Asian And Pacific Economic Review
ISSN: 1000-6052

DIGITAL SECURITY BEHAVIOR AND CYBERSECURITY AWARENESS AMONG GENERATION Z STUDENTS

Ms. Rinal Chodvadiya
Assistant Professor, S. R. Luthra Institute of Management,
Sarvajanik University, Surat
Dr. Jayshree Siddhpuria
Assistant Professor, S. R. Luthra Institute of Management,
Sarvajanik University, Surat
Dr. Drashti Shah
Assistant Professor, S. R. Luthra Institute of Management,
Sarvajanik University, Surat
Ms. Krishna Gandhi
Assistant Professor, S. R. Luthra Institute of Management,
Sarvajanik University, Surat

https://doi.org/10.5281/zenodo.19710565

ABSTRACT:
The boom of digital technologies and the usage of the internet have increased individuals' cybersecurity threats. Digital platforms such as social media, online learning systems, and mobile applications are widely used by Generation Z students, which creates cyber risks. This study evaluates the factors affecting cybersecurity awareness among Generation Z students by analyzing the role of password security practices, browser security knowledge, and social media security awareness.
A quantitative research design was acquired, and primary data were collected from 323 undergraduate and postgraduate students using a structured questionnaire based on a five-point Likert scale. Data analysis was done through Partial Least Squares Structural Equation Modeling (PLS-SEM).
The findings indicate that password security, browser security knowledge, and social media security awareness significantly influence students' cybersecurity awareness. Social media security awareness and password security have stronger effects than the other factors. The study emphasizes the necessity for educational institutions to strengthen cybersecurity awareness and promote safe digital practices among students.
Keywords: Cybersecurity awareness, Generation Z, password security, browser security knowledge, social media security awareness, PLS-SEM.

1. INTRODUCTION

In the current era, rapid growth in internet use and digital technologies has positively transformed the way individuals communicate, access information, and enhance daily activities (Darwish &

Lakhtaria, 2011). Increasing the dependency on digital platforms such as social media, quick commerce, cloud computing, and online banking has led to the exchange of vast amounts of digital data (Wewege & Thomsett, 2020). This improvement increases connectivity and operational efficiency. But each coin has two sides, so simultaneously increase awareness regarding cybersecurity threats and critical concerns in the contemporary digital ecosystem (Qudus, 2025).

In recent times, the digital landscape has witnessed a marked escalation in the prevalence and complexity of cyber threats such as phishing schemes, malware intrusions, identity theft, and large-scale data breaches (Mallick & Nath, 2024). These cyberattacks not only affect organizations and governments but also individual internet users who mistakenly disclose sensitive information online (Mallinder & Drabwell, 2014). Therefore, cybersecurity awareness has become an essential factor in minimizing cyber risks and protecting digital assets.

Generation Z has been nurtured and grown up in a highly digital environment and is one of the most prominent groups of internet users. They extensively consume digital technologies for communication, education, entertainment, and financial activities (Alruthaya & Lokuge, 2021). Their high level of digital engagement usage also increases cybersecurity risks when they do not follow safe online practices (Khan et al., 2023). Social networking platforms are the primary medium for interaction, which involves the sharing of personal information, location data, and other personal details, therefore increasing vulnerability to privacy breaches, identity theft, and online fraud (Soomro & Hussain, 2019).

Therefore, research focuses on the gap between cybersecurity awareness and actual online practices with Gen Z (Ahamed et al, 2026). In real life, many students have minimal knowledge of cybersecurity concepts and fail to implement security measures in their daily lives (Pawlowski & Jung, 2015). Effective cybersecurity implementations not only require awareness but also the application of practices in real life, such as strong password management, secure browsing habits, and proper use of social media (Hennig, 2018). Despite the growing body of literature, few studies comprehensively examine multiple dimensions of cybersecurity behavior—such as password security practices, browser security knowledge, and social media security awareness—within a framework (Almansoori et al., 2023). Based on past studies, these behavioral factors collectively influence cybersecurity awareness among university students.

Therefore, this study aims to identify the key factors affecting cybersecurity awareness among Gen Z students by examining dimensions such as password security practices, browser security knowledge, and social media security awareness. The findings are expected to provide educators and policymakers with valuable insights for developing targeted awareness programs that promote safer digital behavior in educational environments.

2. LITERATURE REVIEW

The growing number of active users of digital platforms, particularly among Generation Z, has raised important concerns about information security behavior and cybersecurity awareness. As a result, scholarly research in this context is expanding for different users and cultures and in different safety environments. The Theory of Planned Behavior proposed the conceptual basis of

this research domain. The Theory of Planned Behavior (TPB), developed by Ajzen (1991), suggests that behavioral intentions are influenced by attitudes, social pressure, and ease of performance.

In the context of cybersecurity, Bada et al. (2015) argue that scaring people into being cautious increases fear and creates uncertainty about the act. Instead, awareness programs should go beyond just giving information. User awareness, their knowledge, and behavioral practices play a significant role in security, whereas awareness programs target safe digital behavior. Overall, the effectiveness of cybersecurity is highest when it is customized as per different cultural users, well-structured, practical, and continuously supported.

In today's digital era, technology has become a significant part of academic life. Students rely on cloud platforms, mobile devices, and online learning systems, which have increased cybersecurity risk within educational institutions. As we move towards a paperless and environmentally conscious society, universities handle a large volume of sensitive academic and personal data. This makes them highly attractive targets for cyberattacks, highlighting the growing need for stronger cybersecurity awareness and protective measures. The literature (Slusky & Partow-Navid, 2012; Parsons et al., 2017) suggests that students' cybersecurity awareness is influenced by password management practices, browser security knowledge, social media behavior, and overall knowledge of staying digitally secure.

Password Security

Password security refers to the ways individuals protect their online accounts by using strong, secure passwords. Even though authentication mechanisms are commonly used for password protection, many users still follow weak practices. Simple passwords, sharing passwords with others, or using the same password across multiple accounts increase the risk of unauthorized access and cyberattacks (Florençio & Herley, 2007; Gaw & Felten, 2006).

Studies have shown that insecure behavior is often driven by the need to memorize multiple complex passwords. As a result, users often save passwords in their browsers or store them in the system. Reusing passwords across platforms makes accounts more vulnerable to security breaches. Cybersecurity attackers often exploit these users' weaknesses through automated password-guessing and brute-force attacks to gain unauthorized access (Gaw & Felten, 2006).

Improving password management practices, such as creating and updating strong and unique passwords and avoiding reuse, significantly promotes cybersecurity awareness and safer online behavior. Password security is recognized as a key factor influencing students' overall cybersecurity awareness (Parsons et al., 2017).

H1: Password security positively influences cybersecurity awareness among Gen Z students.

Browser Security Knowledge

Browser security knowledge refers to individuals' awareness and understanding of safe web browsing practices. Such practices protect against threats like phishing attacks, malicious websites, and malware. Web browsers are the primary gateway for accessing online services, and they have often been targeted by cybercriminals. Unsafe browsing practices make it easier for attackers to steal sensitive information or install harmful software (Vishwanath et al., 2018).

Research suggests that following secure browsing habits, such as avoiding suspicious links and not installing unknown extensions, can significantly reduce cybersecurity risks (Krombholz et al., 2015). Lack of sufficient awareness of these practices amongst students exposes them to various online threats. Hence, improving browser security knowledge is essential to enhancing cybersecurity and promoting safe online behavior among internet users.

H2: Knowledge of browser security positively influences cybersecurity awareness among Gen Z students.

Social Media Security Awareness

Social media platforms are a primary source of sharing information and communication among Generation Z. These platforms allow users to create online content, share opinions, and post personal information. Excessive use of social media has raised privacy and security concerns (Boyd & Ellison, 2007).

Sharing location, photos, and personal information is very common in today's digital era. Sharing personal information on social networking sites increases the risk of identity theft, cyberstalking, and online fraud. Many users accept friend requests from unknown individuals or share sensitive information without fully understanding the potential security risks (Debatin et al., 2009). There was much research indicating that greater awareness of privacy settings, security controls, and reporting mechanisms on social media is associated with better protection against online threats. Therefore, social media awareness plays a positive role in strengthening overall cybersecurity awareness. (Tufekci, 2008; Vishwanath et al., 2018).

H3: Social media security awareness positively influences cybersecurity awareness among Gen Z students.

Cybersecurity Awareness

Cybersecurity awareness means a person understands the pros and cons and is aware of protective measures for digital information and online activities. This includes knowledge of common threats such as phishing attacks, malware, and unsafe online practices, as well as awareness of security tools and proper protocols (Parsons et al., 2017). Many security breaches are caused by human error rather than technical vulnerabilities. Much research indicates that people with greater knowledge are more likely to adopt safe online behavior and follow protocols (Kruger & Kearney, 2006).

In educational institutions, spread cybersecurity awareness, as students use it very frequently for both academic and personal purposes. To reduce cybersecurity risks in academia, people should increase students' awareness of cyber threats and security practices.

3. RESEARCH METHODOLOGY

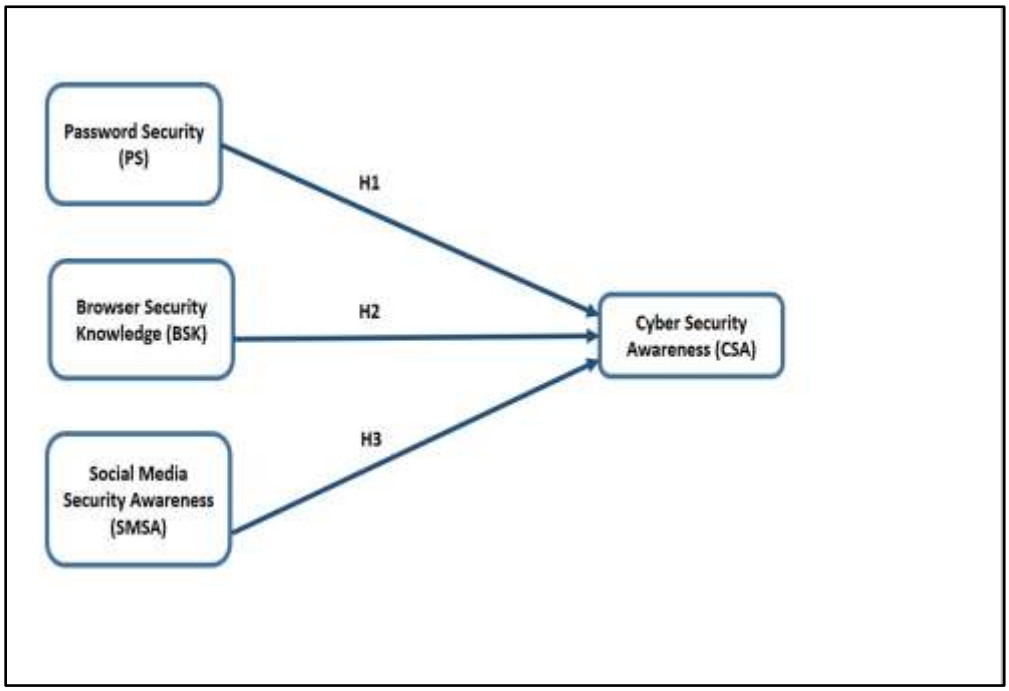
The study employs a quantitative, descriptive research design and conducts a systematic examination of cybersecurity awareness among Generation Z students. This research assesses the relationships among variables and tests associated hypotheses through statistical analysis. In this study, the antecedents include password security practices, browser security knowledge, and social media awareness, reflecting students' overall cybersecurity awareness.

The ideal sample for this study is adult respondents who are comfortable with technology and well-informed about cybersecurity. For this study, we will target Generation Z students who enrolled in undergraduate and postgraduate programs at South Gujarat University. This group is appropriate for examining cybersecurity awareness and the proper use of digital technologies, such as smartphones, social media platforms, and online services, for personal and professional purposes. The adult respondent is better able to evaluate security, passwords, phishing, and other features offered by social media.

The questionnaire was sent to the students using the institute's group administrative approach in December 2025. The total population of management graduate and postgraduate students: 1000 questionnaires were distributed to the target population using the group administration approach. After two weeks, a follow-up reminder email was sent. A total of 420 responses were returned, but only 323 were considered valid in the study, excluding incomplete responses and extreme outliers.

Proposed Research Model

Figure 1: Proposed Research Model



The constructs used in this study were adapted from previously validated cybersecurity scales. Scales are adopted from Mohammed A. Alqahtani's 2022 research: six items measure password security, four items measure browser security, and five items measure social media activities. Four items measure cybersecurity, which are adopted from Nashrawan Taha & Laila Dahabiyeh (2020). As these scales were initially developed in another cultural context, they were cautiously revised and reproduced. To do the same, three professionals dealing in sustainable products and two professors teaching marketing were given the questionnaire to evaluate the content and face validity. They also assessed each item for specificity, representativeness, and precision. The suggestions they gave were objectively incorporated. Responses on all the scale items were recorded on a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). This

questionnaire has two sections. The first section gathered a demographic profile, and the second section comprised measurement items that assess key cybersecurity-related constructs.

4. RESULTS AND DISCUSSION

4.1 Descriptive Statistics

Out of 323 respondents, 60.4 percent were female, and 39.4 percent were male. The median age of the respondents was 22 years because many participants were 18–24 years old. This age group indicates that the sample largely represents Generation Z students who are highly active in digital environments. The majority of respondents were management students (57.6 percent); 30.3 percent were commerce students; 7.1 percent were engineering students; and the remaining were from other educational backgrounds. Regarding digital media, the majority of users use smartphones and laptops daily, while very few use desktops or tablets.

4.2 Measurement Model Assessment

Purification of Scales

Churchill (1979) suggested that removing items with corrected-item-total-correlation (CITC) scores is essential before conducting exploratory factor analysis. Cristobal et al. (2007) proposed a cut-off point of 0.30 to remove an item. Based on the analysis, it was found that the CITC scores for all items were above the cut-off point, so no items were removed at this stage.

Indicator Reliability (Factor Loadings)

The systematic evaluation of the measurement model includes subcomponents: internal consistency reliability, convergent validity, and discriminant validity. Outer loading measures the strength and significance of the relationship between observed variables and their underlying constructs. If the loading value exceeds 0.7, it indicates strong relationships and a significance level of $p < 0.05$.

Table 1: Outer Loading

		Outer loadings
Knowledge of Browser Security	The web browser should be updated regularly	0.822
Knowledge of Browser Security	I should avoid installing extensions from third-party websites	0.810
Knowledge of Browser Security	I must check the security settings and configurations of the web browser periodically	0.880
Knowledge of Browser Security	I must check the browser history and find suspicious activities	0.883
Cyber Security	I am aware of the information security concept.	0.813
Cyber Security	I'm aware of the Malware concept	0.841
Cyber Security	I'm aware of the Antivirus software concept	0.843

Cyber Security	I know that using the https protocol is more secure than using the http protocol in the URL.	0.779
Password Security	Passwords are made up of 12 letters and a combination of letters, digits, or signs.	0.776
Password Security	I must change my password periodically	0.783
Password Security	I can use previously used passwords	0.703
Password Security	I use one strong password for across different websites and accounts	0.763
Password Security	It is annoying to have a long and strong password for each website and account	0.784
Password Security	I often share my passwords with others	0.764
Knowledge Social Network Platforms	It is acceptable to post personal pictures on social media	0.777
Knowledge Social Network Platforms	It is ok to accept friend requests from strangers	0.834
Knowledge Social Network Platforms	There is no problem with sharing my current location publicly on social media	0.834
Knowledge Social Network Platforms	There is no problem with adding all personal information like date of birth, current job, etc.	0.883
Knowledge Social Network Platforms	I know how to report any threat or suspicious activity on social media	0.849

Overall, all the indicator loadings are above the threshold of 0.70, indicating the strong relationship between the observed variables and their constructs. The loading values exceed 0.70; it also supports the convergent validity of the measurement model, suggesting that the indicators adequately represent their intended constructs.

Internal Consistency Reliability

Indicators of internal consistency are composite reliability (CR) and Cronbach's alpha. Values above 0.7 are considered acceptable for both CR and Cronbach's alpha. Commonly accepted standards for interpreting internal consistency using Cronbach's alpha are >0.90 = Excellent, <0.90 and >= 0.80 = Excellent, <0.80 and >= 0.70 = Good, <0.70 and >= 0.60 = Acceptable, <0.60 and >= 0.50 = Poor, and <0.50 = Not acceptable (Cronbach, 1951; Nunnally, 1978). Table 1 below presents Cronbach's alpha values for each item, ranging from 0.631 (password security) to 0.872 (browser security knowledge). So, it represents an acceptable level of reliability for each construct. Average variance extracted (AVE) measures the variance captured by the latent construct relative to the variance due to measurement error. AVE values above 0.5 are typically considered satisfactory. So, it represents an acceptable level of reliability for each construct.

Table 2: Internal Consistency, Reliability, and Convergent Validity

	Cronbach's alpha	**Composite reliability (rho_a)**	**Composite reliability (rho_c)**	**Average variance extracted (AVE)**
Browser Security Knowledge	0.872	0.886	0.912	0.722
Cyber Security Awareness	0.837	0.840	0.891	0.672
Password Security	0.731	0.652	0.725	0.524
Social Media Security Awareness	0.739	0.690	0.698	0.533

Discriminant Validity

Discriminant validity indicates the extent to which each latent construct differs from the others in the model. This measure compares each construct's square root AVE with the correlations among constructs. If AVE is greater than its correlation with other constructs, discriminant validity is supported. Table 3 below counts the values per the Fornell-Larcker criteria; discriminant validity was established in the model, as the AVEs for all constructs were greater than their correlations with other constructs. Another measure of discriminant validity was also measured using the HTMT ratio, which was also lower than 0.85 (Hair et al., 2017)

Table 3: Fornell-Larcker Criterion for Discriminant Validity

	Browser Security Knowledge	**Cyber Security Awareness**	**Password Security**	**Social Media Security Awareness**
Browser Security Knowledge	0.849			
Cyber Security Awareness	0.297	0.819		
Password Security	0.413	0.453	0.569	
Social Media Security Awareness	0.117	0.418	0.312	0.577

Table 4: HTMT Ratio for Discriminant Validity

	Heterotrait-monotrait ratio (HTMT)
Cybersecurity Awareness <-> Browser Security Knowledge	0.348
Password Security <-> Browser Security Knowledge	0.505
Password Security <-> Cyber Security Awareness	0.522
Social Media Security Awareness <-> Browser Security Knowledge	0.428
Social Media Security Awareness <-> Cyber Security Awareness	0.351

Social Media Security Awareness <-> Password Security	0.477

4.3 Model Fit Assessment (SMART PLS)

Table 5 shows the model fit indices, where the overall model is within the acceptable limits suggested by Bagozzi and Yi (1988), Hair et al. (1998), Baumgartner and Homburg (1996), and Doll et al. (1994).

Table 5: Model fit

Model Fit Index	Threshold	Saturated Model	Estimated Model	Bootstrap HI95 / HI99	Result
SRMR	<0.08 Good, <0.10 Acceptable	0.060	0.060	—	Good Fit
d_ULS	Original < HI95	0.692	0.692	0.803 / 0.867	Supported
d_G	Original < HI95	0.157	0.157	0.212 / 0.227	Supported
Chi-square	Lower value indicates better fit	130.241	130.241	—	Acceptable
NFI	≥0.90 Good, ≥0.80 Acceptable	0.808	0.808	—	Acceptable

The standardized root mean square residual (SRMR) was 0.060, below the recommended threshold of 0.08, indicating a good model fit and negligible differences between observed and predicted correlations (Hair et al., 2010). In model discrepancy measures, d ULS (0.692) and d G (0.157) measure the difference between the empirical and model-implied covariance matrices; lower values indicate better model fit. The chi-square value of 130.241 is relatively high, which suggests an acceptable model fit. Another NFI value, 0.808, is below the 0.90 threshold, indicating a good model fit.

4.4 Structural Model Assessment

Structural model assessment includes collinearity diagnostics, coefficient of determination (R^2), effect size (f^2), and path coefficients. A VIF value measures collinearity; values above 3 indicate a potential collinearity problem. VIF values for all constructs are 1.206, 1.317, and 1.108, which are below the threshold value. So, the model does not have collinearity issues. Variance explained by the endogenous variable through the exogenous variable, which is indicated by the R^2 value. The R^2 value for cybersecurity awareness is 0.306, indicating that browser security knowledge, password security, and social media security awareness together explain 30.6 percent of the

variance in cybersecurity awareness among Gen Z students. Evaluation of effect size (f^2) permits the researcher to detect the impact of each independent variable on the dependent variable.

Table 6: Effect Size (f^2)

Relationship	**f-square**	**Effect Size**
Browser Security Knowledge → Cyber Security Awareness	0.022	Small Effect
Password Security → Cyber Security Awareness	0.099	Small Effect
Social Media Security Awareness → Cyber Security Awareness	0.123	Medium Effect

Path Coefficient Analysis (Hypothesis Testing)

Table 7: Path coefficient significance

Hypothesis	**Relationship**	**Path coefficient values**	**P Values**	**Results**
H1	Password Security → Cyber Security Awareness	0.301	0.000	Supported
H2	Browser Security Knowledge → Cyber Security Awareness	0.136	0.011	Supported
H3	Social Media Security Awareness → Cyber Security Awareness	0.308	0.000	Supported

Note: *Significant at 1 percent*

The path analysis results indicate that H1 **($\beta = 0.301$, $p < 0.01$) shows** a significant positive relationship between password security and cybersecurity awareness among students. Students who create strong passwords and regularly update them are more likely to demonstrate higher cyber awareness. **H2 ($\beta = 0.136$, $p < 0.05$) indicates a significant positive** relationship between browser security knowledge and cybersecurity awareness. Students have better knowledge of secure browser practices, such as identifying suspicious websites and avoiding unsafe downloads, and greater awareness of cybersecurity risks. Additionally, H3 **($\beta = 0.308$, $p < 0.01$)** indicates a significant positive relationship between social media security awareness and cybersecurity awareness. Students who understand privacy settings, suspicious links, and potential threats on social media platforms exhibit stronger cybersecurity awareness.

5. CONCLUSIONS

This study investigates the factors that affect cybersecurity awareness among Generation Z students by analyzing the roles of password security practices, browser security knowledge, and social media security awareness. Partial Least Squares Structural Equation Modeling (PLS-SEM) was applied . The result suggests that all three factors significantly affect students' overall cybersecurity awareness. In that context, social media security awareness and password security practices show stronger effects. Conversely, knowledge of browser security shows a comparatively smaller but still significant influence.

The results suggest that students who practice secure password practices, are aware of safe browsing behavior, and understand the risks associated with social media platforms exhibit higher levels of cybersecurity awareness. These results emphasize the importance of being responsible in improving cybersecurity awareness among Generation Z users.

The structural model accounts for 30.6 percent of the variance in cybersecurity awareness, suggesting moderate explanatory power. In general, the study emphasizes enhancing students' knowledge of digital security practices.

6. PRACTICAL IMPLICATIONS

The results of this study provide meaningful insights for educational institutions, policymakers, organizations, and researchers on how to enhance cybersecurity awareness among Generation Z users. Apart from this, the study emphasizes the need to integrate cybersecurity education, digital safety training, and awareness initiatives into the academic environment to equip students with the necessary online security skills.

7. LIMITATIONS OF THE STUDY

The current study has some limitations that should be noted. The data were gathered using an online questionnaire, which may introduce selection bias, as participation was limited to individuals with access to digital devices and willingness to respond to online surveys. This could limit how people with lesser levels of internet involvement are represented.

The study also relies on self-reported responses, which are subject to social desirability bias, where respondents may give answers perceived as socially acceptable rather than accurately reflecting their cybersecurity behavior and knowledge.

Further, the study was conducted among students from a single management institute, which may limit the applicability of the findings. Students from different academic disciplines, institutes, or geographical regions may exhibit varying levels of cybersecurity awareness and digital behavior; therefore, the results should be interpreted with caution when generalized to broader populations.

8. FUTURE SCOPE OF STUDY

This study provides opportunities for future research. In the future, researchers can study factors such as digital literacy, perceptions of online risk, prior experience with cyber threats, and exposure to cybersecurity training.

Researchers can also study actual cybersecurity behavior. Incorporating diverse educational faculties, regions, and age groups can broaden the scope of the study and enhance the generalizability of the findings. Comparative studies across different demographic groups may also help identify differences in cybersecurity awareness.

In addition, future studies can examine the impact of demographic variables, such as gender, age, and digital usage level, on cybersecurity awareness. Longitudinal research may also be conducted to examine how cybersecurity awareness evolves as digital technologies continue to advance.

REFERENCES

Ahamed, B., Polas, M. R. H., Falahat, M., Karim, R., & Tabash, M. I. (2026). Cybersecurity knowledge, social networking, and awareness among Gen Z university students. *Discover Education, 5*(1), 77.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences, 13*(9), 5700.

Alruthaya, A., Nguyen, T. T., & Lokuge, S. (2021). The application of digital technology and the learning characteristics of Generation Z in higher education. *arXiv preprint arXiv:2111.05991*.

Bada, M., Sasse, M. A., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Journal of Cyber Security and Digital Forensics, 4*(1), 118–131.

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Churchill, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research, 16*(1), 64–73. https://doi.org/10.1177/002224377901600110

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297–334. https://doi.org/10.1007/BF02310555

Darwish, A., & Lakhtaria, K. I. (2011). The impact of the new Web 2.0 technologies in communication, development, and revolutions of societies. *Journal of advances in information technology, 2*(4), 204-216.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Florençio, D., & Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th International World Wide Web Conference* (pp. 657–666). ACM. https://doi.org/10.1145/1242572.1242661

Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. In *Proceedings of the Second Symposium on Usable Privacy and Security* (pp. 44–55). ACM. https://doi.org/10.1145/1143120.1143127

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate data analysis* (5th ed.). Prentice Hall.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). Sage Publications.

Hennig, N. (2018). *Privacy and security online: Best practices for cybersecurity*. ALA TechSource, American Library Association.

Khan, F., Arora, S., Pargaien, S., Pande, L., & Khati, K. (2023, September). Exploring the Relationship Between Digital Engagement and Cybersecurity Practices Among College Students:

A Survey Study. In *International Conference on MAchine inTelligence for Research & Innovations* (pp. 147-159). Singapore: Springer Nature Singapore.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News, 190*(1), 1-69.

Mallinder, J., & Drabwell, P. (2014). Cyber security: A critical examination of information sharing versus data sensitivity issues for organisations at risk of cyber-attack. *Journal of business continuity & emergency planning*, *7*(2), 103-111.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Pawlowski, S. D., & Jung, Y. (2015). Social representations of cybersecurity by university students and implications for instructional design. *Journal of Information Systems Education*, *26*(4), 281-294.

Qudus, L. (2025). Advancing cybersecurity: strategies for mitigating threats in evolving digital and IoT ecosystems. *Int Res J Mod Eng Technol Sci*, *7*(1), 3185.

Soomro, T. R., & Hussain, M. (2019). Social media-related cybercrimes and techniques for their prevention. *Applied Computer Systems*, *24*(1), 9-17.

Slusky, L., & Partow-Navid, P. (2012). Students' information security practices and awareness. *Journal of Information Privacy and Security, 8*(4), 3–26.

Taha, A., & Dahabiyeh, L. (2021). College students' information security awareness: A cross-sectional study. *Information Security Journal: A Global Perspective, 30*(2), 73–82. https://doi.org/10.1080/19393555.2020.1858430

Tufekci, Z. (2008). Grooming, gossip, Facebook and MySpace: What can we learn about these sites from those who won't assimilate? *Information, Communication & Society*, *11*(4), 544–564. https://doi.org/10.1080/13691180801999050

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research, 45*(8), 1146–1166. https://doi.org/10.1177/0093650216681050

Wewege, L., Lee, J., & Thomsett, M. C. (2020). Disruptions and digital banking trends. *Journal of Applied Finance and Banking*, *10*(6), 15-56.