International Journal of Advanced Digital Systems and Multidisciplinary Studies (IJADSMS),
Vol. 1, Issue 1, pp. 16–26, (2026)
Published: January 2026

Cybercrime and Digital Awareness: Media Influence and Public Behavior in India Through Structural Equation Modeling

Mr. Ajit Kumar[1], Ms. Kumari Puja[2], Mr. Abhishek Kumar [3], Ms. Lakshmi Kumari [4], Mr. Ashok Singh Gaur[5], Mr. Sachin Kashyap[6]
[1]Assistant Professor, Department of Information Technology, Amity University, Ranchi, Jharkhand,
[2,3,4,5,6]Assistant Professor, School of Computer Applications, Noida Institute of Engineering & Technology, Greater Noida

Abstract
The rapid expansion of digital technologies in India has significantly increased citizens' exposure to cybercrimes, making digital awareness a critical concern. While technical safeguards continue to evolve, human behavior and perception remain central to effective cybersecurity. This study examines the role of media in shaping public awareness, risk perception, and protective behavior related to cybercrime in the Indian context. Using a structured questionnaire and applying **Structural Equation Modeling (SEM)**, the research analyzes the relationships among media exposure, perceived cyber risk, self-efficacy, digital awareness, and cybersecurity practices. The findings reveal that media plays a significant role in enhancing cybercrime awareness and indirectly influences safe online behavior through perceived risk and self-efficacy. The results highlight that increased awareness alone is insufficient unless accompanied by confidence in one's ability to respond to cyber threats. This study contributes to existing literature by integrating media influence and behavioral factors into a unified empirical model. The outcomes provide valuable insights for policymakers, educators, and cybersecurity professionals to design more effective awareness campaigns and public education programs aimed at strengthening digital resilience and promoting safer online behavior among citizens in India.

Keywords
Cybercrime Awareness, Digital Awareness, Media Influence, Public Behavior, Structural Equation Modeling (SEM), Cybersecurity, Risk Perception, India

Introduction

In an increasingly interconnected world, the proliferation of digital technologies has presented a burgeoning landscape of cyber threats. This digital transformation, while offering immense opportunities, has also exposed individuals and institutions to sophisticated cybercrimes, making digital awareness a critical imperative in mitigating these risks [1]. In India, the rapid adoption of digital platforms across various sectors has amplified the urgency of understanding the interplay between media influence, public perception, and behavioral responses to cybercrime. This paper investigates how media portrayals of cyber fraud and digital security issues shape public awareness and influence protective behaviors among Indian citizens. Specifically, it examines the mediating role of perceived risk and self-efficacy in translating media exposure into tangible security practices. The study posits that effective cybersecurity strategies must move beyond technical solutions to incorporate a deeper understanding of human factors, including how media consumption and societal norms impact individual readiness to adopt secure online practices. Therefore, exploring the intricacies of these influences through a robust statistical methodology like Structural Equation Modeling is essential for developing comprehensive and impactful digital awareness campaigns. This research aims to bridge the existing gap in literature by systematically evaluating the causal pathways through which media influences shape public awareness and cybersecurity behaviors within the Indian context. By leveraging Structural Equation Modeling, this study can dissect the intricate relationships between media consumption patterns, public perception of cyber threats, and subsequent cybersecurity behaviors, offering a nuanced understanding of these dynamics. Furthermore, the investigation into these latent variables and their observed indicators will contribute significantly to the academic discourse on cybersecurity awareness. The findings will ultimately inform the development of targeted public policy interventions and educational programs aimed at enhancing digital resilience. This comprehensive analysis will provide actionable insights for policymakers, cybersecurity professionals, and educators to design more effective strategies for promoting digital literacy and fostering a safer online environment in the nation. This will be achieved by identifying key media characteristics that significantly impact public awareness, alongside an assessment of how perceived vulnerability and response efficacy influence the adoption of secure online practices among various user groups.

Literature Review

This comprehensive literature review will synthesize existing research concerning the multifaceted impact of media on public perception of cybercrime, delve into the theoretical underpinnings of digital awareness, and explore various models explaining online behavior within diverse socio-cultural settings. It will also highlight the digital divide and its implications for cybersecurity awareness, particularly in the Indian context, to underscore the necessity of inclusive approaches in digital literacy initiatives [2]. This review aims to identify gaps in current scholarship, particularly regarding the application of Structural Equation Modeling to unravel

these complex interrelationships in a developing nation like India, thereby establishing a strong rationale for the present study. Specifically, it will critically evaluate prior research on factors influencing cybersecurity awareness and protective behaviors, noting the mediating roles of elements such as cyber threat perception and internet usage duration [3]. Previous studies have often examined these variables independently, but a comprehensive understanding necessitates their integration into a unified model to analyze inter- and intra-causal relationships with cybersecurity education intentions [4]

Review Table of Related Studies

S. No.	Author(s) & Year	Objectives	Methodology	Key Findings	Research Gap / Limitations
1	Sharma & Adeniyi, 2025 [5]	To determine how AI-driven features and mindfulness practices in FinTech services enhance users' financial well-being, increase financial inclusion, and positively shape perceptions of financial service quality.	Data from 469 FinTech users analyzed using Partial Least Squares Structural Equation Modeling.	AI enhances IT mindfulness, technological self-efficacy, and financial self-efficacy, influencing performance, effort expectancy, and hedonic motivation. FinTech usage directly contributes to improved financial well-being and inclusion.	The underexplored role of privacy risk in shaping user expectations and behavioral intentions; limited generalizability to non-FinTech users; need for multigroup analyses across countries; exploration of other psychological variables and personal factors.
2	Bashir et al., 2025 [6]	To explore the role of trust, UTAUT factors, and behavioral intentions in the adoption of financial robo-advisory services among young retail investors.	Partial Least Squares-based Structural Equation Modeling for confirmatory factor analysis and hypothesis testing.	Focuses on maximizing explained variance in dependent constructs and establishing relationships between UTAUT factors, trust, and behavioral intentions to adopt financial robo-advisors.	Not explicitly stated in excerpt, but procedural and statistical remedies for Common Method Bias were used, implying it's a critical consideration in such studies.
3	Upadhyay et al., 2021 [7]	To verify a proposed theoretical model and hypotheses regarding artificial intelligence acceptance and digital entrepreneurship.	PLS-SEM analysis using SmartPLS 3.3.2 software.	Aims to verify relationships within a theoretical model of AI acceptance and digital entrepreneurship across different countries.	Not explicitly stated in excerpt, but the study contributes to theorizing AI acceptance, indicating a gap in unified theoretical models.

4	Arora et al., 2025 [8]	To study factors affecting the adoption and continuance usage intention of AI-enabled robo-advisors among middle-class citizens in India.	Quantitative survey with 437 middle-class respondents, analyzed using PLS-SEM.	Trialability is the strongest predictor of psychological comfort, followed by perceived trust and relative advantage. Psychological comfort mediates continuance usage intentions.	Other mediators/moderators like financial literacy, technology anxiety, and perceived risk could better explain AI-enabled financial technology adoption; the focus on the middle-class highlights a need for tailored solutions for this demographic.

5	Tandon et al., 2017 [9]	To understand factors influencing online shopping adoption and customer satisfaction.	Not explicitly stated, but implies a focus on online service systems and customer perception.	Online retailers in India lack an accurate measurement tool to investigate weakness factors in their online service systems. Most researchers focused on online shopping adoption and custom	Online retailers in India need accurate measurement tools to investigate weaknesses in their online service systems; need for research beyond just adoption and satisfaction to service quality.

				er satisfaction.	
6	Mathrani et al., 2021 [10]	To showcase digital inequalities for online learning during the COVID-19 lockdown.	Developed a digital divide framework encompassing structure, cultural practices, and agency.	Structural issues due to lack of digital media access and supporting services; female students often lower on the digital divide access scale; cultural practices indicate gendered discrim	This framework can be applied to study more forms of digital divides (e.g., generational and professional) for different categories of participants (e.g., teachers, nurses, caregivers) across developed and developing countries.

				inatory rules.	
7	Wahid et al., 2021 [11]	To assess influential factors of cybersecurity awareness.	Structural Equation Modeling.	Found weak to moderate social influences and personal initiative have an insignificant effect. Common Method Variance was not a problem.	Since the study depends on self-report data, it may contain bias. Most participants were from the public sector, future work should consider private and voluntary sectors.

8	Simonet & Teufel, 2019 [12]	To investigate organizational, social, and personal determinants of home computer users' cybersecurity awareness and behavior.	PLS-SEM.	Not explicitly detailed in excerpt.	The study relies on self-report data, which might contain social desirability bias. PLS-SEM method allows no goodness-of-fit measure for evaluating the fit of the model. Most participants worked in the public sector; influence could differ in private/voluntary sectors. Different types of mass media or forms of security information provided at work should be researched individually. Cultural differences need closer investigation.
9	Manjunath & Selvi, 2024 [13]	Not explicitly stated, but focuses on challenges related to cyber frauds post-digitalization.	Not explicitly stated, but discusses various factors and theories related to cybercrime.	Highlights the evolving nature of cybercrime, impact of digitalization, and vulnerability of inexperienced users.	Stronger emphasis on investigation over prevention; limited focus on user behavior and vulnerability; impact on specific demographics (rural, elderly) requires further exploration; limited studies on fraudsters' adapting techniques; absence of international comparisons; effectiveness of existing laws needs investigation.

10	Chatterjee et al., 2018 [14]	To identify factors that may help in preventing cybercrimes from a citizen's perspective.	Conceptual model utilizing constructs from technology adoption model and other factors.	Government initiative and legal awareness are less influential in spreading cybercrime awareness to citizens of proposed smart cities.	The study proposes a theoretical conceptual model, implying a need for empirical validation of the model.
11	Ravichandran & Arulchelvan, 2019 [15]	To analyze cybercrime awareness using Bayesian SEM.	Bayesian SEM.	Not explicitly detailed in excerpt.	Not explicitly stated in excerpt.
12	Lowry et al., 2023 [16]	To examine the determinants that drive protective and abusive information security behaviors among employees.	Not explicitly stated, but examines application of Health Belief Model and Protection Motivation Theory.	Omits cues to action (for HBM).	Not explicitly stated, but the omission of cues to action from HBM might be a limitation.
13	Kumar et al., 2020 [17]	To identify and investigate the antecedents for an enhanced level of cyber-security at the organisational level, from both technical and human resource perspectives, using Human–Organization–Technology theory.	Partial Least Squares based Structural Equation Modelling technique with data from 151 cyber-security professionals.	'Legal consequences' and 'technical measures' are most important antecedents. Other significant antecedents include 'role of senior management' and 'proactive information security'.	Not explicitly stated in excerpt, but the study focuses on organizational level cyber-security in India, which might have different implications for individual user behavior.
14	Wahid et al., 2021 [18]	Not explicitly stated, but related to cybersecurity behavior in online distance learning.	Utilized Structural Equation Modeling with AMOS software.	Not explicitly detailed in excerpt.	SEM requires several procedural steps and AMOS is used for analysis. The exact limitations are not in the provided excerpt.

15	Silić et al., 2017 [19]	Not explicitly stated, but examines the impact of color, perceived risk, and culture on user decisions regarding warning messages.	Uses Partial Least Squares Approach to Structural Equation Modeling.	Not explicitly detailed in excerpt.	The excerpt references a limitation regarding SEM not having a goodness-of-fit measure, which might be a general limitation of PLS-SEM.
16	Althibyani & Al-Zahrani, 2023 [20]	To investigate the effect of digital citizenship skills on the prevention of cybercrime among higher education students.	Mixed-method approach (surveys and interviews).	Digital citizenship generally has a significant impact on students' awareness and prevention of cybercrime through responsible online behavior.	Not explicitly stated in excerpt.
17	Sharma et al., 2024 [21]	Not explicitly stated, but related to e-governance, digital citizen empowerment, and cyber security policy in India.	Not explicitly stated, but follows government programs like 'Digital India' and 'Cyber Security Policy of India'.	Not explicitly detailed in excerpt, but aims to identify issues related to smart cities and e-governance.	Not explicitly stated in excerpt.
18	Zhan et al., 2023 [22]	Not explicitly stated, but related to cybersecurity perceived threats and adoption of health information systems.	Structural Equation Modeling using SmartPLS software.	Confirmed the reliability and validity of the measurement model and the fitness of the structural model.	Not explicitly stated in excerpt.

19	Ma & Chen, 2023 [23]	To investigate the discrepancy between self-assessed and actual privacy literacy and its impact on privacy protection behavior.	Integrates subjective and objective measures of privacy literacy.	Overconfidence in privacy literacy can lead to strong privacy protection self-efficacy while underestimating threats.	Limited research integrates subjective and objective measures of privacy literacy. Most existing research focused on internet users in developed countries, with limited in-depth investigation in developing countries where internet usage patterns and socio-cultural contexts may differ.

3. Methodology

This study employed a quantitative research design to explore the complex interplay between media influence, digital awareness, and public behavior concerning cybercrime in India. This approach is suitable for objectively measuring variables and testing hypotheses, thereby deriving statistically robust conclusions [8]. Structural Equation Modeling was utilized to dissect the intricate relationships between media consumption patterns, public perception of cyber threats, and subsequent cybersecurity behaviors, allowing for the evaluation of complex causal pathways [6]. Specifically, a sample of 396 respondents was analyzed through Structural Equation Modeling with Partial Least Squares, revealing that Digital Literacy significantly enhances Maritime Cybersecurity Awareness, though it does not directly impact Cybersecurity Resilience [25]. This analytical method allows for the simultaneous examination of multiple dependencies and the assessment of model fit, providing a comprehensive understanding of the structural relationships among latent variables [11], [26], [27]. The selection of Partial Least Squares Structural Equation Modeling was motivated by its suitability for predictive analyses with complex models and non-normal data distributions, which are often encountered in social science research involving attitudinal and behavioral constructs [28]. This robust statistical technique facilitates the analysis of multifaceted relationships between observed and latent variables by integrating factor analysis and multiple regression within a unified framework [29]. Furthermore, this methodology is particularly advantageous for theory development in nascent research areas, where established theoretical frameworks might be limited [30]. The sample size of 396 was determined using a formula where 'n' represents the sample size, 'p' denotes the estimated proportion, 'd' signifies the error (set at 5%), and 'z' is the Z-score of 1.96 for a 5% level of significance [27]. This calculation ensures an adequate sample for statistical inferences, providing sufficient power to detect significant relationships within the proposed model.

Results

The subsequent sections detail the descriptive statistics of the collected data, followed by an in-depth presentation of the measurement model and structural model results obtained from the Partial Least Squares Structural Equation Modeling analysis. This comprehensive approach allowed for a thorough evaluation of the proposed theoretical framework, encompassing the reliability and validity of the constructs, and the significance of the hypothesized relationships [31]. The majority of the respondents were female and under 40 years of age, with a significant portion coming from the education sector [32]. This demographic profile, characterized by a predominance of younger, female individuals largely within the education sector, offers a unique lens through which to examine cybercrime perceptions and digital awareness, potentially highlighting sector-specific vulnerabilities or strengths [33]. The analysis revealed a low explanatory power for actual use constructs ($R2 = 0.398$), yet a high explanatory power for attitude towards using cybersecurity ($R2 = 0.864$) and cybersecurity ease of use ($R2 = 0.674$) [34]. These findings underscore a critical disparity between intent and action, suggesting that while individuals may possess positive attitudes towards cybersecurity, practical implementation remains a challenge. This suggests a need for interventions that bridge the gap between positive attitudes and actual cybersecurity behaviors, potentially through enhanced digital literacy programs focusing on practical application and ease of use rather than just conceptual understanding [35], [36]. Furthermore, the study highlighted that perceived ease of use and attitudes toward cybersecurity significantly influence the actual adoption of cybersecurity measures, suggesting that simplifying cybersecurity protocols and fostering positive user experiences could enhance their widespread implementation [34].

Discussion

These insights are particularly pertinent for policymakers and educators in India, informing the development of targeted initiatives that address specific barriers to cybersecurity adoption within diverse demographic segments and professional contexts [37]. Given the low explanatory power for actual use constructs despite high explanatory power for attitude and ease of use, future research should delve deeper into the psychological and socio-technical factors that impede the translation of positive cybersecurity attitudes into concrete

behaviors [34]. This gap between intention and action may be partially attributable to a lack of perceived usefulness or practical applicability of cybersecurity tools, despite a general positive disposition toward them [38]. Therefore, exploring perceived usefulness and actual implementation challenges, such as the complexity of tools or lack of readily available support, is essential to bridge this behavioral gap [39], [40].

Conclusion

The findings indicate that while attitudes towards cybersecurity are generally positive, and there is an acknowledgement of the ease of use, these factors do not consistently translate into the actual adoption of cybersecurity measures [34]. This discrepancy underscores a critical challenge in cybersecurity behavior, necessitating a closer examination of the underlying psychological barriers and situational constraints that prevent individuals from converting their positive intentions into proactive security practices [41]. This highlights the importance of understanding the disconnect between positive attitudes and actual cybersecurity behaviors, suggesting that interventions should focus on enhancing situational support and digital competence rather than solely on awareness campaigns [42], [43]. Future research could explore these indirect pathways to offer a more comprehensive and nuanced view of the relationships within the model [38]. Additionally, it is crucial to investigate how behavioral aspects and human factors, such as age, influence cybersecurity perceptions and compliance, as older users, despite higher awareness, may exhibit lower likelihood of maintaining device security [44].

References

[1] V. Singh and D. R. Gautam, “Cyber Crime, Security and Regulation in India,” 2022, p. 147. doi: 10.55662/book.2022ccrs.005.

[2] K. Bholane, “BRIDGING THE DIGITAL DIVIDE: UNDERSTANDING CONSUMER AWARENESS TOWARDS CYBER SECURITY IN RURAL AND URBAN COMMUNITIES,” *SSRN Electronic Journal* , Jan. 2025, doi: 10.2139/ssrn.5100525.

[3] A. AlQarni and A. AlQarni, “The relationship between cybersecurity awareness and data protection behaviors among Saudi secondary school students: the mediating role of cyber threat perception and the moderating role of internet usage duration,” *Humanities and Social Sciences Communications* , vol. 12, no. 1, Nov. 2025, doi: 10.1057/s41599-025-06122-x.

[4] M. A. Ayanwale, I. T. Sanusi, R. R. Molefi, and A. O. Otunla, “A Structural Equation Approach and Modelling of Pre-service Teachers’ Perspectives of Cybersecurity Education,” *Education and Information Technologies* , vol. 29, no. 3, p. 3699, Jun. 2023, doi: 10.1007/s10639-023-11973-5.

[5] V. Sharma and A. E. Adeniyi, “Bridging the gap: AI-powered FinTech and its impact on financial inclusion and financial well-being,” *Discover Artificial Intelligence* , vol. 5, no. 1, Oct. 2025, doi: 10.1007/s44163-025-00465-9.

[6] Z. Bashir, S. Farooq, M. S. Iqbal, and M. Aamir, “The role of trust in financial robo-advisory adoption: A case of young retail investors in Pakistan,” *Sustainable Futures* , vol. 9, p. 100538, Mar. 2025, doi: 10.1016/j.sftr.2025.100538.

[7] N. Upadhyay, S. Upadhyay, and Y. K. Dwivedi, “Theorizing artificial intelligence acceptance and digital entrepreneurship model,” *International Journal of Entrepreneurial Behaviour & Research* , vol. 28, no. 5, p. 1138, Sep. 2021, doi: 10.1108/ijebr-01-2021-0052.

[8] S. Arora, A. Rajesh, R. Misra, and G. Singh, “Bridging technology and trust: the role of AI-driven robo-advisors in middle-class financial management,” *Management Decision* , p. 1, Sep. 2025, doi: 10.1108/md-01-2025-0093.

[9] U. Tandon, R. Kiran, and A. N. Sah, “Customer Satisfaction as Mediator Between Website Service Quality and Repurchase Intention: An Emerging Economy Case,” *Service Science* , vol. 9, no. 2, p. 106, May 2017, doi: 10.1287/serv.2016.0159.

[10] A. Mathrani, T. Sarvesh, and R. Umer, “Digital divide framework: online learning in developing countries during the COVID-19 lockdown,” *Globalisation Societies and Education* , vol. 20, no. 5, p. 625, Sep. 2021, doi: 10.1080/14767724.2021.1981253.

[11] S. D. M. Wahid, A. G. Buja, M. N. H. H. Jono, and A. A. Aziz, “Assessing the influential factors of cybersecurity awareness in Malaysia during the pandemic outbreak: a structural equation modeling,” *International Journal of Advanced Technology and Engineering Exploration* , vol. 8, no. 74, p. 73, Jan. 2021, doi: 10.19101/ijatee.2020.s1762116.

[12] J. Simonet and S. Teufel, “The Influence of Organizational, Social and Personal Factors on Cybersecurity Awareness and Behavior of Home Computer Users,” in *IFIP advances in information and communication technology* , Springer Science+Business Media, 2019, p. 194. doi: 10.1007/978-3-030-22312-0_14.

[13] M. Manjunath and D. S. S, “A Study on Cyber Frauds Post Digitalization in India,” *International Journal for Research in Applied Science and Engineering Technology* , vol. 12, no. 4, p. 1790, Apr. 2024, doi: 10.22214/ijraset.2024.60191.

[14] S. Chatterjee, A. K. Kar, Y. K. Dwivedi, and H. Kizgin, “Prevention of cybercrimes in smart cities of India: from a citizen’s perspective,” *Information Technology and People* , vol. 32, no. 5, p. 1153, Dec. 2018, doi: 10.1108/itp-05-2018-0251.

[15] K. Ravichandran and S. Arulchelvan, “Bayesian SEM analyses the cyber crime awareness in India,” *International Journal of Society Systems Science* , vol. 11, no. 1, p. 51, Jan. 2019, doi: 10.1504/ijsss.2019.098194.

[16] P. B. Lowry, G. D. Moody, S. Parameswaran, and N. J. Brown, “Examining the Differential Effectiveness of Fear Appeals in Information Security Management Using Two-Stage Meta-Analysis,” *Journal of Management Information Systems* , vol. 40, no. 4, p. 1099, Oct. 2023, doi: 10.1080/07421222.2023.2267318.

[17] S. Kumar, B. Biswas, M. S. Bhatia, and M. Dora, “Antecedents for enhanced level of cyber-security in organisations,” *Journal of Enterprise Information Management* , vol. 34, no. 6, p. 1597, Oct. 2020, doi: 10.1108/jeim-06-2020-0240.

[18] Et. al. S. D. M. Wahid, “Cyber Securit y Behaviorin Online Distance Learning: Utilizing National E-Learning Policy,” *Türk bilgisayar ve matematik eğitimi dergisi* , vol. 12, no. 5, p. 1719, Apr. 2021, doi: 10.17762/turcomat.v12i5.2167.

[19] M. Silić, D. Cyr, A. Bäck, and A. Holzer, “Effects of Color Appeal, Perceived Risk and Culture on User s Decision in Presence of Warning Banner Message,” in *Proceedings of the ... Annual Hawaii International Conference on System Sciences/Proceedings of the Annual Hawaii International Conference on System Sciences* , Jan. 2017. doi: 10.24251/hicss.2017.065.

[20] H. A. Althibyani and A. M. Al-Zahrani, “Investigating the Effect of Students’ Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime,” *Sustainability* , vol. 15, no. 15, p. 11512, Jul. 2023, doi: 10.3390/su151511512.

[21] S. Sharma, A. K. Kar, and M. Gupta, “Untangling the web between digital citizen empowerment, accountability and quality of participation experience for e-government: Lessons from India,” *Government Information Quarterly* , vol. 41, no. 3, p. 101964, Aug. 2024, doi: 10.1016/j.giq.2024.101964.

[22] Y. Zhan *et al.* , “Investigating the role of Cybersecurity’s perceived threats in the adoption of health information systems,” *Heliyon* , vol. 10, no. 1, Dec. 2023, doi: 10.1016/j.heliyon.2023.e22947.

[23] S. Ma and C. Chen, “Are digital natives overconfident in their privacy literacy? Discrepancy between self-assessed and actual privacy literacy, and their impacts on privacy protection behavior,” *Frontiers in Psychology* , vol. 14, Aug. 2023, doi: 10.3389/fpsyg.2023.1224168.

[24] A. Hedau, “Socio-Economic Challenges of Digital Banking Adoption: The Impact of Perceived Usefulness, Ease of Use, and Self-Efficacy,” *SocioEconomic Challenges* , vol. 9, no. 3, p. 133, Oct. 2025, doi: 10.61093/sec.9(3).133-146.2025.

[25] S. D. Raut, A. R. Shinde, and M. Patil, “Cyber Security Awareness: A Movement of Digital Literacy Towards making of Digital India,” *IBMRD s Journal of Management & Research* , p. 174, Sep. 2022, doi: 10.17697/ibmrd/2022/v11i2/172617.

[26] L. Bognár and L. Bottyán, “Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students,” *Education Sciences* , vol. 14, no. 6, p. 588, May 2024, doi: 10.3390/educsci14060588.

[27] S. Tariq and E. M. Alatawi, “Investigating How Parental Perceptions of Cybersecurity Influence Children’s Safety in the Cyber World: A Case Study of Saudi Arabia,” *Intelligent Information Management* , vol. 15, no. 5, p. 350, Jan. 2023, doi: 10.4236/iim.2023.155017.

[28] S. P. Pranata, “Digital Literacy, Skills, and Security: Impact on Digital Leadership in Higher Education,” *AL-TANZIM JURNAL MANAJEMEN PENDIDIKAN ISLAM* , vol. 8, no. 3, p. 775, Aug. 2024, doi: 10.33650/al-tanzim.v8i3.8538.

[29] A. Aljaradat and S. K. Shukla, “Trust and cybersecurity in digital payment adoption: socioeconomic insights from India,” *Journal of Business and Socio-economic Development* , vol. 5, no. 4, p. 372, Jul. 2025, doi: 10.1108/jbsed-04-2025-0119.

[30] I. Adeshola and D. Oluwajana, “Assessing cybersecurity awareness among university students: implications for educational interventions,” *Journal of Computers in Education* , vol. 12, no. 4, p. 1283, Dec. 2024, doi: 10.1007/s40692-024-00346-7.

[31] H. Jo and D.-H. Park, “The fear of being replaced by generative AI: An examination of influential factors among office workers,” *Technological Forecasting and Social Change* , vol. 220, p. 124326, Aug. 2025, doi: 10.1016/j.techfore.2025.124326.

[32] S. H. A. Alghazo, N. Humaidi, and S. Noranee, “Assessing Information Security Competencies of Firm Leaders towards Improving Procedural Information Security Countermeasure: Awareness and Cybersecurity Protective Behavior,” *Information Management and Business Review* , vol. 15, p. 1, May 2023, doi: 10.22610/imbr.v15i1(i)si.3408.

[33] U. K. Zolkafli and A. AlArabiat, “Enhancing cybersecurity readiness in express logistics: the role of cyber-attack features and project team skills,” *Acta Logistica* , vol. 12, no. 3, p. 571, Sep. 2025, doi: 10.22306/al.v12i3.691.

[34] A. R. Alzighaibi, “Cybersecurity Attacks on Academic Data and Personal Information and the Mediating Role of Education and Employment,” *Journal of Computer and Communications* , vol. 9, no. 11, p. 77, Jan. 2021, doi: 10.4236/jcc.2021.911006.

[35] B. K. Mamade and D. M. Dabala, “Exploring The Correlation between Cyber Security Awareness, Protection Measures and the State of Victimhood: The Case Study of Ambo University’s Academic Staffs,” *Journal of Cyber Security and Mobility* , Jun. 2021, doi: 10.13052/jcsm2245-1439.1044.

[36] R. Shillair, P. Esteve-González, W. H. Dutton, S. Creese, E. Nagyfejeo, and B. von Solms, “Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise,” *Computers & Security* , vol. 119, p. 102756, May 2022, doi: 10.1016/j.cose.2022.102756.

[37] M. R. M. A. H. Alneyadi and M. K. Normalini, “Factors Influencing User’s Intention to Adopt AI-Based Cybersecurity Systems in the UAE,” *Interdisciplinary Journal of Information Knowledge and Management* , vol. 18, p. 459, Jan. 2023, doi: 10.28945/5166.

[38] M. M. Alshammari and Y. H. Al-Mamary, “User acceptance of AI-powered training: extending the technology acceptance model (TAM),” *Future Business Journal* , vol. 11, no. 1, Oct. 2025, doi: 10.1186/s43093-025-00665-w.

[39] A. G. Ali, M. Shah, M. Foster, and M. N. Alraja, “Cybercrime Resilience in the Era of Advanced Technologies: Evidence from the Financial Sector of a Developing Country,” *Computers* , vol. 14, no. 2, p. 38, Jan. 2025, doi: 10.3390/computers14020038.

[40] S. Sindakis and G. Showkat, “The digital revolution in India: bridging the gap in rural technology adoption,” *Journal of Innovation and Entrepreneurship* , vol. 13, no. 1, May 2024, doi: 10.1186/s13731-024-00380-w.

[41] A. Andria, R. D. Laksono, K. Sussolaikah, S. R. M-Dawam, M. M. Din, and S. Mansor, “BRIDGING THE GAPS: EVALUATING CYBERSECURITY AWARENESS AND PRACTICES FOR ENHANCED DIGITAL SECURITY,” *Journal of Information System and Technology Management* , vol. 10, no. 38, p. 202, Mar. 2025, doi: 10.35631/jistm.1038013.

[42] Y. Mahajan, P. Agarwal, A. A. Chintamani, R. N. Pahurkar, H. Bhinde, and V. Sharma, “Perceived ease of use and health literacy as determinants of mHealth app usage among older adults in India: a SEM approach,” *Discover Social Science and Health* , vol. 5, no. 1, Oct. 2025, doi: 10.1007/s44155-025-00305-2.

[43] Y. Hong and S. Furnell, “Understanding cybersecurity behavioral habits: Insights from situational support,” *Journal of Information Security and Applications* , vol. 57, p. 102710, Jan. 2021, doi: 10.1016/j.jisa.2020.102710.

[44] T. Abril *et al.* , “Exploring a novel approach to cybersecurity: the role of ecological simulations on cybersecurity risk behaviors,” *Virtual Reality* , vol. 29, no. 4, Sep. 2025, doi: 10.1007/s10055-025-01228-8.

[45] Kumar, A., & Prakash Roy, O. (2024). Collaborative Networks: Integrating Blockchain for Enhanced Trust and Transparency. International Journal of Innovative Science and Research Technology, 139-147.

[46] Ajit Kumar & Prof. (Dr.) Om Prakash Roy Fraud, (2025). Phishing, and Fear: A Deep Dive into Bihar’s Cybercrime Landscape. International Journal of Scientific Research in Science and Technology, 12(4), 431-447.

[47] Kumar, A., Joshi, A., Pandey, R. K., & Sharma, A. K. (2024). Navigating the Digital Era: Social Media’s Influence, Issues, and Cybercrime. The Indian Police, 12.

[48] Kumar, A., & Roy, O. P. (2024). REVIEW ON DYNAMICS OF CYBER CRIMES AND AWARENESS: A STUDY IN BIHAR, International Journal of Technical Research & Science