Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Confident yet Concerned: Inconsistencies in Computing Students' Attitudes on Cybersecurity

Victor Adama

avic888@aucklanduni.ac.nz

University of Auckland https://orcid.org/0000-0002-7465-1514

Robert Biddle

Carleton University

Nalin Arachchilage

The Royal Melbourne Institute of Technology

Danielle Lottridge

University of Auckland

Research Article

Keywords: Cybersecurity, Computing Students, Attitude, Digital Resignation, Cybersecurity Fatigue

Posted Date: June 12th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9973914/v2

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

Noname manuscript No.
(will be inserted by the editor)

Confident yet Concerned: Inconsistencies in Computing Students' Attitudes on Cybersecurity

Victor Adama · Robert Biddle · Nalin Arachchilage · Danielle Lottridge

Received: August 2025 / Accepted: May 2026 — International Journal of Information Security

Abstract Today's young adults are most immersed in technology, leading in feelings of powerlessness in managing online privacy across many platforms, and particularly susceptible to phishing attacks. This raises questions about their general, wide-ranging attitudes towards and management of cybersecurity. How do young, tech-savvy adults approach cybersecurity? We seek a better understanding of their cybersecurity knowledge, attitudes and experiences, in particular in addressing deceptive online communications. We surveyed a group of 'lead users': computing university students ($n = 236$). By combining thematic analysis of open-ended responses with quantitative data, we provide insights into their experiences and perceptions. While students demonstrate reasonable cybersecurity awareness, their cybersecurity experiences vary, and inconsistencies exist around their practices, perceptions of responsibility, and support structures. Findings also reveal four key thematic tensions: 1) Computing students are knowledgeable yet have persistent incorrect beliefs, 2) They learn more about keeping safe from sources outside the classroom, 3) They have limited assistance and have fallen victim to cybercrime, and 4) Many are confident, yet others are concerned about their own safety and responsibility. Through cluster analysis of attitudes, we identify two groups, with one feeling less prepared, less confident, yet expressing a desire to learn more. Established measures of intentions and objective knowledge were correlated to preparedness. Self-efficacy correlated to confidence and predicted cluster membership.

Keywords Cybersecurity · Computing Students · Attitude · Digital Resignation · Cybersecurity Fatigue.

V. Adama
University of Auckland E-mail: avic888@aucklanduni.ac.nz

R. Biddle
Carleton University E-mail: robert.biddle@carleton.ca

N. Arachchilage
The Royal Melbourne Institute of Technology E-mail: nalin.arachchilage@rmit.edu.au

D. Lottridge
University of Auckland E-mail: d.lottridge@auckland.ac.nz

1 Introduction

Cybersecurity is hard [38]. However, we would expect tech-savvy young adults in tertiary education, particularly students studying computing, to be some of the best equipped to handle it [61]. Yet, the technical aspects they understand—such as antivirus software, firewalls, and spam filters—have over time proven insufficient to address all cybercrime [26, 46, 33], leaving them vulnerable [4, 25, 62, 23, 41]. In our study, we focus on computing students as 'lead users' [64] to understand contemporary reactions and attitudes to today's cyber climate, and in particular toward social engineering such as phishing, which cuts past technical defences to be today's most effective and pervasive cyber tactic [1, 2, 65].

Young people, especially those studying computing, are deeply embedded in digital ecosystems where their personal data is constantly collected and monitored.

The framing of our study is what Draper and Turow [18] refer to as "digital resignation". They suggest that is a rational response of some people to the widespread monitoring and collection of personal data online: "they are resigned" —"they are convinced that surveillance is inescapable". In 2006, Barnes [6] used the term "privacy paradox" to describe how young people despite disagreeing that "everybody should know everything

PREPRINT

about everyone else", they nevertheless used online platforms for social connections, seemingly unaware that the platforms were public spaces. Much research has followed on general relationships between privacy intent and actual disclosure, and is reviewed and discussed by Kokolakis [37]. Like Barnes, Draper and Turow focus on online platforms, and they suggest people are not necessarily uninformed, nor making careful rational trade-offs. Rather, the reason for the apparent contradiction is that people perceive the power of online platform providers as "inevitable and immovable feature of contemporary life". Their proposal is for a theoretical framework for understanding the phenomenon, based on earlier work on the concept of resignation, addressing feelings of helplessness in crisis, and of futility and cynicism in the face of powerful external influences. Hoffmann et al. described the experience as privacy cynicism, defined as "an attitude of uncertainty, powerlessness and mistrust towards the handling of personal data by online services, rendering privacy protection behaviour subjectively futile" (p. 2) [31].

Those theories all concern *privacy*, meaning access by online platforms to personal information. It is possible that the complex factors shaping paradoxical attitudes and behaviour around privacy may also be affecting security [53], since young adults are seeing as leading as well as vulnerable. Given the difficulty and ever-evolving nature of cybersecurity, the close overlap between privacy and security, this motivates a broad-ranging examination of tech savvy young people's security knowledge (what they know about phishing-related attempts), the practical steps they take to address phishing-related attempts (know-how), their attitudes towards today's cyber climate, and their experiences in addressing phishing. This is an important issue, because if young people studying computing are resigned to cybersecurity vulnerabilities, then we should reconsider cybersecurity support and education. We ask the following research question:

- What are computing students' abilities, attitudes, and experiences around deceptive online interactions, particularly toward phishing?

The complex interplay we anticipate with security (as observed with privacy) led us to an exploratory design approach. While a strong theoretical framing and engagement with frameworks are often ideal, an overemphasis on pre-existing theory can sometimes hinder the discovery of critical insights, especially when the phenomenon under study is still emerging, dynamic, or inadequately theorized. In considering how the field of Information Systems (IS) tends to link empirical data collection to theory, Fink emphasises the need to "leave some room for exceptions... that may yield long-term benefits" (p. 98) [24] when researchers encounter "interesting and consistent evidence that cannot be deductively derived from established theory" (p. 98) [24]. In line with this reasoning, our study adopted a discovery-oriented approach. Rather than forcing the data into a predetermined theoretical framework, we allowed the insights to surface inductively, so that future research efforts could draw stronger theoretical and practical connections. In particular, we attempted to be non-judgemental and avoid emphasis on "compliance".

To assess a reasonably sized sample of computing students, we employ a survey approach. We employ factor analysis to show the strongest concepts, cluster analysis to identify distinct groups of participants, and logistic regression for inferential analysis. The results show a mixed picture, with fair knowledge and some confidence, but simultaneously a range of inconsistencies and concerns. We observed that those with more enthusiasm felt less prepared and confident, and those with less enthusiasm felt more prepared and confident. We discuss computing students' emerging contemporary attitudes towards cybersecurity as well as implications for cybersecurity education. Our study contributes:

- empirical findings on computing students' cybersecurity abilities, attitudes, behaviours, and experiences, and inductively identified themes that reveal inconsistencies across these dimensions.
- identified subgroups that differ in preparedness, confidence and interest. Cluster membership is associated to established scales for cybersecurity intentions (SeBIS), objective knowledge (PEW), word-of-mouth sources, and cluster membership is predicted by self-efficacy.

2 Related Work

Research on computing students' cybersecurity abilities reveals gaps between theoretical knowledge and actual practice. A 2024 survey of 126 undergraduate students in computing-related programs at the University of Colorado, Boulder found that they acknowledged the importance of cybersecurity but lacked understanding of what it entails. They perceived confidentiality, integrity, and availability as more relevant than cybersecurity itself and thought that studying cybersecurity requires advanced maths skills [14]. A 2018 study of 26 computing students at a range of U.S. universities using think-aloud interviews revealed confusion between cybersecurity concepts, such as authentication and authorization, and also about encryption and the role of

PREPRINT

digital certificates. Notably, these misconceptions persisted even among students who had completed cybersecurity courses Thompson et al. [58]. A 2019 survey of 247 students from two universities in Silicon Valley found only 26% agreed or strongly agreed that they were knowledgeable about cybersecurity. The study revealed a troubling contradiction: students acknowledge the risks associated with digital communications but lack adequate strategies for safeguarding their information. Despite being in a tech-savvy region, some participants displayed insufficient awareness of data protection measures such as two-factor authentication (2FA) and the risks of online surveillance. About 8% did not know what two-factor authentication was, and only a minority demonstrated secure behaviours such as using two-factor authentication consistently or employing strong passwords across accounts. Moallem argued that educational institutions fail to adopt proactive strategies to equip students with the necessary skills to mitigate cybersecurity threats[41], echoing findings from Cowit et al. [14].

Studies from other countries show similar results. A survey of 87 students at a Greek university examined how higher educational levels correlated with greater cybersecurity awareness and adherence to good cybersecurity practices and ethical standards [23]. Masters level students demonstrated greater awareness and compliance compared to their undergraduate counterparts. Despite this, there were noticeable gaps in awareness levels. Students specialising in computing exhibited a higher degree of technical knowledge, but also demonstrated a tendency to engage in insecure practices. Their adoption of tools and protective measures was noted to have been minimal and more than half used the same password across multiple accounts.

Other research efforts examined how computing-related students manage passwords. In a 2016 survey of 45 South African university computing students, while participants demonstrated awareness of theoretical knowledge on password policies, many did not implement these principles consistently [25]. Many students reused passwords across multiple accounts, failed to delete unused accounts, wrote passwords down and engaged in other insecure practices. A 2018 study with 481 computing students at a Nigerian university echoed these findings: there was widespread awareness of good password practices but notable failures to apply them in everyday practice [62]. Both studies emphasised that awareness alone was insufficient to ensure protection.

The issue of responsibility emerged as a significant theme in a 2015 study of 274 students enrolled in an introductory Information Systems course. Findings revealed that many students viewed cybersecurity as a technical responsibility associated with IT professionals, rather than something that required their active involvement [47]. Their social representations of cybersecurity tended to focus on external threats like hackers, while personal actions and behavioural risks were often overlooked. The authors argue for instructional design that promotes personal responsibility and contextual understanding, rather than focusing solely on abstract or technical aspects.

Research efforts have also compared computing students to peers from other disciplines. A 2023 study comparing cybersecurity practices between computing and other students at a large U.S. university [15] found that while both groups demonstrated similar levels of practical cybersecurity knowledge, computing students exhibited significantly better password hygiene. Key differences included stronger use of random password elements, more frequent password updates, and higher adoption of two-factor authentication among computing students. Non-computing students were more likely to engage in insecure practices such as using identical or predictable passwords [15]. In contrast, a 2023 study with 1,710 students from eight Chinese universities (grouped into computing, science and engineering, and liberal arts majors) expected that those with computing majors would outperform their peers, however results revealed that all students showed weak password practices regardless of their major. The authors reported that differences in cybersecurity awareness across both categories were largely insignificant[27].

In summary, while computing students often display marginally better awareness of cybersecurity threats and ethical issues than their non-computing peers, this advantage is not consistent or comprehensive. Across studies, a recurring pattern of knowledge–practice gaps and limited engagement with preventive behaviour is observed. While more general research efforts reveal that young adults are particularly susceptible to phishing attacks [52, 36, 3], computing students—a subset of this demographic—are especially compelling to examine. This is mainly because despite their formal exposure to information technology concepts and assumed familiarity with digital environments, the potential paradox between their technical inclination and actual cybersecurity behaviour warrants further attention. Their relative advantage in awareness over non-computing peers is neither consistent nor sufficient to improve safety, underscoring the need to understand the complexities shaping their cybersecurity posture.

PREPRINT

3 Method

To better understand computing students' abilities, attitudes, and experiences around cybersecurity and deceptive online interactions, we employed a mixed-methods survey [32].

3.1 Participants

We recruited 236 participants from a non-cybersecurity computing course at the University of Auckland, an urban university in an OECD country with a Computer Science department that is ranked within the top 100 worldwide. Participants were recruited from undergraduate Human-Computer Interaction (HCI) courses comprising Computer Science (n = 255) and Software Engineering (n = 86) students. Participation was voluntary, and approximately 69% of students chose to take part. As the sample was drawn from an HCI course, it is likely participation was skewed towards students with interests in HCI. However, they were all final year students, and all would have passed earlier courses in programming, algorithms, computer organisation, and mathematics, and a range of more specialised computing courses. Participants were offered course credit for participating, along with the opportunity to win a $200 voucher. 68% of participants were male, 26% female, and 6% preferring not to say. The age distribution was between 16–24 (93%), 25–34 (6%) and 35–44 years old (1%). Approximately 5% had full-time jobs, 43% had part-time jobs, 3% were self-employed, and 37% were not employed. 12% described their employment, reflecting jobs across various sectors, including sales, events, training, finance, IT, and others. Most owned and used various devices (phones 98%, computers 99%, tablets 49%) and accessed the Internet daily (99.5%).

3.2 Survey Design

The survey design followed a process of question development, expert validation with five cybersecurity experts, and pilot testing. A pilot study with a sample of 20 participants was conducted (not included in the final tally of 236). The results highlighted areas where wording was unclear, and response options were limited, enabling us to refine the survey for clarity, relevance, and comprehensiveness.

3.3 Ethical Considerations

Our University requires a comprehensive explanation of ethical considerations be provided before granting clearance for research studies such as ours. We first explained the importance of online fraud and deception such as phishing, and that research has shown the importance of education and training to avoid the danger, referencing Rahman et al. [48] and Gupta et al. [28]. We provided a participant information sheet which explained the purpose of the study, assuring that participation was voluntary and would not affect relationships with the University. Data management procedures to ensure confidentiality were also explained. We offered contact information for support, especially offering cultural support for Māori (the indigenous population of New Zealand). The study received approval from the university's human research ethics committee. We address limitations in this process at the end of this paper.

3.4 Survey Structure

We outline below the structure and flow of the survey. See the appendix for the full survey questions. The survey had an estimated completion time of 28 minutes, as assessed by the Qualtrics survey platform.

Initial Information, Consent and Inclusion Criteria The survey began with a brief introduction to the intent of the study. A link to a Participant Information Sheet was provided. A consent form described rights and options regarding participation.

Cybersecurity Knowledge and Experiences Questions included self-reported IT knowledge, understanding of cybersecurity, perceived ability to recognise deceptive communications (emails, text messages and phone calls), and experiences with cybercrime.

Sources of Cybersecurity Knowledge Open-ended questions asked about the sources of cybersecurity knowledge. This section asked questions to establish knowledge acquisition sources, either through formal education, self-directed learning, online resources, personal experiences, and informal support networks.

Attitudes Toward Cybersecurity Questions in this section asked about their attitudes relating to cybersecurity, its importance and their level of concern about cyber risks. We also asked them to assess their confidence and ability in managing cybersecurity threats. These questions aimed to capture the participants' mindset regarding online safety and their perceived responsibility in protecting themselves.

PREPRINT

Technology Usage To contextualise participants' cybersecurity practices, the survey included questions about technology usage: frequency of use, types of devices and platforms, and online activities.

Cybersecurity Support Networks These questions asked whether participants had trusted persons, such as family members, friends, or professional networks, to turn to for cybersecurity advice. This section aimed to understand how participants cope with cybersecurity issues and where they seek guidance when needed.

Adapted Questions from Established Surveys To enable benchmarking our sample compared to others, we incorporated items from established instruments:

- Objective ability testing questions from the Pew Research Center [45]. We included 7 questions from the Pew survey ability-based questions provide objective assessment about knowledge on key cybersecurity concepts such as multi-factor authentication, phishing, password security, and encryption.
- The Security behaviour Intention Scale (SeBIS) assesses intentions [21], which are related to behaviour [20]. It examines secure practices across key domains: password management, account security, and awareness of online threats. Each item was rated on a five-point Likert scale. Responses are summed for an overall SeBIS score.
- An adapted General Self-Efficacy Scale [50] to gauge confidence in handling cybersecurity challenges. The scale comprises ten items rated on a seven-point Likert scale, yielding a composite General Self-Efficacy (GSE).

Demographic Information The questions included age, gender, educational background, and other relevant factors that could influence their knowledge and attitudes about cybersecurity.

3.5 Data Analysis

3.5.1 Thematic Analysis

Thematic analysis [11], an inductive approach widely used in behavioural science due to its flexibility and nuance, was utilised at two levels: at the level of the open-ended questions and at the level of organising all the survey results into themes. To analyse themes in the answers to open-ended questions, we engaged in data familiarization, coding, theme generation, and validation [11, 44, 39]. The first author immersed himself in the data by repeatedly reading and re-reading the open-ended responses. Weekly research meetings were held where the first author updated the team on the coding progress using a peer debriefing process [39]. The other authors reviewed and validated the codes and themes during these meetings, reaching consensus through discussion.

To identify themes across the qualitative and quantitative data, the author team engaged in a similar reflexive process of discussing results and grouping results. We examine the descriptive statistics of the quantitative data holistically in the context of all of the results. The four major themes emerged as we reflected on implications from all the results obtained. The last theme involved patterns in attitudes and included more targeted statistical analyses which we describe next.

3.5.2 Analysis of Attitudes

To determine the strongest underlying concepts in the attitudes, we employed exploratory factor analysis. We used the R statistics package and followed the methods of Beaujean [7]. We first used the "Scree" test and determined that three was a suitable number of factors, and then used the "Varimax" rotation for exploratory analysis. We looked at factor loadings, having removed items with magnitudes below 0.5. K-means cluster analysis [40] was then used to identify distinct subgroups of participants who share patterns in their attitudes. The "Elbow" and "Silhouette" [7] pre-analysis methods suggested two clusters, and K-means with 100 iterations. 2D structuring based on proximity [35] showed the partitions to be disjoint. We identified two distinct clusters of 119 and 117 participants. We then explored how these clusters differed and the implications.

Our initial hypotheses explored how the results from our initial questions, SeBIS, Pew, and the adapted GSE, related to the results from our questions about attitude. In particular, after our factor analysis, we hypothesised that the SeBIS, reflecting intentions, and the Pew results, reflecting knowledge, would correlate positively with feelings of preparedness. Similarly, we hypothesised that the GSE, reflecting self-efficacy, would correlate positively with feelings of confidence.

After our K-means analysis showed the existence of two clusters in our participant population, we hypothesised that the SeBIS, Pew, and GSE results would show a difference between the two clusters. We also hypothesised that the two clusters would show differences in the sources where participants said they learned about cybersecurity. Finally, based on the studies of students we reviewed in section 2, where it was suggested that students had a knowledge-practice gap, we hypothesized

PREPRINT

that might explain the difference between the two clusters identified.

4 Results

Thematic analysis identified four overarching themes in computing students' abilities, attitudes and experiences across the qualitative and quantitative data:

1. Computing students are knowledgeable yet have persistent incorrect beliefs.
2. They learn more from sources outside the classroom.
3. They have limited assistance and have fallen victim to cybercrime.
4. Many are confident yet others have mixed concerns about safety and responsibility. Below, we describe the themes, drawing on thematic analysis of the open-ended questions and reporting distributions from the quantitative scales.

4.1 Computing Students are Knowledgeable, Yet Have Persistent Incorrect Beliefs

Computing students felt aware of online fraud, with 90% agreeing or strongly agreeing that they had heard a lot about it. They felt confident in their ability to protect themselves, with 77% agreeing or strongly agreeing. They reported encountering deceptive communications:

- 77% had received deceptive emails,
- 88% had received deceptive SMS text messages,
- 47% had received deceptive phone calls, and
- 60% had received deceptive private or direct messages on social media platforms.

Students' perceptions of their own awareness were substantiated by their ability to correctly point out aspects of digital communications that might warrant suspicion and deception attempts. They were adept at describing the tactics employed by cybercriminals to make their fraudulent schemes appear more convincing and explaining how they deceive individuals into divulging sensitive information. Most emphasised receiving deceptive SMS text messages while only about half (47%) had received deceptive phone calls, suggesting that text messaging may be a more common vector for scam attempts across our sample. Lastly, 65% indicated they had been asked to provide information online that they were uncomfortable sharing. Compared to data from National Cybersecurity Alliance, 60% of their sample had experienced phishing messages (p 16), while 67% say they can protect themselves (p 18) [43]. For example:

> *One tactic is creating websites that closely resemble legitimate ones, complete with logos and designs to deceive victims. They also use an urgent tone, often threatening severe consequences to instil fear and prompt immediate action. (P 15)*

> *Using the same URL as a reputable brand i.e ASB or ANZ but changing the 'a' character to a different unicode character thus redirecting the user to a phishing site. (P 45)*

> *They make email names to sound just like company names such as paypalsupport@gmail.com, which is obviously not a real email name but sounds convincing. (P 178)*

Participants were well-versed in identifying sensitive data that should be protected and not shared online. They recognised the importance of safeguarding personal details and login credentials, emphasising the need for vigilance online. For example, participants stated:

> *Naturally, things like username and password obviously are things that I would never give out. I try to avoid purchasing things online, so I suppose I'm cautious about my card credentials.*

> *Personal identifiers such as date of birth, home address, or financial information like credit card numbers, bank account information or passwords. Also, sharing my real-time location through GPS can compromise my privacy and safety. (P 211)*

> *Passwords and security codes. While I value my private information, I know it's out there due to Instagram, Linkedin and Facebook being repositories used by basically everyone. So it's more important to safeguard the information that I use to access these specific accounts since I do not want a threat actor acting on my behalf at all. I use 2FA on everything and I will never disclose any of this information to anyone online. (P 123)*

4.1.1 High Accuracy in Objective Knowledge Assessment

In Figure 1 we show the percentage of participants who correctly answered each question, showing data from both the original Pew survey (N = 1000) and our sample. Overall, more students were correct. Over 75% of the students correctly answered five or more out of the seven selected questions. The highest concentration of participants scored between 5 and 6 (out of 7 questions) on the scale, while less than 18% correctly answered only four questions, and 7% scored less than

PREPRINT

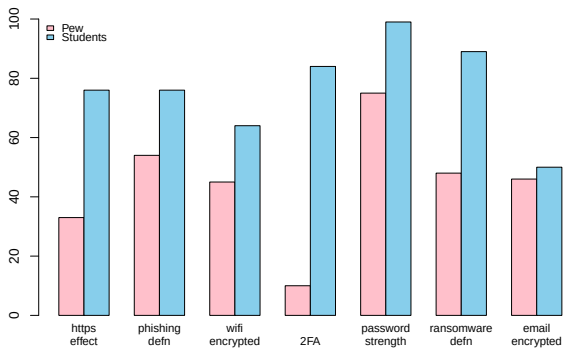


Fig. 1 Percentages of participants correctly answering each question, compared with participants in the Pew study. Full text of questions is shown in the appendix.

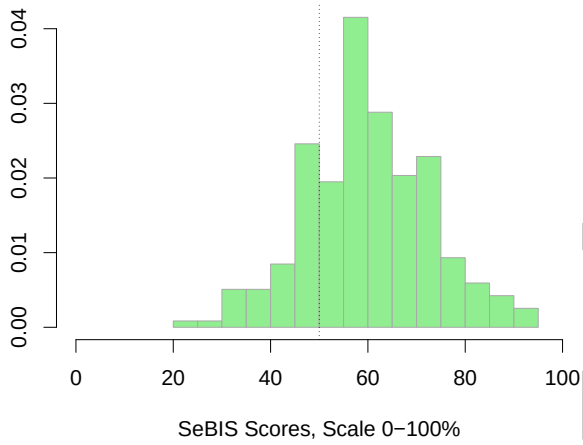


Fig. 2 Distributions of SeBIS scores, with participants reporting moderate to good adherence to 16 security practices; a score of 100% would indicate strong agreement with secure behaviours. The dotted lines indicate the midpoint of possible scores.

4. In comparison, in the original Pew survey [45], only one of these questions was correctly answered by 75% of the participants. (The questions, with correct answers highlighted, are in the appendix.)

4.1.2 Generally Good Cybersecurity Intentions

Students reported good adherence to secure cybersecurity practices (Figure 2). While the SeBIS hasn't been used for other student samples, a study with U.S. employees in a range of sectors [60] shows means over 70% which is higher than the mean for our students: 60%. However, differing contexts may affect responses: employees use desktop computers for work in a shared office, whereas the students typically use laptops for both coursework and personal use.

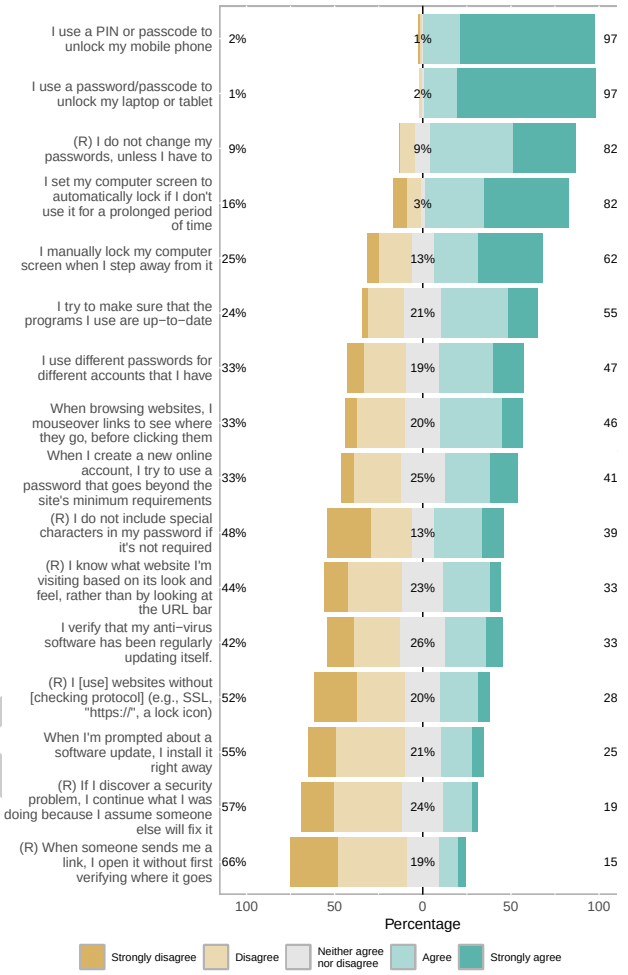


Fig. 3 Distributions of responses to questions to the 16 item SeBIS questionnaire. In calculating the overall score, items marked (R) have reversed scores.

The SeBIS indicates overall pro-active cybersecurity behaviour and it also highlights weak practices (Figure 3). 39% agreed "I do not include special characters in my password if it's not required"; 33% agreed "I know what website I'm visiting based on its look". The "worst" response from the students was the 82% who said they do not change passwords unless they must, but it is not clear how unreasonable that really is. Compared to 2015 when the SeBIS was published, today people have so many passwords that total uniqueness may have become unreasonable, and even experts report some form of password reuse [55].

When asked the practical question about how they would report a suspected online fraud or scam, over half of the participants were unsure what to do. This was particularly true for situations where personal information, such as a home address, phone number, pictures, etc., was compromised rather than login creden-

PREPRINT

tials. Noticeable amongst such responses was a sense of helplessness. A few examples of the responses are:

> *Depends on the information. If it was banking information, I'd call my bank to lock my cards/accounts. If it was information regarding where I live, I'm not sure. Probably just hope nothing malicious gets done with that information. (P 128)*
>
> *First step I would try to delete the information that I have revealed but knowing what's on the internet is on the internet somewhere, I would not be able to do anything else as its likely beyond my reach. (P 136)*
>
> *I would recall what information I gave out and try to change it if possible, like passwords. If it's my contact or personal details I wouldn't know what to do. (P 196)*
>
> *If it involves a password, I would immediately delete it, change the password to the account, and log out all users. If someone were to store a picture of myself, or my address details, I have no clue how I would control it. (P 68)*

Others mentioned they would contact relevant authorities using platform reporting mechanisms (for example, those offered on social media platforms and email clients), and involve the police.

4.1.3 Persistent Incorrect Beliefs

Certain incorrect beliefs were present. For instance, when asked how they decide whether or not to share information/data, they reported primarily relying on the trustworthiness and reputation of the platform (e.g., Microsoft, Amazon). They looked at: whether a site/message was *"professional-looking"*, security features such as `https`. Others simply relied on their instincts. Overall: students' trust judgments were based on cues no longer reliable to definitively guarantee trustworthiness.

4.2 Computing Students Learn More From Sources Outside The Classroom

Our participants reported learning about scams, warnings, password security, phishing, two-factor authentication (2FA), general cybersecurity practices, and identity protection. The most common sources of knowledge were word of mouth, social media, and financial institutions, with 51%, 45%, and 44% respectively (Figure 4). Of the social media, Reddit was mentioned the most frequently, followed by YouTube, Facebook, TikTok and others. Participants learned about protecting sensitive information from banks and about experiences of victims from word of mouth and social media. Examples of their responses are:

> *Everything I know about online scams and stuff, my dad taught me.*
>
> *Friends and family have talked about their personal experiences with times they have almost been scammed or any weird texts that they have received. This gave me more knowledge on strategies of scammers and more information on what to look out for. (P 225)*
>
> *Sometimes I'll see some types of scams going around and how to protect yourself against, but I am sceptical of these since the information is coming from social media. (P 60)*
>
> *Occasionally I receive notifications about recent fraudulent activities targeting members of my bank. It keeps me somewhat informed of what to look out for, but it isn't extensive. (P 50)*

Notably, academic institutions were not the primary source of their knowledge. Only 34% indicated these were a source of knowledge. Few students reported gaining knowledge from news outlets (27%), online advertisements (21%) and their workplaces (19%). Government establishments and NGOs were also less frequent sources of knowledge, with most not gaining knowledge from these sources or being unsure about it.

4.3 Computing Students Have Limited Assistance and Have Experienced Falling Victim to Cybercrime

Most participants (61%) did not have trusted persons to whom to turn for cybersecurity help or advice. Only 19% indicated having someone they trust, and only 13% reported having a "Go-To" person with IT expertise/qualifications. The frequency with which participants sought help from their trusted person was generally low. 15% reached out frequently, 11% weekly and most did so less often. When asked if they keep themselves updated about cybersecurity, 61% admitted that they do not, while only 39% reported active engagement with cybersecurity information.

21% of participants disclosed having fallen to at least one cyber scam or fraud. 16% reported they were not sure if they had fallen victim. 40% of participants reported knowing someone who had fallen victim to a scam or fraud. When asked to share their experiences of falling victim, the participants reported being scammed in various ways. A few reported falling victim as early as 7 and 8 years old. They reported technical attacks, such

PREPRINT

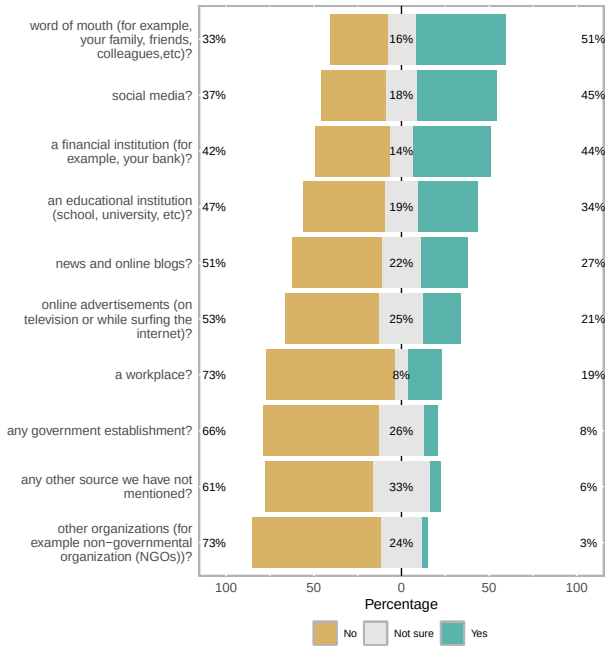


Fig. 4 Distributions of responses to possible sources of participants knowledge, with word of mouth and social media being more prominent sources of knowledge compared to formal institutions.

as phishing with links to fraudulent websites, as well as more general kinds of fraudulent behaviour. One prevalent type of crime involved online marketplaces where they paid for goods or services and did not get anything in return. Compared to [34], 25% of their sample reported financial related losses.

For example:

> *I contacted a seller on FB marketplace, transferred money and attempted to pick up the item, but they blocked me. I contacted the bank, but they said they could not return my money because I authorised the transaction. I contacted the police but they never followed up. (P 42)*

> *A person pretended to sell an item, we agreed for the item to be shipped once payment was received but the item was never sent after payment was sent. (P 170)*

> *I wanted to buy a mattress online. I paid to the person but they then blocked me. (P 41)*

Another category of cybercrime involved clicking on malicious links. Some examples are as follows:

> *I was expecting a package and received a text telling me to make a customs payment. I had just woken up, so I wasn't thinking straight yet and clicked the link to pay. (P 24)*

> *I clicked on a dodgy link, got my entire PC taken over including steam account, discord account and more. They got access to my card number via my steam account. I got everything back in the end but it was scary. (P 157)*

> *I was sent a message from a friend to scan a QR code to join a server on Discord, and then a bot took control of my account, and sent the messages to numerous other friends. (P 68)*

The last major category of reported cybercrime involved loss of money due to bank accounts or card compromise. For example:

> *I woke up and my bank account had been drained of all its money via PayPal. I couldn't link any particular action I did to how my PayPal account was compromised but PayPal were able to reverse the transaction and get my money back. (P 108)*

> *They got access to my bank account and they made payments to themselves but luckily I realized early and contacted my bank, and they sorted everything. (P 44)*

> *Money was taken out of my bank account without my consent via saved bank details I had in one of my online shopping accounts. (P 208)*

4.4 Confident But With Concerns

4.4.1 Many Computing Students Were Confident

Our adapted scale for Self-Efficacy had a roughly normal distribution with a slight skew to the right (Figures 5 and 6). More than half were confident about their self-efficacy and believed they had adequate cybersecurity abilities. We address confidence further in our analysis of their attitudes, next.

4.4.2 A Spectrum of Attitudes and Perceptions

Generally, participants reported confidence and engagement, but there are also responses that suggest less engagement (Figure 7). There was a strong awareness and recognition of the importance of cybersecurity and online protection. 85% agreed that cybersecurity is a necessary part of life (Figure 7). About 80% expressed the need to learn more. There was evidence for beliefs that both individuals and governments should hold responsibility for cybersecurity, with 61% agreeing that individuals are responsible for their safety and 72% believing the government should play a protective role.

PREPRINT

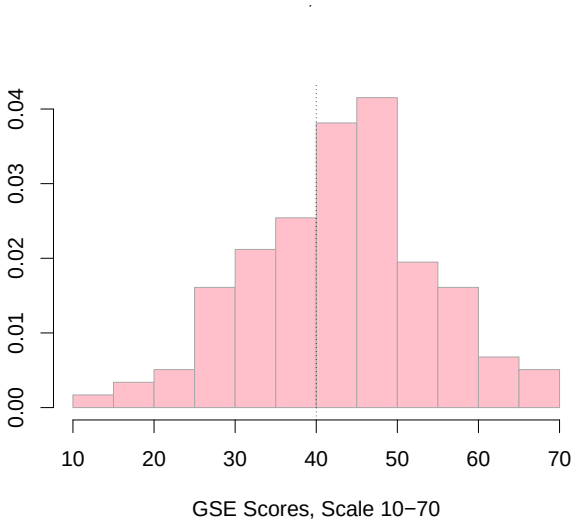


Fig. 5 Distribution of scores to the adapted 10 item General Self-Efficacy Scale. The result reflects a roughly normal distribution with a slight skew to the right (positive self-efficacy). The dotted line indicates the midpoint of possible scores.

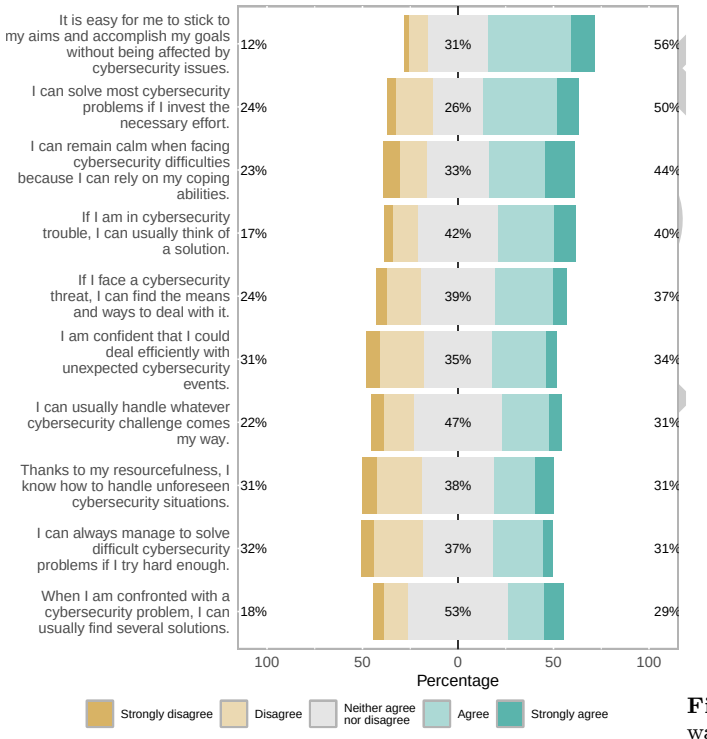


Fig. 6 Distribution of responses to questions to the adapted General Self-Efficacy questionnaire.

An exploratory factor analysis identified three factors, which we labelled "Unprepared", "Confident", and "Interested" (Table 1). They showed acceptable internal consistency with Cronbach's Alphas of .73, .78, and .72, respectively. The Comparative Fit Index (CFI) was .84. This value is moderate for hypothesised concepts, however it is deemed acceptable for exploratory work.

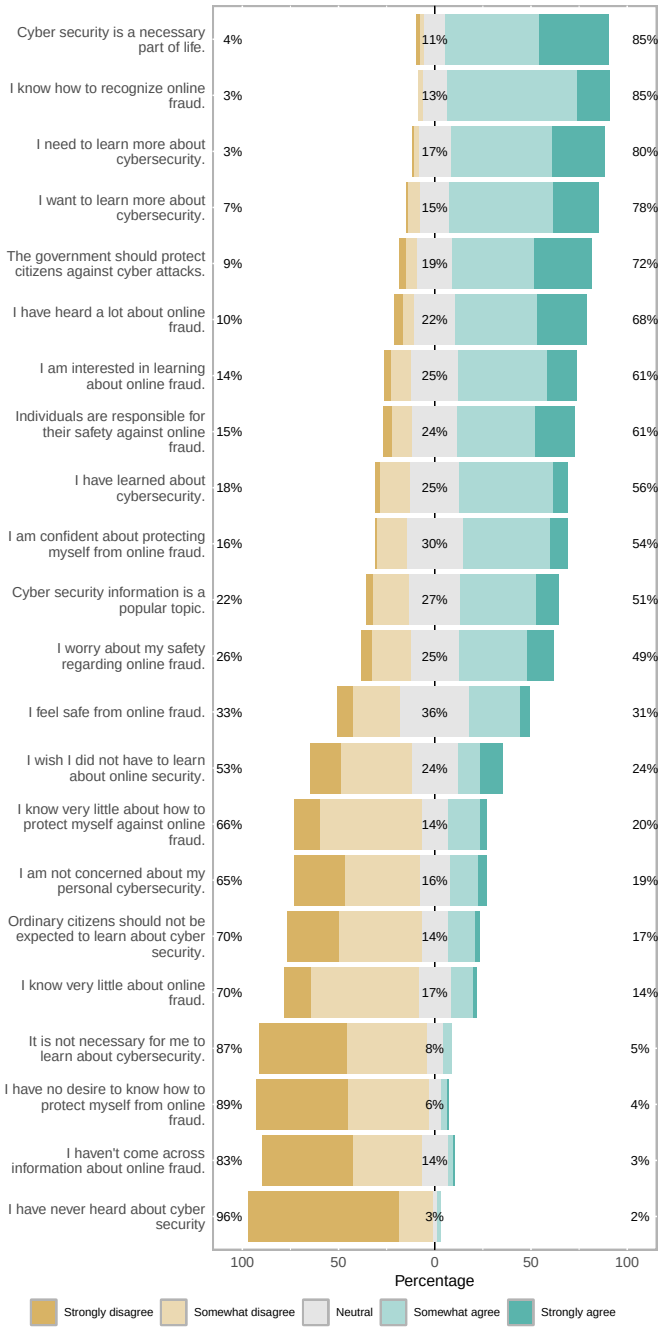


Fig. 7 Distributions of question responses to attitudes towards cybersecurity.

We therefore selected these three factors as a basis for further study.

4.4.3 Clusters with Shared Attitudes

We applied K-means cluster analysis to explore potential subgroups. Cluster 1 (C1) has higher levels of unpreparedness, low levels of confidence, and higher levels

Table 1 Factors from exploratory factor analysis, showing Cronbach's Alpha for each factor, and items with loadings (those with loading magnitudes under .5 removed).

Factor: Unprepared $\alpha = 0.73$	Loading
I know very little about online fraud.	0.71
I know very little about how to protect myself against online fraud.	0.68
I have learned about cybersecurity.	−0.52
I know how to recognize online fraud.	−0.56
Factor: Confident $\alpha = 0.78$	Loading
I feel safe from online fraud.	0.76
I am confident about protecting myself from online fraud.	0.63
I am not concerned about my personal cybersecurity.	0.61
I worry about my safety regarding online fraud.	−0.74
Factor: Interested $\alpha = 0.72$	Loading
I want to learn more about cybersecurity.	0.81
I am interested in learning about online fraud.	0.63

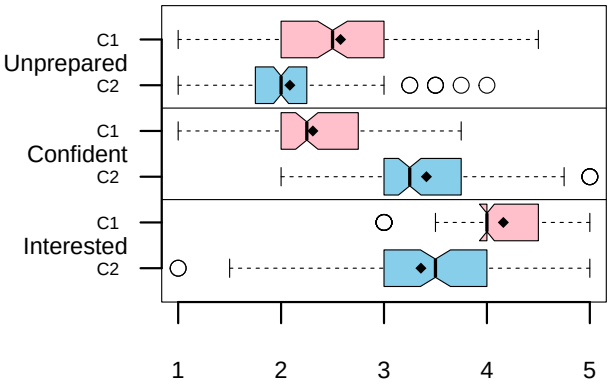


Fig. 8 Two identified clusters across participants, and their factor scores from 1 (Strongly Disagree) to 5 (Strongly Agree). The pink cluster shows a lack of knowledge and capabilities, and less confidence. Interestingly, they are *more* interested in learning.
(The black diamonds show means, black lines are medians, the coloured boxes represent the inner quartiles, and the whiskers represent the outer quartiles; circles represent outliers. Notches indicate ≈ 95% confidence intervals.)

of interest. Cluster 2 (C2) has lower levels of unpreparedness, high levels of confidence, and lower levels of interest in learning more (Figure 8). For each factor, the difference between clusters is significant ($p < .0001$).

In our sample, 119 feel prepared, confident and somewhat interested in learning more and the other 117 feel less prepared, quite unconfident, and very interested in learning more.

4.4.4 Inferential Analysis

We hypothesised there would be a negative correlation between Security Behaviour Intentions (SeBIS) score and the Pew total, each with Factor 1 (Unpreparedness), and a positive correlation between the adapted General Self-Efficacy (GSE) score and Factor 2 (Confidence). We used Pearson's correlation for SeBIS and GSE, and Spearman's for Pew, because it is a limited ordinal scale. Tests supported these hypotheses: SeBIS-F1: $r(234) = -0.39$, $p < .001$; Pew-F1: $\rho(234) = -0.19$, $p = 0.001$; GSE-F2: $r(234) = 0.44$, $p < .001$. The tests were conducted for each cluster separately and showed

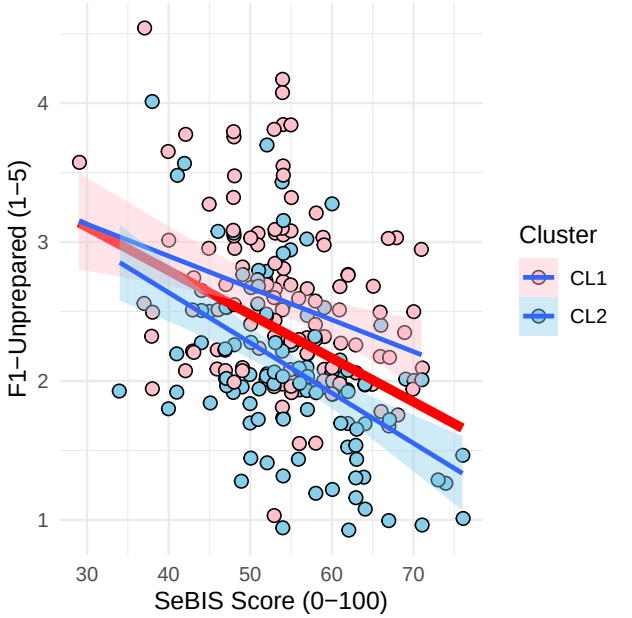


Fig. 9 Scatter plot showing relationship between SeBIS score and Factor 1-Unprepared.[1]

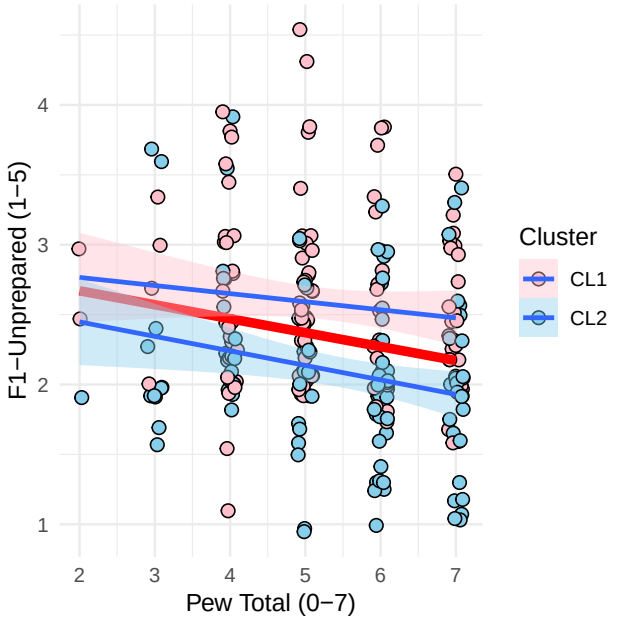


Fig. 10 Scatter plot showing relationship between Pew score and Factor 1-Unprepared. [1]

PREPRINT

Table 2 Comparison of Clusters 1 and 2 by SeBIS, Pew, and GSE scores

	M_1	SD_1	M_2	SD_2	Test result with Effect Size
SeBIS	54.01	8.22	55.24	8.04	$t(233.99) = -1.16$, $p = .123$, $d = -0.15$
Pew	5.25	1.23	5.50	1.30	$W = 6064.5, p = 0.040$ $r = 0.1$
GSE	39.35	10.44	47.70	10.18	$t(233.98) = -6.22$, $p < .001$, $d = -0.81$

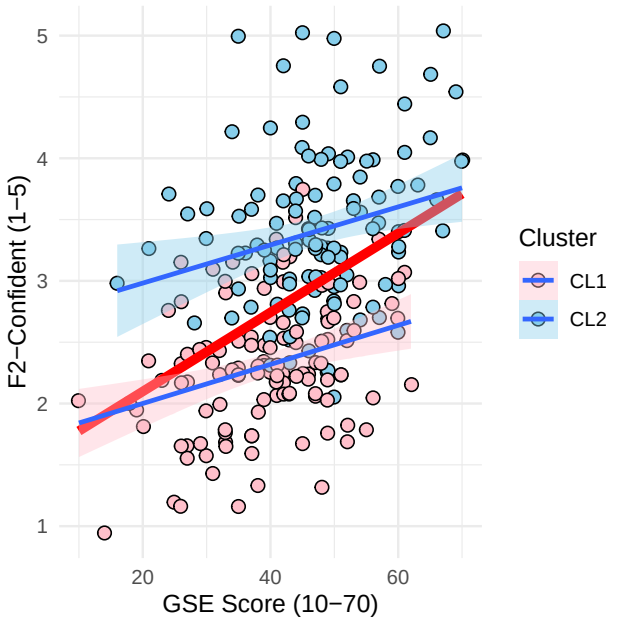


Fig. 11 Scatter plot showing relationship between GSE score and Factor 2-Confident. [1]

similar significant results. Scatter plots for the data are shown in Figures 9, 10, and 11.[1]

We hypothesised that Cluster 1 would score significantly lower than Cluster 2 on SeBIS, PEW, and GSE because the SeBIS would reflect security-conscious behaviour, the Pew would reflect knowledge and a feeling of being well-prepared, and the GSE would reflect feelings of confidence. We conducted one-sided t-tests for SeBIS and GSE, and a Wilcoxon test for the Pew (because the distribution was limited and skew). In each case the Cluster 1 means were lower then the Cluster 2 means. The differences between clusters for Pew and GSE scores showed significant difference, but those for the SeBIS did not: see Table 2. The scatter plot in Figure 9 suggests that the SeBIS results for each cluster are mixed, with both low and high SeBIS scores in each cluster.

To examine *why* the differences between clusters might have arisen, we considered more specific reasons. For example, whether they had a "go to" person, whether that person had expertise, and whether they had previously fallen victim to cybersecurity attacks, or knew someone who had been. We found no significant difference between the clusters for any of these. We then looked at the sources of cybersecurity knowledge reported, hypothesizing differences involving more and less reputable sources. We tested knowledge reported from financial institutions, workplace, education, word-of-mouth, social media, news media, government, and NGOs. Of these, the only significant difference was for word-of-mouth, with Cluster 1 people reporting significantly more use than those in Cluster 2: WoM: $\chi^2(1) = 4.641$, $p = 0.031$ — without correcting for multiple tests. There also was no evidence that people in each cluster used more sources. Lastly, we explored demographic data and found no significant differences for gender, employment, or age — almost all students were in the same age range (16–24).

To summarise, both intentions (SeBIS) and knowledge (Pew) are related to preparedness (F1) and self-efficacy (GSE) is related to confidence (F2). Yet, intentions do not differ so much as to be significant — they are much the same. Cluster 1 reported significantly more knowledge coming from Word-of-Mouth.

Our final hypothesis concerned the essential difference between the two clusters. We noted that the largest difference between clusters is Factor 2: Confidence. We therefore hypothesised that our GSE score might not only correlate to Factor 2: Confidence, but also explain the distinction between the clusters. We conducted a binary logistic regression with GSE score as the predictor, and cluster as the outcome. We found a significant result ($\chi^2(234) = -3.4962, p < .0001; OR = 1.08, 95\% CI = [1.053, 1.117]$). We also conducted the same test on SeBIS and Pew results, with no significant results. We therefore conclude the results with empirical evidence that *self-efficacy* may play a foundational role in explaining the difference between the two clusters we identified.

5 Discussion

Given that today's young people are immersed in technology with complex privacy concerns, are tech savvy yet susceptible and exhibiting gaps between security knowledge and practice, our research question asked: What are computing students' abilities, attitudes, and

[1] Red line shows overall correlation, blue lines show correlation for each cluster, along with 95% confidence bands; points are jittered to better show density.

PREPRINT

experiences around deceptive online interactions, particularly toward phishing? We anticipated that the students' background in computing would show strong abilities. While this was true to some extent, the findings revealed unexpected inconsistencies. The students were more knowledgeable than the general population, but academic courses were not the primary source of their cybersecurity knowledge. We found they lacked adequate support systems, and some had fallen victim to cybercrime. They were mostly confident about their abilities, but they also expressed notable concerns about their safety.

5.1 Contributions and Association to Theory

In our cluster analysis, one set of participants felt less prepared and less confident, while the other felt more prepared and more confident. A well-known but surprising connection between competence and confidence is the "Dunning-Kruger effect", where "poor performers in many social and intellectual domains seem largely unaware of just how deficient their expertise is"[19]. We studied relationships between objective knowledge and confidence in our study, but did not find any evidence that suggested people with less knowledge were more confident. However, it is interesting that our participants with less confidence were on average more keen to learn.

A relevant theory of attitudes is "Security Fatigue" where one feels constantly vigilant online, bombarded with cybersecurity warnings, password requirements, and threat alerts, contributing to fatigue and complacency [26]. This attitude was observed in a workplace context as well as in everyday life [53], for example:

> I think I am desensitized to it—I know bad things can happen. You get this warning that some virus is going to attack your computer, and you get a bunch of emails that say don't open any emails, blah, blah, blah. I think I don't pay any attention to those things anymore because it's in the past. People get weary of being bombarded by "watch out for this or watch out for that" (participant 101 (p. 26)[53])

A related theory "compliance budget" also originates in the workplace and describes how employees weigh the costs and benefits of compliance. When their limit is reached, individuals may refuse to comply or find ways to circumvent requirements, as their willingness declines with the introduction of additional security policies and demands [8]. Students are not under the same demands as employees, yet we observed correlations of behaviour intentions and objective security knowledge to preparedness and confidence. Our logistic regressions points to the deeper source of self-efficacy: "*Perceived self-efficacy is concerned with judgments of how well one can execute courses of action required to deal with prospective situations*" [5].

The phenomena around "digital resignation" [18] and "privacy cynicism" carry some similarities to what we observed in our wide cross section of data on attitudes towards cyber security. For privacy, there is a sense of young people feel resigned to having their data tracked and they feel like any efforts would be "futile." This suggests self-efficacy could be a moot point for some, as asking about self-efficacy for something impossible fundamentally does not make sense. Because we observed interest in cybersecurity alongside a lack of confidence and self-efficacy, this suggests there could possibly also be an emerging attitude of resignation for cyber security; our research suggests this would be important future work.

We observed that those in Cluster 1 (unprepared, lacking confidence, interest in learning) were more likely to learn through word-of-mouth, which is relevant to the "social learning" theory [17]. The reliance on informal sources could relate to the broader issues of confidence — students may feel confusion or a lack of clarity in information coming from these sources, which ultimately may not be increasing their security self-efficacy. We discuss more practical considerations regarding confidence next.

5.2 Confidence: Why Do Students Feel Confident Despite Having Cybersecurity Concerns

It is odd that confidence in the cybersecurity abilities of one of our clusters coexists with significant worries in the same cohort. One possible explanation is the fact that cybercrime is constantly taking different forms and increasing in complexity [42]. Even otherwise confident students might recognise that their abilities have limitations, especially in the face of increasingly sophisticated threats. Automaticity may play a role, where users may behave "automatically", like clicking on phishing links [63]. Especially if they become victims this way, they may feel that they cannot even trust themselves.

Students may feel prepared to handle known risks, but are aware that new and unforeseen dangers can emerge (for example, "zero day" vulnerability attacks [9]). This awareness can create a sense of vulnerability, where confidence in current abilities does not fully alleviate concerns about unknown threats. In comments, computing students rightly noted the significant impact that artificial intelligence could have on cybercrime.

PREPRINT

AI also is most likely going to prove itself to be able to improve scammers ability to conduct fraud to, and possible to a point where even knowledgeable individuals could fall for it. (P 159)

Fake information would appear more frequently, and due to the increasing usage of AI recently, people can create real voices and real images and use them for online fraud in new ways. (P 162)

That scammers are always developing their tactics, and in the future could involve AI that can accurately impersonate relatives/friends. (P 8)

With generative AI able to create legitimate looking communications with both customization, variation, and perhaps even interaction, such threats should be taken seriously [30, 66, 49].

Secure practices seemingly require users to scrutinize online communications with the attentiveness of an expert without clear or consistent guidance [12, 57]. Common cues of legitimacy can a times be unreliable, security advice is often impractical or conflicting, and users are expected to manage tasks that exceed human capabilities. As these challenges accumulate, the burden of staying secure grows, perhaps raising concerns amongst computing students, as shown in previous quotes. Additionally, secure practices may become obsolete. We found that students' trust judgments for the legitimacy were based on cues no longer reliable to definitively guarantee the trustworthiness of certain digital communications.

5.3 Complacency: Why Do Some Express Lack of Interest In Learning About Cybersecurity

A substantial portion of students were not particularly interested in learning more about cybersecurity and improving their abilities; they were more confident yet near-neutral in interest. This is particularly surprising as we anticipated a more engaged posture owing to their IT inclination.

A plausible reason could be a lack of time or resources involved in developing a good cybersecurity posture. Many individuals, such as students, might already be balancing demanding academic schedules, work, and personal commitments, leaving little room for additional learning activities. Cybersecurity might not be considered an immediate priority in this context unless they have faced personal cyber incidents. Results from our factor analysis ("I want to learn more" factor 3) suggests that while some acknowledge the importance of cybersecurity, they struggle to find the capacity to invest the time and resources necessary to develop their abilities, which would be relevant to the theory of "compliance budget". Unlike other well-established aspects of our lives where we outsource certain responsibilities, such as handing our cars to a mechanic to fix, or calling on a plumber to fix a leaking pipe, personal cybersecurity cannot be delegated. Moreover, there may be an effect of attitudes like "digital resignation", or "cynicism", as observed for privacy, on interest in learning about security: some students may simply be accepting that they cannot be fully secure, which unclear implications for learning. For example, students in our sample stated:

I don't know if my efforts to be vigilant are enough or will be enough in the future. I am aware of hacking and that sometimes things are just not in our control. (P 54)

I can't keep up to date with ongoing scams all the time, and there may be moments where I am not in the headspace to think critically. (P 3)

Kind of annoying to keep on tracking new ways that people find ways to hack and online fraud and you have to keep updating your security and learn ways that people try to do fraud on you. (P 77)

How careful do I need to be? Is there a certain number of steps I need to take to ensure I am fully protected? (P 33)

Why is it something that someone needs to do, rather than have a standard that prevents it from happening so often (P 31)

At the outset of this study, we were not anticipating finding attitudes related to cyber security anxiety or resignation. Emerging work coming out this year is showing cyber security anxiety [16] which they distinguish as current concerns, future anticipated threats, and perceived control over outcomes. The notion of perceived control relates back to the observed underlying strength of self-efficacy to explain clusters of attitudes and perceptions related to preparedness, confidence, and interest in learning.

5.4 What Should Constitute Cybersecurity Education For Students and The Public?

Our findings show that computing students were knowledgeable, yet, gaining this knowledge from sources other than academic courses raises several questions. Current standards for cybersecurity tertiary education are to prepare graduates to "design and develop more secure

PREPRINT

code, ensure data security and privacy, and apply a security mindset to their daily activities" (p. 256, [51]) yet there is a disconnect between their formal education and the practical knowledge they possess; this was also observed by others [41]. One potential reason could be the difficulty for academic institutions to keep course content up-to-date with new cybersecurity threats and vulnerabilities. Or, to remain consistent, academic courses might be overly theoretical, emphasising fundamental concepts and abstract theories, with little emphasis on practical, hands-on skills that of importance. As a result, students may not be fully prepared for the dynamic and unpredictable nature of cyber-threats in the real world.

While students may learn theoretical knowledge about computing and cybersecurity in academic settings, they may not be exposed to more practical knowledge about defending oneself in those settings. They may hear practical stories and lessons from friends and social media, which aligns with work on "social learning" [17]. The reliance on informal sources leading to consuming huge amounts of media coupled with the need for constant vigilance amongst many could consequently point to the broader issues of confidence and motivation. Students may feel overwhelmed by the sheer volume, diversity, and complexity of cyber-security information online. This can lead to confusion for some and a sense of helplessness for others, not knowing where to start or what information to trust. Sources of cybersecurity information might convey false or contradictory information. As a result, users can selectively engage only with the most clear and accessible sources. This raises questions about how to present cybersecurity information in a clear, reliable, and comprehensive way. Similar observations were made regarding information on securing home IoT devices [59]: their findings revealed it is extremely challenging to find coherent, actionable and reputable cybersecurity guidance online.

We speculate that it is possible that studying computing synergises with informal sources to improve abilities. These students draw on the same online resources, personal experiences, and real-world encounters as individuals without an IT background, and their academic exposure to computing concepts likely amplifies their ability to better interpret and apply this knowledge. This is in line with research on how computing education makes a difference in cybersecurity awareness between students undertaking a computing-related degree and others [61].

A promising direction would be a focus on a practical, hands-on curricula that aim to improve users' cybersecurity competencies and self-efficacy. Cybersecurity self-efficacy functions as both an antecedent and outcome of numerous psychological and behavioural variables [10]. Interactive and collaborative learning environments can strengthen self-efficacy, thereby encouraging engagement with cybersecurity concepts and practices [56]. Educational interventions grounded in self-efficacy principles can significantly improve users' confidence and attitudes toward using security tools and adopting safe practices [13]. Collectively, these studies demonstrate that cultivating self-efficacy is fundamental for improving everyday users' cybersecurity abilities, suggesting that effective cybersecurity education and interventions should prioritise strategies that build users' confidence, skills, and perceived competence in managing digital threats [54].

While improving education and communications about cybersecurity remain important goals, cybersecurity challenges are systemic. Problems stem from the very low cost of deploying cyber attacks and the lack of reliable identification requirements. Organisational responsibilities may have a role to play, rather than leaving individuals to protect themselves alone.

In summary, our study revealed that even computing students face notable challenges with their personal cybersecurity. They are not immune to mistakes, as shown by inconsistencies in understanding and practice. Furthermore, this reveals the need and importance of adequate support systems and resources, even for such a category. Surprisingly, some students displayed concerning levels of indifference towards cybersecurity. These findings suggest the need to develop better support systems, guidance, and improved educational tools, as well as for more research efforts on the factors that contribute to these attitudes and behaviours.

5.5 Limitations

Self-reported accounts of behaviour are subject to social desirability bias. This is an overarching concern pertaining to security behaviour research. Responses to instruments such as the SeBIS, GSE and certain open-ended questions may not accurately reflect participants' actual behaviours and attitudes, as they can be influenced by social desirability, overconfidence, or limited self-awareness. In our questions on "attitudes" we asked a variety of questions about perceptions and self assessment. Future work should more reflect previous research on cybersecurity attitudes specifically such as that by Hadlington [29] and Faklaris [22]. Also in future studies we aimed to address this concern by conducting follow-up interviews with selected participants to further probe certain aspects.

Another key limitation of this study lies in its sampling approach, as all participants were drawn from a

PREPRINT

single institution. While this provided consistency in curriculum exposure and other contexts, it may limit the generalizability of the findings to broader populations of computing students across different universities or regions. Institutional culture, teaching practices, and resource availability may uniquely shape students' experiences and awareness, potentially leading to results that do not reflect the diversity of computing education environments. Future studies could aim to include participants from multiple institutions to enhance the external validity and applicability of the findings. In a study such as this, we also recognise the importance of debriefing and providing an opportunity for students to learn more about the cybersecurity issues. We intended to do this in class, but the survey was not completed until the end of the semester.

Lastly, personal cybersecurity is quite broad and complex. More studies beyond ours, focusing on different aspects of personal cybersecurity, leveraging other research approach such – as additional follow-up interviews, longitudinal studies is critical to corroborate the data from our survey.

Further studies could explore methods that facilitate the reliable acquisition of cybersecurity abilities, and keep users' cybersecurity awareness current and adaptable. Finally, addressing the lack of adequate support structures is essential. Future research efforts could consider developing and evaluating support systems that facilitate the safe use of technology and assist users in navigating cybersecurity complexities.

6 Conclusion

This study involved a comprehensive survey on computing students' cybersecurity attitudes, behaviours, and experiences, which uncovered inconsistencies: 1) they are objectively knowledgeable yet hold out-of-date heuristics for identifying online deception, 2) they learn from non-academic sources, 3) they have a limited support network and have fallen victim to cybercrime, and 4) we discovered a range of preparedness, with one group more enthusiastic, confident yet feeling less safe and another group feeling unsure, unexcited about learning more, and feeling less concerned about their own safety.

Beyond that, the data and analysis reveal traces of sentiments that resonate with "digital resignation" [18], "security fatigue" [26], the "compliance budget" [8]. These theories warned against stretching user limits with respect to security. They posit that these sentiments are rational reactions to our current cybersecurity landscape.

These findings underscore the need for a two-pronged approach to improving cybersecurity abilities, as some people will be eager and open to learning and acknowledge their need to learn, while others may not be as open nor as concerned. Further research on attitudes, behaviours, and experiences is needed to better understand disparities in cybersecurity interest, knowledge, and practices.

Acknowledgement
We want to acknowledge and appreciate the University of Auckland for the support with the gift cards presented to the raffle draw winner.

References

1. Abawajy, J.: User preference of cyber security awareness delivery methods. Behaviour & information technology **33**(3), 237–248 (2014)
2. Aldawood, H., Skinner, G.: Educating and raising awareness on cyber security social engineering: A literature review. In: 2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE), pp. 62–68. IEEE (2018)
3. Algarni, A., Xu, Y., Chan, T.: An empirical study on the susceptibility to social engineering in social networking sites: the case of facebook. European Journal of Information Systems **26**(6), 661–687 (2017)
4. Aliyu, M., Abdallah, N.A., Lasisi, N.A., Diyar, D., Zeki, A.M.: Computer security and ethics awareness among IIUM students: An empirical study. In: Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010, pp. A52–A56. IEEE (2010)
5. Bandura, A.: Self-efficacy mechanism in human agency. American psychologist **37**(2), 122 (1982)
6. Barnes, S.B.: A privacy paradox: Social networking in the United States. First Monday (2006)
7. Beaujean, A.A.: Factor analysis using R. Practical Assessment, Research & Evaluation **18**(4), n4 (2013)
8. Beautement, A., Sasse, M.A., Wonham, M.: The compliance budget: managing security behaviour in organisations. In: Proceedings of the 2008 new security paradigms workshop, pp. 47–58 (2008)
9. Bilge, L., Dumitraş, T.: Before we knew it: an empirical study of zero-day attacks in the real world. In: Proceedings of the 2012 ACM conference on Computer and communications security, pp. 833–844 (2012)
10. Borgert, N., Jansen, L., Böse, I., Friedauer, J., Sasse, M.A., Elson, M.: Self-efficacy and security

PREPRINT

behavior: results from a systematic review of research methods. In: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, pp. 1–32 (2024)
11. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative research in psychology **3**(2), 77–101 (2006)
12. Chachak, E.: Best practices for secure digital communications. https://www.cyberdb.co/best-practices-for-secure-digital-communications/ (2025). Accessed: 2025-12-19
13. Chen, T., Stewart, M., Bai, Z., Chen, E., Dabbish, L., Hammer, J.: Hacked time: Design and evaluation of a self-efficacy based cybersecurity game. In: Proceedings of the 2020 acm designing interactive systems conference, pp. 1737–1749 (2020)
14. Cowit, N.Q., Ojha, V., Fiesler, C.: How do computing students conceptualize cybersecurity? Survey results and strategies for curricular integration. In: Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1, pp. 234–240 (2024)
15. Cravens, D., Resch, C.: Comparison of password hygiene for computer science and non-computer science undergraduates. In: Proceedings of the 24th Annual Conference on Information Technology Education, pp. 112–117 (2023)
16. Dall, N., Hagge, H.G., Mayer, P., Faklaris, C.: From fear to control: Developing a three-factor scale for cybersecurity anxiety (cybas). Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (2026)
17. Das, S., Kim, T.H.J., Dabbish, L.A., Hong, J.I.: The effect of social influence on security sensitivity. In: 10th Symposium On Usable Privacy and Security (SOUPS 2014), pp. 143–157 (2014)
18. Draper, N.A., Turow, J.: The corporate cultivation of digital resignation. New media & society **21**(8), 1824–1839 (2019)
19. Dunning, D.: Chapter five - the Dunning–Kruger effect: On being ignorant of one's own ignorance. In: Olson, J.M., Zanna, M.P. (eds.) Advances in Experimental Social Psychology, vol. 44, pp. 247–296. Academic Press (2011)
20. Egelman, S., Harbach, M., Peer, E.: 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, CHI '16, p. 5257–5261. Association for Computing Machinery, New York, NY, USA (2016). DOI 10.1145/2858036.2858265. URL https://doi.org/10.1145/2858036.2858265
21. Egelman, S., Peer, E.: Scaling the security wall: Developing a security behavior intentions scale (sebis). In: Proceedings of the 33rd annual ACM conference on human factors in computing systems, pp. 2873–2882 (2015)
22. Faklaris, C., Dabbish, L., Hong, J.I.: A self-report measure of end-user security attitudes (sa-6). In: Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019). Usenix Association (2019)
23. Filippidis, A.P., Hilas, C.S., Filippidis, G., Politis, A.: Information security awareness of greek higher education students—preliminary findings. In: 2018 7th International Conference on Modern Circuits and Systems Technologies (MOCAST), pp. 1–4. IEEE (2018)
24. Fink, L.: The philosopher's corner: The role of theory in information systems research. ACM SIGMIS Database: the DATABASE for Advances in Information Systems **52**(3), 96–103 (2021)
25. Fredericks, D.T., Futcher, L.A., Thomson, K.L.: Comparing student password knowledge and behaviour: A case study. In: HAISA, pp. 167–178 (2016)
26. Furnell, S., Thomson, K.L.: Recognising and addressing 'security fatigue'. Computer Fraud & Security **2009**(11), 7–11 (2009)
27. Guo, H., Tınmaz, H.: A survey on college students' cybersecurity awareness and education from the perspective of china. Journal for the Education of Gifted Young Scientists **11**(3), 351–367 (2023)
28. Gupta, V., Singh, S., Singh, C., Mangla, A.: A systematic review on cybersecurity: Models, threats and solutions. In: 2022 10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-22), pp. 1–6 (2022). DOI 10.1109/ICETET-SIP-2254415.2022.9791666
29. Hadlington, L.: Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon **3**(7) (2017)
30. Heiding, F., Schneier, B., Vishwanath, A., Bernstein, J., Park, P.S.: Devising and detecting phishing emails using large language models. IEEE Access **12**, 42,131–42,146 (2024)
31. Hoffmann, C.P., Lutz, C., Ranzini, G.: Privacy cynicism: A new approach to the privacy paradox. Cyberpsychology: Journal of Psychosocial Research on Cyberspace **10**(4) (2016)
32. Ivankova, N.V., Creswell, J.W., Stick, S.L.: Using mixed-methods sequential explanatory design: From theory to practice. Field methods **18**(1), 3–20 (2006)

PREPRINT

33. Jeong, J., Mihelcic, J., Oliver, G., Rudolph, C.: Towards an improved understanding of human factors in cybersecurity. In: 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), pp. 338–345. IEEE (2019)
34. Joinson, A.N., Dixon, M., Coventry, L., Briggs, P.: Development of a new 'human cyber-resilience scale'. Journal of Cybersecurity **9**(1), tyad007 (2023)
35. Kassambara, A.: Practical guide to cluster analysis in R: Unsupervised machine learning, vol. 1. Sthda (2017)
36. Klütsch, J., Schwab, J., Böffel, C., Zimmermann, V., Schlittmeier, S.J.: Friend or phisher: how known senders and fear of missing out affect young adults' phishing susceptibility on social media. Humanities and Social Sciences Communications **11**(1), 1–14 (2024)
37. Kokolakis, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security **64**, 122–134 (2017)
38. Kovačević, A., Radenković, S.D.: Sawit—security awareness improvement tool in the workplace. Applied Sciences **10**(9), 3065 (2020)
39. Lincoln, Y.S., Guba, E.G.: Naturalistic inquiry. Sage (1985)
40. Malik, A., Tuckfield, B.: Applied unsupervised learning with R: Uncover hidden relationships and patterns with k-means clustering, hierarchical clustering, and PCA. Packt Publishing Ltd (2019)
41. Moallem, A.: Cybersecurity awareness among students and faculty. CRC Press (2019)
42. Murphy, C.: Understanding cybercrime. Briefing: EU Policies—Insight. European Parliamentary Research Service. (2024)
43. National Cybersecurity Alliance: Oh behave: The annual cybersecurity attitudes and behaviors report 2024-2025. Tech. rep., National Cybersecurity Alliance (2025). https://www.staysafeonline.org/articles/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-2025
44. Nowell, L.S., Norris, J.M., White, D.E., Moules, N.J.: Thematic analysis: Striving to meet the trustworthiness criteria. International journal of qualitative methods **16**(1) (2017)
45. Olmstead, K., Smith, A.: What the public knows about cybersecurity. Pew Research Center (2017)
46. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C.: Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & security **42**, 165–176 (2014)
47. Pawlowski, S.D., Jung, Y.: Social representations of cybersecurity by university students and implications for instructional design. Journal of Information Systems Education **26**(4), 281–294 (2015)
48. Rahman, T., Rohan, R., Pal, D., Kanthamanon, P.: Human factors in cybersecurity: A scoping review. In: Proceedings of the 12th International Conference on Advances in Information Technology, IAIT '21. Association for Computing Machinery, New York, NY, USA (2021). DOI 10.1145/3468784.3468789. URL https://doi.org/10.1145/3468784.3468789
49. Roy, S.S., Thota, P., Naragam, K.V., Nilizadeh, S.: From chatbots to phishbots?: Phishing scam generation in commercial large language models. In: 2024 IEEE Symposium on Security and Privacy (SP), pp. 36–54. IEEE (2024)
50. Schwarzer, R., Jerusalem, M.: Generalized self-efficacy scale. J. Weinman, S. Wright, & M. Johnston, Measures in health psychology: A user's portfolio. Causal and control beliefs **35**(37), 82–003 (1995)
51. Servin, C., Aly, S., Cheon, Y., Eaton, E., Guevara, C., Kumar, A., Pirtle, T., Scott, M.: CS2023: ACM/IEEE-CS/AAAI Computer science curricula-specialized platform development. ACM/IEEE-CS/AAAI (2024)
52. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., Downs, J.: Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the SIGCHI conference on human factors in computing systems, pp. 373–382 (2010)
53. Stanton, B., Theofanos, M.F., Prettyman, S.S., Furman, S.: Security fatigue. IT Professional **18**(5), 26–32 (2016)
54. Stavrou, E., Piki, A.: Cultivating self-efficacy to empower professionals' re-up skilling in cybersecurity. Information & Computer Security **32**(4), 523–541 (2024)
55. Stobert, E., Biddle, R.: The password life cycle. ACM Transactions on Privacy and Security (TOPS) **21**(3), 1–32 (2018)
56. Sun, J.C.Y., Lin, H.S.: Effects of integrating an interactive response system into flipped classroom instruction on students' anti-phishing self-efficacy, collective efficacy, and sequential behavioral patterns. Computers & Education **180**, 104,430 (2022)
57. TenFour: Best practices for secure communication online. https://tenfour.nz/secure-communication-best-practices-tenfour/ (2025). Accessed: 2025-12-19

PREPRINT

58. Thompson, J.D., Herman, G.L., Scheponik, T., Oliva, L., Sherman, A., Golaszewski, E., Phatak, D., Patsourakos, K.: Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews. Journal of Cybersecurity Education, Research and Practice **2018**(1), 5 (2018)
59. Turner, S., Nurse, J., Li, S.: When googling it doesn't work: The challenge of finding security advice for smart home devices. In: Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9, 2021, Proceedings 15, pp. 115–126. Springer (2021)
60. Umeugo, W.: Security behavior intention of employees with hearing difficulties: An empirical comparison study. International Journal of Computer Science and Security (IJCSS) **17**(2), 29–43 (2023)
61. Venter, I.M., Blignaut, R.J., Renaud, K., Venter, M.A.: Cyber security education is as essential as "the three R's". Heliyon **5**(12) (2019)
62. Victor, A., Noel, M., Victor, L., Baba, M., Ekundayo, A.: Password knowledge versus password management. I-manager's Journal on Computer Science (2018)
63. Vishwanath, A., Harrison, B., Ng, Y.J.: Suspicion, cognition, and automaticity model of phishing susceptibility. Communication research **45**(8), 1146–1166 (2018)
64. Von Hippel, E.: Lead users: a source of novel product concepts. Management science **32**(7), 791–805 (1986)
65. Wang, Y., Qi, B., Zou, H.X., Li, J.X.: Framework of raising cyber security awareness. In: 2018 IEEE 18th International Conference on Communication Technology (ICCT), pp. 865–869. IEEE (2018)
66. Weinz, M., Zannone, N., Allodi, L., Apruzzese, G.: The impact of emerging phishing threats: Assessing quishing and llm-generated phishing emails against organizations. In: Proceedings of the 20th ACM Asia Conference on Computer and Communications Security, pp. 1550–1566 (2025)

PREPRINT

APPENDIX

Survey Questions

Information

Hi, we are looking for anyone 16 years or older.

We are interested in understanding what you know about online frauds and scams.

If you choose to participate, at the end of the survey, you will be eligible to also enter a raffle draw and win a gift card of $200 (New Zealand Dollars) or its equivalent. Only respondents who complete the survey will qualify to participate in the raffle draw.

Please review the **participant information sheet** via the link below.

LINK TO PARTICIPANT INFORMATION SHEET

CONSENT FORM

This form will be held for a period of six (6) years

Personal Cybersecurity and Understanding of Fraud

Name of Researcher: XX, XX, XX, XX.

I have read the Participant Information Sheet and understood the nature of the research. I have had the opportunity to ask questions and have had them answered to my satisfaction.

- I agree to take part in this research.
- I understand that I am free to withdraw my participation at any time and to withdraw any data traceable to me up to one month after participation.
- I understand that any data used in this research will be securely kept for 6 years after which it will be destroyed.
- I understand the data will be stored separately from my contact information to ensure confidentiality.

Approval: Approved by the University of Auckland Human Participants Ethics Committee on 03/05/2024 for three years. Reference Number xxxxxxxxx.

Page 1 of 16

Start of Block: 2. INCLUSION & EXCLUSION CRITERIA

Do you consent to participating in this survey? ● Yes ● No

Are you 16 years old or older? ● Yes ● No

End of Block: 2. INCLUSION & EXCLUSION CRITERIA

Start of Block: 3. KNOWLEDGE (FRAUD THROUGH TECHNOLOGY QUESTIONS)

Information

In this survey, we are interested in understanding what you know about cyber-related crime (online fraud or scams).

Cybercriminals use technology in deceptive manners to carry out fraud or scams, victimizing people. For example, via technology, they deceive people into:

- Revealing sensitive information such as passwords or bank details.
- Install malicious programs like computer viruses that compromise their security.

Please note that there are no right or wrong answers. It is more helpful for us to hear your honest thoughts and opinions.

Please rate the following statements.

1. I have heard a lot about online fraud.

● Strongly disagree ● Disagree ● Neutral ● Agree ● Strongly agree

2. I know how to protect myself against online fraud.

● Strongly disagree ● Disagree ● Neutral ● Agree ● Strongly agree

3. Can you think of any aspects of a communication (for example, phone call, email, message, SMS/text message) that would make you suspicious of it? (Open ended)

4. Can you think of any tactic(s) cyber scammers use to make their fraud/scams appear more convincing? (Open ended)

5. Have you ever received any email(s) you suspect were deceptive? ● Yes ● No

6. Please describe what you think makes such email(s) deceptive? (Open ended)

7. Have you ever received any text message(s) you suspect were deceptive? ● Yes ● No

8. Please describe what you think makes such text message(s) deceptive? (Open ended)

9. Have you ever received any phone call(s) you suspect were deceptive? ● Yes ● No

10. Please describe what you think makes such phone call(s) deceptive? (Open ended)

11. Have you ever received any PM “private message” / DM “Direct message” on any social media platform you suspect were deceptive? ● Yes ● No

12. Please describe what you think makes such PM “private message” / DM “Direct message” deceptive? (Open ended)

13. Have you ever been asked to provide information online that you felt uncomfortable sharing? ● Yes ● No

14. What types of information are you most cautious about giving out when online? (Open ended)

15. How do you decide whether or not to share information/data on a website or online platform? (It is fine to say "Not sure".) (Open ended)

16. Imagine you were tricked into revealing sensitive information online. What steps would you take next? (It is fine to say "Not sure".) (Open ended)

17. How would you report a suspected online scam or fraud? (It is fine to say "Not sure".) (Open ended)

18. Have you ever filed a report about an online scam or fraud? ● Yes ● No

19. Have you ever fallen victim to a scam or fraud? ● Yes ● No ● Not sure

20. Tell us what happened when you fell victim to a scam or fraud. (Open ended)

21. Do you know someone that has fallen victim to a scam or fraud? ● Yes ● No ● Not sure

22. Tell us what happened in the instances of those you know that have fallen victim to a scam or fraud. (Open ended)

23. Do you keep yourself updated about cybersecurity? ● Yes ● No

24. Please describe how you keep yourself updated about cybersecurity. (Open ended)

25. What concerns do you have about online fraud? Please describe: (Open ended)

24 What concerns do you have about protecting yourself against online fraud? Please describe: (Open ended)

25 Rate your agreement with this statement: "I am an expert in IT (Information Technology)."

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

26 Please describe your IT experience, if any: (Open ended)

End of Block: 3. KNOWLEDGE (FRAUD THROUGH TECHNOLOGY QUESTIONS)

Start of Block: 3.1 SOURCES

1. Have you gained knowledge about online fraud or scams from a financial institution (for example, your bank)? ● Yes ● No ● Not sure

2. Please describe the knowledge you gained from a financial institution. (Open ended)

3. Have you gained knowledge about online fraud or scams from a workplace?

● Yes ● No ● Not sure

4. Please describe the knowledge you gained from a workplace. (Open ended)

5. Have you gained knowledge about online fraud or scams from an educational institution (school, university, etc)? ● Yes ● No ● Not sure

6. Please describe what knowledge you gained about online fraud from an educational institution. (Open ended)

7. Have gained knowledge on online fraud or scams from word of mouth (for example, your family, friends, colleagues,etc)? ● Yes ● No ● Not sure

8. Please describe the knowledge you gained from word of mouth (for example, your family, friends, colleagues, etc). (Open ended)

9. Have you gained knowledge about online fraud or scams from social media?

● Yes ● No ● Not sure

10. Please describe the knowledge you gained from social media. (Open ended)

11. Have you gained knowledge about online fraud or scams from news and online blogs?

● Yes ● No ● Not sure

12. Please describe the knowledge you gained from news and online blogs. (Open ended)

13. Have you gained knowledge about online fraud or scams from any government establishment?
● Yes ● No ● Not sure

14. Please describe the knowledge you gained from the government. (Open ended)

15. Have you gained knowledge about online fraud or scam from other organizations (for example non-governmental organization (NGOs))? ● Yes ● No ● Not sure

16. Please describe the knowledge gained from other organizations such as non-governmental organization (NGOs). (Open ended)

17. Have you gained knowledge about online fraud or scams from online advertisements (on television or while surfing the internet)? ● Yes ● No ● Not sure

18. Please describe the knowledge you gained from online advertisements. (Open ended)

19. Have you gained knowledge about online fraud or scams from any other source we have not mentioned? (Open ended) ● Yes ● No ● Not sure

20. Please describe the knowledge you gained from any other source we have not mentioned and also the source. (Open ended)

End of Block: 3.1 SOURCES

Start of Block: 3.2 ATTITUDES

Please rate the following statements. **Remember**, **there are no right or wrong answers. It is more helpful for us to hear your honest opinions.** *(Strongly disagree (SD), Disagree (D), Neither agree nor disagree (NAD), Agree (A), Strongly agree (SA))*

SN	Question	SD	D	NAD	A	D
1	I know very little about online fraud					
2	I know very little about how to protect myself against online fraud					
3	I have learned about cybersecurity					
4	I know how to recognize online fraud					
5	I need to learn more about cybersecurity					
6	It is not necessary for me to learn about cybersecurity					
7	I worry about my safety regarding online fraud					
8	I feel safe from online fraud					
9	I am not concerned about my personal cybersecurity					
10	I am confident about protecting myself from online fraud					
11	I want to learn more about cybersecurity					
12	I wish I did not have to learn about online security					
13	I am interested in learning about online fraud					
14	I have no desire to know how to protect myself from online fraud					
15	Individuals are responsible for their safety against online fraud					
16	The government should protect citizens against cyber attacks					
17	Cyber security is a necessary part of life					
18	Ordinary citizens should not be expected to learn about cyber security					
19	Cyber security information is a popular topic					
20	I have never heard about cyber security					
21	I have heard a lot about online fraud					
22	I haven't come across information about online fraud					

End of Block: 3.2 ATTITUDES

Start of Block: 4. TECHNOLOGY USAGE QUESTIONS

1. Do you own or have access to a mobile phone? ● Yes ● No

2. How often do you use a mobile phone?
● Daily ● Weekly ● Monthly ● Yearly ● Less often ● Never

3. The mobile phone I use is shared with others. ● Yes ● No

4. Do you own or have access to a personal computer? ● Yes ● No

5. How often do you use a personal computer?
● Daily ● Weekly ● Monthly ● Yearly ● Less often ● Never

6. The personal computer I use is shared with others. ● Yes ● No

7. Do you own or have access to a tablet? ● Yes ● No

8. Tablet usage How often do you use a tablet?
● Daily ● Weekly ● Monthly ● Yearly ● Less often ● Never

Tabled sharing The tablet I use is shared with others. ● Yes ● No

9. How often do you use the internet?
● Daily ● Weekly ● Monthly ● Yearly ● Less often ● Never

10. How often do you use public Wi-Fi networks? (for example at a coffee shop, restaurants)
● Daily ● Weekly ● Monthly ● Yearly ● Less often ● Never

11. How often do you use personal or professional email?
● Daily ● Weekly ● Monthly ● Yearly ● Less often ● Never

12. How often do you use messaging apps?
● Daily ● Weekly ● Monthly ● Yearly ● Less often ● Never

13. How often do you use social media?
● Daily ● Weekly ● Monthly ● Yearly ● Less often ● Never

14. Do you use online banking platform(s), for example bank transactions via your bank's website, mobile app, other?
● Daily ● Weekly ● Monthly ● Yearly ● Less often ● Never

15. Do you use e-commerce platforms for online shopping?
● Daily ● Weekly ● Monthly ● Yearly ● Less often ● Never

16. How often do you use media streaming platforms (for example YouTube, Netflix, TikTok)?
● Daily ● Weekly ● Monthly ● Yearly ● Less often ● Never

End of Block: 4. TECHNOLOGY USAGE QUESTIONS

Start of Block: 5. "GO-TO" SECURITY PERSON

1. Do you have anyone you trust to help you with personal cybersecurity? For example someone you go to for IT help or advice. ● Yes ● No ● Not sure

2. Go to expertise Does the person you trust for cyber security work as an IT expert or have an IT related qualification? ● Yes ● No ● Not sure

3. How often do you go to this person?
● Daily ● Weekly ● Monthly ● Yearly ● Less often ● Never

4. Describe situations where you have asked the person for help. (Open ended)

End of Block: 5. "GO-TO" SECURITY PERSON

Start of Block: 6. Pew Questions & Others

1. PEW 1 What does the "https://" at the beginning of a URL denote, as opposed to http:// (without the "s")?

- That information entered into the site is encrypted
- That the site has special high definition
- That the site is the newest version available
- That the site is not accessible to certain computers
- None of the above
- Not sure

2. PEW 2 Which of the following is an example of a "phishing" attack? (Select all that apply)

- Sending someone an email that contains a malicious link that is disguised to look like an email from someone the person knows
- Creating a fake website that looks nearly identical to a real website, in order to trick users into entering their login information
- Sending someone a text message that contains a malicious link that is disguised to look like a notification that the person has won a contest
- All of the above
- Not sure

3. PEW 4 All Wi-Fi traffic is encrypted by default on all wireless routers.

- True
- False
- Not sure

4. PEW 5 Some websites and online services use a security process called two-step authentication. Which of the following images is an example of two-step authentication?

- A
- B
- C
- D
- Not sure
- None of these

05. PEW 6 Which of the following four passwords is the most secure?

- WTh!5Z
- into*48
- Boat123
- 123456
- Not sure

6. PEW 7 Criminals access someone's computer and encrypt the user's personal files and data. The user is unable to access this data unless they pay the criminals to decrypt the files. This practice is called….

- Ransomware
- Spam
- A botnet
- Driving
- Not sure

7. PEW 11 All email is encrypted by default.

- True
- False
- Not sure

Correct answers are highlighted in yellow. Each question correctly answered was considered to be worth 1 point yielding a range of 0 to 7 possible scores per participant with higher scores indicating greater objective knowledge on tested cybersecurity concepts.

End of Block: 6. Pew Questions & Others

Start of Block: 7. SeBIS

Please rate the following statements. Remember, there are no right or wrong answers. It is more helpful for us to hear your honest opinions. (Possible responses: Strongly disagree (SD), Disagree (D), Neither agree nor disagree (NAD), Agree (A), Strongly agree (SA)). We used conventional Likert scales to gain finer detail rather than the distinct scales in the original instruments.

1. F1 When I'm prompted about a software update, I install it right away.
2. F2 I try to make sure that the programs I use are up-to-date.
3. F3 I manually lock my computer screen when I step away from it.
4. F4 I set my computer screen to automatically lock if I don't use it for a prolonged period of time.
5. F5 I use a PIN or passcode to unlock my mobile phone.
6. F6 I use a password/passcode to unlock my laptop or tablet.
7. F7 (R) If I discover a security problem, I continue what I was doing because I assume someone else will fix it.
8. F8 (R) When someone sends me a link, I open it without first verifying where it goes.
9. F9 I verify that my anti-virus software has been regularly updating itself.
10. F10 (R) When browsing websites, I mouseover links to see where they go, before clicking them.
11. F11 (R) I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.
12. F12(R) I do not change my passwords, unless I have to.
13. F13 I use different passwords for different accounts that I have.
14. F14 When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.
15. F15 (R) I do not include special characters in my password if it's not required.
16. F16 (R) I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).

Each of the questions was answered on a scale from 1 to 5, for each participant we added them up to obtain the Sebis scores (reversing the scale for the questions marked R).

End of Block: 7. SeBIS

Start of Block: 8. GSE

GSE Please rate the following statements. Remember, there are no right or wrong answers. It is more helpful for us to hear your honest opinions. *(Possible responses: Strongly disagree (SD), Disagree (D), Somewhat disagree (SWD), Neither agree nor disagree (NAD), Somewhat agree (SWA), Agree (A), Strongly agree (SA))*. We used conventional Likert scales to gain finer detail rather than the distinct scales in the original instruments.

1. If I face a cybersecurity threat, I can find the means and ways to deal with it.
2. It is easy for me to stick to my aims and accomplish my goals without being affected by cybersecurity issues.
3. I am confident that I could deal efficiently with unexpected cybersecurity events.
4. Thanks to my resourcefulness, I know how to handle unforeseen cybersecurity situations.
5. I can solve most cybersecurity problems if I invest the necessary effort.
6. I can remain calm when facing cybersecurity difficulties because I can rely on my coping abilities.
7. When I am confronted with a cybersecurity problem, I can usually find several solutions.
8. If I am in cybersecurity trouble, I can usually think of a solution.
9. I can usually handle whatever cybersecurity challenge comes my way.
10. I can always manage to solve difficult cybersecurity problems if I try hard enough.

The scale consists of ten questions, using a 7-point scale, and resulting in a composite GSE score of 10 to 70. Higher scores indicating greater self-efficacy in cybersecurity.

End of Block: 8. GSE

Start of Block: 9. DEMOGRAPHICS

In which country do you currently reside?

What is your gender?

- Man
- Woman
- Non-binary / third gender
- Prefer not to say

Which ethnic group do you belong to?

Please specify: _____

What is your highest level of education completed?

- Less than high school
- High school diploma/GED
- Some college or vocational training
- Bachelor's degree
- Master's degree
- Doctoral degree
- Other. Please describe: _____

What is your current employment status?

- Employed full-time
- Employed part-time
- Self-employed
- Unemployed
- Retired
- Other. Please specify: _____

In which sector(s) do you currently work? _____

What is your job title/role? _____

What is your annual household income?

- Less than $25,000
- $25,000 - $49,999
- $50,000 - $74,999
- $75,000 - $99,999
- $100,000 - $149,999
- $150,000 or more
- Prefer not to say

Are you a student? (If yes, please indicate your course of study.)

● No ● Yes Course of study _____.

What is your age?

- 16-24 years old
- 25-34 years old
- 35-44 years old
- 45-54 years old
- 55-64 years old
- 65-74 years old
- 75 years or older

End of Block: 9. DEMOGRAPHICS

Start of Block: 10. FOLLOW UP / COURSE CREDIT / RAFFLE DRAW

Follow Up Thank you for completing the survey. Your answers will remain anonymous. Select 'Yes' to go to another survey to receive course credit for participating (XXXX / XXXX), and where you can opt in to participating in the raffle draw or future research.

● Yes ● No

End of Block: 10. FOLLOW UP / COURSE CREDIT / RAFFLE DRAW