Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
January-June 2024 5(1), 2493–2498

CYBERCRIME AWARENESS AMONG STUDENTS IN JAUNPUR CITY: A COMPARATIVE STUDY

जौनपुर शहर में छात्रों के बीच साइबर अपराध जागरूकता: एक तुलनात्मक अध्ययन

Radha Singh [1], Mili Singh [2]

[1] Research Scholar, Shri Raamshwroop Memorial University, India
[2] Assistant Professor, Shri Raamshwroop Memorial University, India

DOI
10.29121/shodhkosh.v5.i1.2024.2502

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Copyright: © 2024 The Author(s). This work is licensed under a Creative Commons Attribution 4.0 International License.

With the license CC-BY, authors retain the copyright, allowing anyone to download, reuse, re-print, modify, distribute, and/or copy their contribution. The work must be properly attributed to its author.

OPEN ACCESS

ABSTRACT

English: The aim of this study is to determine the level of cybercrime awareness among students in Jaunpur region. Technology has become essential in all aspects of life, from household chores to managing multinational companies and ensuring national security. Despite its benefits, technology also poses risks such as fraud, assault, bullying, sexual harassment, and phishing. It is important for students to understand cybersecurity to prevent such crimes. Data was collected from Veer Bahadur Purvanchal University in Jaunpur, Uttar Pradesh using a questionnaire-based survey. Dr. S. Cybercrime Awareness Scale developed by Rajasekhar (2011) measured the awareness of students. The study considered demographic factors such as gender and location to assess the understanding of cyber threats. T-test was used to test the hypotheses. The findings show that there is no significant difference in cybercrime awareness between male and female students, but there is a significant difference between students from rural and urban areas.

Hindi: इस अध्ययन का उद्देश्य जौनपुर क्षेत्र में छात्रों के बीच साइबर अपराध जागरूकता के स्तर को निर्धारित करना है। घरेलू कामकाज से लेकर बहुराष्ट्रीय कंपनियों के प्रबंधन और राष्ट्रीय सुरक्षा सुनिश्चित करने तक प्रौद्योगिकी जीवन के सभी पहलुओं में आवश्यक हो गई है। अपने लाभों के बावजूद, प्रौद्योगिकी धोखाधड़ी, हमला, धमकाने, यौन उत्पीड़न और फ़िशिंग जैसे जोखिम भी पैदा करती है। ऐसे अपराधों को रोकने के लिए छात्रों के लिए साइबर सुरक्षा को समझना महत्वपूर्ण है। प्रश्नावली-आधारित सर्वेक्षण का उपयोग करके उत्तर प्रदेश के जौनपुर में वीर बहादुर पूर्वांचल विश्वविद्यालय से डेटा एकत्र किया गया था। डॉ. एस. राजशेखर (2011) द्वारा विकसित साइबर अपराध जागरूकता स्केल ने छात्रों की जागरूकता को मापा। अध्ययन में साइबर खतरों की समझ का आकलन करने के लिए लिंग और स्थान जैसे जनसांख्यिकीय कारकों पर विचार किया गया। परिकल्पनाओं का परीक्षण करने के लिए टी-परीक्षण का उपयोग किया गया था। निष्कर्षों से पता चलता है कि पुरुष और महिला छात्रों के बीच साइबर अपराध जागरूकता में कोई महत्वपूर्ण अंतर नहीं है, लेकिन ग्रामीण और शहरी क्षेत्रों के छात्रों के बीच उल्लेखनीय अंतर है।

Keywords: Cybercrime, Awareness, Technology, साइबर अपराध, जागरूकता, प्रौद्योगिकी

1. प्रस्तावना

भारत तेजी से तकनीकी रूप से आगे बढ़ रहा है, अब विश्व स्तर पर दूसरी सबसे बड़ी इंटरनेट आबादी का दावा कर रहा है। जैसे-जैसे डिजिटल दुनिया बढ़ती है, वैसे-वैसे साइबर खतरों के प्रति हमारी संवेदनशीलता भी बढ़ती है। साइबर अपराध भारत और वैश्विक समुदाय दोनों के लिए एक महत्वपूर्ण चिंता का विषय बन गया है। इन अपराधों में कंप्यूटर और इंटरनेट शामिल हैं और इन्हें अक्सर सफेदपोश अपराधों के रूप में वर्गीकृत किया जाता है, जिनमें साइबर धोखाधड़ी, फ़िशिंग, हैकिंग, पहचान की चोरी, डेटा चोरी, ब्लैकमेल, उत्पीड़न और बदमाशी शामिल हैं। साइबर अपराधों में, कंप्यूटर या डेटा या तो अपराध करने का उपकरण हो सकता है या स्वयं लक्ष्य हो सकता है। "साइबर अपराध" शब्द में प्रौद्योगिकी का उपयोग करके की जाने वाली सभी अवैध गतिविधियाँ शामिल हैं। इन अपराधों के पीछे के व्यक्ति आमतौर पर सूचना प्रौद्योगिकी के बारे में अत्यधिक जानकार होते

हैं। साइबर अपराधी कुशल आईटी विशेषज्ञ हैं जो अपराध करने के लिए प्रौद्योगिकी की अपनी समझ का फायदा उठाते हैं, और उनके कार्य राष्ट्रीय सीमाओं या पारंपरिक बाधाओं तक सीमित नहीं होते हैं।

आम तौर पर, साइबर अपराध तीन श्रेणियों में से एक में आते हैं:

1. टारगेट साइबर अपराध: इस प्रकार में कंप्यूटर को जानबूझकर नष्ट करना शामिल है।

2. टूल साइबर क्राइम: यहां किसी अपराध को अंजाम देने के लिए कंप्यूटर का इस्तेमाल किया जाता है।

3. कंप्यूटर आकस्मिक: इस श्रेणी में कंप्यूटर का उपयोग केवल आकस्मिक रूप से अपराध से संबंधित है। जैसे-जैसे तकनीक आगे बढ़ रही है, इंटरनेट और सोशल मीडिया उपयोगकर्ताओं की संख्या बढ़ती जा रही है। COVID-19 महामारी के दौरान और उसके बाद, व्यवसाय, शिक्षा, स्वास्थ्य सेवा, सरकार और उपभोक्ता सेवाओं सहित अधिक सेवाएँ ऑनलाइन हो गई हैं। जबकि सभी उम्र के लोग इंटरनेट, कंप्यूटर और सोशल मीडिया का उपयोग करते हैं, युवा व्यक्ति सबसे अधिक बार उपयोगकर्ता होते हैं। तकनीकी प्रगति के लाभों के बावजूद, इसने साइबर अपराध सहित विभिन्न खतरे भी पेश किए हैं। साइबर अपराध के मामलों में वृद्धि आंशिक रूप से युवाओं में इन मुद्दों के बारे में जागरूकता की कमी के कारण है।

2021 में, पिछले वर्ष की तुलना में भारत में साइबर अपराध रिपोर्टों में उल्लेखनीय वृद्धि हुई, जिसमें 52,000 से अधिक मामले दर्ज किए गए। इस अवधि के दौरान, कर्नाटक और उत्तर प्रदेश सबसे अधिक घटनाओं वाले राज्यों के रूप में उभरे। इन मामलों में मुख्य रूप से व्यक्तियों को धोखा देने या उनकी कामुकता का शोषण करने के प्रयास शामिल थे, जो अक्सर आईटी अधिनियम के अधिकार क्षेत्र के अंतर्गत आते थे।

वर्ष 2020 में साइबर-संबंधित अपराधों के लिए देशभर में 18,400 से अधिक गिरफ्तारियां हुईं, साथ ही 18,000 से अधिक व्यक्तियों को कानूनी कार्यवाही का सामना करना पड़ा। इनमें से, कंप्यूटर से संबंधित अपराध सबसे अधिक थे, इसके बाद स्पष्ट सामग्री के प्रकाशन और प्रसार से जुड़े मामले थे।

साइबर स्टॉकिंग और धमकाने के मामले में, महाराष्ट्र महिलाओं और बच्चों के खिलाफ लगभग 62 मामलों के साथ शीर्ष पर है, इसके बाद 2021 में 13 मामलों के साथ तेलंगाना का स्थान है। राष्ट्रीय स्तर पर, उस वर्ष लगभग 123 ऐसी घटनाएं दर्ज की गईं, जिन्हें भारतीय दंड संहिता की धारा 354 डी के तहत वर्गीकृत किया गया है।

साइबर सुरक्षा सॉफ्टवेयर कंपनी नॉर्टन लाइफलॉक ने खुलासा किया कि पिछले वर्ष के भीतर, 27 मिलियन भारतीय वयस्क पहचान की चोरी का शिकार हुए, जबकि 52% आबादी के पास साइबर खतरों से खुद को बचाने के बारे में जानकारी का अभाव है।

इसके अलावा, गृह मंत्रालय ने 30 अगस्त, 2019 को राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल की शुरुआत की, जिसका उद्देश्य महिलाओं और बच्चों को लक्षित अपराधों पर विशेष ध्यान देने के साथ साइबर घटनाओं की रिपोर्टिंग के लिए एक केंद्रीकृत मंच स्थापित करना है। पोर्टल के आंकड़ों के अनुसार, राष्ट्र की स्थापना से लेकर 28 फरवरी, 2021 तक कुल 317,439 साइबर अपराध की घटनाएं और 5,771 एफआईआर दर्ज की गईं। कर्नाटक में 21,562 साइबर अपराध की घटनाएं और 87 एफआईआर हुईं, जबकि देश भर में साइबर अपराध की घटनाओं की संख्या 50,806 थी। (राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल, 2019)।

साइबर अपराध के प्रकार:

1. **पहचान की चोरी** में धोखाधड़ी करने के लिए किसी की व्यक्तिगत जानकारी, जैसे उनका नाम, सामाजिक सुरक्षा नंबर, या बैंक विवरण चुराना शामिल है। अपराधी इस जानकारी का उपयोग अनधिकृत लेनदेन करने, नए खाते खोलने या यहां तक कि नकली कर रिटर्न दाखिल करने के लिए करते हैं। पीड़ितों को अक्सर गंभीर वित्तीय और भावनात्मक संकट का सामना करना पड़ता है क्योंकि वे अपनी पहचान बहाल करने और धोखाधड़ी वाले रिकॉर्ड को सही करने के लिए संघर्ष करते हैं। पहचान की चोरी से बचाने के लिए, व्यक्तिगत जानकारी की सुरक्षा करना, मजबूत पासवर्ड का उपयोग करना और वित्तीय विवरणों की नियमित रूप से निगरानी करना आवश्यक है।

2. **फ़िशिंग साइबर** अपराधियों द्वारा एक विश्वसनीय इकाई होने का दिखावा करके, आमतौर पर ईमेल, फोन या टेक्स्ट संदेशों के माध्यम से संवेदनशील जानकारी प्राप्त करने का एक भ्रामक प्रयास है। ये संदेश अक्सर वैध प्रतीत होते हैं, जो बैंकों, सोशल मीडिया प्लेटफ़ॉर्म या ऑनलाइन सेवाओं से वास्तविक संचार के स्वरूप और अनुभव की नकल करते हैं। पीड़ितों को दुर्भावनापूर्ण लिंक पर क्लिक करने या पासवर्ड और क्रेडिट कार्ड नंबर जैसी व्यक्तिगत जानकारी प्रदान करने के लिए बरगलाया जाता है। फ़िशिंग घोटालों से बचने के लिए, अनचाहे संदेशों के स्रोत को सत्यापित करना महत्वपूर्ण है और अनुरोध की वैधता की पुष्टि किए बिना कभी भी संवेदनशील जानकारी साझा न करें।

3. **सोशल इंजीनियरिंग** व्यक्तियों को गोपनीय जानकारी प्रकट करने या सुरक्षा से समझौता करने वाले कार्य करने के लिए हेरफेर करने के लिए मानव मनोविज्ञान का शोषण करती है। तकनीकी हैकिंग के विपरीत, सोशल इंजीनियरिंग विश्वास बनाने और लक्ष्यों को धोखा देने की तात्कालिकता की भावना पैदा करने पर निर्भर करती है। सामान्य रणनीति में बहाना बनाना (जानकारी हासिल करने के लिए एक परिदृश्य बनाना), प्रलोभन देना (पीड़ितों को आकर्षित करने के लिए कुछ लुभावनी पेशकश करना), और टेलगेटिंग (किसी प्रतिबंधित क्षेत्र में किसी का पीछा करना) शामिल हैं। अनचाहे अनुरोधों के प्रति जागरूकता और संदेह सामाजिक इंजीनियरिंग हमलों के खिलाफ प्रमुख बचाव हैं।

4. **साइबरस्टॉकिंग** में किसी को परेशान करने, डराने या पीछा करने के लिए इंटरनेट और अन्य डिजिटल साधनों का उपयोग करना शामिल है। इसमें धमकी भरे संदेश भेजना, झूठी जानकारी फैलाना या पीड़ित की ऑनलाइन गतिविधि की लगातार निगरानी करना शामिल हो सकता है। साइबर

स्टॉकर अक्सर अपने पीड़ितों पर नियंत्रण स्थापित करने के लिए सोशल मीडिया, ईमेल और अन्य ऑनलाइन प्लेटफ़ॉर्म का शोषण करते हैं, जिससे महत्वपूर्ण भावनात्मक संकट और भय पैदा होता है। साइबरस्टॉकिंग से खुद को बचाने में गोपनीयता सेटिंग्स को बढ़ाना, व्यक्तिगत जानकारी ऑनलाइन साझा करने के बारे में सतर्क रहना और यदि आवश्यक हो तो कानूनी मदद लेना शामिल है।

5. **बॉटनेट साइबर अपराधियों** द्वारा दूर से नियंत्रित संक्रमित कंप्यूटरों के नेटवर्क हैं। ये समझौता किए गए उपकरण, जिन्हें "बॉट्स" या "ज़ॉम्बी" के रूप में जाना जाता है, का उपयोग वितरित डिनायल-ऑफ-सर्विस (डीडीओएस) हमलों, स्पैम भेजने या डेटा चोरी करने जैसे समन्वित हमलों को करने के लिए किया जाता है। बॉटनेट में हजारों या लाखों संक्रमित डिवाइस शामिल हो सकते हैं, जो उन्हें साइबर अपराध के लिए शक्तिशाली उपकरण बनाते हैं। उपयोगकर्ता अपने सॉफ़्टवेयर को अद्यतन रखकर, विश्वसनीय एंटीवायरस प्रोग्राम का उपयोग करके और संदिग्ध डाउनलोड या लिंक से बचकर अपने कंप्यूटर को बॉटनेट का हिस्सा बनने से बचा सकते हैं।

6. **निषिद्ध सामग्री** का तात्पर्य डिजिटल सामग्री से है जिसका उत्पादन, वितरण या स्वामित्व अवैध है। इसमें ऐसी सामग्री शामिल है जो हिंसा भड़काती है, घृणा को बढ़ावा देती है, या बाल अश्लीलता का गठन करती है। ऐसी सामग्री का वितरण अक्सर इंटरनेट की गुमनामी के कारण होता है, जो कानून प्रवर्तन एजेंसियों के लिए महत्वपूर्ण चुनौतियाँ पैदा करता है। प्रतिबंधित सामग्री के प्रसार से निपटने के लिए, इंटरनेट उपयोगकर्ताओं को अपने सामने आने वाली किसी भी अवैध सामग्री की रिपोर्ट उचित अधिकारियों को करनी चाहिए और ऐसी सामग्री से जुड़ने या उसका प्रसार करने से बचना चाहिए। सरकारों और संगठनों को भी ऑनलाइन प्रतिबंधित सामग्री का पता लगाने और उसे हटाने के लिए प्रभावी नीतियां और तकनीक बनाने में सहयोग करने की आवश्यकता है।

2. साहित्य की समीक्षा

गोयल उर्मिला के 2015 में किए गए अध्ययन में, 120 बी.एड. की साइबर अपराध जागरूकता। हरियाणा के सोनीपत जिले के छात्रों का मूल्यांकन किया गया। निष्कर्षों से संकेत मिलता है कि लिंग ने साइबर अपराध जागरूकता को महत्वपूर्ण रूप से प्रभावित नहीं किया है, लेकिन स्थान ने जागरूकता के स्तर को प्रभावित किया है।

2018 में स्प्रिंग के शोध ने साइबर अपराध के बारे में जागरूकता मापने के लिए एक स्व-संरचित प्रश्नावली का उपयोग किया, जिसमें जनसांख्यिकीय डेटा और 2011 में एस राज शेखर द्वारा मान्य पैमाने को शामिल किया गया। अध्ययन ने परिकल्पनाओं का परीक्षण करने के लिए सहसंबंध और प्रतिशत विश्लेषण को नियोजित किया और साइबर अपराध को रोकने में अंतर्दृष्टि प्रदान की। परिणामों से पता चला कि पुरुष छात्रों ने अपनी महिला समकक्षों की तुलना में अधिक जागरूकता और सकारात्मक अंतर्दृष्टि प्रदर्शित की। इसके अतिरिक्त, 18 से 23 वर्ष की आयु के छात्रों ने 24 वर्ष और उससे अधिक आयु के छात्रों की तुलना में कम धारणा और जागरूकता का स्तर प्रदर्शित किया। बी.एड. की असुरक्षा को कम करने की रणनीतियाँ। विद्यार्थियों में साइबर अपराध के प्रति संवेदनशीलता को भी रेखांकित किया गया, जिसका लक्ष्य उत्पीड़न के प्रति उनकी संवेदनशीलता को कम करना था।

ठाकुर के 2018 के अध्ययन में 16 से 18 वर्ष की आयु के 200 किशोरों का आकलन करने के लिए राजशेखर साइबर-क्राइम जागरूकता स्केल को नियोजित करते हुए "किशोर साइबर-अपराध जागरूकता में लिंग और स्थानीय अंतर" पर चर्चा की गई। उनकी जांच में साइबर के संदर्भ में लिंग और स्थान के बीच एक उल्लेखनीय संबंध का पता चला। अपराध जागरूकता.

2020 में, चौधरी ने विभिन्न जनसांख्यिकीय कारकों पर विचार करते हुए, हरियाणा में उच्च शिक्षा के छात्रों के बीच साइबर अपराध जागरूकता का पता लगाया। अध्ययन में पारंपरिक और व्यावसायिक दोनों पाठ्यक्रमों के 500 छात्र शामिल थे। कुछ अपेक्षाओं के विपरीत, चौधरी ने पाया कि पेशेवर छात्रों ने पारंपरिक पाठ्यक्रमों में अपने समकक्षों की तुलना में साइबर अपराध के बारे में अधिक जागरूकता प्रदर्शित की, जिसमें कोई महत्वपूर्ण लिंग अंतर नहीं देखा गया।

सुवेरा एंड टेलर के 2020 के शोध में पुरुष और महिला बीएड का तुलनात्मक विश्लेषण किया गया। प्रशिक्षुओं को साइबर अपराध के प्रति जागरूक करना। गुजरात के नवसारी जिले में आयोजित उनके अध्ययन में 360 प्रशिक्षुओं को शामिल किया गया और लिंग, क्षेत्र (ग्रामीण बनाम शहरी), और जाति (खुले, एसईबीसी और एसटी-एससी) में समान प्रतिनिधित्व सुनिश्चित करने के लिए एक यादृच्छिक चयन पद्धति को नियोजित किया गया। राजशेखर (2011) द्वारा विकसित साइबर-अपराध जागरूकता स्केल का उपयोग करते हुए और डेटा विश्लेषण के लिए टी-परीक्षणों को नियोजित करते हुए, उन्होंने पुरुष और महिला प्रशिक्षुओं के बीच साइबर अपराध जागरूकता में महत्वपूर्ण अंतर पाया, साथ ही ग्रामीण और शहरी क्षेत्रों के प्रशिक्षुओं के बीच जागरूकता में असमानताएं पाईं। इसके अतिरिक्त, विभिन्न जाति समूहों से संबंधित प्रशिक्षुओं के बीच साइबर अपराध जागरूकता में भिन्नता देखी गई।

समस्या कथन: अध्ययन का उद्देश्य जौनपुर में छात्रों के बीच साइबर-अपराध जागरूकता की जांच करना है।

उद्देश्य:

• साइबर अपराध और उससे जुड़े जोखिमों की बुनियादी समझ विकसित करना।

• जौनपुर क्षेत्र में कॉलेज के छात्रों के बीच साइबर-अपराध जागरूकता के स्तर का आकलन करना।

• लिंग के आधार पर कॉलेज के छात्रों के बीच साइबर-अपराध जागरूकता का विश्लेषण करना।

• इलाके के आधार पर कॉलेज के छात्रों के बीच साइबर-अपराध जागरूकता का मूल्यांकन करना।

परिकल्पनाएँ:

पुरुष और महिला छात्रों के बीच साइबर-अपराध जागरूकता में कोई महत्वपूर्ण अंतर नहीं है।

ग्रामीण और शहरी छात्रों के बीच साइबर-अपराध जागरूकता में कोई महत्वपूर्ण अंतर नहीं है।

चर:				
क्रमांक	चर का नाम	चर की प्रकृति	स्तरों की संख्या	स्तर का नाम
1	लिंग	भेद	2	पुरुष/महिला
2	इलाका	अलग	2	शहरी/ग्रामीण

शोध डिजाइन:

वर्तमान अध्ययन के लिए एक पूर्व-पोस्ट फैक्टो अनुसंधान डिजाइन का उपयोग किया गया था।

सैम्पलिंग:

डेटा संग्रह के लिए यादृच्छिक नमूनाकरण विधि को नियोजित किया गया था। अध्ययन के उद्देश्यों के अनुरूप, वीर बहादुर पूर्वांचल विश्वविद्यालय के छात्रों को यादृच्छिक रूप से चुना गया था। अध्ययन में कुल 60 छात्रों ने भाग लिया, जिसमें 30 छात्र शहरी क्षेत्रों से और 30 छात्र जौनपुर के ग्रामीण क्षेत्रों से थे। इसके अतिरिक्त, नमूने में 30 पुरुष छात्र और 30 महिला छात्राएं शामिल थीं।

टूल विवरण:

साइबर अपराध जागरूकता स्केल (सीसीएएस-आरएस) 2011 में डॉ. एस. राजशेखर द्वारा विकसित किया गया था। इस पैमाने में 42 कथन शामिल हैं, जिनमें 24 सकारात्मक कथन हैं और शेष 18 नकारात्मक कथन हैं। प्रत्येक कथन को "दृढ़ता से सहमत" से लेकर "दृढ़ता से असहमत" तक के पांच-बिंदु पैमाने पर मूल्यांकित किया जाता है। मानकीकरण के बाद, पैमाने को 36 वस्तुओं को शामिल करने के लिए परिष्कृत किया गया, जिसमें 21 सकारात्मक वस्तुएं और 15 नकारात्मक वस्तुएं शामिल थीं। पैमाने पर स्कोर 36 से 180 तक होता है, उच्च स्कोर साइबर-अपराध के बारे में अधिक जागरूकता का संकेत देता है।

वैधता:

साइबर-अपराध जागरूकता स्केल निर्माण वैधता को प्रदर्शित करता है, क्योंकि वस्तुओं का चयन 1.75 के बराबर या उससे अधिक 'टी-वैल्यू' के आधार पर किया गया था। इसके अतिरिक्त, इसकी आंतरिक वैधता 0.87 निर्धारित की गई, जो मजबूत वैधता को दर्शाती है।

विश्वसनीयता:

साइबर-क्राइम अवेयरनेस स्केल की विश्वसनीयता पियर्सन उत्पाद-क्षण सहसंबंध को नियोजित करते हुए, स्प्लिट-हाफ विधि का उपयोग करके स्थापित की गई थी। पूर्ण पैमाने के लिए विश्वसनीयता के गुणांक की गणना स्पीयरमैन-ब्राउन भविष्यवाणी सूत्र का उपयोग करके की गई, जिससे 0.76 का उच्च गुणांक प्राप्त हुआ, जो मजबूत विश्वसनीयता का संकेत देता है।

मानक:

साइबर-अपराध जागरूकता स्केल के लिए जेड-स्कोर और टी-स्कोर मानदंड विकसित किए गए हैं, जो स्केल पर स्कोर की व्याख्या के लिए एक मानकीकृत आधार प्रदान करते हैं।

नतीजे:

उद्देश्य 3: जौनपुर क्षेत्र में कॉलेज के छात्रों के बीच साइबर-अपराध जागरूकता का आकलन करना।

तालिका 1:

छात्रों की व्याख्या की स्कोर रेंज संख्या	**छात्रों की व्याख्या की स्कोर रेंज संख्या**	**छात्रों की व्याख्या की स्कोर रेंज संख्या**
143 और उससे ऊपर	19	उत्कृष्ट जागरूकता
133-142	12	उच्च जागरूकता
123-132	10	औसत से ऊपर जागरूकता

108-122	9	मध्यम/औसत जागरूकता
99-107	8	औसत से कम जागरूकता
80-98	2	कम जागरूकता

तालिका नंबर एक:

पुरुषों के लिए औसत साइबर-अपराध जागरूकता स्कोर 145 है, जबकि महिलाओं के लिए यह 138 है। हालांकि साधनों में अंतर है, 1.96 का टी-वैल्यू इंगित करता है कि अंतर सांख्यिकीय रूप से महत्वपूर्ण नहीं है।

शहरी छात्रों के लिए औसत साइबर-अपराध जागरूकता स्कोर 150.73 है, जबकि ग्रामीण छात्रों के लिए यह 133.63 है। 5.05 के टी-वैल्यू के साथ, शहरी और ग्रामीण छात्रों के बीच साइबर-अपराध जागरूकता में महत्वपूर्ण अंतर है।

उद्देश्य 2: लिंग के आधार पर कॉलेज के छात्रों की साइबर-अपराध जागरूकता का आकलन करना।

परिकल्पना 2: साइबर-अपराध जागरूकता में पुरुष और महिला छात्रों के बीच कोई महत्वपूर्ण अंतर नहीं होगा।

तालिका 2 साइबर-अपराध जागरूकता के संबंध में पुरुष और महिला छात्रों के एन, माध्य, एसडी और टी-मूल्य को दर्शाती है। वे
रिएबल्स एन मीन एसडी टी-वैल्यू महत्वपूर्ण स्तरपुरुष 30 145 4.05 1.97 एन.एस
महिला 30 138 7.13

उद्देश्य 3: इलाके के आधार पर कॉलेज के छात्रों की साइबर-अपराध जागरूकता का आकलन करना।

परिकल्पना 3: साइबर-अपराध जागरूकता में शहरी और ग्रामीण छात्रों के बीच कोई महत्वपूर्ण अंतर नहीं होगा।

तालिका 3 शहरी और ग्रामीण छात्रों के एन, माध्य, एसडी और टी-मूल्य को दर्शाती है।
वेरिएबल्स एन मीन एसडी टी-वैल्यू महत्वपूर्ण स्तर
शहरी 30 150.73 3.47 5.04* 0.01 स्तर पर महत्वपूर्ण अंतर
ग्रामीण 30 133.63 5.89
*पी <0.01 स्तर (महत्वपूर्ण अंतर)

तालिका 3 से पता चलता है कि शहरी छात्रों के लिए औसत साइबर-अपराध जागरूकता स्कोर 150.73 है, जबकि ग्रामीण छात्रों के लिए यह 133.63 है। 5.04 का टी-वैल्यू 0.01 स्तर पर शहरी और ग्रामीण छात्रों के बीच एक महत्वपूर्ण अंतर दर्शाता है।

3. विचार विमर्श

यह अध्ययन छात्रों के बीच साइबर अपराध जागरूकता के स्तर पर केंद्रित है। हमारी पहली परिकल्पना, जिसमें कहा गया है कि पुरुष और महिला छात्रों के बीच जागरूकता में कोई महत्वपूर्ण अंतर नहीं है, डेटा द्वारा समर्थित थी। हालाँकि औसत अंतर ने संकेत दिया कि पुरुष साइबर-अपराध के बारे में थोड़ा अधिक जागरूक हैं और खुद को बचाने के लिए साइबर स्वच्छता तरीकों को अपनाने की अधिक संभावना रखते हैं, यह अंतर सांख्यिकीय रूप से महत्वपूर्ण नहीं था। ऐसा दोनों लिंगों के पास इंटरनेट तक समान पहुंच और साइबर-अपराध जागरूकता के संबंध में समान शैक्षिक अवसरों के कारण हो सकता है।

हमारी दूसरी परिकल्पना, जिसमें कहा गया था कि स्थानीयता छात्रों के बीच साइबर-अपराध जागरूकता को महत्वपूर्ण रूप से प्रभावित नहीं करेगी, अस्वीकृत थी। डेटा से शहरी और ग्रामीण छात्रों के बीच महत्वपूर्ण अंतर का पता चला, शहरी छात्रों ने उच्च जागरूकता प्रदर्शित की। यह विसंगति अवसरों और संसाधनों तक असमान पहुंच से उत्पन्न हो सकती है, जिसके परिणामस्वरूप ग्रामीण छात्रों को अपने शहरी समकक्षों की तुलना में प्रभावी इंटरनेट उपयोग के बारे में कम जानकारी होती है।

ये निष्कर्ष पिछले शोध के अनुरूप हैं, जो छात्रों की भलाई के लिए एक महत्वपूर्ण मुद्दे के रूप में साइबर अपराध जागरूकता के महत्व को रेखांकित करते हैं। छात्रों को साइबर सुरक्षा के बारे में शिक्षित करना और उन्हें साइबर हमलों को रोकने और संभावित साइबर अपराधों से खुद को बचाने के लिए ज्ञान से लैस करना अनिवार्य है।

4. निष्कर्ष

निष्कर्षतः, जौनपुर क्षेत्र में कॉलेज के छात्र साइबर अपराध के प्रति औसत से अधिक जागरूकता प्रदर्शित करते हैं। सर्वेक्षण में शामिल छात्रों में से, 69% ने सामान्य या औसत से ऊपर जागरूकता स्तर का प्रदर्शन किया। निष्कर्षों से पता चलता है कि शिक्षा और तकनीकी प्रदर्शन छात्रों की साइबर अपराध जागरूकता को महत्वपूर्ण रूप से प्रभावित करते हैं, शहरी छात्र अपने ग्रामीण समकक्षों की तुलना में अधिक जागरूकता दिखाते हैं। हालाँकि, लिंग का साइबर अपराध जागरूकता पर कोई स्पष्ट प्रभाव नहीं पड़ा।

5. सुझाव

1) अधिक सटीक और सामान्यीकृत परिणामों के लिए बड़े नमूना आकार के साथ एक अध्ययन करें।
2) विभिन्न अध्ययन क्षेत्रों के आधार पर तुलनात्मक अध्ययन करना।

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Basuroy T. (2022). Number of reported cyber crimes in India 2012- 2021. Statista. Retrieved from https://www.statista.com/statistics/309435/india-cyber-crime-it-act/

Choudhary, D.M. (2020). Cybercrime awareness among higher education students of Haryana in relation to different demographic variables. PalArch Journal of Archaeology of Egypt/Egyptology, 17(7), Article 7.

Goel (2015). Gender and locational differences in cybercrime awareness among adolescents-ProQuest. (Ra.). Retrieved November 24, 2023 from https://www.proquest.com/openview/a68a1a11f0cb4d04c1fca1ccdbc61461/1?pq-origsite=gscholar&cbl=2032134

National Cybercrime Reporting Portal. (2019). Retrieved November 24, 2023, from https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1703509

Suvera, D.P., & Taylor, P.R. (2020). Cyber-crime awareness: A comparative study of male and female B.Ed. trainees.