शिक्षण संस्थानों में शिक्षण स्तर पर साइबर सुरक्षा शिक्षा की प्रासंगिकता

डॉ0 विक्की
असिस्टेंट प्रोफेसर,
शिक्षाशास्त्र विभाग
हर्ष विद्या मंदिर (पी.जी.) कॉलेज,
रायसी, हरिद्वार उत्तराखण्ड

हरीश राम
असिस्टेंट प्रोफेसर,
समाजशास्त्र विभाग
हर्ष विद्या मंदिर (पी.जी.) कॉलेज,
रायसी, हरिद्वार उत्तराखण्ड
ईमेलः harishhitaishi1@gmail.com

सारांश

आज, इंटरनेट बेहतर संचार, बातचीत और सूचनाओं के आदान–प्रदान के माध्यम से लोगों के जीवन को व्यापक रूप से प्रभावित करता है। इन सभी सकारात्मक प्रभावों के बावजूद, यह महत्वपूर्ण नकारात्मक मुद्दों का भी कारण बनता है। हाल के वर्षों में, इंटरनेट उपयोगकर्ताओं के बीच आत्म–नियंत्रण और समग्र जागरूकता की कमी के कारण ऑनलाइन धोखाधड़ी, साइबर बदमाशी, नस्लीय दुर्व्यवहार, जुआ और पोर्नोग्राफी के मामले बढ़े हैं। इसलिए, छात्रों को साइबर बदमाशी, ऑनलाइन धोखाधड़ी और पूर्वाग्रह के लक्ष्य से बचाने के लिए स्कूलों में साइबर सुरक्षा पर जागरूकता और प्रशिक्षण बनाने की आवश्यकता है। शोध से पता चलता है कि इंटरनेट उपयोगकर्ताओं के बीच आत्म–नियंत्रण और जागरूकता का स्तर अभी भी मध्यम और निम्न है। इंटरनेट उपयोगकर्ताओं के बीच साइबर सुरक्षा जागरूकता और ज्ञान सुनिश्चित करने के लिए, युवाओं को साइबरस्पेस में सुरक्षित रूप से काम करने के तरीके के बारे में शिक्षित होने की आवश्यकता है। यह शिक्षा गारंटी देगी कि वे समझते हैं कि साइबर अपराधों से खुद को कैसे बचाना है। इस हद तक, यह शोध पत्र स्कूलों में साइबर सुरक्षा शिक्षा के सार का पता लगाएगा और ऐसी रणनीतियाँ प्रदान करेगा जिनका उपयोग शिक्षक शिक्षण संस्थानों में साइबर सुरक्षा शिक्षा को बढ़ावा देने के लिए कर सकते हैं। इस प्रकार यह पत्र निष्कर्ष निकालेगा कि साइबर सुरक्षा प्रशिक्षण को शिक्षण संस्थान में कैसे लागू किया जा सकता है।

Reference to this paper should be made as follows:

Received: 08.03.2025
Approved: 22.03.2025

डॉ0 विक्की
हरीश राम

शिक्षण संस्थानों में शिक्षण स्तर पर साइबर सुरक्षा शिक्षा की प्रासंगिकता

RJPP Oct.24-Mar.25,
Vol. XXIII, No. I,
Article No. 19
Pg. 146-162

Online available at:
https://anubooks.com/journal-volume/rjpp-sept-2025-vol-xxiii-no1

मुख्य शब्द

साइबर सुरक्षा, साइबर जागरूकता, साइबर शिक्षा

प्रस्तावना

आज बहुत से लोग इंटरनेट का इस्तेमाल चर्चाओं को बढ़ावा देने, अपनी लोकप्रियता बढ़ाने या अपनी भावनाओं को व्यक्त करने के लिए एक मंच के रूप में करते हैं। वे नागरिक पत्रकारिता में भी संलग्न हैं, जहाँ वे अन्य उपयोगकर्ताओं से बढ़े हुए ध्यान के माध्यम से किसी दिए गए मुद्दे को साझा करने वाले पहले व्यक्ति होने से संतुष्टि प्राप्त करते हैं। फेसबुक, इंस्टाग्राम, ट्विटर और यूट्यूब जैसे विभिन्न सोशल मीडिया प्लेटफॉर्म के माध्यम से, इंटरनेट उपयोगकर्ता किसी दिए गए मुद्दे के बारे में अपने वीडियो, फोटो और यहां तक कि टिप्पणियां भी पोस्ट कर सकते हैं। इस तरह, लोग अक्सर अपनी गतिविधियों, बातचीत और अपने दैनिक जीवन के अन्य पहलुओं को पोस्ट करके इंटरनेट के माध्यम से संपर्क में रहते हैं। हालाँकि, कभी–कभी एक समस्या तब उत्पन्न होती है जब ये इंटरनेट उपयोगकर्ता अपनी सुरक्षा या सामग्री की वैधता की चिंता किए बिना जानकारी साझा करने में जल्दबाजी करते हैं।

मल्टीमीडिया और प्रौद्योगिकी में तेजी से प्रगति के इस युग में, इंटरनेट सभी लोगों, वयस्कों या बच्चों के लिए आसानी से सुलभ है। इसलिए, वैश्विक स्तर पर साइबर सुरक्षा जागरूकता की संस्कृति को विकसित करने के लिए कम उम्र में साइबर सुरक्षा पर ज्ञान और शिक्षा का लाभ उठाया जाना चाहिए। शिक्षकों को इंटरनेट के अत्यधिक उपयोग के लाभों के अलावा इसके प्रतिकूल प्रभावों पर ध्यान केंद्रित करना चाहिए जिसमें व्यक्तिगत जानकारी का जोखिम और जुआ, गेमिंग और पोर्नोग्राफी की लत शामिल है [3]। इन प्रतिकूल प्रभावों ने युवा लोगों के मानसिक स्वास्थ्य और व्यवहार को नकारात्मक रूप से प्रभावित किया है, खासकर वास्तविक दुनिया में उनके सामाजिक संपर्कों के संबंध में।

किशोरों और बच्चों के खिलाफ साइबर अपराध माता–पिता और समाज के बीच एक बढ़ती हुई चिंता है, क्योंकि माता–पिता इस बात से अनजान हैं कि उनके घर में साइबर हमले उनके बच्चों के लिए कितने खतरे पैदा करते हैं। आम तौर पर, बच्चे अपने माता–पिता को अपनी इंटरनेट गतिविधियों के बारे में बताने से बचते हैं, एक ऐसा पहलू जो साइबर हमलों से होने वाले नुकसान का पता लगाना अधिक कठिन बना देता है। षोध से यह भी पता चलता है कि युवा लोगों द्वारा इंटरनेट के बढ़ते उपयोग के कारण साइबरबुलिंग की लोकप्रियता बढ़ी है और इससे भी ज्यादा, स्कूली बच्चे सबसे ज्यादा पीड़ित हैं क्योंकि वे बदमाशी का आसान लक्ष्य होते हैं। इससे भी महत्वपूर्ण बात यह है कि बच्चों द्वारा इंटरनेट का उपयोग करने से उन्हें पक्षपातपूर्ण निशाना बनाने, डराने–धमकाने, उत्पीड़न और यौन शोषण का सामना करना पड़ता है।

किशोरों और बच्चों के खिलाफ साइबर अपराध माता–पिता और समाज के बीच एक बढ़ती हुई चिंता है, क्योंकि माता–पिता इस बात से अनजान हैं कि उनके घर में साइबर हमले उनके बच्चों के लिए कितने खतरे पैदा करते हैं। आम तौर पर, बच्चे अपने माता–पिता को अपनी इंटरनेट गतिविधियों के बारे में बताने से बचते हैं, एक ऐसा पहलू जो साइबर हमलों से होने वाले नुकसान का पता लगाना अधिक कठिन बना देता है। शोध से यह भी पता चलता है कि युवा लोगों द्वारा इंटरनेट के बढ़ते उपयोग के कारण साइबरबुलिंग की लोकप्रियता बढ़ी है और इससे भी ज्यादा, स्कूली बच्चे

सबसे ज्यादा पीड़ित हैं क्योंकि वे बदमाशी का आसान लक्ष्य होते हैं। इससे भी महत्वपूर्ण बात यह है कि बच्चों द्वारा इंटरनेट का उपयोग करने से उन्हें पक्षपातपूर्ण निशाना बनाने, डराने–धमकाने, उत्पीड़न और यौन शोषण का सामना करना पड़ता है न्यूयॉर्क पुलिस द्वारा किए गए शोध से पता चला है कि देश में यौन शोषण के लगभग 80% मामले आभासी दोस्ती से जुड़े थे।

अध्ययन में यह भी दावा किया गया है कि इन हमलों के शिकार मुख्य रूप से किशोर हैं, इसलिए युवाओं को साइबर सुरक्षा ज्ञान के महत्व के बारे में जल्दी से जल्दी सिखाने की आवश्यकता है। इंटरनेट गुमनामी भी प्रदान करता है, एक ऐसा पहलू जो कम उम्र के युवाओं को लक्षित करने वाले यौन शिकारियों की पहचान करना और उन्हें गिरफ्तार करना कठिन बनाता है। इस गुमनामी के कारण किशोरों और बच्चों को यौन शोषण का शिकार बनाने के लिए तैयार करना और भी खराब हो गया है, और अधिकारियों द्वारा पता लगाने से बचने के लिए शिकारियों के तरीके लगातार विकसित होते रहते हैं। आज, बच्चे अपने स्मार्टफोन का उपयोग करने में कुशल और दक्ष हो गए हैं, और यह माता–पिता के लिए एक समस्या बन जाती है जो अपने बच्चों को साइबर हमलों से बचाना चाहते हैं या उनकी ऑनलाइन गतिविधियों पर नजर रखना चाहते हैं। सकारात्मक इरादों के साथ, माता–पिता बच्चों को उनकी सुरक्षा की निगरानी या उनकी पहुँच सुनिश्चित करने के उपाय के रूप में इंटरनेट गैजेट्स तक असीमित पहुँच प्रदान करते हैं। हालाँकि, इस स्वतंत्रता और अप्रतिबंधित पहुँच के साथ, साइबर खतरों के प्रति बच्चों की भेद्यता काफी बढ़ गई है, खासकर उन्हें साइबर अपराध के संपर्क में लाकर। जैसे, जब बच्चे इंटरनेट के विभिन्न लाभों का आनंद लेते हैं, तो उन्हें शैक्षणिक संस्थानों में साइबर सुरक्षा शिक्षा के माध्यम से संबंधित खतरों को समझना चाहिए। साइबर सुरक्षा ज्ञान उन्हें इंटरनेट के उपयोग से जुड़े संभावित जोखिमों से बचाने और साइबर नैतिकता को समझने में मदद करेगा। इस संबंध में, शिक्षकों को जवाबदेह इंटरनेट उपयोग को बढ़ावा देने के लिए साइबर सुरक्षा खतरों का प्रसार करने के लिए जिम्मेदार होना चाहिए। इससे साइबर हमलों की व्यापकता को कम करने में मदद मिलेगी। बाजार, तकनीकी और सामाजिक नवाचार के कारण बच्चों द्वारा विभिन्न सोशल मीडिया प्लेटफार्मों का उपयोग तेजी से विकसित हुआ है।

बच्चों के इंटरनेट उपयोग पर किए गए एक अध्ययन से पता चला है कि वे अपना अधिकांश इंटरनेट समय मिनी–फिल्में, कार्टून, एनिमेशन और गाने देखने में बिताते हैं। छोटे बच्चे कार्टून और एनिमेशन पसंद करते हैं, जबकि बड़े बच्चे ब्लॉग, गेम, संगीत वीडियो, मनोरंजक लघु वीडियो, इंटरनेट व्यक्तित्व और सोशल मीडिया में संलग्न होने सहित विभिन्न प्लेटफार्मों पर अधिक परिपक्व सामग्री देखते हैं। इसलिए, इस पृष्ठभूमि की जानकारी के साथ, स्कूलों को बच्चों को संभावित साइबर खतरों से बचाने के लिए डिजिटल साक्षरता सिखाने में महत्वपूर्ण भूमिका निभानी चाहिए। वे माता–पिता को घर पर उनके इंटरनेट उपयोग को प्रबंधित करने और निगरानी करने के बारे में भी मार्गदर्शन कर सकते हैं ताकि वयस्क सामग्री तक आसान पहुँच को प्रतिबंधित किया जा सके। इससे भी महत्वपूर्ण बात यह है कि माता–पिता को सलाह दी जा सकती है कि वे अपने बच्चों के ऑनलाइन बिताए जाने वाले समय को सरल रणनीतियों और गतिविधियों जैसे कि उन्हें घर के कामों में व्यस्त रखना या उनके साथ गुणवत्तापूर्ण समय बिताना आदि का उपयोग करके कैसे नियंत्रित करें।

स्कूलों में साइबर सुरक्षा ज्ञान का प्राथमिक उद्देश्य युवा इंटरनेट उपयोगकर्ताओं को विभिन्न सोशल मीडिया प्लेटफॉर्म का उपयोग करने के संभावित जोखिमों के बारे में शिक्षित करना है। चौट,

सोशल मीडिया, ईमेल, इंस्टेंट मैसेजिंग और ऑनलाइन गेमिंग जैसे विभिन्न इंटरनेट संचार प्लेटफॉर्म उपयोगकर्ताओं को अन्य इंटरनेट उपयोगकर्ताओं से अपमान और पूर्वाग्रही हमलों जैसे साइबर हमलों के लिए उजागर कर सकते हैं। ये हमले कम आत्मसम्मान वाले लोगों के लिए विशेष रूप से समस्याग्रस्त हैं, जो घृणित टिप्पणियों से प्रभावित होने के उच्च जोखिम में हैं, और इससे अवसाद हो सकता है।

उद्देश्य

शिक्षण संस्थानों में इस शिक्षा के सार पर प्रकाश डालने के लिए स्कूलों में साइबर सुरक्षा ज्ञान के निहितार्थ के बारे में कई पिछले अध्ययन किए गए हैं। हालाँकि, बहुत कम लेख साइबर सुरक्षा जागरूकता पैदा करने में स्कूलों द्वारा लागू किए जाने वाले आवश्यक उपायों पर ध्यान केंद्रित करते हैं। इसलिए, इस शोध का मुख्य उद्देश्य स्कूलों में साइबर सुरक्षा शिक्षा की प्रासंगिकता पर चर्चा करना है। यह अत्यधिक उपयोग से जुड़े जोखिमों, जोखिमों के प्रकारों और उन प्रमुख पहलुओं के बारे में जानकारी देगा, जिन्हें शिक्षकों को गुणवत्तापूर्ण शिक्षा प्रदान करने में उजागर करना चाहिए। साइबर सुरक्षा शिक्षा में बाधा डालने वाले कारकों पर चर्चा की जाएगी, साथ ही साइबर सुरक्षा ज्ञान के महत्व पर भी चर्चा की जाएगी जिसका उपयोग शिक्षक अमेरिकी शिक्षा प्रणाली के संदर्भ में स्कूलों में कर सकते हैं।

साइबर सुरक्षा

आज, प्रौद्योगिकी में उद्भव और उन्नति लोगों को दोहरे दायरे का आनंद लेने की अनुमति देती है, यानी आभासी दुनिया और वास्तविक दुनिया। उदाहरण के लिए, लोगों को नकली इंस्टाग्राम और फेसबुक पोस्ट बनाने के लिए जाना जाता है जो गरीबी में रहते हुए शानदार जीवन शैली दिखाते हैं। YouTube, Yahoo और Google जैसे एप्लिकेषन और सर्च इंजन के साथ, महत्वपूर्ण जानकारी अब सभी लोगों के लिए आसानी से उपलब्ध और सुलभ है, जिनके पास कंप्यूटर और फोन जैसे इलेक्ट्रॉनिक गैजेट हैं, जिससे उपयोगकर्ता अपने निर्धारित लक्ष्य को प्राप्त करने या अपने पीड़ितों को लुभाने के लिए संदेश में हेरफेर कर सकते हैं, इसके अलावा, भौतिक बाजार को धीरे–धीरे ई–कॉमर्स के माध्यम से आभासी बाजार द्वारा प्रतिस्थापित किया जा रहा है, जो व्यवसाय करने के लिए अधिक कुशल और लागत प्रभावी दृष्टिकोण साबित होता है। वेबसाइट की नीति के आधार पर, एक खरीदार उस वस्तु की पहचान करता है जिसे वह खरीदना चाहता है, जिसके बाद वह डिलीवरी से पहले या बाद में भुगतान करता है। हालाँकि, ऑनलाइन व्यापार ने नाटकीय रूप से ऑनलाइन धोखाधड़ी और साइबर अपराधों में योगदान दिया है। उदाहरण के लिए, एक खरीदार एक ऐसी वस्तु खरीद सकता है जो मौजूद नहीं है, लेकिन एक ऑनलाइन बाजार में प्रदर्शित है और इस तरह, खरीदार अक्सर अपने पैसे से ठगा जाता है [4]। अन्य उदाहरणों में, खरीदार महत्वपूर्ण व्यक्तिगत जानकारी प्रदान कर सकता है जिसका उपयोग अविश्वसनीय वेबसाइटों से फिशिंग या पहचान की चोरी के लिए किया जा सकता है। इंटरनेट का बढ़ता उपयोग व्यसनों (जुआ, गेमिंग और पोर्नोग्राफी) और साइबरबुलिंग के विकास सहित प्रतिकूल प्रभावों में भी योगदान देता है। इस तरह के मुद्दों को शुरुआती चरण में ही नियंत्रित किया जाना चाहिए ताकि यह सुनिश्चित हो सके कि इंटरनेट उपयोगकर्ताओं पर उनका सीमित प्रभाव हो। इन इंटरनेट खतरों से निपटने का सबसे अच्छा तरीका शिक्षण संस्थानों में साइबर सुरक्षा शिक्षा को शामिल करना है, जहाँ छात्र संभावित घोटालों या खतरों की पहचान करने और दूसरों के साथ ऑनलाइन बातचीत करने की नैतिकता के बारे में जल्दी ही सीख जाते हैं। इस हद तक साइबर सुरक्षा ज्ञान इंटरनेट उपयोगकर्ताओं के बीच

महत्वपूर्ण है क्योंकि इसमें साइबर खतरों पर प्रतिक्रिया करने के तरीके शामिल हैं ताकि यह सुनिश्चित हो सके कि उनका लोगों के जीवन पर सीमित प्रभाव हो ।

शोध से यह भी पता चलता है कि साइबर अपराध किसी भी समय हो सकते हैं, चाहे संगठन, स्थान और व्यक्ति कोई भी हों। इसलिए, यह शिक्षण संस्थानों के सभी स्तरों पर साइबर सुरक्षा ज्ञान के कार्यान्वयन की मांग करता है। साइबर सुरक्षा अनधिकृत इलेक्ट्रॉनिक डेटा उपयोग और अपराधियों की पहुँच से सुरक्षा की स्थिति है इसमें साइबर अपराधों से सुरक्षा सुनिश्चित करने के लिए किए गए उपाय शामिल हैं। स्कूलों में इस ज्ञान को शामिल करने से एक ऐसी संस्कृति विकसित होगी जो कम उम्र से ही नैतिक इंटरनेट उपयोग को अपनाती है, जो अंततः साइबर अपराधियों द्वारा युवा आबादी पर पड़ने वाले नकारात्मक प्रभावों को कम करती है, खासकर बदमाशी के संबंध में सूचना संचार प्रौद्योगिकी (ICT) के विस्फोट और उन्नति से दैनिक जीवन में भारी बदलाव आए हैं। भौगोलिक सीमाओं की परवाह किए बिना संचार कहीं अधिक कुशल है, और सभी के लिए सूचना आसानी से उपलब्ध है। इससे भी महत्वपूर्ण बात यह है कि प्रौद्योगिकी में उन्नति ने एक ऐसे समाज को विकसित करने में मदद की है जो नवाचार और आविष्कारों को अपनाता है। विचारों के आदान–प्रदान के माध्यम से, इंटरनेट उपयोगकर्ता आसानी से महत्वपूर्ण समस्याओं के समाधान विकसित कर सकते हैं और अंततः दीर्घकालिक रूप से अधिक सकारात्मक समुदाय की स्थापना में योगदान दे सकते हैं। हालाँकि, अपराधी इन प्रगति का फायदा उठाकर साइबर अपराधों को अंजाम देने के नए तरीके ईजाद कर सकते हैं, जबकि अधिकारियों द्वारा उनकी गुमनामी और पता न लगा पाना सुनिश्चित करते हैं। वर्ल्ड वाइड वेब ने संगठनों और व्यक्तियों को दूरियों के पार महत्वपूर्ण जानकारी को आसानी से प्रदर्शित और साझा करने में सक्षम बनाया है। हालाँकि, कभी–कभी इस जानकारी का उपयोग हानिकारक उद्देश्यों के लिए किया जा सकता है, जो लोगों के जीवन को नकारात्मक रूप से प्रभावित करता है। उदाहरण के लिए, अपराधी रैनसमवेयर विकसित करते हैं और इसका उपयोग बड़े निगमों को लक्षित करने के लिए करते हैं, जब तक कि उन्हें किसी प्रकार का भुगतान न मिले, महत्वपूर्ण डेटा और जानकारी को उजागर करने की धमकी देते हैं।

साइबर सुरक्षा को उस प्रक्रिया, स्थिति या गतिविधि के रूप में भी वर्णित किया जा सकता है जिसमें संचार प्रणालियों और सूचनाओं को संशोधन, अनाधिकृत पहुँच या शोषण से बचाया जाता है। इसलिए, साइबर सुरक्षा ज्ञान लोगों को रैनसमवेयर [14] जैसे साइबर खतरों से बचाने में मदद कर सकता है। बच्चे अक्सर वयस्क सामग्री जैसे कई खतरों के संपर्क में आते हैं जिनका वे गेम और वीडियो में सामना कर सकते हैंय यह सामग्री उनके मानसिक स्वास्थ्य को नकारात्मक रूप से प्रभावित कर सकती है। इस हद तक, माता–पिता भी यह सुनिश्चित करके साइबर सुरक्षा ज्ञान से लाभान्वित हो सकते हैं कि वे अपने बच्चों को हानिकारक ऑनलाइन सामग्री से बचाने में मदद करें। माता–पिता बच्चों को हानिकारक सामग्री से प्रतिबंधित करने के लिए टेलीविजन और फोन में अभिभावकीय नियंत्रण स्थापित करके और अपने बच्चों को उनकी ऑनलाइन गतिविधियों और संबंधित जोखिमों पर सक्रिय बातचीत में शामिल करके ऐसा कर सकते हैं।

साइबर सुरक्षा के सिद्धांत

आम तौर पर, साइबर सुरक्षा सिद्धांत मार्गदर्शन करते हैं कि लोग और संस्थाएँ साइबर खतरों से खुद को कैसे बचा सकती हैं जो उनके संग्रहीत डेटा और सूचना के लिए हानिकारक हो सकते हैं।

इस तरीके से, साइबर सुरक्षा सिद्धांत महत्वपूर्ण डेटा और सूचना की सुरक्षा में मदद करते हैं, और उन्हें चार मुख्य श्रेणियों में बांटा गया हैय सुरक्षा, नियंत्रण, प्रतिक्रिया और पता लगाना। शासी सिद्धांत अक्सर विभिन्न सुरक्षा जोखिमों के प्रबंधन और पहचान में शामिल होते हैं, जो साइबर खतरों का पता लगाने में मदद करते हैं। इसके अतिरिक्त, सुरक्षा सिद्धांतों को साइबर खतरों के प्रति भेद्यता को रोकने और कम करने में मदद करने के लिए कई सुरक्षा नियंत्रणों को लागू करने के लिए डिजाइन किया गया है। ऐसे प्रतिक्रिया सिद्धांत भी हैं जो विभिन्न साइबर अपराध घटनाओं से उबरने और उनका जवाब देने के लिए डिजाइन किए गए हैं। इसलिए, यह सिद्धांत भविष्य में इसी तरह की घटना को रोकने में मदद करता है। अंत में, पता लगाने के सिद्धांत यह सुनिश्चित करते हैं कि साइबर सुरक्षा घटनाओं का पता लगाया जाए, उन्हें हल किया जाए और नकारात्मक प्रभावों से बचने के लिए समझा जाए। इससे भी महत्वपूर्ण बात यह है कि ये सिद्धांत दिए गए साइबरस्पेस की सुरक्षा सुनिश्चित करने के लिए अपने अलग दिशानिर्देशों (जी 1 से जी 5 लेबल) का पालन करते हैं। उदाहरण के लिए, जी 1 में अक्सर एक मुख्य सुरक्षा अधिकारी शामिल होता है जो साइबर सुरक्षा कार्यक्रमों में निरीक्षण और नेतृत्व प्रदान करता है। इस तरीके से, वे किसी भी गलती से बचने के लिए विभिन्न प्रक्रियाओं की अनदेखी करते हैं। जी 2 भी महत्वपूर्ण है क्योंकि यह कई प्रणालियों, डेटा और अनुप्रयोगों में दोषों की पहचान करने में मदद करता है। इस तरह, उन्हें अक्सर भविष्य के संदर्भ के लिए अनुमति देने के लिए प्रलेखित किया जाता है। जी 3 भी महत्वपूर्ण है क्योंकि यह अनुप्रयोगों, डेटा और विभिन्न प्रणालियों की अखंडता, उपलब्धता और गोपनीयता में मदद करता है। इसके अतिरिक्त, जी 4 भी महत्वपूर्ण है क्योंकि यह विभिन्न ढांचे में एम्बेडेड साइबर सुरक्षा प्रक्रियाओं का प्रबंधन करता है। जी 5 कोड भी महत्वपूर्ण है क्योंकि यह उपयोग के लिए अधिकृत अनुप्रयोगों और प्रणालियों का दस्तावेजीकरण, प्रबंधन और पहचान करने में मदद करता है, सुरक्षा सिद्धांतों में भी विभिन्न श्रेणियां हैं। पहला पी 1 है, जो गोपनीयता, मूल्य, उपलब्धता और अखंडता के अनुसार अनुप्रयोगों को तैनात करने, बनाए रखने और डिजाइन करने में मदद करने के लिए डिजाइन किया गया सिस्टम है। दूसरी ओर, पी 2 को ऑनलाइन उपयोगकर्ताओं को विश्वसनीय आपूर्तिकर्ताओं का समर्थन करने और वितरित करने के लिए डिजाइन किया गया है, इससे संस्थानों को उनकी मासूमियत से लाभ मिलता है। इसके अतिरिक्त, पी 3 है जो साइबर हमलों के लिए सिस्टम की भेद्यता को फैलाने और कम करने में मदद करने के लिए कॉन्फिगर किया गया सिस्टम है। पी 4 यह सुनिश्चित करने में भी महत्वपूर्ण है कि एप्लिकेशन और सिस्टम को जवाबदेह, ऑडिट करने योग्य और सुरक्षित रखा जाए। अंत में, पी 5 यह सुनिश्चित करने में महत्वपूर्ण है कि विभिन्न सुरक्षा कमजोरियों की पहचान की जाए और उन पर अंकुश लगाया जाए।

शैक्षिक संस्थान साइबर सुरक्षा को बनाए रखने में मदद करने के लिए विभिन्न परिपक्वता मॉडलिंग योजनाओं का लाभ उठा सकते हैं। पाँच परिपक्वता स्तरों में शामिल हैं अपूर्ण, प्रारंभिक, प्रबंध, विकासशील और अनुकूलन प्रारंभिक का अर्थ है कि साइबर सुरक्षा सिद्धांतों का उपयोग किया जाता है लेकिन खराब तरीके से। अपूर्ण का अर्थ है कि कोड लागू नहीं किए गए हैं या आंशिक रूप से लागू किए गए हैं। विकासशील मॉडल का मतलब है सिद्धांतों को अच्छी तरह से लागू किया गया है। दूसरी ओर, प्रबंध सिद्धांत का मतलब है कि नियमों को मानक व्यवसाय नीति और अभ्यास के रूप में स्थापित किया गया था। अंत में, अनुकूलन मॉडल का तात्पर्य निरंतर सुधार और अनुकूलन पर एक

जानबूझकर ध्यान केंद्रित करना है। इसलिए, साइबर सुरक्षा अक्सर तब सुनिश्चित होती है जब इन सिद्धांतों को बरकरार रखा जाता है।

साइबर सुरक्षा ज्ञान की आवश्यकता

मल्टीमीडिया और साइबर अपराध जांच प्रभाग द्वारा किए गए शोध से पता चला है कि साइबर–लव घोटाले संयुक्त राज्य अमेरिका से संबंधित हैं [11]। ऐसे मामलों में, घोटालेबाज अक्सर इंटरनेट पर अपने पीड़ितों को ढूंढते हैं और वित्तीय मदद या व्यक्तिगत जानकारी मांगने से पहले यह सुनिश्चित करने में गुणवत्ता समय बिताते हैं कि पीड़ितों की सुरक्षा से समझौता हो सकता है। ये मामले हाल ही में बढ़ रहे हैं, क्योंकि कुछ युवाओं को यह तेजी से पैसा कमाने का एक आकर्षक तरीका लगता है। संयुक्त राज्य अमेरिका में साइबर अपराधों की संख्या में जबरदस्त वृद्धि हुई है, 2012 में 814 मामले और अगले वर्ष 1095 मामले दर्ज किए गए, और 2020 में मुख्य रूप से COVID–19 महामारी के कारण सापेक्ष वृद्धि हुई। ये मामले बड़े पैमाने पर हुए हैं और पीड़ितों के पैसे की हानि में योगदान दिया है। हालाँकि अमेरिका ने इंटरनेट धोखाधड़ी को रोकने के लिए कई उपाय किए हैं, लेकिन यह बुराई आज भी प्रचलित है और बड़ी उम्र के लोगों और युवाओं को निशाना बनाती है। इसके अलावा, इंटरनेट पर अवैध सामानों की धोखाधड़ी से खरीद अमेरिका में प्रचलित है, जिसमें राष्ट्र आवास, पर्यटन और ऑटोमोबाइल क्षेत्र से जुड़े अरबों डॉलर के नुकसान को दर्ज करता है। इसलिए, युवा लोगों के बीच साइबर अपराध को रोकने के लिए स्कूलों में साइबर सुरक्षा शिक्षा को शामिल करने की आवश्यकता है; यह वयस्कता में भी लागू होगा। लोगों के बीच साइबर सुरक्षा ज्ञान की संस्कृति विकसित की जाएगी। इससे भी महत्वपूर्ण बात यह है कि साइबर सुरक्षा ज्ञान और शिक्षा इंटरनेट पर उपलब्ध पोर्नोग्राफी और कंप्यूटर गेम की लत को रोकने में भी महत्वपूर्ण है। इस लत के परिणामस्वरूप अक्सर असामाजिक व्यवहार विकसित होते हैं। चूंकि किशोर अपना अधिकांश समय सामाजिक मेलजोल और कंप्यूटर गेम खेलने में बिताते हैं, इसलिए वे अक्सर आभासी दुनिया की ओर आकर्षित हो जाते हैं और ज्यादातर मामलों में, वे वास्तविक दुनिया से संपर्क खो सकते हैं। समय के साथ कंप्यूटर गेम की लत अपरिहार्य हो सकती है और बच्चों का कीमती समय उनके गैजेट्स में व्यतीत हो सकता है। इस तरह, ऐसे बच्चे अपनी शिक्षा और दोस्तों के साथ बातचीत में संघर्ष कर सकते हैं। इसलिए, इंटरनेट युवा लोगों पर प्रतिकूल प्रभाव डालने के लिए जिम्मेदार है। स्कूलों में साइबर सुरक्षा ज्ञान को लागू करके इसे रोका जा सकता है। इससे भी महत्वपूर्ण बात यह है कि इंटरनेट का अत्यधिक उपयोग नींद के पैटर्न में असंतुलन से जुड़ा है; बच्चे अक्सर अपना रात का समय इंटरनेट ब्राउज करने और वीडियो गेम खेलने में बिताते हैं। आमतौर पर, नींद के पैटर्न में असंतुलन स्वास्थ्य समस्याओं से जुड़ा होता है जो बच्चे के जीवन को प्रभावित कर सकता है। इसलिए, साइबर खतरे विभिन्न तरीकों से आते हैं जो लोगों को कई तरह से प्रभावित करते हैं। उदाहरण के लिए, अत्यधिक इंटरनेट उपयोग को अवसाद और आघात से जोड़ा गया है क्योंकि कुछ लोग इंटरनेट पर जो जीवन देखते हैं उसे जीने की उम्मीद करते हैं। ऐसे मामलों में, इंटरनेट उपयोगकर्ता अक्सर अपने शानदार जीवन को पोस्ट करते हैं जो जीवन से जूझ रहे लोगों के लिए तनावपूर्ण हो सकता है। हालांकि, शोध से पता चला है कि कुछ लोग नकली जीवन पोस्ट करते हैं, जिससे उनके सहकर्मियों को अनावश्यक मनोवैज्ञानिक नुकसान होता है। इसके अतिरिक्त, युवा इंटरनेट उपयोगकर्ताओं के बीच साइबर सुरक्षा ज्ञान महत्वपूर्ण है क्योंकि कुछ को पता नहीं हो सकता

है कि वे साइबर हमलों के शिकार हैं। साथ ही, कुछ इंटरनेट उपयोगकर्ताओं ने अन्य इंटरनेट उपयोगकर्ताओं पर हमला करते समय सचेत न होने की सूचना दी है। उदाहरण के लिए, साइबरबुलिंग बच्चों द्वारा मौज–मस्ती करने और अपने दोस्तों को चिढ़ाने के लिए की जा सकती है। इस संबंध में, वे अपने दोस्तों को होने वाले नुकसान की सीमा से अनजान हो सकते हैं। इसलिए, साइबर सुरक्षा शिक्षा युवा इंटरनेट उपयोगकर्ताओं को साइबरबुलिंग के विभिन्न रूपों के बारे में शिक्षित करेगीय इससे भी महत्वपूर्ण बात यह है कि यह उन्हें ऐसे हमलों को रोकने में मदद करेगी। उदाहरण के लिए, शोध से पता चला है कि जो इंटरनेट उपयोगकर्ता अपनी पोस्ट से टिप्पणियाँ और सूचनाएँ बंद कर देते हैं, वे साइबरबुलिंग से बचने की संभावना रखते हैं।

हमले और कमजोरियाँ

साइबर भेद्यता विभिन्न कंप्यूटर सिस्टम के कार्यान्वयन, डिजाइन, आंतरिक नियंत्रण और संचालन में एक कमजोरी है। इनमें से अधिकांश कमजोरियों को कॉमन वल्नरेबिलिटीज एंड एक्सपोजर (CVE) डेटाबेस द्वारा प्रलेखित और इनपुट किया जाता है। आमतौर पर, कमजोरियों को अनुकूलित स्क्रिप्ट या स्वचालित टूल [5] का उपयोग करके शिकार, शोषण, शोध और रिवर्स इंजीनियर किया जा सकता है। इसलिए, कंप्यूटर सिस्टम की सुरक्षा सुनिश्चित करने के लिए, सबसे पहले उन हमलों को समझना महत्वपूर्ण है जो कंप्यूटर पर किए जा सकते हैं। इन खतरों को समझना उनसे निपटने के उपायों को विकसित करने और इंटरनेट के सुरक्षित उपयोग को सुनिश्चित करने में महत्वपूर्ण है। उदाहरणों में शामिल हैं।

पिछले दरवाजे

बैकडोर एक एल्गोरिथ्म या क्रिप्टोसिस्टम है जो प्रमाणीकरण को बायपास करने में एक गुप्त विधि प्रदान करता है। आम तौर पर, ये साइबर खतरे सुरक्षा नियंत्रणों को पारित करने का एक समाधान प्रदान करते हैं, जो अक्सर इंटरनेट उपयोगकर्ताओं के लिए हानिकारक होते हैं। इसके अतिरिक्त, यह साइबर खतरा खराब कॉन्फिगरेशन और मूल डिजाइन के कारण मौजूद है जो इस तरह के साइबर खतरे को जन्म दे सकता है। इसके अलावा, खतरे को किसी अधिकृत व्यक्ति द्वारा वैध पहुँच की अनुमति देने में नियोजित किया जा सकता है। हालाँकि, साइबर हमलावर बैकडोर का लाभ उठा सकते हैं और दुर्भावनापूर्ण उद्देश्यों के लिए उनका उपयोग कर सकते हैं। किसी भी तरह से, उनके उपयोग की परवाह किए बिना, वे अभी भी इंटरनेट उपयोगकर्ताओं के बीच कमजोरियाँ पैदा करते हैं। आमतौर पर, बैकडोर का पता लगाना मुश्किल होता है, और उन्हें अक्सर किसी दिए गए कंप्यूटर सिस्टम पर स्वीप करने के लिए आईटी विशेषज्ञों की आवश्यकता होती है।

सेवा निषेध हमला

सेवा से वंचित करने वाला हमला अक्सर नेटवर्क या मशीन संसाधन को बाधित करने के लिए डिजाइन किया जाता है। ऐसे मामलों में, वे अक्सर इन संसाधनों को अनुपलब्ध कर देते हैं, जो इंटरनेट उपयोगकर्ताओं के लिए चुनौतीपूर्ण हो सकता है। उदाहरण के लिए, इस मामले में हमलावर केवल गलत पासवर्ड डालकर इंटरनेट उपयोगकर्ताओं को महत्वपूर्ण वेबसाइटों तक पहुँच से वंचित कर सकते हैं। इस तरह, गलत पासवर्ड कई बार डाला जाता है जब तक कि खाता ब्लॉक न हो जाए। आम तौर पर, ये हमले वहाँ बड़े पैमाने पर होते हैं जहाँ कोई हमलावर किसी महत्वपूर्ण स्थान से आता है, और

इसलिए, उनके स्थान का पता लगाना असंभव हो जाता है। इसके अलावा, ये हमले आम तौर पर जॉम्बी कंप्यूटरों में कई संभावित तकनीकों के साथ आम हैं जिनमें शामिल हैं; प्रवर्धन और प्रतिबिंब हमले।

प्रत्यक्ष पहुँच हमले

डायरेक्ट एक्सेस अटैक में अक्सर साइबर हमलावर कंप्यूटर पर भौतिक कब्जा और पहुँच प्राप्त करते हैं। आमतौर पर, इन कंप्यूटरों को अक्सर संग्रहीत जानकारी के कारण किसी दिए गए निकाय और संगठन के लिए महत्वपूर्ण माना जाता है। इसलिए इन कंप्यूटरों तक भौतिक पहुँच पीड़ितों के लिए हानिकारक हो सकती है [3]। इस मामले में, हमलावर ऑपरेटिंग सिस्टम में बदलाव और संशोधन कर सकते हैं जो कंप्यूटर के अंदर के डेटा को प्रभावित करते हैं। इसके अतिरिक्त, हमलावर महत्वपूर्ण लॉगर और सॉफ्टवेयर वर्म स्थापित कर सकते हैं जो कंप्यूटर के अंदर के डेटा और जानकारी को बर्बाद कर सकते हैं। ऐसे मामलों में, जब सुरक्षा प्रणालियाँ कंप्यूटर की सुरक्षा करती हैं, तब भी हमलावर उन्हें बायपास करने के तरीके खोज सकते हैं।

गुप्त रूप से सुनना

हाल ही में ईव्सड्रॉपिंग भी बढ़ रही है, जिसमें हमलावर निजी बातचीत को सुनने का लक्ष्य रखते हैं। आम तौर पर ये अंतरंग बातचीत अक्सर इंटरनेट पर की जाती है, और हमलावर ऐसी चर्चाओं तक पहुँच सकते हैं। उदाहरण के लिए, अमेरिका में NSA और FBI नेटवर्क पर बातचीत की निगरानी के लिए Narus In Sight और Carnivore जैसे सॉफ्टवेयर का उपयोग करते हैं। हालाँकि इस अधिनियम के बारे में विभिन्न आलोचनाएँ हैं, शोधकर्ताओं का दावा है कि यह गोपनीयता का उल्लंघन है, अधिकारियों ने जोर देकर कहा है कि ईव्सड्रॉपिंग राष्ट्रीय सुरक्षा के लिए महत्वपूर्ण है। इस तरह, कई अपराधी हमले करने की योजना बनाते समय पकड़े गए हैं।

फिशिंग

फिशिंग आज बहुत प्रचलित है, और इनका उपयोग संवेदनशील डेटा और जानकारी जैसे पासवर्ड, क्रेडिट कार्ड और उपयोगकर्ता नाम प्राप्त करने में किया जाता है जिसका उपयोग इंटरनेट उपयोगकर्ताओं के खिलाफ हमले करने में किया जा सकता है। यह आमतौर पर इंटरनेट उपयोगकर्ताओं को धोखा देकर किया जाता है, अक्सर उनके उपयोगकर्ता नाम और पासवर्ड लीक करके। आमतौर पर फिशिंग इंस्टेंट मैसेजिंग और ईमेल स्पूफिंग के माध्यम से संचालित की जाती है ताकि यह सुनिश्चित किया जा सके कि इंटरनेट उपयोगकर्ता साइबर हमलावरों पर पूरी तरह से भरोसा करते हैं। तुलनात्मक रूप से, ऐसे हमलावर नकली वेबसाइट बना सकते हैं जो पासवर्ड और उपयोगकर्ता नाम मांगते हैं।

सोशल इंजीनियरिंग

सोशल इंजीनियरिंग एक साइबर हमला है जिसका उद्देश्य इंटरनेट उपयोगकर्ताओं को कार्ड नंबर और पासवर्ड जैसे व्यक्तिगत जानकारी और रहस्यों का खुलासा करने के लिए राजी करना है। आम तौर पर, सोशल इंजीनियरिंग में भरोसेमंद संस्थानों के रूप में प्रस्तुत करके इंटरनेट उपयोगकर्ताओं का विश्वास हासिल करना शामिल है जिसके बाद व्यक्तिगत जानकारी प्राप्त की जाती है। आम तौर पर, हमलावर अक्सर बैंकों, वरिष्ठ अधिकारियों, ग्राहकों और ठेकेदारों का प्रतिरूपण करते हैं, जो उन्हें व्यक्तिगत जानकारी तक पहुँच प्राप्त करने में मदद करता है। अक्सर वित्त और लेखा विभाग के कर्मियों

को अवैध कार्रवाई का अनुरोध करते हुए ईमेल भेजे जाते हैं। स्कूलों में साइबर सुरक्षा शिक्षा भी युवा इंटरनेट उपयोगकर्ताओं को यह सुनिश्चित करने में महत्वपूर्ण साबित हुई है कि वे विभिन्न साइबर खतरों को समझें। उदाहरण के लिए, कंप्यूटर का उपयोग करने वाले इंटरनेट उपयोगकर्ताओं को अक्सर मैलवेयर हमले का सामना करने का खतरा होता है। मैलवेयर दुर्भावनापूर्ण इरादे से बनाया और उपयोग किया जाने वाला वायरस है। आम तौर पर, मैलवेयर में कई सॉफ्टवेयर शामिल होते हैं जो ट्रोजन हॉर्स, वायरस, रूटकिट, क्रिप्टो–जैकिंग, वर्म्स और स्पाइवेयर तक सीमित नहीं होते हैं। इसी तरह, इंटरनेट उपयोगकर्ता रैनसमवेयर हमलों से भी पीड़ित हो सकते हैं। साइबर हमले एक कंप्यूटर सिस्टम पर किए जाते हैं जहाँ सॉफ्टवेयर फिरौती के बदले में महत्वपूर्ण डेटा और जानकारी को एन्क्रिप्ट करता है; यह मैलवेयर किसी दिए गए संगठन को पंगु बना सकता है [14]। इस हद तक साइबर सुरक्षा शिक्षा भविष्य की पीढ़ी के लिए आवश्यक हो सकती है क्योंकि यह एक ऐसे समाज की ओर ले जाएगी जो साइबर सुरक्षा जागरूकता को स्वीकार करता है। इससे भी महत्वपूर्ण बात यह है कि स्कूलों में बच्चों को साइबर सुरक्षा संस्कृति स्थापित करने में मदद करने के लिए ऑनलाइन प्लेटफॉर्म और संसाधनों के जिम्मेदार और सुरक्षित उपयोग पर सषक्त बनाया जा सकता है ।

साइबर सुरक्षा शिक्षा की सीमाएँ

अमेरिका में इस्तेमाल किए जाने वाले सबसे लोकप्रिय सोशल मीडिया एप्लिकेशन में इंस्टाग्राम, फेसबुक, यूट्यूब, ट्विटर और लिंक्ड शामिल हैं। ये एप्लिकेशन यह सुनिश्चित करने के लिए जिम्मेदार हैं कि दोस्त अलग–अलग राज्यों में होने पर भी संपर्क में रहें। इस संबंध में, इन प्लेटफॉर्म ने पूरे देश में संचार जारी रखा है। इससे भी महत्वपूर्ण बात यह है कि मीडिया के पास ऐसे प्रोफाइल हैं जो पूरे अमेरिका में लोगों को समाचार और सार्थक जानकारी प्रदान करते हैं। इस प्रकार, लोग इन सोशल मीडिया एप्लिकेशन में उपलब्ध छवियों, ऑडियो और वीडियो की विशाल श्रृंखला से सीख सकते हैं। हालाँकि, समस्या तब उत्पन्न होती है जब इस जानकारी के विस्फोट के परिणामस्वरूप विभिन्न सुरक्षा और गोपनीयता जोखिम होते हैं ।

इंटरनेट पर मौजूद जानकारी की सटीकता और प्रामाणिकता अक्सर सवालों का विषय रही है। शोधकर्ताओं का मानना है कि इस जानकारी को सत्यापित करना असंभव है क्योंकि ये हमसे लाखों मील दूर लोगों द्वारा पोस्ट की जाती हैं [5] । इसलिए, लोगों को अतिरिक्त सावधानी बरतनी होगी, खासकर इन वीडियो और छवियों को साझा करते समय सबसे महत्वपूर्ण बात यह है कि बच्चों को नकली सूचनाओं से बचाना होगा क्योंकि यह उनके जीवन को गुमराह कर सकती है। इस मामले में, साइबर सुरक्षा शिक्षा यह सुनिश्चित करने में महत्वपूर्ण होगी कि युवा इंटरनेट उपयोगकर्ता नकली सूचनाओं से खुद का बचाव करने के लिए आवश्यक ज्ञान से लैस हों। साथ ही, वे इंटरनेट पर अपने कार्यों की जिम्मेदारी लेना सीख सकते हैं, हालाँकि, साइबर सुरक्षा शिक्षा को कई चुनौतियों का सामना करना पड़ता है जो अक्सर शिक्षण संस्थानों में इसके कार्यान्वयन में बाधा डालती हैं। उदाहरण के लिए, मुख्य चुनौती यह सुनिश्चित करना है कि ट्यूटर्स को आज की विभिन्न साइबर खतरों को गंभीरता से समझने की उनकी क्षमता को बढ़ावा देने के लिए अद्यतित जानकारी के साथ अच्छी तरह से प्रशिक्षित किया जाए। आज अधिक साइबर खतरे अक्सर सामने आते हैं, जो ट्यूटर्स के लिए एक चुनौती है क्योंकि उन्हें सीखना होगा कि ऐसे खतरों से कैसे निपटा जाए। इसके अतिरिक्त, दूसरी

चुनौती यह है कि शिक्षकों के लिए घर पर रहते हुए शिक्षार्थियों द्वारा फोन और कंप्यूटर के उपयोग को ट्रैक करना असंभव हो सकता है। इसलिए, हालाँकि स्कूलों में साइबर सुरक्षा शिक्षा लागू की जा सकती है, फिर भी शिक्षार्थी घर पर साइबर खतरों के संपर्क में रहते हैं। माता–पिता का नियंत्रण भी चुनौतीपूर्ण साबित हुआ है, खासकर उन अभिभावकों के लिए जो हमेषा काम में व्यस्त रहते हैं। अक्सर घर पर छोड़े गए बच्चे फोन और कंप्यूटर जैसे गैजेट के जरिए इंटरनेट का दुरुपयोग करने की संभावना रखते हैं। ऐसे मामलों में, माता–पिता इस बात पर नजर नहीं रख पाते कि उनके बच्चे इंटरनेट का उपयोग कैसे करते हैं, जिससे वे विभिन्न साइबर खतरों के संपर्क में आ जाते हैं। उदाहरण के लिए, बिना देखभाल के छोड़े गए बच्चे पोर्नोग्राफी या वीडियो गेम के आदी हो सकते हैं जिसका उनके मानसिक स्वास्थ्य पर बहुत बुरा असर पड़ सकता है। ऐसे मामलों में, इन बच्चों में बलात्कार और छेड़छाड़ जैसे असामाजिक व्यवहार विकसित होने का ज्यादा जोखिम होता है इसके अतिरिक्त, विशेषज्ञता की कमी शिक्षण संस्थानों में साइबर सुरक्षा शिक्षा के कार्यान्वयन के लिए चुनौतीपूर्ण साबित हुई है। साइबर सुरक्षा पेशेवरों की सीमित संख्या के साथ, स्कूलों में साइबर सुरक्षा शिक्षा को शामिल करना चुनौतीपूर्ण हो जाता है। इससे भी महत्वपूर्ण बात यह है कि निर्देश के कार्यान्वयन के लिए धन और संसाधनों की आवश्यकता होती है जो उन स्कूलों के लिए चुनौतीपूर्ण हो सकता है जो अपने वित्त से जूझ रहे हैं। ऐसे मामलों में, सरकार से धन और अनुदान प्राप्त करने में विफलता से कार्यक्रम का नुकसान हो सकता है। इसके अलावा, स्कूलों में अधिकांश शिक्षकों के पास साइबरस्पेस के बारे में विशेषज्ञता और ज्ञान की कमी है। इसलिए, स्कूलों को बच्चों के बीच साइबर सुरक्षा जागरूकता में मदद करने के लिए आईटी पेशेवरों को नियुक्त करने के लिए मजबूर होना पड़ सकता है। ऐसे मामलों में, सीमित संसाधनों वाले स्कूल आईटी पेशेवरों को नियुक्त करने में विफल हो सकते हैं, जिससे ऐसे कार्यक्रम विफल हो सकते हैं [12]। सरकारी मंत्रालयों को शिक्षण संस्थानों में साइबर सुरक्षा ज्ञान को शामिल करने में स्कूलों की सहायता के लिए आगे आना चाहिए।

आज की तकनीकी प्रगति की गति उन स्कूलों के लिए जोखिम और नई चुनौतियाँ पेश करती है जो अपने पाठ्यक्रम में साइबर सुरक्षा शिक्षा को लागू करना चाहते हैं। इसलिए, आईटी पेशेवरों को अपने कौशल और ज्ञान को नवीनतम तकनीक के अनुसार विकसित करना चुनौतीपूर्ण लग सकता है। ऐसे मामलों में, साइबर खतरों से बच्चों की सुरक्षा सुनिश्चित करना चुनौतीपूर्ण हो सकता है। इसलिए, स्कूलों में इस कार्यक्रम को लागू करने के लिए शिक्षकों को तकनीकी प्रगति और बदलाव के प्रति अपनी संवेदनशीलता बढ़ाने की आवश्यकता है। इसके अतिरिक्त, कुछ शिक्षकों के पास विशेष शिक्षण सामग्री तक पहुँच की कमी हो सकती है जो उनके तकनीकी ज्ञान का विस्तार करते समय चुनौतीपूर्ण हो सकती है। इन सीमाओं को कम करने के लिए, साइबर सुरक्षा सेमिनार और संगोष्ठियों के माध्यम से साइबर सुरक्षा के लिए प्रारंभिक प्रशिक्षण और प्रदर्शन आयोजित किया जाना चाहिए। इससे भी महत्वपूर्ण बात यह है कि इस कार्यक्रम के कार्यान्वयन के लिए छात्रों, शिक्षकों और अभिभावकों दोनों के सहयोग की आवश्यकता है ताकि छात्रों के बीच साइबर सुरक्षा जागरूकता को बढ़ावा दिया जा सके। माता–पिता को यह सुनिश्चित करना चाहिए कि वे अपने बच्चों को फोन और कंप्यूटर पर इंटरनेट का उपयोग करते समय अभिभावकीय नियंत्रण प्रदान करके घर पर अपनी भूमिका निभाएँ। साइबर सुरक्षा प्रशिक्षण के संपर्क में आने वाले लोगों से अक्सर दूसरों को प्रशिक्षित करने की अपेक्षा की जाती है क्योंकि वे साइबर रक्षा में देश का भविष्य हैं।

शिक्षण संस्थानों में साइबर सुरक्षा शिक्षा का महत्व

विभिन्न शोध निष्कर्षों के अनुसार, शिक्षण संस्थान साइबर सुरक्षा शिक्षा से काफी लाभ उठा सकते हैं। शोधकर्ताओं ने खुलासा किया है कि अधिकांश वयस्क अक्सर कार्यक्रमों और सेमिनारों में साइबर सुरक्षा ज्ञान प्राप्त करने के लिए समय या पैसा खर्च करने के लिए तैयार नहीं होते हैं। इस मामले में, ऐसे वयस्क अक्सर ऐसे हमलों से खुद को बचाने के बारे में ज्ञान की कमी के कारण साइबर हमलों का शिकार हो जाते हैं। इसलिए, साइबर सुरक्षा पर पर्याप्त प्रशिक्षण सुनिश्चित करने के लिए स्कूल सबसे अच्छी जगह साबित हुए हैं। ऐसा इसलिए है क्योंकि युवा लोग अक्सर सीखने के लिए तैयार और इच्छुक होते हैं, और यह कौशल उन्हें एक राष्ट्र के रूप में संयुक्त राज्य अमेरिका को साइबर सुरक्षा प्रदान करने में मदद कर सकता है।

स्कूलों में, शिक्षक और प्रशासक साइबर सुरक्षा पर प्रशिक्षण में मदद करने वाली गतिविधियों और कार्यक्रमों का आयोजन कर सकते हैं। इसके अतिरिक्त, अमेरिका में स्कूलों को संघीय सरकार से अनुदान और वित्तीय आवंटन प्रदान किया जाता है ताकि यह सुनिश्चित किया जा सके कि वे किसी भी वित्तीय बाधाओं का सामना कर सकें। इस संबंध में, अमेरिका में स्कूल, विशेष रूप से न्यूयॉर्क में, अपने पाठ्यक्रम में साइबर सुरक्षा शिक्षा को लागू करने के लिए बेहतर स्थिति में हैं। इससे भी महत्वपूर्ण बात यह है कि स्कूल संगोष्ठियों और सेमिनारों का आयोजन कर सकते हैं जहाँ छात्र साइबर सुरक्षा मुद्दों पर अपने दिमाग को खपाते हैं। इससे छात्रों के साइबर सुरक्षा जागरूकता के ज्ञान और कौशल को बेहतर बनाने में मदद मिल सकती है। सरकारी फंडिंग इन सेमिनारों के खर्चों को कवर करने में मदद कर सकती है। इसके अतिरिक्त, साइबर सुरक्षा शिक्षा छात्रों की मानसिकता को बदलने में महत्वपूर्ण साबित हुई है। प्रौद्योगिकी और इंटरनेट में प्रगति ने युवा लोगों में आविष्कार और नवाचार को प्रोत्साहित किया है। इंटरनेट पर वीडियो और चित्र युवा लोगों में रचनात्मकता को बेहतर बनाने में मदद कर सकते हैं। इसलिए, साइबर सुरक्षा जागरूकता युवा इंटरनेट उपयोगकर्ताओं को यह सुनिश्चित करने में मदद कर सकती है कि वे साइबर हमलों का शिकार हुए बिना इंटरनेट से लाभ उठाएँ। आज, अधिकांश लोगों को साइबर सुरक्षा जागरूकता के प्रभावों और महत्व के बारे में जानकारी का अभाव है, एक ऐसा पहलू जो समुदाय के भीतर साइबर नैतिकता से समझौता करता है। इसलिए, शिक्षण संस्थानों में साइबर सुरक्षा शिक्षा को शामिल करने से इंटरनेट उपयोगकर्ताओं के बीच जागरूकता बढ़ाने में मदद मिल सकती है।

स्कूलों में साइबर सुरक्षा जागरूकता को बढ़ावा देने में हितधारक जो रणनीतियाँ

किंडरगार्टन स्कूलों के शिक्षकों ने जोर देकर कहा है कि बच्चों के बीच साइबर सुरक्षा जागरूकता पर चर्चा करने में कार्टून एक महत्वपूर्ण संसाधन हो सकते हैं। इसके अतिरिक्त, प्राथमिक विद्यालयों ने भी उद्धृत किया है कि एनिमेशन छात्रों का ध्यान आकर्षित करने में एक लंबा रास्ता तय करते हैं। इसलिए, साइबर सुरक्षा जागरूकता के महत्व को प्रदर्शित करने वाले जानवरों का उपयोग छात्रों को पढ़ाने के लिए किया जा सकता है। उदाहरण के लिए, ट्यूटर्स ने उद्धृत किया है कि इपिन और उपिन की कहानियाँ छात्रों के बीच साइबर सुरक्षा शिक्षा सिखाने में महत्वपूर्ण हो सकती हैं। इसके अतिरिक्त, संचार और सूचना प्रौद्योगिकी पाठ्यक्रम प्रदान करने वाले हाई स्कूल और विश्वविद्यालय अपने पाठ्यक्रम में साइबर सुरक्षा जागरूकता शामिल कर सकते हैं ताकि यह सुनिश्चित किया जा सके कि

प्रत्येक छात्र को साइबर सुरक्षा के प्रभावों और महत्व को सीखने का मौका मिले। इसके अतिरिक्त, साइबर सुरक्षा से संबंधित सुरक्षा मुद्दों को अन्य पाठ्यक्रमों और विषयों के माध्यम से पढ़ाया जा सकता है। उदाहरण के लिए, अंग्रेजी और साहित्य में, छात्रों को साइबर सुरक्षा जागरूकता पर निबंध लिखने के लिए असाइनमेंट दिए जा सकते हैं। इससे भी महत्वपूर्ण बात यह है कि वाद–विवाद और मॉक पार्लियामेंट जैसी अन्य शिक्षण गतिविधियों में, छात्र साइबर सुरक्षा के विभिन्न पहलुओं पर चर्चा कर सकते हैं। साथ ही, भाषण प्रतियोगिताएँ आयोजित की जा सकती हैं जहाँ केंद्रीय विषय साइबर सुरक्षा है; इससे छात्रों को साइबर सुरक्षा जागरूकता पर प्रशिक्षित करने में मदद मिल सकती है। शिक्षण संस्थानों में साइबर सुरक्षा सप्ताह भी आयोजित किए जा सकते हैं जहाँ छात्र साइबर सुरक्षा के महत्व को सीखते हैं ।

शिक्षकों और ट्यूटर्स के लिए बनाए गए शिक्षा कार्यक्रम भी अपने पाठ्यक्रम में साइबर सुरक्षा पाठ्यक्रम शामिल कर सकते हैं ताकि शिक्षकों को इस विशय पर पूर्ण प्रशिक्षण मिल सके। इसके अतिरिक्त, शिक्षक अपने शिक्षा कार्यक्रमों में पहले से ही पढ़ाते समय छात्रों को उचित मार्गदर्शन प्रदान करेंगे। इससे भी महत्वपूर्ण बात यह है कि साइबर सुरक्षा विषयों को शामिल करने के लिए शिक्षण मॉडल को समायोजित किया जाना चाहिए। इस तरह, आ वाली पीढ़ियाँ समझ सकती हैं कि साइबर खतरों से खुद को कैसे बचाया जाए। इसके अतिरिक्त, सरकार को स्कूलों में साइबर सुरक्षा कार्यक्रमों को लागू करने में होने वाले खर्चों को सब्सिडी देनी चाहिए ताकि यह सुनिश्चित हो सके कि अधिकांश शिक्षण संस्थान अपने पाठ्यक्रम में कार्यक्रम को शामिल करने के लिए प्रेरित हों। इसके अतिरिक्त, साइबर सुरक्षा जागरूकता के माध्यम से, छात्र विभिन्न साइबर खतरों से खुद को बचाना सीख सकते हैं। इससे भी महत्वपूर्ण बात यह है कि युवा इंटरनेट उपयोगकर्ता इंटरनेट पर खुद को सुरक्षित और सुरक्षित रखना सीख सकते हैं। प्रौद्योगिकी तक अपर्याप्त पहुँच और जनसांख्यिकी के बावजूद, शिक्षकों के पास अपने छात्रों को पढ़ाने के लिए आवश्यक साइबर सुरक्षा ज्ञान नहीं है। इस तरह, आने वाली पीढ़ियाँ समझ सकती हैं कि अपनी जानकारी और डेटा को अनाधिकृत पहुँच से कैसे सुरक्षित रखा जाए। हालाँकि, शोधकर्ताओं ने खुलासा किया है कि मूल निवासियों को साइबर सुरक्षा जागरूकता प्रशिक्षण स्वीकार करने में समस्याएँ हैं क्योंकि उनका मानना है कि प्रकृति उन्हें नुकसान से बचाएगी।

साइबर सुरक्षा के बारे में छात्रों और शिक्षकों की समझ को बढ़ाने और उन्नत करने के लिए महत्वपूर्ण ज्ञान प्रदान करना किसी भी साइबर खतरे से सुरक्षित समाज की ओर बढ़ने के लिए महत्वपूर्ण है। इससे भी महत्वपूर्ण बात यह है कि साइबर खतरों से सुरक्षित क्षेत्र साइबर सुरक्षा खतरों के विकास को रोकने में मदद कर सकता है। प्रौद्योगिकी में प्रगति के कारण, हर दिन नए और उभरते मुद्दे सामने आते हैं, और इसलिए, कल इस्तेमाल किया गया समाधान आज अप्रभावी हो सकता है। इसलिए, साइबर सुरक्षा पर कार्यक्रमों को लगातार अपग्रेड किया जाना चाहिए ताकि यह सुनिश्चित हो सके कि वे अद्यतित हैं; इस तरह, वे नई और उभरती समस्याओं से निपट सकते हैं।

प्रौद्योगिकी में प्रगति के कारण, हर दिन नए और उभरते मुद्दे सामने आते हैं, और इसलिए, कल इस्तेमाल किया गया समाधान आज अप्रभावी हो सकता है। इसलिए, साइबर सुरक्षा पर कार्यक्रमों को लगातार अपग्रेड किया जाना चाहिए ताकि यह सुनिश्चित हो सके कि वे अद्यतित हैं; इस तरह, वे नई और उभरती समस्याओं से निपट सकते हैं। हालांकि, कुछ आलोचकों ने स्कूलों में साइबर सुरक्षा प्रशिक्षण और शिक्षा के महत्व पर संदेह किया है क्योंकि उनका दावा है कि इससे स्कूलों को संघर्ष करने के लिए

अतिरिक्त खर्च ही होगा। उदाहरण के लिए, निजी स्कूल जिनके पास सरकारी धन की कमी है, वे स्कूलों में साइबर सुरक्षा शिक्षा को लागू करने को लेकर संशय में हो सकते हैं क्योंकि यह महंगा होगा। खर्चों में आईटी सलाहकारों को काम पर रखना, शिक्षकों को प्रशिक्षित करना और कंप्यूटर खरीदना शामिल है हालांकि यह महंगा है, शोधकर्ताओं ने जोर देकर कहा है कि यह इसके लायक है क्योंकि यह इंटरनेट उपयोगकर्ताओं को साइबर खतरों से बचाने में मदद करता है। चूंकि शिक्षा अक्सर अप टू डेट होती है, इसलिए यह उभरते साइबर सुरक्षा मुद्दों को संबोधित करने में मदद कर सकती है। इसके अलावा, साइबर सुरक्षा जागरूकता को बढ़ावा देने का लक्ष्य रखने वाले स्कूलों का उपयोग यह सुनिश्चित करने के लिए किया जा सकता है कि छात्रों को साइबर सुरक्षा की बेहतर समझ मिले।

संयुक्त राज्य अमेरिका में, साइबर सुरक्षा को बढ़ावा देने के लिए लोगों को प्रशिक्षित करने में मदद करने के लिए जेनसाइबर नामक एक साइबर सुरक्षा जागरूकता कार्यक्रम का आविष्कार किया गया था। यह कार्यक्रम NSF / NSA द्वारा समर्थित ग्रेड स्कूल के शिक्षकों और छात्रों के लिए एक ग्रीष्मकालीन शिविर है। इस कार्यक्रम को लागू करने के बाद से, शिक्षकों और छात्रों ने दावा किया है कि जागरूकता कार्यक्रम के माध्यम से उनकी साइबर सुरक्षा में काफी सुधार हुआ है। इससे भी महत्वपूर्ण बात यह है कि जागरूकता कार्यक्रम ने यह सुनिश्चित किया है कि साइबर अपराध लगभग आधे से कम हो गए हैं, और अधिकांश इंटरनेट उपयोगकर्ता सुरक्षित रूप से इंटरनेट पर सर्फिंग कर रहे हैं।

इसलिए, इस तरह के कार्यक्रमों को पूरे अमेरिका में लागू किया जाना चाहिए ताकि यह सुनिश्चित किया जा सके कि छात्र और शिक्षक स्कूल और घर पर साइबर सुरक्षा में सुधार करें। इसके अतिरिक्त, यह कार्यक्रम आसपास के समुदाय के बीच साइबर सुरक्षा की तैयारी और जागरूकता को बढ़ावा देने में महत्वपूर्ण हो सकता है। इस कार्यक्रम के अलावा, स्कूल साइबर सुरक्षा जागरूकता को बढ़ावा देने पर केंद्रित परिषदों और क्लबों को शामिल कर सकते हैं। छात्र इन क्लबों के माध्यम से साइबर सुरक्षा के बारे में प्रतिस्पर्धा कर सकते हैं और इसे व्यक्तिगत से लेकर सामुदायिक स्तर तक बढ़ावा दे सकते हैं। इन कार्यक्रमों और सेमिनारों के माध्यम से, छात्र साइबर सुरक्षा के बारे में अपने शिक्षकों से दिशा–निर्देश और मार्गदर्शन प्राप्त कर सकते हैं। इस तरह, शिक्षक भी साइबर सुरक्षा से संबंधित अपने कौशल और ज्ञान में सुधार करेंगे। स्ट्रॉब (2014) के अनुसार, शिक्षक और छात्र इन कार्यक्रमों से लाभान्वित हो सकते हैं यदि वे समर्पित और उद्देश्यपूर्ण बनें। इस तरह, इन कार्यक्रमों के उद्देश्यों और लक्ष्यों को रेखांकित किया जा सकता है ताकि यह सुनिश्चित किया जा सके कि सभी छात्र और शिक्षक साइबर सुरक्षा के बारे में एक ही पृष्ठ पर हों। इससे भी महत्वपूर्ण बात यह है कि ये सेमिनार छात्रों के बीच प्रौद्योगिकी के उपयोग को बढ़ाने में मदद करेंगे, जिससे ऐसे आविष्कार और नवाचार होंगे जो कक्षा में उनकी रचनात्मकता को बेहतर बना सकते हैं।

साइबर सुरक्षा जागरूकता के महत्व की समझ को प्रोत्साहित करने में सक्रिय शिक्षण भी आवश्यक साबित होता है। सक्रिय शिक्षण के माध्यम से, छात्र साइबर सुरक्षा खतरों जैसे साइबरबुलिंग के बारे में जागरूकता विकसित कर सकते हैं और ऐसी साइबर सुरक्षा घटनाओं को रोकने में मदद कर सकते हैं। इससे भी महत्वपूर्ण बात यह है कि शिक्षकों को ऐसे मामलों में आत्म–सुरक्षा और साइबर सेक्स को सीमित करना चाहिए ताकि वे हानिकारक साइटों से अवगत रहें। शोधकर्ताओं ने

खुलासा किया है कि ये दूषित साइटें अक्सर व्यक्तिगत जानकारी मांगती हैं जिन्हें अक्सर दुर्भावनापूर्ण उद्देश्यों के लिए पुनर्प्राप्त और उपयोग किया जाता है। इसलिए, माता–पिता, सरकार और शिक्षकों के लिए छात्रों को विभिन्न साइबर सुरक्षा क्षेत्रों के बारे में पढ़ाने और यौन शिक्षा पर आलोचनाओं को दूर करने के तरीके में सक्रिय होना महत्वपूर्ण है।

निष्कर्ष

शोध निष्कर्षों के आधार पर, यह स्पष्ट है कि शिक्षण संस्थानों में साइबर सुरक्षा शिक्षा की आवश्यकता है। ऐसा इसलिए है क्योंकि यह साइबर सुरक्षा जागरूकता बढ़ाकर लोगों को विभिन्न साइबर खतरों से बचाने में मदद कर सकता है। इससे भी महत्वपूर्ण बात यह है कि साइबर सुरक्षा जागरूकता के माध्यम से इंटरनेट उपयोगकर्ता फेसबुक, इंस्टाग्राम, यूट्यूब और ट्विटर जैसे कई सोशल मीडिया प्लेटफॉर्म का उपयोग करते समय अपनी कमजोरियों को समझ सकते हैं। साथ ही, इंटरनेट उपयोगकर्ता अन्य इंटरनेट उपयोगकर्ताओं पर उनके नकारात्मक प्रभावों को समझकर साइबरबुलिंग जैसे कुछ साइबर हमलों को रोकना सीख सकते हैं। इसके अलावा, साइबर सुरक्षा जागरूकता इंटरनेट उपयोगकर्ताओं को विभिन्न साइबर अपराधों से जुड़े कानूनों को समझने में मदद कर सकती है। हालाँकि, साइबर सुरक्षा शिक्षा के कार्यान्वयन में विभिन्न चुनौतियों का सामना करना पड़ता है, जो सरकारी सहायता की कमी से लेकर अपर्याप्त संसाधनों तक होती हैं। इससे भी महत्वपूर्ण बात यह है कि शिक्षकों के पास कौशल और विशेषज्ञता की कमी एक चुनौती है, खासकर जब उनसे अपने छात्रों को साइबर सुरक्षा पर प्रशिक्षित करने की उम्मीद की जाती है। इसलिए, सरकार, माता–पिता, शिक्षकों और साथियों जैसे संबंधित पक्षों को युवा इंटरनेट उपयोगकर्ताओं को साइबरबुलिंग और साइबर अपराधों के अन्य विभिन्न रूपों से बचाने के लिए सर्वोत्तम समाधान विकसित करने चाहिए। अंत में, रेडियो और टेलीविजन जैसे मीडिया को ऐसे अभियानों के माध्यम से साइबर सुरक्षा के महत्व पर बात फैलाने में मदद करनी चाहिए जो बच्चों के लिए दिलचस्प और इंटरैक्टिव हो सकते हैं।

संदर्भ

1. पेन्चेवा, डी., जोसेफ, एच. और अवैस आर. (2020) साइबर को स्कूल में लानाः साइबर सुरक्षा को माध्यमिक विद्यालय शिक्षा में एकीकृत करना। IEEE सुरक्षा और गोपनीयता, 18, पृ० सं०–**68–74**.
2. https://doi.org/10.1109/MSEC.2020.2969409
3. पार्क, एच. हो. (2020) साइबर अपराध निवारण मान्यता पर एक अध्ययनः साइबर अपराध के लिए दंड की मान्यता का अपराध की रिपोर्ट करने के इरादे पर प्रभाव। कोरियन क्रिमिनल साइकोलॉजी रिसर्च, 16, पृ० सं०–**85–98**.
4. https://doi.org/10.25277/KCPR.2020.16.4.85
5. (3), गोस्वामी, ए. (2018) ई–गवर्नेंस के विभिन्न अनुप्रयोगों में साइबर सुरक्षा का प्रभाव। जर्नल ऑफ एडवांसेज एंड स्कॉलरली रिसर्च इन एलाइड एजुकेशन, 15, पृ० सं०–**65–701**
6. https://doi.org/10.29070/15/57309

7. रैडेमेकर, एम. (2016) साइबर सुरक्षा का आकलन 2015. सूचना और सुरक्षाः एक अंतर्राष्ट्रीय जर्नल, 34, पृ० सं०–**93–104.**
8. https://doi.org/10.11610/isij.3407
9. रॉबिन्स, ए. (2015) कंप्यूटर विज्ञान शिक्षा अनुसंधान की मौजूदा चुनौतियाँ कंप्यूटर विज्ञान शिक्षा, 25, पृ० सं०–**115–119**.
10. https://doi.org/10.1080/08993408.2015.1034350
11. हार्ट, एस., एंड्रिया, एम., फेडेरिका, पी. और व्लादिमीरो, एस. (2020) जोखिमः साइबर सुरक्षा जागरूकता और शिक्षा के लिए एक गंभीर खेल। कंप्यूटर और सुरक्षा, 95, लेख आईडीः 101827.
12. https://doio.rg/10.1016/j.cose.2020.101827
13. नेगी, एस. और सुनीता, एम. (2019) मिडिल स्कूल के बच्चों में साइबर बुलिंग व्यवहार को कम करने के लिए साइबर बुलिंग सेंसिटाइजेशन प्रोग्राम (सीबीएसपी) की प्रभावशीलता। इंटरनेशनल जर्नल ऑफ साइबर रिसर्च एंड एजुकेशन, 1, लेख संख्या 5.
14. https://doi.org/10.4018/IJCRE. 2019010105
15. ट्रैप डब्ल्यू. और स्ट्रॉब, जे. (2021) जर्नल ऑफ साइबरसिक्यूरिटी एंड प्राइवेसी : ए न्यू ओपन एक्सेस जर्नल। जर्नल ऑफ साइबर सिक्यूरिटी एंड प्राइवेसी, 1, पृ० सं०–**1–3**.
16. https://doi.org/10.3390/cybersecurity1010001
17. कीथ, एम. (2015) साइबर सुरक्षा शिक्षा, योग्यता और प्रशिक्षण। होलोवे, आर., एड., इंजीनियरिंग और प्रौद्योगिकी संदर्भ, इंस्टीट्यूशन ऑफ इंजीनियरिंग एंड टेक्नोलॉजी, लंदन, पृ० सं०–**1–11**.
18. https://doi.org/10.1049/etr.2014.0029
19. फिचनर, एल. (2018) साइबर सुरक्षा किस तरह की है? साइबर सुरक्षा का सिद्धांत और दृष्टिकोणों का मानचित्रण इंटरनेट नीति समीक्षा, 7,
20. https://doi.org/10.14763/2018.2.788
21. (11), तरासुक, ए. (2020) समाज की साइबर सुरक्षा प्रदान करने में सामाजिक कारक के कुछ पहलू। ज्ञान, शिक्षा, कानून, प्रबंधन, 2, पृ० सं०–**206–211**.
22. https://doi.org/10.51647/kelm.2020.3.2.37
23. (12) होरोविट्ज, बीएम और स्कॉट लुसेरो, डी. (2016) सिस्टम अवेयर साइबर सिक्योरिटीः साइबर सिक्योरिटी को बढ़ाने के लिए एक सिस्टम इंजीनियरिंग दृष्टिकोण। इनसाइट, 19, पृ० सं०–**39–42**
24. https://doi.org/10.1002/inst. 12087
25. (13) पवार, एससी, मेंटे, आरएस और चेंडेज, बीडी (2021) साइबर अपराध, साइबर स्पेस और साइबर अपराध के प्रभाव। कंप्यूटर विज्ञान, इंजीनियरिंग और सूचना प्रौद्योगिकी में वैज्ञानिक अनुसंधान के अंतर्राष्ट्रीय जर्नल, 7, पृ० सं०–**210–2141**

26. https%:/doi.org/10.32628/CSEIT217139
27. (14) स्ट्रॉब, जे. (2014) कंप्यूटर विज्ञान डॉक्टरल शिक्षा में परीक्षाओं का मूल्यांकन कंप्यूटर विज्ञान शिक्षा, 24, पृ० सं०—**25—70.**
28. https://doi.org/10.1080/08993408.2014.890792
29. (15) मोंटेथ, एस., बाउर, एम., एल्डा, एम., गेडेस, जे., व्हाईब्रो, पीसी और ग्लेन, टी. (2021) महामारी के बाद से साइबर अपराध में वृद्धिः मनोरोग के लिए चिंताएँ। वर्तमान मनोरोग रिपोर्ट, 23, लेख संख्या
30. https://doi.org/10.1007/s11920-021-01228-w