Received: Jun '23
Revised:
Accepted: Aug '23

CYBERSECURITY IN EDUCATIONAL INSTITUTIONS: NEED AND EFFORTS
शिक्षण संस्थानों में साईबर सुरक्षा – आवश्यकता एवं प्रयास

Dr. Girdhari Lal Sharma[1] and Dr. Vishnu Kumar[2]
[1,2]Assistant Professor, Dept of Education, Jain Vishva Bharati Institute, Deemed University, Ladnun, Rajasthan, India- 341306
E-mail: [1]girdhari1976@gmail.com

ABSTRACT

The Internet has made information widely available to the public at all times, which is both a blessing and a curse. This is important for any type of business, including educational institutions. Cybersecurity awareness is paramount, as it can help us identify potential threats before they happen. It also provides us with the necessary knowledge to protect ourselves from malicious sites or attacks. Cybersecurity awareness training is important because it teaches students how to protect themselves from phishing scams, malware, ransomware, and cyberattacks on computers. In view of increasing cybercrime, the University Grants Commission (UGC) has asked all universities and higher educational institutions to make the necessary preparations and create an environment to deal with cyber security in their institutions.

इंटरनेट ने हर समय व्यापक रूप से जनता के लिए जानकारी उपलब्ध कराई है, जो एक आशीर्वाद और अभिशाप दोनों है। शिक्षण संस्थानों सहित किसी भी प्रकार के व्यवसाय के लिए यह महत्वपूर्ण है। साइबर सुरक्षा जागरूकता सर्वोपरि है क्योंकि यह संभावित खतरों को होने से पहले पहचानने में हमारी मदद कर सकती है। यह हमें खुद को दुर्भावनापूर्ण साइटों या हमलों से बचाने के लिए आवश्यक ज्ञान भी प्रदान करता है। साइबर सुरक्षा जागरूकता प्रशिक्षण महत्वपूर्ण है क्योंकि यह छात्रों को सिखाता है कि वे फ़िशिंग घोटालों, मैलवेयर, रैंसमवेयर और कंप्यूटर पर होने वाले साइबर हमलों से खुद को कैसे बचा सकते हैं। विश्वविद्यालय अनुदान आयोग (यूजीसी) द्वारा बढ़ते साइबर अपराध को देखते हुए सभी विश्वविद्यालय और उच्च शिक्षण संस्थानों को जरूरी तैयारी करने तथा संस्थानों में साइबर सुरक्षा से निपटने के लिए एक वातावरण तैयार करने को कहा गया है।

Keywords: -Cyber Security, Cyber Security in Educational Institutions, Need for Cyber Security.
मुख्य शब्दावली - साईबर सुरक्षा, शिक्षण संस्थानों में साईबर सुरक्षा, साईबर सुरक्षा की आवश्यकता

मुख्य विषय वस्तु

दुनियां ने जिस गति से तकनीकी क्षेत्र में उन्नति की है, उसी गति से मनुष्य की इंटरनेट पर निर्भरता भी बढ़ी है। आज घर बैठे हमारी पहुच, इंटरनेट के जरिये विश्व के हर कोने तक आसान हो गई है। आज 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। वर्तमान 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।

साइबर अपराध

साइबर अपराध एक आपराधिक गतिविधि है, जिसे कंप्यूटर और इंटरनेट के उपयोग द्वारा अंजाम दिया जाता है। साइबर अपराध, जिसे 'इलेक्ट्रॉनिक अपराध' के रूप में भी जाना जाता है, एक ऐसा अपराध है जिसमें किसी भी अपराध को करने के लिए, कंप्यूटर, नेटवर्क डिवाइस या नेटवर्क का उपयोग, एक वस्तु या उपकरण के रूप में किया जाता है। जहाँ इनके (कंप्यूटर, नेटवर्क डिवाइस या नेटवर्क) जरिये ऐसे अपराधों को अंजाम दिया जाता है वहीँ इन्हें लक्ष्य बनाते हुए इनके विरुद्ध अपराध भी किया जाता है। ऐसे अपराध में साइबर जबरन वसूली, पहचान की चोरी, क्रेडिट कार्ड धोखाधड़ी, कंप्यूटर से व्यक्तिगत डेटा हैक करना, फ़िशिंग, अवैध डाउनलोडिंग, साइबर स्टॉकिंग, वायरस प्रसार, सहित कई प्रकार की गतिविधियाँ शामिल हैं। गौरतलब है कि सॉफ्टवेयर चोरी भी साइबर अपराध का ही एक रूप है, जिसमें यह जरूरी नहीं है कि साइबर अपराधी, ऑनलाइन पोर्टल के माध्यम से ही अपराध करे।

साइबर अपराधों को दो श्रेणियों में बांटा जा सकता है। 1. वे अपराध जिनमें कंप्यूटर पर हमला किया जाता है। इस तरह के अपराधों के उदाहरण हैकिंग, वायरस हमले, डॉस हमले आदि हैं। 2. वे अपराध जिनमे कंप्यूटर को एक हथियार/उपकरण/ के रूप में उपयोग किया जाता है। इस प्रकार के अपराधों में साइबर आतंकवाद, आईपीआर उल्लंघन, क्रेडिट कार्ड धोखाधड़ी, ईएफटी धोखाधड़ी, पोर्नोग्राफी आदि शामिल हैं।

सीईआरटी-इन (इंडियन कम्प्यूटर इमरजेंसी रिस्पांस टीम) के आंकड़ों के अनुसार 2022 में भारत में सबसे अधिक साइबर क्राइम

के मामले दर्ज किए गए हैं। सीईआरटी साइबर सुरक्षा हमलों से निपटने के लिए केन्द्र सरकार की एक नोडल एजेंसी है, जो सूचना प्रौद्यौगिकी मंत्रालय के तहत काम करती है। 2022 के पहले दो महीनों में 2,12,285 मामले दर्ज किए गए हैं, जबकि इसकी तुलना में साल 2018 में 2,8,456 साल 2019 में 3,94,499 घटनाएं 2020 में 11,58,208 और 2021 में 14,2,809 घटनाएं दर्ज की गयी हैं। ये आंकड़े बताते हैं इन तीन बर्षों में साइबर क्राइम के मामले लगभग 7 गुना और कोविड के दौरान अधिक तेजी से बड़े हैं।

ऑनलाइन धोखाधड़ी सबसे ज्यादा भारत में

सीईआरटी से अलग एनसीआरबी के आंकड़े अलग ही कहानी बयां करते हैं। साल 2019 में अपराध दर 3.3 से बढ़कर 2020 में 3.7 हो गयी। रिपोर्ट के मुताबिक साल 2020 में अधिकतर केस धोखाधड़ी के मकसद से दर्ज किए गए 2020 में 60.2 प्रतिशत मामले तकरीबन (50,035 मामलों में से 30,142) दर्ज किए गए। जबकि 6.6 प्रतिशत (3,293) मामले यौन शोषण के पाए गए। इसके अलावा 4.9 प्रतिशत (2,440) केस जबरन वसूली के जारी किए गए थे। आंकड़ों के मुताबिक साल 2020 में ऑनलाइन बैंकिंग धोखाधड़ी के 4047 मामले, ओटीपी जालसाजी के 1093 केस, डेबिट क्रेडिट कार्ड से ठगी की 1194 घटनाऐं, और एटीएम से सम्बन्धित 2160 मामले दर्ज किए गए। रिपोर्ट में बताया गया कि सोशल मीड़िया पर फर्जी सूचना के 578 केस, ऑनलाइन परेशान करने या महिलाओं और बच्चों को साइबर धमकी से जुड़े 972 मामले, जबकि फर्जी प्रोफाइल के 149 और आंकड़ों की चोरी के 98 मामले जारी किए गए हैं।भारत 560 मिलियन से अधिक इंटरनेट यूजर्स के साथ दुनिया का दूसरा सबसे बड़ा ऑनलाइल मार्केट है, इस मामले में भारत केवल चीन से पीछे है। ऐसा अनुमान है 2023 तक देश में 650 मिलियन से ज्यादा इंटरनेट उपयोगकर्ता होंगे। इतना विशाल मार्केट होने के कारण यहां साइबर अपराधों में दिन दिन तेजी बढ़ती ही जा रही है। (पत्रिका , 6 December, 2022)

शिक्षण संस्थानों में साईबर सुरक्षा की आवश्यकता

सिंगापुर स्थित एआई-संचालित डिजिटल रिस्क मैनेजमेंट एंटरप्राइज क्लाउडसेक (CloudSEK) के थ्रेट रिसर्च एंड इंफोर्मेशन एनालिटिक्स डिवीजन द्वारा "साइबर थ्रेट टार्गेटिंग द ग्लोबल एजुकेशन सेक्टर" शीर्षक से जारी एक रिपोर्ट में दावा किया गया है कि भारतीय शिक्षा क्षेत्र साइबर हमलों के लिए सबसे बड़ा टारगेट बना हुआ है। भारत के बाद संयुक्त राज्य अमेरिका, ब्रिटेन, इंडोनेशिया और ब्राजील का स्थान है। रिपोर्ट में यह भी दावा किया गया है कि 2022 के पहले तीन महीनों में 2021 की इसी अवधि की तुलना में डाटा वैश्विक शिक्षा क्षेत्र के लिए साइबर खतरों में 20 प्रतिशत की वृद्धि दर्शाता है।

रिपोर्ट के अनुसार, भारत शैक्षणिक संस्थानों और ऑनलाइन प्लेटफॉर्म के लिए साइबर खतरों का सबसे बड़ा लक्ष्य है। क्योंकि कोविड- 19 वैश्विक महामारी के दौरान दूरस्थ शिक्षा को अपनाना, शिक्षा का डिजिटलाइजेशन और ऑनलाइन लर्निंग प्लेटफार्मों का प्रचलन प्रमुख तौर बढ़ा है, जिससे साइबर हमले की घटनाएं भी बढ़ी हैं। प्लेटफॉर्म के द्वारा पिछले साल एशिया-प्रशांत क्षेत्र में देखे गए साइबर खतरों में से 58 फीसदी भारतीय या भारत आधारित शैक्षणिक संस्थानों और ऑनलाइन प्लेटफॉर्म को टारगेट कर रहे थे। इसके बाद 10 फीसदी साइबर खतरों के टारगेट के साथ इंडोनेशिया दूसरे स्थान पर था। इसमें ऑनलाइन कोचिंग प्लेटफॉर्म बायजू, आईआईएम कोझीकोड और तमिलनाडु के तकनीकी शिक्षा निदेशालय आदि पर हुए साइबर हमले शामिल थे। वहीं, संयुक्त राज्य अमेरिका दुनिया भर में दूसरा सबसे अधिक प्रभावित देश था, जिसमें कुल 19 दर्ज घटनाएं थीं, जो उत्तरी अमेरिका में 86 प्रतिशत खतरों के लिए जिम्मेदार थीं। इनमें हॉवर्ड विश्वविद्यालय और कैलिफोर्निया विश्वविद्यालय जैसे प्रतिष्ठित संस्थानों पर रैंसमवेयर हमले शामिल हैं (अमर उजाला Sun, 01 May 2022)। अतः आज शिक्षण संस्थानों में साइबर अपराधों के प्रति जागरूकता की सर्वाधिक आवश्यकता है जिसे निम्न बिन्दुओं में स्पष्ट किया जा सकता है।

विभिन्न एप्स के प्रति जागरूकता हेतु – आज प्ले स्टोर पर अनेक एप उपलब्ध हैं। इनमें अनेक अनधिकृत होते हैं, जो एक बार फोन में इनस्टॉल होने पर अनेक प्रकार के डाटा चुराते हैं। स्कूल विद्यार्थी, यहाँ तक की कॉलेज विद्यार्थी भी जानकारी के आभाव में बिना सोचे एप डाऊनलोड कर लेते हैं तथा सभी प्रकार की परमीसन देते जाते हैं, जिससे उनकी निजी जानकारी, फोटो, फाइल्स आदि चोरी हो रहे हैं। इनसे बचने हेतु विद्यार्थियों में साइबर जागरूकता आवश्यक है।

गेमिंग एप के प्रति सावधानी हेतु – बच्चों में मोबाइल गेमिंग की आदत निरंतर बढ़ रही है। अनेक ऐसे गेम हैं जिनकी लत बच्चों को लग जाती है, उनके द्वारा बच्चों से निजी जानकारियां तथा पैसों की मांग की जाती है , जिसे वे घरवालों से छुपकर पूरा करते रहते हैं और अनेक बार तो आत्म हत्या तक कर लेते हैं। ये एक गंभीर समस्या बनती जा रही है , जिसे साइबर जागरूकता के माध्यम से ही हल किया जा सकता है।

साइबर बुल्लिंग से बचाब हेतु – साइबर बुल्लिंग का अर्थ है लोगों को सोशल मिडिया या अन्य इंटरनेट प्लेटफार्म से परेसान करना। अपराधियों द्वारा ऐसा अनेक तरीके से किया जाता है, जैसे - सोशल मिडिया के माध्यम से दोस्ती कर व्यक्तियों से नजदीकी बढ़ाना तथा बाद में उनकी निजी जानकारियों को लेकर परेशान करना, साथ ही ऑनलाइन ब्लेकमेल करना। किशोर विद्यार्थियों के साथ ऐसा अक्सर हो रहा है जिससे वे शारीरिक एवं मानसिक

प्रताड़ना झेलते हैं। इनसे बचने हेतु विद्यार्थियों में साइबर जागरूकता आवश्यक है।

सेक्सटोर्सन से बचाब हेतु - सेक्सटोर्सन एक ऐसा साइबर अपराध है जिसका शिकार अनेक बच्चे तथा किशोर विद्यार्थी हो रहे हैं तथा आत्म हत्या तक कर रहे हैं। सोशिअल मीडिया पर दोस्ती तथा विडियो कालिंग का बढ़ता चलन आज आम बात है। शातिर साइबर ठग ईसी का लाभ उठाते हैं और उनके अश्लील विडियो या फोटो बनाकर फिर ब्लेकमेल करते हैं। बदनामी के डर से ये युवक – युवतियां उनके हाथ की कठपुतली बनकर अपराधियों के इशारों पर नाचते हैं तथा अनेक प्रकार का उत्पीडन सहते हैं। इनसे बचने हेतु विद्यार्थियों में साइबर जागरूकता आवश्यक है।

बैंकिंग फ्रॉड से बचाब हेतु – डिजिटलीकरण के इस दौर में मोबाइल बैंकिंग लेन-देन का सर्वाधिक प्रयुक्त होने वाला साधन है। निश्चित ही इससे लेन-देन, खरीददारी आदि बहुत सुलभ हो गया है हमें बैंकों में घंटों लाइन में लगने से मुक्ति मिल गयी है लेकिन थोड़ी सी लापरवाही या असावधानी से नुकसान भी बड़ा हो जाता है। रोजाना हैकर्स अनेक लोगों के अकाउंट से कितना ही पैसा चुरा रहे हैं। के.वाई.सी अपडेट के नाम पर या लौटरी का पैसा देने के नाम पर या अन्य कोई लालच देकर ओ टी पी पूछ लेते हैं और पूरा पैसा चुरा लेते हैं। अनेक विद्यार्थी भी इसका शिकार हो रहे हैं। इस प्रकार के फ्रौड्स से बचने हेतु भी विद्यार्थियों में साइबर जागरूकता आवश्यक है।

सोशिअल मीडिया फ्रौड्स से बचाब हेतु - सोशिअल मीडिया आज बच्चे , युवा तथा बुजुर्ग सभी को पूर्णतः अपनी गिरफ्त में ले चुका है। प्रत्येक मोबाइल में फेसबुक, इन्स्टाग्राम, ट्विटर, व्हाट्सएप आदि का पाया जाना सामान्य बात है। ज्यादातर समय लोग इन एप्स पर बिताते हैं। जानकारी के आभाव में अनेक बच्चे तथा युवा विद्यार्थी अपने निजी फोटोग्राफ, विडियो तथा अन्य निजी जानकारियां इन एप्स पर अपलोड कर रहे हैं तथा अनजान लोगों से मित्रता कर रहे हैं। साइबर अपराधी इन निजी जानकारियों का गलत तरीके से उपयोग कर लड़के – लड़कियों को ब्लेकमेल करते हैं तथा उनका शारीरिक , मानसिक एवं आर्थिक शोषण करते हैं। लड़कियां इस प्रकार के अपराधों का अधिक शिकार हो रही हैं। अतः सोशिअल मीडिया के सुरक्षित उपयोग हेतु भी साइबर जागरूकता आवश्यक है।

साइबर स्टोकिंग से बचाब हेतु – ऑनलाइन माध्यम से की गई छेड़खानी को साइबर स्टोकिंग कहा जाता है। इसमें अपराधी ईमेल या मेसेज भेजकर किसी को भी परेशान करते हैं। इस समस्या से पीड़ितों में महिलाओं एवं बच्चों का प्रतिशत तीन चौथाई है। भारत में साइबर स्टोकिंग का पहला मामला 2001 में दर्ज किया गया था स्कूल या कॉलेज जाने वाली लड़कियों को अनेक अपराधी तत्व अश्लील मेसेज , फोटो या ईमेल भेजकर मानसिक रूप से प्रताड़ित करते हैं तथा अपनी मांगें मनवाने के लिए बाध्य करते हैं। इससे बचाब हेतु भी साइबर सुरक्षा जागरूकता आवश्यक है।

साइबर ठगी होने पर क्या करें ? की जानकारी हेतु – साइबर अपराध का शिकार होने पर ज्यादातर लोग, मुख्यतः बच्चे व महिलाएं शारीरिक, मानशिक व् आर्थिक रूप से प्रताड़ित होते रहते हैं तथा किसी को न तो बताते हैं और न ही कहीं शिकायत करते हैं। साइबर अपराध बढ़ने का यह सबसे बड़ा कारण है। अतः आज आवश्यकता है साइबर अपराध के प्रति जागरूकता की । विद्यार्थियों को शिक्षण संस्थानों में यह बताना जरुरी है की किसी भी साइबर अपराध का शिकार होने पर डरने , घबराने या छुपाने की जरुरत नहीं है बल्कि इसकी शिकायत तुरंत की साइबर क्राइम पोर्टल cybercrime.gov.in या 1930 नम्बर पर फोन करके तुरंत ही करनी चाहिए। इस हेतु भी शिक्षण संस्थानों में साइबर जागरूकता कार्यक्रमों का आयोजन आवश्यक है।

शिक्षा क्षेत्र में साइबर जागरूकता हेतु किये जा रहे प्रयास

विश्वविद्यालय अनुदान आयोग (यूजीसी) ने बढ़ते साइबर अपराध को देखते हुए सभी विश्वविद्यालय और उच्च शिक्षण संस्थानों को जरूरी तैयारी करने तथा संस्थानों में साइबर सुरक्षा से निपटने के लिए एक वातावरण तैयार करने को कहा है। इसके लिए इस क्षेत्र से जुड़े विशेषज्ञों की मदद लेने को भी कहा गया है। आयोग का मानना है कि आने वाले दिनों में इंटरनेट और डिजिटल कामकाज को और बढावा मिलेगा। ऐसे में साइबर सुरक्षा को लेकर जागरूकता जरूरी है।

यूजीसी सचिव रजनीश जैन ने उपकुलपतियों को लिखे पत्र में कहा है, ''सरकार राष्ट्रीय साइबर सुरक्षा रणनीति दस्तावेज तैयार करने की प्रक्रिया में है और इस बीच यह निर्णय किया गया है कि स्कूल स्तर पर साइबर सुरक्षा जागरूकता शुरू हो जानी चाहिए जहां पाठ्यक्रम साइबर सुरक्षा कदमों के साथ शुरू हो सकता है और इसमें आईआईटी तथा उच्च शिक्षा स्तर पर उत्तरोत्तर आक्रामक तथा रक्षात्मक पहलू शामिल हों।''(NBT, Dec.02,2020)

इसके साथ ही आयोग ने गृह मंत्रालय की ओर से साइबर अपराधों से बचाव को लेकर जारी किए गए दिशा-निर्देशों की भी सभी को जानकारी देने को कहा है। यूजीसी का यह कदम इसलिए भी अहम है, क्योंकि देश में मौजूदा समय में प्रतिदिन औसतन तीन हजार से ज्यादा साइबर अपराध की घटनाएं हो रही हैं। आने वाले दिनों में इनकी संख्या और बढ़ने की आशंका है। यही वजह है कि सरकार ने अपने स्तर पर इससे बचाव की मुहिम को तेज किया है।

1. साइबर सुरक्षा पर पाठ्यक्रम - विश्वविद्यालय अनुदान आयोग (UGC) ने सभी विश्वविद्यालयों और उच्च शिक्षा संस्थानों को निर्देशित किया है कि वह साइबर सुरक्षा पर कार्य करें और इस विषय को पाठ्यक्रम में शामिल करें. साथ ही सभी संस्थानों से एकेडमिक फ्रैटर्निटी को सुविधाजनक बनाने के लिए प्रोत्साहित करें।

2. शिक्षण संस्थानों 'साईबर सिक्योरिटी अवेयरनैस' अभियान - सभी महाविद्यालयों व विश्वविद्यालयों में 'साईबर सिक्योरिटी अवेयरनैस' अभियान चलाने का निर्णय लिया है ताकि विद्यार्थियों, कर्मचारियों व समाज के अन्य लोगों को 'साईबर फ्रॉड' होने से बचाया जा सके। इसके तहत संस्थानों को नियमित रूप से इसे लेकर सेमिनार, क्विज़,पोस्टर पेंटिंग, हैकथान और प्रतियोगिताओं आदि के माध्यम से साइबर अपराधों के प्रति जागरूकता उत्पन्न करना है।

3. साइबर सुरक्षा जागरुकता हेतु कार्यशालाओं का आयोजन - शिक्षण संस्थानों में साइबर क्राइम के बढ़ते खतरों से आगाह करने के साथ सुरक्षा नियमों के बारे में बताया जाएगा। साइबर विशेषज्ञ की मदद से स्कूलों-कॉलेजों में नियमित तौर पर कार्यशालाएं आयोजित की जाएंगी। विद्यार्थियों को इंटरनेट पर आपराधिक गतिविधियों के बारे में जानकारी देकर बचाव के उपाय बताए जाएंगे।

4. CyberDost की शिक्षा - साइबर अपराध की रोकथाम और इसको लेकर लोगों को जागरुक करने के लिए गृह मंत्रालय ने साइबर दोस्त '@CyberDost' नाम से एक ट्विटर हैंडल लॉन्च किया है. इस हैंडल पर अभी तक वीडियो, तस्वीरों और लिखित कंटेंट के जरिए लोगों को एक हजार से ज्यादा साइबर सुरक्षा टिप्स दिए जा चुके हैं. साइबर अपराध के खिलाफ चलाए जा रहे अभियान से जुड़ने के लिए सरकार के सोशल मीडिया हैंडल से भी जुड़ा जा सकता - https://twitter.com/ Cberdost, Faebook- https://www.facebook.com/Cyberdost14c, Instagram- https://www,istagaram.com /Cyberdosti4c , Telegram - https://t.me/cyberdosti4c

5. 'साइबर जागरुकता दिवस का आयोजन - साइबर अपराध पर अंकुश लगाने के लिए शिक्षा विभाग ने हर सरकारी व निजी स्कूलों में महीने के पहले बुधवार को 'साइबर जागरूकता दिवस' मनाने का आदेश जारी किया है। इस दौरान विद्यार्थियों को साइबर अपराध से बचने के उपाय बताए जाएंगे।इसके तहत स्कूलों में लघु फिल्में दिखाई जाएंगी। साथ ही संगोष्ठी, वाद विवाद प्रतियोगिता, भाषण, प्रश्नोत्तरी प्रतियोगिता, नारा लेखन प्रतियोगिता, आदि का आयोजन होगा। स्किट के जरिए भी विद्यार्थियों को जागरूक किया जाएगा। इन कार्यक्रमों में छठी से 12वीं कक्षा तक के ही विद्यार्थी हिस्सा लेंगे।

6. पुस्तिका का प्रकाशन - गृह मंत्रालय ने कहा है कि साइबर अपराध से छात्रों को जागरुक करने के लिए सरकार ने उनके लिए पुस्तिका का प्रकाशन कराया है. इस पुस्तिका की सहायता से शिक्षक ऑनलाइन सुरक्षा के सत्र संचालित कर सकेंगे। इन सत्रों के जरिए विद्यार्थियों को ऑनलाइन सुरक्षा के विभिन्न पहलुओं जैसे उपकरणों की सुरक्षा, फोन व ऑनलाइन घोटालों से सावधानी, सोशल मिडिया शिष्टाचार के बारे में प्रशिक्षित किया जाएगा। जिम्मेदार नेटीजन बनाया जाएगा। इंटरनेट का उपयोग करने वाला व्यक्ति नेटीजन कहलाता है।

निष्कर्ष

आज हम सभी डिजिटल दुनियां का एक हिस्सा हैं , जहाँ हर क्षेत्र की तरह शिक्षा क्षेत्र भी निरंतर साइबर हमलों का शिकार हो रहा है । किसी संस्थान को साइबर हमलों से बचाने के सबसे महत्वपूर्ण पहलुओं में से एक जागरूकता है । अनेक विद्यार्थी फिशिंग , बुलिंग , सेक्सटोर्सन, रैंसमवेयर, स्पैम आदि साइबर हमलों के शिकार हो रहे हैं जो की चिंताजनक स्थिति है । अतः स्कूलों में साइबर सुरक्षा जागरूकता कार्यक्रम अनिवार्य होना चाहिए ताकि छात्रों और स्टाफ के सदस्यों, हर कोई ऑनलाइन सुरक्षित रहना सीख सके। छात्र सुरक्षा सुनिश्चित करने के लिए शिक्षण संस्थानों को सख्त नीतियां लागू करने की आवश्यकता है। विश्वविद्यालय अनुदान आयोग (यूजीसी) द्वारा साइबर सुरक्षा जागरूकता हेतु जारी निर्देशों को सभी शिक्षण संस्थानों को अनिवार्य रूप से पालन करना चाहिए ताकि हम अपने विद्यार्थियों तथा अन्य कर्मियों को साइबर अपराधों से सुरक्षित रख सकें ।

REFERENCES

1. Amankwa, Eric (2021). "Relevance of Cybersecurity Education at Pedagogy Levels in Schools", Journal of Information Security, Vol. 12, No. 04, October 2021, (https://www.scirp.org/journal/paperinformation.aspx?paperid=111804)
2. Negi, S. and Sunita, M. (2019) Effectiveness of Cyber Bullying Sensitization Program (CBSP) to Reduce Cyber Bullying Behavior among Middle School Children. International Journal of Cyber Research and Education, 1, Article No. 5. (https://doi.org/10.4018/IJCRE.2019010105)
3. Pencheva, D., Joseph, H. and Awais, R. (2020) Bringing Cyber to School: Integrating Cybersecurity into Secondary School Education. IEEE Security & Privacy, 18, 68-74. (https://doi.org/10.1109/MSEC.2020.2969409)
4. https://www.amarujala.com/
5. https://www.aicte-india.org/cyber-securityhindi
6. https://www.egyankosh.ac.in/bitstream/123456789/76767/3/Unit-10.pdf
7. https://isea.gov.in/