साइबर सुरक्षा की आधारभूत जानकारी प्राप्त कर हम इसके खतरों से काफी हद तक अपना बचाव कर सकते हैं। सावधानियों के माध्यम से हम अपनी व्यक्तिगत और संवेदनशील जानकारी की सुरक्षा कर सकते हैं। प्रतिदिन बढ़ रहे साइबर खतरों से खुद का तथा अपने परिचितों का बचाव कर सकते हैं। एआई के उपयोग से साइबर सुरक्षा को काफी आसान बना दिया है। एआई के द्वारा भारी मात्रा में डेटा को संसाधित और विश्लेषण करने,नए खतरों के अनुकूल होने और सुरक्षा संचालन के विभिन्न पहलुओं के लिए अत्यधिक उपयोगी सिद्ध होता है। एआई के उपयोग से साइबर सुरक्षा के लिए अत्यधिक महत्वपूर्ण है।

References:1. https://onlinecourses.nptel.ac.in/noc23_cs127/preview

2. https://www.nist.gov/blogs/taking-measure/why-security-and-privacy-matter digital-world

3. https://pg-p.ctme.caltech.edu/blog/cybersecurity/ai-in-cybersecurity

4. https://github.com/GiacomoLaw/Keylogger