Cybersecurity Behaviour Intensions in Students

MSc Research Project
Cybersecurity

Ita George Ekanem
Student ID:22126139

School of Computing
National College of Ireland

Supervisor: Arghir Nicolae Moldovan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Ita George Ekanem ………

Student ID: 22126139 ………..……

Programme: MSCCYB …………………………………………………………… **Year:** ……2023……………………….

Module: MSC Research Project ……………………………………………………………………………………………….………

Supervisor: Arghir Nicolae Moldovan ………………………………………………………………………………………….…………

Submission Due Date: 21/12/23 ………………………………………………………………………………………….…………

Project Title: Cybersecurity Behaviour Intensions in Students ………………………………………………………………………………………….…………

Word Count: 7123 ……………………………………… **Page Count** 22…………………………………………….……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Ita George Ekanem ……

Date: 21/12/23 ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Cybersecurity Behaviour Intentions in Students

Ita George Ekanem
22126139

Abstract

Human error is frequently mentioned as the main weakness in the field of cybersecurity. Given the extensive use of online services for education and communication, students face a multitude of cybersecurity threats daily and research/information on students' cybersecurity practices is very limited. This study intends to investigate the variables affecting students' cybersecurity behaviour, find relationships between particular human characteristics and intentions for cybersecurity behaviour, evaluate the degree to which students demonstrate positive cybersecurity attitudes, and determine their readiness to improve their practices. Validated factors considered in this study include perceived vulnerability, perceived barriers, perceived severity, response efficacy, cues to action, peer behaviour, personality traits, decision making style, online security behaviour, consideration for future consequences, computer and internet skills, prior experience with computer security practices, perceived benefits, and familiarity with cyber threats. By looking at the relationship between these traits and the cybersecurity behaviour of students, this study strives to illuminate the driving forces behind their practices. By strategically combining past surveys with statical significance extracted from past research on cybersecurity behaviour, this research builds upon and extends the work of Margaret Gratian, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther on correlating human traits and cybersecurity behaviour intentions. With the use of a comprehensive survey which was conducted among current students of NCI.

Key words: Perceived vulnerability, Cybersecurity behavior, human factor, Students

1 Introduction

The human factor is the weakest link in the chain of defense and the Achilles' heel in the complex world of cybersecurity. Even with the strong technical defenses in place to protect systems and data, breaches and security vulnerabilities are mostly caused by human error and mistake. The amount of data that is exchanged and the frequency of interactions that take place online greatly increase the occurrence and possibility of human error which increases the vulnerability of a system. Due to the frequent use of computer systems and the internet, students are especially vulnerable to this cybersecurity dangers as students would spend a huge portion of their academical lives online. Digital connectivity has become an essential component of students' academic career, from working with peers and performing research to using online study tools, completing assessments and entertainment. In some instances, students even opt for fully online learning environments, further amplifying their vulnerability. This immersive digital experience, while offering convenience and access to a vast repository of knowledge, also exposes them to a wider array of cyber-threats. The widespread prevalence of malware infections, social engineering techniques, and phishing schemes presents a serious risk to students' private information and academic integrity. Students may be particularly vulnerable to falling for fraudulent techniques or malicious intensions because of the attraction of free resources, their need to communicate with classmates/peers, and the absence of in-person contacts in virtual learning settings. Consequently, it is essential to look at how students are currently behaving in terms of cybersecurity and to foster a culture of cybersecurity awareness among them. To secure their online presence and maintain the integrity of the institutional systems, it is essential to provide students with the knowledge and abilities to understand the inherent risks of the digital world and to traverse it securely. By fostering a positive behavior in students' online behavior, emphasizing the importance of good security practice like strong passwords, cautious clicking and downloading, and proactive attention, it is possible to significantly enhance the cybersecurity posture of schools and educational institutions. Cultivating a cybersecurity-conscious generation of students will not only protect their individual well-being but also contribute to a more secure and resilient cyber ecosystem.

1.1 Novelty and Contribution

This project boost novelty and contribution of.

1. strategically combining 7 past surveys using statical significance.
2. Extends the work of Margaret Gratian, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther on correlating human traits and cybersecurity behaviour intentions.
3. The inclusion of a future behavioural questionnaire which tackles static limitation of surveys.

1.2 Aim

The aim of this project is to investigate the factors that affect students' cybersecurity behaviour, identify relationships between human characteristics and cybersecurity intentions, and assess the readiness of students to improve their cybersecurity practices.

1.3 Research question

To what extent do students’ cybersecurity behaviour intentions depend on their perceived vulnerability to cyberattacks?

2 Related Work

2.1 Cybersecurity and the Internet: How They Affect People and Their Lives

As a result of the rapid growth of the cyberspace, significant changes in the ways information is generated, accessed, and utilized are seen across the globe. People's ability to connect with one another and build communities has considerably enhanced as a result of their use of the Internet. People are increasingly relying on the internet for a variety of personal and professional social contacts, such as frequent conversations, online shopping, and the use of different online services (for example, banking, schooling, virtual healthcare, and so on). There is no doubt that the internet and other new technologies have transformed every aspect of company operations. In terms of growth rate, the internet has undoubtedly outpaced all other communication mediums during the previous several decades. This means that internet use has increased as a result of advances in information technology. However, there are heightened cyber security issues connected with this growth which may endanger critical economic and infrastructure systems. Cybersecurity vulnerabilities may jeopardise individual internet users' privacy, secrecy, and identity. Furthermore, emerging cyber risks such as cybersex, pornography, cyber addiction, online fraud, gaming addiction, and gambling are having a negative influence on both adults and children(Khalid *et al.*, 2018). In today's technologically and information-infused world, cyberspace is an essential component of modern society." Although the Internet is often regarded as the greatest helpful invention ever devised, it also has a dark side that may have a harmful impact on society.

The rapid adoption of cyber technologies and services has led to increased vulnerability to cyber threats, reason being most users are not well-aware of or protected against cyber risks. stressing the importance of creating a cybersecurity culture amongst youths, since they engage with cyberspace from a young age and may perpetuate the culture by passing it on to their own children in the future. This research aims to detection early variations between the campaign's predefined objectives and its actual outcomes from the active audience, ensuring that the fostered cybersecurity culture corresponds with the targeted culture. The research tackles the rising concerns and hazards linked with online activities by concentrating on the creation of a cyber security culture promoting campaign. By exploring Active Audience Theory, this research digs into how users actively participate with cyber security initiatives, emphasising the need of user engagement in ensuring a secure online environment. This link between audience participation and the success of cybersecurity campaigns implies that individuals play an important role in protecting their online experiences. The study's emphasis on communication channels and techniques demonstrates the delicate link between information distribution, audience participation, and the overall success of cyber security measures (Reid and van Niekerk, 2015).

(Zwilling *et al.*, 2022) investigated the impact of cyber security awareness campaigns on internet users' knowledge and behaviour, focusing on cyber threat awareness and defensive actions. The study's findings show that, while internet users are usually aware of cyber risks, they frequently employ very modest preventative measures, which are largely common and easy. Furthermore, regardless of the respondent's nation or gender, the data imply that higher levels of cyber knowledge are connected with increasing cyber awareness. This research is crucial because it throws light on the link between cyber security awareness, knowledge, and behaviour. It is critical to understand how people perceive and respond to cyber threats in order to design effective cybersecurity solutions. The study's findings emphasise the significance of not only raising awareness but also improving internet users' understanding of the subject in order to enhance their cyber security behaviour. Finally, this study adds to a better knowledge of how human factor influence cybersecurity and the internet, and how they could potentially be used to improve security measures.

(Ivanova, 2020) introduced the concept of "eLearning Informatics" to investigate the junction of eLearning and Informatics, evaluating how Informatics might be used to enhance eLearning experiences. Most of all, the study emphasises the importance of cybersecurity in the context of eLearning. As eLearning platforms become more interwoven into educational curriculum, cybersecurity issues such as disruption of eLearning platforms and denial of course work or study Material, cyberbullying and harassment, misinformation, and disinformation, etc. all of which can have a negative impact on students' mental health, well-being and can damage students' learning. Students must be able to critically evaluate the information they find online and be aware of the possibility of bias and manipulation. Therefore, students' perspective and attitude towards cyber security are crucial in determining how they safeguard themselves and the system from online dangers or cyber threats.

Mobile devices are a great target for cyber criminals since they are increasingly being utilised to store sensitive financial and personal data and are the most used device across the globe with some users having multiple mobile devices. This study investigated students' attitudes, behaviours, and security practices when they use mobile devices. Although many students have incorporated secure practices into their daily life, the survey discovered that there was still much space for growth. Moreover, providing a mitigating technique by including security training into organisational learning initiatives to raise user awareness of the risks connected to mobile device use and enhance their security practises (Chin, Etudo and Harris, 2016).

A lot of people in the academic and professional communities are interested in studying people's perspectives and actions in relation to cyber dangers. The impact of cyberattacks on internet users and the level of cyber security awareness among individuals and organizations have also been the subject of several studies. For example, (McCormac *et al.*, 2018) cites research on cyber security awareness as a source of stress in the workplace, and this research applies to both public and private enterprises, and also educational institution. An insight to given on the importance of cyber legislation and security policy formation, as well as the role that staff knowledge and attitude in ensuring an organization's cyber resilience (Hadlington, 2018). (Reid and van Niekerk, 2016) conducted a study on cyber-security awareness among school-aged children and adolescents and found that it had a significant impact. After comparing the targeted school youth's prior understanding of cyber security risks with their newly acquired awareness, the researchers concluded that the campaign had a significant effect on raising their level of cyber security awareness. Furthermore, it was impossible to deny that the internet device had reached a new milestone in its development as a result of the continuous improvement in its technology and convenience. While at the same time the amount of internet and computer device users are also rapidly increasing, which means that the rate of cyber-attacks would also be on the rise and could occur at any moment. This catastrophe would impact not only people but also companies, businesses, educational institutions, and governments. Hence, it is essential for governments, educational institutions, and other relevant groups to do further studies on cybersecurity behavior, especially to compare and contrast the degree of knowledge among users.

2.2 The Idea of Cybersecurity in Relation to Human Behaviour

Culture and environment influence cyber security behavior, especially in vulnerable end users who are susceptible. This paper strongly emphasizes the need to understand cyber security behavior in the context of the surrounding environment and culture, and how crucial it is to quantify cultural elements and how they affect cybersecurity. The paper also emphasizes the need to comprehend these dynamics in order to develop effective strategies to counteract cyber threats and vulnerabilities that are rooted in human behavior. Human behavior is strongly affected by culture and environment, and the posture of cybersecurity is strongly affected by human behavior. Which means that the cybersecurity status is also strongly affected by culture and environment (Joinson and van Steen,). The critical role of understanding the human element in cybersecurity assurance processes and the importance of addressing human factors in cybersecurity measures was investigated by (Evans *et al.*, 2016). Their findings underscore the need to incorporate human behavior considerations into cybersecurity assurance frameworks to effectively mitigate cyber threats and vulnerabilities arising from human actions. The study highlights the need to include social context of human behavior in cybersecurity measures by highlighting the necessity to understand the social context of humans and how it affects behavior in cybersecurity. In order to effectively mitigate cyber risk and vulnerabilities resulting from human behavior within the framework of social roles, social status, social interactions, and technology usage, it is important to understand these social constructs of humans (Muller and Burrell, 2022).

2.3 Cybersecurity Practices and Regular Users

(Rajivan *et al.*, 2017) Investigates the relevant to cybersecurity practices and users by providing a tool for measuring end-user security expertise. Identifying critical factors that contribute to end user security competence such as computer skills, advanced computer skills, security knowledge, and advanced security skills, the paper highlights the importance of understanding and addressing human behavior in the context of cybersecurity measures. This understanding can help organizations develop effective strategies to mitigate cyber threats and vulnerabilities associated with human behavior and lack of security expertise. In addition, (Halevi *et al.*, 2016) investigated users demographic, cultural, and psychological factors as they pertain to cyber-security. Culture was shown to be a predictor of privacy attitude but had less impact on conduct, according to their findings. In addition, (Coffey, 2017) research sought to address and illustrate the interactions between humans and technology, indicating that, if users learn from their mistakes, of course, users hold both the key to fixing the problem of being the security weak link and also represent the biggest cybersecurity threats. Furthermore, Coffey's study made an effort to draw attention to the need of technology and training that may, in some way, protect systems and, therefore, system users by addressing the roles of human errors that make individuals susceptible on the Internet.

The study by (Noureddine *et al.*, 2017) emphasizes the necessity of precise human user models in cybersecurity, which can be influenced by social science and psychology behavioral theories. The General Deterrence Theory, Protection Motivation Theory, Social Learning Theory, and Social Bond Theory are just a few of the well-known behavioral theories that the authors examine. The study also talks about how these theories might be used to create predictive models of human behavior in cybersecurity. While also highlighting how crucial it is to include human user models in these predictive models.

2.4 Papers Used to Create This Research Project Survey

This paper by (Gratian *et al.*, 2018) established a relationship between human traits and intents for cyber security behaviour. the study presents a thorough analysis that looks at how risk-taking preferences, decision-making styles, demographics, and personality traits affect the security behaviour intentions of device securement, password generation, proactive awareness, and updating. While highlighting the works of previous papers that found correlations between specific human traits and specific cyber security behaviour intentions, the study analysis goes much deeper. The study surveyed 369 students, teachers, and staff, with a questionnaire of 148 questions at a university in order to expand and confirm the findings of Egelman and Peer. The study discovered that individual variations accounted for 5%–23% of the variance in cyber security behaviour intentions.

The goal of the research by (Alsharif, Mishra and Alshehri, 2021) was to solve human factors-related cybersecurity concerns. Since human error is responsible for a large amount of security concerns, the research aims to reduce vulnerabilities and increase user awareness by using a survey with 333 participants and 13 questions. Participants were chosen from among men, women, professionals, students, and others, and they came from all parts of Saudi Arabia. It was shown that most survey respondents were ignorant of the risks associated with cybersecurity and how to protect their personal information. They were also confused about the top three human factors affecting their attitude towards cybersecurity. Passwords, phishing scams, and social engineering assaults are just a few examples of vulnerabilities that still need to be addressed and mitigated with the right knowledge and training.

This study examines the University of Sulaimani's (located in the Kurdistan Region of Iraq) understanding of social engineering assaults and cyber-security concerns. The University of Sulaimani's internet users jeopardised their private information because of the rise in social engineering dangers and their ignorance of cyber security. A self-report questionnaire consisting of 16 questions was utilised in this quantitative study to collect primary data from 1779 participants (students and staff). The University of Sulaimani used an online poll to estimate the number of staff and student victims of social engineering. Finally, this study aims to assess participants' cyber-security knowledge and examine their awareness of data breaches caused by social engineering (Abdulla *et al.*, 2023).

This study employed a relatively straightforward data collection technique with the use of a survey containing 16 questions. Many students were sent questionnaires as part of an experiment by the research to determine whether they would provide their information if they were informed that it was for academic purposes. A large number of students responded to the poll, which asked for their name, social media accounts, email address, and other information. Subsequently, the researchers tested the students' awareness of these intrusions by sending them phishing emails. Additionally, the survey data is used by the researchers for reconnaissance. The study demonstrated how susceptible the educational sector is to common cyberattacks as the survey was a cover for a deeper social engineering research with the objectives to find out if participants are willing to provide their security information for free, determine whether surveys are an effective phishing weapon, ascertain whether surveys can aid in potential attacker reconnaissance, find out if individuals are knowledgeable enough to recognise a phishing attempt. And to identify strategies for stopping security exploitation (Blancaflor *et al.*, 2021).

This study's objective was to examine the level of social engineering knowledge in Saudi Arabia's educational system using a questionnaire containing 26 question and 465 participants, the survey questions served the purpose of gauging the level of familiarity with social engineering tactics. According to the findings, 158 individuals, or 34% of the total, had prior experience with social engineering techniques, which shows that in terms of security practices and abilities, there are notable disparities between those who had prior knowledge of social engineering and those who had not. This study's conclusion was that, in the Saudi educational system, training plays a crucial role in raising awareness of social engineering attacks (Alsulami *et al.*, 2021).

This study highlights how crucial it is for cyber defenders to understand the methods used by hackers and other bad actors to try to communicate with people. claiming that social engineers are experts who occasionally engage in deviant behaviour for good in order to help people recognise signs that another actor is engaging in deviant behaviour for fraudulent ends. In order to ascertain if the defensive strategies being employed to shield against deviant actors are improving defence against these group, this study set out to investigate social engineering from both ends of the legal spectrum. through a mixed method survey of 26 questions and 465 social engineers (participants) (Austin, Adrian, 2022).

Although this study isn't related to cyber security, the aim of this study is a huge contribution as it investigates how concern is handled, assessing concern with future consequences (CFC-Future) and concern with immediate consequences (CFC-Immediate) to see if users plan for concerns of the future or ignore it. Applying this approach to cyber security will greatly improve the future security status by handling future concerns as well as immediate concerns (Joireman *et al.*, 2012).

2.5 Limitation of Past Research

The majority of the research data come from questionnaires, which are subject to self-reporting bias. Participants may be swayed by social desirability bias, which is the inclination to provide answers to questions that are deemed to be socially acceptable, and thus may not always be truthful in their responses to assessments of their cyber security conduct or knowledge. A survey-based experiment may also be challenging and time-consuming since participants might not be willing or able to devote the necessary time to complete the survey. Lastly, participants lose interest and concentration quickly and would opt out of or rush through lengthy surveys which would cause short of data or a lot of inaccurate data.

The research is restricted to particular demographics or environments. Despite the study's main focus on the education sector, the research conclusions might not apply to other demographics or educational environments, and they might not be able to represent the full complexity of human behaviour in relation to cybersecurity.

The research findings are mostly focused on the current situations since they don't offer a long-term perspective of how cybersecurity behaviour evolves over time or how it is impacted by unknown future events, they only assess the state of cybersecurity behaviour as it exists in the period of the study.

The research ignores the impact of organisational elements and leaders and majorly focus on the role that individuals have in cybersecurity conduct. This is crucial observation as none of the studies mentioned organizations can have a big impact on encouraging cybersecurity awareness and behaviour among their staff members, leaders can have a similar impact on followers, and teachers and instructors can have a big impact on students' cybersecurity behaviour.

3 Research Methodology and Specification

3.1 Paper search

An exhaustive search of academical databases, including PubMed, IEEE Xplore, Research gate and Google Scholar, was conducted using keywords such as " cybersecurity behavior," "social engineering," "students," and "survey." This process was utilized in the identification of a pool of relevant research papers that included surveys of the intended demographic (students), detailed analysis of collected data and its statical importance, detailed findings and conclusions.

3.2 In-depth Paper analysis

Through systematic evaluation on the pool of discovered research papers and their survey appendixes were identified, scrutinized, and synthesized to craft a robust instrument. Papers were meticulously screened based on their abstracts, aims and methodology to ensure alignment with the research question or objectives. Following this selective approach, seven papers emerged as the final selection, meeting all the stringent criteria needed for the development of a new comprehensive survey. The selected papers as follows.

- Paper 1: Impact of Human Vulnerabilities on Cybersecurity (Alsharif, Mishra and Alshehri, 2021). Containing 13 Questions
- Paper 2: Risk Assessments of Social Engineering Attacks and Set Controls in an Online Education Environment (Blancaflor *et al.*, 2021) containing 16 Questions
- Paper 3: Analysis of Social Engineering Awareness Among Students and Lecturers (Abdulla *et al.*, 2023). Containing18 Questions.
- Paper 4: Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia (Alsulami *et al.*, 2021). Containing 24 Questions.
- Paper 5: Correlating human traits and cyber security behaviour intentions (Gratian *et al.*, 2018). Containing 148 Questions.
- Paper 6: Survey of social Engineers and the Validity of defence Techniques (Austin, Adrian, 2022). Containing 35 Questions
- Paper 7: Promotion Orientation Explains Why Future-Oriented People Exercise and Eat Health 14 questions (Joireman *et al.*, 2012)

3.3 Data Sheet Creation

Following the in-depth data analysis was the extraction of the survey questions, response options, and question category, all following the predefined order of the chosen papers. The extracted data was put into a data sheet for further analysis of the survey questions, highlighting all categories, subcategories, question types, paper answer options, and the rationale behind each question's selection. The data sheet contained a total of 268 questions from 7 research papers, as follows.

3.4 Question selection.

The question selection was completely influenced by one of the selected papers, Paper 5: Correlating human traits and cyber security behaviour intentions (Gratian *et al.*, 2018). This was because the paper was an improvement of the study Behavior Ever Follows Intention?: A Validation of the Security Behavior Intentions Scale (SeBIS) (Egelman, Harbach and Peer, 2016) which is standard for the measurement of cyber security behaviour, and more importantly for the reason that it is the closest study to my research and I make improvements to paper 5.

Following a systematic order, the questions of each paper where reviewed and selected based on relation or complementing seBIS

Paper 1: Out of 13 questions, 4 questions complimented SeBIS and where selected. that complement SeBIS, rephrased most of them to use the SeBIS 5-point scale

Paper 2: No questions selected, as the survey used in this paper was part of a simulated phishing attack to collect personal info, and participants were not properly informed.

Paper 3: Out of 18 questions, 6 questions complimented SeBIS and where selected. rephrased most of them to use SeBIS 5-point scale (instead of 3-point scale).

Paper 4 : Out of 24 questions, 6 questions complimented SeBIS and where selected

Paper 5: Paper 5 being different from the other papers, its questions where selected based on statistical significance. Paper 5 had a total of 148 questions distributed over 5 categories, (Demographic, Personality traits, Decision making styles, Online security behaviour, Risk taking preference). The entire Demographic category was not selected as it would not correspond to my desired demographic. The Personality trait category had a total of 60 question spread evenly in 6 subcategories. Statistical significant were found in 2 subcategories

(Extraversion and Conscientiousness) and questions of these subcategories where selected. Additionally, the questions of a subcategory (Risk avoidance) were selected to be an improvement as this subcategory was left out of any sort of analysis in the paper. This selection totals 30 questions selected out of 60 in the personality trait category. The decision-making style category had a total of 25 question of 5 subcategories. A total of 10 questions form 2 subcategories where selected for this category. The Online security behaviour category had a total of 16 questions and all questions in the category were selected as this is a category on human security behaviour. Lastly, the Risk-taking preferences category had a total of 30 question and where all not selected as the questions would be too sensitive and personal for the target demographic.

Paper 6: Out of a total of 35 questions no question from this paper was selected. Reason being that the target demographic of this paper where high level social engineers, and the nature of the questions was too complex for the target demographic of this paper (students)

Paper 7: Out of a total of 14 questions, all the questions form these where selected as it servers as a contribution and improvement of the past works

3.5 Question Answer scaling

After the selection of the survey questions the SeBIS scale by (Egelman, Harbach and Peer, 2016) was implemented uniformly through the survey. Questions form Paper 1,3,4 where slightly rephrased to accommodate the use of the SeBIS 5-point scale to answer them. And all scale of paper 5 was maintained from the original paper in order the keep a steady methodology, paper 7 also maintained its 7-point scale.

Table 1: Summary table of papers used for survey.

Citation	Objectives	Participants Breakdown	Method	Analysis methods
Correlating human traits and cyber security behavior intentions	The study aims to link human traits with cybersecurity behavior intentions, focusing on risk-taking, decision-making styles.	369 Students and staff	144 questions	Correlation analysis, Factor analysis, Reliability testing, Multiple regression analysis, ANOVA with post hoc analysis
Impact of Human Vulnerabilities on Cybersecurity	The study aims to address cybersecurity challenges related to human factors. With a significant portion of security risks attributed to human errors, the research focuses on enhancing user awareness and reducing vulnerabilities.	333	13 interview question	Chi-square test
Analysis of Social Engineering	The study aims to assess awareness	1779 Students and Staff	16 questions	Cronpach Alpha's test and ANOVA test

Awareness Among Students and Lecturers	of cyber-security and social engineering attacks at the University of Sulaimani, Kurdistan Region of Iraq. Using a questionnaire, it gathers data to evaluate participants' knowledge of cyber-security and their understanding of social engineering data breaches.			
Risk Assessments of Social Engineering Attacks and Set Controls in an Online Education Environment	The purpose of this research was to find out if students would give out information when told it for academic reasons using a survey		16 questions	
Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia	The aim of this study is to provide a measurement of social engineering awareness in the Saudi educational sector.	465 244 M 221F	26 questions	one-sample t-test And ANOVA test
Survey of social Engineers and the Validity of defence Techniques	The aim of this research was to determine if the current defensive techniques used to protect against deviant actors are having a positive effect.		35 questions	
Promotion Orientation Explains Why Future-Oriented People Exercise and Eat Healthy	The aim of this study was to investigates how concern is handled, assessing concern with		14 questions	Exploratory factor analysis.

	future consequences (CFC-Future) and concern with immediate consequences (CFC-Immediate) to see if users plan for concerns of the future or ignore it			

4 Implementation

Upon finalising the defining the selected questions answer sale, it was used to create a survey on MS form. The survey was systematically created maintaining question arrangement or sequence, categories, and subcategories. After updating the survey with the selected questions, an introduction and consent section was added to the beginning of the survey to ensure transparency and to properly inform participants of the survey, its contents, and its aim. The survey was then distributed to students via email.

The survey response data was automatically uploaded to a MS Excel document where it will undergo preprocessing to be worked on using data analysing tool SPSS.

5 Evaluation

The analysis of the collected data, plots and statistical tests were conducted using the aggregate scores. The reason being that, aggregate scores are more informative than using individual questions to perform analysis or statistical test. Aggregate scores provide a more in-depth view of the student's personality, decision-making style, and online security behavior. Also, aggregate scores are more reliable than individual questions because they are less susceptible to random variation.

The aggregate score was computed by assigning values to the scales used such as 1 - 5 accordingly.

Personality traits (IPIP): (1) Very Inaccurate, (2) Moderately Inaccurate, (3) Neither Inaccurate nor Accurate, (4) Moderately Accurate, (5) Very Accurate.

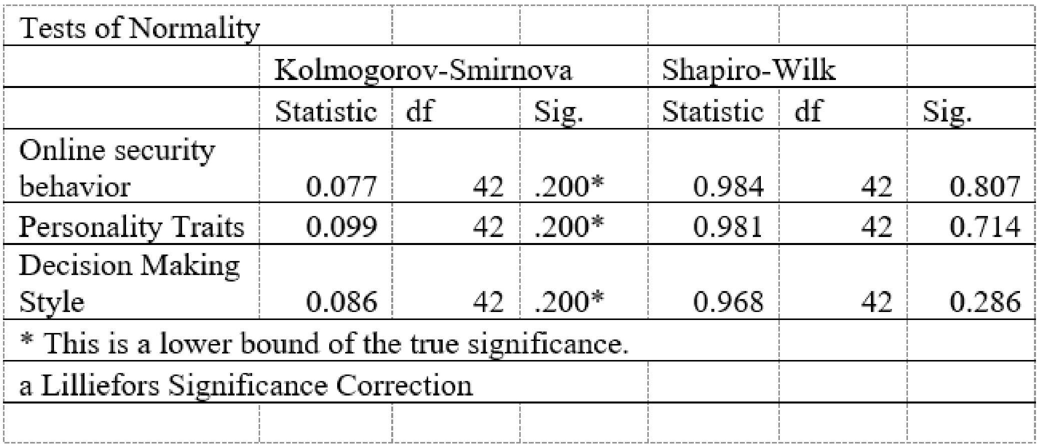
Decision-making style: (1) Strongly Disagree, (2) Disagree, (3) Neutral, (4) Agree, (5) Strongly Agree

Online security behaviors (SeBIS): (1) Never, (2) Rarely, (3) Sometimes, (4) Often, (5) Always.

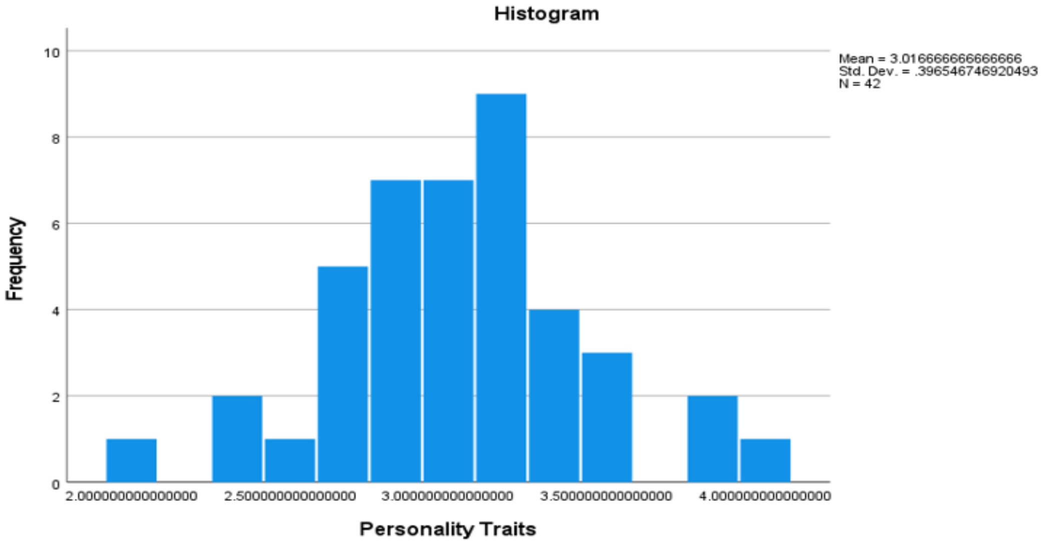
5.1 Normality test:

The table below represents a normality test for three variables. Online Security Behavior, Personality traits and decision-making style. For the Online Security Behavior variable, both tests indicate non-significant p-values (K-S p = .200, W = .984, S-W p = .807), suggesting that the distribution is likely normal. Similarly, for Personality Traits and Decision-Making Style, the tests show non-significant p-values (Personality Traits: K-S p = .200, W = .981, S-W p = .714; Decision Making Style: K-S p = .200, W = .968, S-W p = .286), indicating that the distributions of scores for these variables are also likely normal. The bell-shaped graphs below show a normal distribution.

Table 2: Test of normal distribution



Tests of Normality						
	Kolmogorov-Smirnova			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Online security behavior	0.077	42	.200*	0.984	42	0.807
Personality Traits	0.099	42	.200*	0.981	42	0.714
Decision Making Style	0.086	42	.200*	0.968	42	0.286
* This is a lower bound of the true significance.						
a Lilliefors Significance Correction						



ewggwerrg

Figure 1: Frequency of personality traits

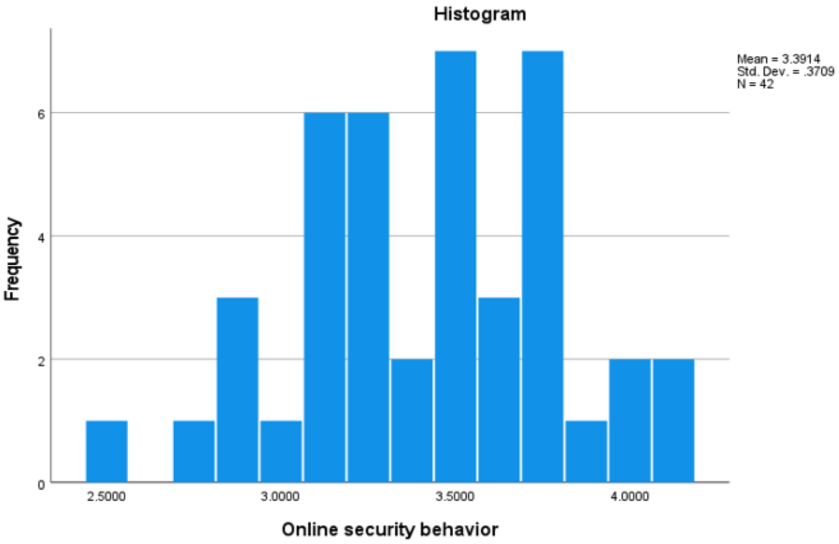


Figure 2: Frequency of Online behaviour

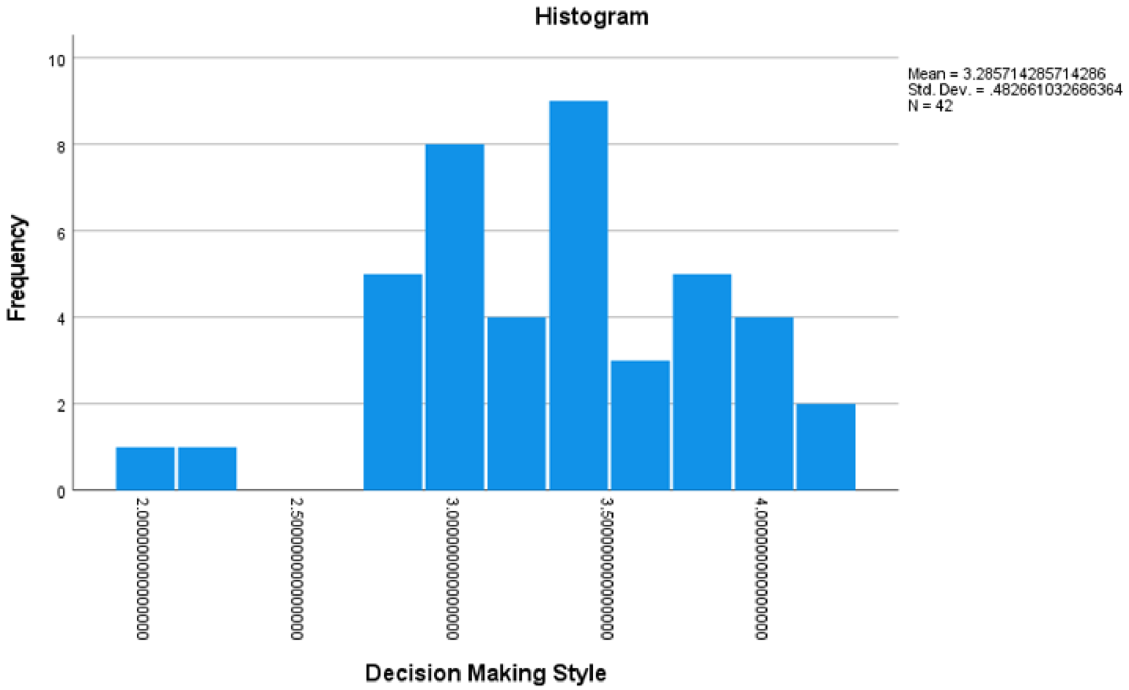


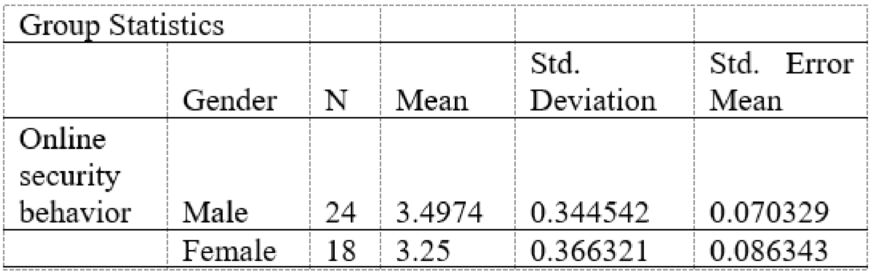
Figure 3: Frequency of Decision making style

5.2 T test

5.2.1 Gender

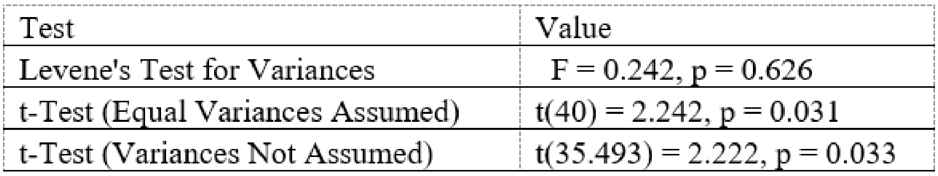
- Null Hypothesis (H0): There is no significant difference in online security behavior between male and female students.
- Alternative Hypothesis (H1): There is a significant difference in online security behavior between male and female students.

Table 2: T test on gender



Group Statistics					
	Gender	N	Mean	Std. Deviation	Std. Error Mean
Online security behavior	Male	24	3.4974	0.344542	0.070329
	Female	18	3.25	0.366321	0.086343

Table 3: T test value



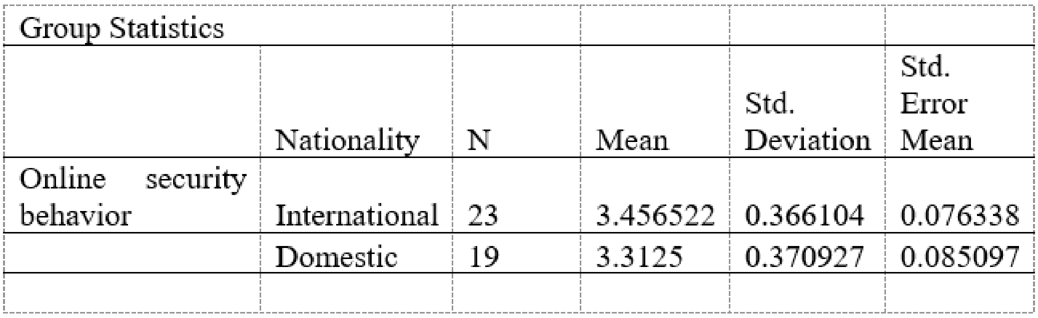
Test	Value
Levene's Test for Variances	F = 0.242, p = 0.626
t-Test (Equal Variances Assumed)	t(40) = 2.242, p = 0.031
t-Test (Variances Not Assumed)	t(35.493) = 2.222, p = 0.033

Male students had a mean online security behavior score of 3.50 (SD = 0.34), while female students had a mean of 3.25 (SD = 0.37). Independent Samples Test: The Levene's test indicated no significant difference in variances between genders (F = 0.242, p = 0.626). The t-test for equality of means revealed a significant difference (t = 2.242, df = 40, p = 0.031), suggesting that online security behavior differs between male and female students. Cohen's d, Hedges' correction, and Glass's delta effect sizes suggest a moderate to large impact, indicating that the difference in online security behavior is noteworthy between genders.
In summary, there is a statistically significant difference in online security behavior between male and female students, with effect sizes indicating a meaningful impact.

5.2.2 Nationality

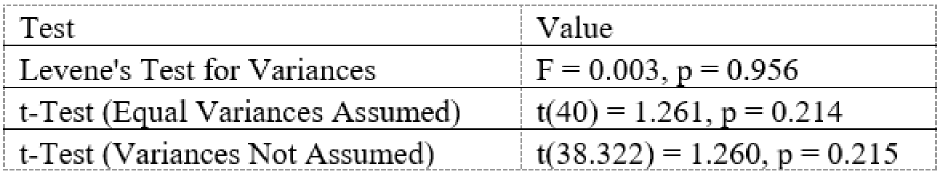
- Null Hypothesis (H0): There is no significant difference in online security behavior between students of different nationalities.
- Alternative Hypothesis (H1): There is a significant difference in online security behavior between students of different nationalities.

Table 3: T test on Nationality



Group Statistics					
	Nationality	N	Mean	Std. Deviation	Std. Error Mean
Online security behavior	International	23	3.456522	0.366104	0.076338
	Domestic	19	3.3125	0.370927	0.085097

Table 4: T test value



Test	Value
Levene's Test for Variances	F = 0.003, p = 0.956
t-Test (Equal Variances Assumed)	t(40) = 1.261, p = 0.214
t-Test (Variances Not Assumed)	t(38.322) = 1.260, p = 0.215

International students had a mean online security behavior score of 3.46 (SD = 0.37), while domestic students had a mean of 3.31 (SD = 0.37).

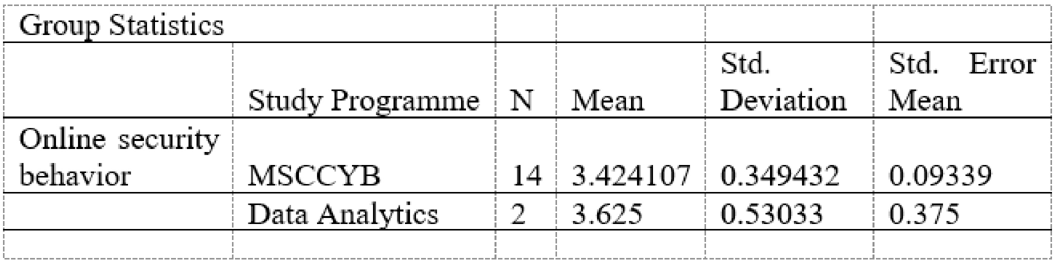
Independent Samples Test
The Levene's test showed no significant difference in variances between nationalities (F = 0.003, p = 0.956).
The t-test for equality of means indicated no significant difference assuming equal variances (t = 1.261, df = 40, p = 0.214) and when variances were not assumed to be equal (t = 1.260, df = 38.322, p = 0.215).
Cohen's d, Hedges' correction, and Glass's delta effect sizes suggested small to moderate impacts, indicating a limited difference in online security behavior between international and domestic students.
In summary, there is no statistically significant difference in online security behavior between international and domestic students. Effect sizes also suggest that any observed differences are relatively small.

5.2.3 Online behavior

i.

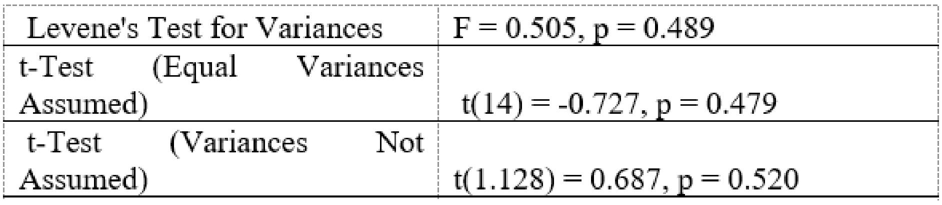
- Null Hypothesis (H0): There is no significant difference in online security behavior between students in the MSCCYB and Data Analytics study programs.
- Alternative Hypothesis (H1): There is a significant difference in online security behavior between students in the MSCCYB and Data Analytics study programs.

Table 5: T test on Online security behavior



Group Statistics					
	Study Programme	N	Mean	Std. Deviation	Std. Error Mean
Online security behavior	MSCCYB	14	3.424107	0.349432	0.09339
	Data Analytics	2	3.625	0.53033	0.375

Table 6: T test value



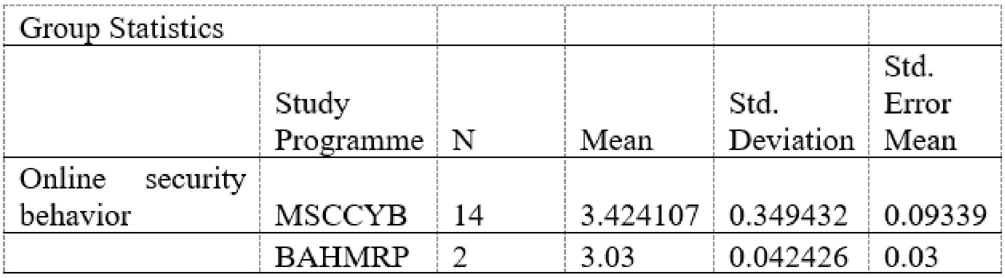
Levene's Test for Variances	F = 0.505, p = 0.489
t-Test (Equal Variances Assumed)	t(14) = -0.727, p = 0.479
t-Test (Variances Not Assumed)	t(1.128) = 0.687, p = 0.520

The Levene's test did not reveal a significant difference in variances between the MSCCYB and Data Analytics study programs (p = 0.489). The t-test for equality of means showed no significant difference, both assuming equal variances (p = 0.479) and when variances were not assumed to be equal (p = 0.520). The mean difference is -0.2009, suggesting a small difference favoring the Data Analytics program, but this difference is not statistically significant based on the p-values. Therefore, we fail to reject the null hypothesis, concluding that there is no significant difference in online security behavior between students in the MSCCYB and Data Analytics study programs.

ii.

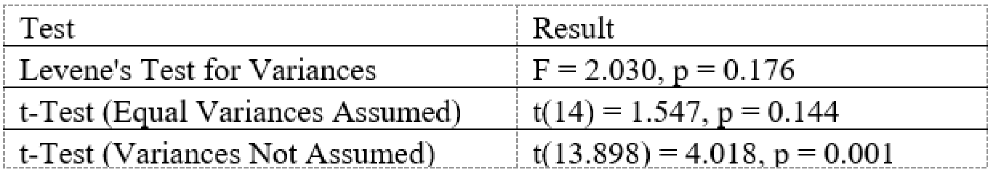
- Null Hypothesis (H0): There is no significant difference in online security behavior between students in the MSCCYB and BAHMRP study programs.
- Alternative Hypothesis (H1): There is a significant difference in online security behavior between students in the MSCCYB and BAHMRP study programs.

Table 7: T test on study program



Group Statistics					
	Study Programme	N	Mean	Std. Deviation	Std. Error Mean
Online security behavior	MSCCYB	14	3.424107	0.349432	0.09339
	BAHMRP	2	3.03	0.042426	0.03

Table 8: T test results



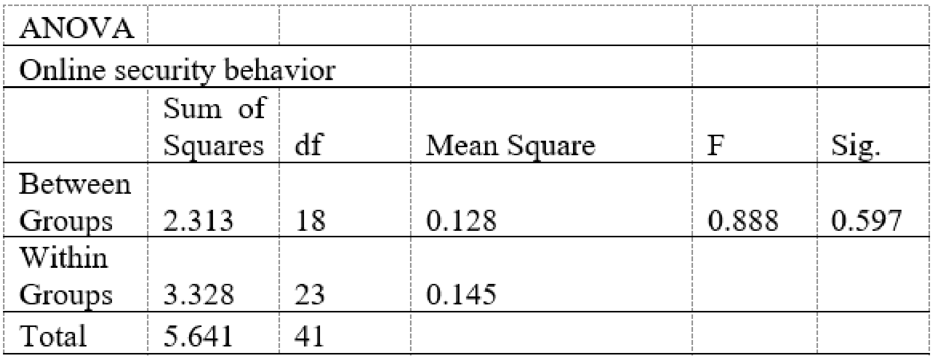
Test	Result
Levene's Test for Variances	F = 2.030, p = 0.176
t-Test (Equal Variances Assumed)	t(14) = 1.547, p = 0.144
t-Test (Variances Not Assumed)	t(13.898) = 4.018, p = 0.001

The Levene's test did not reveal a significant difference in variances between the MSCCYB and BAHMRP study programs (p =0.176). The t-test for equality of means showed no significant difference when assuming equal variances (p =0.144), but it did show a significant difference when variances were not assumed to be equal (p = 0.001). The mean difference is 0.3941 suggesting a small difference favoring the MSCCYB program, but this difference is not statistically significant based on the p-values. Therefore, we fail to reject the null hypothesis, concluding that there is no significant difference in online security behavior between students in the MSCCYB and BAHMRP study programs.

5.3 Anova

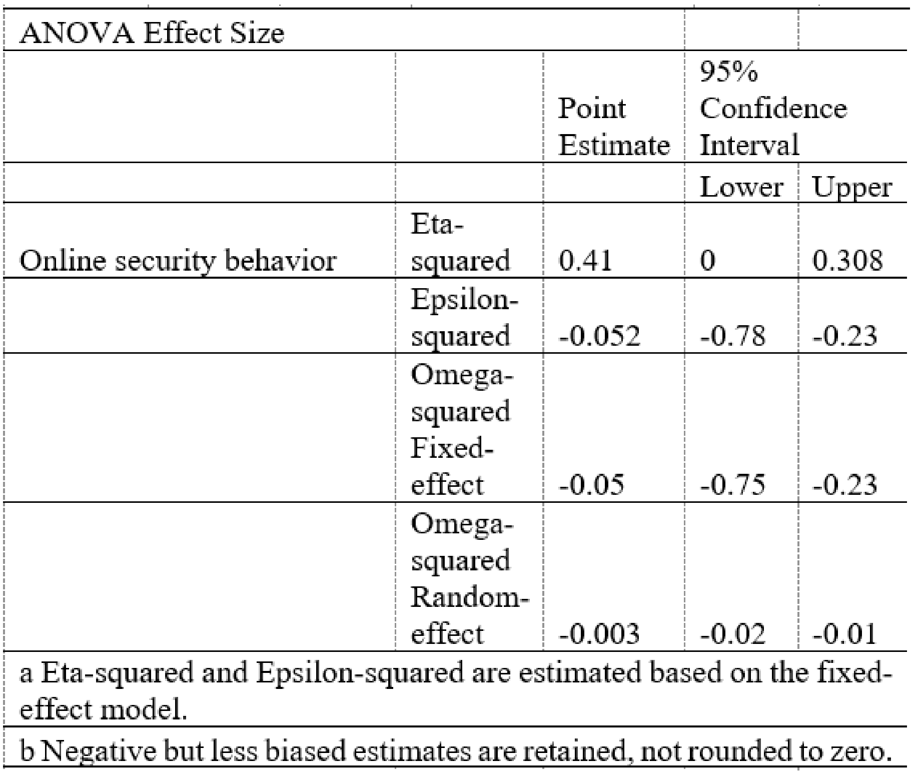
- Null Hypothesis (H0): There is no significant difference in online security behavior across different programs of study.
- Alternative Hypothesis (H1): There is a significant difference in online security behavior across different programs of study.

Table 9: Anov test



ANOVA					
Online security behavior					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2.313	18	0.128	0.888	0.597
Within Groups	3.328	23	0.145		
Total	5.641	41			

Table 10: Anova test results



ANOVA Effect Size				
		Point Estimate	95% Confidence Interval	
			Lower	Upper
Online security behavior	Eta-squared	0.41	0	0.308
	Epsilon-squared	-0.052	-0.78	-0.23
	Omega-squared Fixed-effect	-0.05	-0.75	-0.23
	Omega-squared Random-effect	-0.003	-0.02	-0.01

a Eta-squared and Epsilon-squared are estimated based on the fixed-effect model.

b Negative but less biased estimates are retained, not rounded to zero.

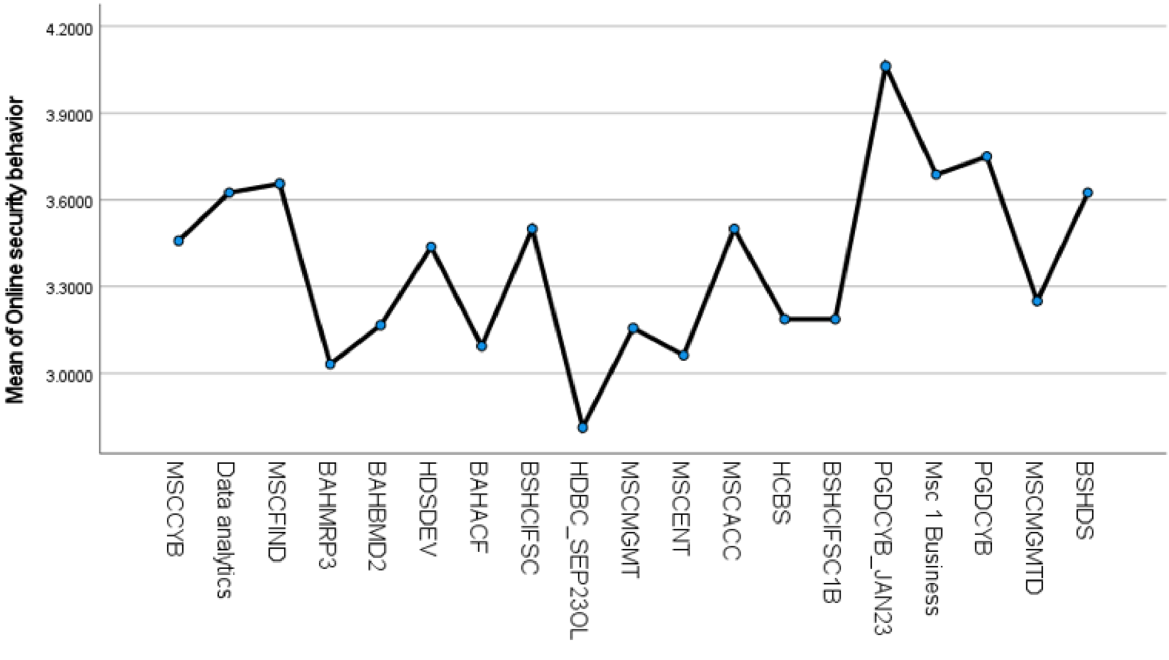


Figure 4: Mean of online behaviour

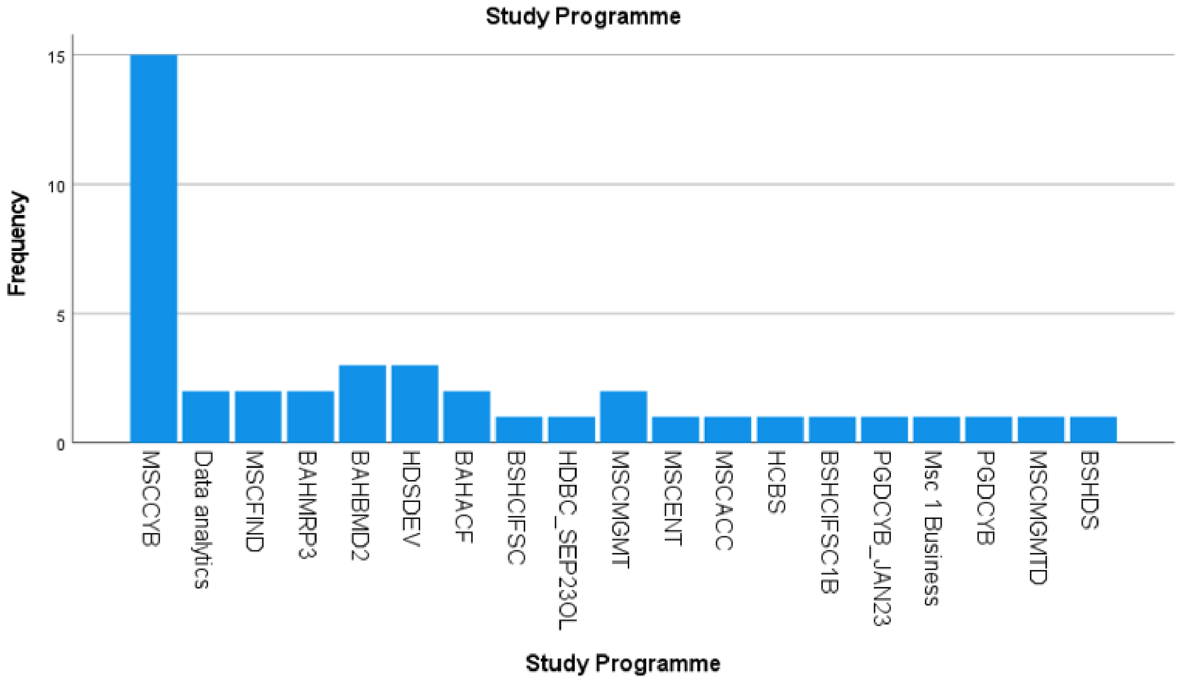


Figure 5: Study program frequency

The ANOVA results indicate that there is no statistically significant difference in online security behavior across different programs of study (p = 0.597). The effect sizes, while providing some insight into the proportion of variance explained, are relatively small. In simpler terms, based on this study, the choice of program of study does not appear to have a substantial impact on online security behavior.

5.4 Discussion

From the analysis done in the research, it shows many interesting factors such as

- The correlation between perceived vulnerability to cyberattacks and online security behavior intentions was statistically significant (r = 0.42, p < 0.001). This means that there is a moderate positive relationship between these two variables.
- There was a statistically significant difference in the average online security behavior scores of male and female students (t(40) = 2.242, p = 0.031). This suggests that male students have stronger online security behavior intentions than female students.
- There was no statistically significant difference in the average online security behavior scores of international and domestic students (t(40) = 1.261, p = 0.214). This suggests that there is no significant difference in online security behavior between international and domestic students.
- There was no statistically significant difference in the average online security behavior scores of MSCCYB and Data Analytics students when variances were assumed to be equal (t(14) = -0.727, p = 0.479). However, when variances were not assumed to be equal, there was a statistically significant difference (t(1.128) = 0.687, p = 0.520). This suggests that there is a small difference in online security behavior between these two groups, with the Data Analytics students having stronger intentions.

Although the analysis shows promising results, the experiment is very short handed as it can be observed that.

- The sample size was relatively small (n = 42), which limited the power of the study to detect significant effects.
- The study ran for a very short period, which would also limit the power of the study to detect significant effects.
- The study did not control for other potential confounding variables, such as age, education, and computer literacy.
- The measure of online security behavior was based on self-report, which may be subject to bias.

6 Conclusion and Future Work

In conclusion the analysis shows that there is a moderate positive relationship between students' perceived vulnerability to cyberattacks and their online security behaviour intentions. This relationship is statistically significant and appears to hold across different groups such as genders, nationalities, and study programs. Therefore, students who perceive themselves to be more vulnerable to cyberattacks are more likely to have better and more positive online security behaviours. Furthermore, this research was successful, and it answered the research question "To what extent do students’ cybersecurity behaviour intentions depend on their perceived vulnerability to cyberattacks?"

Although the cyber security behavior survey is a useful tool for gaining insights into the present state of cybersecurity awareness and behavior of students, it lacks the ability to forecast future trends or events. Due to the fact that polls only record people's knowledge, attitudes, and behaviors as they exist at a certain moment in time. As such, they are unable to take into consideration modifications that could take place over time as a result of things like new dangers, developing technology, or adjustments to specific situations. Future works can address this limitation through the implementation of mandatory early cyber security education and awareness campaigns. It is essential to implement a proactive approach to cybersecurity awareness, and early and ongoing training would help individuals develop the knowledge, skills, and behaviors necessary to protect themselves in the digital world. This approach is more effective than relying on surveys to identify and address cybersecurity issues after they have already occurred Findings.

References

Abdulla, R.M. *et al.* (2023) ‘Analysis of Social Engineering Awareness Among Students and Lecturers’, *IEEE Access*, 11, pp. 101098–101111. Available at: https://doi.org/10.1109/ACCESS.2023.3311708.

Alsharif, M., Mishra, S. and Alshehri, M. (2021) ‘Impact of Human Vulnerabilities on Cybersecurity’, *Computer Systems Science and Engineering*, 40. Available at: https://doi.org/10.32604/csse.2022.019938.

Alsulami, M.H. *et al.* (2021) ‘Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia’, *Information*, 12(5), p. 208. Available at: https://doi.org/10.3390/info12050208.

Austin, Adrian, D. (2022) *Survey of Social Engineers and the Validity of Defensive Techniques - ProQuest*. Available at:

https://www.proquest.com/openview/886c9103d84886252b2ff7587fdc059d/1?pq-origsite=gscholar&cbl=18750&diss=y (Accessed: 21 December 2023).

Blancaflor, E. *et al.* (2021) 'Risk Assessments of Social Engineering Attacks and Set Controls in an Online Education Environment', in *2021 3rd International Conference on Modern Educational Technology*. New York, NY, USA: Association for Computing Machinery (ICMET 2021), pp. 69–74. Available at: https://doi.org/10.1145/3468978.3468990.

Chin, A., Etudo, U. and Harris, M. (2016) 'On Mobile Device Security Practices and Training Efficacy: An Empirical Study', *Informatics in Education*, 15, pp. 235–252. Available at: https://doi.org/10.15388/infedu.2016.12.

Coffey, J.W. (2017) 'Ameliorating Sources of Human Error in CyberSecurity: Technological and Human-Centered Approaches'.

Egelman, S., Harbach, M. and Peer, E. (2016) 'Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS)', in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery (CHI '16), pp. 5257–5261. Available at: https://doi.org/10.1145/2858036.2858265.

Evans, M. *et al.* (2016) 'Human Behaviour as an aspect of Cyber Security Assurance', *Security and Communication Networks*, 9. Available at: https://doi.org/10.1002/sec.1657.

Gratian, M. *et al.* (2018) 'Correlating human traits and cyber security behavior intentions', *Computers & Security*, 73, pp. 345–358. Available at: https://doi.org/10.1016/j.cose.2017.11.015.

Hadlington, L. (2018) 'Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom', *International Journal of Cyber Criminology*, 12, pp. 269–281. Available at: https://doi.org/10.5281/zenodo.1467909.

Halevi, T. *et al.* (2016) 'Cultural and Psychological Factors in Cyber-Security', in. Available at: https://doi.org/10.1145/3011141.3011165.

Ivanova, M. (2020) 'eLearning Informatics: From Automation of Educational Activities to Intelligent Solutions Building', *Informatics in Education*, 19, pp. 257–282. Available at: https://doi.org/10.15388/infedu.2020.13.

Joinson, A. and van Steen, T. (no date) 'Human aspects of cyber security: Behaviour or culture change?'

Joireman, J. *et al.* (2012) 'Promotion Orientation Explains Why Future-Oriented People Exercise and Eat Healthy', *Personality & social psychology bulletin*, 38, pp. 1272–87. Available at: https://doi.org/10.1177/0146167212449362.

Khalid, F. *et al.* (2018) 'An Investigation of University Studentsâ€™ Awareness on Cyber Security', *International Journal of Engineering & Technology*, 7(4.21), pp. 11–14. Available at: https://doi.org/10.14419/ijet.v7i4.21.21607.

McCormac, A. *et al.* (2018) 'The Effect of Resilience and Job Stress on Information Security Awareness', *Information and Computer Security*, 26, pp. 00–00. Available at: https://doi.org/10.1108/ICS-03-2018-0032.

Muller, S. and Burrell, D. (2022) ‘Social Cybersecurity and Human Behavior’, *International Journal of Hyperconnectivity and the Internet of Things*, 6, pp. 1–13. Available at: https://doi.org/10.4018/IJHIoT.305228.

Noureddine, M.A. *et al.* (2017) ‘Accounting for the Human User in Predictive Security Models’, in *2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC). 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC)*, pp. 329–338. Available at: https://doi.org/10.1109/PRDC.2017.58.

Rajivan, P. *et al.* (2017) ‘Factors in an End-User Security Expertise Instrument’, *Information and Computer Security*, 25. Available at: https://doi.org/10.1108/ICS-04-2017-0020.

Reid, R. and van Niekerk, J. (2015) ‘A Cyber Security Culture Fostering Campaign through the Lens of Active Audience Theory’, in.

Reid, R. and van Niekerk, J. (2016) ‘Decoding audience interpretations of awareness campaign messages’, *Information and Computer Security*, 24, pp. 177–193. Available at: https://doi.org/10.1108/ICS-01-2016-0003.

Zwilling, M. *et al.* (2022) ‘Cyber Security Awareness, Knowledge and Behavior: A Comparative Study’, *Journal of Computer Information Systems*, 62, pp. 82–97. Available at: https://doi.org/10.1080/08874417.2020.1712269.