Journal of Technology and Value Addition, Volume 7 (2), July, 2025: (70-90)

Research Article

Cybersecurity Awareness among Undergraduates using Digital Platforms: A Case Study of the University of Sri Jayewardenepura

R.A.C. Nilakshi* and H.P.T.N. Silva

chamikaranathunga7@gmail.com

Department of Social Statistics, Faculty of Humanities and Social Sciences, University of Sri Jayewardenepura, Sri Lanka

Abstract

Recent technological advancements have enhanced information exchange, yet many remain vulnerable to cybersecurity threats due to low awareness. The lack of cybersecurity awareness is a growing issue in educational institutions, where the majority of undergraduates heavily rely on digital platforms, often failing to implement basic security practices, risking both personal and institutional data. This research aims to identify the factors influencing the level of cybersecurity awareness among undergraduates when using digital platforms. The data were collected using an online questionnaire with a random sample of 336 final-year undergraduates at the University of Sri Jayewardenepura, selected due to their impending entry into professional environments where cybersecurity is vital. The cybersecurity awareness level is assessed through three dimensions: prevention and precautions, cybercrimes and threats and their impacts. Data analysis was conducted using descriptive statistics, Chi-square tests and Structural Equation Modelling (SEM) via SPSS and SmartPLS. The results revealed that while students demonstrated a relatively high level of awareness regarding cybercrimes and their consequences, their awareness of preventive and precautionary practices was significantly lower. SEM findings indicated that digital skills, knowledge factors and cybersecurity attitudes have significant positive effects on overall awareness with digital skills emerging as the most influential factor. Although gender, faculty, and living sector influenced specific dimensions, these variables did not significantly moderate the overall structural relationships. The findings highlight a critical gap between understanding cybersecurity threats and adopting protective behaviors. This emphasizes the urgent need for educational institutions to implement skill-based training to improve preventive cybersecurity practices among undergraduates.

Keywords: *Cybersecurity, Cybersecurity Awareness, Digital Platforms, Digital Skills, Undergraduates*

1. Introduction

Modern technology's quick development has changed our way of life. As a result, both the social and business worlds have started to provide more services and adopt new technology to provide clients access to their data from any location, at any time. The number of hackers and organized cybercrime gangs have increased dramatically as a result of that. On average, 97 victims fall prey to cybercrimes every hour, and two internet users have their data leaked every second (Griffiths, 2023). This alarming trend highlights the pressing need for cybersecurity awareness, particularly among digitally active populations.

Cybersecurity awareness refers to an individual's understanding of cyber risks and their ability to take informed precautions to protect data and digital systems (ENISA, 2020). It encompasses knowledge of threats such as phishing, malware, ransomware, and social engineering, as well as safe digital practices including password hygiene, secure browsing, and software updates (Parsons *et al.,* 2017). During 2020-2023, the ratio of Internet users in Sri Lanka improved significantly, rising from 36 percent to 51 percent. By 2024, the rate of Internet users was around 56% (World Bank, 2024). In terms of the status of cyber security in the country, Sri Lanka was ranked 83rd out of 182 countries in terms of Global Cybersecurity Index (GCI) which is a trusted reference that measures the commitment of countries to cybersecurity at a global level (International Telecommunication Union, 2021).

Despite GCI rank of the country, incidents reported to Sri Lanka Computer Emergency Readiness Team (CERT) which occurred due to the lack of cyber security awareness have increased to 20,628 in the year 2023. In the year 2022, 16,301 incidents were reported. This is nearly a 26.54% increase in reported incidents compared to the year 2022 (Sri Lanka CERT, 2023). Sri Lanka CERT receives a variety of incidents such as involving social networks, emails compromise, phishing attacks, websites compromise, scams, privacy violations, financial frauds, etc. There has been a significant increase in social media related matters which occurred due to lack of cyber security awareness during the year of 2023. Out of a total of 20,628 reported incidents, 20,219 were related to social media (Sri Lanka CERT, 2023). According to the statistics of Sri Lanka CERT, lack of cyber security awareness has become a serious problem in the country.

In the meantime, the COVID-19 epidemic has urged educational institutions to give instruction using internet technology. Many software required for online learning are not free to download and use. Many pirated software violations in higher education have been found in supporting their activities by campus officials, educators, teaching staff and students (Omar *et al.,* 2019). While these technologies

were provided for free, they nonetheless offer several hazards to user's privacy and personal information, primarily in the form of hacking, malware, cyberbullying, phishing, online scams, ransomware, and identity theft. While raising awareness about cyber security is crucial, it is especially important to focus on university students.

University students are considered a vulnerable group in the digital space. As heavy users of online platforms for communication, learning, and collaboration, they are frequently targeted by cybercriminals (Agrafiotis *et al.,* 2021). Despite increasing digital activity among Sri Lankan students, there remains a lack of empirical research on their cybersecurity awareness. Key concepts such as digital literacy, defined as the ability to critically engage with digital technologies in a safe and responsible manner (UNESCO, 2018), are not adequately examined in local academic contexts. As a leading national institution, its student population reflects a critical segment of Sri Lanka's digitally engaged youth. Understanding their awareness levels and digital behaviors will provide insights for shaping effective cybersecurity education strategies in Sri Lankan higher education.

In view of the context, this paper explores the cyber security awareness level of undergraduates using digital platforms and affecting factors to it through a sample of University of Sri Jayewardenepura.

1.1. Objectives

The main objective of the study will be achieved through the following specific objectives.

1. To measure the cyber security awareness level of undergraduates using digital platforms.
2. To compare the differences in the cyber security awareness level using digital platforms among selected facilities: faculty of humanities and social sciences and faculty of applied sciences, faculty of management studies & commerce and faculty of medical sciences.
3. To discover the differences in the cyber security awareness level using digital platforms among gender of the students: male, female
4. To uncover the differences in the cyber security awareness using digital platforms among the living sector of students: urban, semi urban, rural.
5. To identify the main factor impacting on the difference level of cyber security awareness of undergraduates using digital platforms

2. Literature Review

Under the review of this empirical literature, the empirical evidence on the cyber security awareness level is reviewed.

2.1. Demographic Factors

In this research, four criteria of demographic profiles are examined which are gender, age, living sector faculty and purchase online. The study carried out by Garba *et al.,* (2020) identified females as more likely to become victims of a cybersecurity attack in Nigeria. Another survey investigated the cybersecurity awareness in Zimbabwean universities from the perspectives of the students by Matyokurehwa *et al.,* (2020). The findings reveal that there were no differences on gender and age on cyber security awareness while there were differences on education level and institution on cyber security awareness. The research carried out by Nallainathan (2021) focused on study among rural area citizens in Sri Lanka regarding cyber security awareness and factors relating to it. In conclusion of the study, the overall applicability of cyber security principles was still quite low.

2.2. Digital Inequalities Factors

Digital Skills and frequency of internet use are the two criteria which are examined under the Digital Inequalities profile. Deursen *et al.* (2016) conducted research by developing a reliable instrument based on a strong conceptual framework, measuring five types of internet skills: operational, informational navigation, social, creative, and mobile. Dodel *et al.* (2020) extended this research in Uruguay, investigating cyber-safety behaviors. Digital inequalities were measured on two different levels: frequency of Internet use through a cellphone and digital skills. Both were measured through a Likert-scale question and Digital skills were measured using Internet Skills Scale (ISS) which was developed and validated by Deursen *et al.,* (2016) through eight items concerned with creative, operational, and social online abilities.

2.3. Knowledge Factors

Under the knowledge profile, cybersecurity knowledge and browser security awareness are key considerations. Kovacevic *et al.* (2020) found that knowledge is a dominant factor influencing cybersecurity behavior. Despite being digital natives, many students lacked the knowledge and confidence to protect themselves online. Similarly, Alharbi and Tassaddiq (2021), in a study at Majmaah University in Saudi Arabia, found that students' cybersecurity and browser security knowledge were

insignificant in predicting awareness levels. Onyema *et al.* (2021) surveyed undergraduates and reported that while students had basic knowledge of cybersecurity, their understanding of protection strategies was limited. Most participants were aware of threats like viruses, phishing, spamming, identity theft, spoofing, and hacking, but lacked practical skills to mitigate them.

2.4. Social Network Activities

Alharbi and Tassaddiq (2021) conducted research regarding the cyber security awareness among students of Majmaah University in Saudi Arabia. According to the results of this study, social networking enhanced cybersecurity awareness, observed that only 14.2% of the respondents were aware of the cybersecurity issues encountered through social networking and positively influenced the awareness level of the respondents about cyber threats. The study on the factors impacting university students' cybersecurity awareness was carried out by Alqahtani (2022) at Imam Abdulrahman Bin Faisal University in Saudi Arabia. Social media activities were one of the key areas of this study. According to the results, the social media activities positively and significantly affect cybersecurity awareness.

2.5. Password Management

Nallainathan (2021) studied cybersecurity awareness among rural citizens in Vavuniya, Sri Lanka, and found weak password management practices. Over half of the respondents reused passwords across multiple accounts, and 15% used passwords with fewer than eight characters, increasing vulnerability to brute-force attacks. Similarly, Alqahtani (2022) examined cybersecurity awareness among university students at Imam Abdulrahman Bin Faisal University in Saudi Arabia. The study revealed that students exhibited low levels of cybersecurity awareness, particularly in password security. These findings highlight widespread deficiencies in basic password practices.

2.6. Cyber Security Attitudes

Chandarman and Niekerk (2017) studied cybersecurity awareness among students at a private tertiary institution in Durban. Students showed generally responsible attitudes, such as rejecting risky behaviors like disabling security settings, ignoring updates, or posting offensive content. However, many believed they wouldn’t receive

malware from friends, which could lead to unintentional threats. In contrast, Kamalulail *et al.* (2022) surveyed 201 individuals and found that attitude did not significantly influence cybersecurity awareness. Using multiple linear regression, the study revealed that the attitude factor had no statistical impact on awareness levels, suggesting attitudes alone may not predict secure online behavior.

2.7. Qualification in IT Field

Nallainathan (2021) investigated cybersecurity awareness among 320 rural households in Vavuniya, Sri Lanka. The study found that individuals who had studied ICT in school or through IT courses had better access to IT instructors, contributing to higher cybersecurity awareness. In contrast, older individuals who completed education before IT was introduced lacked such access, making them more vulnerable. Inter-variable analysis showed that younger populations demonstrated greater awareness and employed stronger cybersecurity practices. The findings suggest that formal IT education significantly enhances cybersecurity awareness and that a generational gap exists due to unequal exposure to digital literacy training.

2.8. Level of Cyber Security Awareness using Digital Platforms

Nagahawatta *et al.* (2020) assessed cybersecurity awareness among Sri Lankan university students through a questionnaire targeting various degree programs. The study found that while students demonstrated a moderate level of cybersecurity awareness and could recognize cybercrime as a threat, notable gaps remained, particularly in addressing emerging cyber risks. In Malaysia, Fatokun *et al.* (2020) explored social media safety awareness among youth and found overall awareness to be low. The correlation between social media usage and safety awareness was weak, indicating a lack of understanding of associated risks. Garba *et al.* (2022) investigated cybersecurity awareness among students in Northeastern Nigeria, finding high awareness regarding internet banking but only moderate awareness of issues such as cyberbullying and self-protection. Similarly, Raju *et al.* (2022) studied cybersecurity awareness at Universiti Teknologi MARA (UiTM), Terengganu. Although students were aware of common threats like cyberbullying and data privacy risks, many still engaged in unsafe behaviors such as password sharing and accessing untrusted websites. The findings across these studies highlight the need for deeper cybersecurity education.

3. Materials and Methods

3.1. Data

The study focused on 4th-year undergraduates from four faculties at the University of Sri Jayewardenepura: The Faculty of Humanities and Social Sciences, Management Studies and Commerce, Applied Sciences, and Medical Sciences. These students were chosen due to their frequent use of digital platforms and their upcoming transition into professional environments where cybersecurity practices will be crucial, making it important to assess their current level of cybersecurity awareness. A sample of 336 undergraduates, representing 13.50% of the population, was selected using stratified sampling to ensure equal faculty representation. Both primary and secondary data were utilized for the study. The researcher conducted a web-based survey, employing "Google Forms" as the method after conducting a pilot survey, enabling the selection of an unbiased sample within the university.

3.2. Research Model

In this study, the level of cyber security awareness is considered as the dependent variable and it measures through three dimensions which are prevention and precaution, crimes/threats and impact. The demographic factors, digital inequalities factors, knowledge factors, social network activities, password management, cyber security attitudes and qualification in IT are considered as the independent variables in the study (Figure 1).

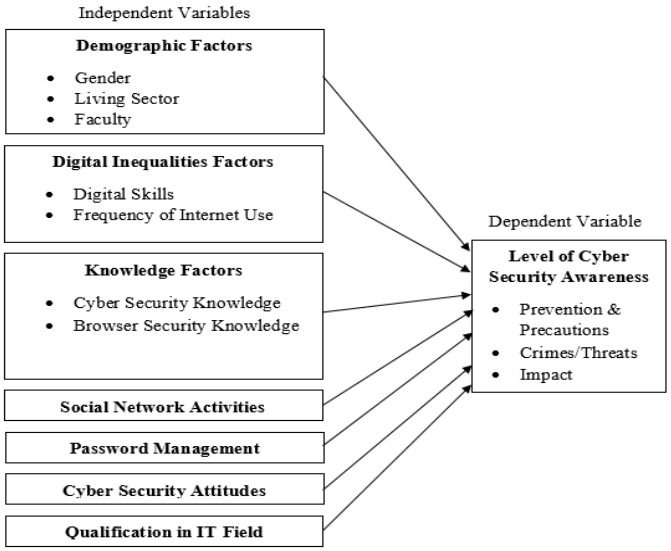

Figure 1: Conceptual framework of the study

3.3. Research Instrument

This study employed a quantitative research design using a structured questionnaire as the research instrument (Appendix 1) to assess cybersecurity awareness among undergraduates. The instrument consisted of four main sections: demographic factors, level of cybersecurity awareness, digital inequalities and knowledge, and privacy and confidentiality. The questionnaire was developed by the researchers and informed by validated frameworks and prior studies, including Deursen *et al.* (2016), Kovacevic *et al.* (2020), and Parsons *et al.* (2017). Items were adapted to suit the Sri Lankan university context and focused on digital behavior, risk awareness and cybersecurity knowledge. A pilot study was conducted with 30 undergraduate students to assess clarity, consistency, and reliability. Based on the feedback, minor revisions were made to improve item phrasing. Cronbach's alpha values exceeded 0.70, indicating acceptable internal consistency. The final questionnaire was distributed across selected faculties using stratified random sampling.

3.4. Methods

3.4.1. Sampling Method

This study adopted a stratified random sampling method to ensure representation across selected faculties at the University of Sri Jayewardenepura. Although the university comprises 11 faculties, the study focused on four: Management Studies and Commerce, Humanities and Social Sciences, Applied Sciences, and Medical Sciences, due to practical limitations related to time and cost. According to university records, the target population of 4th-year undergraduates across these faculties totaled 2,484. Using Cochran's formula, with a 95% confidence level, 5% margin of error, and an estimated population proportion of 0.5, the minimum required sample size was calculated to be 385**.** However, for practical implementation, equal allocation was used across the four strata (faculties), resulting in a final sample size of 336, with 84 respondents selected from each faculty. Equal allocation ensured balanced representation, regardless of faculty size, while maintaining the randomness of selection within each stratum.

Table 1: Equal Allocation to the Sample Size

Faculty	Number of 4th year undergraduates	**Allocated Proportion**
Management studies and commerce (FMSC)	1223	**84**
Humanities and Social Sciences (FHSS)	740	**84**
Applied Sciences (FAS)	351	**84**
Medical Sciences (FMS)	170	**84**
Total	2484	**336**

3.4.2. Data Analyzing Method

The dataset, using tables, pie charts, and bar charts to present distributions. Principal component analysis was applied to assess both overall and dimension-specific cybersecurity awareness levels while chi-square tests examined associations between independent and dependent variables. Structural Equation Modeling (SEM) was employed to explore complex relationships among multiple latent constructs such as digital skills, knowledge and attitudes measured through 1-5 Likert scale questions. SEM was selected for its ability to simultaneously assess measurement and structural models, offering a comprehensive evaluation of direct and indirect effects within the proposed theoretical framework. Analytical tools used included SPSS, Minitab, EViews, Excel, and SmartPLS.

The study's Structural Equation Modeling (SEM) focused on evaluating the measurement model, which examines relationships between 40 observed variables and 6 latent constructs: digital skills, knowledge factors, social network activities, password management, cybersecurity attitudes, and cybersecurity awareness (with dimensions of prevention and precaution, crimes/threats, and impact).

First, construct reliability and validity were assessed. Cronbach's alpha and composite reliability (Rho_c) for all constructs exceeded the threshold of 0.70, confirming internal consistency. Convergent validity was supported by outer loadings above 0.70, Rho_A, and average variance extracted (AVE) values above 0.50. Discriminant validity was confirmed using the Fornell-Larcker criterion, as the square root of AVE for each latent variable was greater than its correlations with other variables, indicating distinct constructs.

Collinearity analysis showed all variance inflation factor (VIF) values were below 5, indicating no multicollinearity issues. Goodness of fit indices included a

Standardized Root Mean Square Residual (SRMR) of 0.06 (below 0.10) and a Normed Fit Index (NFI) of 0.77, demonstrating acceptable model fit.

Based on the model, the following hypotheses were tested regarding factors impacting the cybersecurity awareness level of undergraduates using digital platforms:

- H01: Digital Skills have a significant positive impact on cybersecurity awareness.
- H02: Knowledge Factors have a significant positive impact on cybersecurity awareness.
- H03: Social Network Activities have a significant positive impact on cybersecurity awareness.
- H04: Password Management has a significant positive impact on cybersecurity awareness.
- H05: Cybersecurity Attitudes have a significant positive impact on cybersecurity awareness.

The validated SEM confirms that the constructs are reliable and valid, the model fits the data well, and there are no collinearity issues. These results support the theoretical framework and the proposed hypotheses, highlighting key factors influencing cybersecurity awareness among undergraduates.

4. Results

The descriptive analysis of the study revealed that a significant proportion of undergraduates in the selected faculties of the University of Sri Jayewardenepura were females, constituting 59.23%, and a majority of surveyed undergraduates reside in suburban areas.

Regarding qualifications in the IT field, 35.71% of respondents lacked any IT or IT-related qualification, while only 5.06% possessed a Bachelor's degree in IT/IT-related fields. Given the study's focus on the use of digital platforms, understanding user experiences and utilization was crucial. The results indicated that digital platforms such as WhatsApp, Facebook, Instagram, and YouTube had the highest user engagement among the surveyed undergraduates.

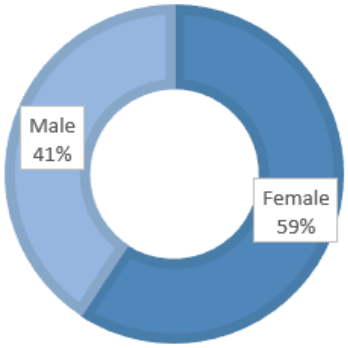

Figure 2: Composition of respondents based on gender

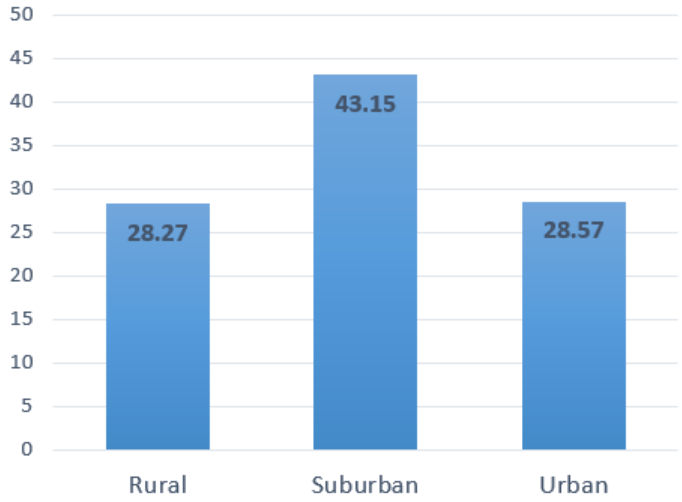

Figure 3: Composition of the respondents based on living sector

The research successfully achieved the sub-objective of estimating the cyber security awareness level among undergraduates. The overall cyber security awareness level was found to be relatively high, averaging 76.65%. To delve deeper into the research problem, each dimension under overall cyber security awareness was separately measured. The analysis revealed that awareness levels in the dimensions of impact and crimes/threats were relatively high, with means of 76.72 and 75.26, respectively. However, awareness in the dimension of prevention and precaution was notably lower, with a mean of 42.71. This suggested that while undergraduates generally

possessed a considerable awareness of cybercrimes/threats and their consequences using digital platforms, there was a relatively lower awareness of preventive practices associated with digital platform use.

Table 2: Descriptive Summary of Cybersecurity Awareness

Descriptive Summary Statistics	Overall Cybersecurity Awareness	Prevention and Precaution	Cybercrimes/ Threats	Impact
Mean	76.67	42.71	75.26	76.72
Standard Deviation	18.45	23.85	21.09	20.15
Skewness	-1.06	0.31	-0.98	-0.91
Kurtosis	1.79	-0.73	1.26	0.87

The chi-square test results revealed that only awareness of crimes/threats is influenced by the gender of undergraduates. Additionally, the living sector significantly impacted overall cyber security awareness and prevention and precaution awareness among undergraduates. Notably, urban sector undergraduates exhibited higher mean scores, averaging 81.03, for overall cyber security awareness and its individual dimensions, while rural sector undergraduates had the lowest mean scores, averaging 72.10 for overall cyber security awareness and each corresponding dimension.

Table 3: Relationship between Qualification in IT and Overall Cyber Security Awareness Level

Test	Overall Cyber Security Awareness Level	Prevention and Precaution	Crimes/ Threats	Impact
Pearson Chi-Square	30.61	74.36	27.82	35.98
	(0.01)	(0.00)	(0.03)	(0.00)
Likelihood Ratio	31.52	79.38	30.08	38.02
	(0.01)	(0.00)	(0.01)	(0.00)
Linear-by-Linear	11.12	23.91	5.26	10.29
Association	(0.00)	(0.00)	(0.02)	(0.00)
N of Valid Cases	336	336	336	336

According to table 3, p-values of overall cyber security awareness (0.01), prevention and precaution awareness (0.00), crimes/threats awareness (0.03) and impact awareness (0.00) clearly indicate that p-values are significant which can be

concluded in 95% confidence that there is a relationship between qualification in IT field and overall cyber security awareness, prevention and precaution awareness, crimes/threats awareness and impact awareness. It implies that not only overall cyber security awareness level, its each dimension is also impacted by the undergraduates' qualification in the IT field.

The research aimed to identify factors influencing the cyber security awareness level of undergraduates using digital platforms, considering digital skills, knowledge factors, social network activities, password management, and cyber security attitudes as key factors. Structural equation modeling revealed that digital skills, knowledge factors, and cyber security attitudes significantly and positively impacted the overall cyber security awareness level.

Table 4: Results of Path Coefficients of the SEM

Path	Original sample (β)	Sample mean	Standard deviation	T statistics	P values
Digital Skills -> Cyber Security Awareness	0.36	0.36	0.06	5.62	0.00
Knowledge Factors -> Cyber Security Awareness	0.28	0.28	0.06	4.29	0.00
Social Network Activities -> Cyber Security Awareness	0.04	0.04	0.04	1.10	0.26
PAS_MAN_ -> Cyber Security Awareness	0.07	0.07	0.04	1.70	0.08
CYS_ATT_ -> Cyber Security Awareness	0.17	0.17	0.06	2.94	0.00

Table 4 summarizes the direct effects of key factors on overall cybersecurity awareness. Digital skills ($\beta = 0.36$, $p < 0.00$), knowledge factors ($\beta = 0.28$, $p < 0.00$), and cybersecurity attitudes ($\beta = 0.17$, $p = 0.00$) demonstrated statistically significant positive relationships, thereby supporting hypotheses H01, H02, and H05. In contrast, social network activities ($\beta = 0.04$, $p = 0.26$) and password management ($\beta = 0.07$, $p = 0.08$) exhibited positive but statistically insignificant effects, leading to the rejection of hypotheses H03 and H04. These results suggest that digital skills, knowledge, and attitudes are key determinants of cybersecurity awareness among undergraduates.

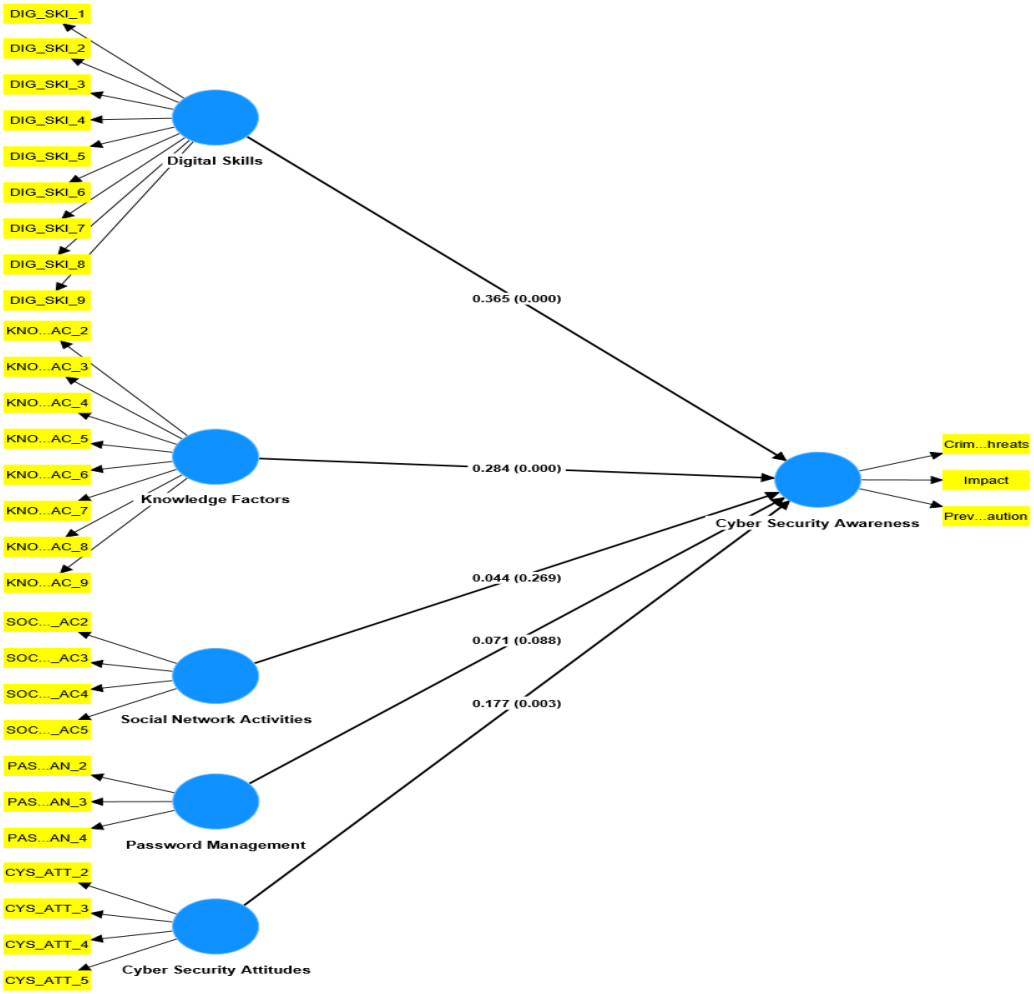

Figure 4: Structural model illustrating key factors influencing overall cybersecurity awareness

To visually represent the interrelationships among the latent constructs, a correlation matrix (Figure 5) was developed based on the Fornell–Larcker criterion values presented in Appendix B1. The correlation matrix illustrates the relationships among the six latent constructs considered in the study. The diagonal elements represent the square roots of the Average Variance Extracted (AVE) for each construct, while the off-diagonal values indicate the inter-construct correlations. As shown in Figure 5, Digital Skills and Cybersecurity Awareness (r = 0.64) exhibit the strongest correlation, followed by Cybersecurity Attitudes (r = 0.52). Social Network Activities show the weakest associations with other variables (r = 0.23-0.38). These findings confirm discriminant validity and suggest that while the constructs are related, each measures a distinct dimension of cybersecurity awareness.

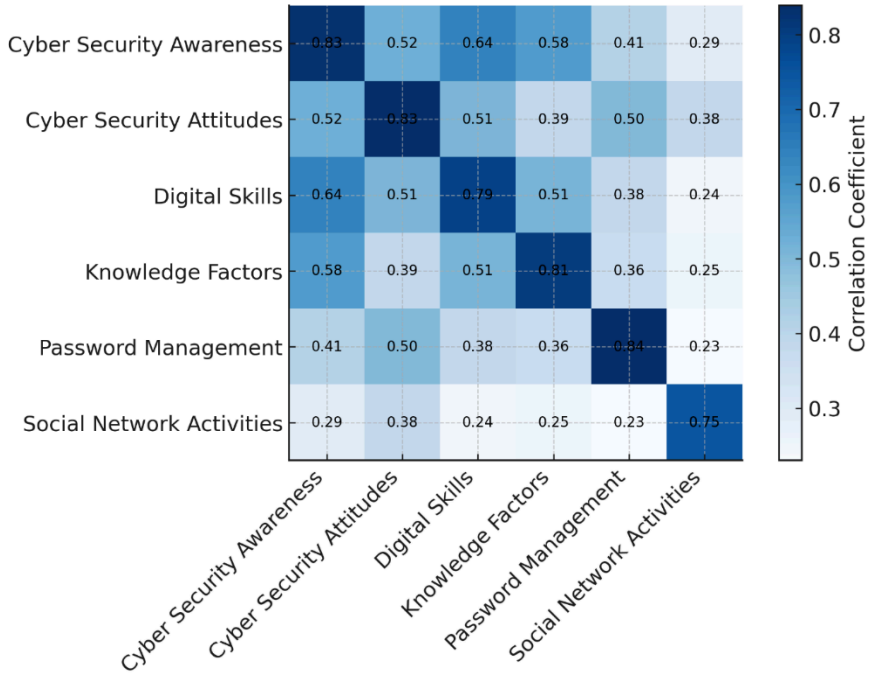

Figure 5: Correlation Matrix of latent constructs

Further analysis, focusing on prevention and precaution, crimes/threats awareness, and impact awareness, indicated that digital skills and knowledge factors consistently influence all dimensions. Password management solely impacted prevention and precaution awareness, while cyber security attitudes impacted all dimensions except prevention and precaution. Upon evaluating all executed structural models, it was evident that the independent variable of digital skills emerges as the primary factor influencing overall cyber security awareness, as well as awareness in crimes/threats and impact. Strong digital skills among undergraduates correlated with higher levels of cyber security awareness, indicating that an improvement in digital skills was likely to enhance overall awareness.

Further research aimed to examine how these factors interact with the latent variables in the model and shedding light on their moderating effects by remodeling the existing model to incorporate faculty, gender and living sector of the students as moderators. According to Figure 6, P-values clearly indicate gender, faculty and

living sector as moderators are not significant for any of the relationships in the model.

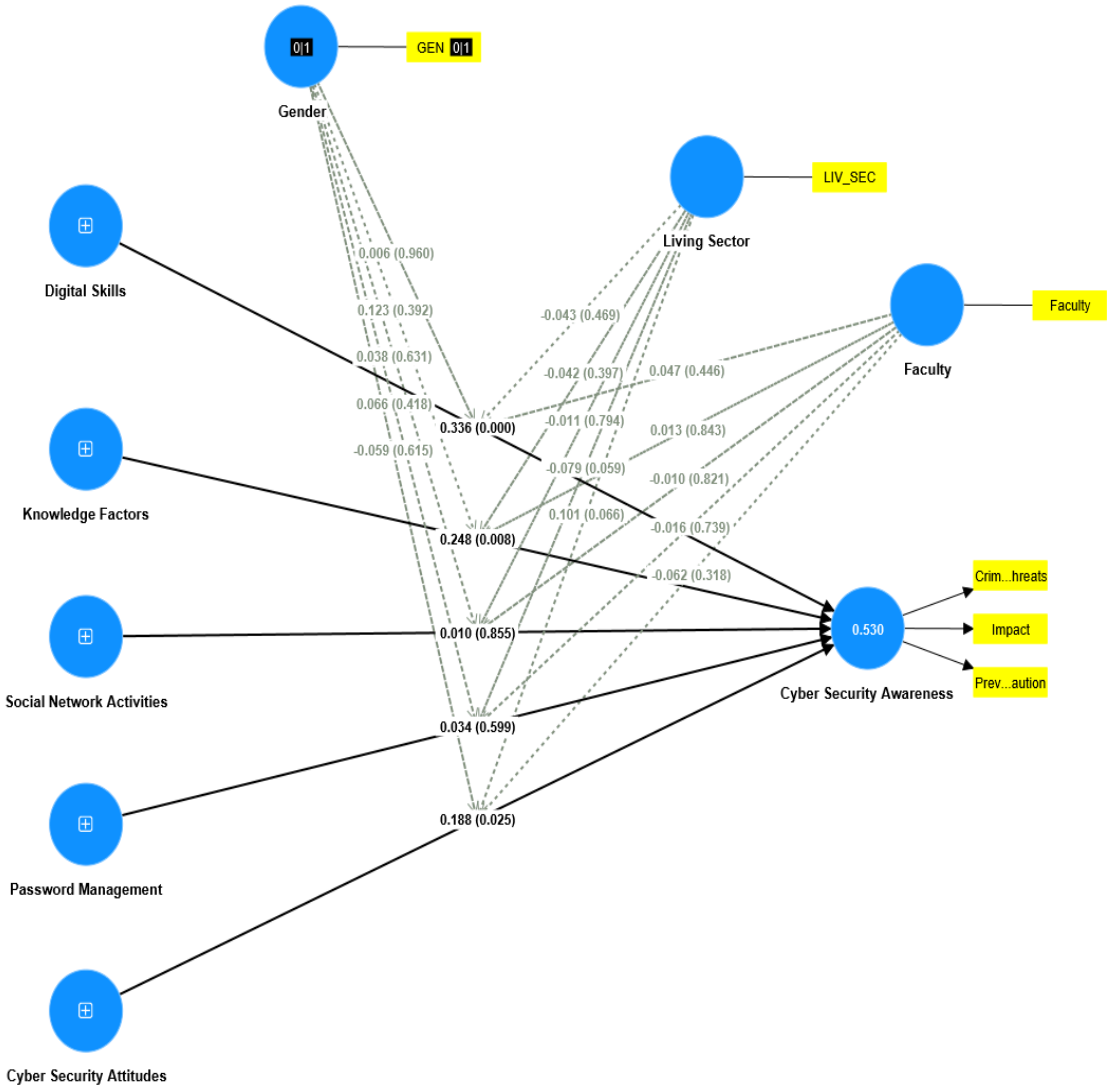

Figure 6: Existing model after incorporating Faculty, Gender and Living sector as moderators

5. Discussion

This study assessed the cybersecurity awareness levels of undergraduates at the University of Sri Jayewardenepura and explored the influence of digital skills,

knowledge factors, social network activities, password management, and cyber security attitudes using digital platforms.

Descriptive results showed minor differences in cybersecurity awareness across living sectors, with urban students scoring higher. However, the structural model found no significant effects for gender, faculty, or living sector, aligning with Matyokurehwa *et al.* (2020) but differing from Garba *et al.* (2020), who reported greater female vulnerability. These findings suggest increasing digital accessibility in Sri Lanka. Notably, students with IT qualifications demonstrated significantly higher awareness across all dimensions, supporting the view that formal IT education enhances digital competence and confidence.

Further, results revealed that while the overall cybersecurity awareness level was relatively high, students demonstrated notably low awareness in the dimension of prevention and precaution. This finding mirrors Onyema *et al.* (2021) and Kovacevic *et al.* (2020), who observed that although university students often possess baseline awareness of threats such as phishing, spamming, and hacking, they frequently lack the practical knowledge to implement protective behaviors. This suggests the awareness-action gap where students recognize risks but fail to adopt preventive measures likely due to insufficient training or a lack of perceived relevance.

Digital skills identified as the most influential factor of cybersecurity awareness, confirming the work of Deursen *et al*. (2016) and Dodel *et al.* (2020), who emphasized the critical role of digital competencies in cyber-safety behaviors. In a broader technological context, digital skills enable users not only to interact safely with platforms but also to navigate browser security settings, recognize phishing patterns and manage app permissions effectively. However, the digital skills assessed in this study were based on self-perception and general abilities.

Contrary to prior studies, password management and social network activities did not significantly influence cybersecurity awareness in this research. This contradicts findings by Alqahtani (2022) and Nallainathan (2021), who reported weak password practices and risky social media behaviors as major vulnerabilities among students. This difference may be due to people becoming too used to or relying too much on technology, like autofill, biometric logins, or security warnings. These tools can give a false sense of safety, showing the need for efforts that encourage users to be more

actively involved in protecting their personal information. Cybersecurity knowledge and attitudes had significant positive effects on cybersecurity awareness, aligning with previous studies. However, low scores in prevention and precaution dimension highlight a shortfall in applying knowledge and positive attitudes to real-world practices.

6. Conclusion

This study examines the key factors affecting cybersecurity awareness among undergraduates using digital platforms. While overall cybersecurity awareness level is relatively high, undergraduates show a significant gap in applying preventive measures. Digital skills, knowledge, and positive cybersecurity attitudes were found to significantly enhance awareness, highlighting the importance of both technical ability and mindset. In contrast, behaviors like poor password practices and risky social network activities did not show a strong connection to cybersecurity awareness, possibly due to overdependence on automated security features.

To address these gaps, the study recommends incorporating practical cybersecurity training into all undergraduate programs, focusing on real-life scenarios. National digital literacy initiatives should also be introduced, specifically targeting the students without IT backgrounds and those in non-urban areas. Developers are encouraged to build more user-friendly and interactive security tools such as password strength indicators, phishing alert systems and gamified learning modules.

However, the study is limited by its focus on a single institution and depends on self-reported data. Future research should expand to multiple institutions. Overall, the findings highlight the importance of a combined effort from education, policy and technology to improve cybersecurity awareness and create a safer digital environment for undergraduates.

7. Acknowledgment

The authors wish to express their sincere gratitude to the University of Sri Jayewardenepura for providing the necessary academic environment and resources to conduct this study. Special appreciation is extended to the academic staff for their valuable guidance, constructive feedback, and continuous support throughout the research process. The authors also gratefully acknowledge the participation of the final-year undergraduates, whose cooperation and willingness to contribute were vital to the successful completion of this study. Finally, the authors would like to

thank their families, colleagues, and mentors for their unwavering encouragement and support, which greatly contributed to the realization of this research.

8. References

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., and Upton, D. (2021). Cyber harm: Concepts, taxonomy and measurement. Journal of Cybersecurity, 7(1), pp.17. https://doi.org/10.1093/cybsec/tyy006

Alharbi, T. and Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. Big Data and Cognitive Computing, 5(2), pp.23.

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*, 12(5), pp.2589-2595.

Chandarman, R. and Niekerk, V. B. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. *The African Journal of Information and Communication (AJIC)*, *20*(3), pp. 25-29.

Deursen, A. J. A. M., Helsper, E. J., and Eynon, R. (2016). Development and validation of the Internet Skills Scale (ISS). *Information, Communication and Society*, *19*(6), pp. 804-823.

Dodel, M., Kaiser, D., and Mesch, G. (2020). Determinants of cyber-safety behaviors in a developing economy: *The role of socioeconomic inequalities, digital skills and perception of cyber-threats.* 25(3), pp-7-9.

ENISA. (2020). *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity* [online]. Available from: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity [accessed 21 June 2025].

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *Journal of Physics: Conference Series*, *1339*(1), 012098. https://doi.org/10.1088/1742-6596/1339/1/012098

Garba, A. A., Siraj, M. M., and Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. *International Journal of Electrical and Computer Engineering (IJECE)*, *12*(1), pp.572-581.

Garba, A. A., Siraj, M., Othman, S. H., and Musa, M. A. (2020). A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria. *International Journal on Emerging Technologies.* 11(5): pp. 41-49.

Griffiths, C. (2023). AAG IT Services [online]. Available from: https://aag-it.com/the-latest-cyber-crime-statistics/ [accessed 25 March 2023].

International Telecommunication Union. (2021). *Global Cybersecurity Index (GCI) 2020*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx [accessed 21 June 2025].

Kamalulail, A., Abdul Razak, N. E. N., Omar, S. A., and Mohamed Yusof, N. (2022). Awareness of Cybersecurity: A Case Study in UiTM Negeri Sembilan Branch, Seremban Campus. *E-Academia Journal*, *11*(1), pp. 18266-18275.

Matyokurehwa, K., Rudhumbu, N., Gombiro, C., and Mlambo, C. (2021). Cybersecurity awareness in Zimbabwean universities: Perspectives from the students. *Security and Privacy*, *4*(2), pp. 141-149.

Nagahawatta, R. T. S., Warren, M., & Yeoh, W. (2020). A Study of Cyber Security Issues in Sri Lanka. *International Journal of Cyber Warfare and Terrorism,* 10(3), pp. 59-72. DOI: 10.4018/IJCWT.2020070105

Nallainathan, S. (2021). Study among Rural area citizens regard to Cyber Security awareness and Factors relating to it. *International Journal Of Engineering Development And Research, 9*(1), pp. 322-326.

Omar N. A., Zakuan Z. Z., and Saian R., Software Piracy Detection Model Using Ant Colony Optimization Algorithm. *Journal of Physics: Conference Series*, 855, pp. 012031. doi: 10.1088/1742-6596/855/1/012031.

Onyema, E. M., Edeh, C. D., Gregory, U. S., Edmond, V. U., Charles, A. C., and Richard-Nnabu, N. E. (2021). Cybersecurity Awareness Among Undergraduate Students in Enugu Nigeria. *International Journal of Information Security*, *5*(1), pp. 34-42.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, 42, pp. 165–176.

Raju, R., Abd Rahman, N. H., & Ahmad, A. (2022). Cyber security awareness using digital platforms among students in a higher learning institution. *Asian Journal of University Education, 18*(3), pp. 756–766.

Sri Lanka CERT|CC. (2023). *Annual activity report* (23rd ed.). The National CERT. Availablefrom:https://www.cert.gov.lk/wpcontent/uploads/annual_reports/Annual%20Report%202023.pdf [accessed 14 July 2024].

UNESCO Institute for Statistics. (2018). A global framework to measure digital literacy. *UNESCO* [online]. Available from: https://uis.unesco.org/en/blog/global-framework-measure-digital-literacy [accessed 21 June 2023].

World Bank. (2024). *Individuals using the Internet (% of population) - Sri Lanka* [online].Available:https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2024andmost_recent_year_desc=falseandstart=2020 [accessed 21 June 2024]

Appendices

Appendix A

Table A1: Content of the Questionnaire

Section & Topic	Content	Code
Part 1 Demographic Factors	Gender of the Respondent	GEN
	Age of the Respondent	AGE
	District where Respondent lives	DIS
	Living Sector of the Respondent	LIV_SEC
	Nearest Town	NEA_TOW
	Faculty of the Respondent	FAC
	Department of the Respondent	DEP
	IT/IT related highest qualification (Completed/following)	IT_HIG_QUA
	How does Respondent come to the university	HOW_COM_UNI
Part 2 Level of Cyber Security Awareness	Level of Cyber Security Awareness	LEV_CYB_SEC
	What is meant by " Cyber Security"	LEV_CYS_1
	Using digital platforms is a giving up rights to digital platforms providers to use my personal data	LEV_CYS_2
	When adding new friends to social media, it is better to inspect their background	LEV_CYS_3
	When making online purchases, it is better to inspect the seller's background	LEV_CYS_4
	Criticize someone harmfully through social media is a cyberbullying	LEV_CYS_5
	Clicking suspicious links and online advertisements can be a type of cyber attack	LEV_CYS_6
	Getting sensitive information illegally from someone is a hacking	LEV_CYS_7
	Personal images can be misused when uploading them into digital platforms	LEV_CYS_8
	Financial lost can be occurred when providing banking details without checking its authenticity	LEV_CYS_9

	Digital devices can be damaged when downloading digital media (music, games, films) from unlicensed sources	LEV_CYS_10
	Sri Lanka Computer Emergency Readiness Team (CERT) is the legal institution for report cyber security incidents	LEV_CYS_11
	How to report a cyber-security incident to get a legal action	LEV_CYS_12
Part 3 Digital Inequalities and Knowledge Factors	On average, how much hours do you spend at internet per day (Please give only number eg: 2 or 2.5) ?	HOU_SPE_INT
	Normally, how much data amount in GB do you consume within a month	GB_AMO_CON
	The digital platforms you have being using or have used: Facebook	DIG_PLA_FB
	The digital platforms you have being using or have used: Instagram	DIG_PLA_INS
	The digital platforms you have being using or have used: Whatsapp	DIG_PLA_WHA
	The digital platforms you have being using or have used: Linkdin	DIG_PLA_LIN
	The digital platforms you have being using or have used: Moodle	DIG_PLA_MOO
	The digital platforms you have being using or have used: Quora	DIG_PLA_QUO
	The digital platforms you have being using or have used: Youtube	DIG_PLA_YOU
	The digital platforms you have being using or have used: Spotify	DIG_PLA_SPO
	The digital platforms you have being using or have used: Amazon	DIG_PLA_AMA
	The digital platforms you have being using or have used: AliExpress	DIG_PLA_ALI
	The digital platforms you have being using or have used: Other	DIG_PLA_OTH
	If there are any other digital platforms you have being using or have used, mention it here.	DIG_PLA_OTH_USE
	The device do you mostly use in order to access internet	DEV_MOS_USE

	The place do you mostly use to access internet	PLA_MOS_USE
	Digital Skills	DIG_SKI
	I know how to download and upload files/photos/videos	DIG_SKI_1
	I know how to adjust privacy settings	DIG_SKI_2
	I know how to use shortcut keys	DIG_SKI_3
	I know which information I should and shouldn't share online	DIG_SKI_4
	I know how to change who I share content with	DIG_SKI_5
	I know how to remove friends from my contact lists	DIG_SKI_6
	I know how to edit a photograph	DIG_SKI_7
	I know how to make and edit a video	DIG_SKI_8
	I know how to write a comment on a blog, website or a forum	DIG_SKI_9
	Knowledge Factors	KNO_FAC
	Main cyber security concept of CIA triad (Confidentiality, integrity, availability)	KNO_FAC_1
	Use of antivirus software	KNO_FAC_2
	Software updates can prevent security vulnerabilities	KNO_FAC_3
	Cyber security threats (Eg:- Malware attacks, social-engineering attacks...)	KNO_FAC_4
	Risks on social media (Eg:- Cyberbullying, cyberstalking, privacy concerns)	KNO_FAC_5
	Updating web browser can keep the device safe and secure	KNO_FAC_6
	Avoiding installing extensions from third party websites is a cyber-security prevention	KNO_FAC_7
	Checking security settings and configurations of the web browser periodically ensures the secure	KNO_FAC_8
	Checking browser history and find suspicious activities help to keep safe browsing	KNO_FAC_9
	It is not OK to publish private photographs on digital platforms	SOC_NET_AC1

Part 4 Privacy and Confidentiality	Accepting invitations from outsiders seems not OK	SOC_NET_AC2
	There is a concern with openly posting one's present location on digital platforms	SOC_NET_AC3
	There is a problem with adding all personal information to digital platforms	SOC_NET_AC4
	There is a problem with online banking and purchasing items from digital platforms	SOC_NET_AC5
	I select a password with least 12 characters, numbers and symbols	PAS_MAN_1
	I change my password periodically	PAS_MAN_2
	I usually do not use previously used passwords	PAS_MAN_3
	I use different passwords for different accounts	PAS_MAN_4
	I do not share my passwords with others	PAS_MAN_5
	My friends would not send me anything malicious or scams through email	CYS_ATT_1
	Even updating my security software is too time consuming, it is important	CYS_ATT_2
	Even the security settings and tools slow me down, I do not disable them because they're important	CYS_ATT_3
	Even it is a waste of time to change passwords, you can still be safe	CYS_ATT_4
	It is not OK to download digital media (music, films, games) from any website	CYS_ATT_5
	Give our opinions and suggestions that can increase the level of cyber security awareness among undergraduates	OPI_CYS_AWA

Table A2: Variable for measuring Level of Cyber Security Awareness

Construct	Dimension	Statement	Variable
Level of Cyber	Prevention & Precaution	What is meant by " Cyber Security"	LEV_CYS_1

Security Awareness			
		Using digital platforms is a giving up rights to digital platforms providers to use my personal data	LEV_CYS_2
		When adding new friends to social media, it is better to inspect their background	LEV_CYS_3
		When making online purchases, it is better to inspect the seller's background	LEV_CYS_4
		Sri Lanka Computer Emergency Readiness Team (CERT) is the legal institution for report cyber security incidents	LEV_CYS_11
		How to report a cyber-security incident to get a legal action	LEV_CYS_12
	Crimes/ Threats	Criticize someone harmfully through social media is a cyberbullying	LEV_CYS_5
		Clicking suspicious links and online advertisements can be a type of cyber attack	LEV_CYS_6
		Getting sensitive information illegally from someone is a hacking	LEV_CYS_7
	Impact	Personal images can be misused when uploading them into digital platforms	LEV_CYS_8
		Financial lost can be occurred when providing banking details without checking its authenticity	LEV_CYS_9
		Digital devices can be damaged when downloading digital media (music, games, films) from unlicensed sources	LEV_CYS_10

Table A3: Variable for measuring Digital Skills

Construct	Statement	Variable
Digital Skills	I know how to download and upload files/photos/videos	DIG_SKI_1
	I know how to adjust privacy settings	DIG_SKI_2
	I know how to use shortcut keys	DIG_SKI_3
	I know which information I should and shouldn't share online	DIG_SKI_4

	I know how to change who I share content with	DIG_SKI_5
	I know how to remove friends from my contact lists	DIG_SKI_6
	I know how to edit a photograph	DIG_SKI_7
	I know how to make and edit a video	DIG_SKI_8
	I know how to write a comment on a blog, website or a forum	DIG_SKI_9

Table A4: Variable for measuring Knowledge Factors

Construct	Statement	Variable
Knowledge Factors	Main cyber security concept of CIA triad (Confidentiality, integrity, availability)	KNO_FAC_1
	Use of antivirus software	KNO_FAC_2
	Software updates can prevent security vulnerabilities	KNO_FAC_3
	Cyber security threats (Eg:- Malware attacks, social-engineering attacks...)	KNO_FAC_4
	Risks on social media (Eg:- Cyberbullying, cyberstalking, privacy concerns)	KNO_FAC_5
	Updating web browser can keep the device safe and secure	KNO_FAC_6
	Avoiding installing extensions from third party websites is a cyber-security prevention	KNO_FAC_7
	Checking security settings and configurations of the web browser periodically ensures the secure	KNO_FAC_8
	Checking browser history and find suspicious activities help to keep safe browsing	KNO_FAC_9

Table A5: Variable for measuring Social Network Activities

Construct	Statement	Variable
Social Network Activities	It is not OK to publish private photographs on digital platforms	SOC_NET_AC1
	Accepting invitations from outsiders seems not OK	SOC_NET_AC2
	There is a concern with openly posting one's present location on digital platforms	SOC_NET_AC3

	There is a problem with adding all personal information to digital platforms	SOC_NET_AC 4
	There is a problem with online banking and purchasing items from digital platforms	SOC_NET_AC 5

Table A6: Variable for measuring Password Management

Construct	Statement	Variable
Password Management	I select a password with least 12 characters, numbers and symbols	PAS_MAN_1
	I change my password periodically	PAS_MAN_2
	I usually do not use previously used passwords	PAS_MAN_3
	I use different passwords for different accounts	PAS_MAN_4
	I do not share my passwords with others	PAS_MAN_5

Table A7: Variable for measuring Cyber Security Attitudes

Construct	Statement	Variable
Cyber Security Attitudes	My friends would not send me anything malicious or scams through email	CYS_ATT_1
	Even updating my security software is too time consuming, it is important	CYS_ATT_2
	Even the security settings and tools slow me down, I do not disable them because they're important	CYS_ATT_3
	Even it is a waste of time to change passwords, you can still be safe	CYS_ATT_4
	It is not OK to download digital media (music, films, games) from any website	CYS_ATT_5

Appendix B

Table B1: Fornell Larcker criterion of the model

Construct	Cyber Security Awareness	Cyber Security	Digital Skills	Knowledge Factors	Password Management	Social Network

		Attitudes				Activities
Cyber Security Awareness	**0.832**					
Cyber Security Attitudes	0.524	**0.835**				
Digital Skills	0.638	0.506	**0.791**			
Knowledge Factors	0.576	0.385	0.511	**0.807**		
Password Management	0.412	0.499	0.379	0.364	**0.839**	
Social Network Activities	0.289	0.384	0.243	0.252	0.23	**0.747**