An Exploration of Students' Cyber Threats Perception in the Digital Age

D Mothisi*[1], M Mujinga[2]

[1,2]School of Computing, University of South Africa

E-mail: 33570353@mylife.unisa.ac.za[1], mujinm@unisa.ac.za [2]

Abstract. This study aims to investigate cyber threat awareness among students from a rural-based university and propose a model to enhance their awareness. Students rely on information and communication technologies (ICTs) for educational and personal activities. Students in rural areas may have less cybersecurity education and awareness than their urban counterparts. This can affect their awareness of malware, social engineering, and other cyber threats. It also heightens the challenges students face in mitigating security breaches. Data was collected using a survey to assess students' awareness of cyber threats. This assisted in determining students' knowledge, attitude, and behaviour (KAB) when engaged in online activities. The results indicated that less than 20 per cent of the students are aware of threats like Trojan horses, phishing, and keyloggers. The limited awareness of these threats could negatively impact students' ability to protect their information resources. It is recommended that rural-based students are continuously made aware of cyber threats. This study proposes the student online threat awareness model (SOTAM) to enhance cyber threat awareness among students.

Keywords: Attitude; Awareness; Behaviour; Cybersecurity; Cyber threats.

1. Introduction

The number of students using information and communication technologies (ICTs) is increasing. Mobile devices contribute to the high number of students using the internet because they do not require additional hardware to be online, provided they have network connectivity and data [1]. Technological inventions offer internet users benefits such as cost-saving and convenience. Teleconferencing applications enable people to have real-time online meetings irrespective of their geographical location. Students can attend daily lectures online using applications such as Microsoft Teams and Zoom in the comfort of their homes or university residences, eliminating travelling expenses. The internet has enabled online transactions such as money transfers from one bank account to another. Online shopping, e-learning, and social media interactions are some of the activities conducted by students online. The benefits of using the internet are sometimes offset by drawbacks associated with cyber threats [2]. Social networking platforms connect people online, enabling them to share ideas worldwide. They also support professional networking and allow individuals to engage with others based on shared interests. However, social networking platforms may facilitate fraudulent activities such as identity theft [3]. This enables cybercriminals to steal and use victim's online credentials to commit cybercrimes [4]. Tracing the person who committed the crime is difficult because perpetrators use the victim's credentials.

Awareness of potential risks and threats inherent in cyberspace is critical as it enables students to take precautionary steps to safeguard their information resources. Students' data may be susceptible to online attacks as they participate in various online activities. For instance, falling victim to a phishing attack may

lead a student to financial and emotional distress [5]. Educating students about cyber threats can influence how they perceive online risks and threats. This study aims to investigate cyber threat awareness among students from a rural-based university and propose a model to enhance their awareness. This study answers the research question: How do students perceive and respond to cyber threats?

The remainder of this paper is organised into the following sections: Section 2 presents the literature review, providing comprehensive details about cybersecurity frameworks and awareness. Section 3 outlines the research method undertaken in this study to achieve the study's objectives. Section 4 discusses the results obtained from the study, presenting key findings about the research question. Section 5 concludes the paper by summarising the main findings and discussing their implications.

2. Literature review

2.1. Cybersecurity frameworks

Several cybersecurity awareness frameworks address various aspects that influence the behaviour of users. The cybersecurity culture model was designed to assess and enhance employee readiness to deal with cybersecurity challenges. The model posits that the human element in cybersecurity impacts an organisation's overall security posture [6]. The organisational level of the model encompasses security access, operations and security governance. The individual level focuses on employees' attitudes, awareness, behaviours, and competencies.

The human aspects of information security (HAIS) model measures information security awareness by focusing on various behavioural and cognitive elements influencing secure practices within an organisation [7]. The knowledge, attitude, and behaviour (KAB) components are central to the HAIS. The knowledge component examines the user's understanding of security policies, procedures, and best practices. Attitude refers to an individual's mindset and beliefs regarding the importance of information security. Positive attitudes motivate users to follow protocols, while negative attitudes lead to risky behaviour [8]. The behaviour component concerns users' actions and practices to protect information resources. Individual factors refer to users' characteristics that influence their behaviour. Organisational factors are elements within the workplace that shape how information security practices are adopted and followed by employees. Intervention factors involve specific programs implemented to improve information security awareness among users.

The mobile information security awareness scale (MISAS) measures information security awareness among mobile device users. It seeks to address the growing concerns around mobile security due to the increased number of people using mobile devices [9]. One of the factors outlined by the MISAS is instant messaging and navigation. This factor emphasises the importance of maintaining good online practices when engaging in instant messaging and navigation. Another factor is password protection – passwords are essential for securing personal information and preventing unauthorised access to accounts [10]. This underscores the role of using strong passwords to reduce the risk of identity theft and data breaches.

The security awareness improvement tool (SAWIT) aims to improve employee understanding and practices related to information security. The tool uses training methods, interactive learning, and assessment mechanisms to assist employees in identifying various security threats [11]. The SAWIT tool is used to conduct simulations by sending mock phishing emails to employees. The simulations help test employees' ability to identify possible threats [12]. After performing these simulations, providing feedback to those who failed to recognise the threats is critical. Emphasis is placed on what the employees have missed and how to avoid similar instances.

A common feature of the reviewed models is the emphasis on individuals' KAB. The models address security access and governance issues. Emphasis is placed on implementing intervention measures to enhance users' cybersecurity awareness. Training users is critical to creating awareness and improving overall security practices. Another key aspect addressed by the models is advancing organizational factors; these assist in shaping how users adopt information security practices. However, the reviewed

models do not provide enough information about the threats inherent in cyberspace. This is another reason the proposed model highlights cyber threats to improve student awareness

.

2.2. Challenges handling security breaches

The ability of some malware to change their code structure makes it difficult to detect [13]. Delays by software vendors in publishing software updates can have undesirable security implications for students. Attackers use tools to scan computer systems to identify security vulnerabilities. Some tools do not require human intervention to execute [14]. Once a vulnerability is identified on a computer's system, it will be used to gain unauthorized access and launch an attack. Students without knowledge of cyber threats and their propagation techniques may be tricked into revealing sensitive information. Attackers use popular platforms such as social networks to post media embedded with malware.

2.3. Managing occurrences of a security breach

Threat mitigation strategies should focus on both technological solutions and the role of computer users [15]. This highlights the importance of user awareness and appropriate interventions in reducing the effects of a security breach. Isolating an infected computer system is one way of dealing with a security breach [16]. The isolated infected computers help stop the spread of malware. Threat detection can be achieved using software programs such as antivirus [17]. Compliance with institutional policies cannot be overemphasized as it fosters students to safeguard personal information resources. Students must comply with university policies and standard operating procedures. Institutions of higher learning require students to use passwords that meet a specified level of complexity.

2.4. The proposed cybersecurity awareness model

The student online threats awareness model (SOTAM) examines factors influencing cybersecurity awareness. The model provides insights into students' online experiences to guide relevant stakeholders in developing appropriate interventions to enhance safe online practices. The SOTAM model was developed after a comprehensive review of cybersecurity awareness models. The model takes a holistic view of cybersecurity, integrating various aspects to enhance student awareness. The model consists of three layers: fundamental factors, awareness and practice and online activities. The model considers students' biographic information critical in influencing behaviour. Tailored interventions for training and education are prioritised. Continuous reinforcement is essential and is achieved through simulations and assessments. In addition, feedback is personalised according to user roles to improve engagement. The integration of these elements enables the SOTAM to provide an adaptable approach to creating a strong cybersecurity culture. As shown in Figure 1, each layer consists of critical components affecting students' cybersecurity awareness.

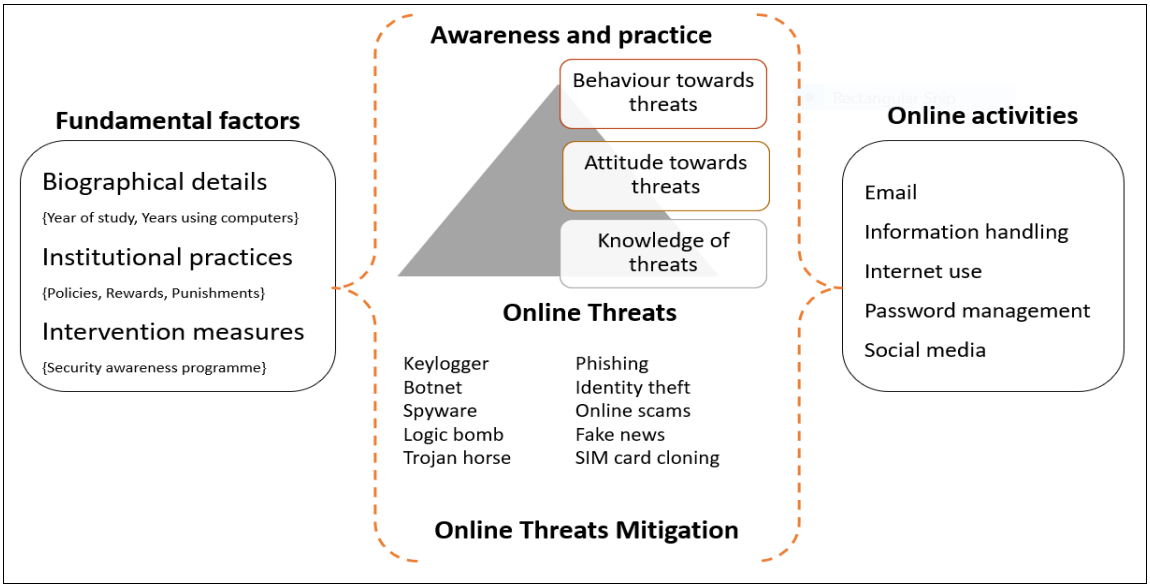

Figure 1. The student online threats awareness model

The fundamental factors layer. Demographics such as age and education are essential in shaping students' attitudes and behaviour about cybersecurity awareness [20]. This layer contains students' biographic details to ensure that implemented intervention measures are tailored according to individual student's profiles. Institutional practices refer to measures established by institutions to guide users to act in a way that safeguards institutional information resources. Organisational culture encompasses the shared values, beliefs, and norms that define how individuals within an organisation interact and work together [21]. For instance, the model considers adopting reward and punishment systems as an ideal way to influence students' online behaviour. The students will likely repeat a particular behaviour if a reward is linked to it. Non-compliance to institutional practices is discouraged by using punishments [22]. This is done to minimise unacceptable online behaviours. Educating users is essential because their vulnerability is determined by their level of KAB [23]. Intervention measures such as security awareness programs aim to positively influence how students perceive cyber threats.

The role of fundamental factors in the SOTAM. The fundamental factors significantly influence students' awareness and practices toward cyber threats. Institutional policies play a crucial role in shaping these practices. For instance, requiring students to create passwords with at least eight characters, including special characters, numbers, and a mix of upper- and lower-case letters, promotes secure habits. Offering rewards for compliance with safe practices enhances engagement, while penalties for negligence serve as effective deterrents. Intervention measures, such as information security awareness programs, improve students' knowledge and cultivate positive attitudes and behaviours toward online threats. A lack of knowledge and awareness can make it difficult for students new to computers to identify and mitigate cyber threats. This underscores the importance of fundamental factors in shaping students' cybersecurity awareness and behaviour online. Fundamental factors shape the scope and type of online activities students engage in. Students with limited computer experience often confine their online use to basic activities like social media and email. In contrast, students with more computer experience will likely engage in advanced activities like online banking and e-commerce. Some institutions implement measures to block access to certain websites when using the university's computer resources.

The awareness and practice layer. The awareness and practice layer addresses the students' knowledge, attitude, and behaviour towards cyber threats. This layer also highlights the importance of threat mitigation by discussing various ways of minimising the consequences of a security breach.

Students who are aware of cyber threats and their repercussions tend to have a positive attitude when engaging in online activities [24]. This is another reason students are given detailed information about possible threats encountered in cyberspace. Newly acquired knowledge about cybersecurity brings security shifts in attitudes and behavioural [25]. Awareness of the risks and consequences of downloading application programs from unauthorised sites can change how individuals perceive cyber threats. It is essential to install and regularly update antivirus programs to detect malware [26]. This is ideal because some threats can remain idle on a computer system for a specific period without detection and only attack when a particular condition has been met [22].

The role of awareness and practice in the SOTAM. Awareness and practice are critical in determining how individuals respond to online threats. A student's KAB towards cyber threats is shaped by fundamental factors such as biographical details, intervention measures, and institutional practices. Information security awareness programs teach students to understand the nature of cyber threats. Students who are aware of specific cyber threats will have a positive attitude, behaving in a way that safeguards their information resources. An experienced student might know the risks of clicking on email attachments from unknown senders, while a novice user may be unaware. Awareness of cyber threats impacts how students interact online. For example, a student who recognizes the risk of fake news will likely verify the information before sharing it with others. Cyber threat awareness is crucial in deterring students from engaging in unsafe online practices.

Online activities. The online activities layer of the model focuses on creating awareness about the risks inherent in cyberspace. Students use various online platforms and services daily to achieve their goals. Increased students' dependence on email communication for personal and educational purposes may threaten sensitive information [27]. Social media and entertainment platforms are popular among students [28]. This highlights why students should be aware of cyber threats and their propagation techniques. Awareness of online threats empowers students to distinguish between acceptable and unacceptable online behavior [29]. There is a common trend among students to disclose their credentials to third parties voluntarily [22]. A personalized intervention approach is recommended using an appropriate delivery method to suit the intended user's profile.

The role of online activities in the SOTAM. Institutional policies are implemented to regulate certain activities conducted on the university's network. For instance, users needing remote access to the institution's domain to complete specific tasks must use a virtual private network (VPN). Fundamental factors such as biographic details can inform the type and extent of online activities the students conduct. Inexperienced students using computers tend to engage in simple activities such as using the learning management system to submit assignments and complete quizzes. Awareness shapes the quality and security of online activities. For example, students who are aware of the subscriber identity module (SIM) card cloning will not disclose their contact details on social media. The type of online activities conducted by the students might expose them to certain risks. Clicking links and email attachments from unknown senders might put the user at risk of phishing attacks. Poor password management, such as writing passwords on notebooks or sharing them with others, makes the account susceptible to hacking.

The preceding discussions highlight the interconnectedness of the SOTAM layers. The fundamental factors shape students' awareness and practice by influencing their knowledge, attitudes, and behavior towards cyber threats. Awareness and practice depend on fundamental factors to improve knowledge, shape attitudes, and encourage secure behaviors. Awareness and good practices influence how safely students perform online activities and mitigate threats.

3. Method

This study employed a quantitative research design using an online survey to collect data. The quantitative approach was selected to facilitate statistical analysis and enable the generalisation of findings across the target population. The target population for this study comprised students enrolled in a

South African rural-based university. A total of 385 students participated in the survey. Simple random sampling was used to ensure each student had an equal chance of being selected. This method enhances the representativeness of the sample and minimises selection bias. A structured online questionnaire was used for data collection. The survey measured key variables relevant to the study's objectives. The online survey was administered using Google Forms. A link to the survey was distributed to the students through their emails. Respondents were provided with an informed consent form outlining the purpose of the study, confidentiality assurances, and voluntary participation rights. Descriptive statistics were used to summarise the demographic characteristics and responses. Inferential statistical tests such as ANOVA and regression analysis were conducted to identify relationships between variables. The statistical analyses were performed using Statistical Package for the Social Sciences (SPSS). This study adhered to ethical research guidelines. Approval to conduct the study was obtained from the rural-based university. Participants were assured anonymity and confidentiality and could withdraw from the survey without penalty.

4. Results and discussions

Data was collected using a Google-based form. Firstly, the dataset addresses key indicators to answer the research question. Secondly, the data was gathered using the human aspects of the information security questionnaire (HAIS-Q), a tool validated by other studies to produce consistent and reliable results [19]. This study employs an adapted version of HAIS-Q, further enhancing its relevance. Recent studies have reported similar trends in cybersecurity awareness, highlighting a persistent lack or low level of cyber threat awareness among students. This underscores the applicability of the data to the current cybersecurity landscape. A study by [30] found that students exhibit low awareness of cyber threats and recommended being taught about scams and prevention strategies. The authors also emphasised the importance of educating students about the risks of sharing sensitive information with strangers online. The sentiments are shared by [31], who adds that orientation programs that address cyber threats should be provided to students. Further findings reveal that students' online practices do not align with the desired behaviour that fosters the protection of information resources [32]. Likewise, [33] highlighted the need to educate students about comprehensive network and data security knowledge to protect themselves effectively in cyberspace. These insights validate the relevance and importance of the dataset used in this study.

The questionnaire consisted of 3 sections: demographic details, user activities and awareness of threats, and knowledge, attitude, and behavior of users. The demographic details section offers essential background information about the students, including their gender, age, years of computer usage, place of residence while studying, and level of study. This information is essential for designing tailored cybersecurity interventions. The user activities and awareness of threats section identifies students' online activities and provides insights into their knowledge of cyber threats. It provides details about the sources through which students became aware of threats, such as posters, workshops, newsletters, social meetings, and online materials. The users' knowledge, attitude, and behavior section employs a 5-point Likert scale (1 = Strongly disagree, 5 = Strongly agree) to assess students' responses across five key areas: social media, email, password management, internet use, and information handling. Table 1 presents a sample of the questionnaire items.

Table 1. Sample questionnaire items

Number	Question
1.	I post anything I want about fellow students on social media.
2.	I always click on email links with interesting content regardless of who the sender is
3.	Using the same password for student accounts, email, and social media is a good practice.
4.	I should not download files from websites while on the University's network.
5.	The best way to destroy printed personal information is by throwing it in the dustbin.

The knowledge, attitude and behaviour section of the questionnaire contains 45 questions. The questions are distributed equally among the five focus areas, each having nine questions. These questions are further spread equally to address the KAB components. The HAIS-Q influenced the questionnaire design. The questions address the students' KAB when engaged in various online activities. A pilot study was conducted before the actual data collection, in which 19 samples were chosen. A Cronbach's Alpha of 0.780 indicated sufficient reliability for the main study.

The student residence profile reveals a diverse distribution. Most students, 36%, reside in university on-campus accommodations, benefiting from internet access through Wi-Fi in their residences. A significant number of the students, 35%, reside in off-campus accommodations. This group of students do not have the luxury of internet access enjoyed by on-campus students. The other 29% of students are staying at home. Students staying at home and those staying off-campus might not access the internet regularly like those at on-campus residences. This highlights the need for tailored support for all residence types. For instance, when planning intervention measures that employ self-paced approaches, considerations should be made to target when most students are available on campus. Table 2 shows students' biographic information.

Table 2. Students' biographic details

	Age	Year of Study	Experience using computers
	18-20 Years	First Year	0 – 3 Years
	(191)	(179)	(267)
	21-25 Years	Second Year	4 – 6 Years
	(248)	(132)	(34)
	26-30 Years	Third Year	7 – 9 Years
	(44)	(101)	(47)
	31-35 Years	Fourth Year	10 – 12 Years
	(14)	(46)	(32)
	36 Years and above	Postgraduate	13 Years and above
	(14)	(49)	(38)
Total	(511)	(507)	(418)

Table 2 shows that most students (48%) are in the 21-25 age group. This is followed by students aged 18-20, comprising 37% of the respondents. Students in the first and second year of study represent the largest groups, with 35% and 25.8% of respondents. The second smallest group is postgraduate students, with 9.7% of the respondents. The smallest group is fourth-year students, with only 9% of the respondents. Most students (51.5%) have used computers between 0-3 years. The second most common group is students using computers for 4-6 years. A small fraction of students have used computers for more than ten years.

These insights indicate that most of the respondents are under the age of 25 years and in their first or second year of study. The information further suggests that most students are inexperienced in using computers. The SOTAM highlights that considering these insights can assist university stakeholders in planning intervention measures that influence students' online behavior. Figure 2 provides an overview of students' online activities.

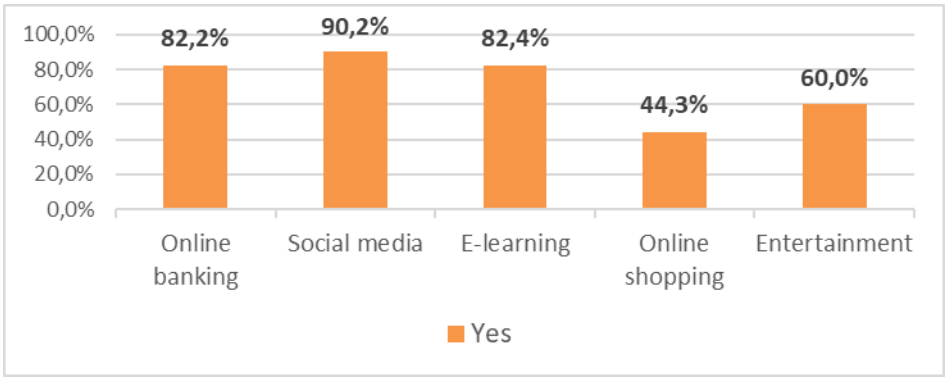

Figure 2. Overview of students' online activities

Figure 2 shows that 90.2% of students engage in social media activities. Students use platforms like Facebook, Instagram, Twitter, and TikTok to connect with peers, share videos and post messages. The high adoption of social media is attributed to the significance of social interaction among the students. Students using e-learning account for 82.4%. The common use of e-learning underscores the role of online platforms, such as learning management systems, in supporting teaching and learning activities. Online banking is used by 82.2% of students. Online banking benefits students by eliminating time spent travelling and waiting in queues for services. Entertainment activities are conducted by 60% of the students. Students who participate in online shopping account for 44.3% of students. The online activities layer on the SOTAM emphasizes the importance of understanding students' online perception of cyber threats when engaged in certain activities. Figure 3 shows the level of threat awareness among the students.

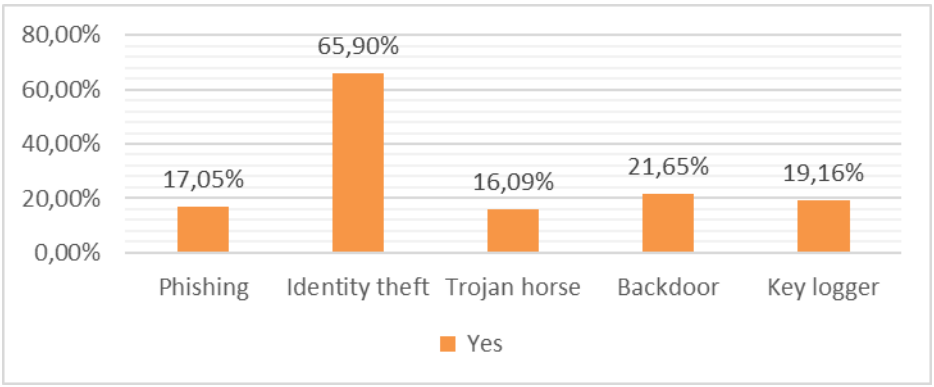

Figure 3. Level of students' threat awareness

Figure 3 shows that 65.90% of students are aware of identity theft. This suggests that most students are familiar with the risk of having their personal information stolen online. The extent to which students show awareness of Trojan horses, phishing, backdoors, and keyloggers is insufficient, suggesting that most students are unaware of these threats' potential risks. This level of unawareness requires relevant university stakeholders to educate students about these threats. The SOTAM recommends addressing various online threats that students may encounter in cyberspace. This is done by highlighting the threat's characteristics and their propagation techniques to create awareness. The Pearson correlation coefficients in Table 3 show the correlations between students' knowledge of cyber threats associated with conducting specific online activities.

Table 3. Knowledge of cyber threat

1.	**Social media**	**Pearson Correlation**	1				
		Sig. (2-tailed)					
2.	**Email**	**Pearson Correlation**	.037	1			
		Sig. (2-tailed)	.409				
3.	**Password management**	**Pearson Correlation**	.043	.236**	1		
		Sig. (2-tailed)	.340	.000			
4.	**Internet Use**	**Pearson Correlation**	.111*	.131**	.120**	1	
		Sig. (2-tailed)	.017	.005	.010		
5.	**Information handling**	**Pearson Correlation**	.007	.095*	.142**	.231**	1
		Sig. (2-tailed)	.877	.042	.002	.000	

**. Correlation is significant at the 0.05 level (2-tailed). **. Correlation is significant at the 0.01 level (2-tailed).*

There is generally a very weak correlation between the investigated variables. A very weak positive correlation exists between the students' social media knowledge of threats associated with internet use (r=.111) and information handling (r=.007). There is also a weak correlation between students' knowledge about email and associated threats when using the internet (r=131) and password management (r=.095). However, a strong correlation exists between internet use and information handling (r=.142), confirming internet use as a good predictor of information handling.

Correlations between knowledge, attitude, and behavior. The correlation coefficients of the investigated variables indicated the absence of multicollinearity. A linear regression analysis determined the relationship between students' knowledge (independent variable) and attitude (dependent variable) about cyber threats when conducting online activities. Table 4 depicts the model summary for the regression analysis.

Table 4. Knowledge regression model

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.135[a]	.018	.016	.90189	.018	9.449	1	509	.002

a. Predictors: (Constant), Knowledge

The results show that R Square = .018 is statistically significant (p =.002). This suggests that students' knowledge of cyber threats accounts for a slight variance (1.8%) in students' attitudes towards cyber threats. Given the F-statistic of 9.449 and a p-value of 0.002, the independent variable significantly predicts the dependent variable. This means that a student's knowledge predicts their attitudes towards cyber threats. Table 5 shows a linear regression analysis to determine the relationship between students' knowledge and attitude (independent variables) and behaviour (dependent variable).

Table 5. Knowledge and attitude regression model

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.302[a]	.091	.088	1.02155	.091	25.365	2	504	.000

a. Predictors: (Constant), Knowledge, Attitude

The R Square = .091 is statistically significant (p <.001), as shown in Table 5. This suggests that students' knowledge and attitude about online risks and threats account for a slight variance (9.1%) in students' behaviour. The F-statistic of 25.365 and a p-value of 0.000 indicate that the independent variables significantly predict the dependent variable. A statistically significant relationship exists between the predictors (knowledge and attitude) and the outcome (behavior). Students' knowledge and attitude towards cyber threats can predict their online behavior.

4.1 Students perception of cyber threats

In this section, the study's research question is answered. How do students perceive, and respond to cyber threats? The students demonstrate proficiency in understanding threats associated with email use by not opening links or attachments from unknown senders. This indicates that they know the risks of clicking on email attachments. This is a good online practice because it minimizes the chances of students falling victim to threats such as phishing. The students engage in responsible social media use. They demonstrate this by assessing social media platform privacy settings to decide which information to share publicly. Knowing that some information should not be shared publicly may prevent attacks such as identity theft. Students' knowledge of cyber threats enables them to approach possible threats positively when engaged in online activities.

The students must improve how they respond to online threats when engaged in internet use and password management activities. The students download resources from unauthorized platforms. By doing this, they risk inadvertently downloading and installing threats onto their computer systems, putting their information resources at risk. The students demonstrate a tendency to share their passwords with third parties. This is exacerbated by the fact that they re-use the same password on several accounts. Another shortcoming related to password management is that the students are reluctant to change their password. The SOTAM enhances students' cybersecurity awareness by offering a structured and practical approach to meet their needs. By emphasizing the consequences of security breaches associated with poor security practices, students can be influenced to adopt safe online behavior. The SOTAM recommends implementing practical simulations wherein mock phishing emails help students respond to possible threats effectively.

5. Conclusion

The study recommends that students improve their knowledge of cyber threats associated with information handling and password management. The students display undesirable online behaviours concerning internet use and password management. The study further indicates that students with more years of using computers are more likely to know about online risks and threats. These groups of students demonstrate positive approaches and improved response mechanisms to cyber threats, leading to better online behaviour.

Implementing intervention measures guided by the SOTAM can significantly enhance students' awareness of cyber threats and promote good online behavior. Planned intervention measures should prioritise gaps in knowledge and undesirable behaviors. For instance, delivering awareness programs using a learning management system allows students to use self-paced resources to learn about information handling and password management. Lessons learned using this delivery method can be reinforced using quizzes and gamification strategies that foster retention and provide instant feedback on cybersecurity awareness topics.

6. References

[1] T. Moletsane and P. Tsibolane, "Mobile Information Security Awareness among Students in Higher Education : An Exploratory Study," *2020 Conf. Inf. Commun. Technol. Soc. ICTAS 2020 - Proc.*, pp. 1–6, 2020, doi: 10.1109/ICTAS47918.2020.233978.

[2] H. S. Berry, "Survey of the Challenges and Solutions in Cybersecurity Awareness Among College Students," *2023 11th Int. Symp. Digit. Forensics Secur.*, pp. 1–6, 2023, doi: 10.1109/ISDFS58141.2023.10131851.

[3] P. M. W. Musuva, K. W. Getao, and C. K. Chepken, "A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility," *Comput. Human Behav.*, vol. 94, no. August 2018, pp. 154–175, 2019, doi: 10.1016/j.chb.2018.12.036.

[4] Z. Mador, "Keep the dark web close and your cyber security tighter," *Comput. Fraud Secur.*, vol. 2021, no. 1, pp. 6–8, Jan. 2021, doi: 10.1016/S1361-3723(21)00006-3.

[5] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of the art and open research challenges," *Comput. Secur.*, vol. 73, pp. 519–544, 2018, doi: 10.1016/j.cose.2017.12.006.

[6] A. Georgiadou, S. Mouzakitis, K. Bounas, and D. Askounis, "A Cyber-Security Culture Framework for Assessing Organization Readiness," *J. Comput. Inf. Syst.*, vol. 62, no. 3, pp. 452–462, 2022, doi: 10.1080/08874417.2020.1845583.

[7] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, 2014, doi: 10.1016/j.cose.2013.12.003.

[8] S. Aurigemma and T. Mattson, "Exploring the effect of uncertainty avoidance on taking voluntary protective security actions," *Comput. Secur.*, vol. 73, pp. 219–234, Mar. 2018, doi: 10.1016/J.COSE.2017.11.001.

[9] F. Erdoğdu, S. Gökoğlu, and M. Kara, "'What about users?': Development and validation of the mobile information security awareness scale (MISAS)," *Online Inf. Rev.*, vol. 45, no. 2, pp. 406–421, 2021, doi: 10.1108/OIR-04-2020-0129.

[10] S. Althubaiti and H. Petrie, "Instructions for creating passwords: How do they help in password creation," in *HCI 2017: Digital Make Believe - Proceedings of the 31st International BCS Human Computer Interaction Conference, HCI 2017*, 2017, vol. 2017-July. doi: 10.14236/ewic/HCI2017.55.

[11] A. Kovačević and S. D. Radenković, "SAWIT-security awareness improvement tool in the workplace," *Appl. Sci.*, vol. 10, no. 9, 2020, doi: 10.3390/app10093065.

[12] M. M. Al-Daeef, N. Basir, and M. M. Saudi, "Security awareness training: A review," in *Lecture Notes in Engineering and Computer Science*, 2017, vol. 2229, pp. 446–451.

[13] J. M. Blythe and L. Coventry, "Costly but effective: Comparing the factors that influence employee anti-malware behaviours," *Comput. Human Behav.*, vol. 87, no. August 2017, pp. 87–97, 2018, doi: 10.1016/j.chb.2018.05.023.

[14] J. E. Thomas, "Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks," *Int. J. Bus. Manag.*, vol. 13, no. 6, p. 1, 2018,

doi: 10.5539/ijbm.v13n6p1.
[15] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommun. Syst.*, vol. 67, no. 2, pp. 247–267, 2018, doi: 10.1007/s11235-017-0334-z.
[16] M. Nieles, K. Dempsey, and V. Y. Pillitteri, "NIST Special Publication 800-12 Revision 1 - An introduction to information security," *NIST Spec. Publ.*, 2017, doi: 10.6028/NIST.SP.800-12r1.
[17] S. Chakraborty, "A Comparison Study of Computer Virus and Detection Techniques," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. © 2017 IJSRCSEIT*, vol. 1, no. 2, pp. 236–240, 2017, Accessed: May 16, 2021. [Online]. Available: www.ijsrcseit.com
[18] A. Kovacevic, N. Putnik, and O. Toskovic, "Factors Related to Cyber Security Behavior," *IEEE Access*, vol. 8, pp. 125140–125148, 2020, doi: 10.1109/ACCESS.2020.3007867.
[19] A. Da Veiga, "A model for information security culture with creativity and innovation as enablers – refined with an expert panel," *Inf. Comput. Secur.*, vol. 658, 2023, doi: 10.1108/ICS-11-2022-0178.
[20] J. D. Wall, P. Palvia, and J. D'Arcy, "Theorizing the Behavioral Effects of Control Complementarity in Security Control Portfolios," *Inf. Syst. Front.*, 2021, doi: 10.1007/s10796-021-10113-z.
[21] M. Bogale, L. Lessa, and S. Negash, "Building an information security awareness program for a bank: Case from Ethiopia," 2019.
[22] D. Jeske and P. van Schaik, "Familiarity with Internet threats: Beyond awareness," *Comput. Secur.*, vol. 66, pp. 129–141, 2017, doi: 10.1016/j.cose.2017.01.010.
[23] M. Sas, G. Reniers, K. Ponnet, and W. Hardyns, "The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour," *Saf. Sci.*, vol. 144, no. August, p. 105447, 2021, doi: 10.1016/j.ssci.2021.105447.
[24] S. Chakraborty, "Module Functioning of Computer Worm, PC Virus and Anti Virus Programs," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. © 2017 IJSRCSEIT*, vol. 1, no. 2, pp. 2456–3307, 2017.
[25] A. J. Burns, M. E. Johnson, and D. D. Caputo, "Spear phishing in a barrel: Insights from a targeted phishing campaign," *J. Organ. Comput. Electron. Commer.*, vol. 29, no. 1, pp. 24–39, 2019, doi: 10.1080/10919392.2019.1552745.
[26] S. R. Saha and A. K. Guha, "Impact of Social Media Use of University Students," *Int. J. Stat. Appl.*, vol. 2019, no. 1, pp. 36–43, 2019, doi: 10.5923/j.statistics.20190901.05.
[27] P. Nyblom, G. Wangen, and V. Gkioulos, "Risk perceptions on social media use in Norway," *Futur. Internet*, vol. 12, no. 12, pp. 1–40, 2020, doi: 10.3390/fi12120211.
[28] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, 2014, doi: 10.1016/j.cose.2013.12.003.
[29] G. Alotibi, "A Cybersecurity Awareness Model for the Protection of Saudi Students from Social Media Attacks," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 2, pp. 13787–13795, 2024, doi: 10.48084/etasr.7123.
[30] G. S. Prakasha, J. J. Leiva-Olivencia, A. Simpson, T. Grundmeyer, and A. Kenneth, "Lived Experiences, Challenges, and Coping Mechanisms of Undergraduate Students on Cybersecurity in Digital Environments," *Comput. Sch.*, vol. 41, no. 3, pp. 328–350, 2024, doi: 10.1080/07380569.2024.2363341.
[31] C. Melchior and U. Soler, "Security of Personal Data in Cyberspace in the Opinion of Students of the University of Udine," *Cybersecurity Law*, vol. 11, no. 1, pp. 227–247, 2024, doi: 10.35467/cal/188451.

[32] M. Yildirim and M. E. Erendor, "A Comparative Analysis of Cyber Security Behaviours of University Students," *Edpacs*, vol. 69, no. 6, pp. 28–45, 2024, doi: 10.1080/07366981.2024.2356298.