The Scientific Temper (2025) Vol. 16 (7): 4543-4550
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2025.16.7.06
https://scientifictemper.com/

RESEARCH ARTICLE

Assessing the information security awareness among Ghanaian University students

Hannah Ayaba Tanye*, Henry Akwetey Matey, Isaac Asampana, Albert Akanlisikum Akanferi, Douglas Yeboah, Augustina Dede Agor

Abstract

There is a growing concern about University students' safety on Online platforms used for learning and related personal activities. With the changes in the way most Institutions are shifting towards blended learning, it cannot be overemphasized that a growing concern of Institutions of the safety of their students on these platforms. These concerns are obvious in the mass literature on the security awareness of students. The literature has shown a multifaceted reason that can influence the security awareness of students on online platforms. This is no different from what is happening in the University of Professional studies, Accra (UPSA) in Ghana. This research aims to find out the level of students' knowledge and behavior and the level of their security awareness in the UPSA community in their online engagement. The results of this research will be of help to the UPSA Management and the IT department to draw up programs and policies and to put measures in place to ensure safer online interactions for students.

Keywords: Security, University, Online platforms, Human, Policies, Computer.

Introduction

The importance of information security knowledge in higher education cannot be emphasized since it encourages students to be watchful and accountable. In an increasingly interconnected world, risk mitigation requires not only theoretical frameworks but also practical awareness and informed use of digital technologies. In this sense, Ghanaian colleges, like others throughout the world, face distinct difficulties, especially as online services and electronic banking become more widely used within their schools. As mentioned, adopting secure methods may be more likely when there is less complexity and perceived utility. This research emphasizes how important it is for colleges to offer thorough and approachable information security education in order to promote proactive participation.

There is a growing concern of University students' safety on online platforms used for learning and related personal activities. With the changes in the way most institutions are shifting towards blended learning, it cannot be overemphasized a growing concern among Institutions about the safety of their students on these platforms. These concerns are obvious in the mass literature on the security awareness of students. The literature has shown a multifaceted reasons that can influence the security awareness of students on online platforms. This is no different from what is happening at the University of Professional Studies, Accra (UPSA) in Ghana. This research aims to find out the security behaviour of students in their usage of Information Technology at the UPSA community in their online engagement. The results of this research will be of help to the UPSA Management and the IT department to know the impact of the awareness measures put in place and to review programs and policies, and to put measures in place to ensure safer online interactions for students.

Additionally, good career counseling can improve students' ability to make decisions about their educational and professional pathways by helping them comprehend the ethical ramifications of digital activity (Esseh *et al*., 2021). Research literature has suggested that Institutions may foster a strong security culture, which is crucial in the

Information Technology Department, University of Professional Studies, Accra, Ghana.

***Corresponding Author:** Hannah Ayaba Tanye, Information Technology Department, University of Professional Studies, Accra, Ghana, E-Mail: Hannah.tanye@upsamail.edu.gh

How to cite this article: Tanye, H.A., Matey, H.A., Asampana, I., Akanferi, A.A., Yeboah, D., Agor, A.D. (2025). Assessing the information security awareness among Ghanaian University students. The Scientific Temper, **16**(7):4543-4550.

Doi: 10.58414/SCIENTIFICTEMPER.2025.16.7.06

Source of support: Nil

Conflict of interest: None.

Received: 13/06/2025 **Accepted:** 26/06/2025 **Published**: 31/07/2025

current digital environment, by giving priority to socio-demographic factors, technological exposure among others. The objectives of the study are:

- To assess the general level of information security awareness among UPSA students.
- To measure participants' ability to recognize and respond appropriately to security incidents or threats.
- To determine the frequency and effectiveness of secure practices such as password management, software updates, and use of antivirus tools.
- To recommend strategies for improving information security awareness and practices among UPSA Students

Review of the Literature

According to research, universities and the academic sector are some of the least secure settings for information security (Bongiovanni (2019) in Kraus *et al*. n.d.). This is mostly caused by institutions' open-access policies, which make it simple to obtain important data, as well as a lack of strong security protocols and user awareness. Furthermore, research has shown that college students frequently display inadequate information security practices, leaving both their institutions and themselves vulnerable to cyberattacks.

Research already conducted shows how crucial it is to address information security awareness in the classroom. According to a study on undergraduate business college students' awareness of information security, students frequently don't understand the significance of information security and appropriate security procedures (Frik *et al*., 2022).

In a research conducted by Bhagavatula *et al*., 2021, 303 participants' browsing histories were examined during a four-year period in order to gauge their interaction with websites related to six significant security events. They discovered that just sixteen percent of participants went to a website pertaining to the occurrence, and even fewer of them took proactive measures like learning more about it or enhancing their security. It was discovered that the likelihood of reading about an occurrence was influenced by variables like age, proactive security knowledge, and technological affinity. In order to guarantee user safety, the researchers underlined the necessity of efficiently disseminating information about security incidents and investigating alternative strategies outside of depending solely on user awareness and education. Research also shows that there lack of understanding about available settings and their effectiveness (Bhagavatula *et al*., 2022; Frik *et al*., 2022).

Literature has also shown that human factors can influence security issues and suggested that failure to comply with security policies is due to poor work factors, work security culture, and individual personal traits (Yeng *et al*., 2021). Marin, Allodi, and Zannone (n.d.) were of the view that to assess how human factors can be used to enhance training and awareness initiatives and cultivate an organization's culture that encourages constructive cybersecurity practices, further studies and experiments are needed. Despite technological improvements to compact security issues, human factors are still the weakest link and must be addressed (Huraj *et al*., 2023). Studies have also suggested the use of the *Human Aspects of Information Security Questionnaire (*HAIS-Q) that evaluates people's knowledge, attitude, and behavior regarding cybersecurity measures in order to determine their level of information security awareness (Rizal & Setiawan, 2024). There has also been suggestions intentional forgetting, that is introducing new behaviour and ensure that that uses forget old insecure behaviour by reducing the information that needs to be transmitted to employees, and suppressing obsolete routines (Hielscher *et al*., 2021). The studies have also suggested the introduction of security champions in organizations (Menges *et al*., 2023). In order to promote the broad adoption of sound security practices, some research findings emphasize the significance of making positive security and privacy recommendations more common on online social media (Bhagavatula *et al*., 2022). Research has also highlighted how critical it is to fix password practice flaws and stress the necessity of all-encompassing instructional strategies that include different security aspects. To address the particular requirements of students from a variety of academic fields, institutions must think about modifying their teaching methods (Guo & Tinmaz, 2023). However, it has been established that students have different levels of security with smartphones and computers and behave differently in protecting their smartphones than their computers (Taha & Dahabiyeh, 2021). That is why literature has suggested all-encompassing strategies that include different security aspects(Guo & Tinmaz, 2023). There is not much studies to assess the knowledge that students exhibit in certain areas of the Information technology usage. There is has been training and the influence of the security awareness of students. There has not been any follow-up research to test whether there has been changes in the security behavior of students on systems. Their self-efficacy on how well they can and deal with security situations in their usage of Information technology is very necessary (Borgert *et al*., 2024).

The use of passwords is commonplace in our daily lives. We must use passwords to secure our information and safeguard everything that is vital to us, whether we are logging into our computers, smartphones, banks, or other devices (Davis *et al*., 2022). Not only may we lose access to our personal information if someone with bad intent knows our passwords, but identity theft could cost us everything (Zaland *et al*., 2021). Although it's crucial to update our passwords from time to time, requiring changes too regularly may actually make them worse.

Protecting internet-connected devices, including smartphones, laptops, PCs, tablets, and Internet of Things devices (Jumani *et al*., 2023) from intrusions and illegal access is known as device security. Strong authentication, mobile device management software, and limited network access are usually necessary for device security(Rezapour *et al*., 2021).

Email security guards against loss, compromise, and unwanted access to email accounts and conversations. It entails employing mechanisms like encryption and authentication in order to stop unwanted communications and cyberattacks (Jumani *et al*., 2023).

The term "internet security" refers to security measures intended to safeguard networks, web browsers, web apps, websites, and systems as well as the activities of staff members and other users when they are linked to the internet. Users and company assets are shielded from cybersecurity risks and attacks by internet security solutions(Rezapour *et al*., 2021).

Social media is a group of online resources that let people interact, exchange information, and produce content. Social media platforms can be used to connect with people in communities or to stay in touch with friends and family. The use of social media must be done with caution since there is a potential to lose personal information through inappropriate means(Cain & Imre, 2022).

Theoretical Framework

This study is base on the Theory of Planned Behaviour (TPB). The TPB initial construct is behavioral intention, which refers to the driving forces behind conduct (Ajzen, 1991in Marin *et al*. 2023). The likelihood of engaging in a particular conduct increases with the strength of the intention to do so. The second construct is attitude toward the behavior, which is the degree to which an individual views a certain behavior favorably or unfavorably. Behavioral beliefs and outcome assessments make up attitude. The third construct is the subjective norm, which is societal pressure to engage in or refrain from engaging in a particular activity. Subjective norms are made up of normative views and compliance desire. Another important component of the TPB is perceived behavioral control, which describes how easy or difficult people believe it to be.

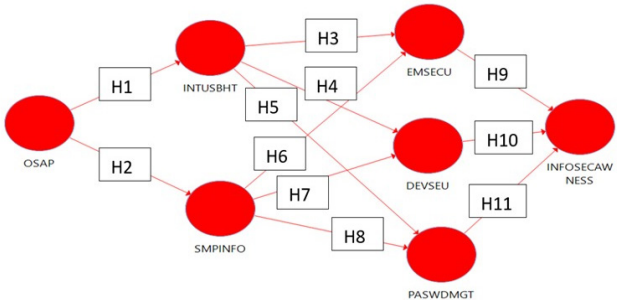


Figure 1: Theoretical framework

Table 1: Theoretical framework

OSAP	Organizational support and security policies (IV)
INTUSBHT	Internet usage and safe browsing habits (IV)
SMPINFO	Social media and Personal Information (IV)
EMSECU	Email Security (IV)
DEVSEU	Device Security (IV)
PASWDMGT	Password Management (IV)
INFOSECAWNESS	Information Security Awareness (DV)

By highlighting the importance of awareness, motivation, and self-control in forming secure behaviors, this theory informs the HAIS-Q. In order to forecast and improve security-compliant behavior in businesses or educational environments, the framework is made to fully comprehend these human variables. The theoretical framework is shown in Figure 1 with the various variables and hypotheses. Table 1 above shows the abbreviations of the various variables in the theoretical framework.

Materials And Methods

Study Design and Settings

The study is a quantitative study and the use of descriptive statistics to determine the characteristics of students and their level of awareness. The study is based on TPB, which informs the HAIS-Q, which evaluates people's knowledge, attitude, and behavior regarding cybersecurity measures in order to determine their level of information security awareness (Rizal & Setiawan, 2024). The questionnaire is structured into different sections. These sections are password management, device security, email security, internet usage, social media and personal information, and organizational support and policies. A self-administered questionnaire was used in conducting the survey. This study was conducted in Ghana at the University of Professional Studies, Accra (UPSA), with the students as the target population. The main objective is to assess the level of Information security awareness of UPSA students.

Results And Discussion

The measurement model refers to the systematic procedures employed to assess the reliability and validity of the constructs used in a research framework. This step is crucial in structural equation modeling (SEM), as it ensures that the constructs accurately reflect the underlying theoretical concepts they are intended to measure. Following the guidelines of Hair *et al*. (2019), the present study examined three core aspects of the measurement model. First, indicator loadings and internal consistency reliability were evaluated to determine the extent to which observed variables (indicators) consistently represent the latent constructs. Indicator loadings above the recommended threshold (typically ≥ 0.70) indicate that each item is a

good representation of its associated construct. Internal consistency was further assessed using composite reliability (CR) and Cronbach's alpha to ensure that items within the same construct are interrelated and produce stable results. Second, convergent validity was tested to confirm that the indicators of a specific construct converge or share a high proportion of variance in common. This was assessed using the average variance extracted (AVE), where values of 0.50 or higher suggest that the construct explains at least 50% of the variance in its indicators, thereby supporting convergent validity. Third, discriminant validity was evaluated to ensure that each construct is empirically distinct from other constructs within the model. This was assessed using the Fornell-Larcker criterion and the Heterotrait-Monotrait (HTMT) ratio. Discriminant validity ensures that the constructs are not only conceptually unique but also statistically independent from one another. These evaluations strengthen the credibility of the measurement model by verifying that the constructs are measured accurately and meaningfully, thus providing a sound basis for subsequent analysis of the structural model. Table 2 shows the details of demographic of Respondents with attributes gender, age, and educational level.

Measurement Model Analysis

This study used partial least squares structural equation modeling (PLS-SEM) to evaluate indicator loadings. Table 3 shows the Indicator Loadings and Internal Consistency Reliability. As presented in Table 3, most items met the recommended threshold loading value of > 0.708, consistent with the guideline provided by Muhaimin *et al*. (2020). According to Hair *et al*. (2019), internal consistency reliability should be assessed using both Cronbach's alpha (α) and composite reliability (CR). In line with their recommendations, α values should exceed 0.700, while CR values should be greater than 0.708. Table 3 provides the specific values obtained in this study, all of which meet these criteria, confirming satisfactory internal consistency across the constructs. Convergent validity, a component of construct validity, refers to the degree to which items that are supposed to measure the same construct are indeed closely related. This study used the PLS-SEM algorithm in SmartPLS to compute average variance extracted (AVE), where a value of 0.500 or higher indicates that the construct explains at least 50% of the variance in its indicators. As shown in Table 3, all constructs had AVE scores above 0.500, supporting strong convergent validity. For discriminant validity, Hair *et al*. (2019) define it as the extent to which a construct is empirically distinct from other constructs in the model. Table 4 indicates Discriminant validity using Fornell–Larcker Criterion. The Fornell-Larcker criterion was used for this assessment, requiring that the square root of each construct's AVE be greater than its correlations with other constructs. The results in (Table 5) confirm that this condition was met for all constructs, thus establishing discriminant validity. Further assessment using the Heterotrait-Monotrait ratio (HTMT) of correlations was also conducted, as high HTMT values (above 0.900) can indicate a lack of discriminant validity. Table 6 shows that all HTMT values were below the 0.900 threshold and significantly different from 1, further confirming that the constructs in the model are empirically distinct.

Table 2: Demographic of respondents

Attribute	*Category*	*Frequency*	*Percentage*
Gender	Male	180	60
	Female	120	40
Age (in years)	15-19	22	7.33
	20-29	200	66.67
	30-39	60	20
	40-49	18	6
Educational level	100	50	16.67
	200	182	60.67
	300	60	20
	400	8	2.67

Structural Model Analysis

The study investigates the relationships between exogenous and endogenous variables, as illustrated in Figure 2 and detailed in Table 6. Specifically, it examines seven key constructs: Organizational Support and Security Policies, Internet Usage and Safe Browsing Habits, and social media and Personal Information, Email Security, Device Security, and Password Management as independent variables (IVs); and Information Security Awareness as the dependent variable (DV). The researcher aims to explore the direct associations among these variables to understand the relationship among these factors and how they turn to influence information security awareness.The results for H1 indicate a statistically significant positive relationship between Organizational Support and Security Policies (OSAP) and Internet Usage and Safe Browsing Habits (INTUSBHT), with a path coefficient of ($\beta = 0.282$, $t = 4.596$, $p = 0.000$). This suggests that robust institutional support such as clearly communicated security policies, management commitment, and ongoing training positively influences employees' online behavior. The results for H2 demonstrate a statistically significant and positive relationship between Organizational Support and Security Policies (OSAP) and social media and Personal Information Practices (SMPINFO), with ($\beta = 0.342$, $t = 8.366$, $p = 0.000$). This indicates that organizations that actively promote security awareness and enforce usage policies tend to foster more responsible social media behavior among their members. As a result,

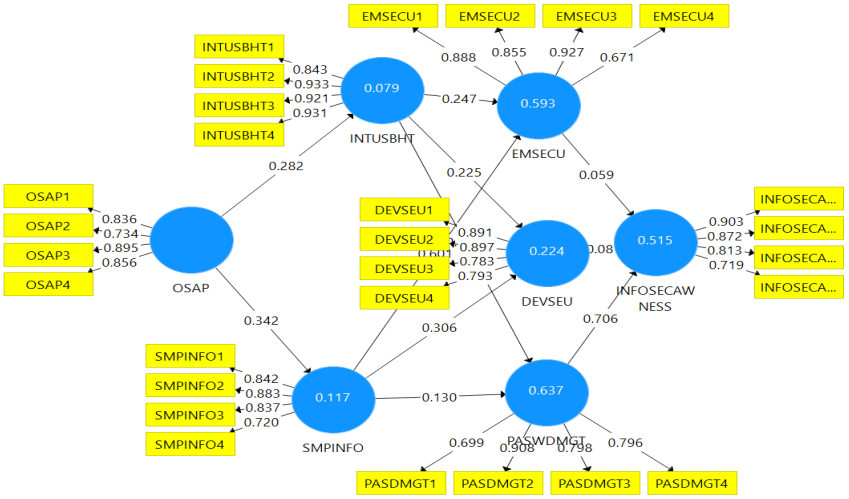


Figure 2: PLS Results for measurement model

Table 3: Indicator Loadings and Internal Consistency Reliability

Latent variable	*Manifest Variable*	*Indicator Loadings*	*Cronbach's (α)*	*Rho_A*	*Composite Reliability (CR)*	*Average Variance Extracted (AVE)*
DEVSEU	DEVSEU1	0.891	0.863	0.877	0.907	0.710
	DEVSEU2	0.897				
	DEVSEU3	0.783				
	DEVSEU4	0.793				
EMSECU	EMSECU1	0.888	0.860	0.908	0.905	0.707
	EMSECU2	0.855				
	EMSECU3	0.927				
	EMSECU4	0.671				
INFOSECAWNESS	INFOSECAWNESS1	0.903	0.850	0.896	0.898	0.688
	INFOSECAWNESS2	0.872				
	INFOSECAWNESS3	0.813				
	INFOSECAWNESS4	0.719				
INTUSBHT	INTUSBHT1	0.843	0.928	0.932	0.949	0.824
	INTUSBHT2	0.933				
	INTUSBHT3	0.921				
	INTUSBHT4	0.931				
OSAP	OSAP1	0.836	0.851	0.867	0.900	0.693
	OSAP2	0.734				
	OSAP3	0.895				
	OSAP4	0.856				
PASDMGT	PASDMGT1	0.699	0.813	0.829	0.879	0.646
	PASDMGT2	0.908				
	PASDMGT3	0.798				
	PASDMGT4	0.796				
SMPINFO	SMPINFO1	0.842	0.845	0.887	0.893	0.677
	SMPINFO2	0.883				
	SMPINFO3	0.837				
	SMPINFO4	0.720				

Table 4: Discriminant validity using Fornell–Larcker Criterion

	DEVSEU	*EMSECU*	*INFOSECAWNESS*	*INTUSBHT*	*OSAP*	*PASWDMGT*	*SMPINFO*
DEVSEU	0.843						
EMSECU	0.488	0.841					
INFOSECAWNESS	0.188	0.44	0.83				
INTUSBHT	0.402	0.593	0.48	0.908			
OSAP	0.21	0.337	0.259	0.282	0.832		
PASWDMGT	0.34	0.595	0.714	0.791	0.267	0.804	
SMPINFO	0.436	0.743	0.357	0.575	0.342	0.542	0.823

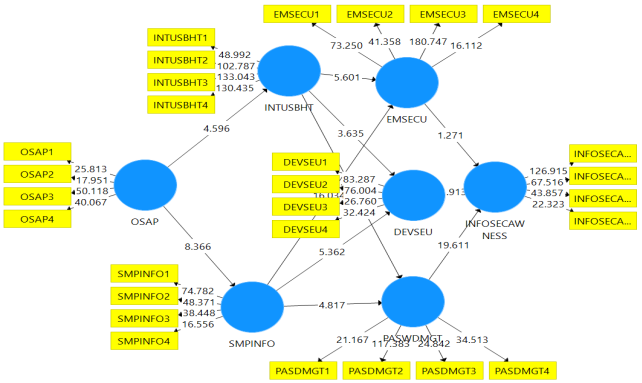
Table 5: Heterotrait-Monotrait Ratio (HTMT)

	DEVSEU	*EMSECU*	*INFOSECAWNESS*	*INTUSBHT*	*OSAP*	*PASWDMGT*	*SMPINFO*
DEVSEU							
EMSECU	0.580						
INFOSECAWNESS	0.212	0.484					
INTUSBHT	0.443	0.658	0.519				
OSAP	0.233	0.381	0.313	0.320			
PASWDMGT	0.412	0.693	0.823	0.908	0.322		
SMPINFO	0.486	0.804	0.367	0.627	0.375	0.605	

employees are more likely to safeguard their personal data and exercise caution in digital communication. H3 findings reveal a statistically significant and positive relationship between Internet Usage and Safe Browsing Habits (INTUSBHT) and Email Security (EMSECU), with (β = 0.247, t = 5.601, p = 0.000). This implies that individuals who engage in responsible internet usage are also more vigilant in managing their email security, such as avoiding phishing links and using multi-factor authentication. The results for H4 show a statistically significant positive relationship between Internet Usage and Safe Browsing Habits (INTUSBHT) and Device Security (DEVSEU), indicated by (β = 0.225, t = 3.635, p = 0.000). This suggests that users who demonstrate secure browsing habits are also likely to take preventive actions to protect their devices. H5 reveals a strong, statistically significant positive relationship between Internet Usage and Safe Browsing Habits (INTUSBHT) and Password Management (PASWDMGT), with (β = 0.716, t = 21.147,p = 0.000). This high coefficient indicates that individuals who engage in cautious browsing are significantly more likely to adopt secure password practices such as using complex passwords, avoiding reuse, and utilizing password managers. Results for H6 show a statistically significant and strong positive relationship between social media and Personal Information (SMPINFO) and Email Security (EMSECU), with (β = 0.601, t = 16.034, p = 0.000). This implies that users who are cautious with personal information on social media also apply similar caution to email usage. The findings for H7 reveal a statistically significant positive relationship between social media and Personal Information (SMPINFO) and Device Security (DEVSEU), with (β = 0.306, t = 5.362, p = 0.000). This suggests that users who exercise caution on social media are also more likely to implement device-level security practices. H8 demonstrate a statistically significant positive relationship between social media and Personal Information (SMPINFO) and Password Management (PASWDMGT), with (β = 0.130, t = 4.817, and p = 0.000). This suggests that digital responsibility in one area may enhance broader cybersecurity practices. H9 indicate a positive but statistically insignificant relationship between Email Security (EMSECU) and Information Security Awareness (INFOSECAWNESS), with (β = 0.059, t = 1.271, p = 0.204). This may imply that isolated secure email behavior does not strongly predict overall cybersecurity awareness. Users may view email security as a task-specific habit rather than part of a comprehensive security framework, thereby reducing its influence on broader awareness. H10 reveals a negative and statistically insignificant relationship between Device Security (DEVSEU) and Information Security Awareness (INFOSECAWNESS), with (β = -0.081, t = 1.913,p = 0.056). Though close to the significance threshold, this inverse relationship suggests potential gaps in how users perceive device security in relation to their broader cybersecurity knowledge. It may also indicate overreliance on default device protections without a deeper understanding of underlying security risks. The findings for H11 also reveal a strong, statistically significant positive relationship between Password Management (PASWDMGT) and Information Security Awareness (INFOSECAWNESS), with (β = 0.706, t

Table 6: Path Coefficients and Significance

hypothesis	*Path*	*β*	*T Statistics*	*P Values*
H1	OSAP -> INTUSBHT	0.282	4.596	0.000
H2	OSAP -> SMPINFO	0.342	8.366	0.000
H3	INTUSBHT -> EMSECU	0.247	5.601	0.000
H4	INTUSBHT -> DEVSEU	0.225	3.635	0.000
H5	INTUSBHT -> PASWDMGT	0.716	21.147	0.000
H6	SMPINFO -> EMSECU	0.601	16.034	0.000
H7	SMPINFO -> DEVSEU	0.306	5.362	0.000
H8	SMPINFO -> PASWDMGT	0.130	4.817	0.000
H9	EMSECU -> INFOSECAWNESS	0.059	1.271	0.204
H10	DEVSEU -> INFOSECAWNESS	-0.081	1.913	0.056
H11	PASWDMGT -> INFOSECAWNESS	0.706	19.611	0.000



**Significant at P<0.01 ***Significant at P<0.05

Figure 3: PLS results for final model

Table 7: Coefficient of determination R2

VARIABLES	R Square
DEVSEU	0.224
EMSECU	0.593
INFOSECAWNESS	0.515
INTUSBHT	0.079
PASWDMGT	0.637
SMPINFO	0.117

= 19.611, p = 0.000). which suggests that individuals who exhibit strong password practices are more likely to possess heightened overall cybersecurity awareness.

Coefficient of Determination R^2

Table 7 shows Coefficient of Determination R2. The coefficient of determination (R^2) reflects the proportion of variance in an endogenous variable that is explained by its associated exogenous variables, thereby assessing the model's predictive accuracy. R^2 values range from 0 to 1, with higher values indicating stronger explanatory power. An R^2 value of 0.75 or higher is considered substantial, 0.50 is moderate, and 0.25 is weak(Hair *et al*., 2018, 2019, 2021). In this study, the model demonstrates strong predictive accuracy for cyber-attacks (R^2 = 0.803), whereas the predictive accuracy for Training Impact is relatively weak (R^2 = 0.300), as illustrated in Figure 3.

Conclusion

The findings of this study underscore the multifaceted nature of student information security awareness, highlighting the critical roles played by both individual behaviors and institutional support systems. The conceptual model employed, which integrated key areas such as Password Management, Device Security, Email Security, Internet Usage, Social Media and Personal Information, and Organizational Support and Policies, provided a comprehensive framework for evaluating the level of awareness among students.

The results revealed varying levels of awareness across the components. While students demonstrated moderate understanding of password best practices and basic device security measures, gaps remained in the areas of phishing awareness, responsible internet use, and protecting personal data on social media platforms. These vulnerabilities suggest that many students may not fully grasp the real-world consequences of poor information security practices.

Importantly, the study also found that organizational support and clear institutional policies have a significant influence on student behavior and awareness. Institutions that actively promote information security through training programs, policy enforcement, and regular awareness

campaigns tend to have students who are better informed and more cautious in their digital practices.

In conclusion, strengthening student information security awareness requires a dual approach: empowering students with the knowledge and tools needed for safe digital practices, and fostering a supportive institutional environment that prioritizes and reinforces cybersecurity awareness. Universities must invest in ongoing education, policy development, and infrastructure to mitigate risks and prepare students for a secure digital future.

Acknowledgement

We acknowledge the contribution of all the co-authors and also the University of professional studies and its students.

References

Bhagavatula, S., Bauer, L., & Kapadia, A. (2021). What breach? Measuring online awareness of security incidents by studying real-world browsing behavior. *ACM International Conference Proceeding Series*, 180–199. https://doi.org/10.1145/3481357.3481517

Bhagavatula, S., Bauer, L., & Kapadia, A. P. U. (2022). *"Adulthood is trying each of the same six passwords that you use for everything": The Scarcity and Ambiguity of Security Advice on Social Media*. *6*(November). https://doi.org/10.1145/3555154

Borgert, N., Jansen, L., Friedauer, J., & Sasse, M. A. (2024). *Self-Efficacy and Security Behavior : Results from a Systematic Review of Research Methods*. https://doi.org/10.1145/3613904.3642432

Cain, J. A., & Imre, I. (2022). Everybody wants some: Collection and control of personal information, privacy concerns, and social media use. *New Media & Society, 24(12), 2705-2724.*

Davis, D. K., Chowdhury, M. M., & Rifat, N. (2022). *Password Security: What Are We Doing Wrong?* https://doi.org/, doi: 10.1109/eIT53891.2022.9814059

Esseh, S. S., Afeafa, L., & Kwesi, R. S. (2021). Career Choices of Students in Senior High Schools in Ghana. *Journal of Education and Practice*, 78–90. https://doi.org/10.7176/jep/12-10-10

Frik, A., Kim, J., Sanchez, J. R., & Ma, J. (2022). *Users' Expectations About and Use of Smartphone Privacy and Security Settings*. https://doi.org/10.1145/3491102.3517504

Guo, H., & Tinmaz, H. (2023). *A survey on college students' cybersecurity awareness and education from the perspective of China*. *11*(3), 351–367.

Hair, J. F., Hult, G. T. M., Ringle, C., Sarstedt, M., Danks, N., & Ray, S. (2021). Partial least squares structural equation modeling (PLS-SEM) using R: A workbook. In *Springer*.

Hair, J. F., Risher, J. J., & Ringle, C. M. (2018). *When to use and how to report the results of PLS-SEM*. *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hielscher, J., Kluge, A., Menges, U., & Sasse, M. A. (2021). "Taking out the Trash": Why Security Behavior Change requires Intentional Forgetting. *ACM International Conference Proceeding Series*, 108–122. https://doi.org/10.1145/3498891.3498902

Huraj, L., Lengyelfalusy, T., Hurajová, A., & Lajčin, D. (2023). Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students. *TEM Journal*, *12*(2), 623–633. https://doi.org/10.18421/TEM122-05

Jumani, A., Shi, J., Laghari, A., Hu, Z., Shahani, A. U. N., & Qian, H. (2023). Fog computing security: A review. *SECURITY AND PRIVACY. 6. 10.1002/Spy2.313*.

Kraus, L., Švábenský, V., Horák, M., Vykopal, J., & Čeleda, P. (n.d.). *Want to Raise Cybersecurity Awareness ? Start with Future IT Professionals* . 236–242. https://doi.org/10.1145/3587102.3588862

Marin, I. A., Burda, P., Zannone, N., & Allodi, L. (2023). The Influence of Human Factors on the Intention to Report Phishing Emails. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3544548.3580985

Menges, U., Hielscher, J., Kocksch, L., Kluge, A., & Angela Sasse, M. (2023). Caring Not Scaring - An Evaluation of a Workshop to Train Apprentices as Security Champions. *ACM International Conference Proceeding Series*, 237–252. https://doi.org/10.1145/3617072.3617099

Rezapour, R., Asghari, P., Javadi, H. H. S., & Ghanbari, S. (2021). Security in fog computing: A systematic review on issues, challenges and solutions. *Computer Science Review*, *41*. https://doi.org/doi.org/10.1016/j.cosrev.2021.100421.

Rizal, M. A., & Setiawan, B. (2024). Information Security Awareness Literature Review: Focus Area for Measurement Instruments. *Procedia Computer Science*, *234*(2023), 1420–1427. https://doi.org/10.1016/j.procs.2024.03.141

Taha, N., & Dahabiyeh, L. (2021). *College students information security awareness: a comparison between smartphones and computers College students information security awareness : a comparison between smartphones and computers*. *October 2020*. https://doi.org/10.1007/s10639-020-10330-0

Yeng, P. K., Fauzi, M. A., & Yang, B. (2021). Assessing the effect of human factors in healthcare cyber security practice: An empirical study. *ACM International Conference Proceeding Series*, 472–476. https://doi.org/10.1145/3503823.3503909

Zaland, Z., Bazai, S. U., Marjan, S., & Ashraf, M. (2021). *"Three-Tier Password Security Algorithm for Online Databases*. https://doi.org/doi: 10.1109/IISEC54230.2021.9672434.