Online at: https://researchtrendsjournal.com
Indexed Journal

ISSN No: 2584-282X
Peer Reviewed Journal

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 3; Issue 4; 2025; Page No. 219-224

Received: 14-04-2025
Accepted: 27-06-2025
Published: 29-07-2025

ग्राहकों और बैंक कर्मचारियों के बीच साइबर सुरक्षा जागरूकता के स्तर का विश्लेषण करना

[1]Rakesh Kumar Rai, [2]Dr. Subhasish Basu and [3]Dr. Aiman Fatma

[1]Research Scholar, Department of Commerce, P.K. University, Shivpuri, Madhya Pradesh, India
[2]Supervisor, Department of Commerce, P.K. University, Shivpuri, Madhya Pradesh, India
[3]Associate Professor, Department of Commerce, P.K. University, Shivpuri, Madhya Pradesh, India

DOI: https://doi.org/10.5281/zenodo.18699881

Corresponding Author: Rakesh Kumar Rai

सारांश

साइबर-हमले लगातार विकसित हो रहे हैं और लगातार बढ़ रहे हैं तथा व्यापक हो रहे हैं। हमलावर अपनी रणनीति और तकनीकों में सुरक्षा टीमों की तुलना में तेज़ी से सुधार कर रहे हैं तथा उनके तरीके हर साल अधिक परिष्कृत होते जा रहे हैं। इसलिए, यह शोध समीक्षाओं, लेखों, साक्षात्कारों और केस स्टडी के माध्यम से वर्तमान साइबर सुरक्षा योजनाओं और अवधारणाओं का अध्ययन करने के लिए किया गया है। इसका उद्देश्य उपयोगकर्ताओं के बीच साइबर सुरक्षा और इसके नियमों के बारे में जागरूकता पैदा करना है। इसने यह मूल्यांकन करने का प्रयास किया है कि कितने लोग ऑनलाइन लेनदेन करते समय वास्तव में साइबर सुरक्षा नियमों का उपयोग कर रहे हैं।

मूलशब्द: साइबर सुरक्षा, ऑनलाइन बैंकिंग, ऑनलाइन, बैंकिंग, जागरूकता।

प्रस्तावना

वैश्विक वित्तीय परिदृश्य में चुनौतियों की एक निरंतर विकसित श्रृंखला सामने आ रही है, जिसमें परिचालन संबंधी कमियाँ, बाजार में अस्थिरता, भू-राजनीतिक अनिश्चितताएँ, साइबर सुरक्षा खतरे और विनियामक अनुपालन और ऋण स्तरों पर आशंकाएँ शामिल हैं। इन जोखिमों में वित्तीय संकटों को ट्रिगर करने, बाजार में व्यवधान पैदा करने और वैश्विक आर्थिक विकास को प्रभावित करने की अलग-अलग डिग्री की क्षमता होती है। वित्तीय संस्थानों, नियामकों और बाजार के खिलाड़ियों को इस बदलते माहौल में सतर्क और अनुकूलनशील रहना चाहिए। इन खतरों को संबोधित करने और कम करने के लिए, सक्षम जोखिम प्रबंधन, नियामक निरीक्षण, तकनीकी नवाचार और अंतर्राष्ट्रीय सहयोग महत्वपूर्ण घटक हैं।

वर्तमान में, साइबर सुरक्षा सभी संगठनों के लिए एक बढ़ती चुनौती है। पिछले वर्ष में, यह स्पष्ट हो गया है कि बैंकिंग क्षेत्र में इसके बुनियादी ढांचे और साइबर सुरक्षा उपायों में कई कमियाँ थीं। डिजिटल परिवर्तन ने बैंकिंग उद्योग को मौलिक रूप से बदल दिया है, जिसके परिणामस्वरूप दक्षता में वृद्धि हुई है, पहुँच में विस्तार हुआ है और ग्राहकों के लिए बेहतर अनुभव हुआ है। फिर भी, इस तेज़ डिजिटलीकरण ने साइबर खतरों को भी बढ़ा दिया है, जिससे वित्तीय संगठनों के लिए साइबर सुरक्षा एक सर्वोपरि मुद्दा बन गई है। वर्तमान में, बैंकों को मैलवेयर हमलों, फ़िशिंग, पहचान की चोरी, रैनसमवेयर, अवैध डेटा उल्लंघनों और साइबर अपराध के तेजी से उन्नत प्रकारों सहित कई खतरों का सामना करना पड़ता है।

इन पारंपरिक जोखिमों के अलावा, ऑनलाइन बैंकिंग से जुड़े कई उभरते खतरे तत्काल ध्यान देने की मांग करते हैं। उदाहरण के लिए, मोबाइल बैंकिंग एप्लिकेशन का व्यापक रूप से अपनाया जाना, उपयोगकर्ताओं को कम से कम सुरक्षा उपायों के साथ काम करने पर बढ़ी हुई कमज़ोरियों के प्रति उजागर करता है, जिससे अनधिकृत पहुँच और धोखाधड़ी का जोखिम काफी बढ़ जाता है। इसके अलावा, जैसे-जैसे बैंक अपने आंतरिक बचाव को मजबूत करते हैं, साइबर अपराधी तीसरे पक्ष के नेटवर्क और साझा बैंकिंग सिस्टम को तेज़ी से निशाना बना रहे हैं, जिनमें अक्सर मज़बूत

सुरक्षा उपायों की कमी होती है, जिससे हमलों के लिए आसान प्रवेश बिंदु बन जाते हैं।
तेज़ी से बढ़ता क्रिप्टोकरेंसी बाज़ार इन चुनौतियों को और भी जटिल बनाता है; इस क्षेत्र में नवजात विनियामक ढाँचा और तकनीकी नवाचार की तेज़ गति साइबर हमलों के लिए अवसर पैदा करती है जो सुरक्षा खामियों का फ़ायदा उठाते हैं। ये बहुआयामी जोखिम अभिनव साइबर सुरक्षा रणनीतियों की तत्काल आवश्यकता को उजागर करते हैं जो गतिशील खतरे के परिदृश्य के अनुकूल हो सकते हैं और डिजिटल बैंकिंग पारिस्थितिकी तंत्र की सुरक्षा कर सकते हैं।

साहित्य की समीक्षा

सिंह, प्रभात. (2023) [11] हम एक समकालीन, डिजिटल और वैश्वीकृत दुनिया में रहते हैं। जहाँ दक्षता और सुविधा प्रबल है, हालाँकि यह आसानी एक कीमत पर आती है। ई-बैंकिंग कई लाभ प्रदान करती है; फिर भी, यह चुनौतियों या मुद्दों से रहित नहीं है। ऐसा ही एक मुद्दा बैंकिंग उद्योग के अंदर साइबर सुरक्षा बनाए रखना है। यह अध्ययन साइबर खतरों के कई आयामों पर चर्चा करता है। भारत में साइबर सुरक्षा के लिए नियामक ढांचा। यह पेपर भारत में साइबर सुरक्षा के लिए अलग-अलग कानूनों की आवश्यकता पर अंतर्दृष्टि प्रदान करता है।
सी.पी., कृष्णा. (2024) डिजिटल बैंकिंग की तीव्र प्रगति ने साइबर सुरक्षा खतरों में वृद्धि की है, जिससे वित्तीय संस्थान और उनके ग्राहक खतरे में हैं। यह अध्ययन डिजिटल बैंकिंग में महत्वपूर्ण साइबर सुरक्षा चिंताओं, उनके परिणामों और रोकथाम के विकल्पों की जांच करता है। अध्ययन में अनुभवजन्य केस स्टडी और डेटा व्याख्या शामिल है, जो वर्तमान सुरक्षा समाधानों की प्रभावकारिता के बारे में जानकारी प्रदान करता है। विविध साइबर सुरक्षा चिंताओं, बदलते खतरे के माहौल और इन जोखिमों को कम करने में प्रौद्योगिकी के कार्य की गहन जांच प्रस्तुत की गई है। यह अध्ययन नियामक अनुपालन, नीतिगत सुझावों और साइबर सुरक्षा में उभरते रुझानों की जांच करता है।
पॉल (2024) यह सार बैंकिंग उद्योग के भीतर साइबर सुरक्षा का सारांश प्रस्तुत करता है, जिसमें भारतीय संस्थानों के लिए इसके महत्व, समस्याओं और निवारक रणनीतियों पर जोर दिया गया है। साइबर सुरक्षा में नेटवर्क सुरक्षा, एप्लिकेशन सुरक्षा और सूचना सुरक्षा जैसे क्षेत्रों सहित डिजिटल संपत्तियों को अवांछित पहुँच से सुरक्षित रखना शामिल है। भारतीय बैंकों को कई साइबर खतरों का सामना करना पड़ता है, जैसे फ़िशिंग योजनाएँ, डेटा उल्लंघन और रैनसमवेयर हमले, जिनके लिए मल्टी-फ़ैक्टर प्रमाणीकरण, नियमित सुरक्षा ऑडिट और स्टाफ़ प्रशिक्षण पहल जैसे कड़े निवारक उपायों की आवश्यकता होती है। साइबर जोखिमों से सफलतापूर्वक निपटने के लिए सेक्टर और सरकारी संस्थाओं के बीच सहयोग को ज़रूरी माना जाता है। तेज़ी से बदलते डिजिटल माहौल में बैंकिंग उद्योग में विश्वास, प्रतिष्ठा और स्थिरता को बनाए रखने के लिए साइबर सुरक्षा को महत्वपूर्ण माना जाता है।
शेखर (2023) 21वीं सदी में, इंटरनेट तकनीक को बेहतरीन प्रदर्शन के लिए बढ़ाया गया है और सभी उपयोगकर्ताओं द्वारा इसका व्यापक रूप से उपयोग किया जाता है। डिजिटल बैंकिंग क्षेत्र शीर्ष पांच में है और लगातार NEFT, Google Pay और Ponape जैसी ऑनलाइन तकनीकों का उपयोग करता है। ऑनलाइन बैंकिंग के बढ़ते उपयोग के बावजूद, बैंकिंग उद्योग के भीतर साइबर अपराध पिछले कुछ वर्षों में बढ़ रहे हैं। यह कहा गया है कि 50% साइबर अपराध एटीएम, डेबिट कार्ड और ऑनलाइन बैंकिंग से जुड़े हैं। बैंकिंग उद्योग अन्य उद्योगों की तुलना में अधिक बार साइबर हमलों का सामना कर रहा है। यह अध्ययन बैंकिंग उद्योग में साइबर हमलों और ऐसे खतरों के खिलाफ साइबर सुरक्षा को बढ़ाने के तरीकों की जांच करता है।
मूंदड़ा, आदर्श (2024).इस शोध का उद्देश्य वित्तीय संस्थानों पर साइबर अपराध के हानिकारक प्रभावों की जांच करना और इसके परिणामों को कम करने के लिए एक मजबूत साइबर सुरक्षा ढांचे का विकास करना है। हाल ही में बैंक इसके प्राथमिक लक्ष्य रहे हैं। भारत में कई बैंक अक्सर बड़े पैमाने पर मैलवेयर हमलों के अधीन होते हैं, जो निजी और संवेदनशील जानकारी से समझौता करते हैं और काफी वित्तीय नुकसान का कारण बनते हैं। इस शोध का उद्देश्य यह पहचानना है कि कौन से उद्योग क्षेत्र साइबर हमलों के लिए अधिक संवेदनशील हैं और साइबर सुरक्षा नीतियों के विकास और अनुकूलन को सुनिश्चित करना है। रिपोर्ट में विभिन्न साइबर खतरों और अपराधों की केस स्टडी जांच शामिल है, जिसके कारण काफी वित्तीय नुकसान हुआ है, साथ ही सरकारी वेबसाइटों, शैक्षणिक प्रकाशनों और शोध पत्रों सहित विभिन्न इंटरनेट संसाधनों से प्राप्त द्वितीयक डेटा विश्लेषण भी शामिल है। यह लेख साइबर शासन के बारे में अंतर्दृष्टि प्रदान करेगा जो वित्तीय संस्थानों, बैंकों और बड़े पैमाने पर समाज को लाभान्वित करेगा।

शोध पद्धति

अनुसंधान डिजाइन

शोध डिजाइन एक व्यापक योजना है जो शोध परियोजना के उद्देश्यों को परिभाषित करती है और उन उद्देश्यों को पूरा करने के लिए जो भी इच्छाएं पूरी की जानी हैं, उनके लिए दिशानिर्देश प्रदान करती है। दूसरे शब्दों में, यह शोध परियोजना को पूरा करने के लिए एक सामान्य योजना है।

डेटा संग्रहण के लिए उपकरण

डेटा संग्रह या डेटा का संग्रह अनुसंधान की प्रक्रिया में एक महत्वपूर्ण चरण हो सकता है। डेटा एकत्र करने के लिए आप जो उपकरण चुनते हैं, वह इस बात पर निर्भर करेगा कि आप किस तरह का डेटा एकत्र करना चाहते हैं और आप इसे कैसे एकत्र करने की योजना बना रहे हैं।

इस शोध को तैयार करने में कई सामान्य डेटा संग्रह उपकरणों का उपयोग किया गया

- प्रश्नावली
- बैठक
- व्याख्याओं
- सरकारी स्रोत
- प्रयोगशाला प्रयोग
- इलेक्ट्रॉनिक मेल या इलेक्ट्रॉनिक संदेश

नमूना डिजाइन

नमूनाकरण डिज़ाइन एक गणितीय फ़ंक्शन है जो आपको यह संभावना देता है कि एक निश्चित नमूना लिया जाएगा। चूँकि नमूनाकरण लगभग सभी शोध परियोजनाओं का आधार है, इसलिए नमूनाकरण डिज़ाइन का अध्ययन सांख्यिकी का एक महत्वपूर्ण हिस्सा है। प्रत्यक्ष अध्ययन एक खंड-आधारित अध्ययन हो सकता है। नतीजतन, नमूनाकरण तकनीक और नमूनाकरण डिज़ाइन समय पर लक्ष्य प्राप्त करने में महत्वपूर्ण भूमिका निभाते हैं।

डेटा विश्लेषण और परिकल्पना परीक्षण पूरा करना

डेटा विश्लेषण मुख्य रूप से वर्णनात्मक और भिन्न सांख्यिकीय परीक्षणों का उपयोग करके किया जाता है। डेटा को प्रस्तुत करने के लिए अभिव्यंजक सांख्यिकी और चार्ट / ग्राफ़ का उपयोग किया जाता है, जबकि अनुमानात्मक सांख्यिकी का उपयोग परिकल्पना का परीक्षण करने के लिए किया जाता है। डेटा विश्लेषण करने के लिए विभिन्न वर्णनात्मक और विभिन्न सांख्यिकीय परीक्षणों का उपयोग किया जाता है। वर्णनात्मक सांख्यिकी के साथ ग्राफ़ का उपयोग डेटा प्रस्तुत करने के लिए किया जाता है जबकि अनुमानात्मक सांख्यिकी का उपयोग परिकल्पना का परीक्षण करने के लिए किया जाता है।

- ची स्क्वायर टेस्ट
- एनोवा

डेटा विश्लेषण

यह अध्याय मात्रात्मक और गुणात्मक दोनों तरह के डेटा के विश्लेषण से संबंधित है। प्राथमिक डेटा इंटरनेट बैंकिंग के ग्राहकों के उपयोग, अपने बैंक खाते में साइबर अपराध का अनुभव करने वाले और पीड़ित बनने वाले ग्राहकों और साइबर अपराध का अनुभव न करने वाले या गैर-पीड़ित लोगों के संबंध में एकत्र किया गया था।

सभी लिंगों में साइबर सुरक्षा नियमों के बारे में जागरूकता

साइबर सुरक्षा के बारे में जागरूकता में लोगों को कार्रवाई करने के लिए पर्याप्त रूप से जागरूक करना शामिल है। इसके लिए सिर्फ़ नियमों का एक सेट नहीं, बल्कि सुरक्षा मानसिकता बनाने की ज़रूरत है। संक्षेप में, यह सिर्फ़ खतरों के बारे में जागरूक होने के बारे में नहीं है, बल्कि खतरों और संगठन और उसके लोगों पर उनके प्रभाव को समझने के बारे में भी है, जिसमें खुद भी शामिल हैं।

तालिका 1: साइबर सुरक्षा नियमों के बारे में लिंग के आधार पर जागरूकता

ऑनलाइन लेनदेन में सुरक्षा नियमों के प्रति आप कितने चिंतित और जागरूक हैं?		लिंग		कुल
		पुरुष	महिला	
पूरी तरह।	गिनती करना	119	76	195
	प्रतिशत (%)	27.5	25.9	26.9
थोड़ा	गिनती करना	261	190	451
	प्रतिशत (%)	60.4	64.6	62.1
बिल्कुल नहीं	गिनती करना	52	28	80
	प्रतिशत (%)	12.0	9.5	11.0
कुल	गिनती करना	432	294	726
	प्रतिशत (%)	100.0	100.0	100.0

उपरोक्त तालिका 1 से पता चलता है कि 119 पुरुष और 76 महिलाएं ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों के बारे में पूरी तरह से अवगत थे, 261 पुरुष और 190 महिलाएं ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों के बारे में आंशिक रूप से अवगत थीं। हालाँकि, 52 पुरुष और 28 महिलाएँ ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों के बारे में बिल्कुल भी नहीं जानती थीं।

तालिका 2: काई-स्क्वायर परीक्षण

	कीमत	डीएफ	असिम्प्. सिग. (2-पक्षीय)
पियर्सन ची-स्क्वायर	1.689ए	2	.430
संभावना अनुपात	1.705	2	.426
रैखिक-दर-रैखिक एसोसिएशन	.033	1	.856
वैध मामलों की संख्या N	726		

उपरोक्त परीक्षण में शून्य परिकल्पना को अस्वीकार नहीं किया गया है क्योंकि $p>0.05$ (0.430) है। इसलिए, साइबर सुरक्षा नियमों और लिंग के बारे में जागरूकता एक दूसरे से स्वतंत्र हैं।

सभी आयु वर्गों में साइबर सुरक्षा नियमों के बारे में जागरूकता

सर्वेक्षण के लिए 18 से लेकर 60 वर्ष से अधिक आयु के विभिन्न आयु समूहों के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका विभिन्न आयु समूहों के बीच साइबर सुरक्षा नियमों के बारे में जागरूकता को दर्शाती है।

तालिका 3: आयु वर्ग के अनुसार साइबर सुरक्षा नियमों के बारे में जागरूकता

ऑनलाइन लेनदेन में सुरक्षा नियमों के प्रति आप कितने चिंतित और जागरूक हैं?		आयु				
		18 से 25	25 से 46	46 से 60	60 से ऊपर	कुल
पूरी तरह	गिनती करना	96	95	2	2	195
	प्रतिशत (%)	30.3	25.1	7.1	100.0	26.9
थोड़ा	गिनती करना	183	252	16	0	451
	प्रतिशत (%)	57.7	66.5	57.1	0.0	62.1
बिल्कुल नहीं	गिनती करना	38	32	10	0	80
	प्रतिशत (%)	12.0	8.4	35.7	0.0	11.0
कुल	गिनती करना	317	379	28	2	726
	प्रतिशत (%)	100.0	100.0	100.0	100.0	100.0

उपरोक्त तालिका 3 यह निर्धारित करती है कि सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 96 उत्तरदाता 18 से 25 आयु वर्ग के थे, 95 उत्तरदाता 25 से 46 आयु वर्ग के थे, 02 उत्तरदाता 46 से 60 आयु वर्ग के थे और 02 उत्तरदाता 60 वर्ष और उससे अधिक आयु वर्ग के थे जो ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों से पूरी तरह अवगत थे। 18 से 25 आयु वर्ग के 183 उत्तरदाता, 25 से 46 आयु वर्ग के 252 उत्तरदाता और 46 से 60 आयु वर्ग के 16 उत्तरदाता ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों से आंशिक रूप से अवगत थे। हालांकि, 18 से 25 आयु वर्ग के 38 उत्तरदाता, 25 से 46 आयु वर्ग के 32 उत्तरदाता और 46 से 60 आयु वर्ग के 10 उत्तरदाता ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों से बिल्कुल भी अवगत नहीं थे।

तालिका 4: काई-स्क्वायर परीक्षण

	कीमत	डीएफ	असिम्प्. सिग. (2-पक्षीय)
पियर्सन ची-स्क्वायर	31.646ए	6	.000
संभावना अनुपात	27.492	6	.000
रैखिक-दर-रैखिक एसोसिएशन	3.327	1	.068
वैध मामलों की संख्या N	726		

उपरोक्त परीक्षण में शून्य परिकल्पना को $p<0.05$ (0.000) के रूप में खारिज कर दिया गया है। इसलिए, साइबर सुरक्षा नियमों के बारे में जागरूकता और आयु एक दूसरे से स्वतंत्र नहीं हैं।

शिक्षा जगत में साइबर सुरक्षा नियमों के बारे में जागरूकता:
सर्वेक्षण के लिए अलग-अलग शैक्षणिक पृष्ठभूमि वाले 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका अलग-अलग शैक्षणिक पृष्ठभूमि वाले विभिन्न उत्तरदाताओं के बीच साइबर सुरक्षा नियमों के बारे में जागरूकता को दर्शाती है।

तालिका 5: शिक्षा जगत में साइबर सुरक्षा नियमों के बारे में जागरूकता

ऑनलाइन लेनदेन में सुरक्षा नियमों के प्रति आप कितने चिंतित और जागरूक हैं?		शिक्षा							कुल
		एच एस सी तक	डिप्लोमा	स्नातक	स्नातकोत्तर	पी एच. डी.	सीए	रिसर्च स्कॉलर	
पूरी तरह	गिनती करना	21	0	69	95	2	8	0	195
	%	39.6	0	24.9	26.2	16.7	57.1	0	26.9
थोड़ा	गिनती करना	22	4	165	246	6	6	2	451
	%	41.5	66.7	59.6	68	50	42.9	100	62.1
बिल्कुल नहीं	गिनती करना	10	2	43	21	4	0	0	80
	%	18.9	33.3	15.5	5.8	33.3	0	0	11
कुल	गिनती करना	53	6	277	362	12	14	2	726
	%	100	100	100	100	100	100	100	100

उपरोक्त तालिका 5 में बताया गया है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 195 (21 एच.एस.सी. तक, 69 स्नातक, 95 स्नातकोत्तर, 02 पी.एच.डी. और 08 चार्टर्ड अकाउंटेंट) उत्तरदाता साइबर सुरक्षा नियमों के बारे में चिंतित और पूरी तरह से अवगत थे। 451 (22 एच.एस.सी. तक, 4 डिप्लोमा, 165 स्नातक, 246 स्नातकोत्तर, 06 पी.एच.डी., 06 चार्टर्ड अकाउंटेंट और 02 रिसर्च स्कॉलर) उत्तरदाता भी चिंतित थे, लेकिन साइबर सुरक्षा नियमों के बारे में आंशिक रूप से जानते थे। हालांकि, 80 (10 एच.एस.सी. तक, 02 डिप्लोमा, 43 स्नातक, 21 स्नातकोत्तर और 04 पी.एच.डी.) उत्तरदाता बिल्कुल भी चिंतित नहीं थे और न ही वे साइबर सुरक्षा नियमों के बारे में जानते थे।

तालिका 6: काई-स्क्वायर परीक्षण

	कीमत	डीएफ	असिम्प्. सिग. (2-पक्षीय)
पियर्सन ची-स्क्वायर	45.457ए	12	.000
संभावना अनुपात	46.234	12	.000
रैखिक-दर-रैखिक एसोसिएशन	2.264	1	.132
वैध मामलों की संख्या N	726		

उपरोक्त परीक्षण में शून्य परिकल्पना को $p<0.05$ (0.000) के रूप में खारिज कर दिया गया है। इसलिए, साइबर सुरक्षा नियमों और शिक्षा के बारे में जागरूकता एक दूसरे से स्वतंत्र नहीं हैं।

विभिन्न लिंगों के बीच नकद जमा के वित्तीय लेनदेन
सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 7 विभिन्न लिंगों द्वारा किए गए नकद जमा के वित्तीय लेन-देन को दर्शाती है।

तालिका 7: विभिन्न लिंगों में नकद जमा के वित्तीय लेनदेन

			नकद जमा		कुल
			नहीं	हाँ	
लिंग	पुरुष	गिनती करना	221	211	432
		लिंग के भीतर %	51.2	48.8	100
	महिला	गिनती करना	143	151	294
		लिंग के भीतर %	48.6	51.4	100
कुल		गिनती करना	364	362	726
		लिंग के भीतर %	50.1	49.9	100

तालिका 7 से पता चलता है कि सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएँ थीं। इन 432 पुरुषों में से 211 पुरुष नकद जमा का वित्तीय लेन-देन करना पसंद करते हैं जबकि 221 पुरुष नकद जमा का वित्तीय लेन-देन ऑनलाइन करना पसंद नहीं करते हैं। इसी तरह, इन 294 महिलाओं में से 151 महिलाएँ नकद जमा का वित्तीय लेन-देन करना पसंद करती हैं जबकि 143 महिलाएँ नकद जमा भेजना ऑनलाइन करना पसंद नहीं करती हैं।

तालिका 8: काई-स्क्वायर परीक्षण

			असिम्प.	सटीक सिग. (दो तरफा)	सटीक सिग. (1-पक्षीय)
	कीमत	डीएफ	सिग. (दो तरफा)		
पियर्सन ची-स्क्वायर	.444ए	1	0.505		
निरंतरता सुधार	0.349	1	0.555		
संभावना अनुपात	0.444	1	0.505		
फिशर का सटीक परीक्षण				0.545	0.277
रैखिक-दर-रैखिक एसोसिएशन	0.443	1	0.506		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि नकद जमा का उपयोग और लिंग स्वतंत्र नहीं हैं (काई-स्क्वायर 0.444, df 1, p>0.05)। इस प्रकार, नकद जमा जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है। कोई भी व्यक्ति नकद जमा कर सकता है, चाहे वह परिवार का कमाने वाला सदस्य हो या आश्रित सदस्य। इसलिए, नकद जमा जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

विभिन्न लिंगों के बीच नकद निकासी के वित्तीय लेनदेन

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 9 विभिन्न लिंगों द्वारा किए गए नकद निकासी के वित्तीय लेन-देन को दर्शाती है।

तालिका 9: विभिन्न लिंगों में नकद निकासी के वित्तीय लेनदेन

			नकद निकासी		कुल
			नहीं	हाँ	
लिंग	पुरुष	गिनती करना	211	221	432
		लिंग के भीतर %	48.8	51.2	100
	महिला	गिनती करना	130	164	294
		लिंग के भीतर %	44.2	55.8	100
कुल		गिनती करना	341	385	726
		लिंग के भीतर %	47	53	100

तालिका 9 से यह देखा जा सकता है कि सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएँ थीं। इन 432 पुरुषों में से 221 पुरुष नकद निकासी के वित्तीय लेन-देन करना पसंद करते हैं जबकि 211 पुरुष ऑनलाइन नकद निकासी के वित्तीय लेन-देन करना पसंद नहीं करते हैं। इसी तरह, इन 294 महिलाओं में से 164 महिलाएँ नकद निकासी के वित्तीय लेन-देन करना पसंद करती हैं जबकि 130 महिलाएँ ऑनलाइन नकद निकासी के वित्तीय लेन-देन करना पसंद नहीं करती हैं।

तालिका 10: काई-स्क्वायर परीक्षण

	कीमत	डीएफ	असिम्प्. सिग. (1-पक्षीय)	सटीक सिग. (1-पक्षीय)	सटीक सिग. (1-पक्षीय)
पियर्सन ची-स्क्वायर	1.502ए	1	0.22		
निरंतरता सुधार	1.32	1	0.25		
संभावना अनुपात	1.5	1	0.22		
फिशर का सटीक परीक्षण				0.23	0.13
रैखिक-दर-रैखिक एसोसिएशन	1.5	1	0.22		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि नकद निकासी का उपयोग और लिंग स्वतंत्र नहीं हैं (काई-स्क्वायर 0.444, df 1, p>0.05)। इस प्रकार, नकद निकासी जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है। कोई भी व्यक्ति नकद निकाल सकता है, चाहे वह परिवार का कमाने वाला सदस्य हो या आश्रित सदस्य। इसलिए, नकद निकासी जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

निष्कर्ष

हमारा समाज एक साइबर-भौतिक समाज बन रहा है जो हमारे दैनिक जीवन के सभी पहलुओं में सूचना और संचार प्रौद्योगिकी (ICT) पर आधारित है, जिससे IT सुरक्षा की आवश्यकता मौलिक हो गई है। साइबर सुरक्षा की अमूर्त प्रकृति, सामाजिक-तकनीकी निर्भरता, साइबर सुरक्षा के खिलाफ लड़ाई का अस्पष्ट प्रभाव और विवादास्पद प्रकृति इसे उपयोगकर्ताओं के लिए एक उत्तेजक क्षेत्र बनाती है। अध्ययन से पता चलता है कि मात्रात्मक तरीकों का उद्देश्य साइबर सुरक्षा के बारे में जागरूकता पैदा करना है जिसके लिए भविष्य में उपयोग के लिए कुछ नियमों और विनियमों का पालन किया जाना चाहिए। व्यक्ति को हमेशा नियमों और विनियमों का पालन करना चाहिए।

संदर्भ

1. इकबाल स, नवाज द. साइबर सुरक्षा में उभरते रुझान और भविष्य की चुनौतियाँ: एक व्यापक समीक्षा. 2024.
2. नेग्रेया पीसी. उच्च प्रभाव वाली साइबर सुरक्षा घटनाओं का व्यापक विश्लेषण: केस स्टडीज़ और निहितार्थ. 2023. doi:10.13140/RG.2.2.17461.65763.
3. शुकुर फ, शुकुर स. IoT आधारित साइबर सुरक्षा खतरों का व्यापक विश्लेषण. जर्नल ऑफ एप्लाइड आर्टिफिशियल इंटेलिजेंस. 2023;4:12–21. doi:10.48185/jaai.v4i2.920.
4. अहमद अ, मौलाना र, यासिर म. डिजिटल परिवर्तन के युग में साइबर सुरक्षा चुनौतियाँ: सूचना प्रणालियों का एक व्यापक विश्लेषण. जर्नल इंफॉर्मेटिक, एजुकेशन एंड मैनेजमेंट (जेआईईएम). 2024;6:7–11. doi:10.61992/jiem.v6i1.57.
5. अकेलो ब. संगठनात्मक सूचना सुरक्षा खतरे: स्थिति और चुनौतियाँ. वर्ल्ड जर्नल ऑफ एडवांस्ड इंजीनियरिंग टेक्नोलॉजी एंड साइंसेज. 2023;11:148–162. doi:10.30574/wjaets.2024.11.1.0152.
6. ज़ेबारी द, असद र. साइबर सुरक्षा खतरे, भेद्यता, चुनौतियाँ और प्रस्तावित समाधान. एप्लाइड कंप्यूटिंग जर्नल. 2022:227–244. doi:10.52098/acj.202260.
7. रेहान अ. डिजिटल युग में साइबर सुरक्षा: खतरों का आकलन और बचाव को मजबूत करना. 2024. doi:10.13140/RG.2.2.31480.25607.
8. गोराई स, बेरा स, कुमार म. भारत में साइबर सुरक्षा के मुद्दे और चुनौतियाँ. कंप्यूटर विज्ञान, इंजीनियरिंग और सूचना प्रौद्योगिकी में वैज्ञानिक अनुसंधान के अंतर्राष्ट्रीय जर्नल. 2025;11:159–166. doi:10.32628/CSEIT251112.
9. अलसैफ़ उ, शहाथा अ. साइबर सुरक्षा खतरों के लिए दृष्टिकोण और कठिनाइयों का एक व्यापक विश्लेषण: लेख समीक्षा. मुस्तनसिरिया जर्नल ऑफ प्योर एंड एप्लाइड साइंसेज. 2024;2:126–139. doi:10.47831/mjpas.v2i4.164.
10. गोनी अ, जहाँगीर मउ, रॉय चौधरी र. साइबर सुरक्षा पर एक अध्ययन: वर्तमान खतरों का विश्लेषण, जटिलताओं को समझना और रोकथाम रणनीतियों को लागू करना. इंटरनेशनल जर्नल ऑफ रिसर्च एंड साइंटिफिक इनोवेशन. 2024;10:507–522. doi:10.51244/IJRSI.2023.1012039.
11. सिंह ह, खत्री अ, कौर अ. नवीनतम तकनीकों पर साइबर

सुरक्षा चुनौतियों और इसके उभरते रुझानों का एक अध्ययन. इंजीनियरिंग प्रौद्योगिकी और विज्ञान में आधुनिकीकरण का अंतर्राष्ट्रीय अनुसंधान जर्नल. 2023;5:1085–1090. doi:10.56726/IRJMETS47270.
12. फिशर ईए. साइबर सुरक्षा मुद्दे और चुनौतियाँ: संक्षेप में. 2015.
13. सलमान ह, अलसाजरी अ. साइबर सुरक्षा खतरों का विकास और प्रभावी सुरक्षा के लिए रणनीतियाँ: एक समीक्षा. SHIFRA. 2023:1–13. doi:10.70470/SHIFRA/2023/009.
14. लेस्माना द, अफिफुद्दीन म, एड्रियान्टो अ. डिजिटल आर्थिक परिवर्तन में चुनौतियाँ और साइबर सुरक्षा खतरे. इंटरनेशनल जर्नल ऑफ ह्यूमैनिटीज एजुकेशन एंड सोशल साइंसेज (IJHESS). 2023;2. doi:10.55227/ijhess.v2i6.515.
15. महतो स, साह र, सपकोटा स. साइबर सुरक्षा चुनौतियाँ और खतरे: डिजिटल दुनिया में जोखिम. विज्ञान, संचार और प्रौद्योगिकी में उन्नत अनुसंधान के अंतर्राष्ट्रीय जर्नल. 2024:651–655. doi:10.48175/IJARSCT-22497.

Creative Commons (CC) License
This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY 4.0) license. This license permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.