Issues in Information Systems
Volume 26, Issue 3, pp. 149-157, 2025

DOI: https://doi.org/10.48009/3_iis_2025_2025_112

Cybersecurity awareness among post-secondary students

Natalya Bromall, *Robert Morris University*, *bromall@rmu.edu*
Peter Draus, *Robert Morris University*, *draus@rmu.edu*
Sushma Mishra, *Robert Morris University*, *mishra@rmu.edu*
Kevin Slonka, *St. Francis University*, *KSlonka@francis.edu*
Judit Trunkos, *Robert Morris University*, *trunkos@rmu.edu*

Abstract

This study examines the level of cybersecurity awareness among different groups of post-secondary students, focusing primarily on two research goals. The first goal was to determine if the overall level of cybersecurity awareness among the students is sufficiently high. The second goal was to determine if the levels of cybersecurity awareness differ among the students of different levels (graduate vs. undergraduate), different genders, and particularly different areas. We hypothesized that the students pursuing IT-related majors demonstrate better awareness than non-IT majors. The findings indicated overall high level of cybersecurity awareness among all students, with a few exception focus areas, and a small but statistically significant difference between the level of cybersecurity awareness of IT and non-IT majors. No statistically significant differences were found between the students grouped by their gender or by their program level, graduate and undergraduate. The study reveals specific focus areas in cybersecurity that need to be addressed in post-secondary curricula.

Keywords: cybersecurity, post-secondary students, HAIS-Q, cybersecurity awareness

Introduction

In the years since the COVID-19 pandemic, educational institutions have migrated from traditional, fully on-ground learning to a mix of traditional and online learning, which includes fully online as well as hybrid courses (Mehta et al., 2024). This shift includes the new or highly increased adoption of various cloud-based technologies into the everyday routine, such as learning management systems, student information systems, virtual meeting platforms, email and file sharing platforms, and, as of recent years, artificial intelligence platforms. The extremely expanded use of cloud technologies, which translates to a wider attack surface for malicious actors, means that those in educational settings (both students and faculty) are more likely than ever to become targets of cyber-attacks (Eltahir & Ahmed, 2023).

These attacks come in all shapes and sizes and target all levels of educational institutions, from back-end infrastructure to faculty and students. Needing to protect sensitive data under the regulations of FERPA (educational records, PII, etc.), financial aid data under Title IV of the Higher Education Act of 1965, proprietary research data, and even government sensitive/classified data if the university engages in government contract work means that educational institutions have a wide attack surface with high-value targets. Whereas typical organizations can institute strict cybersecurity controls due to their homogeneous personnel, IT assets at educational institutions need to be accessed by various classes of personnel (staff,

faculty, students, public) that may or may not be able to have proper safeguards enforced. For example, many universities require some level of cybersecurity training for employees but typically require none for students. With many educational institutions lacking the infrastructure and manpower to implement zero-trust strategies and properly defend against cyber-attacks, a student laptop compromise could lead to eventual disaster in the datacenter (Lallie et al., 2025). Students, often lacking the experience and training of industry professionals, have been found to have various deficiencies in cybersecurity awareness. While some may have a basic understanding of the most common cyber-attacks (Senthilkumar & Easwaramoorthy, 2017), others are unaware of data usage and privacy protections (Moallem, 2018). Additionally, although students may possess basic cyber knowledge, that knowledge is rarely used in practice (Zwilling et al., 2020). Password security, the primary method used to grant access and protect sensitive data, is specifically deficient among students (Alqahtani, 2022).

A recent study noted a significant gap in research on cybersecurity awareness between undergraduate and graduate students and investigated this issue in an initial, limited-scope analysis. The researchers postulated the existence of a Cybersecurity-Resilience Gap, whereby something occurs between a student's undergraduate and graduate studies that increases their cybersecurity awareness (Goliath et al., 2024). This study picks up where the previous left off, increasing the scope by analyzing data from students in multiple majors at multiple institutions. In these efforts, the following research questions are posed:

RQ1: *What is the overall awareness of cybersecurity among various levels of post-secondary students?*
RQ2: *What are the differences in overall cybersecurity awareness between students with IT and Non-IT related majors?*

The rest of the paper is organized as follows: The next section provides a critical review of the relevant literature followed by a description of the methodology. The following section presents data collection and analysis. The results are then presented with discussions about the implications and limitations of the study.

Literature Review

Cybersecurity is an important topic and becomes increasingly important each year as more and more of our lives move into the digital environment. As our lives become more complex, cybersecurity becomes more complicated as well (Bak et al., 2024; Okika et al., 2025). Adejumo and Ogburie noted this multifaceted aspect of cybersecurity when they were looking at safeguarding financial information. They listed such strategies to include "encryption, multi-factor authentication, artificial intelligence-driven threat detection, and blockchain technology… artificial intelligence and machine learning in cybersecurity provides proactive defense mechanisms." They also noted that "consumer awareness and education on cyber hygiene are essential to reducing vulnerabilities, as social engineering attacks continue to exploit human error" (Adejumo & Ogburie, 2025, p.25). Each time an innovation, like Artificial Intelligence or Machine Learning, comes around. It impacts Cybersecurity and changes the landscape (Okika et al., 2025; Xu et al., 2025). Yet, cybersecurity is a broad subject that encompasses both technological and behavioristic components as noted by Magdalinou et al. (2022), "Human factors play an important role in maintaining information security as it is evident that non secure practices applied by employees may increase the vulnerability of the systems and lead to privacy issues" (p. 24). This is manifested in different ways, but social engineering is a significant target in cybersecurity attacks.

Social engineering

Mersainas, Bada & Furnell (2025) recently noted that, "the realization that a notable portion of security incidents have a human-related component" (p. 148). Other researchers have noted this as "critical

vulnerabilities in cybersecurity" (Okika et al., 2022, p.148). Styoutomo & Ruldeviyani (2023) highlighted the risks associated with social engineering have increased with the rapid deployment of remote work and other work from home schemes. Part of protecting against social engineering is making sure that users are aware of both cybersecurity and the policies that are in place to protect the system. The level of cybersecurity awareness is the first step in educating the users on what their role is when implementing a comprehensive cybersecurity protocol. There is a large body of research looking at cybersecurity policies, but Cram & D'Arcy (2025) argue that much of that research looks at why users violate the policies and not where they even know what their policies are or even what their role in cybersecurity actually is.

One aspect of this area of research is gathering the data without bias. Since researchers need to ask users what they know and don't know and why they acted the way they did. Bognár, L., & Bottyán (2024) summarized this issue by writing, "reliance on self-reported data introduces potential biases, such as social desirability bias, where respondents may overstate positive behaviors and underreport risky ones" (p. 588). Even if the users know a policy or risk, it doesn't actually mean that they will follow the policy. Kruger and Kearney (2006) noted that this aspect of cybersecurity is no different than any other controls put in place in an organization. Of interest is work done by Parsons et al. (2014) which showed that cybersecurity awareness increased user's attitudes towards the cybersecurity policies themselves. While policies are internal to the institution, they often reflect governance and legal requirements of the institution. Cybersecurity awareness has become as much a regulatory requirement as a cybersecurity requirement (Bak et al., 2024; Okika et al., 2025). These regulatory requirements go beyond direct employees and include the work that is outsourced. This means that cybersecurity awareness goes beyond internal employees and the organizational policies (Ranas et al., 2020).

Cybersecurity Awareness

The user's level of cybersecurity awareness has become the baseline measurement for determining the level of risk for behavioral or social engineering attacks but also is an effective deterrent to cybersecurity attacks (Abrahams et al., 2024). There is supporting evidence that not only is knowledge power but that there is a correlation between cybersecurity awareness and such aspects of security as password security measures (Ahmad et al., 2024). Other researchers have found correlation between higher security awareness and resistance to phishing attacks (Parsons et al., 2017). To measure correlation, researchers need a measure of cybersecurity awareness (Kruger & Kearney, 2006). One such measure is the HAIS-Q.

HAIS-Q

The HAIS-Q is a common tool for measuring cybersecurity awareness and reliability and validity testing has shown it to be a robust tool (Parsons et al, 2014 & 2017; McCormac et al., 2017). The HAIS-Q consists of a series of Likert type questions broken into 7 areas of focus: Password Management, Email Use, Internet Use, Social Media Use, Mobile Devices, Information Handling and Incident Reporting. Bak et al. (2024) found "The HAIS-Q questionnaire is found to be more frequently used than other questionnaires" (p. 306).

Gender and School Level Differences

Some researchers have reported finding interactions between genders, grade level and their core on some of the areas of focus in the HAIS-Q (Xu et al., 2024; Goliath et al., 2024). Cybersecurity is a constantly evolving multifaceted area of Information Security that utilizes a variety of hardware, software and behavioral tools to be effective. Security awareness not only is one measure of the human aspect of cybersecurity, but it also has been demonstrated to help with cybersecurity compliance and influence on the users' perception of cybersecurity policies. The HAIS-Q is a very common and tested tool to measure cybersecurity awareness.

Methodology

HAIS-Q, a well-established and frequently used instrument for measuring cybersecurity awareness, was chosen as the data collection instrument in this study. The HAIS-Q standard questionnaire includes 63 questions grouped into 7 areas of focus. Each area is organized as a matrix with three vertical categories (Knowledge, Attitude, and Behavior) and three horizontal items representing the essential security behaviors related to a given focus area. For example, the area of focus shown in Table 1 is Password Management, with the following three items: (1) Using the same password, (2) Sharing passwords, and (3) Using a strong password. Each item has three matching statements phrased slightly differently according to the column it is in. For example, the Knowledge category of Sharing passwords is formulated as "I am allowed to share my work passwords with colleagues", while the Behavior category is formulated as "I share my work passwords with colleagues".

Table 1. Sample Area of Focus in HAIS-Q Table

Focus area: Password Management			
	Knowledge	**Attitude**	**Behavior**
Using the same password	It's acceptable to use my social media passwords on my work accounts	It's safe to use the same password for social media and work accounts	I use different passwords for my social media and work accounts
Sharing passwords	I am allowed to share my work passwords with colleagues	It's a bad idea to share my work passwords, even if a colleague asks for it	I share my work passwords with colleagues
Using a strong password	A mixture of letters, numbers, and symbols is necessary for work passwords	It's safe to have a work password with just letters	I use a combination of letters, numbers, and symbols in my work passwords

The online survey used in this study included HAIS-Q questions rated on a 5-point Likert scale based on the respondent's agreement with the statement. Each question was rated in direct or reverse order, depending on its connotation. Each area of focus included 9 questions; therefore, the score of 45 was the maximum possible score in each of the seven areas. The scores were also aggregated based on the three vertical categories: Knowledge, Attitude, and Behavior. With 21 questions in each category, the score of 105 was the maximum possible score in each of these three categories. Data analysis included the analysis of descriptives, a series of independent sample t-tests comparing the scores by various groups, and a Pearson correlation test to determine correlations between the categories.

Results and Discussion

The sample included 102 graduate and undergraduate students from multiple universities and programs; two students skipped all but one area of focus; therefore, they were removed from the pool. Eight more students did not answer all 7 areas questions, which explains variations in the sample size in the following tests. Overall, we received approximately 100 valid responses in each section. The sample size was skewed toward IT students, with 2/3 of the students from IT majors and 1/3 of the students pursuing other majors, with the absolute majority, 90% of the students, enrolled in undergraduate programs. There was also substantial gender discrepancy with only 25% female respondents and 61% male (Table 2). The non-IT group included 9 female and 18 male students, while the IT group included 43 male and only 16 female students.

Table 2. Sample Demographics

Program		Age		Gender		Major	
Graduate	9	**18-21**	70	**Female**	25	**IT**	68
Undergrad	81	**22-27**	15	**Male**	61	**Non-IT**	32
		28-34	5	**Non-binary**	2		
No resp	10	**No resp**	10	**No resp**	12	**No resp**	
Total	100	**Total**	100	**Total**	100	**Total**	100

RQ1: Overall Cybersecurity Awareness

Kruger and Kearney, 2006 define a score of 80% or higher on a security awareness measurement scale similar to HAIS-Q as a good level of security awareness. The HAIS-Q scores in this study showed overall high levels of cybersecurity awareness among the students of all majors. As shown in Figure 1, all average scores were above the 80% threshold, with the minimal score of 36.4 received in Social Media Use focus area. The score of 36/45 marked 80%, so any score of 36 or higher would indicate a high level of awareness in the corresponding focus area.

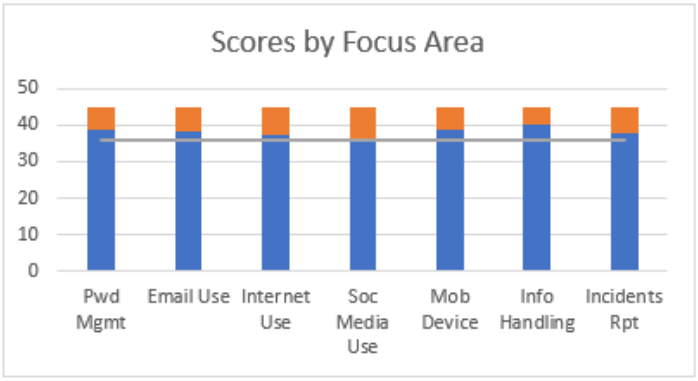

Figure 1: Overall Awareness Scores by HAIS Domain

In addition to exploring the scores by the areas of focus, we looked at the vertical categories identified as Knowledge, Attitude, and Behavior. With the maximum possible scores of 105 in each category, the overall Behavior score was 82.86 (78.9%), the Knowledge score was 83 (79%), and the Attitude score was 87.2 (83%). As we see, the first two scores are just below the 80% threshold of the "Good" category in Kruger's classification; while maintaining the good attitude toward cybersecurity, the students mostly showed high average scores in knowledge and behavior. After drilling down to the focus areas, only three categories showed average results: the knowledge of email use practices and the behaviors in internet and in social media use (Table 3).

Table 3. The Results of the HAIS-Q Survey by Focus Area

Focus Area	Knowledge	Attitude	Behavior	Total
Password Management	87.5%	85.1%	87.4%	86.7%
Email Use	78.5%	89.4%	86.5%	84.9%
Internet Use	81.1%	88.5%	78.6%	82.7%
Social Media Use	81.3%	86.7%	74.6%	80.9%
Mobile Device Use	86.0%	88.3%	84.5%	86.2%
Information Handling	88.3%	90.8%	90.0%	89.8%
Incident Report	82.6%	86.1%	82.4%	83.8%

RQ 2: Differences between IT and Non-IT Students

An independent sample t-test comparing the IT and the non-IT group showed small but significant differences between the groups' average scores in all but one area of focus (Table 4). Surprisingly, the only focus area where we did not observe any significant difference was Social Media Use. This focus area has also received the lowest scores, barely passing the 80% threshold.

Table 4. Differences between IT and Non-IT Students' Scores

	Major	N	Mean	Sig
Password Management	IT	68	39.5294**	.046
	Non-IT	32	37.8750	
Email Use	IT	67	38.8060**	.028
	Non-IT	32	36.8125	
Internet Use	IT	65	37.8615**	.045
	Non-IT	32	35.9063	
Social Media Use	IT	62	36.4677	.363
	Non-IT	31	36.1290	
Mobile Device Use	IT	62	39.6129**	.017
	Non-IT	30	37.2000	
Information Handling	IT	61	41.4098**	.002
	Non-IT	30	38.2333	
Incident Report	IT	61	38.3934**	.026
	Non-IT	29	36.1724	

**Mean difference is significant at the 0.05 level

While the IT group scored significantly higher than the non-IT group in six out of seven focus areas, no such differences were found between the groups' scores for the three horizontal categories. The overall scores in Knowledge, Attitude, and Behavior were computed by adding all scores in each of the three columns. We observed an almost perfect correlation between the scores for these three categories (Table 5). This led us to conclude that if a student scored high or low in one category, they would score the same way in any other category with almost a 100% chance. There is a very low chance of a gap between knowledge and actual behavior, between attitude and behavior, etc.

Table 5. Pearson's Correlation for Knowledge, Attitude, and Behavior

	Knowledge	Attitude	Behavior
Knowledge	**1**	**.975****	**.972****
Attitude	**.975****	**1**	**.959****
Behavior	**.972****	**.959****	**1**

**Correlation is significant at the 0.01 level

No significant differences were found in any scores between the students of different genders and different educational levels (graduate vs. undergraduate). This study was expected to confirm the results of the study by Goliath et al. (2024), which demonstrated a significant difference in cybersecurity awareness between graduate and undergraduate students; however, no such difference was found in our sample. This could be explained by the small number of graduate students, which was not sufficient for a t-test. The sample was also skewed toward male students and toward IT majors; however, in that case, all groups included sufficient subjects to run the tests.

Conclusion

This study had two goals. First, we explored the overall level of cybersecurity awareness among post-secondary students. The HAIS-Q survey scores used in the study demonstrated high levels of awareness

through almost all categories. Exceptions included the knowledge of email cybersecurity issues and behavioral aspects of the Internet use and social media use. The last two categories are extremely important because they show what the students actually do (or what they are willing to do) in the most common activities: browsing the Internet or working with social media. No significant difference was found in the levels of cybersecurity awareness between the groups based on the students' gender or their age.

Second, we compared the levels of cybersecurity awareness between the students pursuing IT majors and those with non-IT majors. Small but significant differences were found between cybersecurity awareness in those groups in all focus areas except social media use – the area where the students also showed the lowest level of awareness. Finally, the study demonstrated almost perfect correlations between the three domains of cybersecurity awareness: knowledge, attitude, and behavior. This suggested that the students in our sample "practice what they preach", so it is extremely unlikely that a student, for example, would demonstrate high level of cybersecurity knowledge but a much lower level of the correct attitude or behavior.

References

Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: a review of employee engagement and accountability. Computer Science & IT Research Journal, 5(1), 100-119.

Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. World Journal of Advanced Research and Reviews, 25.

Ahamed, B., Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Fahad, A. A., Chowdhury, S., & Rani Dey, M. (2024). Empowering students for cybersecurity awareness management in the emerging digital era: the role of cybersecurity attitude in the 4.0 industrial revolution era. Sage Open, 14(1), 21582440241228920.

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. Applied Sciences, 12, 1-21.

Bak, G., Berek, L., Som, Z., Ujhegyi, P., & Répás, J. (2024). On the Way to Updating the Measurement of Information Security Awareness–a Literature Analysis. Interdisciplinary Description of Complex Systems: INDECS, 22(3), 305-316.

Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. Education Sciences, 14(6), 588.

Cram, W. A., & D'Arcy, J. (2025). Barking up the wrong tree? Reconsidering policy compliance as a dependent variable within behavioral cybersecurity research. Information Systems Frontiers, 1-12.

Eltahir, M. E. & Ahmed, O. S. (2023). Cybersecurity awareness in African higher education institutions: A case study of Sudan. Information Science Letters, 12, 171-183. DOI: 10.18576/isl/120113

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & security, 25(4), 289-296.

Goliath, S., Tsibolane, P., & Snyman, D. (2024). Exploring the cybersecurity-resilience gap: An analysis of student attitudes and behaviors in higher education. arXiv preprint arXiv:2411.03219v1. https://doi.org/10.48550/arXiv.2411.03219

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector. Computers, 14(2), 1-28.

Magdalinou, A., Kalokairinou, A., Malamateniou, F., & Mantas, J. (2022). Assessing internal consistency of HAIS-Q: a survey conducted in Greek hospitals. In Advances in Informatics, Management and Technology in Healthcare (pp. 24-27). IOS Press.

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. Australasian Journal of Information Systems, 21.

Mehta, K. J., Aula-Blasco, J., & Mantaj, J. (2024). University students' preferences of learning modes post COVID-19-associates lockdowns: In-person, online, and blended. PLoS One, 19(7), 1-21.

Mersinas, K., Bada, M., & Furnell, S. (2025). Cybersecurity behavior change: A conceptualization of ethical principles for behavioral interventions. Computers & Security, 148, 104025.

Moallem, A. (2018). College students information security awareness: A comparison between smartphones and computers. Education and Information Technologies, 26, 1721-1736.

Okika, N., Okoh, O. F., & Etuk, E. E. (2025). Mitigating Insider Threats and Social Engineering Tactics in Advanced Persistent Threat Operations through Behavioral Analytics and Cybersecurity Training. International Journal of Advance Research Publication and Reviews, 2(3), 11-27.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Computers & Security, 66, 40-51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & security, 42, 165-176.

Ranas, T., Fariz, A., Dirgantara, B., Muhamad, A., & Ruldeviyan, Y. (2020). Measuring information security awareness of client's information security: case study at PT XYZ. International Journal of Advances in Electronics and Computer Science, 7(7), 2394-2835.

Senthilkumar, K. & Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in Tamil Nadu. Proceedings of the IOP Conference Series: Materials Science and Engineering: Vellore, India.

Styoutomo, Y. A., & Ruldeviyani, Y. (2023). Information Security Awareness Raising Strategy Using Fuzzy AHP Method with HAIS-Q and ISO/IEC 27001: 2013: A Case Study of XYZ Financial Institution. CommIT (Communication and Information Technology) Journal, 17(2), 133-149.

Xu, X., Hong, W. C. H., Kolletar-Zhu, K., Zhang, Y., & Chi, C. (2024). Validation and application of the human aspects of information security questionnaire for undergraduates: effects of gender, discipline and grade level. Behaviour & Information Technology, 43(12), 2799-2820.

Xu, J., Wang, Y., Chen, H., & Shen, Z. (2025). Adversarial Machine Learning in Cybersecurity: Attacks and Defenses. International Journal of Management Science Research, 8(2), 26-33.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62, 82-97.