




Cybersecurity awareness among accounting students at a South African public university

**Authors:**Pranisha Rama¹ Ben Marx¹ Rozanne Smith¹ **Affiliations:**

¹Department of Accounting,
College of Business and
Economics, University of
Johannesburg, Johannesburg,
South Africa

Corresponding author:

Pranisha Rama,
pranishar@uj.ac.za

Dates:

Received: 07 Oct. 2024

Accepted: 08 Apr. 2025

Published: 20 June 2025

How to cite this article:

Rama, P., Marx, B. & Smith, R.,
2025, 'Cybersecurity
awareness among accounting
students at a South African
public university', *South
African Journal of
Information Management*
27(1), a1948. [https://doi.org/
10.4102/sajim.v27i1.1948](https://doi.org/10.4102/sajim.v27i1.1948)

Copyright:

© 2025. The Authors.
Licensee: AOSIS. This work
is licensed under the
Creative Commons
Attribution License.

Background: Cybersecurity awareness at universities is increasingly becoming a critical concern, as educational institutions are prime targets for cyberattacks. that is pertinent globally but specifically in South Africa, where universities have experienced a notable rise in cybersecurity threats and attacks.

Objectives: This study aims to understand how accounting students handle cybersecurity challenges and identify areas where education can be enhanced to better equip students for the digital age.

Method: A mixed-methods approach was employed to assess the current state of cybersecurity awareness among accounting students, utilising questionnaires with both open- and close-ended questions.

Results: The findings indicate that accounting students exhibit different levels of cybersecurity awareness, with some demonstrating strong knowledge of cyber risks and protective measures, while others show significant gaps in understanding and practice. While there is a clear understanding of common phishing signs and good cyber hygiene practices, awareness of advanced threats and social engineering tactics still needs to be improved. The variability in students' ability to identify fake phishing invoices and suspicious LinkedIn requests highlights areas in need of increased cybersecurity awareness.

Conclusion: The results of this study underscore the necessity for enhanced and focused cybersecurity awareness education and training programmes within university curricula to better prepare students for the evolving cyber threat landscape.

Contribution: Cybersecurity awareness education fosters cybersecurity consciousness among the accounting workforce, which is essential for navigating the digital economy and preparing accounting students for this transition. This transition contributes to curriculum development in cybersecurity awareness education in the Fourth Industrial Revolution (4IR) era.

Keywords: cybersecurity; cybersecurity awareness; cybersecurity education; cyber threats; accounting education; accounting students; accounting professionals.

Introduction

The intensifying scale of global cybercrime, characterised by more sophisticated attacks and widespread data breaches, has made cybersecurity awareness an increasingly critical and topical issue across industries and sectors worldwide (Kritzinger 2017; Yusif, Hafeez-Baig & Anachanser 2024). In a world where evolving technology is the new normal, it has become even more difficult for organisations to make users aware of emerging risks as cybersecurity risk escalates (Fouad 2024). This highlights the importance of organisations implementing cybersecurity awareness initiatives for individual cyber users working within the organisations. Emerging technologies such as artificial intelligence (AI), machine learning, cloud computing, big data and the Internet of Things (IoT) continue to grow and will revolutionise the way organisations manage risks within the business (Moallem 2019).

The education sector is ranked among the highest in cyber risk globally and in South Africa (Shava 2022), and at present, universities are faced with the most significant number of cyberattacks within the education sector (Hart et al. 2020; Taha & Dahabiyeh 2021). This is because, to a cybercriminal, sensitive research data, intellectual property and the banking details of thousands of both staff and students are considered valuable. Consequently, universities continue to see increased cyberattacks (Ulven & Wangen 2021). In South Africa, the University of Mpumalanga and the Tshwane University of Technology (TUT) became the most recent cyberattack targets,

Read online:

Scan this QR
code with your
smart phone or
mobile device
to read online.

impacting compromised, sensitive data (Govender 2024; Mungadze 2021).

While many students are at risk of being targets of cyberattacks, accounting students are also faced with large amounts of valuable data based on their future profession (Roohani & Zheng 2019). Accounting professionals are regarded as custodians of financial data, which represents a highly valuable asset and a frequent target for cybercriminals. Accordingly, accounting professionals are often seen to be at higher risk of being hacked (Von Solms & Langerman 2020). The accounting profession is evolving in its role and is now required to adapt to the ever-changing IT landscape; as such, accounting professionals primarily handle sensitive financial data, making them prime targets for phishing scams, malware infections and ransomware attacks (Richardson 2020). While it is essential to enhance accounting students' technical knowledge of cybersecurity, it is equally important to provide practical education on the specific threats they may encounter, ensuring they are prepared to address real-world cybersecurity challenges (Dewu & Barghathi 2019). Accounting professionals are expected to have technical and analytical skills encompassed in the speciality area of cybersecurity, which consists of both technical and analytical skills (Berikol & Killi 2021), and are further required to be aware of cybersecurity threats, such as phishing, malware and ransomware so that they can protect themselves and act as the human firewall (Ulven & Wangen 2021).

Despite the increasing frequency and severity of cyberattacks, particularly in the education sector and among accounting professionals, there is a lack of adequate cybersecurity awareness and training tailored to accounting students (Boss, Gray & Janvrin 2022). This gap in awareness poses a significant risk, as accounting students handle sensitive financial data that are highly attractive to cybercriminals. Threats such as phishing, malware and ransomware exploit this vulnerability, potentially leading to financial fraud and data breaches. Thus, this research article aims to assess cybersecurity awareness among accounting students at a South African public university, specifically regarding these threats, and to identify gaps that can be addressed within the accounting curriculum.

The study differed from prior South African research that focused on cybersecurity awareness in developing countries (Chang & Coppel 2020) and cyber awareness at private tertiary institutions (Chandarman & Van Niekerk 2017). Other studies in South Africa have focused explicitly on cyber initiatives (Mashiane, Dlamini & Mahlangu 2019) and cybersecurity as an emerging challenge to the national security information of small organisations (Broeders 2021). Thus, to the researchers' best knowledge, this is the first study addressing cybersecurity awareness focusing on accounting students at a South African public university.

The remainder of the article is organised as follows: the following section broadly describes the theoretical

frameworks used for this article; after that, the literature review and different types of threats are discussed. The research methodology is then explained, followed by a discussion of the results of cybersecurity awareness among accounting students. The final section, wherein the contribution to knowledge is discussed, along with areas for improvement, limitations of the study and suggestions for future research, concludes the article.

Theoretical framework: The theory of planned behaviour

Cybersecurity awareness consists of two elements, which are: one, knowledge transferred on cybersecurity threats, and two, behaviour with such cyber awareness (Aljniebi 2020). An organisation must be responsible for the knowledge transfer of cyber threats, which is necessary to drive the required behaviour towards cybersecurity (Kovacevic, Putnik & Toskovic 2020). Furthermore, understanding the factors that influence online behaviour is essential for developing effective and cohesive cybersecurity awareness education. The theory of planned behaviour (TPB) is the theoretical framework guiding this study.

When successfully implementing technology, the fundamental aspects are driven by the actual technology and people (Farooq, Ndiege & Isoaho 2019). Prediction of the end user's behaviour is vital in implementing successful technology. Once an end user's attitude is clearly understood, awareness programmes can be designed appropriately (Furnell & Vasileiou 2017). Cybersecurity awareness is driven by behaviour; thus, the TPB is considered an appropriate theory for this study. The TPB is considered one of the most influential theories in driving behaviour (Hina & Dominic 2020). The TPB has also been proven to be one of the most influential theories on security compliance. The TPB is driven by the user's attitude towards cybersecurity. According to Mahabi (2010), attitude is the fundamental aspect that drives an individual's behaviour to be ethical or unethical; therefore, understanding attitude will indicate a further understanding of the drivers behind ethical behaviour. The TPB thus helps in gaining insight into which factors influence attitude and how this impacts cybersecurity awareness (Burns & Roberts 2013). The purpose of awareness presentations is to focus attention on security (Bongiovanni, Renaud & Cairns 2020). Awareness allows individuals to recognise IT security concerns and respond accordingly (Wilson & Hash 2003). Based on this explanation, it can be concluded that making individuals aware of cyber risks is one aspect, but behaviour needs to be driven accordingly (Bongiovanni et al. 2020). Most organisations develop cybersecurity campaigns to communicate envisioned threats and risks to employees and set standards for how employees should behave in a cyber environment. However, organisations must understand the human behavioural factors within cybersecurity management to ensure success (Von Solms & Langerman 2020). Within this study, the aim is to identify how accounting students respond to cybersecurity

awareness, which then provides a basis of items to be included in an accounting curriculum. The TPB is considered highly appropriate for this study as it helps to predict and understand how attitudes, perceived control and social influences shape cybersecurity awareness and behaviour among accounting students, driving the effectiveness of awareness initiatives.

Literature review

Cybersecurity awareness

With the increasing emphasis on cybersecurity awareness, the National Institute of Standards and Technology (NIST) framework also includes cybersecurity awareness of threats and related training as a core focus area (NIST 2020). Kortjan and Von Solms (2014) explain that universities must train individuals for their professional careers, which are now driven by technology. Meyer (2021) acknowledges that accounting curricula do not currently include cybersecurity awareness as part of their offerings. They further contend that while accounting programmes are beginning to include information technology (IT) as part of the curricula, and students are becoming more technologically informed, this does not mean that students know how to protect their data or how to respond to cybersecurity threats.

In a study on cyber awareness conducted by Slusky and Partow-Navid (2012) among accounting students at the California State University, it was found that although the majority of the users were able to gain knowledge from cyber awareness training, they mostly viewed cyber awareness training as a mere tick-box exercise and were not able to apply the knowledge gained to real-life situations. The study further states that a user's attitude needs to be understood in order to provide an effective training programme on cyber awareness. In another study by Al-Janabi and Al-Shourbaji (2016) at a university in the Middle East, it was found that users within a university environment did not have the required knowledge, training and understanding of cyber awareness and therefore were not able to apply cybersecurity awareness and its practical application in their day-to-day work. Senthilkumar and Easwaramoorthy (2017) conducted a study on cyber awareness among five hundred accounting student users in five various colleges in Tamil Nadu (a state in India), and it was found that many users were dependent on antivirus, which was programmed into a system, rather than being aware of cyber threats. The study found that users did not view cyber awareness as important and, therefore, were not able to identify a phishing email. Kirwan, Fullwood and Rooney (2018) conducted a cyber awareness study among 295 Malaysian university students and found that these students did not have any awareness of cyber threats and furthermore were not able to identify any suspicious links. A third of the students in the sample indicated that they did not consider browsing safe while browsing on social media sites. These studies illustrate the importance of cybersecurity awareness among students and in particular among accounting students.

Cybersecurity awareness for accounting students

While accounting curricula have traditionally focused on integrating ethics, digitisation and various technologies, decision-making and even strategy management, it is as essential to expose accounting students to cybersecurity (Rikhardsson & Yigitbasioglu 2018). Textbooks used in the accounting curriculum may include a basic level of information on cybersecurity, but accounting students need to gain a more in-depth understanding of cybersecurity, prompting questions like, 'How do cybersecurity threats work?' 'What specific actions can be taken to mitigate cybersecurity threats?' (Roohani & Zheng 2019:114). Although current textbooks may offer a basic introduction to cybersecurity, there is a growing demand among accounting students for a deeper understanding of how cybersecurity threats operate and the specific actions that can be taken to mitigate these risks. This includes cybersecurity governance, assessing cybersecurity risk and learning about controls that will mitigate such risks (Poongodi, Hamdi & Wang 2023). Addressing this need better equips future accounting professionals to navigate the complexities of the digital landscape and enhances their ability to safeguard their organisations against cybersecurity threats.

In a study conducted by Jackson, Michelson and Munir (2023) focusing on how universities, employing organisations and professional associations are preparing early-career accountants for new technology, it was found that universities can better prepare students for emerging technology, including cybersecurity. This study further emphasises that preparing accounting students adequately for market demands is crucial, and that universities play a critical role in developing education to adapt to such market demands (Jackson et al. 2023). Universities can provide students with cybersecurity acumen, emphasising that students and academics must improve their technological knowledge, which will result in more efficient accounting practices within the accounting curriculum. This study explores the impact of emerging technology on the future accountant in the cybersecurity space. Universities must adapt their curricula to an ever-changing technological landscape, better prepare students for what the employment market requires and improve their knowledge of technology such as cybersecurity (Zhang et al. 2020).

When a curriculum considers cybersecurity as part of its offering, educating accounting students on cybersecurity threats and risks ensures that accounting students are equipped with the relevant knowledge required to manage cybersecurity challenges that organisations face and therefore meet employer expectations (Fakoya-Michael & Fakoya 2020). Zhang et al. (2020) argue that failure to address areas such as cybersecurity in the accounting curriculum reduces the employability and work readiness of accounting graduates. Gulin, Hladika and Valenta (2019) conducted a study that analysed the challenges that digitalisation brings for the accounting profession, and it was found that such

challenges require universities to change and modify their education programmes to prepare accounting students for work in the modern environment, which is automated and digitised. Including cybersecurity in the accounting curriculum ensures that students gain the knowledge to manage cybersecurity challenges and meet employer expectations (Gyekye & Amo 2024). Furthermore, as digitalisation continues to transform the accounting profession, universities must update their programmes to prepare students for the evolving demands of a modern, automated and digitised work environment.

The approach towards cybersecurity education development should not just be a textbook approach that provides an overview of cybersecurity. It should also be able to provide students with details about cybersecurity threats so that they can identify such threats (Henderson, Lapke & Garcia 2016). Accounting curricula provide students with a strong theoretical background to core modules. However, this approach is changing as the world advances towards a technological future, and cybersecurity awareness is one area that will assist students in navigating the technological future (Meyer 2021). Accounting students must learn cybersecurity assurance and awareness of cybersecurity threats (Roohani & Zheng 2019).

User understanding of privacy and security risks is fundamental as technology continues to accelerate at a rapid rate (Ulven & Wangen 2021). Many organisations rely on technology to conduct their business, and accounting professionals must adapt to this technology to ensure effective business activities. Although IT departments contribute to the solution, the impact permeates the entire organisation, necessitating user awareness of cybersecurity threats. In the event of a cyberattack, a business may not be able to conduct operations, which adversely impacts the financial and reputational standing of the organisation.

Grégoire, Salle and Tripp (2015) found that any failures in a technology chain can lead to brand damage in several ways. An organisation with a website that goes down can result in dissatisfied customers, ultimately resulting in a loss of revenue. This study focused on the impact of failures such as technology, and the effect it has on customers, particularly if taken to social media platforms. Understanding threats is thus important in creating mitigation strategies (Grégoire et al. 2015). Organisations face cybersecurity threats through email, websites, e-commerce and even apps, because of the use of digitisation within an organisation (Jawaid 2022). Hackers are now focusing on manipulating employees into divulging information through technology.

User information, such as identity numbers, personal cell phone numbers, financial data and even banking information, is all subject to a security breach in the form of a cyberattack. Common cybersecurity threats that accounting professionals need to become aware of are phishing, malware and ransomware, with ransomware emanating from phishing and malware (Rama 2016). This is supported by Ngoma (2019),

who stated that phishing, malware and ransomware are on the rise, and that users are most vulnerable to these threats. Ngoma's study focused on the impact of cybersecurity threats and the consequences of these threats on the economy. Accounting students must be educated on cybersecurity threats to be able to identify these threats. In the event of a security breach emanating from cybersecurity threats, what the end user does to protect the data comes down to the awareness and knowledge of cybersecurity (Furnell & Vasileiou 2017). Therefore, cybersecurity awareness is vital in protecting an organisation's IT infrastructure by educating users on safe cyber practices in identifying cybersecurity threats.

Accounting students are required to understand cybersecurity threats to protect the university network, to develop life skills in protecting their personal data and to prepare for their future careers (Stanciu & Tincea 2016). With the lack of cybersecurity awareness around cybersecurity threats, cybersecurity awareness must be built into the accounting curriculum. Boss et al. (2020) state that:

Awareness of cybersecurity as an important topic in the context of practice will produce better informed professionals. (p. 30)

This emphasises the need to provide students with education about cybersecurity threats, including phishing, malware and ransomware, among others. This study focuses on cybersecurity threats such as phishing, malware and ransomware that are highly relevant to accounting students and is noted as a limitation. Accounting students must be equipped with cybersecurity knowledge because financial data is a prime target for cybercriminals. As future custodians of sensitive financial information, they will need to recognise and mitigate threats like phishing, which will lead to malware and ransomware and can cause financial fraud, data breaches and reputational damage for organisations (Thomas 2018).

Phishing

Phishing is the practice of sending unwanted email communications while pretending to be a reputable company. It is also a type of spam attack in which data such as usernames, passwords and credit card numbers are requested by a con artist, typically a hacker (or phisher) posing as a trustworthy organisation (Alabdian 2020). This is emphasised by Ibinaie (2019), who describes phishing as one of the most serious problems that has victimised many Internet users. Phishing refers to a social engineering attack in which a phisher attempts to trick users into divulging sensitive information by pretending to be a reputable organisation using an automated method (Ibinaie 2019). The attacker hopes that the target will believe the message and divulge the victim's sensitive information. In recent years, phishing attacks have affected organisations in all sectors (Chanti & Chithralekha 2022). Ninety-four per cent of organisations have reported being impacted by phishing attacks (Al-Qahtani & Cresci 2022). As a result of a widespread lack of awareness, phishing attacks are common. Phishing leads to catastrophic financial losses and data breaches (Rajitha & Priya 2022). Common phishing signs include non-

personalised greetings, urgent or threatening language, URLs that do not match and are not secure, poor grammar or misspellings, subject matter that does not relate to you and requests for personal information (Rama 2016). While these signs are relevant currently, phishing is expected to become more sophisticated.

Malware

Malware is an abbreviated term for malicious software (Somya, Bansal & Ahmad 2016). Atanassov and Chowdhury (2021) warn users that malware is a software that unknowingly infiltrates the computer system and is written with malicious intent; thus, it intrudes into a system or a service with the intent of changing how it usually behaves, such as by allowing unauthorised access, restricting computer resources or disclosing sensitive data (Atanassov & Chowdhury 2021).

Ransomware

Ransomware is a serious threat and has only worsened in recent years, causing enormous financial damage (Hart 2022). As hackers adopt increasingly complex methods of encrypting data and extorting businesses, ransomware has increased. Ransomware is a type of malware that can be formatted by holding specific files hostage until a fee or ransom is paid (Yuste & Pastrana 2021). Ransomware also has the potential to affect business continuity, resulting in financial losses and reputational damage should the hacker expose the information without the custodian's consent (Bouveret 2018; Chandrasena 2022).

Research methodology

This study employs a mixed-methods approach (qualitative and quantitative data) to data collection (Harrison III 2013). A mixed-method research approach, combining open- and closed-ended questions, provides both quantifiable data for statistical analysis and deeper insights into attitudes and behaviours, enhancing the validity and richness of research findings. A questionnaire, consisting of open-ended and closed-ended questions, was developed from existing literature. The questionnaire was split into two main sections: perceptions of cybersecurity and statements around general awareness of cybersecurity threats. Subsequently, students were presented with five different images and were required to identify the legitimacy of each of the images presented. Image one was a phishing email from the university (Figure 1); image two was a fictitious LinkedIn request (Figure 2); image three was a legitimate university login page (Figure 3) and the last two images were invoices, where invoice one was a phishing invoice (Figure 4), and invoice two was legitimate (Figure 5). Where images consisted of warning signs, these included fake links, urgent requests, etc. The details of the selected university have been removed for ethical purposes based on the ethical clearance received for this study.

The open-ended questions focused on obtaining comments from participants, and the close-ended questions used a

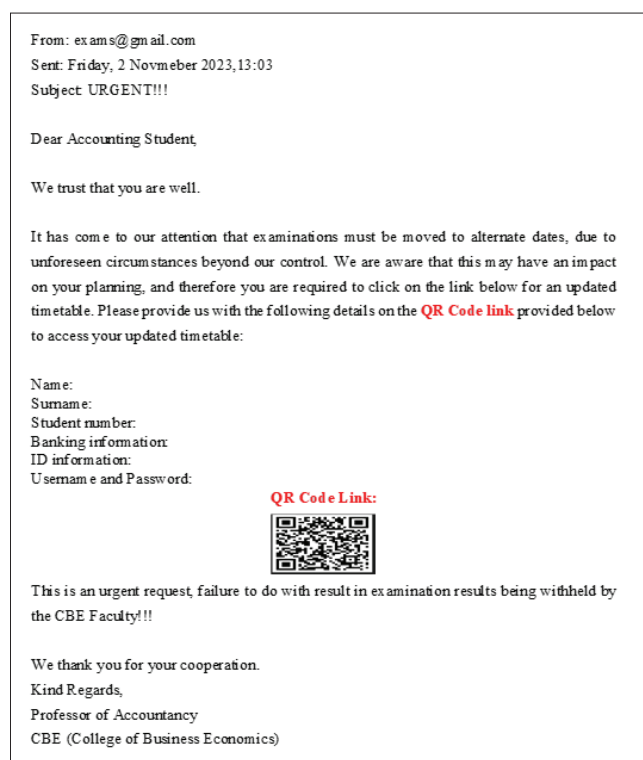


FIGURE 1: Phishing email.

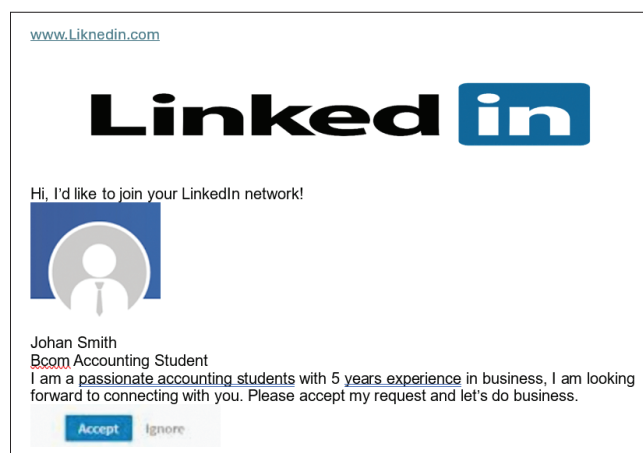


FIGURE 2: LinkedIn request.

Likert scale of 1–5 ('1. = strongly disagree, 2. = disagree, 3. = neither agree nor disagree, 4. = agree, 5. = strongly agree'), as well as yes or no questions. Students were presented with various statements about cybersecurity awareness and were required to select the most appropriate response using the Likert scale and yes or no responses where applicable. The yes or no questions were used in instances where students were required to identify whether a particular image was phishing or not. A Likert scale, in this case, would distort the student's response, and a true reflection of the awareness would not be obtained – hence the yes or no option.

The data were collected using Google Forms, and 415 usable responses were received from final-year (third-year) accounting students at a South African public university.

FIGURE 3: Login page.

Source: Chhay, A., 2022, *Fake invoice phishing scams*, Information Technology, viewed 03 September 2024, from <https://it.lbl.gov/fake-invoice-phishing-scams/>.

FIGURE 4: Phishing invoice.

These students were selected for their experience gained over a 3-year curriculum. Quantitative data were received from the Likert scale, and qualitative data were received from the comments posed by students who completed the questionnaire. Statistical Package for the Social Sciences (SPSS) was used for the analysis of quantitative data. Comments provide qualitative data that can give deeper

Source: Frevvo, 2021, *Purchase orders vs invoices – what you need to know*, Procurement Automation, viewed 26 March 2025, from <https://www.frevvo.com/purchase-order-workflows>.

FIGURE 5: Legitimate invoice.

insights into participants' thoughts, feelings and experiences, which may not be captured by quantitative measures alone and help contextualise the quantitative data, providing background and reasons behind the numerical responses (Sutton & Austin 2015).

Cronbach's alpha was used to measure reliability. This measurement indicates consistency in how participants would have answered a questionnaire. Cronbach's alpha ranges from 0 to 1, with higher values denoting higher internal consistency, where a reliable measure of anything above 0.7 is considered acceptable (Kennedy 2022). A standard deviation (SD) is a measure of how dispersed the data is from the mean, and an acceptable number is no more than 2. It is commonly assumed by statisticians that 68% of all data points will be within ± 1 SD from the mean and 95% of all data points will be within ± 2 SD from the mean (Sheats & Pankratz 2002).

The findings are displayed in Table 1, Table 2, Table 3, Table 4, Table 5, Table 6 and Table 7 and are tabulated according to the order in which the questions were presented to the students in the questionnaire. The various tables use the mean and SD as a display method. The SD obtained for all findings was within an acceptable range and therefore was accepted in all cases.

Ethical considerations

Ethical clearance to conduct this study was obtained from the University of Johannesburg School of Accounting Research Ethics Committee (SAREC20240222/01).

Results

The detailed Results are discussed below.

Perceptions on cybersecurity

The objective of this section is to establish cybersecurity perceptions among accounting students.

Results in Table 1 provide the findings on perceptions of cybersecurity awareness. For this section, a Cronbach's alpha of 0.708 was achieved, indicating that the results are reliable.

It is positive to note that students view the importance of protecting their personal devices (4.64), which is closely linked to students seeing the importance of using cybersecurity in their daily lives (4.35). This is followed by students indicating an understanding of the concept of cybersecurity (4.09). These items ranked as the top three, indicating that students agree to have an understanding of cybersecurity. Students were also asked if they had experienced a cyber breach (2.28); the lower mean with a higher SD would be expected, as not every student would have been exposed to a breach. While this lower mean is expected, it still indicates that cybersecurity threats target these students. Questions on the breach were posed to students and are discussed below. It is important for accounting students to gain an understanding of cybersecurity, for them to identify cybersecurity threats (Rama 2016). These questions related to a student's personal encounter with cybersecurity, which impacts them daily, emphasise the need for cybersecurity awareness.

While accounting students show some level of understanding, the areas of concern are the limited inclusion of cybersecurity within the accounting curriculum (3.36), and students indicating that they do not know how to protect their data (3.93). These two aspects are closely linked; hence, should cybersecurity be included in the accounting curriculum, students will know how to protect themselves better (Boss et al. 2022). This concurs with literature indicating that accounting curricula have limited to no inclusion of cybersecurity (Meyer 2021). Teaching students how to protect their personal data (email, banking information, safe browsing, etc.) should be seen as a life skill, thus emphasising the importance of teaching students about cybersecurity (Birt, Safari & De Castro 2023).

TABLE 1: Perceptions of cybersecurity awareness.

Perception	Mean	SD
I am aware of the concept of cybersecurity	4.09	0.98
The university includes cybersecurity as part of the accounting curriculum	3.36	1.11
I understand the importance of protecting my own personal data (ID number, cell phone number, personal details)	4.64	0.86
I understand how to protect my data	3.93	1.01
I have experienced a breach (provide details in the comments box below)	2.28	1.22
Cybersecurity is important in my day-to-day activities (e.g. while using my cell phone, laptop, browsing the internet, etc.)	4.35	0.98

SD, standard deviation; ID, identity number.

Students were asked to comment on their perceptions of cybersecurity. The comments generated attest to and correlate with the quantitative findings, indicating that students see the importance of cybersecurity, with students being able to identify risks that organisations face because of cybersecurity threats. This is vital to protect sensitive data. Some of the students' comments are indicated below (To ensure participant confidentiality, only participant codes were used within this article):

'Cybersecurity can affect anyone at any time so the need to ensure awareness on cybersecurity is vital to all mobile device users. Certain prevention elements of cybersecurity are not firm or strong enough to handle certain dangers such as hacking of computers as the user may be hacked unknowingly. Therefore, there are some vague prevention and security implementation procedures that hold no strength amongst possible breaches of cybersecurity.' (Participant 1)

'A lot of education still needs to be done with regards to cybersecurity so that people are more aware of the risks and what controls to put in place. For instance, I now have enabled two factor authentication on my social media accounts to avoid someone accessing my account without my consent.' (Participant 1)

'I think cybersecurity is very important to learn in the world we live in as more things are moving into the digital world and the introduction of AI having security over your data is very important as it will protect you from a lot of risks and threats. Most of our information is digital and it is important to protect it as damages may be done it land in the wrong hands. Overall I think each and every individual must learn about cybersecurity and how to protect themselves from this.' (Participant 43)

Comments on the breaches students experienced are described below, with comments being generated based on common threats and signs experienced during these breaches. These real-life breaches bring to light the vulnerability of students, who remain a soft target for hackers:

'I experienced a potential security breach through a misleading link that portrayed my bursary scheme credentials to reaffirm my contact details and personal information. Luckily, I identified the link had no correlation to how the bursary scheme usually performs their procedures regarding confirmation of details and as a result I deleted the link before any potential breach.' (Participant 37)

'My student email was ever hacked.' (Participant 129)

'I have had my social media account hacked. I also have received emails and WhatsApp messages from scammers.' (Participant 145)

'I had anonymous numbers sending me messages to update my banking details or pay a certain amount using a link in order to access free delivery of free goods posing as post office [South Africa] SA I did not know this until the Post office SA issued a statement that they are not involved with that.' (Participant 268)

Cybersecurity awareness section

This section aims to establish whether students understand cybersecurity awareness fundamentals and threats and can identify cybersecurity threats. The results of this section are included in Table 2, Table 3, Table 4, Table 5, Table 6 and Table 7. A Cronbach's alpha of 0.891 was obtained, making the results reliable.

TABLE 2: Cybersecurity awareness fundamentals.

Statement	Mean	SD
I understand what a cybersecurity threat is	3.96	0.96
I am familiar with the concept of phishing	3.93	1.16
I am familiar with the concept of malware	3.55	1.24
I am familiar with the concept of ransomware	3.09	1.30
I understand the consequences of a cybersecurity threat	3.90	0.97
I know the signs of phishing emails	3.73	1.17
I know the signs of malware	3.13	1.29

SD, standard deviation.

TABLE 3: Email from university.

Statement	Yes	No	Total
The email above is a legitimate email	38 9.2%	377 90.8%	415 100.0%
I would respond to the email	32 7.7%	383 92.3%	415 100.0%
The link within the email is safe to click on	31 7.5%	384 92.5%	415 100.0%
It is safe to provide the details as requested in the email (name, surname, student number, banking information, username and password)	24 5.8%	391 94.2%	415 100.0%
This is a genuine urgent request as it impacts my exam results	40 9.6%	375 90.4%	415 100.0%

The findings in Table 2 indicate that students understand what a cybersecurity threat is (3.96) and the consequences thereof (3.90). This indicates that students mostly agree with the statements. This is promising, considering that accounting professional bodies require students to understand what a threat is and the consequences thereof (Chartered Institute of Management Accountants [CIMA] 2022); South African Institute of Chartered Accountants [SAICA] 2022). Students rated understanding phishing (3.93) and the applicable signs highly (3.73); this is positive to note, as phishing is one of the most targeted cybersecurity threats and, in many cases, is targeted at students (Atanassov & Chowdhury 2021; Rama 2016).

Lower scores were obtained in understanding the concept of ransomware (3.09), the concept of malware (3.55) and the identification of malware signs (3.13), indicating that students mostly neither agree nor disagree, which alludes to a lack of understanding of these aspects. In many cases, malware can result in a ransomware attack. Thus, users are required to understand these concepts (Bouveret 2018; Chandrasena 2022). While students have indicated some level of understanding around cybersecurity threats, more emphasis must be placed on enhanced cybersecurity awareness (Rama 2016).

Statements around the emails (Table 2) were posed to students to test their response to the legitimacy of the email provided (90% answered correctly), whether a student would respond to the email (92% answered correctly), the safety of the link (93% answered correctly), whether it is safe to provide details per the fake email (94% answered correctly) and the genuineness of the email (90% answered correctly). There are no significant discrepancies noted from these findings. These findings clearly indicate that students can identify phishing signs within an email. The findings indicate that students generally have a high level of awareness and practical skills in identifying various signs of phishing emails.

TABLE 4: LinkedIn request.

Statement	Yes	No	Total
The LinkedIn request is a legitimate request	153 36.9%	262 63.1%	415 100.0%
I would respond to the LinkedIn request	128 30.8%	287 69.2%	415 100.0%
It is safe to accept this LinkedIn request	130 31.3%	285 68.7%	415 100.0%

While students can identify phishing signs, ongoing training and updates on new phishing tactics are essential to maintain and enhance cyber awareness (Rama 2016). Educational institutions should integrate regular cybersecurity awareness education into their curricula to keep students informed about the evolving nature of cyber threats (Furnell & Vasileiou, 2017). These findings emphasise the importance of continuous education on cybersecurity threats.

The findings on the LinkedIn request are presented in Table 4. The LinkedIn request presented to students is perceived to be from a legitimate organisation; however, hackers often use this to scam people into divulging information and may also use it as a platform to infiltrate malware into a user's computer (Alabdan 2020).

The findings in Table 4 indicate that students struggle to identify key signs of fake LinkedIn connection requests. The lower scores across different indicators suggest that students are not fully equipped with the necessary skills to recognise fraudulent LinkedIn invitations. This gap in awareness highlights the need for targeted educational efforts and the inclusion of cybersecurity awareness as part of university curricula.

These findings stress the importance of enhancing educational programmes focused on social media and professional networking security. Universities should consider incorporating specific education on identifying fake profiles and connection requests on platforms like LinkedIn and other social media avenues (Ibinaie 2019). Providing real-life examples and practical exercises on the identification of warning signs could help students develop a more nuanced understanding of the signs of fake LinkedIn requests (Bérubé & Gendron 2022).

The results in Table 5 present findings on the login page. While these are positive to note, concerns remain around students not updating their passwords on a regular basis. Thirty-eight point eight per cent of students do not update their passwords on a regular basis, and this opens up the risk of a cybersecurity threat being deployed (Alabdan 2020). Even though a smaller percentage of students (22.9%) indicated that they had shared their usernames and passwords with a friend or someone they trust, this is concerning, as it opens up the entire network and the user's information to a cybersecurity threat (Gourgiotou 2018).

The findings indicate that students generally have a high level of awareness and practical skills in identifying legitimate login pages. These findings highlight the importance of continuing

TABLE 5: Login page.

Statement	Yes	No	Total
The login page is legitimate	403	12	415
	97.1%	2.9%	100.0%
It is safe to provide my login details (username and password)	399	16	415
	96.1%	3.9%	100.0%
My password is updated on a regular basis	254	161	415
	61.2%	38.8%	100.0%
I have shared my login details with a friend or someone that I trust	95	320	415
	22.9%	77.1%	100.0%

TABLE 6: Invoices.

Statement	Yes	No	Total
Invoice 1 is a legitimate invoice	200	215	415
	48.2%	51.8%	100.0%
Invoice 2 is a legitimate invoice	349	66	415
	84.1%	15.9%	100.0%
It is safe to approve invoice 1	183	232	415
	44.1%	55.9%	100.0%
It is safe to approve invoice 2	340	75	415
	81.9%	18.1%	100.0%

education on cybersecurity threats, particularly those associated with the sharing of passwords and login details. While students can identify legitimate login pages, ongoing education is essential to maintain and enhance their cybersecurity awareness. Universities should integrate regular cyber awareness sessions into their curricula to keep students informed about the evolving nature of cybersecurity threats and the importance of passwords while navigating the cyber landscape (Meyer 2021).

Table 6 presents findings on the invoice images. Students were presented with two invoices. The invoices were selected for this aspect of cybersecurity awareness because accounting students were the main unit of analysis, and, as part of their future careers, they will be required to analyse and work with documents such as invoices. Having the correct level of cybersecurity awareness is thus important in preparing students adequately for their future roles.

Invoice 1 was a fake invoice, and Invoice 2 was a legitimate one. Just over half (51.9%) correctly identified invoice 1. However, it is concerning that almost half of the students were not able to identify this correctly. Invoice 2 showed a better response, with 84.1% of students correctly identifying that the invoice was, in fact, legitimate.

Discussion

The overall findings are tabulated in Table 7. The findings related to the invoices indicate a varying degree of cybersecurity awareness among students, with strong awareness of common phishing signs and good cyber hygiene practices but moderate to low awareness of advanced threats and social engineering tactics. The variability in identifying fake phishing invoices and LinkedIn requests also points to areas for improvement. The TPB suggests that enhancing attitudes towards the importance of recognising advanced threats, increasing

TABLE 7: Overall basis of cyber awareness presented to students.

Image	Correctly identified	Incorrectly identified	Total
1. Email	90.8	9.2	100
2. LinkedIn request	63.1	36.9	100
3. Login page	97.1	2.9	100
4. Invoice 1	51.8	48.2	100
5. Invoice 2	84.1	15.9	100

the emphasis on these issues within students' social environments, and building their confidence in handling such threats could improve their overall cybersecurity awareness and should thus be included in the accounting curriculum accordingly.

These findings highlight the need for comprehensive education on all aspects of cybersecurity, from basic to advanced threats. Universities should tailor their curricula to address the gaps identified, ensuring that students receive targeted training on advanced cyber threats and social engineering tactics. Real-life examples and practical exercises can enhance students' ability to recognise and respond to cybersecurity threats (Roohani & Zheng 2019). The findings from this study compare with previous studies, where similar results were noted – for example, users not being able to apply cybersecurity awareness to real-life and practical situations, as well as clicking on fake links within phishing emails (Al-Janabi & Al-Shourbaji 2016; Kirwan et al. 2018; Senthilkumar & Easwaramoorthy 2017; Slusky & Partow-Navid 2012). Students struggled to identify a phishing email, a fake LinkedIn request and distinguish between two invoices, one legitimate and one fraudulent, similar to those encountered in real-life scenarios.

Recommendations

- Students should be taught about warning signs relating to phishing, malware, ransomware and other cyber threats. This includes recognising suspicious email attachments. Students should be provided with unusual login attempts and unexpected pop-ups that may indicate a security risk.
- Students should be taught about safe password usage, and the importance of passwords includes the importance of strong, unique passwords.
- Students should be provided with education on social engineering and safety practices around cybersecurity, including best practices to verify identities and avoid falling victim to scams.
- Students should be provided with real-life examples through case studies, illustrating the impact of cybersecurity threats. For example, students can analyse fraudulent invoices, phishing emails and identity theft cases to understand how attackers exploit security weaknesses.
- Students should be educated about data-security and the ethical considerations of being aware, focusing on the consequences of data breaches in the accounting and business sectors.

Conclusion

It was established that the present study has provided valuable insights into cybersecurity awareness among accounting students at a South African public university. The findings contribute to the growing body of literature on cybersecurity awareness in higher education, particularly with accounting students. Given the critical role that accounting professionals play in handling sensitive financial data, cybersecurity awareness is essential for their future careers.

The results indicate that, while accounting students show an understanding of specific cybersecurity threats, such as recognising phishing emails, there are notable gaps in their awareness, particularly concerning the cybersecurity warning signs within LinkedIn profiles and invoice areas directly relevant to their professional responsibilities. These findings highlight the need for targeted cybersecurity education programmes specifically designed for accounting students.

To address these gaps, universities should consider integrating cybersecurity awareness into the accounting curriculum, emphasising its importance throughout the qualification. Although curriculum constraints may pose challenges, developing a dedicated cybersecurity course within a learning management system could further enhance students' preparedness.

This study's limitations include its focus on one public university and its being limited to final-year students, as well as addressing only phishing, malware and ransomware. Future research should expand to other South African universities, allowing for a comparative analysis of cybersecurity awareness levels across different institutions and expanding the research scope to other threats. Such research could provide a more comprehensive understanding of cybersecurity awareness among accounting students in the country, informing more effective educational strategies.

Acknowledgements

This article is partially based on the author, P.R.'s PhD dissertation entitled, 'A Case Study of Cybersecurity Education for Accounting Students', toward the degree of PhD Auditing in the Department of Accountancy, University of Johannesburg, South Africa, with supervisors B.M. and R.S.

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Authors' contributions

P.R., B.M. and R.S. contributed to the paper in the writing and final compilation of the article.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability

The data that support the findings of this study are available from the corresponding author, P.R., upon reasonable request.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any agency affiliated with the authors.

References

- Al-Janabi, S. & Al-Shourbaji, I., 2016, 'A study of cyber security awareness in educational environment in the Middle East', *Journal of Information and Knowledge Management* 15(1). <https://doi.org/10.1142/S0219649216500076>
- Al-Qahtani, A.F. & Cresci, S., 2022, 'The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19', *IET Information Security* 16(5), 324–345.
- Alabdan, R., 2020, 'Phishing attacks survey: Types, vectors, and technical approaches', *Future Internet* 12(10), 168. <https://doi.org/10.3390/fi12100168>
- Aljniabi, A., 2020, 'Human behaviour in cyber security', Master's thesis, The British University in Dubai.
- Atanassov, N. & Chowdhury, M.M., 2021, 'Mobile device threat: Malware', in *2021 IEEE international conference on Electro Information Technology (EIT)*, IEEE, May 14–15, Mt. Pleasant, MI, USA, pp. 007–013.
- Berikol, B.Z. & Killi, M., 2021, 'The effects of digital transformation process on accounting profession and accounting education', in K.T. Çaliyurt (ed.), *Ethics and Sustainability in Accounting and Finance, Volume II*, pp. 219–231, Springer Nature, Singapore.
- Bérubé, J. & Gendron, Y., 2022, 'Through students' eyes: Case study of a critical pedagogy initiative in accounting education', *Accounting Education* 31(4), 394–430. <https://doi.org/10.1080/09639284.2021.1997768>
- Birt, J., Safari, M. & De Castro, V.B., 2023, 'Critical analysis of integration of ICT and data analytics into the accounting curriculum: A multidimensional perspective', *Accounting & Finance* 63(4), 4037–4063. <https://doi.org/10.1111/acfi.13084>
- Bongiovanni, I., Renaud, K. & Cairns, G., 2020, 'Securing intellectual capital: An exploratory study in Australian universities', *Journal of Intellectual Capital* 21(3), 481–505. <https://doi.org/10.1108/JIC-08-2019-0197>
- Boss, S.R., Gray, J. & Janvrin, D.J., 2022, 'Accountants, cybersecurity isn't just for "techies": Incorporating cybersecurity into the accounting curriculum', *Issues in Accounting Education* 37(3), 73–89. <https://doi.org/10.2308/ISSUES-2021-001>
- Bouveret, A., 2018, *Cyber risk for the financial sector: A framework for quantitative assessment*, International Monetary Fund, Washington, DC.
- Broeders, D., 2021, 'Private active cyber defense and (international) cyber security – Pushing the line?', *Journal of Cybersecurity* 7(1), tyab010. <https://doi.org/10.1093/cysec/tyab010>
- Burns, S. & Roberts, L., 2013, 'Applying the theory of planned behaviour to predicting online safety behavior', *Crime Prevention and Community Safety* 15(1), 48–64. <https://doi.org/10.1057/cpcs.2012.13>
- Chandarmar, R. & Van Niekerk, B., 2017, 'Students' cybersecurity awareness at a private tertiary educational institution', *African Journal of Information and Communication* 20, 133–155. <https://doi.org/10.23962/10539/23572>
- Chandrasena, S., 2022, 'Data preservation and risk management in management information systems', *South Florida Journal of Development* 3(1), 1459–1479. <https://doi.org/10.46932/sfjdv3n1-112>
- Chang, L.Y. & Coppel, N., 2020, 'Building cyber security awareness in a developing country: Lessons from Myanmar', *Computers & Security* 97, 101959. <https://doi.org/10.1016/j.cose.2020.101959>
- Chanti, S. & Chithralekha, T., 2022, 'A literature review on classification of phishing attacks', *International Journal of Advanced Technology and Engineering Exploration* 9(89), 446–476. <https://doi.org/10.19101/IJATEE.2021.875031>
- Chhay, A., 2022, *Fake invoice phishing scams*, Information Technology, viewed 03 September 2024, from <https://it.lbl.gov/fake-invoice-phishing-scams/>
- CIMA, 2022, *CIMA – CGMA cybersecurity tool*, viewed 12 July 2022, from <https://www.cimaglobal.com/Research-Insight/CGMA-Cybersecurity-Tool/>
- Dewu, K. & Barghathi, Y., 2019, 'The accounting curriculum and the emergence of Big Data', *Accounting & Management Information Systems/Contabilitate Si Informatica de Gestiune* 18(3), 417–442. <https://doi.org/10.24818/jamis.2019.03006>
- Fakoya-Michael, S.A. & Fakoya, M.B., 2020, 'Library usage by university accounting students: A comparison of contact and open distance learning institution in South Africa', *Journal of Academic Librarianship* 46(1), 102093. <https://doi.org/10.1016/j.acalib.2019.102093>
- Farooq, A., Ndiege, J.R.A. & Isoaho, J., 2019, 'Factors affecting security behavior of Kenyan students: An integration of protection motivation theory and theory of planned behavior', in *IEEE AFRICON* 2019, pp. 1–8, Accra, Ghana, September 23–25, IEEE, Piscataway, NJ.

- Fouad, N.S., 2024, 'Cyber biosecurity in the new normal: Cyberbio risks, pre-emptive security, and the global governance of bioinformation', *European Journal of International Security* 9(4), 1–21. <https://doi.org/10.1017/eis.2024.19>
- Frevvo, 2021, *Purchase orders vs invoices – what you need to know*, Procurement Automation, viewed 26 March 2025, from <https://www.frevvo.com/purchase-order-workflows>
- Furnell, S. & Vasileiou, I., 2017, 'Security education and awareness: Just let them burn?', *Network Security* 2017(12), 5–9. [https://doi.org/10.1016/S1353-4858\(17\)30122-8](https://doi.org/10.1016/S1353-4858(17)30122-8)
- Gourgoutou, E., 2018, 'Trainee teachers' collaborative and reflective practicum in kindergarten classrooms in Greece: A case study approach', *Educational Review, USA* 2(1), 117–128. <https://doi.org/10.26855/er.2018.01.001>
- Govender, P., 2024, *Tshwane University of Technology suffered massive data breach after its computer systems were hacked*, viewed 13 September 2024, from <https://www.news24.com/news24/southafrica/news/tshwane-university-of-technology-suffered-massive-data-breach-after-its-computer-systems-were-hacked-20240212>
- Grégoire, Y., Salle, A. & Tripp, T.M., 2015, 'Managing social media crises with your customers: The good, the bad, and the ugly', *Business Horizons* 58(2), 173–182. <https://doi.org/10.1016/j.bushor.2014.11.001>
- Gulin, D., Hladika, M. & Valenta, I., 2019, 'Digitalization and the challenges for the accounting profession', *ENTRENOVA-Enterprise Research Innovation*, 5(1), 428–437.
- Gyekye, K.A. & Amo, O., 2024, 'Quality of accounting graduates and employers' expectations in Ghana', *Journal of International Education in Business* 17(3), 395–415
- Harrison III, R.L., 2013, 'Using mixed methods designs in the Journal of Business Research, 1990–2010', *Journal of Business Research* 66(11), 2153–2162. <https://doi.org/10.1016/j.jbusres.2012.01.006>
- Hart, J., 2022, 'The evolution of ransomware and its impacts on organizations', Master's thesis, Utica University.
- Hart, S., Margheri, A., Paci, F. & Sassone, V., 2020, 'Riskio: A serious game for cyber security awareness and education', *Computers & Security* 95, 101827. <https://doi.org/10.1016/j.cose.2020.101827>
- Henderson, D., Lapke, M. & Garcia, C., 2016, 'SQL injection: A demonstration and implications for accounting students', *AIS Educator Journal* 11(1), 1–8. <https://doi.org/10.3194/1935-8156-11.1.1>
- Hina, S. & Dominic, P.D.D., 2020, 'Information security policies' compliance: A perspective for higher education institutions', *Journal of Computer Information Systems* 60(3), 01–211. <https://doi.org/10.1080/08874417.2018.1432996>
- Ibinaïye, D.D., 2019, 'Identification and classification of phishing websites using machine learning–random forest', Doctoral dissertation, Dublin, National College of Ireland
- Jackson, D., Michelson, G. & Munir, R., 2023, 'Developing accountants for the future: New technology, skills, and the role of stakeholders', *Accounting Education* 32(2), 150–177. <https://doi.org/10.1080/09639284.2022.2057195>
- Jawaid, S., 2022, *Cyber security: etiology and importance*, Preprints, 2022080235..
- Kennedy, I., 2022, 'Sample size determination in test-retest and Cronbach alpha reliability estimates', *British Journal of Contemporary Education* 2(1), 17–29. <https://doi.org/10.52589/BICE-FY266HK9>
- Kirwan, G.H., Fullwood, C. & Rooney, B., 2018, 'Risk factors for social networking site scam victimization among Malaysian students', *Cyberpsychology, Behavior, and Social Networking* 21(2), 123–128. <https://doi.org/10.1089/cyber.2016.0714>
- Kortjan, N. & Von Solms, R., 2014, 'A conceptual framework for cyber security awareness and education in SA', *South African Computer Journal* 52. <https://doi.org/10.18489/SACJ.V52I0.201>
- Kovacevic, A., Putnik, N. & Toskovic, O., 2020, 'Factors related to cyber security behavior', *IEEE Access* 8, 125140–125148. <https://doi.org/10.1109/ACCESS.2020.3007867>
- Kritzinger, E., 2017, 'Growing a cyber-safety culture amongst school learners in South Africa through gaming', *South African Computer Journal* 29(2), 16–35. <https://doi.org/10.18489/sacj.v29i2.471>
- Mahabi, V., 2010, *Information security awareness: System administrators and end-users perspectives at Florida State University*, viewed from <http://diginole.lib.fsu.edu/et>
- Mashiane, T., Dlamini, Z. & Mahlangu, T., 2019, 'A rollout strategy for cybersecurity awareness campaigns', in *Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS 2019)*, February 18–19, 2019, Academic Conferences and Publishing International, Oxford, Stellenbosch, South Africa, pp. 243–250.
- Meyer, C., 2021, *Fit cybersecurity into your accounting courses – Extra credit*, viewed 08 February 2023, from <https://www.journalofaccountancy.com/newsletters/extra-credit/fit-cybersecurity-into-accounting-courses.html>
- Moallem, A., 2019, *Cybersecurity awareness among students and faculty*, CRC Press/Taylor & Francis Group, Boca Raton, FL.
- Mungadze, S., 2021, *University of Mpumalanga thwarts R100m hack attempt*, ITWeb, viewed 27 October 2021, from <https://www.itweb.co.za/content/Kjlyrvw1jmmMk6am>
- National Institute of Standards and Technology (NIST), 2020, *Implementation plan for the NICE strategic plan*, viewed 01 March 2022, from www.nist.gov/nice
- Ngoma, M.L., 2019, 'Cybersecurity awareness in South African public sector organisations', Master's thesis, University of Johannesburg.
- Poongodi, M., Hamdi, M. & Wang, H., 2023, 'Image and audio caps: Automated captioning of background sounds and images using deep learning', *Multimedia Systems* 29(5), 2951–2959. <https://doi.org/10.1007/s00530-022-00902-0>
- Rajitha, M. & Priya, R., 2022, 'A review on cyber threats analysis using data mining techniques—with special reference to phishing attacks', *International Journal of Modern Developments in Engineering and Science* 1(5), 13–14.
- Rama, P., 2016, *An evaluation of information technology security threats: A case study of the University of Johannesburg*, ProQuest, viewed 10 May 2022, from <https://www.proquest.com/openview/992d04d911eb6b89a1429bd448a6ca37/1?pq-origsite=gscholar&cbl=2026366&diss=y>
- Richardson, A.J., 2020, 'Professionalization and intraprofessional competition in the Canadian accounting profession', in G.J. Murphy (ed.), *A history of Canadian accounting thought and practice*, pp. 183–208, Routledge, London.
- Rikhardsson, P. & Yigitbasoglu, O., 2018, 'Business intelligence & analytics in management accounting research: Status and future focus', *International Journal of Accounting Information Systems* 29, 37–58. <https://doi.org/10.1016/j.accinf.2018.03.001>
- Roohani, S.J. & Zheng, X., 2019, 'Using ten teaching modules and recently publicized data-breach cases to integrate cybersecurity into upper-level accounting courses', in T. Calderon (ed.), *Advances in accounting education: Teaching and curriculum innovations*, vol. 23, pp. 113–125, Emerald Publishing Limited, Bingley.
- SAICA, 2022, *CA2025 – CA of the future*, viewed 12 July 2022, from <https://ca2025.co.za/>
- Senthilkumar, K. & Easwaramoorthy, S., 2017, 'A survey on cyber security awareness among college students in Tamil Nadu', *IOP Conference Series: Materials Science and Engineering* 263(4), 042043. <https://doi.org/10.1088/1757-899X/263/4/042043>
- Shava, E., 2022, 'Reinforcing the role of ICT in enhancing teaching and learning post-COVID-19 in tertiary institutions in South Africa', *Journal of Culture and Values in Education* 5(1), 78–91. <https://doi.org/10.46303/jcve.2022.7>
- Sheats, R.D. & Pankratz, V.S., 2002, 'Understanding distributions and data types', *Seminars in Orthodontics* 8(2), 62–66. <https://doi.org/10.1053/sodo.2002.32075>
- Slusky, L. & Partow-Navid, P., 2012, 'Students' information security practices and awareness', *Journal of Information Privacy and Security* 8(4), 3–26. <https://doi.org/10.1080/155356548.2012.10845664>
- Somya, B., Bansal, P. & Ahmad, T., 2016, 'Methods and techniques of intrusion detection: A review', in *International conference on smart trends for information technology and computer communications*, pp. 518–529, Springer, Singapore.
- Stanciu, V. & Tinca, A., 2016, 'Students' awareness on information security between own perception and reality: An empirical study', *Accounting and Management Information Systems* 15(1), 112–130.
- Sutton, J. & Austin, Z., 2015, 'Qualitative research: Data collection, analysis, and management', *Canadian Journal of Hospital Pharmacy* 68(3), 226. <https://doi.org/10.4212/cjhp.v68i3.1456>
- Taha, N. & Dahabiyeh, L., 2021, 'College students' information security awareness: A comparison between smartphones and computers', *Education and Information Technologies* 26(2), 1721–1736. <https://doi.org/10.1007/s10639-020-10330-0>
- Thomas, J., 2018, 'Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks', *International Journal of Business Management* 12(3), 1–23. <https://doi.org/10.5539/ijbm.v13n6p1>
- Ulven, J.B. & Wangen, G., 2021, 'A systematic review of cybersecurity risks in higher education', *Future Internet* 13(2), 39. <https://doi.org/10.3390/fi13020039>
- Von Solms, J. & Langerman, J., 2020, 'Risks and threats arising from the adoption of digital technology in Treasury', in *Information and cyber security: 19th International Conference, ISSA 2020*, Pretoria, South Africa, August 25–26, 2020, pp. 1–19.
- Wilson, M. & Hash, J., 2003, *Building an information technology security awareness and training program*, National Institute of Standards and Technology (NIST), Gaithersburg, MD.
- Yusif, S., Hafeez-Baig, A. & Ananchans, C., 2024, 'Internet governance and cyber-security: A systematic literature review', *Information Security Journal: A Global Perspective* 33(2), 158–171. <https://doi.org/10.1080/19393555.2023.2268608>
- Yuste, J. & Pastrana, S., 2021, 'Avaddon ransomware: An in-depth analysis and decryption of infected systems', *Computers & Security* 109, 102388. <https://doi.org/10.1016/j.cose.2021.102388>
- Zhang, Y., Xiong, F., Xie, Y., Fan, X. & Gu, H., 2020, 'The impact of artificial intelligence and blockchain on the accounting profession', *IEEE Access* 8, 110461–110477. <https://doi.org/10.1109/ACCESS.2020.3000505>