The African Journal of Information Systems

Volume 15 | Issue 2 Article 3

September 2023

Phishing Attacks: A Security Challenge for University Students Studying Remotely

Blessing Nyasvisvo
University of the Western Cape, 3804796@myuwc.ac.za

Joel M. Chigada
University of the Western Cape, chigadajm@gmail.com

Recommended Citation

Nyasvisvo, Blessing and Chigada, Joel M. (2023) "Phishing Attacks: A Security Challenge for University Students Studying Remotely," *The African Journal of Information Systems*: Vol. 15: Iss. 2, Article 3.
Available at: https://digitalcommons.kennesaw.edu/ajis/vol15/iss2/3

Phishing Attacks: A Security Challenge for University Students Studying Remotely

Cover Page Footnote

The authors acknowledge the opportunity granted by the editor of this journal to publish the paper. We also acknowledge the reviewers for their insights and constructive feedback for this paper. We want to acknowledge the participants for their time and inputs during the data collection process.

The African Journal of Information Systems

Phishing Attacks: A Security Challenge for University Students Studying Remotely

Research Paper

Volume 15, Issue 2, September 2023, ISSN 1936-0282

Blessing Nyasvisvo
University of the Western Cape
e-mail address: 3804796@myuwc.ac.za

Joel Chigada
University of the Western Cape
e-mail address: chigadajm@gmail.com

(*Received October 2022, accepted July 2023*)

ABSTRACT

The emergence of the deadly global respiratory coronavirus disease (COVID-19) in 2019 claimed many lives and altered the way people live and behave as well as how companies operated. Considerable pressure was exerted on Institutions of Higher Learning (universities) to salvage the academic projects through the process of business model reconfiguration. Students were required to study remotely and were, therefore, exposed to phishing and scamming cyber-attacks. The effects of these attacks were examined in this study with the support of literature and empirical research leading to appropriate recommendations being proposed. Data were obtained through semi-structured interviews from students at a selected public-funded university. Atlas.Ti was used for data analysis to identify usable and sensible themes. The study established that students were aware of the factors that exposed them to phishing and scamming attacks but lacked the skills to identify such attacks before becoming victims.

Keywords

Anti-virus, coronavirus disease, cybercrime, identity theft, phishing, pop-up ads.

INTRODUCTION

The global emergence of the respiratory coronavirus disease (COVID-19) in 2019 claimed many lives and altered the way most people lived and behaved. This necessitated the reconfiguration of business models. Considerable pressure was exerted on institutions of higher learning, specifically universities, to salvage the academic project through business process reconfiguration. It was decided that an appropriate solution was to move to online learning management systems (LMS), ushering in an era of remote learning. Digital transformation entails leveraging emerging technologies such as LMS, Internet of Things and artificial intelligence thereby introducing new business processes (Warner & Wager, 2019). Adopting online and remote LMS was intended to bring students closer to their lecturers and to manage data and processes whilst providing value-added services to the university community (Chigada & Madzinga, 2021). This had the goal of enabling university courses to remain relevant during and after the pandemic. Universities are viewed as knowledge repositories, innovation incubators and centers of excellence. Therefore, they should recognize the need to be agile, rethink new teaching and learning models and tools, foster digital talent, and adopt a collaborative approach and culture (Warner & Wager, 2019). Furthermore, universities have the resources and ability to harness digital technologies to improve processes, performance, research, teaching and learning (Warner & Wager, 2019).

Education is a critical part of every economy and contributes to the sustainable development of that economy. Thus, the closure of institutions of higher learning due to COVID-19, although brief, was concerning for the ministries of higher and tertiary education of most nations. According to the United Nations Educational, Scientific and Cultural Organization (UNESCO, 2020), approximately 10 million African students' studies were disrupted due to the closure of tertiary institutions. E-learning is defined as a learning process that happens over a digital platform where teachers and students can send and receive learning material via an established network (Tamrat & Teferra, 2020). Some institutions already had e-learning incorporated into the way they taught, but most had to acquire appropriate information systems and other tools to continue providing their services to their students.

Institutional websites incorporating e-learning portals can be used to send course content and learning and research materials to students (Pham & Ho, 2020). For example, students and academics at a public-funded university in South Africa access learning materials using the iKamva LMS. Personal communication between learners and lecturers is, however, via email services such as gmail.com. e-Learning sites are generally secure, and students are required to use their credentials (username and password) to access the content of that e-learning space. Webinar usage has also aided the way in which teaching and learning are conducted; most lectures and seminars are facilitated through Zoom, Skype, Microsoft Teams or Google meetings. Webinars involve delivering presentations, seminars, and teaching workshops online with interaction between students and lecturer by means of Internet media (video and sound). Many people in different geographic locations can attend webinars (Hassan et al., 2020).

Over-reliance by universities on e-learning platforms to deliver learning resources to students has had repercussions because cybercriminals have had ample time to identify loopholes in these platforms (Raza et al., 2020*).* Chigada and Madzinga (2021) assert that cybercriminals do not attack a system immediately but take time studying the weaknesses of the system and determining how long it would take the organization to discover a data breach. Phishing no longer only happens via emails; hackers have found ways to intrude into Zoom webinars while students are active and may display X-rated content or steal students' log-in credentials. This proves that the threats that these actors pose are evolving rapidly to ensure that they fool many victims. Cybercriminals use phishing and scamming tactics to trick students into revealing their credentials unknowingly (Dreese, 2018). Tactics include offering false free promotional codes to access textbook sites, COVID-19 updates, and emails that appear as if they were sent by the university. Students become victims because they think they are interacting with a legitimate entity. These mischievous activities generally have one thing in common, students are requested to urgently insert their credentials. According to the Anti-Phishing Working Group Phishing Trends Report (2018)*,* credentials stolen via phishing and scamming platforms are used for nefarious acts such as fraud and identity theft. These acts could seriously affect an average student. Therefore, this study was conducted to raise awareness amongst the student community at large. An exponential growth rate of cybercrimes was reported during the peak of the COVID-19 pandemic because of the move to work from home (WFH). This primarily exposed people who were connecting to a corporate network using unsecured public Wi-Fi. In addition, the acceptance of bring your own device (BYOD) policies can result in less advantaged students sharing devices with their peers, thus further exposing a student's credentials (Chigada & Daniels, 2021). Students have borne the brunt of cyber-attacks during teaching and learning activities (Pranggono & Arabo, 2021).

A review of the literature showed a scarcity of studies that investigated phishing attacks and the challenges they posed to students studying remotely during the emergence of the global COVID-19 pandemic. No study was found to have investigated this in South Africa. However, a preliminary investigation with distance online-learning students that was outside the scope of this current study indicated that they were not vulnerable to phishing attacks. Further investigations into these claims revealed that the students were not aware that many email messages were suspicious and potentially harmful to their devices. We discovered that students lacked awareness and understanding of how phishing attacks were designed to target potential victims. Students did not understand that phishing attacks are a form of cybercrime. It is against this background that the current study investigated factors that expose students to phishing attacks and suggested appropriate interventions to mitigate the effects of phishing attacks. This study investigated common phishing attacks, interventions, and effects of phishing attacks on students studying remotely. The following research questions guided us to address the study objectives:

- What factors expose students to phishing attacks?
- What the common phishing attacks are used by cybercriminals?
- What are the effects of phishing attacks on students?
- What interventions can mitigate phishing attacks?

LITERATURE REVIEW

Cybercrime

All computer-mediated activities perpetrated with the intention of stealing information or data assets, tampering with or deleting information, denying access to information technology infrastructure and extortion are cybercrime (Khan et al., 2020; World Health Organization [WHO], 2020. Chang and Coppel (2020) define cybercrime as the ability of threat actors to infiltrate a company's IT infrastructure remotely with the intention of stealing from the company or individual. Anastasiou et al. (2020) state that cybercriminals use modern technologies to illegally access company networks or cell phones. Chigada (2023:5) defines cybercrime as "any unlawful activities perpetrated by criminals through Internet-based transactions with the intention of destroying, inflicting emotional and psychological harm, financial loss and reputational damage to a person or organisation". Given the different perspectives of definitions of cybercrime, we concluded that there is no universally accepted definition. In light of the above, we adopt the definition of cybercrime given by Chigada (2023). This definition captures the major tenets of the key discussions of this study.

The emergence of COVID-19 in December 2019 contributed significantly to the phishing scourge. Cybersecurity experts say that the WHO, Centre for Disease Control, the financial sector, universities, healthcare institutions and government departments have been major targets of cyber-attacks and threats (Chigada & Madzinga, 2021). Cybercriminals are aware that these institutions process and store large volumes of client or patient information, which in many instances includes identity documents (IDs), banking details, addresses and contact details. This information has a readily available grey market with buyers prepared to pay well for it knowing that they would profit from criminal acts enabled by the access to the acquired data (Bowen & Seth, 2020). Hamman et al. (2017) identify twelve different types of cybercrimes and include phishing attacks, the subject of discussion in this study.

Phishing Attacks

Social engineering attacks such as phishing emails and scamming are among the most serious cybersecurity threats (McAlaney & Hills, 2020). Social engineering means persuading unsuspecting people to comply with the cybercriminal's instructions for them to surrender their confidential information (Chen et al., 2020). Chigada and Madzinga (2021) state that cybercriminals use spoofed emails to scam and steal victims' identities which are then used for malicious activities. Due to the COVID-19 regulations, many employees and students started to WFH using their own smart devices; this exacerbated the vulnerability of potential phishing victims (Iyengar et al.,2020). Persuasion and deceit play a major role in the success of digital scams and phishing emails (Ferreira & Teles, 2019). This literature review examines the effects of phishing and scamming via the Internet for students studying from home during the COVID-19 pandemic. Over the years, many types of cybersecurity threats having been shown to exist; phishing is the oldest of them and has a sixty percent chance of working (Prasad & Rohokale, 2020).

Types of Phishing Attacks

Various definitions for phishing have been proposed and discussed by researchers and cybersecurity experts. The term phishing is continuously evolving; hence, there is no one specific definition for the term; it can be defined in various ways based on context and its use. Alkhalil et al. (2021) define phishing as a socio-technical attack, which is designed by the threat actor to acquire certain information from the victim by exploiting an existing vulnerability through social engineering techniques to lure the victim into taking a specific action that will immediately cause damage. We will refer to the definition used by Alkhalil et al. (2021) throughout the paper when referring to phishing because of its depth in explaining the term. Different types of Phishing attacks include email, spear, smishing and clone.

(i) Email Phishing: Phishing emails are fraudulent messages designed by cybercriminals to make them appear as if they were sent by a legitimate sender so that users are more likely to believe the message and act upon it (Guarda et al., 2019). Such emails seem to have been sent by a bank, university, or any other entity associated with the recipient's daily activities. Phishing emails are usually convincing to the eyes of an ordinary user and usually contain a link which the recipient is pressured to click on. Burns et al. (2019) suggest that the use of well-known logos, brands and layout make these emails look real and this is what deceives victims.

(ii) Spear Phishing: This is similar to ordinary phishing but is targeted at an individual as the cybercriminal has gathered information about the target before sending the phishing email (Aleroud et al., 2020). The information harvested is used to create a tailor-made email that looks genuine. The contextual information about the target is the main factor that makes spear phishing likely to succeed.

(iii) Smishing: In this approach criminals attempt to persuade mobile phone users to install malicious software onto their devices, share sensitive information, or send money to cybercriminals. Smishing is derived from short message services (SMS) + Phishing = smishing (Baillon et al., 2019). These persuasive messages are also distributed on WhatsApp and usually contain a link that directs the victim to a site that mimics a well-established entity (Choudhary & Jain, 2018).

(iv) Clone Phishing: This type of attack is where cybercriminals clone a website that the victim frequently visits (Binks, 2019). The cloned website looks like a genuine website and prompts the user to enter log-in credentials (Alkhalil et al., 2021). Criminals often use e-commerce websites as bait and display items at a discount so that the victim will make a purchase using their banking details.

These types of phishing have a strong influence on students' exposure and susceptibility.

FACTORS EXPOSING STUDENTS TO PHISHING ATTACKS

Social Media

Research in the cybersecurity environment shows that social media contributes to the exposure of students to phishing attacks (Tonkolu, 2019). Social media can be defined as a collection of websites and applications that allow users to join social networks and share information online (Fuchs, 2021). According to Broadhurst et al. (2018), emails containing details that are of interest to the targeted student tend to make the attack succeed. Attackers spend time collecting private information related to the targeted student so that they can use it in a phishing email and to perpetuate their scams (De Kimpe et al., 2018). Social media sites have been the data mining field (source of such information) for cybercriminals in recent years (Parker & Flowerday, 2020). With over one billion active users monthly, Meta (formerly Facebook) remains the most popular social media site on the Internet. A range of personal and confidential data is exchanged on the web, making it a prime target for hackers (Seng et al., 2019). According to Birlea (2020), information such as photos, travel plans, accomplishments, meetings, and any other personal data shared on social media sites can be manipulated to construct a very credible phishing email. Cybercriminals can devise complex and sophisticated means of attacking their victims because people spend a lot of time on social networking platforms.

Working Remotely

There are several reasons why WFH provides cybercriminals with new opportunities. Firstly, according to Eigbrecht and Ehlers (2020), a decrease in attention span is found amongst WFH students and staff because the home environment is not always conducive to working and studying. As a result, WFH creates a huge opportunity for cybercriminals to lure distracted victims into making rushed decisions that require sharing their credentials. Secondly, hackers find the change in the environment useful since more shopping and payment of bills is being done online (Khan et al., 2020). Hence, there has been an increase in the registration of malicious websites, spam, and phishing emails. Thirdly, home-based work increases exposure to cyber-risks because individuals connect through less-reliable and unsecured public Wi-Fi connections (Simonovich, 2020; Chigada & Madzinga, 2021). Fourthly, the use of personal devices (e.g., BYOD) allows users to connect to the corporate network with several devices - there might not be any restriction on the number of devices an individual can connect to the company's network (Chigada & Daniels, 2021). When students operate from home-settings there is a high likelihood that friends, siblings and family members would use the same Internet-enabled devices, which creates additional windows of opportunity for social engineering attacks (Simonovich, 2020; Chigada & Daniels, 2021). Humans are central in business processes and many people are regularly working remotely. As emphasis is placed on human intelligence, firms might overlook the fact that individual ethical behaviour is a key aspect of human intelligence (Chigada, 2020).

Unsecured Public Wi-Fi Networks

Students were stopped from attending activities on campus because of the social distancing regulations imposed by WHO (Sahu, 2020). This resulted in limited use of the university's Wi-Fi and virtual private network (VPN) which are relatively secure and are monitored regularly (House & Radu, 2020). This contributed to the increased number of phishing cases since many students had to study and work using cheap and unsecured public Wi-Fi at home (Choi et al., 2021). Cybercriminals find it relatively easy to phish students using an unsecured network and it may be difficult to detect and prevent phishing attacks on a network with weak protection (House & Radu, 2020). These less well-protected networks contribute to students' exposure to phishing. The authors assert that there are several features that make free Wi-Fi hotspots appealing to both consumers and hackers. One is the lack of authentication required in these environments to establish a network connection, which provides hackers with an additional opportunity to gain unrestricted access to unsecured devices linked to the same network (Quade, 2020).

Hackers positioning themselves between the legitimate user and the connect point pose the greatest security threat to the Wi-Fi connection. Hence, the user communicates with the hackers instead of with the hotspot. The hacker then passes this information to the chevalier (Quade, 2020). House and Radu (2020) posit that in such instances the hacker has access to every piece of information sent out on the Internet while working in this set-up, including important emails, credit card details, identity information and security credentials for the organization. Once armed with this information, the hackers can access the user's systems as if they were the user, whenever and wherever they want to. Insecure Wi-Fi connections can be used by hackers to spread malware. Since students tend to share files across networks, malware can infect other computers. There are instances where hackers access the connection point itself, causing pop-up windows to appear during the connection process, possibly offering an upgrade to a popular piece of software. By clicking the pop-up window, malware is installed (Quade, 2020).

Curiosity to Know the Latest COVID-19 News

During the global COVID-19 pandemic, people were eager to get hold of the latest information. Curiosity increased after the first lockdown started and people searched for information on various websites. According to Stein-Zamir et al. (2020), there was an exponential rise in the development of cloned websites. Users visiting these spoofed sites were particularly likely to be exposed to phishing. Students constantly searched for statistics regarding COVID-19 cases and information relating to when the university would announce a return to campus. Several popular platforms were targeted (Diaz et al., 2020). Users were enticed to subscribe to spoofed websites to get the most recent news sent to them using their emails and as a result were exposed to phishing attacks (Parker & Flowerday, 2020). These factors made students susceptible to phishing scams, but such sites do not discriminate, anyone can fall victim to the attacks.

Khan et al. (2020) state that, during the peak of the global COVID-19 pandemic, cybercriminals identified an opportunity to target research, teaching and learning institutions since they knew that students, academics and other staff were focusing on the pandemic. We agree that the focus for everyone during the peak period of the global pandemic was to obtain as much information as possible. Khan, et al. (2020) posit that in this period there were many unreported incidents of cyber-attacks with the victims provided with disinformation that led to the loss of sensitive private information and financial resources.

EFFECTS OF PHISHING ATTACKS ON STUDENTS

Once students fall victim to a phishing attack, there are negative effects that follow. Gomes, Reis and Alturas (2020) highlight how social engineering tricks can be harmful to the system, but to an even greater extent the victim suffers. Cyber-attacks and threats include identity theft and monetary loss, learning inconveniences and reputational damage.

Identity Theft and Monetary Loss

Identity theft is a criminal act that involves the use of someone's details, such as names and identity document numbers, and pretending that they are your own (Floderus & Rosenholm, 2019). Chen, Gaia, and Rao (2020) say that college students and business employees are usually targets for spear-phishing targets by cybercriminals. The stolen information may be used to open multiple credit cards, fake IDs, or even perpetuate hate crimes (Nmachi & Win, 2021). Identity theft contributes to phishing because identity is central in all aspects of our lives. A study carried out in South Korea showed that a significantly larger number of the respondents expressed fear of the consequences of identity theft than for any other crime on the Internet (Choi et al., 2021). The literature reveals that most cases of online identity theft result in monetary loss and other forms of fraud. Chigada (2020) established that cases of identity theft where merchants have lost large sums of money have been widely reported by financial institutions.

Learning Inconveniences

New methods of learning, such as Zoom meetings, have become common since the start of the COVID-19 pandemic (Aiken, 2020). However, some the tools adopted in e-learning have huge security concerns associated with them as they are easily penetrated by hackers (Aiken, 2020). According to Wagenseil (2020), lectures taking place online have frequently had to be adjourned due to security breaches and pornographic content being displayed on the screen. These breaches start with a single phishing email with a link sent to one of the students; by clicking the link given, access is granted to attackers (Henry & Shellenbarger, 2020).

Other inconveniences have been experienced when Zoom webinars have been disrupted through distributed denial of services (DDoS). In DDoS hackers overwhelm the bandwidth required, leading to bandwidth depletion; computer resources are flooded with spurious requests that use up all the bandwidth; the attacks are aimed at the network or server resulting in traffic congestion and hence slow the server or cause it to crash so that no legitimate user can access it. Hence, in DDoS normal operations are disrupted creating challenges for the organization or individual and halting business activities. Quade (2020) describes DDoS as a cyber-attack denying legitimate users from accessing computing services. With the aid of the Information and Communication Services, it should be easy to distinguish DDoS traffic from legitimate traffic.

Reputational Damage

Phishing often obtains user credentials, and the victims suffer consequences related to what their information has been used for (Breakstone et al., 2021). These victims often find that their names and details have been used to commit crimes or for socially unacceptable behavior (such as fraud, online bullying, or distributing X-rated content on social media or during video conferencing meetings) (Alkhalil et al., 2021). As a result, the victim’s reputation is often adversely affected. Phishing generally involves identity theft and monetary fraud and destroys reputations and causes psychological damage. Hence it should be understood and be taken seriously by Internet users.

MITIGATING PHISHING ATTACKS

As indicated in the introductory section of this study, there is no consensus regarding the factors that expose students to phishing attacks, let alone possible interventions to completely eradicate the wave of cyber-attacks that students are threatened by. There is no single, reliable, system-based solution that can completely prevent online phishing (Williams & Joinson, 2020). Sumner and Yuan (2019) argue that the best solution is to teach Internet users how to spot a phishing attack before harm is done. In this section the researchers analyze current measures users should be able to implement to combat phishing threats on the Internet.

Awareness Through Education

Chigada (2023) states that the rapid increase of technology and Internet use for daily activities requires us to understand how phishing works and raise awareness in our communities. The more effective students are in identifying phishing emails, spoofed websites and links that require one to register, the less vulnerable the university community will be (Oest et al., 2020). Yanakiev et al. (2020) explain how social engineering attacks aim to manipulating people to share critical information willingly. Hence, this study advocates for frequent awareness campaigns to help people to identify these attacks easily and timeously.

Browser-Based Detection

Recent browser-based phishing detection functionality on web-browsers, such as Chrome and Mozilla Firefox, has become increasingly effective in identifying potential phishing attacks and warning the user about them (Oest et al., 2020). However, the lag period might hinder the effectiveness of this measure amongst different browsers (Arshad et al., 2021). This means the flagging of the attack and warning message to the user is delayed. Benavides et al. (2020) present a systematic literature review of machine and deep learning approaches that, combined with browser detection, can complement each other in assisting the user to identifying phishing attacks.

Email Impersonation Protection

Email messaging is the means most frequently used by cybercriminals to lure students into sharing their credentials and submitting to scammers (Broadhurst et al., 2020). Gmail checks the universal resource locators (URL) contained in an email against a blacklist. A warning is sent to the user of a suspect email if a URL matches a blacklisted address (Ali, 2019). The best action is to immediately report the email when a user identifies a phishing email in their inbox because this helps the machine learning tool to prevent future attacks (Atimorathanna et al., 2020). To avoid the menace of phishing attacks, students should treat every email and link they receive in their mailbox with caution (Lawal & Cavus, 2019).

Malware Protection and Firewalls

Most studies recommend malware protection and firewall installation on all the electronic devices that students use for online activities. Guo et al. (2020) concur and mention the importance of malware detection software that blocks malicious links. Zhu (2020) states that firewalls can block phishing attacks on spoofed websites, but they warn the user of suspicious activity only approximately 70% of the time. One can conclude that a variety of measures can be used by students to detect phishing attacks, but without sufficient human vigilance these measures might be in vain.

The top entities targeted by phishers are Netflix, Facebook, WhatsApp, Microsoft, and PayPal, and this is an indication of how phishing impacts on people's lives and livelihoods (Alwanain, 2019). Phishing is a social engineering technique, which means it focuses on manipulating human behavior and emotions. Therefore, no software alone can address phishing attacks without human involvement in identifying the phishing attacks (Shaw, 2020). According to Miller et al. (2020) phishing awareness training should be a must for every Internet user. Their findings suggest that users who are educated and aware of what phishing attacks look like are less likely to be preyed on compared to those who do not know about phishing (Miller et al., 2020). End-user awareness training by big technology companies should be a priority; they should take responsibility for educating their subscribers regarding phishing attacks (Singh et al., 2019).

Fang et al. (2019) recommend that users change their passwords frequently and also discourage saving passwords on a web browser, since this can make it quite easy to become a victim of malware attacks. Dawood, Ibrahim and Abu-Ulbeh (2019) agree; users, especially students, should always be cautious when they enter their passwords online. Before entering your credentials, the webpage URL and domain names in email headers should be examined carefully; look out for spelling errors; and note the language tone being used (Dawood et al., 2019). Ference (2017) suggests that users should avoid clicking on pop-up advertisements when they are surfing the Internet because that is where phishers set their bait. Data-security platforms or anti-virus software that help you spot any signs of an attack should be enabled by every Internet user (Parsons et al., 2019). Be aware that if the offers seem too good to be true, it is probably a scam, and you are about to be a victim of phishing (Ference, 2019).

QUALITATIVE RESEARCH METHODOLOGY

The study investigated the effects of phishing attacks and explored factors that exposed students studying remotely. We carefully considered the philosophical assumptions that informed this research (Creswell & Creswell, 2017). When addressing questions relating to the forms of reality, we used the subjective ontological stance to decide what could or could not be observed. We focused on how reality could be observed (if it could be observed) and our relationship with this reality (epistemology). We chose a qualitative methodology to complement the subjective ontological stance and philosophical view. Qualitative research is when the researcher seeks to establish an understanding of the phenomena being studied from the views of participants (Creswell & Creswell, 2017). We adopted this methodology because our objective was to address the research problem through direct interaction and personal conversations with participants. Semi-structured interviews allowed us to ask probing questions where we felt more information was required (Creswell & Creswell, 2017).

Sampling Process and Data Collection

The research population for this study was 25,000 students; however, a sample of 8 students was selected because we reached a point of data saturation at that point. A saturation point in qualitative research refers to the point at which no new information is discovered in data analysis (Creswell & Creswell, 2017). This redundancy or saturation point is a signal to researchers that data collection may cease. Creswell and Creswell (2017) state that the saturation point is reached when enough data has been collected to a point that now new facts are provided by participants. The participants were selected using inclusion/exclusion criteria, a process where the authors identify the participants to be included in the sample in a consistent, reliable, uniform, and objective manner. Non-probability purposive and convenience sampling techniques were found suitable to apply the inclusion/exclusion criteria because these sampling techniques permit the researcher's personal judgments on who to include or exclude from the study (Sharma, 2017). According to Etikan et al. (2016) purposive sampling is a non-random technique that does not rely on underlying theories or prescribe a set number of participants. Purposive sampling allows us to depend on our judgment when selecting participants to take part in the study. Participants were identified and selected for possessing characteristics that made them eligible for this study. This included gender, whether they were registered students, age and possessing relevant experience which enabled them to provide information for the study. We started with 8 participants, and after collecting data from them we realized that there were no new insights from the participants, thus, we then decided to stop at 8 participants.

Semi-structured interviews are a verbal interaction between the interviewee and the interviewer, where the interviewer attempts to elicit information using a prepared list of questions as a guide (Bryman, 2017). Prior to each interview, we familiarized the participants about the phishing phenomenon to ensure their maximum contribution to the study. Each interview session started with a brief overview of the purpose of the study, the topic and how people become victims. We explained that phishing was a form of cybercrime and that potential victims were usually contacted through unsolicited emails containing messages prompting the intended victims to respond by clicking a URL which mimicked a legitimate site. The interviews were conducted using the Zoom video conferencing platform and were recorded on the researchers' Google drive in line with social distance health protocols because data were collected at the peak of the global COVID-19 pandemic. The interviews were recorded since the interviewees had given their consented. Participants had the right to participate or withdraw from the interviews without any repercussions.

Data Analysis

Bryman (2017) defines data analysis as "the computation of raw facts to produce information" (p. 213). "Data analysis is a crucial part of any research because it summarizes collected data" (Kabir, 2016:211). In this study, since the authors gathered data through an online video conference platform, the authors were also research instruments. We understood, described, and interpreted participants' experiences and perceptions of a phenomenon. We adopted thematic data analysis to identify patterns of factors that influenced students' exposure to phishing attacks on the Internet while studying from home during the Covid-19 pandemic. Thematic analysis is defined as a process of identifying, analyzing, and interpreting themes within qualitative data (Maguire & Delahunt, 2017). We used Atlas.Ti to identify emerging themes from the interview transcriptions. Atlas.Ti is a strong qualitative data analysis tool that aids the authors in the data analysis process by analysing and interpreting texts utilizing coding (Smit, 2002). Whilst using Atlas.Ti, we adopted a six-step approach which included familiarity, generating initial codes, generating themes, reviewing themes, naming themes, and lastly the write-up of the report (Elo & Kyngäs, 2008). The interviews were transcribed using Dragon speech transcription software to ensure accuracy, and error-free, easy-to-read responses from the participants. All research findings were presented in text format.

FINDINGS

Eight participants were interviewed and their responses were recorded and transcribed. All participants were registered students at the Western Cape university. Six participants were studying for undergraduate degrees while two were completing postgraduate studies. Participants' identities were kept anonymous throughout the study and pseudonyms were used. There were four female participants and four male participants.

Factors that Exposed Students to Phishing Attacks

All the participants acknowledged that scamming incidences have been increasingly prevalent within the university community since the beginning of the COVID-19 pandemic. The most evident themes from the interviews have been summarized in Figure 1.

When asked whether studying online had increased the levels of phishing attempts, all participants agreed that it had and provided examples of scamming and phishing attempts they had received in the past months. One interviewee stated that, "I have been receiving a lot of phishing emails and text messages informing me about competitions I have won iPhone 12 but to my surprise, I never entered such competitions.*"*

Another participant stated that, *"I constantly use my laptop and phone to do my assignments daily and I always feel like I am exposed to some very persuasive pop-up adverts. Quite sometimes I have been tempted to click on them, especially when I saw sneakers that I wanted on sale."*

It is evident from the above quotations that participants were feeling increasingly exposed to phishing and scamming attempts and that they were aware of factors that exposed them to such attacks. Constant use of emails while studying from home allows cybercriminals to manipulate these emails to encourage students to give their credentials willingly. Attackers are becoming skilled in luring students to click on pop-up ads that have been created to appeal to the target. Participants mentioned that the use of unsecured networks in their homes and restaurants hotspots are contributing to their exposure to being scammed. *"I think our home Wi-Fi network is not as secure as the Wi-Fi network I used to use at the university library, and I worry this might leave me exposed to phishing and scamming attacks."*

Participants mentioned that they have encountered several mimicked websites during their online studies. Responses highlighted that some of these malicious websites are difficult to detect since they look exactly the same as the actual website and hence it is easy for them to fall victim.

Participant 5 described how he became a victim of a malicious website by stating that:

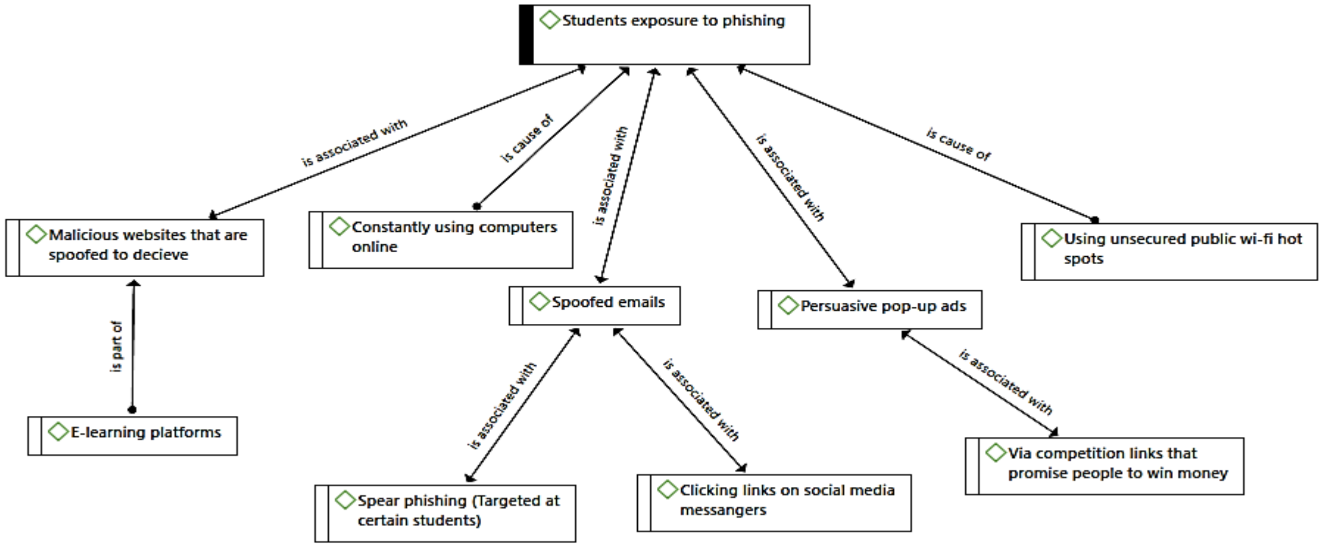
> I thought I was buying an Economics textbook on 'TakeALot' but to my surprise, it was not the actual website. I saw the advert on Twitter, and it directed me to the website where the book was on sale. I entered my details and debit card number to purchase and as soon as I finished the website disappeared and I never received any confirmation email of my order, and my money was already withdrawn.

The extracts given above demonstrate that everyone using an Internet-enabled device and anyone using emails or social media frequently should be vigilant and carefully check the messages they receive. It is important to take note of how easily participants were lured by phishing messages. Therefore, the findings are important in emphasizing the need for awareness and education in order to avoid being a victim of phishing attacks.

Figure 1 summarizes the key themes that emerged for this research question.

Figure 1

Students' Exposure to Phishing


Students exposure to phishing
is associated with
is cause of
is associated with
is associated with
is cause of
Malicious websites that are spoofed to decieve
Constantly using computers online
Using unsecured public wi-fi hot spots
Spoofed emails
Persuasive pop-up ads
is part of
E-learning platforms
is associated with
is associated with
is associated with
Spear phishing (Targeted at certain students)
Clicking links on social media messangers
Via competition links that promise people to win money

Phishing Attacks Used by Cybercriminals

The participants provided mixed responses regarding what techniques cyber attackers use to spy on potential targets. The majority of the participants have not been victims of phishing and scamming but a few of them have personally encountered these cybercriminals. Nevertheless, most participants had information to share about techniques cyber attackers have been using recently to catch them or their relatives and friends.

Participant 1 stated that:

> I saw a bursary opportunity on LinkedIn, and it appeared to be a legitimate opportunity. Hence, I proceeded to apply for it since I need financial aid with my tuition fee. I entered my banking details and ID number. I did not receive any response after I completed the application and the moment, I told my father about the opportunity he advised me to block my bank card because the opportunity might be a scam.

The statement from Participant 1 shows how cybercriminals target their victims knowing their situations. This decreases the chance of one being able to identify attacks. Participants also stated that recently they have been receiving text messages on their smartphones that they have won huge data bundles from their service provider; for them to claim the bundles they are required to navigate to the service provider website via the provided link.

> As a student I require data bundles to survive, for example, to attend Zoom classes, browse the Internet, watch movies and series, and communicate. Hence why when I received a text message that said I won 700GB of data bundles I was so excited, but I knew it was just too good to be true.

Participant 4,2021 stated that *"I once received a text message about a job opportunity but to my surprise it wanted me to pay 100 rands to submit my application so that I could be considered."*

It is evident from this study that scamming and phishing attacks are always evolving and are diverse. This shows that students can suffer significant losses if they fall for traps set by criminals. Another participant opened up in the interview with the researcher regarding how she lost money. This showed how far cybercriminals are willing to go to get what they want.

Participant 8 mentioned this:

> I saw a WhatsApp message which had a direct link to the online store in one other group I had joined that gave updates about the Covid-19 pandemic. The message was about helping people who were not able to buy food because they lost their jobs hence, they were selling foods items at a lower price, and they would deliver for free. I bought 500 rands worth of items but when I realized it was a scam, they had already withdrawn 1000 rands that were in my account when I purchased.

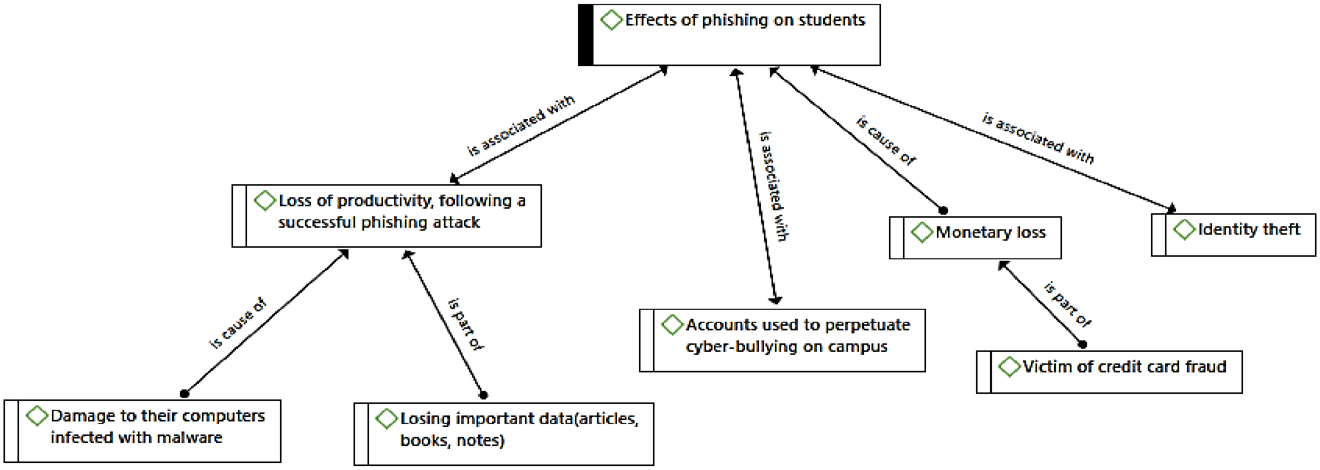
It emerged from the study that cyber attackers are not only using phishing emails to deceive victims but are also coming up with additional ways to mask their attacks so that they look real to the victim.

Effects of Phishing Attacks on Students

Various phishing and scamming attack outcomes and side effects that affect students were identified in the study. Themes that emerged from the responses included a decrease in productivity, monetary loss, identity theft, cyber-bullying, and damage to hardware and software. A summary of the findings is depicted in Figure 2 below.

Figure 2

Effects of Phishing on Students


Effects of phishing on students
is associated with
is associated with
is cause of
is associated with
Loss of productivity, following a successful phishing attack
Monetary loss
Identity theft
is cause of
is part of
is part of
Accounts used to perpetuate cyber-bullying on campus
Victim of credit card fraud
Damage to their computers infected with malware
Losing important data(articles, books, notes)

Participants said they are terrified of the thought of someone else using their identity and pretending to be them because one can never know what they will do. For this reason alone, all participants agreed that they ensure that they do not give out their identity numbers over the Internet unless they are sure of the source.

One participant stated that:

> As a student, I think losing your identity details can negatively affect you in the future if the cybercriminals use your information to commit fraud or theft. You might realize you have a criminal record on your identification number when you start applying for certain necessities which you never knew about.

Identity theft can cause serious effects such as damaged credit because the cybercriminals can open accounts in your name and never return the due amount which will ruin any person. This was stated by Participant 7, 2021.

The most frequently mentioned effect was losing money or savings. All the participants emphasized that monetary loss could affect their mental health and livelihoods during these difficult times where the majority of people are unemployed and those employed do not have sufficient job security because of the COVID-19 pandemic. Every participant agreed that stress levels increase due to being scammed.

> When they wiped my bank account after I purchased from their website. I felt so stupid, and I was always angry with everyone in my life. I constantly ask myself till today 'how was I so dumb to fall for those tricks.

Another participant mentioned how monetary loss can be evident a long time after you have already forgotten about any purchases that you might have made that might give you clues to identify the root of the problem. Participant 5, 2021 stated that *"*Sometimes they harvest your card details to commit credit card fraud and by the time you realize that your credit card has a lot of repayments due it will be too late.*"*

It emerged from the study that participants fear losing productive time while trying to fix the after-effect caused by being a victim of phishing and scamming. They mentioned that on occasion they receive emails with attachments that they should install on their devices, and this ends up leading to their computer's performance deteriorating.

One participant mentioned:

> I once downloaded software using a link from my emails and the moment, I installed this program my laptop crashed. The effect was that I could not finish my assignments and I was not able to attend a class for a week until it was fixed.

Mitigating Phishing Attacks

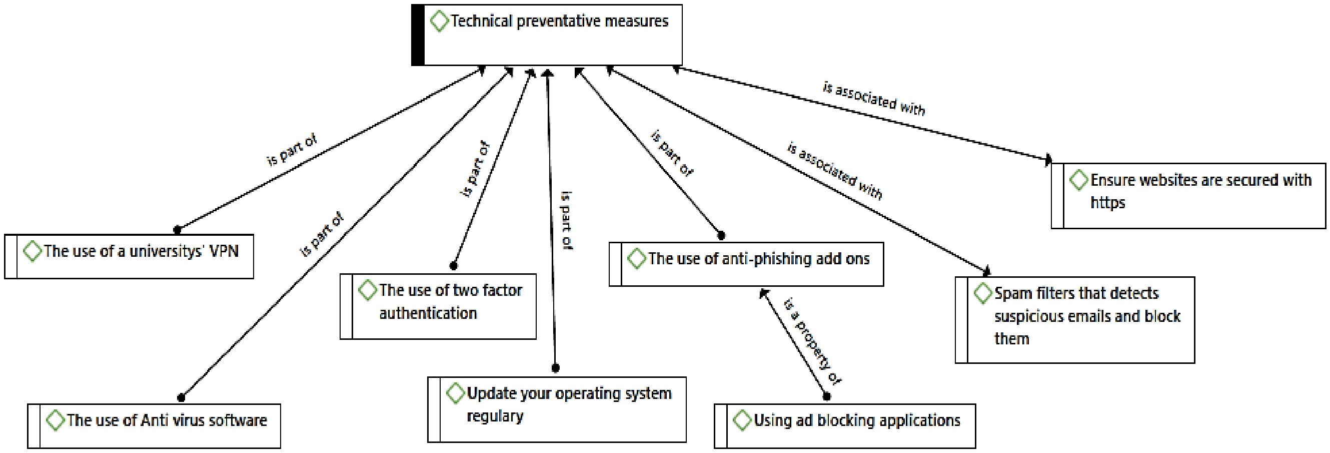
It was revealed in this study that students can find ways to protect themselves and reduce the susceptibility rate of them being victims. Most of the participants were aware of preventative measures they could take, and they shared their responses. Figure 3 depicts the detailed summary of these measures. At this stage, it is evident that if certain measures are not adhered to, the number of student victims that will be affected by the effects discussed above will increase exponentially.

Participants mentioned in their responses that "I installed spam filters on my laptop and smartphone, this helped me to not receive spam emails that usually contain most phishing emails". While participant 6, 2021 stated that "I installed anti-phishing and ad-blocker software to identify phishing messages on pop-up ads. Now I rarely receive these adverts."

Figure 3 summarizes themes that emerged for technical preventive measures.

Figure 3

Preventative Measures


Technical preventative measures
is associated with
is associated with
is part of
is part of
is part of
is part of
is part of
Ensure websites are secured with https
The use of a universitys' VPN
The use of anti-phishing add ons
Spam filters that detects suspicious emails and block them
The use of two factor authentication
is a property of
The use of Anti virus software
Update your operating system regulary
Using ad blocking applications

Other mitigation techniques mentioned were the use of the VPN provided by the university when doing any school-related activities since it is protected and there are sites that are restricted (access by the students is controlled) as they might lead to students being phished and scammed. In order to safeguard oneself against phishing attacks, participant 3, 2021 indicated that "I try by all means to avoid using unsecured networks hence why I use the VPN provided by the university to access all my course-related work."

The most common intervention mentioned by the participants was the use of anti-virus software. All the participants agreed that anti-virus software helps them to identify malicious websites and secures their devices. When they try to install malicious software programs the anti-virus software blocks downloads before any damage occurs.

Participants 1, 2, 7, and 8 stated that:

> The use of anti-virus software such as AVAST and Norton can be helpful when you navigate the Internet. They are also cheap to buy and easy to update, I always get alerts when I navigate to an unsecured site or even if I try to install corrupted software programs.

A few participants mentioned two-factor authentication as useful in assisting students to secure their credentials. It emerged that many applications (for example, Twitter and Gmail) have two-factor authentication. Even if cybercriminals get access to the students' credentials, they will not be able to log into an account without explicit approval from the account owner. The victim can quickly change the credentials as soon as an alert is received that someone is trying to log into their account and the whole situation is defused.

One participant mentioned that "I use two-factor authentication on all my accounts that allow me to activate it because it gives me the final say and I know if someone is trying to gain access of my Gmail account before they do."

Participants in this study were very aware of phishing and scamming attacks; however, in the responses they mentioned that it is of utmost importance to keep on learning about how to protect oneself from these attacks. Some participants advocated for students to attend cybersecurity modules at university to train and educate themselves on the issues regarding cybersecurity threats. Figure 4 provides a summary of findings under this theme.

> At our university, we do have courses about cybersecurity, but most students do not attend them because this is not part of their degree curriculum. After I was scammed money, I decided to register for the cybersecurity course to learn more of how to protect myself even though I am studying Law.

Participant 1, 2021 had this to say “I would advise other students to attend cybersecurity events and seminars to ensure that they are up-to-date with what tricks criminals are using and how to mitigate them.”

Participants mentioned that they change their passwords regularly so that they avoid saving passwords on their browsers. This limits the risk of cybercriminals gaining access to accounts and limits guesswork which might lead to information about the credentials being breached. A vivid answer was proffered by participant 2, 2021 who indicated that, “I change my password every month, to make it harder for criminals. I don’t want my log-in credentials to be known.”

It was revealed that only a few participants knew how to report a phishing attempt that they encounter. One of the participants mentioned that it is very important to report phishing attacks to the university IT department or to the browser and application you are using. This helps the browsers to flag a type of messages as harmful in the future. “I report every phishing email that I identify in my inbox to Gmail and the next time I receive such emails it will be flagged with a warning symbol.” (Participant 3, 2021)

Most of the participants that were interviewed agreed that if they are instructed to navigate to a website that requires their credentials, such as bank details or Netflix login, they will first go to their browser and then navigate to the particular site without using the link provided. Two of the participants mentioned that they do not pay attention to those details.

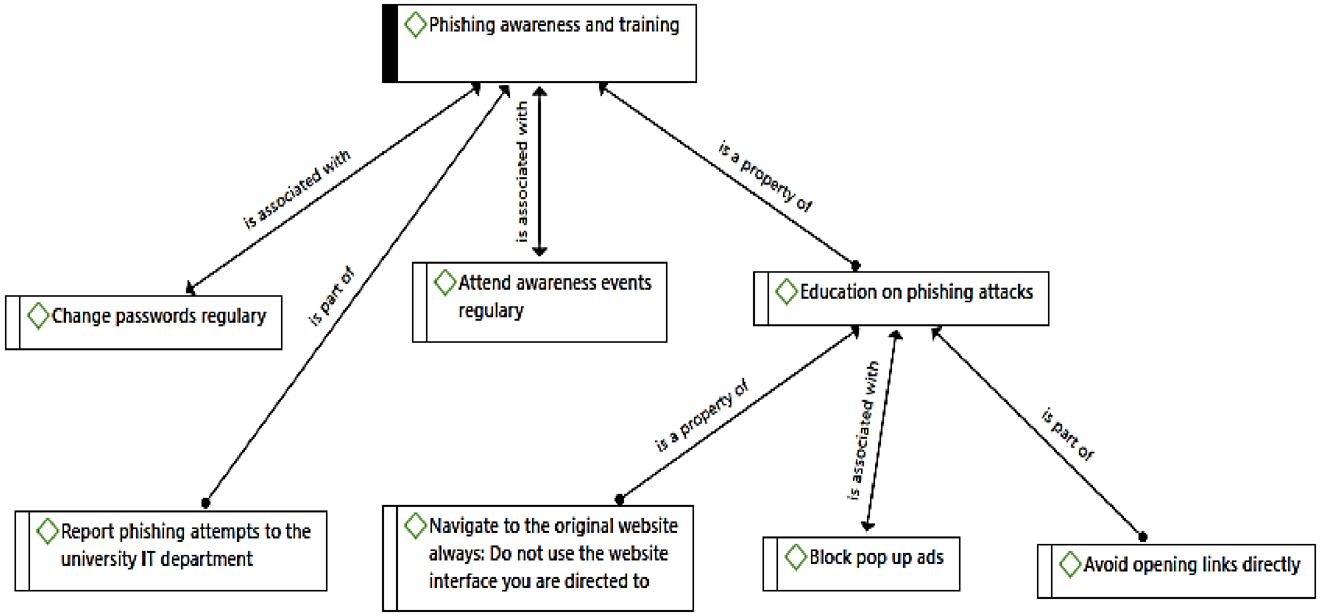
Participants 2,3,4,5 and 8 stated that:

> With all the knowledge we have gathered about phishing attacks, we are very vigilant of the links we click on while surfing online and we always opt to navigate to the actual website on our own without the guidance of a link.

Figure 4 provides a summary of phishing awareness and training themes that emerged.

Figure 4

Phishing Awareness and Training


Phishing awareness and training
is associated with
is part of
is associated with
is a property of
Change passwords regulary
Attend awareness events regulary
Education on phishing attacks
is a property of
is associated with
is part of
Report phishing attempts to the university IT department
Navigate to the original website always: Do not use the website interface you are directed to
Block pop up ads
Avoid opening links directly

DISCUSSION

The findings from the first research question show that students were exposed to phishing attacks by connecting to the university network through the use of unsecured Wi-Fi (Choi et al., 2021). Participants indicated that during the COVID-19 lockdown period there was an increase in the number of unsolicited email messages that were received prompting students to enter competitions and exposing them to persuasive pop-up adverts. One participant used a malicious website to buy an economics textbook only to discover that it was a deceptive site. The advert was flighted on Twitter, and it appeared to be a genuine website. After credit card, personal and other sensitive information were captured the participant lost money to cybercriminals. Participants' responses revealed how easily one can become a target of phishing and how difficult it was to distinguish between a genuine website and a malicious one (House & Radu, 2020). Participants also indicated that they were exposed to phishing attacks through the e-learning management platform, incessant use of computers and personal mobile devices, clicking on social media messages, the use of public Wi-Fi hotspots and sharing friends or family members' devices. These views are supported by Zamir et al. (2020) and Gupta and Singh (2021) who state that phishing emails are used with malicious websites through the use of links that direct victims to the mimicked sites and once on those sites confidential information is requested.

In response to the second research question, participants indicated that phishing attackers were aware that accessing online learning materials was an easy and convenient point of entry for them. They knew that students and lecturers were using online learning management systems, therefore it was easy to send malicious messages to this target group (Eigbrecht & Ehlers, 2020). Findings from the study indicated that social networking platforms such as LinkedIn, Twitter, Meta and Instagram were increasingly turning into playgrounds for cybercriminals. Criminal elements target their victims using information that is readily available on LinkedIn and purport to be selling genuine learning materials. This was a huge red-flag and should be considered by students so that they do not fall prey to criminal syndicates. Other findings showed that participants were frequently targeted when looking for job opportunities; for example, text messages are sent instructing the victim to pay an administration fee in order to secure employment. In all of these phishing attacks complex strategies were deployed by cybercriminals to avoid being detected. This finding is supported by Chung et al. (2020) who state that cybercriminals are avoiding the traditional phishing tricks, but are developing innovative techniques, such as social media phishing and pop-up adverts, to attract victims. Parker and Flowerday (2020) highlight the ways in which social engineering techniques have developed; cybercriminals can manipulate the human in order to get all the information they need without hacking any computers. The use of social engineering techniques in phishing is one of the findings of this study. Baillon et al. (2019) support the view raised during the interviews, namely that cybercriminals are coming up with new and creative ways to deceive people; for example, the scams no longer occur through emails alone. This is why Baillon et al. (2019) advise individuals to keep on educating themselves about phishing and scamming attacks.

The next research question focused on the effects of phishing attacks on students. Participants referred to a loss of productivity, damage to computers through malware, data loss, financial losses, being a victim of credit card fraud, identity theft and cyberbullying. Once someone falls victim to a phishing attack, they are likely to suffer negative effects (Reis & Alturas, 2020). Nmachi and Win (2021) explained how identity theft is one of the most severe phishing effects since it is central to our existence. For example, people use IDs to open accounts and conduct many transactions that require IDs. The research results described how two of the participants became victims of identity theft and the effects (monetary loss) because their identity details were exposed. Alkhalil et al. (2021) explain how phishing can destroy reputation as victims' details are used to commit fraud, engage in online bullying, and to distribute pornographic content on work and learning platforms.

In relation to the last research question, participants proposed a number of interventions in order to mitigate phishing attacks. For example, taking extra steps to understand how phishing works is an ideal way to identify a phishing attack (Breakstone et al., 2021). As cybersecurity attacks are constantly evolving, it is evident that continuous awareness becomes vital to help people understand cybersecurity threats and be more vigilant while surfing online (Yanakiev et al., 2020). Oest et al. (2020) argue that browser-based phishing detection on web browsers should be mandatory for everyone operating online. Phishing detection software can be efficient for students since it identifies and warns the user of potential phishing attacks (Arshad et al., 2021). The findings show that some participants are very aware of phishing detection software, but other participants have no idea what those are. People should take the initiative to understand how phishing works and raise awareness amongst the community members (Signh & Meenu, 2020). In a study by Ali (2019), it is stated that people should report any phishing emails or attacks they encounter to assist the algorithm to block such attacks immediately. Zhu (2020) agrees that the installation of firewalls and malware protection on students’ computers can block malicious links and spoofed websites and alert the user of any suspicious activities.

Chigada and Madzinga (2021) explain how hackers have used spoofing to manipulate targeted victims to donate bitcoins because these victims thought that the emails were coming from the WHO. To avoid this type of scam, people are advised to always navigate to the original site on their browser rather than just clicking on a link in the email (Chigada & Madzinga, 2021). In the findings, participants say that educating oneself on how to identify phishing attacks is important in combating phishing and scamming threats. Yanakiev et al. (2020) agree and recommend that frequent awareness campaigns and cybersecurity courses should be provided for the student community and society at large to help them identify phishing attacks. Similarly, Abukari and Bankas (2020) say that security awareness programs are key to educating and training people to equip themselves in identifying potential threats that might emanate from working from home. Threat actors have been highly motivated since the beginning of the COVID-19 pandemic, and they are constantly improving their scamming methods (Khan et al., 2020).

Implications

Despite the negative effects of phishing attacks, there have not been reports of wide-spread damage on the university community as a whole. However, the findings from this study are a clear sign that people should not be caught unaware. Everyone should be vigilant and should constantly check the communications they receive on their devices, specifically portable devices (Yanakiev et al., 2020).

Implications for Research

This study has affirmed that phishing and scamming attacks are prominent types of cybercrime. This study has created the foundation on which future research could be undertaken using a large sample size. The views obtained from one university are not necessarily a reflection of events occurring at other universities; future research could determine what is happening at other institutions and comparative studies could be carried out. Hence, future research could be undertaken involving large samples and multiple data sources to enhance the reliability and validity of the findings. The results of the study can be further validated with other universities by examining the factors that expose students and staff members to phishing attacks. In addition, targeted campaigns underpinned by robust theories could be carried out to raise awareness among students and staff about phishing attacks and other forms of cybercrime. Given the exponential growth of cybercrimes, universities should embark on continuous technical improvements to counter evolving and innovative phishing attacks. Lastly, this study advocates for reviews of policy for institutions of higher learning to enhance existing interventions.

Implications for Practice

This study has many implications for students, academics, and all other university staff. Firstly, it emerged from the findings that participants found it useful to be well-educated regarding the subject of phishing and scamming so as to be able to counter phishing attempts. Students should regularly attend seminars, events, and awareness campaigns held at their institutions to learn about the continuous evolvement of phishing. Students and staff should educate themselves about phishing attacks and also pressure their universities to include cybersecurity modules in a curriculum that would be accessible to all. Hence, this study advocates for ongoing education and awareness within the university community as this can make a huge impact towards reducing the total number of victims.

Secondly, the findings show that technical and non-technical preventative measures, if used properly, can be effective to mitigate the numerous existing phishing and scamming attacks aimed at students. Most participants recommended the use of anti-virus software, spam filters, and two- or multifactor authentication to assist them in preventing some of the attempts that might lead to being victims. Therefore, this study recommends students install and activate these tools to reduce the level of susceptibility to phishing and scamming attacks while studying online. Students should ensure that their preventative software applications are regularly updated with the latest features as this will reduce the success rate of new and more sophisticated phishing attacks by cybercriminals.

Thirdly, participants revealed that they were not able to identify or detect phishing and scamming attacks as quickly as possible which resulted in some of them being victims. This study recommends that students learn from existing literature on phishing attacks, types of phishing and how they are perpetrated in order to have some knowledge of phishing attacks. This might help an average student develop skills to identify phishing attacks. Students should look out for domain errors whenever they receive emails and SMSs that redirect them to a website. These errors are very common in phishing attacks. For example, an email from your local bank account might be missing a letter in the domain name or URL, this should be where your doubts are raised; it is also advisable to navigate to the actual domain through your browser to confirm the error. Most companies use their company names as domain names therefore, if you receive an email with a Gmail domain name claiming to be from a well-known company that is probably a scamming attempt. Students should read through the whole email or message and decide if it makes sense. One should check for no grammatical errors because the occurrence of these errors should raise your suspicions regarding the legitimacy of the sender of this email and it should prompt you to investigate whether it might be a phishing attempt. Students should scrutinize the attachments and links that they receive in their inboxes; one should not install software attachments without one hundred percent assurance as to who has sent them. If there are links requiring students to click to navigate to a particular website where they need to input sensitive information, they should always visit the site using the search bar of a browser, never use the link provided.

In most phishing attempts a sense of urgency is created to pressure the targeted individuals to act quickly and without checking. Hence, if you identify a coercive tone in the message or email you should be suspicious. The urgency is created in different ways, however; mostly one will be rushed to login in into the given account to pay a certain amount that is due or to get a bargain while it is available, or to provide sensitive information. Cybercriminals usually build their mimicked websites in a rush and, hence, the sites do not look as professional as those of the actual company. They may use poor resolution images and the functionality is limited. Thus, students should ensure they carefully assess the website design before they interact with it. Lastly, URLs are useful when identifying unsecured and potentially phishing websites. Instead of the typical "https://" prefix, which signifies a secure site, phishing websites frequently use the "http://" prefix. Furthermore, the spelling of a phishing website's URL will typically differ in small ways from that of the company it purports to represent.

Limitations of the Study and Future Scope

Various limitations were encountered in this study due to the COVID-19 social distancing protocols as the movement of people was restricted. Data were collected from only eight participants who were reachable at the time of the study and those participants were from different universities within the Western Cape province. Therefore, the findings in this study do not reflect the views and experience of students outside the sample. For future research, the researcher recommends further investigations into phishing susceptibility amongst students and ways that would assist in designing stronger and self-learning anti-phishing security systems.

CONCLUSION

This study focused on identifying factors that exposed students to phishing and scamming attacks on the Internet while studying from home during the Covid-19 pandemic. Phishing and scamming attacks remain a dominant cybersecurity threat against individuals and organizations. The most clearly identified themes in this study showed that human naivety and vulnerability are the main drivers for the increased susceptibility of phishing and scamming attacks. Students' experiences and perspectives were that phishing attacks were difficult to identify and avoid because they were perpetrated using complex strategies. It has been identified that using unsecured Wi-Fi networks, constant use of computers, malicious websites, opening links or attachments from suspicious senders, and many other factors expose students to the dangers of being phished or scammed. In addition to previously known phishing mediums, such as emails and the web, it has emerged that cybercriminals are constantly inventing new phishing approaches using SMS, voice messages and social media to scam students while the goal remains unchanged. Furthermore, studying from home has increased the chance of students becoming victims due to the amount of time they spend studying online and the large number of emails they receive. Consequently, the key contributions of this study were to provide insights on how phishing attacks have developed, ranging from obtaining sensitive information and user credentials to damaging reputation, cyber-bullying, identity theft, disrupting online lectures and perpetrating financial crimes targeting students. In addition, the study made recommendations for students to take proactive actions against malicious email messages. Students' perspectives and experiences demonstrate the need for training and education programs for society regarding phishing attacks. Universities have a duty to ensure that corporate networks have security protocols and controls in place to guard against external intrusive emails that find their way to students' computers that are connected on the university' server.

REFERENCES

Abukari A. M., & Bankas E. K. (2020). Some cyber security hygienic protocols for teleworkers in Covid-19 pandemic period and beyond. *International Journal of Scientific & Engineering Research*, *11*(4), 1404-1407.

Aiken, A. (2020). Zooming in on privacy concerns: Video app Zoom is surging in popularity. In our rush to stay connected, we need to make security checks and not reveal more than we think. *Index on Censorship*, *49*(2), 24-27. https://doi.org/10.1177/0306422020935792

Aleroud, A., Abu-Shanab, E., Al-Aiad, A., & Alshboul, Y. (2020). An examination of susceptibility to spear phishing cyber-attacks in non-English speaking communities. *Journal of Information Security and Applications, 55,* 1-15. https://doi.org/10.1016/j.jisa.2020.102614

Ali, G. A. (2019). September. Phishing email: Could we get rid of it? A review on solutions to combat phishing emails. In Saeed, F., Mohammed, F., Gazem, N. (Eds). *Emerging trends in intelligent computing and informatics. IRICT 2019 advances in intelligent systems and computing* (Vol. 1073, pp. 849-856). Springer. https://doi.org/10.1007/978-3-030-33582-3_80

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: Recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 1-23. https://doi.org/10.3389/fcomp.2021.563060

Alwanain, M. (2019). An evaluation of user awareness for the detection of phishing emails. *International Journal of Advanced Computer Science and Applications 10*(10), 323-238.

Anastasiou, A., Androutsou, T., Costarides, V., Pitoglou,S., & Giannouli, D. (2020). *Cybercrime and Private Health Data: Review, current developments, and future trends*. IGI Global. https://doi.org/10.4018/978-1-6684-6311-6.ch047

Anti-Phishing Working Group. (2018). Phishing activity trends report, 2nd Quarter 2018. https://apwg.org/trendsreports/

Arshad, M., Khem, C., Yan, B., & Ouk., S. (2021). Evaluation of GPM-IMERG and TRMM-3B42 Precipitation Products over Pakistan. *Atmospheric Research, 249,* Article 105341. https://doi.org/10.1016/j.atmosres.2020.105341

Atimorathanna, D. N., Ranaweera, T. S., Pabasara, R. D., Perera, J. R., & Abeywardena, K. Y. (2020). NoFish; total anti-phishing protection systems. *In Proceedings of the 2nd International Conference on Advancements in Computing* (ICAC). (Vol. 1, pp. 470-475). IEEE. https://doi.org/10.1109/ICAC51239.2020.9357145

Baillon, A., De Bruin, J., Emirmahmutoglu, A., Van De Veer, E., & Van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. *PloS One*, *14*(12), 1-15. https://doi.org/10.1371/journal.pone.0224216

Benavides, E., Fuertes, W., Sanchez, S., & Sanchez, M. (2020). Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review. In A. Rocha & R. Pereira (Eds.), *Developments and advances in defense and security. Smart innovation, systems and technologies*, (Vol 152, pp. 51-64). Springer. https://doi.org/10.1007/978-981-13-9155-2_5

Binks, A. (2019). The art of phishing: Past, present and future, *Computer Fraud & Security, 2019*(4*).* https://doi.org/10.1016/S1361-3723(19)30040-5

Birlea, M. C. (2020). *Phishing attacks: Detection and prevention*. ArXiv. https://doi.org/10.48550/arXiv.2004.01556

Bowen, S. M., & Seth, G. (2020). *What was it that got me into Cyber*? LinkedIn. https://www.linkedin.com/in/smbowen

Breakstone, J, Smith, M., Wineburg, S., Rapaport, A., Garland, M., & Saavedra, A. (2021). Students' civic online reasoning: A national portrait. *Educational Researcher*, *50*(8), 505-515. https://doi.org/10.3102/0013189X211017495

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2020). *Phishing risks in a university student community* (Trends & issues in crime and criminal justice no. 587). Australian Institute of Criminology. https://doi.org/10.52922/ti04251

Bryman, A. (2017). *Quantitative and qualitative research: Further reflections on their integration*. Routledge.

Burns, A. J., Johnson, M. E., & Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 24-39.

Chang, L., & Coppel, N. (2020). Building cybersecurity awareness in a developing country: Lessons from Myanmar. *Computers & Security*, *97*, 1-10. https://doi.org/10.1016/j.cose.2020.101959

Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, *133*, 113-287.

Chigada, J. (2023). *Towards an aligned South African National Cybersecurity Policy Framework* [Doctoral dissertation, University of Cape Town]. OpenUCT. http://hdl.handle.net/11427/38253

Chigada, J. (2020). A qualitative analysis of the feasibility of deploying biometrics authentication systems to augment security protocols of bank card transactions. *South African Journal of Information Management*, *22*(1), 1-9. https://doi.org/10.4102/sajim.v22i1.1194

Chigada, J., & Daniels, N. (2021). Exploring information systems security implications posed by BYOD for a financial services firm, *Business Information Review*, *38*(3), 1-12. https://doi.10.1177/02663821211036400

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1), 1-11. https://doi.org/10.4102/sajim.v23i1.1277

Choi, J., Kruis, N. E., & Choo, K. S. (2021). Explaining fear of identity theft victimization using a routine activity approach. *Journal of Contemporary Criminal Justice*, *37*(3), 406-426. https://doi.org/10.1177/10439862211001627

Choudhary, N., Jain, A.K. (2018). Comparative analysis of mobile phishing detection and prevention approaches. In Satapathy, S., Joshi, A. (eds). *Information and communication technology for intelligent systems (ICTIS 2017*): *Vol. 1*. *Smart Innovation, Systems and Technologies* (83). Springer. https://doi.org/10.1007/978-3-319-63673-3_43

Chung, J., Koay, J. Z., & Leau, Y. B. (2020). A review on social media phishing: Factors and countermeasures. In M. Anbar, N. Abdullah & S. Manickam (Eds.), *Advances in cyber security. ACeS 2020. Communications in computer and information science*, (Vol. 1347, pp. 657-673). Springer. https://doi.org/10.1007/978-981-33-6835-4_43

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approach*. Sage Publications.

Dawood, M., Ibrahim, O. B., & Abu-Ulbeh, W. A. R. A. (2019). Enrich awareness of users to detect phishing websites. *International Journal of Engineering and Advanced Technology*, *8*(63), 648-650. https://doi.org/10.35940/ijeat.F1119.0986S319

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., & Ponnet, K. (2018). You’ve got mail! Explaining individual differences in becoming a phishing target. *Telematics and Informatics*, *35*(5), 1277-1287. https://doi.org/10.10106/j.tele.2918.02.009

Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behaviour. *Cryptologia*, *44*(1), 53-67.

Eigbrecht, L., & Ehlers, U. D. (2020). Students’ perspectives and strategies on studying at home in times of Covid-19 learnings from podcast conversations and an online survey. In *Proceedings of European Distance and E-Learning Network Conference*, (Vol. 2, pp. 21-30). European Distance and E-Learning Network.

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, *62*(1), 107–115. https://doi.org/10.1111/j.1365-2648.2007.04569.x

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1-4. https://doi.org/10.11648/j.ajtas.20160501.11

Fang, Y., Zhang, C., Huang, C., Liu, L., & Yang, Y. (2019). Phishing email detection using improved RCNN model with multilevel vectors and attention mechanism. *IEEE Access*, *7*, 56329-56340. https://doi.org/10.1109/ACCESS.2019.2913705

Ference, S. B. (2017). The armor of awareness. *Journal of Accountancy*, *223*(3), 1-3.

Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human-Computer Studies*, *125*, 19-31. https://doi.org/10.1016/j.ijhcs.2018.12.004

Floderus, S., & Rosenholm, L. (2019). *An educational experiment in discovering spear phishing attacks* [Bachelor's thesis, Blekinge Institute of Technology]. Digitala Vetenskapliga Arkivet.

Fuchs, C. (2021). *Social media: A critical introduction*. Sage.

Guarda, T., Augusto, M. F., Lopes, I. (2019). The art of phishing. In Á. Rocha, C. Ferrás & M. Paredes (Eds.), *Information Technology and Systems*. *Proceedings of ICITS 2019*. *Advances in Intelligent Systems and Computing* (918). Springer. https://doi.org/10.1007/978-3-030-11890-7_64

Gomes, V., Reis, J., & Alturas, B. (2020). Social engineering and the dangers of phishing. In *Proceedings of the 15th Iberian Conference on Information Systems and Technologies (CISTI)*, (pp. 1-7). IEEE. https://doi.org/10.23919/CISTI49556.2020.9140445

Gupta, P., & Singh, A. (2021). Phishing website detection using machine learning. In S. Fong, N. Dey & A. Joshi (Eds.), *ICT analysis and applications. Lecture notes in networks and systems,* (Vol. 154, pp. 183-192). Springer. https://doi.org/10.1007/978-981-15-8354-4_19

Guo, Z., Cho, J. H., Chen, R., Sengupta, S., Hong, M., & Mitra, T. (2020). Online social deception and its countermeasures: A survey. *IEEE Access, 9,* 1770-1806. https://doi.org/10.1109/ACCESS.2020.3047337

Hamman, S. T., Hopkinson, K. M., Markham, R. L., Chaplik, A. M., & Metzler, G. E. (2017). Teaching game theory to improve adversarial thinking in cybersecurity students. *IEEE Transactions on Education*, *60*(3), 205-211. https://doi.org/10.1109/TE.2016.2636125

Henry, A., & Shellenbarger, T. (2020). To zoom or not to zoom? Choosing a videoconferencing platform. *Nurse Author & Editor*, *30*(4), 30-34. https://doi.org/10.1111/nae2.9

House, D., & Radu, E. (2020). VPN usage in higher education: A study to mitigate risk related to public Wi-Fi usage. In *Proceedings of Information Security and Privacy*, (pp. 1-4). Association for Information Systems.

Iyengar, K., Mabrouk, A., Jain, V. K., Venkatesan, A., & Vaishya, R. (2020). Learning opportunities from COVID-19 and future effects on health care system, *Diabetes Metab Syndr*, *14*(5), 943-946. https://doi.org/10.1016/j.dsx.2020.06.036

Kabir, S. M. S. (2016). Methods of data collection: In *Basic guidelines for research: An introductory approach for all disciplines* (1st ed.) Book Zone Publication.

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). *Ten deadly cyber security threats amid COVID-19 pandemic*. TechRxiv. https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792

Lawal, A., & Cavus, N. (2019). Detection and prevention of social media cybercrime among students. In *Proceedings of the 11th Annual International Conference on Education and New Learning Technologies,* (pp. 3773-3779). IATED Digital Library. https://doi.org/10.21125/edulearn.2019.0977

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *All Ireland Journal of Teaching and Learning in Higher Education*, *8*(3), 3351-33514. http://ojs.aishe.org/index.php/aishe-j/article/view/335

McAlaney, J., & Hills, P. J. (2020). Understanding phishing email processing and perceived trustworthiness through eye tracking. *Frontiers in Psychology*, *11*, 1-13. https://doi.org/10.3389/fpsyg.2020.01756

Miller, B., Miller, K., Zhang, X., & Terwilliger, M. G. (2020). Prevention of phishing attacks: A three-pillared approach. *Issues in Information Systems*, *21*(2), 1-8. https://doi.org/10.48009/2_iis_2020_1-8

Nmachi, W. P., & Win, T. (2021). Mitigating phishing attack in organisations: A literature review. *In CS & IT Conference Proceedings*, *11*, (1), 75-83. https://doi.org/10.5121/csit.2021.110105

Oest, A., Zhang, P., Wardman, B., Nunes, E., Burgis, J., Zand, A., Thomas, K., Doupé, A., & Ahn, G. J. (2020). Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In *Proceedings of the 29th Usenix Security Symposium*, (pp. 361-377). https://www.usenix.org/conference/usenixsecurity20/presentation/oest-sunrise

Parker, H. J., & Flowerday, S. V. (2020). Contributing factors to increased susceptibility to social media phishing attacks. *South African Journal of Information Management*, *22*(1), 1-10. http://doi.org/10.4102/sajim.v22i1.1176

Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies*, *128*, 17-26. https://doi.org/10.1016/j.ijhcs.2019.02.007

Pham, H. H., & Ho, T. T. H. (2020). Toward a 'new normal'with e-learning in Vietnamese higher education during the post COVID-19 pandemic. *Higher Education Research & Development*, *39*(7), 1327-1331. https://doi.org/10.1080/07294360.2020.1823945

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters, 4*(2), 1-6. https://doi.org/10.1002/itl2.247

Prasad, R., & Rohokale, V. (2020). Cyber threats and attack overview. In *Cyber Security: The Lifeline of Information and Communication Technology, (*pp. 15-31). Springer. https://doi.org/10.1007/978-3-030-31703-4_2

Raza, S. A., Qazi, W., Khan, K. A., & Salam, J. (2021). Social isolation and acceptance of the learning management system (LMS) in the time of COVID-19 pandemic: An expansion of the UTAUT model, *Journal of Education Computing*, *59*(2), 183–208.

Sahu, P. (2020). Closure of universities due to coronavirus disease 2019 (COVID-19): Impact on education and mental health of students and academic staff. *Cureus*, *12*(4), 1-5. https://doi.org/10.7759/cureus.7541

Seng, S., Kocabas, H., Al-Ameen, M. N., & Wright, M. (2019). Poster: Understanding user's decision to interact with potential phishing posts on Facebook using a vignette study. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, (pp. 2617-2619). Association for Computing Machinery. https://doi.org/10.1145/3319535.3363270

Sharma, G. (2017). Pros and cons of different sampling techniques. *International Journal of Applied Research*, *3*(7), 749-752.

Shaw, C. (2020). *Why phishing works and the detection needed to prevent it* [Master's thesis, Utica College]. ProQuest.

Simonovich, L., (2020, January). *Are utilities doing enough to protect themselves from cyber-attack?*, World Economic Forum. https://www.weforum.org/agenda/2020/01/are-utilities-doing-enough-to-protect-themselves-from-cyberattack/.

Singh, K., Aggarwal, P., Rajivan, P., & Gonzalez, C. (2019). Training to detect phishing emails: Effects of the frequency of experienced phishing emails. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, (Vol. 63, No. 1, pp. 453-457). Sage.

Smit, B. (2002). Atlas.Ti for qualitative data analysis. *Perspectives in Education*, *20*(3), 65-76. https://hdl.handle.net/10520/EJC87147

Stein-Zamir C., Abramson, N, Shoob, H, Libal,E., Bitan, M., Cardash, T., Cayam, R., & Miskin, I. (2020). A large COVID-19 outbreak in a high school 10 days after schools' reopening, Israel, May 2020. *Eurosurveillance*, *25*(29), pii=2001352. https://doi.org/10.2807/1560-7917.ES.2020.25.29.2001352

Sumner, A., & Yuan, X. (2019). Mitigating phishing attacks: An overview. In *Proceedings of the 2019 ACM Southeast Conference*, (pp. 72-77). Association for Computing Machine. https://doi.org/10.1145/3299815.3314437

Tamrat, W., & Teferra, D. (2020, April 9). *Covid-19 poses a serious threat to higher education. University.* University World News. https://www.universityworldnews.com/post.php?story=20200409103755715

UNESCO. (2020, March 4). *290 million students out of school due to COVID-19: UNESCO releases first global numbers and mobilizes response*. https://www.unesco.org/en/articles/290-million-students-out-school-due-covid-19-unesco-releases-first-global-numbers-and-mobilizes

Williams, E. J., & Joinson, A. N. (2020). Developing a measure of information seeking about phishing, *Journal of Cybersecurity*, *6*(1), 1-16. doi:10.1093/cybsec/tyaa001

Yanakiev, Y., Traeber-Burdin, S., & Marble, J. (2020). *Final Report of Research Task Group HFM-259: Human systems integration approach to cybersecurity*. Academia. https://www.academia.edu/43488596/Human_Systems_Integration_Approach_to_Cyber_Security_D%C3%A9marche_dint%C3%A9gration_humain_syst%C3%A8mes_appliqu%C3%A9e_%C3%A0_la_cybers%C3%A9curit%C3%A9_Final_Report_of_Research_Task_Group_HFM_259_Distribution_and_Availability_on_Back_Cover

Zhu, H. (2020). Online meta-learning firewall to prevent phishing attacks, *Neural Computing and Applications*, *32*(23), 17137–17147. https://doi.org/10.1007/s00521-020-05041-z