देवानां भद्रा सुमतिर्ऋजूयताम्।। ऋ० १/८९/२

ISSN : 2395-7115
Oct. 2025
Vol.-22, Issue-4(2)

Impact Factor
8.642

Bohal Shodh Manjusha

AN INTERNATIONAL PEER REVIEWED, REFEREED MULTIDISCIPLINARY
& MULTIPLE LANGUAGES RESEARCH JOURNAL
UGC Valid Journal (The Gazette of India, Extraordinary Part III, Section 4, Dated July 18, 2018)

संवाद से समाधान तक : विविध विमर्शों का संगम

Editor
Dr. Naresh Sihag
Advocate

Special Issue Editor
Dr. Vikas Sharma

Publisher :
Gugan Ram Educational & Social Welfare Society (Regd.)
#202, Old Housing Board, Bhiwani, Haryana-127021

स्व. चौ. गुगनराम सिहाग व उनकी छोटी बहन स्व. श्रीमती गीना देवी के शुभाशीर्वाद से प्रकाशित

JOURNAL OF HUMANITIES, COMMERECE, SCIENCE, MANAGEMENT & LAW

बोहल शोध मञ्जूषा

Bohal Shodh Manjusha

AN INTERNATIONAL PEER REVIEWED, REFEREED
MULTIDISCIPLINARY & MULTIPLE LANGUAGES RESEARCH JOURNAL

Vol. 22 | ISSUE-4(2) | (अक्टूबर 2025) | ISSN : 2395-7115

प्रेरणा :
चौ. एम. सिहाग

विशेषांक सम्पादक :
डॉ. विकास शर्मा
गुरू विद्यापीठ

सम्पादक :
डॉ. नरेश सिहाग 'बोहल', एडवोकेट
एम.ए. (समाजशास्त्र, लोक प्रशासन, हिन्दी शिक्षा शास्त्र, पत्रकारिता),
एम.फिल (समाजशास्त्र, हिन्दी) एम. लिब., एल-एल.बी. (ऑनर्स),
डिप्लोमा पंचायती राज (रजत पदक विजेता), पी.एच.डी. (हिन्दी)
डी.लिट् (मानद उपाधि), काठमांडू, नेपाल

प्रकाशक :
गुगनराम एजुकेशनल एण्ड सोशल वैलफेयर सोसायटी (रजि.)
202, पुराना हाऊसिंग बोर्ड, भिवानी-127021 (हरियाणा)

अनुक्रमाणिका – अक्टूबर 2025 (विशेषांक)

क्र.	विषय	लेखक	पृष्ठ
1.	सम्पादकीय	डॉ. विकास शर्मा	09–09
2.	अमरकांत के उपन्यासों में चित्रित नारी जीवन की समस्याएँ	डॉ. अमित कुमार सिंह	10–12
3.	रेणु की कहानियों में चित्रित ग्राम्य-जीवन एवं लोक-कलाएँ	डॉ. अनामिका सिंह	13–17
4.	Virtual Paradigms and Ethical Imperatives : An Exegetical Study of the Metaverse Through Indian Science Fiction	ANCHAL SHARMA	17-22
5.	मृदा संरक्षण और टिकाऊ कृषि में संवाद	अर्जुन रन्धावे	23–26
6.	सामुदायिक सशक्तिकरण में संवाद/समाधान का महत्व	डॉ. अश्वनी कुमार ध्रुव	27–30
7.	Scenario of Intellectual Property Right (IPR) in Indian Context	Dr. Avadhesh Kumar Koshal	31-35
8.	साइबर सुरक्षा जागरूकता बढ़ाने में शिक्षा की भूमिका	डॉ. भुपेन्द्र कौर	36–40
9.	संजीव के उपन्यास 'फाँस' में मानवीय संवेदना	बॉबी कुमार, डॉ. ज्योत्स्ना शर्मा	41–46
10.	An Empirical Study of Women Empowerment by the Economic Activities of Self Help Groups in Chhattisgarh	DR. DEVESH PAL	47-51
11.	भक्तिकालीन काव्य में संस्कृति और प्रकृति विमर्श	डॉ. दिलीप सिंह राजपूत	52–57
12.	उत्तराखण्ड की ग्रामीण अर्थव्यवस्था के अन्तर्गत किसानों की आर्थिक – सामाजिक समस्याएँ एवं उनके समाधान	गगन दीप सिंह	58–61
13.	संवाद से समाधान तक : विविध विमर्शों में गजल की भूमिका एवं अभिव्यक्ति का सौंदर्यशास्त्र	हर्षना के. डांगरे	62–66
14.	DESMIDS OF BANDA , BUNDELKHAND DIVISION UTTAR PRADESH , INDIA	IQBAL HABIB	67-74
15.	संजीव के उपन्यास 'मुझे पहचानो' में नारी जीवन	डॉ. ज्योत्स्ना शर्मा	75–80
16.	साहित्य का समाज पर प्रभाव	डॉ. कंचन आर्या	81–86
17.	दिव्यांगजनों के लिए समावेशी संवाद	डॉ. लक्ष्मी मिश्रा	87–91
18.	परंपरागत संगीत कलाओं के जतन एवं संवर्धन में संवाद का अनन्य साधारण महत्व	प्रा. माधुरी अ. पाटील	92–96

19.	आदिवासी संस्कृति, भाषा, कला एवं जीवन शैली	मोनिका भामकर	97–101
20.	दलित साहित्य के क्रांतिसूर्य – पद्मश्री नामदेव ढसाल	नितिन सुभाषराव कुंभकर्ण	102–106
21.	समय से संवाद करता रचनाकार (सन्दर्भ– रवींद्रनाथ का साहित्य)	डॉ. पुष्पा कुमारी	107–110
22.	आधुनिक हिंदी उपन्यासों में दिव्यांग विमर्श	डॉ. राजकुमार	111–114
23	सुधा ओम ढींगरा की कहानी 'अनुगूँज' में स्त्री विमर्श	रक्षा बघेल, डॉ. ज्योत्स्ना शर्मा	115–118
24.	भारतीय लोकतंत्र : चुनौतियां और सुदृढ़ीकरण	डॉ. रमेश राम	119–124
25.	पर्यावरण विमर्श	डॉ. रामकली शर्मा	125–129
26.	अनामिका की कविताओं में स्त्रीवादी दृष्टिकोण	डॉ. रम्या एल	130–133
27.	जेंडर और समाज : बदलते परिपेक्ष्य	डॉ. रूपा आर्या	134–139
28.	डी.एल.एड. प्रशिक्षणार्थियों के लिए समयनिष्ठता और जीवनतोष के प्रशिक्षण में वृद्धि के उपाय : साहित्य समीक्षा	प्रो.(डॉ.) संतोष कुमार शर्मा	140–143
29.	मुक्तिभाव से लोकसंवाद तक : महाराष्ट्र के भक्तिगीतों की यात्रा	डॉ. सारिका श्रावणे	144–148
30.	**Effective Communication Skills : Processes of Dialogue and Resolution**	**Dr. Shefali Mendiratta**	**149-154**
31.	शहरीकरण : प्रवासन और सामाजिक परिवर्तन	डॉ. सिमरन	155–160
32.	21वीं सदी के किसानों की आत्महत्या : मनोवैज्ञानिक सामाजिक कारण	स्नेहा दीपक वानखेडे	161–165
33.	भाषा और साहित्य का अंतर्संबंध	सोनू कुमारी	166–169
34.	तीसरा सप्तक के कवियों का सामाजिक एवं सांस्कृतिक संदर्भ : एक अध्ययन	सुमन माखीजा	170–175
35.	शिक्षा में संवाद-आधारित शिक्षण	डॉ. सुनील कुमार चतुर्वेदी	176–180
36.	सामाजिक आन्दोलन की भूमिका	डॉ. तनुजा गुप्ता	181–190
37.	आदिवासी हिंदी कविता : स्वर, संवेदना और संघर्ष	वंदना गुप्ता	191–194
38.	हिंदी कहानी साहित्य में त्यौहार एवं उनका सामाजिक महत्व	विकास राव	195–197
39.	हिमांशु जोशी की कहानी 'मनुष्य चिह्न' में स्त्री-विमर्श	डॉ. ज्योत्स्ना शर्मा, वीरेन्द्र कुमार	198-201
40.	वैदिक साहित्य में पर्यावरण चेतना	सरिता चौहान	202–206
41.	उत्तरी पश्चिमी मध्य प्रदेश में प्रचलित पहेलियों में प्रतीक एवं बिंब विधान	दीपिका रानी, प्रो. (डॉ.) मनीषा	207–210

www.bohalshodhmanjusha.com
Impact Factor : 8.642

Bohal Shodh Manjusha ISSN : 2395-7115
Oct. 2025 Page No. : 36-40

AN INTERNATIONAL PEER REVIEWED, REFEREED MULTIDISCIPLINARY
& MULTIPLE LANGUAGES RESEARCH JOURNAL

साइबर सुरक्षा जागरूकता बढ़ाने में शिक्षा की भूमिका

डॉ. भुपेन्द्र कौर
सहायक प्राध्यापक, शिक्षा शास्त्र विभाग
आईएफटीएम विश्वविद्यालय, मुरादाबाद (यू0पी0)

सार –

शिक्षा के द्वारा मनुष्य का सम्पूर्ण विकास होता है। शिक्षा एक ऐसी प्रक्रिया है जो जन्म से लेकर मृत्यु तक चलती रहती। मनुष्य जिसमें औपचारिक तथा अनौपचारिक रूप से कुछ न कुछ सीखता रहता है। इसी सीखने की प्रक्रिया में वह अच्छा और बुरा अनेक प्रकार की गतिविधियों को अपने में समाहित करता है। मनुष्य अपने जीवन में शिक्षा को अपनाकर अपनी जीविका कमाने में भी इसका प्रयोग करता है। आज तकनीकी के क्षेत्र में भी अनेक विकास हुए है जिसमें शिक्षा ने भी अहम भूमिका निभाई है। इसी क्रम में साइबर क्राइम और साइबर सुरक्षा भी सामने आते है। आज के आधुनिक एवं तकनीकी युग में साइबर क्राइम का बोलबाला है। इस क्षेत्र में समाज के लोगों को जागरूक करने की आवश्यकता है जिसके लिए शिक्षा एक उचिम माध्यम है। साइबर सुरक्षा जागरूकता बढाने में शिक्षा की महत्वपूर्ण भूमिका रही है। शिक्षा के द्वारा छात्रों तथा समाज के अन्य लोगों को साइबर खतरों से जागरूक किया जा सकता है तथा उन्हें साइबर हमलों से बचने के लिए किया जा सकता है। आसान शब्दों में कहा जा सकता है कि साइबर सुरक्षा जागरूकता के माध्यम से जाना जा सकता है। हमारी सुरक्षा को क्या खतरा है तथा संभावित जोखिम से बचने के लिए क्या कार्य जिम्मेदारी के साथ करना चाहिए।

प्रस्तावना –

साइबर सुरक्षा जागरूकता कर्मचारियों को साइबरस्पेस से जुडे खतरों के बारे में जागरूक करने या शिक्षित करने की एक प्रक्रिया है। वास्तव में सुरक्षा जागरूकता किसी भी व्यवसाय को सुरक्षित करने के लिए आवश्यक है। लोगों को जागरूक करने के उद्देश्य से अक्टूबर माह को साइबर सुरक्षा जागरूकता माह के रूप में मनाया जाता है। इसके अर्न्तगत व्यक्तियों एवं संगठनों को साइबर सुरक्षा को और बेहतर बनाने के लिए डिजिटिल दुनिया में सुरक्षा की दृष्टि शिक्षा के द्वारा शिक्षित करके इसके बचाव के लिए कदम उठाये जा सके। साइबर सुरक्षा जागरूकता क्या है–साइबर सुरक्षा जागरूकता कर्मचारियों को साइबरस्पेस में छिपे खतरों और परेशानियो से काम करने के तरीकों के बारे में शिक्षित करने की एक सतत प्रक्रिया है। साइबर खतरों में उल्लेखनीय वृद्धि के साथ, आपके कार्यबल और व्यवसाय को ऑनलाइन सुरक्षित रखने के लिए साइबर सुरक्षा जागरूकता अत्यंत महत्वपूर्ण है। साइबर सुरक्षा जागरूकता अपने कर्मचारियों को साइबर अपराधियों द्वारा इस्तेमाल किए जाने वाले दुर्भावनापुर्ण तरीकों, उनके आसान शिकार बनने के तरीकों, संभावित खतरों की पहचान

करने के तरीके और इन घातक खतरों का शिकार होने से बचने के लिए क्या करना चाहिए, के बारे में शिक्षित करने में मदद करती है। यह आपके कर्मचारियों को सही ज्ञान और संसाधन प्रदान करके संभावित खतरों को पहचानने और उन्हे नुकसान पहुँचाने से पहले ही चिन्हित करने में सक्षम बनाती है।

साइबर सुरक्षा के लिए शिक्षा –

साइबर सुरक्षा किसी भी संगठन के लिए एक आवश्यक जानकारी है जो किसी भी स्तर पर डिजिटिल क्षेत्र में काम करता है, और शिक्षा क्षेत्र में इसका कोई अपवाद नहीं है। वैश्विक महामारी और तकनीकी ने ऑनलाइन शिक्षा को जन्म दिया है जिसका प्रचलन दिन–प्रतिदिन बढता जा रहा है। जिसके कारण शिक्षको के साथ–साथ प्रशासन के भी अनेक चुनौतियों का सामना करना पड़ रहा है। डिजिटल सुरक्षा की शिक्षा प्रदान करने में आने वाली कठिनाईयों को ध्यान में रखते हुए अनेक शैक्षिक संस्थान तैयार नहीं है। शिक्षा क्षेत्र में भी कार्यबल को प्रौद्योगिकी और इंटरनेट के उपयोग के संबंध में सुरक्षा को बढावा देकर साइबर सुरक्षा के प्रति अधिक जागरूक बनाना जिसमें शिक्षा और प्रशिक्षण की महत्वपूर्ण भागीदारी है। साइबर सुरक्षा जागरूकता कार्यक्रम विकसित करना एक सामान्य प्रक्रिया है। सुरक्षा सामग्री का चुनाव करना संसाधन तैयार करना, प्रशिक्षित सामग्री और उपकरणों का परीक्षण करना ज्यादा समय लेने वाला और उपकरणों का परीक्षण करना ज्यादा समय लेने वाला हो सकता है।

कर्मचारियों में रूचि पैदा करना और उन्हें शामिल करना हमेशा एक चुनौती होती है। दोहराए जाने वाले पाठ्यक्रम, बहुत अधिक जानकारी, पाठयक्रम की अवधि और जटिलता कर्मचारियों की भागीदारी को हतोत्साहित कर कर सकती है।

शिक्षा के डिजिटलीकरण में सुरक्षा के लिए चुनौतियाँ –

वर्तमान समय में देखा जाये तो शिक्षा का क्षेत्र अपराध का लक्ष्य बना है क्योंकि अनेक लोग उन समस्याओं से परिचित है खासकर वो जिनको शिक्षण संस्थाओं का ऑनलाइन उपस्थिति को सुरक्षित रखना पड़ता है। ऐसे समय में साइबर हमलों से सुरक्षित करने के लिए उनके पास विशेषज्ञ, धन तथा जरूरी संसाधन की कमी है या पूर्ति नही है, एवं हमलावर इस बात से परिचित है।

साइबर सुरक्षा जागरूकता में शिक्षा महत्व –

साइबर अपराध से बचाव में शैक्षिक संस्थानों के सामने अनेक कठिनाईयों में एक साइबर सुरक्षा जागरूकता की तरफ इशारा करती हैं। 2023 डेटा ब्रीच की लागत रिपोर्ट के अनुसार, शिक्षा क्षेत्र में डेटा ब्रीच की लागत औसतन +3.65 मिलियन USD है, जो कि 2022 में +3.65 मिलियन से थोड़ा कम है, किन्तु फिर भी यह आँकड़े चौकाने वाले है। चेक पॉइंट रिसर्च की एक रिर्पोट में बताया जाता है कि प्रति सप्ताह 2,000 से अधिक हमलें शिक्षा और अनुसंधान अन्य क्षेत्रों की तुलना में दोगुना सबसे अधिक लक्षित उद्योग है। सर्वोत्तम सुरक्षा प्रणलियों एवं उपायों के उपलब्ध होने के बावजूद, कई संगठन अभी भी सुरक्षा उल्लंघनों का सामना करते हैं। दुर्भाग्य से, अक्सर मानवीय त्रुटि ही कई डेटा उल्लंघनों का एक प्रमुख कारण रही है। वेरिजोन की 2022 डेटा उल्लंघन जाँच रिपोर्ट के अनुसार, 80 प्रतिशत ज्यादा उल्लंघनों में मानवीय पहलू शामिल थे, जिनमें सोशल इंजीनियरिंग हमले, त्रुटियाँ और चुराए गए क्रेडेंशियल्स का दुरूपयोग शामिल है। खतरा पैदा करने वाले लोग किसी संगठन के नेटवर्क और सिस्टम में घुसपैठ करने के लिए इसी कमजोरी का फायदा उठाने की कोशिश

करते है। यही पर साइबर सुरक्षा जागरूकता की भूमिका आती है।

साइबर सुरक्षा जागरूकता प्रशिक्षण –

साइबर सुरक्षा जागरूकता प्रशिक्षण एक ऐसा कदम है जिसे संस्था या संगठन अपना डेटा और अन्य संपत्ति की सुरक्षा के लिए बढाता है। साइबर अपराध के लगातार बढने से साइबर सुरक्षा सभी प्रकार के व्यवसायों के लिए सर्वोच्च प्राथमिकता बन गई है। साइबर सुरक्षा प्रशिक्षण किसी भी संस्था या संगठन की साइबर की साइबर सुरक्षा रणनीति का एक महत्वपूर्ण उपकरण (घटक) है। सुशिक्षित और प्रशिक्षित कर्मचारी इन खतरों से शीघ्र परिचित हो जाते है, जिसके कारण साइबर घटनाओं का जोखिम काफी कम हो सकता है। शिक्षा में, एक भी मानवीय गलती के कारण गंभीर घटना होने की संभावना अधिक होती है। शिक्षा में दोनों ही चरों (शिक्षक और छात्र) द्वारा हमलावरों को घुसपैठ करने या संस्था को नुकसान करने का मौका दिया जा सकता है। कहा जा सकता है कि 75 प्रतिशत डेटा उल्लंघनों में मानवीय तत्वों के शामिल होने की जानकारी मिलती है, साइबर सुरक्षा जागरूकता उन्हें रोकने का महत्वपूर्ण भाग है।

पिछले कुछ समय में, साइबर सुरक्षा जागरूकता प्रशिक्षण मुख्य सुरक्षा पेशेवरों तक सीमित रहने से लेकर आईटी प्रशासकों और अन्य कर्मचारियों की संख्या, उनकी जागरूकता की डिग्री, बजट आदि के आधार पर भिन्न हो सकता है। साइबर सुरक्षा जागरूकता प्रशिक्षण की उपेक्षा करने या नियमित रूप से प्रशिक्षण न देने से आपके व्यवसाय पर गंभीर परिणाम हो सकते हैं, जैसे–कानूनी दंड, वित्तीय नुकसान और सुधार की लागत, बौद्धिक संपदा की हानि, कंपनी की प्रतिष्ठा को नुकसान, ग्राहकों के विश्वास में कमी, इत्यादि। आखिरकार, आपकी कंपनी की साइबर सुरक्षा रणनीति उतनी ही मजबूत है जितनी आपकी सबसे कमजोर कड़ी हमारे कर्मचारी है।

हालाँकि साइबर सुरक्षा जागरूकता साइबर अपराध की समस्याओं का समाधान नहीं करती, लेकिन वर्तमान में व्यवसाय से संभावित समस्याओं को कम करने के लिए इसके महत्व को समझा जाता है। अधिकांश कंपनियाँ अपने कर्मचारियों को अनेक प्रकार का सुरक्षा जागरूकता प्रशिक्षण प्रदान करती हैं। देखा जाए तो वर्तमान में साइबर सुरक्षा जागरूकता अनिवार्य है। साइबर सुरक्षा जागरूकता कार्यक्रम विकसित करना चुनौतीपूर्ण हो सकता है। अपराधी लगातार साइबर के हमलों के नित नये तरीके अपनाते रहते है। नई तकनीकी के साथ तालमेल बिठाना और प्रशिक्षण कार्यक्रमों को बनाना और अपनाना जितना आसान है उससे कही ज्यादा मुश्किल है। इससे साइबर सुरक्षा प्रशिक्षण तेजी से पुरानी हो जाती है क्योंकि जो ज्ञान और कौशल वर्तमान में काम कर रहे है वो भविष्य के खतरों के लिए पूर्ण नहीं है।

शैक्षिक संस्थानों के सामने आने वाली मुख्य साइबर सुरक्षा चुनौतियाँ निम्नलिखित है –

1. ऑनलाइन शिक्षण प्लेटफार्म में संस्थाओं द्वारा इस्तेमाल किये जाने वाले सुरक्षित शिक्षण प्लेटफॉर्म का अभाव है। निजी उपकरणों का प्रयोग, कमजोर पासवर्ड और सुरक्षा की झूठी भावना इस समस्या को और अधिक बढाती है।
2. रक्षात्मक प्रथाओं और उपकरणों के साथ तालमेल बनाकर न रखना खतरे की तरफ इशारा करता है, जिससे अनुकूलनीय समाधानों के बिना प्रणालीयों की सुरक्षा करना एक कठिन कार्य के समान है।
3. तकनीकी तंत्र के विस्तार का मतलब हमले की सतह का बड़ा होना, तथा बिना वजह तकनीकी के समायोजन से सुरक्षा संबंधी खामियां पैदा होने लगती है।

4. अनेक संस्थाओं को गम्भीर वित्तीय बाधाओं का सामना करना पड़ता है, उन्हें बुनियादी कार्यो के लिए भी धन जुटाने में संघर्श करना पडता है, इसमें साइबर सुरक्षा उपायों की तो बात ही छोड़िए।
5. जिस प्रकार स्वास्थ्य सेवा या अन्य वित्तीय सेवाएँ अपना कार्य करती है। उसी प्रकार शिक्षा क्षेत्र भी अपनी गोपनीयता के लिए कड़े नियम कानून बनाता है और लागू करता है।
6. स्टाफ और विभाग के पास तकनीकी, खतरों और सुरक्षा की सर्वोत्तम प्रथाओं के बारे में ज्ञान के अनेक स्तर हो सकते हैं, जिनमें से प्रत्येक के लिए अपने सीखने के मार्ग की आवश्यकता होती है।
7. वार्षिक शैक्षणिक कैलेण्डर में सीमित समय और अनेक गतिविधियाँ होने के कारण संस्थानों के पास जागरूकता गतिविधियों के लिए समय की कमी होने की वजह से कम मूल्य और परिणाम प्राप्त होते है।

शिक्षा में साइबर सुरक्षा के लिए फायदे –

1. शिक्षा के माध्यम से साइबर सुरक्षा के खतरों को पहचानना तथा उनसे बचने के तरीको की जानकारी प्राप्त होती है।
2. इससे विद्यार्थियों में महत्वपूर्ण सोच एवं समस्या–समाधान करने का कौशल बढता है।
3. इससे विद्यार्थियों में डिजिटिल नागरिकता की भावना का विकास होता है।
4. इससे जुडकर विद्यार्थियों में साइबर सुरक्षा से जुडे कानून और नियमों की जानकारी प्राप्त होती है।

शिक्षा में साइबर सुरक्षा के पहल –

1. साइबर सुरक्षा शिक्षा के लिए राष्ट्रीय पहल (NICE)।
2. साइबर सुरक्षा कैरियर और अध्ययन के लिए राष्ट्रीय पहल (NICCS)।
3. साइबर सुरक्षा जागरूकता कार्यक्रम।

शिक्षा में साइबर सुरक्षा के सुझाव –

1. पासवर्ड का सही इस्तेमाल करे।
2. सार्वजनिक वाई–फाई का इस्तेमाल करने से बचे।
3. अपनी डिवाइस, नेटवर्क, और डेटा को सुरक्षित रखें।
4. अपने साफटवेयर को नियमित रूप से अपडेट करते रहे।

निष्कर्ष –

साइबर अपराधियों के लिए शिक्षा का क्षेत्र एक आम लक्ष्य है, क्योंकि शैक्षिक संस्थानों में अनेक ऐसे कारक होते है जिन पर आसानी से हमला किया जा सकता है, एवं जिनकी सुरक्षा करना कठिन कार्य है। संस्थाओं में भारी मात्रा में संवेदनशील डेटा का प्रबन्धन किया जाता है, जिसमें कि छात्र व अध्यापक के खाते, फंडिंग, स्टाफ के मुददे और डिवाइस साइबर क्राइम हमले के लिए एक बड़ा क्षेत्र है, इन हमलों से बचाव के लिए एक मजबूत और स्तरीय सुरक्षा रणनीति की जरूरत है, तथा एक ठोस साइबर सुरक्षा जागरूकता प्रशिक्षण कार्यक्रम जरूरी है। साइबर सुरक्षा का बढता महत्व विद्यार्थियों मे पहचान की चोरी, साइबर बदमाशी, फिशिंग घोटाले और मैलवेयर संक्रमण सहित विभिन्न ऑनलाइन खतरों का शिकार होने के समस्याओं को बढ़ावा दे रहा है। शिक्षा के बिना उचित साइबर सुरक्षा की जानकारी देना अति आवश्यक है। विद्यार्थी जनजाने में आनॅलाइन व्यवहार में अपनी भागीदारी करने लगते है, जिससे उनमें अनेक खतरों के प्रति संवेदनशीलता आ सकती है। नवीनतम साइबर

खतरों और निवारक उपायों के बारे में जानकारी रखकर, आप अपने डिजिटल सुरक्षा तंत्र को बेहतर बना सकते हैं। फिशिंग स्कैम और रैंसमवेयर जैसे सामान्य आक्रमणों को समझने से आप संभावित जोखिमों को पहले से पहचानकर उन्हें कम कर सकते हैं।

ग्रन्थ सूची -

1. Hester, S & Eglin, P (1992). A Sociology of Crime. London. Rouledge Publications.
2. Moore, R. (2005) "Cyber crime : Investigating High-Technology Computer Crime." Cleveland, Mississippi : Anderson Publishing.
3. Padhy, P (2006), Crime and Criminology, Principles of Criminology, New Delhi: Mehra Press Ltd.
4. Rebecca & Jeanne, M. (2011) Criminology. Encyclopedia of the Social and cultural Foundation of Education. New Delhi : SAGE Publications.
5. Tanner, R.E.S. (2007). Social Impact of Cyber Crime. New Delhi. Concept Publishing Company.

Email:srsingh2472@gmail.com