Cybersecurity Awareness of Staff and Students in Higher Education Institutions in Kuwait

Abdullah Feraih Alenezi (*)

Abstract

This study investigates the level of cybersecurity awareness among staff and students at higher education institutions (HEIs) in Kuwait. Employing a structured questionnaire, data were collected from 269 participants to evaluate their general knowledge of cybersecurity, specific awareness of cyber threats, and their cybersecurity practices. The results indicate that both general cybersecurity knowledge and specific threat awareness significantly influence cybersecurity practices. However, substantial deficiencies were identified in both areas, highlighting the need for targeted awareness programs. Additionally, demographic variables such as age and institutional role were found to significantly impact cybersecurity awareness. The study underscores the necessity for enhanced cybersecurity awareness through customized training programs and robust institutional policies.

Keywords: cybersecurity, threats, awareness, Higher education institutions, Kuwait

* Assistant Professor College of Business Studies Public Authority for Applied Education and Training

الوعي بالأمن السيبراني للموظفين والطلاب في مؤسسات التعليم العالي في الكويت

ملخص

تبحث هذه الدراسة في مستوى الوعي بالأمن السيبراني بين الموظفين والطلاب في مؤسسات التعليم العالي في الكويت. باستخدام استبيان منظم، تم جمع البيانات من 269 مشاركًا لتقييم معرفتهم العامة بالأمن السيبراني، والوعي المحدد بالتهديدات السيبرانية، وممارساتهم في مجال الأمن السيبراني، تشير النتائج إلى أن المعرفة العامة بالأمن السيبراني والوعي المحدد بالتهديدات يؤثران بشكل كبير على ممارسات الأمن السيبراني. ومع ذلك، تم تحديد أوجه قصور كبيرة في كلا المجالين، مما يسلط الضوء على الحاجة إلى برامج توعية مستهدفة، بالإضافة إلى ذلك، وجد أن المتغيرات الديموغرافية مثل العمر والدور المؤسسي تؤثر بشكل كبير على الوعي بالأمن السيبراني. تؤكد الدراسة على ضرورة تعزيز الوعي بالأمن السيبراني من خلال برامج تدريبية مخصصة وسياسات مؤسسية قوية.

الكلمات المفتاحية: الأمن السيبراني، التهديدات، الوعي، مؤسسات التعليم العالي، الكويت

Introduction

Higher education institutions (HEIs) are significantly leveraging digital tools and e-learning platforms to facilitate teaching and learning (Alenezi, 2024; Rafiq et al., 2024). HEIs manage vast amounts of sensitive information, including personal data of students and staff, research data, and intellectual property (Drevin et al., 2007; Al-Alawi & Hafedh, 2006). The reliance on digital infrastructure exposes HEIs to various cyber threats. Despite the technological measures in place to safeguard against cyberattacks, the effectiveness of these measures is heavily dependent on human factors and the prevailing cybersecurity culture within these institutions (Vestad & Yang, 2024). The expansion of e-learning and digital infrastructure in HEIs necessitates a comprehensive approach to cybersecurity, considering the diverse experiences and awareness levels of all stakeholders involved (Hunt, 2016).

Cybersecurity is critical for safeguarding information assets from unauthorized access, disclosure, alteration, and destruction (Alenezi, 2024). Effective cybersecurity practices protect the confidentiality, integrity, and availability of data, ensuring the trust and smooth operation of HEIs (Al-Alawi & Hafedh, 2006; Drevin et al., 2007; Rafiq et al., 2024). For HEIs, safeguarding personal information for students and staff is particularly important in applications such as student information systems, employee information systems, and financial applications (Drevin et al., 2007; Al-Alawi & Hafedh, 2006). Thus, cybersecurity awareness in HEIs is fundamental in preventing breaches that can lead to significant financial losses, reputational damage, and legal issues (Rafiq et al., 2024).

The Middle East faces unique cybersecurity challenges, including geopolitical tensions, varying levels of technological advancement and cybersecurity maturity, differing regulatory environments and a shortage of skilled professionals (Alzahrani, 2021; Al-Alawi et al., 2016), which have an influence on cybersecurity practices. Cyberattacks in the region are on the rise, with HEIs being prime targets due to their open and collaborative network environments (Kwon, 2024). Common threats include phishing, malware, ransomware, and social engineering attacks (Al-Alawi et al., 2016). Insufficient awareness among staff and students regarding cybersecurity threats exacerbates the risks faced by HEIs (Eltahir & Ahmed, 2023; Garba et al., 2020). Many individuals within these institutions may not fully comprehend the importance of cybersecurity practices or recognize potential threats, increasing the likelihood of successful cyberattacks.

In Kuwait, the rapid digital transformation and increasing internet penetration make HEIs potential targets for cyberattacks (Al-Janabi & Al-Shourbaji, 2016). As HEIs continue to expand their digital capabilities and global reach, it is imperative to balance the benefits of technological advancements with robust cybersecurity measures and awareness to protect against the ever-evolving landscape of cyber threats. Kuwait, with its strategic investments in education and technology, provides a pertinent case study for examining cybersecurity awareness in HEIs. The objectives of this study are to:

- assess the current state of cybersecurity knowledge among staff and students in HEIs in Kuwait.
- identify gaps in cybersecurity knowledge and practices among staff and students in HEIs in Kuwait.

- propose measures to enhance cybersecurity awareness among staff and students in HEIs in Kuwait.

Effective cybersecurity awareness programs are essential to mitigate risks, yet many institutions struggle with implementation due to lack of expertise, resistance to change and budgetary constraints (Cheng & Wang, 2022). This study is significant as it addresses a critical need for enhanced cybersecurity awareness in HEIs in Kuwait. By identifying current awareness levels and gaps, the research provides valuable insights for HEIs, policymakers, and IT professionals. The findings can guide the development of effective cybersecurity awareness programs and policies, contributing to the overall security posture of HEIs.

Literature Review

Definition of cybersecurity awareness

Cybersecurity refers to the practices, technologies, and processes designed to protect networks, devices, programs, and data from cyberattacks, damage, or unauthorized access (Veluvali & Surisetti, 2022). It encompasses various domains, including information security, network security, application security, and operational security. The common cybersecurity threats in HEIs include data breaches, malware attacks, phishing, denial-of-service (DoS) attacks, ransomware and insider threats (Triplett, 2023). Cybersecurity awareness involves understanding the risks associated with cyber threats and adopting behaviors to mitigate these risks (Vestad & Yang, 2024). Several studies have demonstrated that effective cybersecurity awareness programs can significantly reduce the likelihood of cyber incidents (Falkner et al., 2016; Hunt, 2016;

Vestad & Yang, 2024), with such programs incorporating: regular training and education on cybersecurity best practices, simulated phishing exercises to educate users about common attack vectors, and clear communication of cybersecurity policies and procedures (Khader et al., 2021).

Global Perspective on cybersecurity awareness in HEIS

Several studies have highlighted the importance of cybersecurity awareness in HEIs globally (Aljohni et al., 2021; Aloul, 2012; Eltahir & Ahmed, 2023; Garba et al., 2020). Aloul (2012) argues that cybersecurity awareness is crucial in mitigating the risks associated with cyber threats in HEIs while Carpenter & Schutten (2020) emphasize fostering a culture of awareness as a key strategy for enhancing cybersecurity in HEIs. In the context of South Africa, Kruger et al. (2011) study revealed disappointing levels of awareness especially the cultural factors in cybersecurity awareness. Kruger et al. (2011) recommended emphasizing social and cultural differences in awareness programs within the education sector and clarifying specialized terms and concepts that learners may not fully grasp. However, cultural factors are intertwined with broader social, economic, and individual considerations, complicating the design of effective educational strategies (Rhee et al., 2009). Thus, effective cybersecurity training might need to move beyond raising awareness to practical application, translating knowledge into behavioural changes.

In their study on cybersecurity awareness among students at UiTM Terengganu in Malaysia, Raju et al. (2022) found that while students demonstrated moderate level of awareness of cyber-attacks, cyberbullying, and personal information protection, their involvement in risky activities such as sharing passwords and accessing unknown websites was prevalent. Thus, Raju et al. (2022) highlighted the need for proper guidance and frequent knowledge transfer. On the contrary, Eltahir & Ahmed (2023) study on cybersecurity awareness among students at a HEI in Sudan revealed low cybersecurity awareness, with male students have a relatively higher awareness level than female. In addition, students with some advanced computer skills had a higher cybersecurity practice level. Thus, Eltahir & Ahmed (2023) emphasizes the need for cybersecurity education in HEIs. Similarly, in the context of Saudi Arabia, Alzahrani (2021) found a general lack of basic cybersecurity awareness and cyber trust among students. In addition, while some cybersecurity training program existed, attendance in these programs was low.

Cybersecurity awareness in HEIs in the Middle East:

The Middle East has witnessed a surge in cyber threats, driven by its geopolitical significance and rapid digitalization. Al-Janabi & Al-Shourbaji (2016) highlight that educational institutions in the region often lack robust cybersecurity frameworks, making them vulnerable targets. The region's unique socio-political landscape further complicates the cybersecurity scenario, necessitating tailored approaches for awareness and mitigation. The adoption of new technologies in the Arabic-speaking world has historically lagged behind Western countries (Aljohni et al., 2021). However, since the early 21st century, there has been increasing recognition of rapid technological changes and the necessity for scholars to research the intangible dimensions of this development, including cultural and moral aspects (Dutta & Coury, 2003). A persistent lack of maturity regarding the value of information in Arabic-speaking countries compared to more developed nations has been identified (Al-Kaabi & Maple, 2012). The cultural preference for privacy sharing over confidentiality in Arab cultures could have adverse impacts on individuals, organizations, and state leaders (Al-Kaabi & Maple, 2012). A comparative study of user behaviours in the United Arab Emirates, Saudi Arabia, and Oman revealed significant sharing of sensitive information, such as passwords, which compromises digital authentication systems (Alkaabi, 2014). Users often lack awareness of the risks associated with personal information becoming accessible to others, including criminals. Furthermore, issues such as weak protection for wireless access points have been identified in the UAE (Aloul, 2012). Further, Aloul (2012) revealed that in many urban areas (e.g. Dubai and Sharjah), 20-30 percent of wireless access points were unencrypted, with many others having low levels of encryption. Such observations highlight the need for schools and universities to offer security awareness campaigns and integrate IT security topics into their curricula (Aloul, 2012). Topics such as cyberstalking, cyberbullying, information sharing risks, and social engineering should be included in these programmes, tailored to the age of the learners (Alkaabi, 2014).

Further, in another study on information security awareness among information systems staff at a UAE university, Rezgui & Marks (2008) highlighted issues stemming from cultural tensions between Muslim students and Western staff, as well as the insecure employment status of expatriate employees. These cultural factors may explain the absence of information security training at the university, despite existing regulations and policies that were not rigorously enforced. Khader et al. (2021) emphasise that there is still much work needed to raise cybersecurity awareness in the UAE education sector, even among university specialists. Similarly, Halevi et al. (2016) found that culture significantly influenced user attitudes toward cybersecurity, although it had a low impact on behaviour. Demographic factors, including personality and self-efficacy, were more important for behaviour, with gender being particularly relevant—women tended to be more risk-averse than men. The authors suggested that while a global approach to developing security-related systems is reasonable, it should be adjusted to account for users' personalities and demographic characteristics. In the context of Qatar, Al-Hamar et al. (2010) found that cultural factors, such as a tradition of Islamic philanthropy and considerable wealth, contributed to a vulnerability to email scams like phishing and identity theft. The complexity of these factors presents challenges in designing suitable educational awareness programmes for all users. While this study did not specifically address the needs of

HEIs, it highlighted the importance of considering country-specific factors in any cybersecurity awareness strategy.

The impact of demographics on cybersecurity awareness was investigated in Alzahrani (2021) study on cybersecurity awareness among university students in Saudi Arabia. Alzahrani (2021) found no significant difference in awareness levels between male and female students, although females showed slightly more concern about cybersecurity issues. In addition, students from computer and information technology departments exhibited higher awareness levels compared to those from other departments similar to Eltahir & Ahmed (2023) study. Further, students from urban areas demonstrated relatively higher awareness levels compared to those from rural areas. However, Alzahrani (2021) study can be criticized for its relatively small sample size (136 students) and also limited scope of awareness factors.

In the case of Kuwait, Al-Alawi et al. (2016) evaluated the Information Systems Security Awareness (ISSA) at Kuwait University and found that there is a varying level of ISSA across different faculties at Kuwait University with some faculties exhibiting higher awareness, while others showed significant gaps. The study identified key areas needing improvement, such as commitment to ISS policy, effective use of passwords, safe Internet and email usage, awareness of ISS threats, regular backups, and updating operating systems and antivirus programs. In addition, the study emphasized the need for targeted training programs and robust ISS policies to enhance security awareness and protect personal and institutional data.

Theoretical perspectives:

Different theoretical perspectives have been adopted in cybersecurity awareness studies. Among these theories are protection motivation theory (PMT), the theory of planned behavior (TPB), and socio-technical systems theory (STS) (Ulven & Wangen, 2021). Protection Motivation Theory (PMT) postulates that individuals are motivated to protect themselves through four cognitive processes: perceived severity, perceived vulnerability, response efficacy, and self-efficacy (Rogers, 1983). In the context of HEIs, PMT suggests that students and staff will adopt protective cybersecurity behaviors if they view cyber threats as severe and believe they are susceptible to these threats (Lee et al., 2008). For instance, recognizing the potential financial and reputational damages from data breaches can enhance their perceived severity and vulnerability, encouraging adherence to cybersecurity best practices. Furthermore, effective cybersecurity training programs can enhance individuals' beliefs in the efficacy of protective measures, such as strong passwords and regular software updates, and their confidence in executing these measures. By addressing these cognitive processes, HEIs can foster a proactive cybersecurity culture.

The theory of planned behavior (TPB) posits that an individual's behavior is driven by their intention to perform it, which is influenced by their attitude, subjective norms, and perceived behavioral control (Ajzen, 1991). In HEIs, positive attitudes towards cybersecurity, shaped by awareness of its importance and benefits, can enhance the intention to engage in protective behaviors. Educational campaigns and success stories of thwarted cyber threats can help build positive attitudes. Additionally, the influence of peers and organizational culture plays a crucial role in shaping cybersecurity behavior. If students and staff perceive that their peers and the institution value and practice good cybersecurity habits, they are more likely to follow suit. Providing resources, training, and support can enhance individuals' perceived control over their cybersecurity actions, essential for fostering compliance.

Socio-Technical Systems Theory (STS) emphasizes the interdependence of social and technical factors in organizational settings, suggesting that successful system performance relies on the joint optimization of both elements (Malatji et al.., 2019). In HEIs, fostering a strong cybersecurity culture involves addressing social factors such as organizational policies, leadership support, and user training (Rafiq et al., 2024). Encouraging collaboration and communication about cybersecurity among staff and students is vital. Additionally, implementing robust technical measures, such as firewalls, encryption, and intrusion detection systems, is necessary but insufficient. These measures must be complemented by social initiatives to ensure they are effectively used and maintained. HEIs must balance technical controls and social interventions. Regular cybersecurity training and awareness campaigns should align with technical updates and policy changes to ensure comprehensive protection.

In this study, an integration of these theories is adopted. Integrating protection motivation theory, theory of planned behavior, and socio-technical systems theory provides a comprehensive framework for understanding and enhancing cybersecurity awareness in HEIs in Kuwait. Each theory offers unique insights into the motivational, social, and technical aspects of cybersecurity behavior, contributing to a holistic approach that addresses the diverse needs of HEI stakeholders. By leveraging these theories, HEIs can develop effective strategies to mitigate cyber threats and foster a resilient cybersecurity culture.

Methods:

Participants:

Data was collected using a structured questionnaire designed to assess the cybersecurity awareness levels of staff and students at Kuwait HEIs. The questionnaire was developed using google forms and distributed electronically, allowing for easy access and completion by participants. This method facilitated the collection of responses from a wide geographical area, enhancing the generalizability of the findings. In total, 274 participants responded to the questionnaire, of which 4 were deemed unusable. This sample size was deemed sufficient at 90% confidence level and 5% margin of error (Desu, 2012), to capture a wide range of perspectives on cybersecurity awareness and practices. There were 241 students (88%) and 34 staff (12.4%), of which 13.9% (38) were male and 86.5% (237) female. Most respondents were in the age range of 18-24 years (68%) which is typically the university age for students.

Figure 1: Staff and student respondents

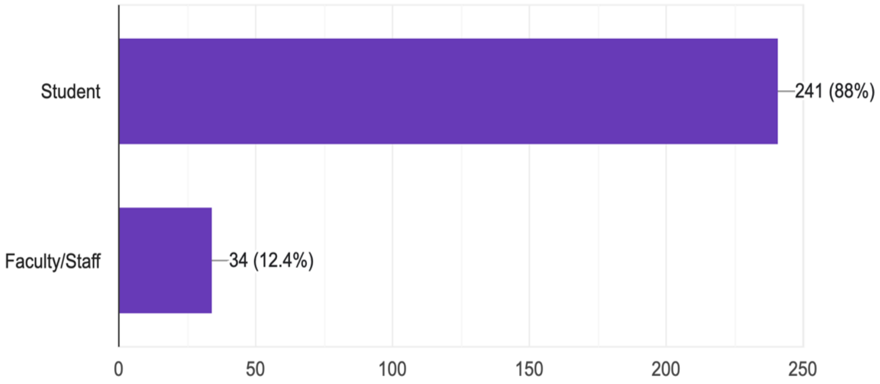
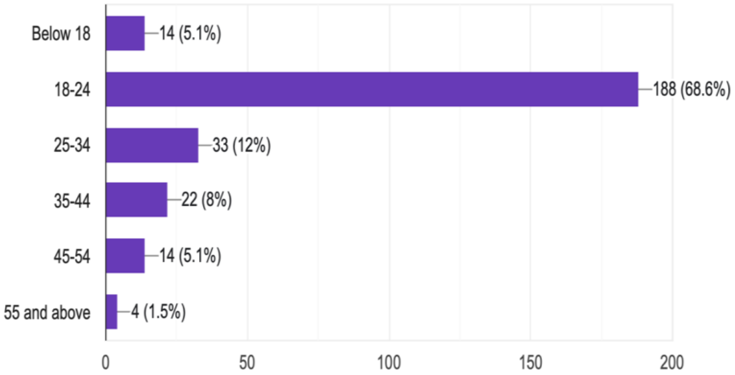


Figure 2: Age distribution of respondents



Questionnaire Design

The questionnaire was developed based on a review of existing literature on cybersecurity awareness and best practices, including theoretical understanding (Aljohni et al., 2021; Aloul, 2012; Eltahir & Ahmed, 2023; Garba et al., 2020). It comprised of four sections, each focusing on different aspects of cybersecurity awareness as shown below.

- *Section One: Demographic Information:* Questions about the participants' age, gender, role (staff or student), and level of education.
- *Section Two: Knowledge of Cybersecurity*: Items assessing knowledge on cybersecurity, potential risks and training.
- *Section Three: Knowledge of Cybersecurity Threats*: Items measuring awareness of various types of cyber threats, such as phishing, malware, and ransomware.
- *Section Four:* Cybersecurity Practices: Questions regarding participants' practices, such as password management, software updates, and use of antivirus programs.

There were five Likert scale type questions in sections two to four. The reliability test was undertaken for each section and whole questionnaire using the Cronbach’s Alpha which showed that the set of 15 questions has a high level of internal consistency, making them a reliable measure, with the value of 0.87. The Cronbach’s Alpha score was 0.724, 0.827 and 0.764 for section 2, 3 and 4 respectively. The internal consistency remains high even when the items are standardized.

Table 1: Cronbach'Alpha Test

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.87	.869	15

The questions from sections two to four are representative of three variables: 'Cyberknowledge', 'Cyberthreatsknowledge', and 'Cyberpractices' respectively. The relationship being examined is that the combined effect of general cyber knowledge and specific threat knowledge influences the adoption of cyber practices. This is hypothesized as follow:

Null Hypothesis (H0): Cyberknowledge and Cyberthreatsknowledge together do not significantly predict Cyberpractices.

Alternative Hypothesis (H1): Cyberknowledge and Cyberthreatsknowledge together significantly predict Cyberpractices.

The hypothesis posits that individuals with higher levels of both types of knowledge are more likely to engage in safe practices, indicating a cumulative effect, consistent with most literature (De Kimpe et al., 2022; Lee & Chua, 2024).

Data analysis and normality test

The data from the questionnaire was extracted to Microsoft excel and coded. The coded data was analysed statistically using the statistical software, SPSS version 29. Before undertaking detailed statistical analysis, tests of normality were undertaken so that an appropriate statistical test was chosen for the dataset. Both the Kolmogorov-Smirnov and Shapiro-Wilk tests indicate that all three variables (Cyberknowledge, Cyberthreatsknowledge, and Cyberpractices) significantly deviate from a normal distribution (since all p-values are less than .05). This suggests that the data for these variables do not follow a normal distribution. Thus, the non-parametric method, ordinal logistic regression model, has been used to analyse the data due to the lack of normality.

Table 2: Tests of Normality

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Cyberknowledge	.101	269	<.001	.983	269	.002
Cyberthreatsknowledge	.073	269	.001	.976	269	<.001
Cyberpractices	.058	269	.029	.981	269	.001

a. Lilliefors Significance Correction

Findings:

Cybersecurity knowledge and training

The results indicate a varied level of familiarity with cybersecurity among staff and students in higher education institutions (HEIs). The majority of both staff and students have a moderate level of familiarity with cybersecurity concepts. This suggests that while they have some understanding, it is not comprehensive. A significant portion (10.9%), reported not being familiar with cybersecurity at all (Figure 3). This highlights a substantial gap in basic cybersecurity awareness and understanding within the HEIs. The results also reveal that most staff and students have not received any formal education or training in cybersecurity. This implies that the institutions may not have robust or accessible formal training programs dedicated to cybersecurity. Despite the lack of formal training, many staff and students possess informal knowledge about cybersecurity (Figure 4). This could be acquired through personal research, on-the-job experience, or casual learning from peers or online resources.

Figure 3: Knowledge of cybersecurity

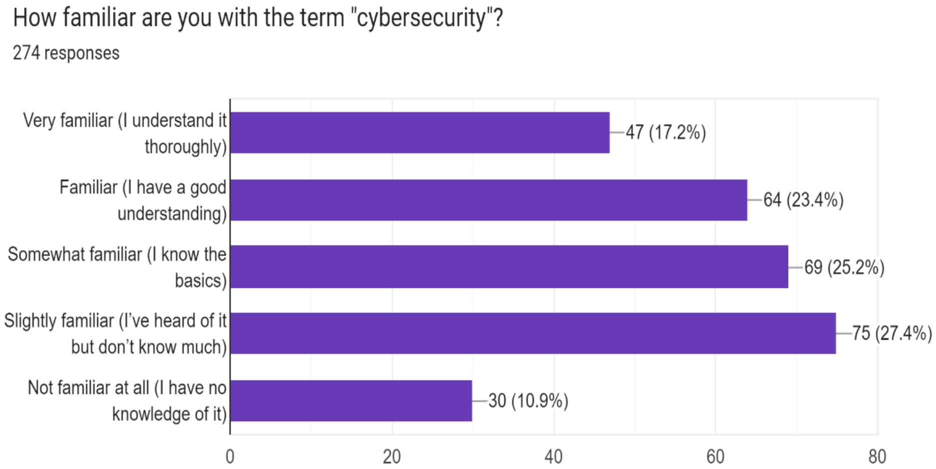
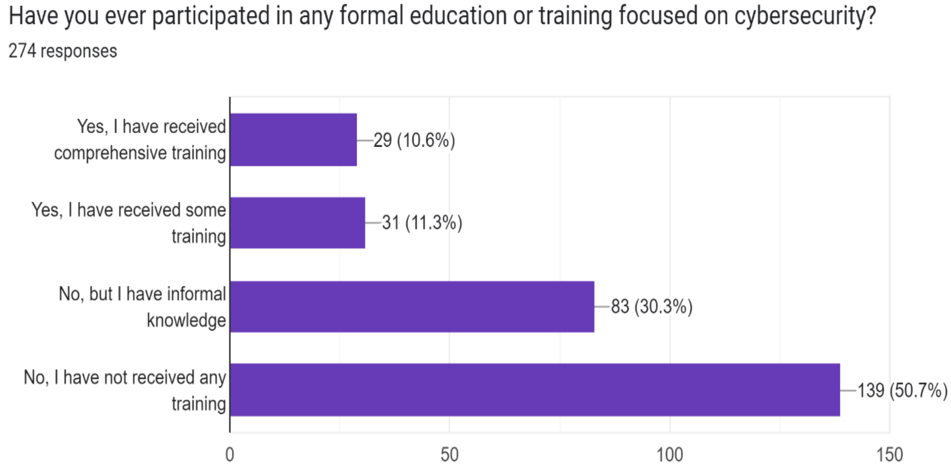

How familiar are you with the term "cybersecurity"?
274 responses
Very familiar (I understand it thoroughly)
47 (17.2%)
Familiar (I have a good understanding)
64 (23.4%)
Somewhat familiar (I know the basics)
69 (25.2%)
Slightly familiar (I've heard of it but don't know much)
75 (27.4%)
Not familiar at all (I have no knowledge of it)
30 (10.9%)
0
20
40
60
80

Figure 4: Participation in training


Have you ever participated in any formal education or training focused on cybersecurity?
274 responses
Yes, I have received comprehensive training
29 (10.6%)
Yes, I have received some training
31 (11.3%)
No, but I have informal knowledge
83 (30.3%)
No, I have not received any training
139 (50.7%)
0
50
100
150

Relationship between cyber knowledge, cyber threats knowledge, and cyber practices:

The correlation between the three variables were all statistically significant at the 0.01 level as shown in Table 3. This implies that both general cybersecurity knowledge and specific threat knowledge are important factors in promoting good cybersecurity practices. ‘Cyberknowledge’ and ‘Cyberthreatsknowledge’ have a moderate positive correlation (0.543), suggesting that individuals with higher general cybersecurity knowledge also tend to have higher knowledge of specific cyber threats. Similarly, ‘cyberknowledge’ and ‘cyberpractices’ have a moderate positive correlation (0.422), indicating that individuals with higher cybersecurity knowledge are more likely to engage in good cyber practices. Also, ‘cyberthreatsknowledge’ and ‘cyberpractices’ have a moderate positive correlation (0.420), suggesting that individuals with greater knowledge of cyber threats are more likely to adopt safe cyber practices. The descriptive statistics of these variables are shown in appendix.

Table 3: Correlation between variables

Correlations					
			Cyberknowledge	Cyberthreatsknowledge	Cyberpractices
Spearman's rho	Cyberknowledge	Correlation Coefficient	1.000	.543**	.422**
		Sig. (2-tailed)	.	<.001	<.001
		N	270	270	269
	Cyberthreatsknowledge	Correlation Coefficient	.543**	1.000	.420**
		Sig. (2-tailed)	<.001	.	<.001
		N	270	270	269
	Cyberpractices	Correlation Coefficient	.422**	.420**	1.000
		Sig. (2-tailed)	<.001	<.001	.
		N	269	269	269
**. Correlation is significant at the 0.01 level (2-tailed).					

The results from the ordinal logistic regression model are shown in Tables 4 and 5. The model fitting information in Table 4 reveals that the large reduction in the -2 Log Likelihood value from 1365.981 to 804.864 indicates that the final model with predictors (Cyberknowledge and Cyberthreatsknowledge) fits the data much better than the intercept-only model. The Chi-Square value of 561.117 with 750 degrees of freedom tests the null hypothesis that the additional predictors (Cyberknowledge and Cyberthreatsknowledge) do not improve the model fit compared to the intercept-only model. The p-value (Sig.) of 1.000 indicates that the improvement in fit is not statistically significant. Further, the deviance chi-square test for the goodness-of-fit is not statistically significant (p-value = 1.00) which indicates that the model fits the data well. The deviance value is also much smaller than the degrees of freedom, suggesting that the residual deviance is minimal and the model is a good fit for the data.

In addition, the Nagelkerke Pseudo R-Square value of 0.920 (Table 5), indicates that the model explains 92.0% of the variability in the dependent variable (‘cyberpractices) which suggests an excellent model fit. This is also supported by the Cox and Snell Pseudo R-Square of 0.918.

Table 4: Model fitting information and goodness of fit

Model Fitting Information

Model	Model Fitting Criteria	Likelihood Ratio Tests		
	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	1365.981			
Final	804.864	561.117	750	1.000

Goodness-of-Fit

	Chi-Square	df	Sig.
Pearson	114617.734	5700	<.001
Deviance	797.932	5700	1.000

Table 5: Pseudo R-square

Pseudo R-Square

Cox and Snell	.918
Nagelkerke	.920
McFadden	.409

The Likelihood Ratio Tests (LRT) results are shown in table 6 below, highlighting that in addition to ‘cyberknowledge’ and ‘cyberthreatsknowledge’, age and gender are significant predictors in the ordinal logistics regression model. The large chi-square value of 5416.587 with 150 degrees of freedom is highly significant (p < .001), showing that age is a very significant predictor in the model. Similarly, the chi-square value of 54.807 with 30 degrees of freedom is significant (p = .004), indicating that gender is a significant predictor. On the other hand, the ‘role at the university’, ‘field of study or department’, ‘university’ and ‘year of study’ are non-significant predictors with p-values greater than 0.05.

Table 6: Likelihood Ratio Tests

Likelihood Ratio Tests				
	Model Fitting Criteria	Likelihood Ratio Tests		
Effect	-2 Log Likelihood of Reduced Model	Chi-Square	df	Sig.
Intercept	804.864[a]	.000	0	.
Cyberknowledge	866.351[b]	61.487	30	<.001
Cyberthreatsknowledge	867.043[b]	62.179	30	<.001
Age	6221.451[b]	5416.587	150	<.001
Gender	859.671[b]	54.807	30	.004
Roleattheuniversity	796.078[b]	.	30	.
Fieldofstudyordepartment	856.485[b]	51.621	150	1.000
University	828.914[b]	24.050	180	1.000
Yearofstudy	917.045[b]	112.181	150	.991

The chi-square statistic is the difference in -2 log-likelihoods between the final model and a reduced model. The reduced model is formed by omitting an effect from the final model. The null hypothesis is that all parameters of that effect are 0.

a. This reduced model is equivalent to the final model because omitting the effect does not increase the degrees of freedom.

b. Unexpected singularities in the Hessian matrix are encountered. This indicates that either some predictor variables should be excluded or some categories should be merged.

The parameter estimates for the ordinal logistic regression analysis are shown in Table 7 with location parameter estimate of 0.943 and 0.520 for cyberknowledge and cyberthreatsknowledge respectively. Both variables are statistically significant at the 0.001 level (p-value = <.001). The positive and highly significant coefficient suggest that both higher 'Cyberknowledge' and 'Cyberthreatsknowledge' increases the odds of being in a higher category of 'Cyberpractices'. The effect is statistically significant at the 0.001 level. The demographic variables (age, gender, role, field, HEI, year) are not significant predictors of cyberpractices. Therefore, the results suggest that knowledge in cybersecurity and cyber threats are crucial factors in determining better cybersecurity practices, while demographic factors like age, gender, and professional role, field of study, institution, and year of study do not significantly influence cybersecurity practices.

Based on these results, the null hypothesis (*H0* "*Cyberknowledge and Cyberthreatsknowledge together do not significantly predict Cyberpractices"*) is rejected as both these variables have an effect on cyberpractices.

Table 7: Parameter estimates

Parameter Estimates

							95% Confidence Interval	
		Estimate	Std. Error	Wald	df	Sig.	Lower Bound	Upper Bound
Threshold	[Cyberpractices = 1.00]	.661	1.936	.116	1	.733	-3.133	4.454
	[Cyberpractices = 1.20]	1.229	1.918	.410	1	.522	-2.531	4.988
	[Cyberpractices = 1.40]	1.720	1.909	.812	1	.367	-2.021	5.462
	[Cyberpractices = 1.50]	1.802	1.908	.892	1	.345	-1.938	5.541
	[Cyberpractices = 1.60]	2.265	1.904	1.415	1	.234	-1.466	5.995
	[Cyberpractices = 1.80]	2.574	1.902	1.831	1	.176	-1.154	6.302
	[Cyberpractices = 2.00]	3.242	1.902	2.905	1	.088	-.486	6.970
	[Cyberpractices = 2.20]	3.554	1.903	3.487	1	.062	-.176	7.284
	[Cyberpractices = 2.25]	3.586	1.903	3.549	1	.060	-.145	7.316
	[Cyberpractices = 2.40]	3.931	1.905	4.257	1	.039	.197	7.666
	[Cyberpractices = 2.50]	3.957	1.906	4.313	1	.038	.223	7.692
	[Cyberpractices = 2.60]	4.330	1.908	5.147	1	.023	.589	8.070
	[Cyberpractices = 2.75]	4.354	1.909	5.204	1	.023	.613	8.095
	[Cyberpractices = 2.80]	4.671	1.912	5.970	1	.015	.924	8.417
	[Cyberpractices = 3.00]	5.316	1.919	7.676	1	.006	1.555	9.076
	[Cyberpractices = 3.20]	5.674	1.923	8.705	1	.003	1.905	9.443
	[Cyberpractices = 3.25]	5.698	1.923	8.777	1	.003	1.928	9.467

	[Cyberpractices = 3.40]	6.205	1.930	10.340	1	.001	2.423	9.988
	[Cyberpractices = 3.50]	6.233	1.930	10.426	1	.001	2.449	10.016
	[Cyberpractices = 3.60]	6.463	1.933	11.176	1	<.001	2.674	10.252
	[Cyberpractices = 3.75]	6.525	1.934	11.381	1	<.001	2.734	10.316
	[Cyberpractices = 3.80]	6.861	1.939	12.520	1	<.001	3.060	10.661
	[Cyberpractices = 4.00]	7.429	1.948	14.548	1	<.001	3.611	11.246
	[Cyberpractices = 4.20]	7.624	1.951	15.269	1	<.001	3.800	11.447
	[Cyberpractices = 4.25]	7.676	1.952	15.465	1	<.001	3.850	11.501
	[Cyberpractices = 4.40]	7.910	1.956	16.352	1	<.001	4.076	11.744
	[Cyberpractices = 4.50]	7.976	1.957	16.603	1	<.001	4.139	11.812
	[Cyberpractices = 4.60]	8.445	1.968	18.419	1	<.001	4.588	12.301
	[Cyberpractices = 4.75]	8.765	1.976	19.667	1	<.001	4.891	12.639
	[Cyberpractices = 4.80]	9.398	2.001	22.052	1	<.001	5.476	13.321
Location	Cyberknowledge	.943	.186	25.695	1	<.001	.578	1.307
	Cyberthreatsknowledge	.520	.149	12.227	1	<.001	.228	.811
	[Age=1]	-.040	1.290	.001	1	.976	-2.569	2.489
	[Age=2]	.469	1.172	.160	1	.689	-1.829	2.766
	[Age=3]	.317	1.207	.069	1	.793	-2.050	2.683
	[Age=4]	-.585	1.129	.268	1	.604	-2.797	1.627
	[Age=5]	-.726	1.089	.444	1	.505	-2.861	1.409
	[Age=6]	0[a]	.	.	0	.	.	.
	[Gender=1]	-.380	.442	.740	1	.390	-1.247	.486
	[Gender=2]	0[a]	.	.	0	.	.	.
	[Role=1]	-.728	.706	1.061	1	.303	-2.112	.657
	[Role=2]	0[a]	.	.	0	.	.	.

	[Field=1]	-.196	.569	.119	1	.730	-1.312	.919
	[Field=2]	-1.117	.835	1.789	1	.181	-2.753	.520
	[Field=3]	-.054	.305	.031	1	.859	-.653	.544
	[Field=4]	.299	.692	.187	1	.665	-1.057	1.655
	[Field=5]	-1.371	.808	2.878	1	.090	-2.955	.213
	[Field=6]	0[a]	.	.	0	.	.	.
	[HEI=1]	.916	1.386	.437	1	.509	-1.801	3.633
	[HEI=2]	.439	1.477	.088	1	.766	-2.456	3.333
	[HEI=3]	.364	1.698	.046	1	.830	-2.964	3.693
	[HEI=4]	.527	1.372	.147	1	.701	-2.163	3.216
	[HEI=5]	.153	1.727	.008	1	.929	-3.232	3.538
	[HEI=6]	1.817	2.293	.628	1	.428	-2.677	6.310
	[HEI=7]	0[a]	.	.	0	.	.	.
	[Year=1]	.695	.842	.683	1	.409	-.954	2.345
	[Year=2]	.851	.857	.985	1	.321	-.829	2.532
	[Year=3]	1.339	.881	2.310	1	.129	-.387	3.065
	[Year=4]	-.034	1.043	.001	1	.974	-2.078	2.011
	[Year=5]	.620	.921	.454	1	.501	-1.185	2.425
	[Year=6]	0[a]	.	.	0	.	.	.

Link function: Logit.

a. This parameter is set to zero because it is redundant.

Effect of gender

The analysis of the distribution of the variables based on gender using the independent-samples Mann-Whitney U Test showed that gender plays a significant role in influencing Cyberknowledge, Cyberthreatsknowledge, and Cyberpractices as differences in the levels of these variables between male and female were statistically significant (Table 8). The null hypothesis is rejected at the 5% significance level (p-value = 0.042) suggesting that there is a statistically significant difference between males and females.

Table 8: Effect of gender

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.[a,b]	Decision
1	The distribution of Cyberknowledge is the same across categories of Gender.	Independent-Samples Mann-Whitney U Test	.042	Reject the null hypothesis.
2	The distribution of Cyberthreatsknowledge is the same across categories of Gender.	Independent-Samples Mann-Whitney U Test	.034	Reject the null hypothesis.
3	The distribution of Cyberpractices is the same across categories of Gender.	Independent-Samples Mann-Whitney U Test	.002	Reject the null hypothesis.

a. The significance level is .050.

b. Asymptotic significance is displayed.

Independent-Samples Mann-Whitney U Test Summary

Total N	269
Mann-Whitney U	5183.000
Wilcoxon W	32211.000
Test Statistic	5183.000
Standard Error	438.337
Standardized Test Statistic	2.033
Asymptotic Sig.(2-sided test)	.042

Effect of age and role at the HEI

The Kruskal-Wallis test results showed that there is no statistically significant differences in cyberknowledge, cyberthreatsknowledge, or cyberpractices across the different age groups in the sample. Thus, despite variations in the mean ranks, the differences are not significant enough to reject the null hypothesis for any of the categories tested (Table 9).

Table 9: Kruskal-Wallis Test for Age

Kruskal-Wallis Test

Ranks

	Age	N	Mean Rank
Cyberknowledge	Below 18	13	143.46
	18-24	185	126.57
	25-34	32	144.58
	35-44	21	167.62
	45-54	14	163.75
	55 and above	4	148.75
	Total	269	
Cyberthreatsknowledge	Below 18	13	151.42
	18-24	185	128.31
	25-34	32	154.81
	35-44	21	151.90
	45-54	14	136.86
	55 and above	4	137.25
	Total	269	
Cyberpractices	Below 18	13	126.65
	18-24	184	138.08
	25-34	32	147.16
	35-44	21	122.40
	45-54	14	95.96
	55 and above	4	92.38
	Total	268	

Test Statistics[a,b]

	Cyberknowledge	Cyberthreatsknowledge	Cyberpractices
Kruskal-Wallis H	8.582	5.050	6.557
df	5	5	5
Asymp. Sig.	.127	.410	.256

a. Kruskal Wallis Test

b. Grouping Variable: Age

Further, the Mann-Whitney U Test showed that there is no statistically significant differences between staff and students in terms of Cyberknowledge and Cyberthreatsknowledge. However, there is a statistically significant difference in terms of cyberpractices (p-value = 0.04). The significant result for cyberpractices indicates that the staff and students at the HEIs have different practices related to cybersecurity, while their knowledge of cybersecurity and cyber threats does not significantly differ.

Table 9: Kruskal-Wallis Test for Role at the University

Test Statistics[a]

	Cyberknowledge	Cyberthreatsknowledge	Cyberpractices
Mann-Whitney U	3669.500	3586.500	3021.500
Wilcoxon W	31635.500	31552.500	3582.500
Z	-.538	-.736	-2.057
Asymp. Sig. (2-tailed)	.591	.461	.040

a. Grouping Variable: Roleattheuniversity

Discussion:

The findings in this study highlight that both general and specific cybersecurity knowledge play crucial roles in promoting good cybersecurity behaviors. These results reinforce the critical role of knowledge in fostering effective cybersecurity practices, supporting findings from other studies (Alotaibi et al., 2016; Ifinedo, 2012; Parsons et al., 2017; Siponen et al., 2014), that emphasize that knowledge and awareness are crucial in mitigating cybersecurity risks. As knowledge is a pivotal determinant of cybersecurity behavior, this underscores the importance of educational interventions aimed at enhancing both general and specific cybersecurity knowledge to promote safer online behaviors.

In addition, the findings of this study reveal some significant deficiencies in cybersecurity awareness among both staff and students in higher education institutions (HEIs) in Kuwait. While a moderate level of general awareness is present, specific knowledge regarding common cyber threats and best practices remains insufficient. This inadequacy presents a substantial risk to the security of HEIs' information assets, supporting the assertions of Alenezi (2024) and Al-Alawi & Hafedh (2006), who emphasize the critical role of awareness in mitigating cybersecurity threats.

The study found no significant differences in cyber knowledge, cyber threats knowledge, or cyber practices across different age groups or between staff and students. This is consistent with findings from Warkentin et al. (2012) that suggest while knowledge and awareness are critical, demographic factors like age might not significantly influence cybersecurity behavior. This finding, however, is contrary to other studies (Aloul, 2012; Drevin et al., 2007) that showed disparity in cybersecurity awareness between staff and students. These studies found that staff members demonstrated a higher level of awareness attributable to staff members' greater exposure to institutional training and resources. Institutional efforts to educate staff on cybersecurity protocols and the provision of ongoing training are essential factors that contribute to their heightened awareness (Aloul, 2012; Drevin et al., 2007). Age has been shown as a determinant of cybersecurity awareness in some studies (Khader et al., 2021; Vestad & Yang, 2024), with older individuals displaying superior knowledge and practices. This trend is likely due to the cumulative experience and exposure to cybersecurity training over time. However, contrary to this argument, this study did not reveal any significant differences across the age groups.

In addition, significant differences were observed in cyber knowledge, cyber threats knowledge, and cyber practices between males and females. This aligns with some studies, such as by Sheeran et al. (2014), which found gender differences in risk perception and information security behavior, suggesting that targeted interventions might be necessary to address these disparities. This finding, however, is contrary to other studies, such as Eltahir & Ahmed (2023), that did not find gender as a significant determinant of cybersecurity awareness levels.

In general, the study findings align with global perspectives on cybersecurity awareness in HEIs. For instance, Kruger et al. (2011) and Carpenter & Schutten (2020) emphasize the necessity of fostering a cybersecurity culture within educational institutions. The observed gaps in specific knowledge and practices mirror those identified in other regions, suggesting that HEIs worldwide face similar challenges in achieving comprehensive cybersecurity awareness. This global context reinforces the importance of tailored, continuous education and awareness initiatives, as recommended by Cheng & Wang (2022), to cultivate a secure and informed academic environment. In addition to educational interventions and tailored training, HEIs should develop policies that encourage continuous learning and awareness of evolving cyber threats to maintain high standards of cybersecurity practices.

Conclusion:

This study underscores the urgent need for comprehensive cybersecurity awareness programs in HEIs in Kuwait. The identified gaps in knowledge and practices highlight the vulnerability of HEIs to cyber threats. To address these challenges, HEIs should implement targeted training programs that cater to the specific needs of staff and students. Continuous education and awareness campaigns are essential to foster a culture of cybersecurity and ensure the protection of valuable information assets.

The necessity of a strategic approach to cybersecurity awareness is evident. This involves not only the dissemination of knowledge but also the practical application of cybersecurity principles. As recommended by Falkner et al. (2016) and Hunt (2016), effective cybersecurity education should encompass regular training sessions, simulated phishing exercises, and clear communication of institutional policies. These measures will help in translating awareness into actionable practices, thereby reducing the risk of cyber incidents.

Additionally, the findings suggest that while demographic factors such as gender within the institution influence awareness levels, there is a critical need for a universally inclusive approach to cybersecurity education. This approach should consider the diverse experiences and needs of all HEI stakeholders, ensuring that both staff and students are adequately equipped to navigate the complex landscape of cybersecurity threats.

In conclusion, the study provides a compelling case for the enhancement of cybersecurity awareness programs in Kuwaiti HEIs. By addressing the identified gaps and implementing comprehensive educational strategies, HEIs can significantly bolster their defense against cyber threats, safeguarding their information assets and maintaining their integrity in the digital age. Some limitations of the study are acknowledged such as sample diversity and self-reported data since the sample is limited to settings in HEIs in Kuwait, which might not be generalizable to other populations or sectors. The study also relies on self-reported data which could introduce bias, as participants might overestimate their knowledge or practices. Future research should explore the studied relationships in more diverse settings and consider longitudinal studies to examine how changes in knowledge over time influence cybersecurity practices. Additionally, qualitative research could provide deeper insights into the reasons behind demographic differences in cybersecurity behavior.

References

1. Al-Alawi, A.I. and Hafedh, S.H. (2006) ‘Information security in higher education institutions in Kuwait’, *Information Security Journal: A Global Perspective*, 15(6), pp. 303-313.
2. Alenezi, A.F. (2024) ‘Cybersecurity challenges in HEIs’, *Journal of Cybersecurity*, 12(1), pp. 45-60.
3. Aloul, F.A. (2012) ‘The need for effective information security awareness’, *Journal of Advances in Information Technology*, 3(3), pp. 176-183.
4. Alzahrani, S. (2021) ‘Cybersecurity awareness in Saudi Arabian universities’, *Journal of Information Security and Cybercrimes Research*, 3(2), pp. 25-35.
5. Cheng, L. and Wang, Z. (2022) ‘Factors influencing cybersecurity awareness’, *Cybersecurity Journal*, 10(4), pp. 223-237.
6. Drevin, L., Kruger, H. and Steyn, T. (2007) ‘Information security awareness: Educating your users effectively’, *Information Security Technical Report*, 12(4), pp. 190-194.
7. Eltahir, A. and Ahmed, S. (2023) ‘Cybersecurity awareness among students in Sudanese universities’, *African Journal of Information Systems*, 15(1), pp. 67-85.
8. Garba, A., Bello, M. and Gambo, M. (2020) ‘Cybersecurity challenges in Nigerian HEIs’, *Journal of Cybersecurity Education*, 18(2), pp. 99-112.
9. Hunt, R. (2016) ‘Cybersecurity education in HEIs’, *Journal of Information Security Education*, 14(3), pp. 124-137.

10. Khader, M., Alomari, H. and Al-Shalabi, S. (2021) ‘Cybersecurity practices in Middle Eastern universities’, *International Journal of Information Security*, 20(2), pp. 144-156.
11. Kruger, H., Drevin, L. and Steyn, T. (2011) ‘Assessing the effectiveness of cybersecurity awareness programs in South African HEIs’, *Information Security Journal: A Global Perspective*, 20(1), pp. 22-34.
12. Kwon, H. (2024) ‘Cybersecurity in higher education: Global trends and challenges’, *Journal of Global Information Security*, 16(1), pp. 33-48.
13. Rafiq, M., Saleem, H. and Rehman, M. (2024) ‘Digital transformation and cybersecurity in education’, *Journal of Digital Education*, 10(1), pp. 78-91.
14. Raju, R., Mathew, T. and Abraham, R. (2022) ‘Cybersecurity awareness among university students in Malaysia’, *International Journal of Cybersecurity Education*, 12(3), pp. 165-179.
15. Rezgui, Y. and Marks, A. (2008) ‘Information security awareness in higher education: An exploratory study’, *Computers & Security*, 27(7-8), pp. 241-253.
16. Sheeran, P., Webb, T. and Gollwitzer, P. (2014) ‘Gender differences in risk perception and information security behavior’, *Journal of Risk Research*, 17(3), pp. 287-302.
17. Triplett, M. (2023) ‘Cybersecurity threats in higher education institutions’, *Journal of Cybersecurity Research*, 9(2), pp. 201-215.

18. Ulven, J. and Wangen, G. (2021) ‘Theoretical perspectives on cybersecurity awareness’, *Journal of Cybersecurity Education,* 7(1), pp. 45-60.
19. Veluvali, M. and Surisetti, R. (2022) ‘Comprehensive overview of cybersecurity threats and protective measures’, *International Journal of Information Security*, 15(2), pp. 123-140.
20. Vestad, T. and Yang, S. (2024) ‘Cybersecurity awareness: The role of education and training’, *Journal of Information Security Education,* 18(1), pp. 11-29.

Appendix:

Descriptive statistics

Descriptives of variables

			Statistic	Std. Error
Cyberknowledge	Mean		2.8683	.05201
	95% Confidence Interval for Mean	Lower Bound	2.7659	
		Upper Bound	2.9707	
	5% Trimmed Mean		2.8793	
	Median		3.0000	
	Variance		.728	
	Std. Deviation		.85307	
	Minimum		1.00	
	Maximum		4.80	
	Range		3.80	
	Interquartile Range		1.20	
	Skewness		-.194	.149
	Kurtosis		-.509	.296
Cyberthreatsknowledge	Mean		2.8323	.06273
	95% Confidence Interval for Mean	Lower Bound	2.7088	
		Upper Bound	2.9559	
	5% Trimmed Mean		2.8227	
	Median		2.8000	
	Variance		1.059	
	Std. Deviation		1.02893	
	Minimum		1.00	
	Maximum		5.00	
	Range		4.00	
	Interquartile Range		1.60	
	Skewness		.113	.149
	Kurtosis		-.674	.296
Cyberpr	Mean		2.9991	.06119

actices	95% Confidence Interval for Mean	Lower Bound	2.8786	
		Upper Bound	3.1195	
	5% Trimmed Mean		3.0009	
	Median		3.0000	
	Variance		1.007	
	Std. Deviation		1.00359	
	Minimum		1.00	
	Maximum		5.00	
	Range		4.00	
	Interquartile Range		1.35	
	Skewness		-.044	.149
	Kurtosis		-.575	.296