Cyber Safe or Cyber Risk? An assessment of student practises in password security, phishing and social engineering

Akash Kumar, Priyadarsi Nanda
Faculty of Engineering and IT
University of Technology Sydney (UTS), Australia

ABSTRACT:

Universities are attractive targets for cyberattacks due to open networks and a large number of users, primarily students. This research examines cybersecurity practices among higher-education students, focusing on three areas: password security, phishing awareness, and social-engineering vulnerability. A survey of 146 students from various Australian universities revealed that while students have a moderate awareness of cybersecurity dangers, their practices are inconsistent. High rates of password reuse and poor complexity were noted, and many participants struggled to identify phishing indicators. Postgraduate students generally demonstrated better cybersecurity behaviours compared to undergraduates. Additionally, previous cybersecurity training was linked to improved detection of social engineering, though the effect was limited. Participants expressed a strong interest in practical cybersecurity training, preferring interactive and self-directed methods over traditional lectures. The findings underscore the need for systematic, behaviour-based interventions and structured cybersecurity education within institutions. Future research should explore causal factors, test training interventions, and conduct cross-cultural comparisons to enhance the understanding of cybersecurity practices among students.

KEYWORDS: Cyber Hygiene, Cybersecurity Education, Higher Education, Human Factors, Password Security, Phishing Awareness, Social Engineering, Student Behaviour

INTRODUCTION:

Background and Threat Landscape:

Over the past few years, the level and magnitude of cyberthreats against educational settings has significantly increased. Sensitive student records, research data and financial information are all high value targets of attackers because they are usually stored in institution [1]. The security issues are often encountered by students themselves: the lack of proper passwords, phishing, and other risky actions make a lot of them vulnerable to identity theft, finances, and data breaches. Learning institutions do not generally offer students comprehensive training in the field of cybersecurity and the majority of users merely ignore the advice given on the subject (including identifying phishing or social engineering threats) [2]. Overall, the threat environment and the open campus culture are changing, which makes the university students an urgent security issue.

Password Security:

Password security can be described as the act of using and developing a strong and unique password to safeguard online accounts. The first web of defence of cybersecurity is strong passwords; They must not be easy to guess or predict, but lots of users, including students, use weak passwords, which are customized according to personal data, frequent words, or some simple pattern [3]. A longitudinal study at a American university revealed that reuse of passwords was much more dangerous than simply making account with common passwords: 32 percent of accounts with email credentials were hacked using reused passwords, where only 6.5 percent of accounts were compromised using known common passwords [2]. This shows that the activities of students with passwords (reuse, share, and poor composition) would prove to be very influential in increasing complexity of security threats on campus.

Phishing and Social Engineering:

Phishing is a social engineering attack where criminals and other malicious individuals cheat users into disclosing personal information or credentials. Phishing refers to a type of criminal mechanism that uses social engineering in conjunction with technical subterfuge to steal consumers with personal identity data and financial account detail

[4]. Practically, phishing is often associated with emails, which pretend to be legitimate organizations and entice the victims to follow harmful links or fill in their logins details on fake websites to complete the process. Phishing is highly widespread: it has been termed as the primary source of data breach, and the most effective threat vehicle [4]. Students in the university are not an exception. Successful phishing may invade university accounts and result in theft of credentials, infection by malware and stolen institutional data.

Social engineering is in general terms, all methods of exploiting the psychology of man to acquire illegal entry or knowledge. Instead of technical exploits, it appeals to such emotions as trust, fear, urgency, or curiosity. Social engineering is an approach that aims at the human aspect of the security systems, which means that it deceives people into inappropriate actions that weaken security [5]. These are not limited to email phishing, but also the phone scams, text messages, websites and face-to-face pretexting. Sophisticated versions Furthermore, spear phishing (attacks directed at executives), whaling (attacks at executives), baiting (physical media enticement), and watering-hole attacks, are all instances of social engineering through the exploitation of the use of context. Social engineering can also be used to overcome high-tech defences because of the vulnerability of people.

LITERATURE REVIEW:

University Students' Cybersecurity Practices:

University students are considered at risk because their cybersecurity knowledge and behaviours have become the focus of intensive. This is pointed out by large-scale surveys: in one study of more than 41,000 students, only 4% reported having ever been trained on information security [6].This disparity of formal education leads to risky behaviour. Indeed, recent surveys observe that a significant proportion of young exhibit bad cyber hygiene: only one in five 18-25 year-olds changes their passwords regularly, and only 43% of this cohort updates their software and devices; Likewise, only 36 percent of these younger customers install any antivirus protection [7]. These results indicate that even digital natives can be careless about basic security measures.

The present review summarizes recent survey-based and theoretical research on major domains of student's cybersecurity behaviours, including phishing awareness, password practices, social engineering vulnerability and general cyber hygiene. The study underlines international attitudes and contrasts the results in various educational setting.

Phishing Awareness and Susceptibility:

Fraud and other scams play on the human factor (out of curiosity, trust, authority) to fool the users. In a survey of Norwegian university students, 84% said they got phishing emails and 64% got phishing SMS messages [8]. The same trends are observed all over the world. As demonstrated by [9], students tend to incorrectly label spam emails as legal when facing phishing emails and are particularly bad at identifying spear-phishing (highly personalized) messages. That is, students may become self-assured in their skills to identify scams. A study of South African students by [10] revealed that more than half of them acknowledged the poor level of their knowledge about phishing, but the majority of them were sure that they were safe to use the Internet they thought that it is dangerous. Such a sense of false security implies that not every student views themselves as particularly vulnerable.

Password Security Behaviours:

The password is the first line of account security, but studies have shown that students tend to have poor password behaviour. The weaknesses in survey studies in various countries are staggering. Only the use of passwords containing 8 or more characters was found to be used by only around 63 percent of students in one large study in Turkey and worst of all, 80 percent acknowledged that they have used personal details (birthdates, names, and so on) as a password [11].

Reuse of passwords is also quite common. Not many students appear to follow the suggested tools such as password manager and two-factor authentication (2FA) is not used by everyone. In the Gen Z survey, 58% responded that they used 2FA on any account which is unexpected but still results in over 40% being unprotected by this additional security [7]. Students remain much less likely to use distinct strong passwords [12]. Generally,

students prefer to use weak, patterned, or personal passwords, which are usually easily guessable and reuse them extensively.

Social Engineering Susceptibility:

The term social engineering is used loosely to refer to non-technical manipulations that fool users into giving out information or engaging in risky behaviours. As with other human targets, university students fall prey to these tricks. Experiments and the survey show that students tend to loosen up when the attacker invokes trust or familiarity. As an example, [13] demonstrated that uncomplicated reasons worked properly to make the students surrender their personal information; the proposal to assist a friend or enter a raffia duped a lot of respondents. These tricks play upon the principles of persuasion as suggested by Cialdini (liking, reciprocity, authority, etc.). Similarly, such attacks as vishing (voice phishing) and smishing (SMS phishing) rely on the same psychology. These are rarely explicitly studied, but there have been informal reports that many students are too trusting on the phones or social media.

In the context of email-based social engineering, customized attacks will again be more effective. [14] compared generic spam to personalized scams and concluded that spear-phishing emails were far more engaging than generic blasts due to their personalization. That is, a single personal mention (e.g. mentioning university events or names) is significant. This means that knowledge based on social context (learned through social networks or college gossip) can significantly enhance the strength of a scam in its attack on students.

Psychological and demographic considerations are also in play. Students can be influenced to obey a request because they have cognitive biases (overconfidence, willingness to help, fear of missing out). An example is when students think an email is real, or looks real, when it says it is official or urgent (e.g. your exam grades, or scholarship offer). On the other hand, awareness training has the ability to lower success. Research indicates that students who were informed they would see phishing did much better at identifying a deception than an uninformed control group [15]. So, social engineering attacks capitalize on inherent human behaviours and students are no exception to human behaviours, but risk can be mitigated through organized awareness campaigns. In general, students are quite vulnerable to social engineering: invocation to trust, authority, or familiarity regularly trump caution.

General Cyber Hygiene and Broader Behaviours:

In addition to phishing and passwords, cyber hygiene includes daily security practices: security software updates, antivirus, device configuration, and safe internet usage. According to surveys, the overall level of hygiene in students is ambivalent. [16] used a 30-item questionnaire on the knowledge of, awareness of and behaviour regarding cyber hygiene among university students. The researchers discovered that the security behaviours students reported to be are acceptable but their awareness and knowledge were very low [16]. That is, a lot of students will follow some safe practices through rote such as periodical updates or simple rules about passwords, but they will not have a deeper grasp of the material or be proactive. To illustrate demographic correlations, women and students in higher years tended to score higher, yet the awareness in general was still unacceptable [16].

Latest statistics support these fears. As reported, the percentage of the youth updating their devices is only at 43%; additionally, only a paltry 36% of the respondents in that Gen Z survey even had antivirus installed: when asked about their tendency to use unsecured public Wi-Fi, only about one-third (35) of Gen Z indicated that they did not do so, indicating that many will connect to an open network with no protection; likewise, fewer than half resort to reviewing suspicious activity of their bank or email accounts [7]. Such fundamental breaches expose students to malwares, account hacks and data breaches.

Weak practices are also indicated in studies of mobile device use. Although only 43 percent of students used auto-lock or strong lock-screens regularly in 2019, a decrease from 53 percent in 2014, many still failed to implement essential security measures such as short timeouts, PINs, or passcodes; furthermore, the vast majority neglected to protect their devices against recovery options, as more than half did not utilize remote wipe or location tracking features [17]. These basic mobile precautions cannot possibly safeguard the immense personal information stored on students cell phones [18]

On a positive note, there are some promising statistics. According to the study conducted by [16], they described regular practices e.g. not clicking on suspicious links, use of simple filtering applications, etc. in general, so this is why the term acceptable behaviour was adopted. In addition, 58% Gen Z Most of the 2FA users means the majority of students have implemented multi-factor authentication on at least some accounts, which is higher than a few older demographics [7]. Nevertheless, these partial achievements are compensated by other shortcomings. According to education researchers, the majority of students do not ever backup their data, think little about digital privacy settings, and do not have a definite policy on how they use their devices.

Overall, cyber hygiene among university students is a concerning and ambivalent profile. They show certain safe behaviours (e.g. basic password creation, partial 2FA use), but there are significant deficits in awareness and consistency [16].Their vulnerability to attack is not acceptable, especially with the constantly evolving threat environment and the digital lives of students.

Research Gap:

Although there has been a vast amount of research on cybersecurity awareness and internet safety, the majority of existing research has been conducted on individual dimensions of cybersecurity behaviour among students, including phishing awareness, password security, or social engineering, as opposed to assessing these dimensions as a set in a cohesive model. As an illustration, recent studies by [14] and [8] can be viewed as interesting perspectives on the topic of phishing vulnerability and susceptibility, whereas [11] and [12] are dedicated to the use of passwords and password reuse and password management, respectively. Nevertheless, there is little integrative work examining and correlating the knowledge, attitudes, and behaviours of students on more than one cybersecurity domain at a time. This piecemeal methodology does not allow us to have a comprehensive view of the relationship between various online safety behaviours, and whether the vulnerability to one (e.g., phishing) predicts the vulnerability to others (e.g., password hygiene).

Moreover, the majority of the previously done studies occurs in Europe and North America and even in parts of Asia, there are very few empirical studies done on the students of Australian universities or in the similar academic settings. This physical distance constrains the overall applicability of available results to different educational and cultural environments. Moreover, previous studies have tended to base their research on self-reported perceptions of security awareness, when in fact these perceptions have not been supported by behavioural measures or structured surveys to determine realistic knowledge. Thus, this study aims to fill these gaps by carrying out a thorough evaluation of the cybersecurity competence of students in the context of phishing, password management, and social engineering. The results are expected to benefit both the academic knowledge and the development of specific programs of awareness of students.

To address the identified security gaps, this study is guided by the following research questions:
• RQ1: How do students manage and secure their passwords, and does this differ across academic levels?
• RQ2: What is the level of phishing awareness among students, and how accurately can they identify phishing attempts?
• RQ3: How aware are students of social engineering tactics?
• RQ4: What are students' attitudes and training preferences?

RESEARCH METHODOLOGY:

Research Design:

This paper has a quantitative descriptive research design in that it aims to determine the depth of cybersecurity competence and the behavioural pattern among the students in the university. The aim is to determine how students understand and practice in three key domains (e.g., password management, phishing awareness, and social engineering susceptibility) and find out the correlation between demographic (e.g., academic year, gender, program level) and cybersecurity behaviour.

A quantitative study is especially suitable to cybersecurity behavioural research since it opens the possibility of collecting data systematically using structured data collection tools, including questionnaires [19]. This method

allows defining patterns and trends in a general population, not considering individual experiences. The research design is cross-sectional and non-experimental, i.e. data was taken at one time, with no control at any variable. Such an approach is efficient to identify the level of cybersecurity recognition among university students and decide on the prevalence of certain behavioural patterns and myths.

Participants and Sampling:

The study population of this study is the university students who are pursuing their undergraduate and postgraduate studies. Since the study targeted cybersecurity awareness and the behaviour of the population, given the fact that the students are frequent technology users, they were chosen as the population of interest because they interact with the online platform daily to carry out their academic, financial, and personal activities.

Participants were recruited using a convenience sampling technique through online university groups and student organizations. This method was practical and ensured voluntary participation without the need for personal data, maintaining anonymity. The study aimed to gather over 100 valid responses for diverse demographic representation.

Eligibility criteria included being enrolled in a higher education institution (university or college) and being at least 18 years old, addressing ethical considerations for adult participation. The sample consisted of undergraduate and postgraduate students from various disciplines, allowing for valuable comparisons of academic experience in relation to cybersecurity competence.

Survey Instrument and Structure:

The main instrument of data collection used in this study was a structured online survey that was created with the help of Google Forms. Previous scholarly research on the subject of cybersecurity awareness and student behaviour conducted by [20] & [10] informed the choices made by the survey design.

The questionnaire was divided into four major sections and each of them was aimed at assessing different aspects of cybersecurity awareness and practice:
Demographic Data- Age, gender, academic degree (undergraduate/ postgraduate) and year of study of the collected participants. This data facilitated a subgroup analysis and allowed one to put behavioural differences into perspective.
Password Security Practices- They contain questions that evaluate password creation behaviours, password reuse, password management application, and password familiarity with two-factor authentication.
Phishing Awareness - Determined how participants were able to recognize the presence of phishing attacks, prior experience with phishing emails, and their behaviour after encountering a suspicious link or message.
Social Engineering and General Cyber Hygiene - The orientations were aimed at more general online safety practices, including sharing behaviour, pretexting reaction, and care routines, such as updating devices and using antivirus software.

The majority of the questions were developed in the multiple-choice, short answers, checkboxes and Likert-scale (e.g., 1 = Strongly Disagree to 5 = Strongly Agree) format as they were intended to include both factual and attitudinal answers. The design provided consistency in measurement of data and eased the analysis in quantitative terms.

A pilot test of the survey was done in advance to test clarity, wording and flow. 5 participants were used to conduct the test. The results of this pilot test guided the improvement of the ambiguous questions and ensured that the average time taken to complete the questions was around 6-8 minutes.

Data Collection Procedure:

The collection of data occurred for one month. The survey link was distributed by using several online platforms such as WhatsApp student groups, university mailing lists, and social media websites. The link was preceded by a brief introduction message that detailed the purpose of the research, the expected time required to complete the research and said that it was confidential.

The entire process was voluntary, and the respondents had the right to drop out at any point through closing the form before submitting the form. All the participants gave informed consent at the start of the questionnaire. These were contained in the consent statement which detailed the study purpose, anonymity of the data collection process, and the use of the responses as academic data. After the survey had been completed, a message of gratitude was shown to the participants reiterating that their cooperation was appreciated and that all information would be kept anonymous.

Data Validation and Authenticity:

To make the responses authentic, several checks were adopted. To begin with, the survey categorically ensured that the respondents were current university students who were of age 18 years and above. The responses that did not meet this criterion were eliminated in data cleaning.

Second, the email collection feature was turned on first to be sure that the real accounts of students were verified. Nevertheless, to conform to the ethical requirements and privacy of participants, no emails were kept or analysed based on them, but they were utilized to check them in the process of data collection and anonymized afterward.

Third, the account option of one response was turned on. This made sure that only one legitimate response was obtained.

Lastly, simple data screening was conducted to detect incomplete or inconsistent data (e.g. conflicting responses e.g. never heard of phishing and later clicked a phishing link). These reviews were done and where necessary, the responses were rejected in order to preserve the integrity of the data.

Data Analysis Methods:

Data obtained in the Google forms were exported into Microsoft Excel and analysed through the SPSS (Statistical Package for the Social Sciences) and Microsoft Excel as descriptive statistics. As the research will be mainly quantitative and exploratory, summarizing of trends, frequencies, and correlations between variables was the focus.

The process of analysis was as follows:
Descriptive Statistics: The frequency distributions and percentages were determined on all the items of the survey to determine general trends in cybersecurity behaviours and attitudes of students.
Comparative Analysis: Data were divided under the demographics (gender, academic level, and study year) to determine whether there is a possible difference in the awareness or patterns of behaviour.
Cross-Variable Correlation: Cross-tabulations and correlation coefficients were used to analyse the relationships between key variables, which were: password strength, phishing recognition, and social engineering awareness.
Visual Presentation: Results and Discussion sections have graphs and charts that were developed to present findings in a clear manner.

This method of analysis offered a broad and specific data regarding the student practices in cybersecurity. Often, e.g., the frequencies table was used to find out the percentage of students using password managers or it was possible to find out using correlation whether students who were sure about their ability to notice phishing had better password habits.

DATA ANALYSIS & RESULTS:

Overview of Data Analysis Process:

The results of the student cybersecurity survey were obtained in the form of the data, which were analysed quantitatively with the help of the Statistical Package for the Social Sciences (SPSS) (IBM Corp., 2025)). Only 146 valid responses were chosen after qualifying the responses (students aged 18 and above, who are taken up with a higher education) to qualify. The data included demographic, behavioural data about password management, phishing knowledge, and social engineering vulnerability.

The review was conducted using the four major steps in the research approach:

- Descriptive Statistics - Frequency demonstrates and percentages were used to summarize the cybersecurity behaviours of students.
- Comparative Analysis - The differences between demographic groups (undergraduate and postgraduate, gender, academic year) were tested.
- Correlation Analysis - The connections between variables of importance in cybersecurity (e.g., the correlation between trust in phishing recognition and locking passwords) were researched.
- Visual Presentation - Graphical displays were created to facilitate the meaning of results.

The results provided in the following subsections are consistent with research sub-questions and hypotheses provided in the introduction section above.

Demographic Profile of Respondents:

146 valid responses were received among students in different academic programs. Gender, academic level, year of study and university were used to classify the respondents.

- Gender: There were an equal representation of 56% males and 44% females, as shown in Table 1 & Figure 1.
- Academic Level: 64% undergraduate and 36% postgraduate students (Figure 2).
- Year of Study: The students were of all years with the highest percentage of undergraduate 6th(final) year (Figure 3).
- University: The students who participated in the survey were representatives of 7 universities, including University of Technology Sydney (UTS), Macquarie University, the University of Sydney, University of Wollongong, University of New South Wales (UNSW) and Western Sydney University with majority (3%) of them being students of the UTS (Figure 4).

This distribution shows varied representation of the student body of the university, which guarantees good generalization by the student body.

Table 1: Gender based Ratio

What is your gender? (Male/Female/Transgender/Prefer Not to Say)					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	64	43.8	43.8	43.8
	Male	82	56.2	56.2	100.0
	Total	146	100.0	100.0	

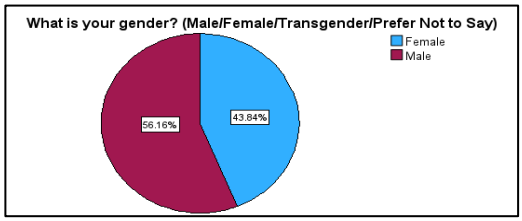

Figure 1: Gender Distribution of Respondents

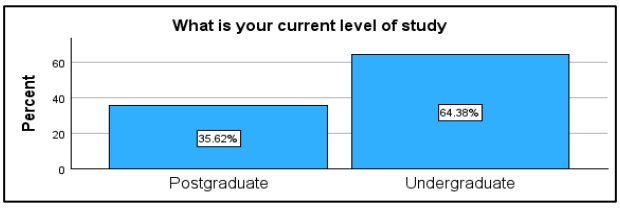

Figure 2: Academic Status of Survey Participants

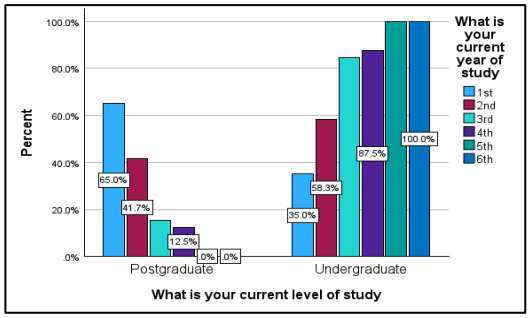

Figure 3: Distribution of Participants by Academic Level and

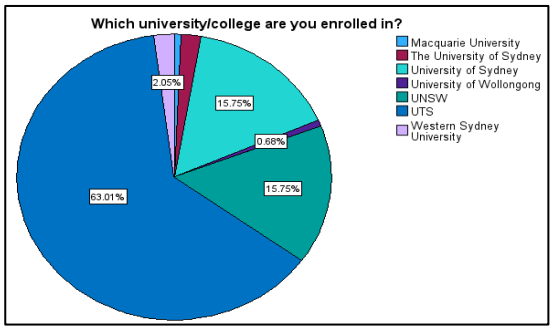

Figure 4: Respondent Distribution Across Universities

Password Security Practices:

Research Sub-question 1: How do students manage and secure their passwords, and does this differ across academic levels?

Hypothesis (H1): Postgraduate students demonstrate significantly stronger password management behaviour than undergraduate students.

The descriptive findings showed that 43.8% of the students said that they use the same password on more than one account, and 52.1% said that they do not use the same password on more than one sites (figure 5). Two-factor authentication (2FA) on their accounts was noted to be used by about 56.2 % of the respondents, which is an average awareness (figure 6).

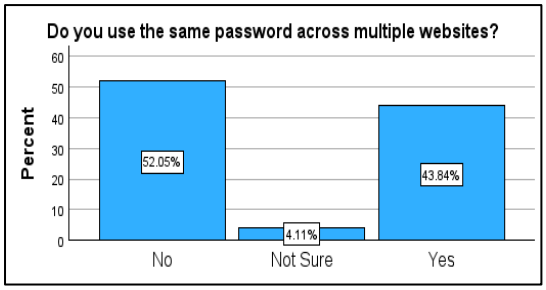

Figure 5: Participant Responses on Password Reuse Behaviour

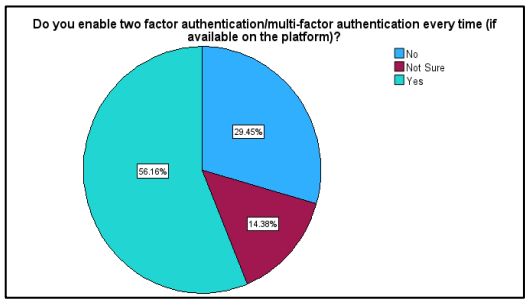

Figure 6: Participant Adoption of Two-Factor

Cross-tabulation of undergraduates and postgraduates revealed that the students with postgraduates had a higher percentage of using a unique password in all their accounts (71.2) as compared to the undergraduates (41.5) (figure 7). A Chi-square test was used to prove that the difference between the two groups was statistically significant (2 = 14.141, $p < 0.001$), which supported Hypothesis 1.

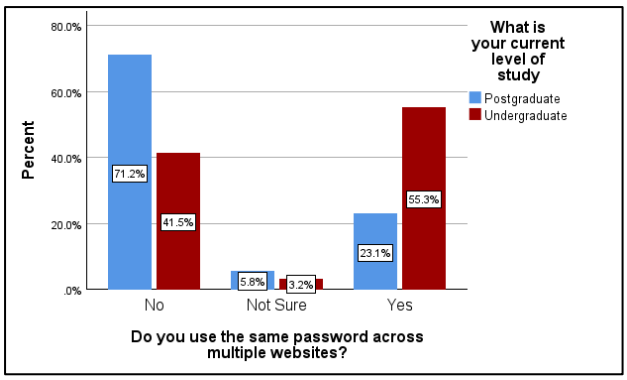

Figure 1: Response to password reuse

The respondents were requested to provide information regarding the criteria that they used to create passwords. Although the length and usage of symbols were widely considered, only 54.8% of students said they included lowercase and uppercase letters, numeric and special characters, which is a best practice towards good password hygiene (figure 8).

The results prove that despite the knowledge of students about password best practices, a significant number of them do not always use them. The trend is consistent with the past research [10] as the awareness does not necessarily transform into safe conduct.

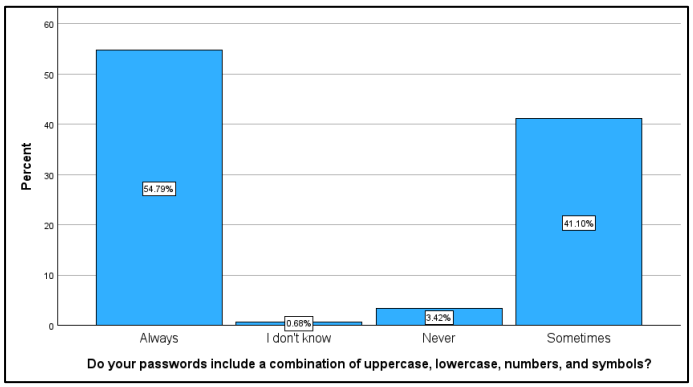

Figure 2: Percentage of Respondents Creating Passwords with Full Character Complexity

Phishing Awareness and Recognition:

Research Sub-question 2: What is the level of phishing awareness among students, and how accurately can they identify phishing attempts?

Hypothesis (H_2): Postgraduate students will demonstrate higher phishing detection accuracy than undergraduate students.

Responding to the question: Have you ever received a phishing e-mail, 89.04% of the participants answered: Yes, which proves that exposure to phishing is widespread among university students (figure 9). Nevertheless, in case presented with sample scenarios, only appx 6% could correctly identify all phishing indicators (level 4), most of them could not identify all the indicators (figure 10).

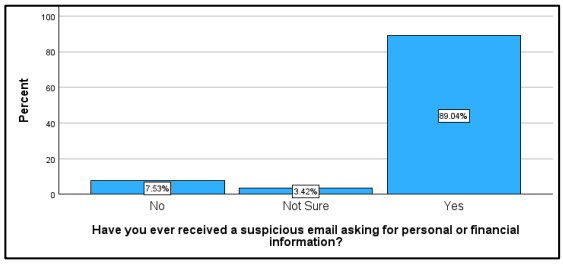

Figure 9: Prevalence of Receiving Suspicious Emails

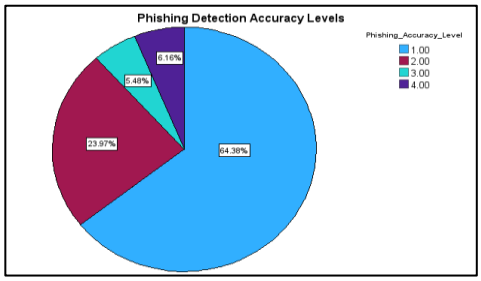

Figure 10: Phishing Detection Accuracy Levels

A chi-square test of independence revealed a significant relationship between academic level and phishing detection accuracy, $\chi^2(3) = 32.01$, $p < .001$. Postgraduate students showed more distributed performance across accuracy levels, with 5.48% achieving the highest accuracy score compared to only 0.68% of undergraduate students (figure 11). This supports Hypothesis 2 and suggests that advanced academic experience may contribute to greater security awareness.

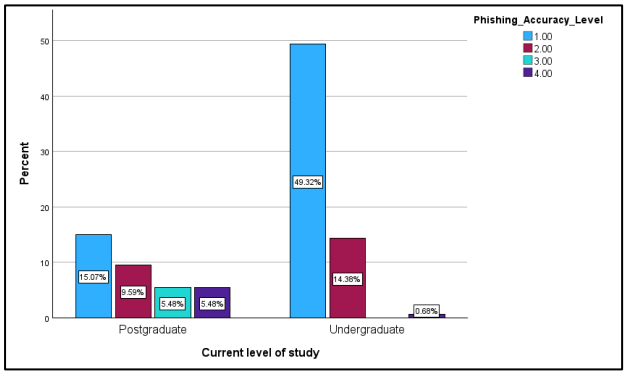

Figure 3: Security Awareness by Level of Study

Remarkably, there was a huge discrepancy between reported confidence and real accuracy of detection. Even though the percentage of students who consider themselves to have been confident is 48.63% (figure 12), the distribution of the percentage of students who identify themselves as confident is not highly expected to be found at the highest performance level. The percentage of students with perfect scores was low (5.48 %), and most of the confident students did not have a high accuracy level (figure 13).

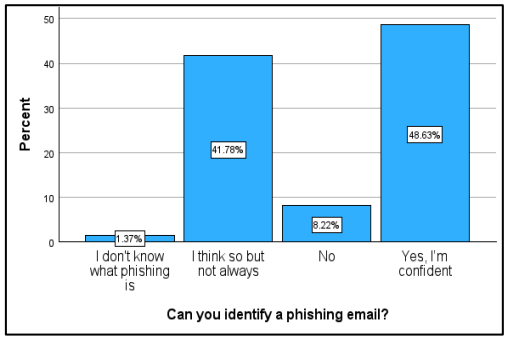

Figure 12: Self-Assessed Ability to Identify Phishing

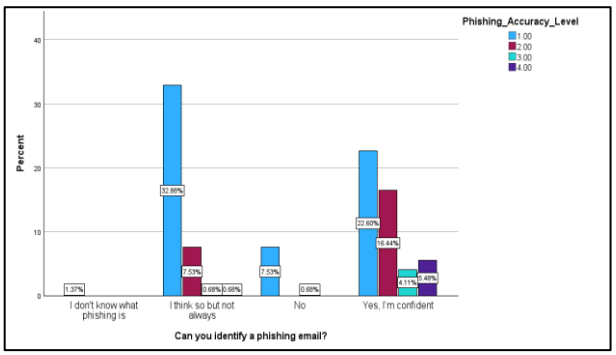

Figure 13: Comparison of confidence and phishing accuracy

Social Engineering Awareness and Susceptibility:

Research Sub-question 3:

How aware are students of social engineering tactics, and how do they respond to simulated manipulation scenarios?

Hypothesis (H_3):

Students who have received previous cybersecurity training will show higher social engineering detection rates.

To determine the comprehension of social engineering among students, the survey used multiple choice questions that were aimed at recognizing social engineering techniques and how to behave in case of a deceptive situation.

On the question, have you ever heard of social engineering in cybersecurity? 54.11 % of the respondents answered Yes, 26.03 % answered Not Sure and 19.86 % responded Never heard of it (figure 14).

This finding indicates that even though there are a few students who are conversant with the term, quite a significant proportion of the population does not have a clear idea of what social engineering involves.

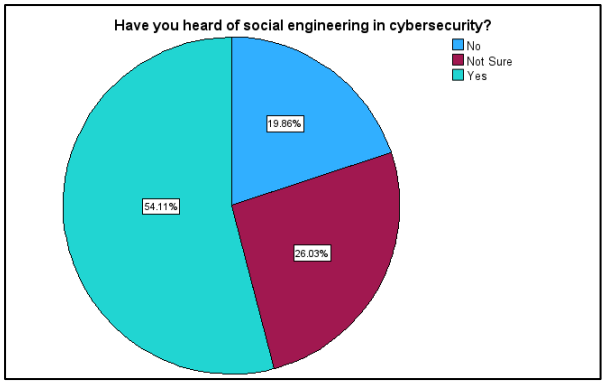

Figure 4: Participant Familiarity with the Term "Social Engineering"

Also, given the situational prompt, -
What would you do in case you receive a call with a so-called IT support person, requesting your log-in information?
Then, meanings differed between responses greatly (figure 15).
49.32% said they would ask for proof,
5.48% indicated that they report to the police,
34.25% would ignore the request, and
7.53 % confessed that they could provide information.

This trend shows that, despite the majority of the students being cautious, a significant percentage of them are susceptible to persuasion and posing as authority, which is one of the fundamental features of social engineering.

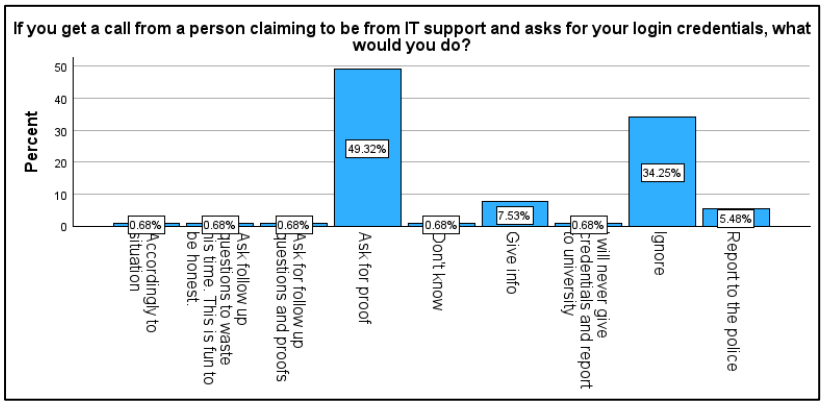

Figure 5: Actions Upon Receiving a Suspicious Credential Request

Lastly, a question of whether the students have ever been contacted by a person posing as IT personnel, a bank officer, or any other figure of authority was presented; 28.77% of the students responded with a yes, suggesting the students have experienced social engineering attacks in real life (figure 16).

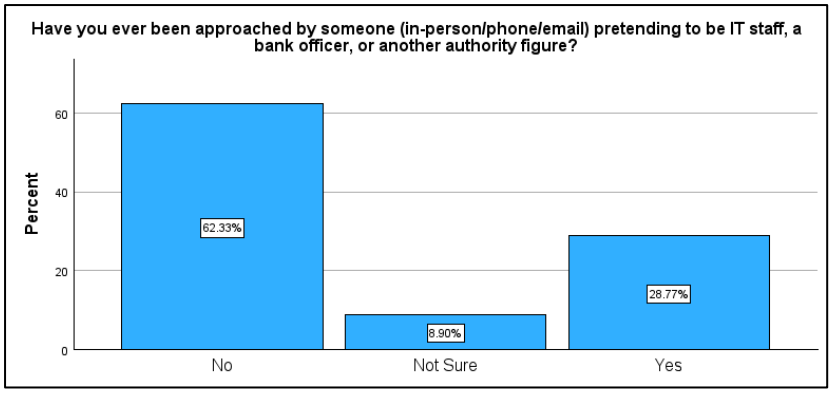

Figure 6: Participant Exposure to Impersonation Scams (IT, Bank, etc.)

These results indicate that the majority of students on the one hand have some theoretical knowledge about social engineering, but most of them do not understand what happens in situations because they are not aware of some manipulation methods.

Additionally, A chi-square test of independence demonstrated a very high significance of the relationship between cybersecurity training and social engineering detection ability, $\chi^2(1) = 13.44$, $p < .001$. The impact was considerable: after the training, 94.3% of trained students were able to find social engineering example, and just 71.1% of untrained students (table 2). This difference of 23.2 percentage, which is of significant support to the hypothesis that formal cybersecurity training significantly enhances social engineering recognition skills.

Table 2: Cross-Tabulation of Cybersecurity Training Attendance by Social Engineering Identification Accuracy

Have you ever taken a course or attended a session about cybersecurity? * SE_Accuracy Crosstabulation					
			SE_Accuracy		Total
			.00	1.00	
Have you ever taken a course or attended a session about cybersecurity?	No	Count	22	54	76
		% within Have you ever taken a course or attended a session about cybersecurity?	28.9%	71.1%	100.0%
	Yes	Count	4	66	70
		% within Have you ever taken a course or attended a session about cybersecurity?	5.7%	94.3%	100.0%
Total		Count	26	120	146
		% within Have you ever taken a course or attended a session about cybersecurity?	17.8%	82.2%	100.0%

Cyber Habits and Attitudes:

Research Sub-question 4:

What are students' attitudes, confidence levels, and training preferences toward cybersecurity awareness?

This part will look at the overall perception of cybersecurity among the students such as their self-confidence in their knowledge, their formal training, and the type of learning they would like to receive.

Upon inquiring regarding their general confidence regarding cybersecurity knowledge, majority of the students had rated themselves as moderate with most of them scoring level 5 out of five. Only a few of them said that they felt very confident with a corresponding number saying that they felt low confidence (1 or 2).

This result leads to the conclusion that students are aware of the significance of cybersecurity, but they are doubtful about their practical capabilities (figure 17).

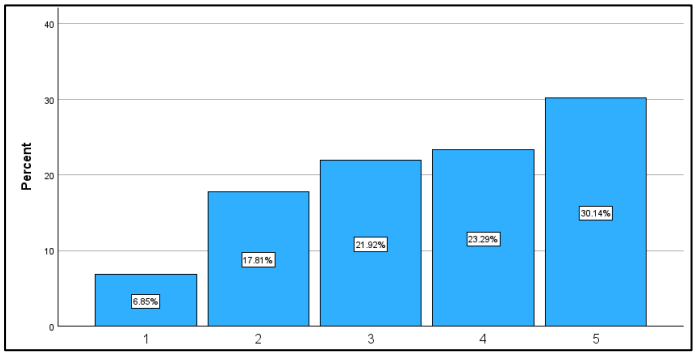

Figure 7: Participant Confidence Levels in Overall Cybersecurity Knowledge

Only a few respondents answered in the affirmative when asked about their experience of formal training on cybersecurity. Still, responding to the question of whether they would be eager to participate in further awareness campaigns, a majority of the respondents confirmed their eagerness to participate in cybersecurity education provided with the opportunity to do it.

Students also mentioned the kind of training and support they would like received by their university. The online self-training and email tips/newsletters were the most popular ones (figure 18).

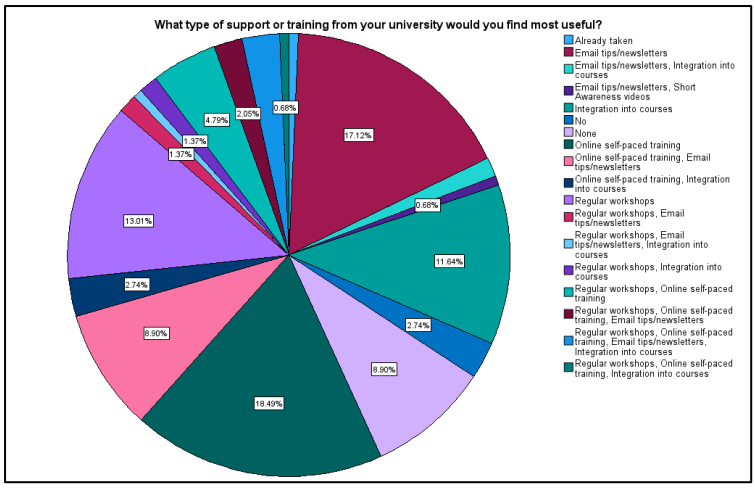

Figure 8: Most Useful Types of Cybersecurity Training as Identified by Students

In general, the findings show that, Students show moderate self-confidence on cybersecurity. The majority are not well trained formally, but eager to join awareness campaigns. They prefer loose and convenient kinds of learning that fit well into their education. The insights indicate that to develop long-term cybersecurity competence among students, institutions may develop continuous and interactive teaching programs, e.g., blended online-based and email-tips.

Correlation Between Cybersecurity Domains:

Another area that the study explored is the correlation between significant dimensions of cybersecurity: cybersecurity training, phishing awareness, and social engineering resistance. The findings showed that there was a strong positive relationship between cyber training and social engineering resistance ($r = .30$, $p < .001$) and a weaker and significant relationship between training and phishing detection ($r = .17$, $p < .05$). Nonetheless, there

was no meaningful correlation between knowledge of social engineering and accuracy in the detection of phishing (r =.00, p=.985) indicating that these two might be separate security skillsets (table 3).

Table 3: Correlations Between Cybersecurity Training, Phishing Awareness, and Social Engineering Resistance

Correlations				
		Phishing_Accuracy	SE_Accuracy	Previous_Training
Phishing_Accuracy	Pearson Correlation	1	.002	.165*
	Sig. (2-tailed)		.985	.047
	Sum of Squares and Cross-products	15.021	.027	3.849
	Covariance	.104	.000	.027
	N	146	146	146
SE_Accuracy	Pearson Correlation	.002	1	.303***
	Sig. (2-tailed)	.985		<.001
	Sum of Squares and Cross-products	.027	21.370	8.466
	Covariance	.000	.147	.058
	N	146	146	146
Previous_Training	Pearson Correlation	.165*	.303***	1
	Sig. (2-tailed)	.047	<.001	
	Sum of Squares and Cross-products	3.849	8.466	36.438
	Covariance	.027	.058	.251
	N	146	146	146
*. Correlation is significant at the 0.05 level (2-tailed).				
***. Correlation at 0.001(2-tailed)				

DISCUSSION:

This paper investigated password practices and attitudes toward cybersecurity in 146 Australian university students, how (1) postgraduate (PG) students showed stronger password habits than undergraduates (UG), (2) postgraduates identified phishing better, (3) formal training was related to social engineering identification and (4) the general cybersecurity attitudes and training preferences. In general, we can find that the higher the level of study and training, the more security practices and awareness is somehow better, but there are gaps. We proceed to test our hypotheses one by one and contrast our findings with previous studies and draw conclusions.

Password Practices: Undergraduates vs. Postgraduates

In line with anticipations, postgraduates observed a high level of password-management behaviour compared to undergraduates. The students of the PG tended to use unique and complex passwords and password managers, and a significant proportion of the UG respondents acknowledged the reuse of simple passwords. This gap is only echoed by current research: [21] discovered that there is a vast Cybersecurity-Resilience Gap between UGs and PGS, where postgraduates show better results in the major aspects of security such as password management. Similarly, [22] also found out that more advanced students (higher academic year) were less susceptible to

phishing attacks, which means that they were more likely to have better underlying security practices (such as password hygiene). This study's findings are thus consistent with the idea of a postgraduate inflection point of cybersecurity maturity.

Conversely, other previous research is of the view that additional academic experience has diminishing marginal returns after a certain level of education is achieved. [23] provide the example of that the absence of continuous training of all students, staff, and faculty is a fundamental weakness of higher education cybersecurity. Provided that the majority of students at any level do not get much formal training on password protection, a postgrad status does not necessarily mean impeccable practices. However, according to our results, the level of safer password behaviour is higher among the students of the PG group (who are more likely to receive more coursework or workplace experience) than it is among the UG students. This is in line with the notion that there is a relationship between age and academic progression and improved security habits [21].

Implications: The increased password-behaviours of the postgraduates indicate that the universities need more effective password-security education on the undergraduate level. Specifically, the narrowing of the Cybersecurity-Resilience Gap described by [21] might be facilitated with the help of custom interventions (e.g. the compulsory orientation on password-hygiene). Baseline habits may be improved by encouraging the use of password managers and multi-factor authentication among students on their first year. Future studies can also look into particular curricular or extracurricular conditions and reasons why the PGs perform better, is it due to extra work in a course, professional experience or even just due to age maturity.

Cybersecurity Training and Social Engineering Detection:

Hypothesis 3 was that formal cybersecurity training leads to improved social engineering attack detection. Students who listed their attendance of cybersecurity courses or workshops were more likely to score higher on social-engineering situations in our data. Such positive correlation is in line with [24], who established that participants who were trained in cyber and those in cyber clubs were less prone to phishing. It is also in line with the general anticipation that education enhances awareness.

However, the association between them was not high. This is similar to [25], who observed that the more the exposure (e.g. heavy social media use) the higher the phishing risk is irrespective of training. Very active online students might have a greater number of threats, and they might require additional training as opposed to receiving less. Additionally, there is a warning in the large study conducted by [26], according to their study results, formal training did not have significant effects on the actual rates of phishing clicks. According to their work, the quality and recency of training is important, and that self-reported knowledge surveys (such as ours) may be overstating the real-world competence.

Implications: Instead of lectures, which are one-off, it is probable that continual, practical exercises are required. Education, as suggested by [26] should be included into a layered defence; we agree that training cannot be the only action implemented. Further studies might examine the training approaches (e.g. gamified modules, peer-led workshops) that are most likely to facilitate knowledge translation into vigilant behaviour particularly among students involved in risky actions on the internet [25].

Students' Cybersecurity Attitudes and Training Preferences:

Students in our sample had a moderate level of concern regarding cybersecurity with many students saying that they thought that security training is important and their university should provide more. Nevertheless, approximately 50 per cent of the respondents admitted that they consider a typical security lecture boring and expressed the desire to use interactive training tools or gamified ones. This trend is echoed by [27], who believe that university education must have ongoing and interactive awareness campaigns based on the role of students. Gamification and real-world simulations were also regularly cited as favourite tools by students interviewed during our survey, reflecting the desire to have innovative pedagogues in cybersecurity education.

However, one of the most interesting findings was that the awareness of social engineering among students in a similar university, as found by [28], was below the expected: 63% of their Nigerian university students were

unfamiliar with social engineering, and half of them have been victimized by phishing. According to our results, the Australian students are not so poorly informed as that extreme case, however, they are vulnerable. The enthusiasm which was demonstrated by numerous students with regards to further training indicates that it is not the problem of awareness but possibly the way it is done.

Implications: The data of the attitudes suggests that the universities need to invest in student-centred and culture-building strategies. As an example, it would be possible to incorporate short phishing tests as a part of coursework or develop cyber-captains among students, as they prefer active work. Surveying students may also be conducted on a regular basis by the institutions to help customize the content. Conversely, the general positive attitude (students desiring additional training) is an advantage; it means that the students are willing to learn. Future research may look into motivational variables (peer influence, course credit, etc.) that lead to student participation in security training.

Implications for Higher Education and Future Research:

The above conclusions have significant implications. In the case of higher education institutions, the fact that difference levels are evident in study indicates that the core principles of security (strong passwords, awareness of phishing) are to be introduced at the undergraduate level, rather than presumed. Password management and email security be part of the curriculum related to freshmen [21], which we also support. Besides, the low efficacy of single training, the universities must implement a layered approach to security: train and educate people simultaneously training on spam filters with two-factor authentication; as well as perform regular simulated phishing attacks to sustain that awareness over time [26].

As a future research study, our research indicates several avenues. To begin with, bigger samples in several institutions would make it stronger in generalization. Second, longitudinal research would be able to follow whether the benefits of PG students are maintained after graduation, and whether the UG-level interventions would reduce the gap. Third, the qualitative research (focus groups, interviews) could prove the reason why the overall performance of the PG students is higher than that of the UGs, whether it is the job experience in the real world or the developed risk perception. Lastly, it would be desirable to conduct experimental analyses of various training platforms (gaming, micro-learning, etc.) by predisposed student choices. These tests might be used to investigate whether the weak correlations that we reported between training and detection can be enhanced with more interesting formats.

Limitations of the Study:

Self-report bias: Our data is based on surveys of students, and this is likely to exaggerate good practices and awareness. Respondents may provide socially desirable responses (e.g. inflating the complexity of their passwords or knowledge of phishing).

Sample size and composition: The sample used is rather small (146 respondents) and is not random as it represented different Australian universities. It might not be the most representative of disciplines and demographics (e.g. STEM vs. non-STEM). This restricts the extrapolation of results.

Cross-sectional design: We measured attitudes and self-reported behaviours at a single point in time. The cause-and-effect inferences (e.g. training leads to better detection) are therefore weak, longitudinal or experimental studies would be required to validate such effects.

Scope of survey: The items of phishing recognition and social engineering detection were hypothetical questions of scenario, rather than real phishing experiments. According to [26], test performance may differ significantly between the actual behaviour and the test. Thus, we should take our findings regarding the accuracy of detection lightly.

Notwithstanding such shortcomings, this research illuminates key trends in student cyberspace awareness and identifies actionable steps in the case of educational organizations. Combining the presented findings with the literature presented allows gaining a deeper insight into the ways in which higher education can create a more cyber-resilient community.

CONCLUSION:

This paper has looked into the cybersecurity behaviours, awareness, and attitudes of Australian higher education students, including the password practices, phishing awareness, social engineering vulnerability, and the preference toward cyber training. The results indicate that students have a minimum knowledge of the concepts of cybersecurity, but this knowledge is not always transformed into safe cyberspace behaviour. A large proportion of respondents remained users of the same password, they did not identify phishing indicators well enough and they were found to be susceptible in simulated instances of social-engineering manipulation. These behavioural discrepancies denote that one solely cannot be knowledgeable to guarantee cyber-secure behaviour among university students.

Another interesting finding of this study was the security behavioural patterns in undergraduate and postgraduate students, where postgraduates show more password hygiene and slightly higher phishing detection skills. This is probably due to years of experience in the academic field or maturity or previous training in security related issues. The correlation between the training of cybersecurity and increased awareness of the attempts of manipulations was positive and not that strong, indicating that the nature and method of delivering training can be equally critical as training itself. These behavioural observations are consistent with the current state of scholarly discourse, which is becoming more and more focused on explaining that cybersecurity threats within the university context are not exclusively due to knowledge deficiency but rather to the macro habitual, convenience-related decision-making within the virtual setting.

The study adds to the existing body of research on student cybersecurity by offering a data-driven and narrow-focused account on the Australian higher-education data. The majority of literature available on student cybersecurity is based in North America, Europe or Asia; there is not much student-level evidence available in Australia especially in areas that involve a combination of behavioural self-reporting and scenario-based testing. This current research thus adds to the existing body of literature by providing region-specific results and to confirm the existing global data that students remain a high-risk group within the cyber security system, not due to lack of awareness about what is risky, but because safe behaviours are not always applied.

It is also observed in the analysis that students expressed readiness to undergo more training on cyber matters, and they also indicated that they want more interactive, engaging and practical forms of training rather than the traditional lecture-based awareness training. This implies a timely need by the universities to transform their learning strategy with regards to cyber education, to occur as an active delivery of knowledge as opposed to a passive one and be a continuous, experiential and behaviour changing intervention. In general, the work confirms that to enhance cybersecurity in higher education, it is necessary to pay attention not only to technological protection but also to human behaviour and practice, as well as the strategy of learning.

STATEMENTS AND DECLARATIONS:

Ethical Approval:

The aspect of ethical compliance was very important in this research. Since the study was quantitative because the researchers used human subjects (students), all measures complied with the general tenets of the National Statement of Ethical Conduct in Human Research [29].

The subjects had been made aware of their rights like voluntary participation, anonymity and prerogative to pull out any time before submission. No information that could have been used to identify any individual was gathered so that anonymity was upheld.

The study was associated with low ethical risk because it did not include vulnerable populations, sensitive health information or deception.

Consent to Participate:

Informed consent to participate was obtained electronically from all participants prior to completion of the survey.

Consent for Publication:

Not applicable.

Conflict of Interest:

The author declares no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding:

The author received no financial support for the research, authorship, and/or publication of this article.

Data Availability:

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES:

[1] E. Morrow, “Scamming higher ed: An analysis of phishing content and trends,” *Computers in human behavior,* vol. 158, pp. 108274, 2024.

[2] K. Klasan, I. Dunder, and S. Seljan, "Assessing Information Security Awareness among Secondary School Teachers." pp. 1508-1513.

[3] T. I. Tanni, T. Taharat, M. S. Parvez, S. T. A. Rumee, and M. I. Zaber, “Is My Password Strong Enough?: A Study on User Perception in The Developing World,” *EAI Endorsed Trans. Creative Technol.,* vol. 9, no. 30, pp. e3, 2022.

[4] E. D. Frauenstein, and S. Flowerday, “Susceptibility to phishing on social network sites: A personality information processing model,” *Computers & security,* vol. 94, pp. 101862-18, 2020.

[5] R. M. Abdulla, H. A. Faraj, C. O. Abdullah, A. H. Amin, and T. A. Rashid, “Analysis of social engineering awareness among students and lecturers,” *IEEE Access,* vol. 11, pp. 101098-101111, 2023.

[6] B. Kelly, “Does Your Institution Provide Information Security Awareness Training?,” *EDUCAUSE Review (Online)*, 2019.

[7] E. Woollacott. "Gen Z has a cyber hygiene problem," September, 2025; https://www.itpro.com/security/gen-z-has-a-cyber-hygiene-problem#:~:text=Despite%20their%20reputation%20as%20digital,it%20comes%20to%20cybersecurity%20practices.

[8] T. T. Berre, V. Eggemoen, T. D. Haugrud, W. H. Le, and M. Sandnes, "Phishing awareness among students at NTNU." pp. 1117-1124.

[9] M. Butavicius, K. Parsons, M. Pattinson, and A. McCormac, “Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails,” 2016.

[10] R. Chandarman, and B. Van Niekerk, “Students' cybersecurity awareness at a private tertiary educational institution,” *The African Journal of Information and Communication,* vol. 20, pp. 133-155, 2017.

[11] A. ŞENOL, T. TALAN, and C. AKTÜRK, “A RESEARCH ON UNIVERSITY STUDENTS'AWARENESS OF CYBER SECURITY: CASE STUDY OF PASSWORD USAGE,” 2021.

[12] A. Nisenoff, M. Golla, M. Wei, J. Hainline, H. Szymanek, A. Braun, A. Hildebrandt, B. Christensen, D. Langenberg, and B. Ur, "A {Two-Decade} Retrospective Analysis of a University's Vulnerability to Attacks Exploiting Reused Passwords." pp. 5127-5144.

[13] R. Bleiman, and A. Rege, "An Examination in Social Engineering: The Susceptibility of Disclosing Private Security Information in College Students." pp. 47-XII.

[14] R. G. Broadhurst, K. Skinner, N. Sifniotis, B. Matamoros-Macias, and Y. Ipsen, “Phishing and cybercrime risks in a university student community,” 2020.

[15] M. Pattinson, C. Jerram, K. Parsons, A. McCormac, and M. Butavicius, “Why do some people manage phishing e-mails better than others?,” *Information management & computer security,* vol. 20, no. 1, pp. 18-28, 2012.

[16] S. Barakovic, and J. B. Husic, “Cyber hygiene knowledge, awareness, and behavioral practices of university students,” *Information security journal.,* vol. 32, no. 5, pp. 347-370, 2023.

[17] A. Chin, B. Jones, and P. Little, “A Comparative Analysis of Smartphone Security Behaviors and Practices,” *International Journal of Education and Development using Information and Communication Technology,* vol. 17, no. 3, pp. 57-80, 2021.

[18] M. A. Harris, R. Brookshire, and A. G. Chin, “Identifying factors influencing consumers’ intent to install mobile applications,” *International journal of information management,* vol. 36, no. 3, pp. 441-450, 2016.

[19] J. W. Creswell, and J. W. Creswell, *Research design : qualitative, quantitative, and mixed methods approaches*, Sixth edition. ed., Thousand Oaks, California: SAGE, 2023.

[20] A. Tick, D. J. Cranfield, I. M. Venter, K. V. Renaud, and R. J. Blignaut, “Comparing Three Countries’ Higher Education Students’ Cyber Related Perceptions and Behaviours during COVID-19,” *Electronics (Basel),* vol. 10, no. 22, pp. 2865, 2021.

[21] S. Goliath, P. Tsibolane, and D. Snyman, “Exploring the Cybersecurity-Resilience Gap: An Analysis of Student Attitudes and Behaviors in Higher Education,” 2024.

[22] R. C. Dodge, C. Carver, and A. J. Ferguson, “Phishing for user security awareness,” *Computers & security,* vol. 26, no. 1, pp. 73-80, 2007.

[23] R. Armas, and H. Taherdoost, “Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm,” *Information (Basel),* vol. 16, no. 5, pp. 336, 2025.

[24] A. Diaz, A. T. Sherman, and A. Joshi, “Phishing in an academic community: A study of user susceptibility and behavior,” *Cryptologia,* vol. 44, no. 1, pp. 53-67, 2020.

[25] S. O. Bello, C. Obunadike, O. Ogunleye, and S. Adeniji, “Impact Of Web (URL) Phishing and Its Detection,” *International Journal of Scientific Research and Management (IJSRM),* vol. 12, no. 04, pp. 484-493, 2024.
[26] A. T. Rozema, and J. C. Davis, “Anti-Phishing Training (Still) Does Not Work: A Large-Scale Reproduction of Phishing Training Inefficacy Grounded in the NIST Phish Scale,” 2025.
[27] N. Ben-Asher, and C. Gonzalez, “Effects of cyber security knowledge on attack detection,” *Computers in human behavior,* vol. 48, pp. 51-61, 2015.
[28] O. U. Gift, A. E. Omolara, A. Y. Abass, and E. C. Ubaka, “Social Engineering Awareness Evaluation in University of Abuja: A Pragmatic Approach,” 2024.
[29] NHMRC, “National Statement on Ethical Conduct in Human Research (2025),” 2025.

ACKNOWLEDGEMENT:

We would like to thank students who took part in the survey and shared their time and knowledge as communication would not have been possible in this case and we appreciate the University of Technology Sydney that has helped me to conduct this work by availing the academic structure, resources, and research climate.

APPENDIX:

The following questionnaire was administered to collect data on students' cybersecurity practices, phishing awareness, and social engineering susceptibility.

Table 4: Survey Questionnaire Items

Section	Survey Question	Response Type
Eligibility & Enrolment	Do you confirm that you are currently enrolled in a university or college and are 18 years or older?	Yes/No
Demographics	Are you currently enrolled in a university or college?	Yes/No
Demographics	Which university/college are you enrolled in?	Short text
Demographics	What is your current level of study?	UG/PG/PHD/Other
Demographics	What is your major/field of study?	Short text
Demographics	Are you an international student at this university?	Yes/No
Demographics	What is your gender?	Male/Female/Transgender/Prefer not to say
Digital Usage	Which of the following academic platforms have you used?	Multiple selection
Digital Usage	How often do you access your university portal?	Daily/A few times a week/Rarely/Never
Password Practices	Do you use the same password across multiple websites?	Yes/No
Password Practices	How long are your typical passwords?	MCQ (length categories)
Password Practices	Do you use any of the following to manage your passwords?	Multiple selection
Password Practices	Do your passwords include uppercase, lowercase, numbers, and symbols?	Yes/No
Password Practices	Do you enable two-factor/multi-factor authentication when available?	Yes/No/Sometimes
Online Behaviour	How often do you use VPN when you go online?	Always/Sometimes/Never/I don't know
Online Behaviour	How often do you check your email?	Always/Sometimes/Never/I don't know
Phishing Awareness	Have you ever received a suspicious email asking for personal or financial information?	Yes/No

Phishing Awareness	If you received an email claiming to be from your university but had errors and asked for login info, what would you do?	MCQ
Phishing Awareness	Can you identify a phishing email?	Yes/No/Not sure
Phishing Awareness	If you identified a phishing message, what clues made you suspicious?	Multiple selection
Cyber Incidents	Have you ever fallen victim to a cyber-incident (account hacked, money loss, data theft)?	Yes/No
Cyber Incidents	If yes, what happened?	Open-ended
Social Engineering	Have you heard of social engineering in cybersecurity?	Yes/No/Not sure
Social Engineering	If you get a call from someone claiming to be IT support asking for login credentials, what would you do?	MCQ
Social Engineering	Which of the following are examples of social engineering?	Multiple selection
Social Engineering	Have you ever been approached by someone pretending to be IT staff/bank officer/authority figure?	Yes/No
Social Engineering	If yes, what did they ask you to do?	Open-ended
Cyber Attitudes	How confident are you in your cybersecurity knowledge?	Likert scale (1–5)
Cyber Attitudes	Have you ever taken a cybersecurity course/session?	Yes/No
Cyber Attitudes	Would you be interested in cyber awareness training?	Yes/No
Cyber Attitudes	What type of training would you find most useful?	Multiple selection
Open Feedback	Do you have any suggestions for improving cyber safety for students?	Open-ended