Int. J. Inf. Sec. manuscript No.
(will be inserted by the editor)

Securing the Remote Office: Reducing Cyber Risks to Remote Working through Regular Security Awareness Education Campaigns.

Giddeon Njamngang Angafor, [a,1], **Iryna Yevseyeva,**[1], **Leandros Maglaras,**[2]

[1]Faculty of Computing, Engineering and Media, School of Computer Science and Informatics, De Montfort University, Leicester, UK
[2]School of Computing, Engineering and the Built Environment, Edinburgh Napier University, Edinburgh, UK

Received: date / Accepted: date

Abstract Cyber security threats, including risks to remote workers, are varied and diverse, with the number of scams and business email compromise breaches increasing. Firms and their staff are experiencing mass phishing attacks, several typical precursors to more sinister attacks like cyber-enabled fraud, ransomware, and denial of service (DDoS) attacks. Threat actors are leveraging new technologies such as machine learning and artificial intelligence (AI) to deliver sophisticated scam and phishing messages that are challenging for users to identify as malicious. Several businesses are increasing technical efforts in critical areas, including network hardening, robust patching, anti-malware, ransomware detection applications, and multi-factor authentication to detect, prevent, and recover from potential threats. Despite that, these measures provide only a partial solution if the users who access the systems do not have good security awareness training. In this study, we review some cyber risks related to remote working and detail how they can be remediated through regular security awareness education campaigns (SAECs). The study presents the results of a proof of concept (PoC) experiment conducted to establish the value of regular SAECs in the fight against scams and phishing attacks against remote workers. The pilot results confirm that securing the remote office requires a robust SAEC. It argues that to be successful and help staff protect business systems and data, SAECs must be regular and varied, providing opportunities for staff to understand what to look for in suspicious scams and phishing emails. Moreover, they must provide opportunities for staff to practice their knowledge and understanding through practical exercises such as spam and phishing simulation exercises, which could help users avoid falling victim to spam and phishing emails.

Keywords Practical-experiential Learning · Working from Home · Remote Working · COVID-19 · Security Awareness Education Campaigns · Cyber Security

1 Introduction

The 2019 coronavirus COVID-19 outbreak challenged governments and public and private corporations and forced individuals to be confined indoors. Global travel reached a standstill, with several governments directing their populations to stay home while most national and international borders were closed. Public institutions and activities that required people to gather in enclosed spaces, such as schools, shops, entertainment facilities, and numerous other businesses, were temporarily closed as a countermeasure to control the rapid expansion of the virus [1]. Several other crisis management strategies were adopted to reduce or contain the spread while continuing with essential operations. Measures like social distancing and lockdowns were introduced to limit person-to-person transmissions. Most businesses took up remote working, which required embedding remote information technology (IT) services to ensure their everyday activities could survive under challenging circumstances and continue to operate virtually. Despite that, some businesses that had invested effort, time, and budget in modern digital remote working equipment still experienced significant rises in cyber-related attacks as a side effect of COVID-19 [1]. The same research maintained that threat actors took advantage of online behavior and trends at the heart of the crisis and used the pandemic as an opportunity to carry out social engineering attacks themed around the subject of

[a]e-mail: giddeon.angafor@my365.dmu.ac.uk

coronavirus to distribute various malware packages to businesses since they were aware of people's interest in the subject of COVID-19. Tasheva in [2] states that malicious actors exploited fears linked to the health crisis, sending fake COVID-19 updates and alarming phishing messages to collect user information or install malware on users' devices. The study highlights that many new Internet users were easy targets as they were not prepared for this threat; besides that, they had not been instructed to face it and had limited knowledge of how to use the Internet safely.

The less technically mature businesses, whose IT set-up did not allow remote working facilities were equally active, with many trying to catch up as they struggled to set up remote-working environments for their staff. Several companies in this category turned to new and existing web or teleconferencing technologies such as Google Meet, FaceTime, Microsoft Teams, and Zoom to contain, eradicate, and recover from the crisis. Several companies hurriedly bought new IT services that would help them adapt to the demand for remote working at speed and scale [3]. Other businesses revamped their physical offices and created policies in a panic to enable employees to work from home, often without spending time and effort on essential preparations such as training or security arrangements. As person-to-person interactions were limited, traditional in-person activities such as classroom and in-person training and development with face-to-face interactions were discouraged. These measures significantly impacted business training departments and education institutions, forcing them to increase their online presence, utilizing virtual applications mainly to provide essential services and keep businesses afloat. Many of these companies rushed their digital transformation, often without thinking through and adopting cyber risk mitigation measures such as reviewing and securing the home networks of their staff and providing security awareness training. Failure to follow these basic security measures made securing their data and systems' confidentiality, integrity, and availability a primary cyber security concern [4, 5].

This paper details some cyber threats to remote workers. It introduces security awareness education campaigns and discusses why they are an essential control to such threats. Moreover, it presents the results of a practical experiment PoC, which uses regular, bite-sized SAECs to deal with scams and phishing, two common corporate cyber security threats to remote workers. The subsequent sections are as follows: Section two presents a background to the study, and Section three discusses the methodology used in the study. In contrast, Section Four presents the literature review results and an overview of the PoC experiment using regular bite-sized incident response (IR) and security awareness education campaigns. In Section Five, we discuss the results highlighting any significant findings from the PoC, while Section Six draws conclusions and indicates the limitations of the study.

2 Background

Several studies [6–8], maintain that the COVID-19 pandemic prompted many organizations to rapidly move to remote and online working, converting their staff from on-premises to remote workforces. The authors in [8] argue that in Germany alone, more firms than ever made provision for their employees to work from home in the wake of the COVID-19 pandemic. A survey carried out between October 2020 to June 2022 established that 2000 German businesses switched from office to home working per month throughout the pandemic. In a similar study of pandemic work-from-home trends in the US, Yang et al. in [9] established that before the COVID-19 pandemic, about 5% of Americans had been working predominantly from home for more than three days per week. However, the situation changed after the pandemic outbreak, with the percentage of remote workers skyrocketing to an estimated 37% of Americans working from home full-time by 2020. In a similar study, both Wang et al. in [10] and Barrero et al. [11] argue that the coronavirus caused about one-third of US workers to shift to remote work, adding that since then, nearly every American who could work from home is doing so now, post the pandemic.

The shift from physical office buildings to home and remote offices often required staff to adapt to new information technologies (IT) systems and applications, with many having to quickly learn and acquire new skills and competencies to be able to meet the demands of the job. A study in [3] highlights this dilemma maintaining that several companies turned to new ways of working. They maintained that these businesses sought to expand their IT systems, networks, and bandwidths quickly to meet the demands of remote working which became the 'new normal,'. Adding that in the rush to implement these services, several firms forgot to factor in appropriate cyber security controls. IT teams may have bypassed their everyday processes and procedures in supporting businesses to make significant changes to enable their staff to work remotely. [3] maintains that doing this could have violated, weakened, or even eliminated their IT and security policies. Sebastian in [6] highlights the same issues, maintaining that businesses struggled to balance flexibility and security for remote work during the pandemic. [6] elaborates that a significant proportion of staff in every country worked from home during the COVID-19 pandemic. Employers might not have accounted for this scale of load on their IT infrastructure, especially their cyber security preparedness.

Quick changes to accommodate the move from offices to homes, especially during the pandemic, were often accompanied by a lack of proper 'work-from-home policies and procedures [12]. Equally, there was no clear guidance to staff and little preparation to deal with the cyber risks related to teleworking, making several businesses easy targets for threat actors. Even before the cyber security loopholes created by the COVID-19 pandemic, cybercriminals and threat actors were already becoming increasingly intelligent, employing sophisticated tools and techniques to attack users. However, since the pandemic and the post-pandemic era, they are taking advantage of the opportunities created by the COVID-19 pandemic, especially staff vulnerabilities and failure to follow recommended cyber security behaviors to perpetrate attacks on users operating remotely. According to [4], the pandemic generated different cybersecurity challenges for businesses due to employees working predominantly from home. Due to this change, many organizations allowed their staff to use their personal computers, relying on their private home networks and other resources such as personal routers and virus protection [10]. Pranggono in [3] and Wang & Alexander in [10] elucidated that by allowing staff to use personal devices for remote work without essential cyber security awareness training or preparation, businesses inadvertently exposed their systems and data to be compromised. Moreover, they left staff open and vulnerable to attacks as their devices lacked corporate networks' cyber security controls and protection. The research adds that staff working remotely would most likely be vulnerable as their security solutions were tailored to individuals instead of enterprise-level solutions that businesses can provide against hacker attacks, especially for sensitive information.

2.1 Research questions

The three specific research questions that this study seeks to answer are outlined below.

RQ1: What are regular security awareness education campaigns?

RQ2: Why are regular SAECs an essential control against threats to remote workers?

RQ3: How can regular SAECs improve the security of remote workers?

To address the research questions posed in RQ1, RQ2 and RQ3, we conducted a literature review and undertook a practical proof of concept experiment to test the proposed approach.

3 Literature Review

A literature search using a 'keyword search strategy was undertaken to enable us to answer both RQ1 and RQ2. The search targeted traditional academic databases and bibliographic sources. Table 1 below provides details of the data collection and systematization process.

The traditional academic and bibliographic database searches produced 146 articles. The team reviewed them first by abstract, followed by a full review for those requiring further analysis to determine their suitability for inclusion. After the full-text review, 58 articles that did not meet the criteria for inclusion were excluded. To be considered for inclusion articles had to be written in English. They also needed to address subjects such as security awareness education, cyber threats, and risks associated with home, remote, or virtual working. The remaining 88 articles were reviewed again. A further 23 were excluded as they did not significantly address the cyber security challenges associated with remote working, how to address such challenges, or security awareness education campaigns. Another 4 were eliminated as they concentrated more on health and safety than cyber security. After a review of the 61 articles left, we discarded 6 more as they dealt with physical security awareness. This left us with 55 articles that were found relevant for inclusion in the paper.

3.1 Security awareness education campaigns (SAECs)

To fully understand what security awareness education campaigns are and why they are seen as an essential control against some cyber risks experienced by remote workers, it is crucial to understand what cyber or information security awareness campaigns are. This definition is an essential first step to enable this study to put into context cyber or information security awareness training campaigns and their purpose(s). Security awareness campaigns or training, also called information security awareness training programs or campaigns [13], is the vehicle for disseminating information that all users, such as employees, including managers, consumers, and citizens, need to help them understand what safe and acceptable digital, online behaviour is. Similarly, Abawajy in [14] proposes that security awareness campaigns mainly focus on raising online end users' cyber security awareness. Both these definitions attest that SAECs are the medium used to communicate security requirements and appropriate

Table 1 Data collection and systematization process.

Item	Description
Research Strings	String 1: ”Working from Home”, ”Virtual Office”, or ”Remote Working.” String 2: ”Cyber Security Threats During COVID-19.” String 3: ”Security Awareness Education Campaigns” or ”SAECs.” String 4: ”Cybersecurity Threats and ”Remote” or ”Home” or Virtual Working.” String 5: ”Securing the Remote Officer” or” Mitigating Cyber Risks from Remote Workers.
Online Databases	IEEE, Elsevier, Emerald Insight, Springer, Google Scholar, ScienceDirect, SCOPUS, Taylor and Francis, WoS. Others include resources from COVID-19 Research Journals, websites, and bibliographies.
Period of Search	December 2022 to February 2023
Area of Research	Security Awareness Education and Cyber threats and Risks. Associated with Home, Remote or Virtual Working.
Language	English
Documents	Articles, Reviews, and Editorials

behaviours for users of information systems. According to the NIST Special Publication 800-16, SAECs or ’Awareness is not training’. It maintains that security awareness campaigns focus users’ attention on security, allowing them to recognise and respond appropriately to security concerns. CybSafe [15] highlights this notion by stating that SAECs help to educate employees on security risks and best practices. They assist them in identifying and responding to potential threats and can help establishments reduce the risk of data breaches, malware infections, phishing attempts, and other malicious activities. For Pattinson et al. [16], security awareness education campaigns are the process of ensuring that ’an individual’s knowledge of, and attitude towards, safe, risk-averse behaviour when using a digital device such as a workstation computer at work, a home laptop, a mobile phone or a tablet device’ is improved. According to these researchers, an essential or defining characteristic of SAECs, highlighted by Kovačević & Radenković (2020), is that they should be treated as a continual process because new attacks constantly appear as new technologies are introduced.

The definition adopted for this paper is that of CybSafe [15], which maintains that SAECs help to educate employees on security risks and best practices. They assist IT system staff and users in identifying and responding to potential threats. They can help establishments reduce the risk of data breaches, malware infections, phishing attempts, and other malicious activities. SAECs are the process followed to ensure that staff or employees develop the ability to understand and seek to avoid actions that an individual may do that would put the confidentiality, integrity, and availability of data and information systems at risk. From this definition, it is apparent that cyber security awareness education campaigns centres around understanding and developing skills in the safe and acceptable use of digital and online services. For this to happen, Bada et al. in [13] contend that developing such understanding and the necessary skills requires a change. They insist that users or staff must be able to understand and apply the advice, and they must be motivated and willing to do so. While these researchers agree that it requires an understanding of and a willingness to apply security awareness knowledge, they insist that staff and users must also see it as their responsibility to protect the confidentiality, integrity, and availability of their data and any systems entrusted to their care.

Moreover, businesses need to ensure that SAECs are conducted regularly to ensure that employees remain up-to-date with the latest security trends and can recognize potential threats to their systems (CybSafe, 2023). Due to the increase in the number and complexity of cyber threats, these researchers hold that it is essential for employees’ knowledge and understanding of the latest security risks and best practices to address them to be constantly improved. The best way to achieve this is through regular SAECs to ensure that employees remain up-to-date with the latest security trends and can recognize potential threats.

3.2 SAECs as an essential control against threats to remote workers

SAECs have been known to play an essential role in organisations’ security. Studies such as CybSafe [15] and Bada et al. [13] support this theory, maintaining that security awareness training is crucial to any business’s security strategy. According to recent research, it helps employees understand the importance of cyber security and teaches them how to identify potential threats and respond appropriately. Besides that, it provides employees with the knowledge and skills needed to identify, report, and prevent security incidents (CybSafe, 2023). Moreover, SAECs are essential in the fight against cyber threats and risks to remote users because threat actors are becoming increasingly sophisticated, employing a range of tools and technologies that have devastating effects on businesses. In addition, as every business's protection depends on its staff, who have been described as the weakest link, [17], it is vital to target the end users. While Kovačević et al. [18] established that some organisations had realised the need to invest in security tools to protect their systems and data, several firms opted primarily for technical protection while overlooking employee security awareness education. This observation is corroborated by Georgiadou et al. [1], who found that businesses that exhibited a better organisational security culture while working from home during COVID-19 concentrated mainly on technical controls. The security guidelines provided by the management of these companies during the coronavirus period focused on corporate network access management issues. They targeted areas such as 'Virtual Private Network (VPN), usage and avoidance of wireless connections' with less or no emphasis on employee awareness of how to protect their asset's safety, such as password protection, locking devices while away from their desk, updating software and guarding against phishing emails [1]. Though alarming, such evidence is not surprising because research by Aldawood & Skinner in [19] found that many organisations know what an excellent cyber security culture is but struggle to implement it. Many end up concentrating too much on technical controls leaving out the human capital cyber security knowledge base vulnerable and susceptible to attack. Given these findings and the fact that there is a significant shift to remote working and that the number of attacks targeting remote workers is growing and likely to increase, employee security awareness must be seen as a priority and not just a 'nice to have' option. Moreso because some studies have argued that although users are aware of the risks in cyberspace, most do not follow best practices, and there is a need for permanent structured training [17].

Another reason SAECs have a pivotal role against cyber threats to remote workers is that most breaches and cyber risks encountered while working remotely, mainly since the advent of COVID-19, are 'human factors' threats. These are threats that rely on human error to be effective. They include attacks that usually rely on a user falling prey to phishing scams by clicking on an Internet or email link. Such threats could be addressed through awareness education, which has been described as 'the first line of defense' [20]. Figure 1 outlines some cyber threats experienced by users during the pandemic that could have been mitigated through SAECs pre- and post-COVID-19.

As illustrated in Figure 1, examples of some human factors or human error cyber-attacks experienced by remote workers during the pandemic and post-COVID-19 were scams, spam, and phishing emails, which threat actors used to target vulnerable users and businesses [3]. Middaugh [21] elaborates that a typical example of these scams was the distribution of phishing emails to hospital employees during the COVID-19 pandemic. She contends that the phishing emails were disguised as crucial information about the COVID-19 virus, often promising personal protective equipment such as N95 masks or lifesaving ventilators for sale. On other occasions, they disguised the messages, making them appear as messages sent by corporate communications from within the business, either containing documents with executable (.exe) files or embedded with malicious links that would install malware or launch an attack once opened or when the reader clicks on them. These threats exploited users' interest in pandemic news to collect their personal data, which was used to commit crimes such as malware distribution, identity theft, and forgeries, often impersonating government agencies and tax entities [22]. Such risks can best be addressed through SAECs because an effective awareness campaign can equip employees to be fully aware of insecure or suspicious links, including what they should do if targeted by potentially suspicious email phishing frauds.

While many of the breaches were caused by failures in various systems and technologies, such as poor coding practices, lack of proper testing, and failure to apply security patches, most were due to human error, which researchers have described as the weakest link [10]. Examples of 'human error' risks that users were exposed to during the pandemic included clicking on links, unsolicited emails from unidentified sources, and using the same password on various websites. Others included downloading free software, such as anti-virus software from unidentified sources, and utilizing free access to public Wi-Fi. Some staff reported downloading digital media such as games, movies, and music from unknown sources and using personal electronics such as laptops, tablets, smartphones, and other removable devices such as USB sticks to store business data or information [10]. While the threats highlighted above are not an exhaustive list of issues experienced by remote workers, it is essential to emphasize that the weakest links are always users, especially staff who access business networks. As such, it is incumbent on businesses to take the necessary steps to implement regular SAECs, ensuring that they train staff to take responsibility for the security of their network and devices [21].

Some studies have insisted that security awareness education and training, especially for remote workers, has always been problematic. For example, Furnell in [23] and Furnell & Shah in [24] highlighted that there

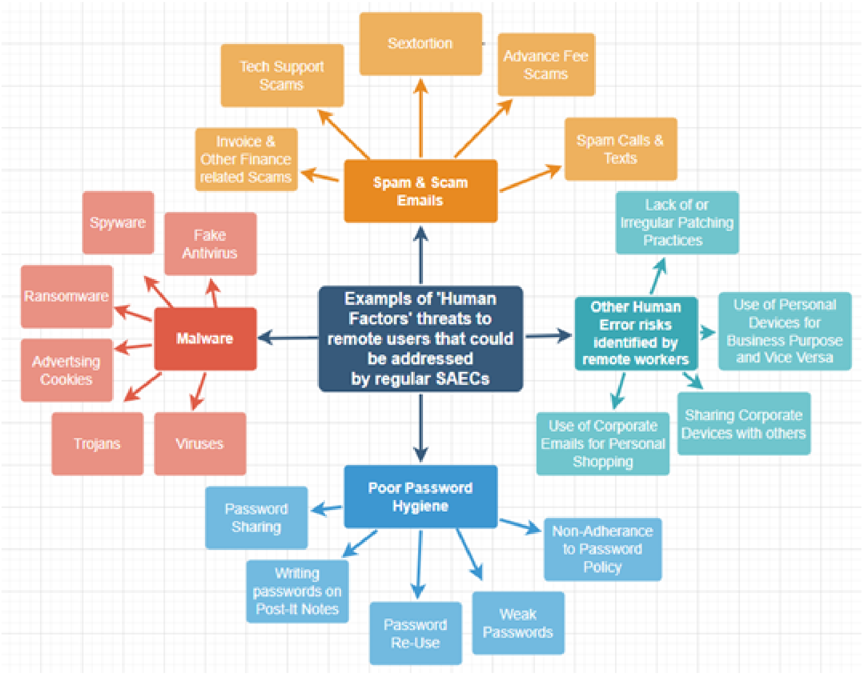

Sextortion
Tech Support Scams
Advance Fee Scams
Invoice & Other Finance related Scams
Spam Calls & Texts
Spam & Scam Emails
Spyware
Fake Antivirus
Lack of or Irregular Patching Practices
Ransomware
Malware
Exampls of 'Human Factors' threats to remote users that could be addressed by regular SAECs
Other Human Error risks identified by remote workers
Use of Personal Devices for Business Purpose and Vice Versa
Advertising Cookies
Trojans
Viruses
Use of Corporate Emails for Personal Shopping
Sharing Corporate Devices with others
Poor Password Hygiene
Password Sharing
Non-Adherance to Password Policy
Writing passwords on Post-It Notes
Password Re-Use
Weak Passwords

Fig. 1 ‘Human factors’ threats that could be addressed through SAECs.

had been shortcomings in user awareness education for remote workers, as it has mostly not been seen as a priority. Despite that, Kovacevic et al. insist in [18] that though there are challenges, as highlighted by Furnell, SAECs are essential because even though employees use computers and the Internet regularly and may be aware of security risks, many are unsure of the measures required to protect the confidentiality, integrity, and availability of information in cyberspace. Using the example of phishing, they argue that even if they have heard about it, some users may not know how to identify and respond appropriately to a targeted phishing email [17]. This argument suggests that SAECs are essential in teaching users tools and techniques to reduce cyber security organisational risks.

As this study confirms SAECs are essential in the fight against cyber threats, especially those related to remote workers. They help employees gain knowledge and develop skills to recognize, report, and prevent security incidents. As such, they must be regular and have staff buy-in, designed to be simple and practical, enabling users to understand and build the skills and aptitudes required to spot and avoid cyber risks. That explains why Middaugh in [21] insists that SAECs should assist staff in discriminating between less cautious users (”clickers”) and more cautious ones, who do not to click on anything without verifying the sender or checking to see if the link is legitimate. This is because most phishing emails may seem to come from a reputable source. However, if reviewed carefully, users who have adequate training can pick up clues of phishing emails or scams, such as grammatical mistakes and embedded hyperlinks, which identify them as fake or suspicious.

4 Regular SAECs proof of concept (PoC) experiment

This section of the paper summarises the results of the PoC experiment.

To answer the RQ3, we carried out a range of experiments as part of a PoC, beginning with a survey, followed by 2 awareness campaigns made up of a practical ’show and tell’ session, a security awareness communicating newsletter, followed by 3 spam and fishing simulation tests.

Participants for the experiment were selected from across 5 small to medium-sized businesses, most of whom worked predominantly from home. A proportion was classed as ’hybrid’ though they stated that they have only visited the office on one or two odd occasions since the COVID-19 pandemic. Participants were drawn from different departments within the participating business. They came from the Human Resources (HR), Service

Desk, IT Support, Finance, and Learning and Development.

Scholars have employed various methods and strategies to avoid bias, which Siadati et al. in [25] argue can exist in all research. We maintained the same participants in all 3 exercises to avoid potential biases. This bias reduction strategy aligns with the “counterbalance schedule” approach to avoiding bias in research put forward by Siadati et al. [25], which suggests that academic bias can be reduced by maintaining the same participant demographics throughout a research project. In the context of the scam and email exercises, we used the same teams across different departments, with each respondent completing all 3 tests at different intervals. Besides that, we varied the examples in the test to ensure that they differed from the samples shown to the participants during the show-and-tell training.

To measure participants’ knowledge and establish their understanding of security awareness education and participation in SAECs, we started the PoC with a survey. The survey aimed to establish participants’ knowledge and discover some cyber threats they experienced while working remotely. It also sought to establish their knowledge and understanding of spam and phishing messages, whether they can identify spam and phishing, how often they have taken part in SAECs recently, and gauge participants’ views on whether SAECs can improve security awareness.

The ’show-and-tell’ exercise sought to help participants develop skills that would enable them to identify common human factors and threats to remote workers. Risks such as scams and phishing messages often come with embedded malware that, if not discovered, can cause serious security threats.

The final exercise was a series of real-world simulation challenges to help participants practice their knowledge. It also sought to give the research an indication as to whether using regular SAECs with varied and diverse approaches is a novel tactic to address security challenges experienced by remote workers. The detailed description and results of the survey and the 3 simulation tests are discussed in the sections below.

4.1 Results of the survey

Respondents from 6 small to medium-sized businesses answered the call for participation in the experiment. Most participants worked predominantly from home, with a small proportion classed as ’hybrid’. However, they stated that they have only visited the office on one or two odd occasions since the COVID-19 pandemic. The specific business sectors participants came from included Customer Services, with 6 respondents, 12%, and Information Technology, with 20 participants, accounting for 40% of all respondents. 9 respondents, which makes up 18%, came from Local Government and Councils, 5 participants, 10% from the Financial Industry, 8, 16% from the Healthcare Sector and 2 respondents, 4% from the Commercial sector, see Figure 2 for details of business sectors represented in the study.

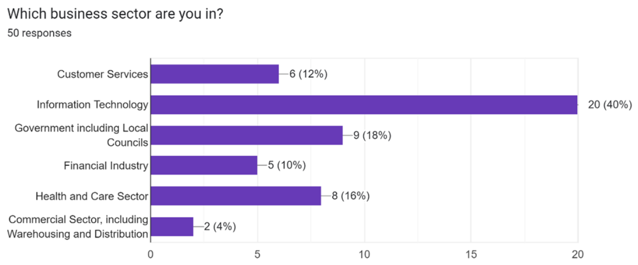


Fig. 2 Industries in which survey respondents work.

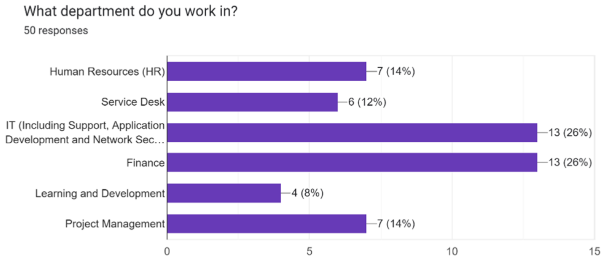


Fig. 3 Number of respondents/department & percentage.

The call for participation was answered by 50 respondents representing different departments across 6 business sectors listed in Figure 2 above. All 50 participants took part in the study from start to finish. They came from Human Resources (HR), the Service Desk, and the IT Department (IT Support, Application Development, and Network Security). Others were from Finance, Learning and Development, and Project Management. The most represented departments were the Information Technology and Finance departments, with 13 respondents each, making a combined total of 52%, followed by Human Resource and Project Management, with 7 participants each and a combined percentage total of 28%. The Service Desk followed this with 6 respondents, 12%, while Learning and Development with 4 respondents, 8%. Figure 3 lists represented departments.

Regarding their qualifications, 28 respondents, 56%, were degree holders, and 11, 22%, had a Masters or Master of Business Administration (MBA). 6, 12% were holders of a Diploma, and 3, 6% had Advanced Level

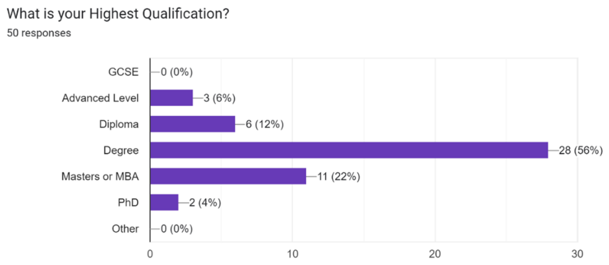


Fig. 4 Number of respondents foe each department and percentage.

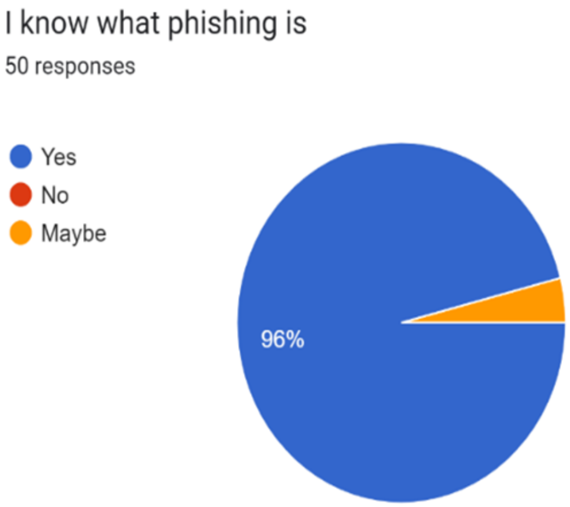


Fig. 5 Percentage of participants who stated they knew what phishing is.

Certificate 2, 4% were holders of a Doctor of Philosophy (PhD) certificate. Figure 4 shows a breakdown of the range of qualifications held by survey respondents .

When asked about their knowledge of phishing, 48 participants, 96%, confirmed that they knew what phishing was, while 2, or 4%, were unsure, see Figure 5.

Regarding their knowledge and understanding of spam, 96% or 48 participants stated that they know what spam and phishing are, which indicates that they could identify and deal with threats spread through these attack vectors. As shown in Figure 6, only 2 participants, making up 4%, were uncertain about what spam and phishing meant.

When asked about their knowledge of social engineering, 42 respondents, 84%, said they knew what it was; 7 participants, 14% of respondents, said they did not know, while 1 participant, making up 2%, said they were unsure, see Figure 7.

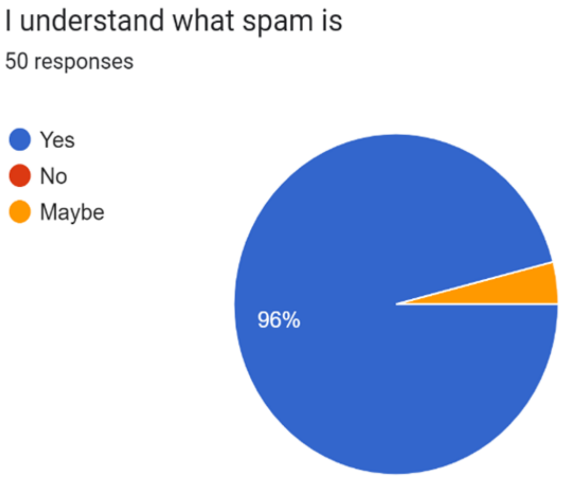


Fig. 6 Percentage of participants who stated that they know what spam is.

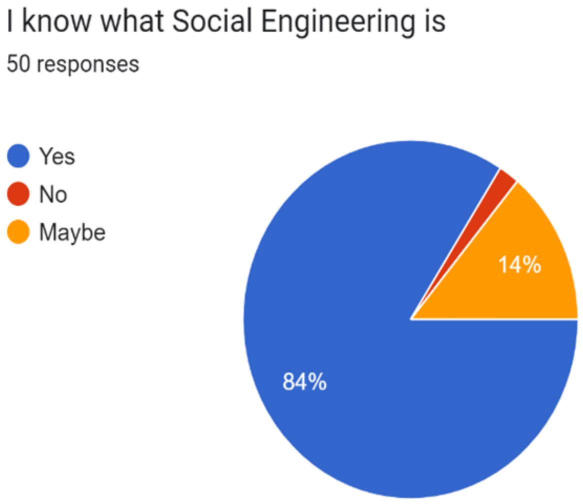


Fig. 7 Percentage of respondents who stated that they know what social engineering is.

Asked about their working mode, 36 respondents, or 72%, stated they were remote workers, in contrast, 13, or 26%, stated they were hybrid workers, while 1 or 2

As shown in Figure 9, out of the 50 responses received, 46 individuals, 92%, answered that they started working remotely during COVID-19. 8%, 4 respondents stated that they had been working remotely before the pandemic.

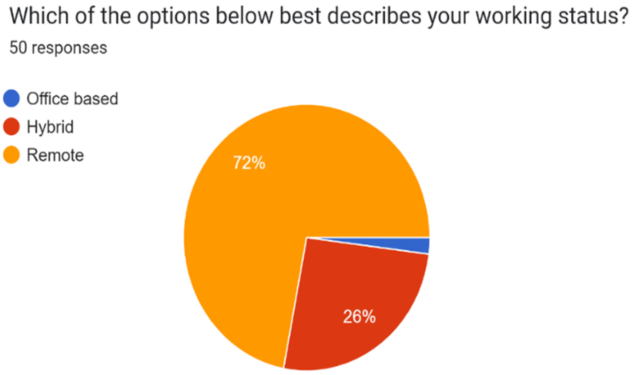


Fig. 8 Working modes of survey participants.

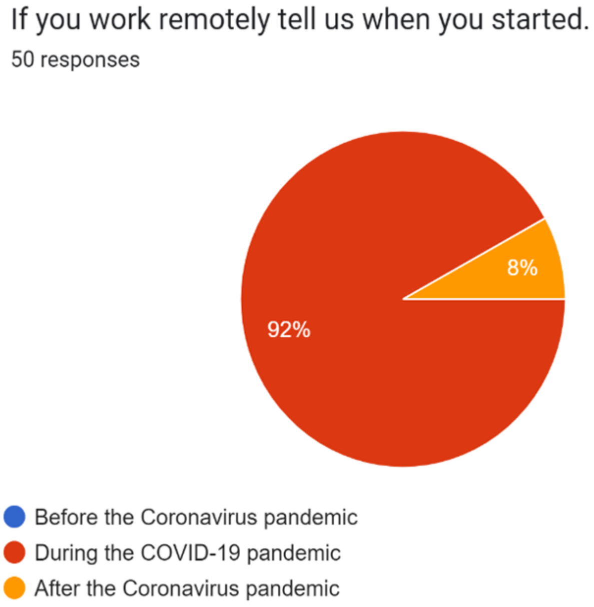


Fig. 9 Starting period of remote working

The next question, see Figure 10, asked participants about their exposure to cyber threats, especially scams and phishing emails, while working remotely. 40 respondents, or 80%, stated they had been targeted with scams and phishing email messages while working from home. These included scam emails requesting payments to release items and those instructing them to click links to enter personal details. 8 respondents, 16%, had been targeted with phishing emails requesting them to click on a link and enter personal details. In comparison, 2 respondents, or 4%, received scam emails about payments for an imaginary parcel.

When asked about their ability to identify scams and phishing emails, 42 respondents, 84%, said they may be able to recognise scams or phishing. In contrast, 7 or 14% responded that they can confidently identify scams and phishing messages, while 1 participant, 2%, stated that they cannot figure out scams and phishing emails, see Figure 11

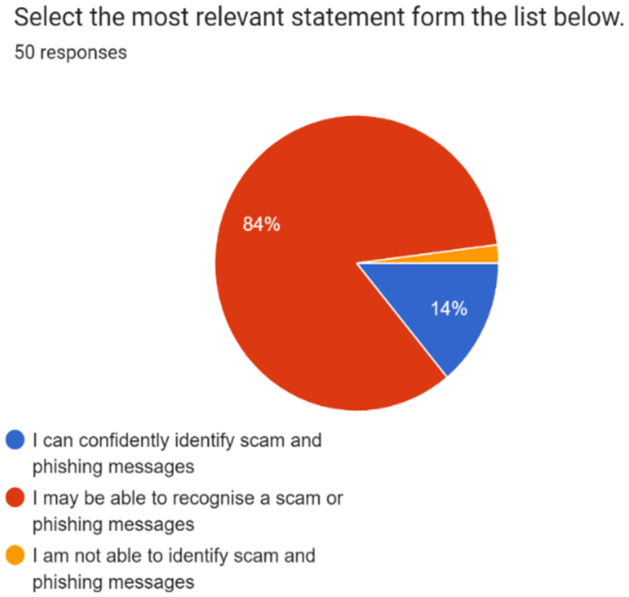


Fig. 10 Types of scams and phishing emails people receive while working from home.

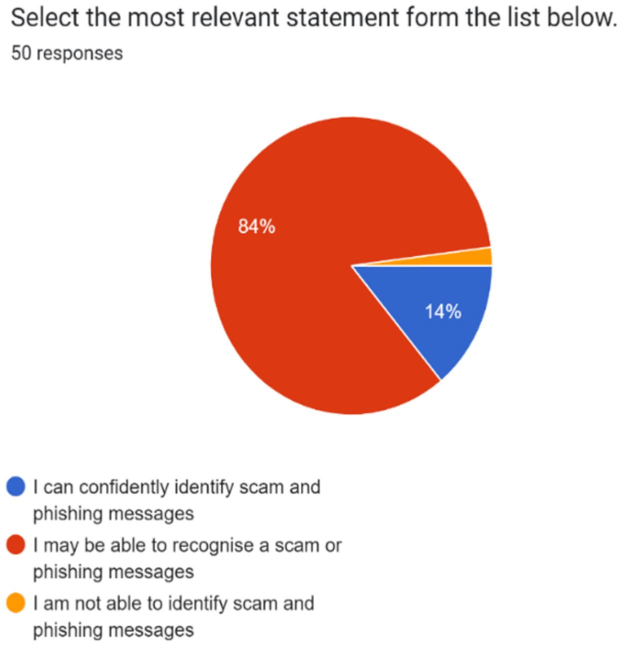


Fig. 11 Participants' ability to recognize scams or phishing emails

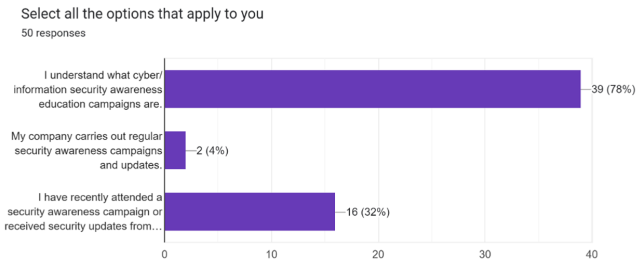


Fig. 12 Security awareness knowledge and participation in awareness campaigns.

When asked about their knowledge and experience of SAECs and security updates, including whether their businesses performed regular SAECs and if they have taken part in one recently, participants responded as follows: 39 respondents, 78%, stated that they knew what SAECs are. However, only 2, or 4%, stated that their organisations performed regular SAECs, while 16, or 32%, maintained that they have recently participated in one. Most of those who had participated in the exercises were from the IT of Financial sectors; see Figure 12.

The final survey question asked respondents if they believed regular security awareness campaigns encouraged users to be cyber security conscious. As evident in Figure 13, 68% or 34 participants, confirmed that they believed regular security awareness education encouraged people to be cyber security aware or conscious about security threats. In contrast, 16 respondents, representing 32%, stated that they did not know if security awareness education campaigns helped people be more conscious about cyber security.

4.2 The 'show and tell' security awareness campaign

Following the initial survey, we scheduled an awareness campaign over Microsoft Teams aimed at helping participants develop their knowledge, understanding and skills in identifying scam and phishing emails. Using a freely available Internet resource, see Figure 14; we 'walked through' an example of a typical scam or phishing email, pointing out key features of scam and phishing messages. The exercise demonstrated to participants how to identify possible spam and phishing emails.

4.3 Security newsletter

Following the show-and-tell session in which participants learned how to identify scam and phishing emails, participants were introduced to another SAEC resource, the Security Newsletter. It contained information and updates on Social Engineering. The newsletter explained social engineering and provided advice and guidance on detecting possible social engineering attacks. Figure 15 shows a screenshot of the security newsletter used in the security PoC exercise.

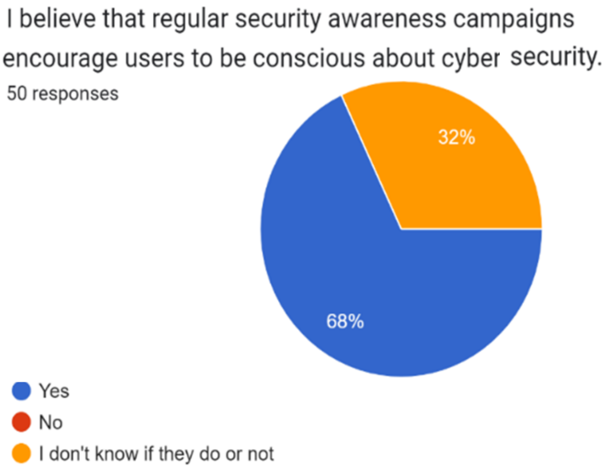
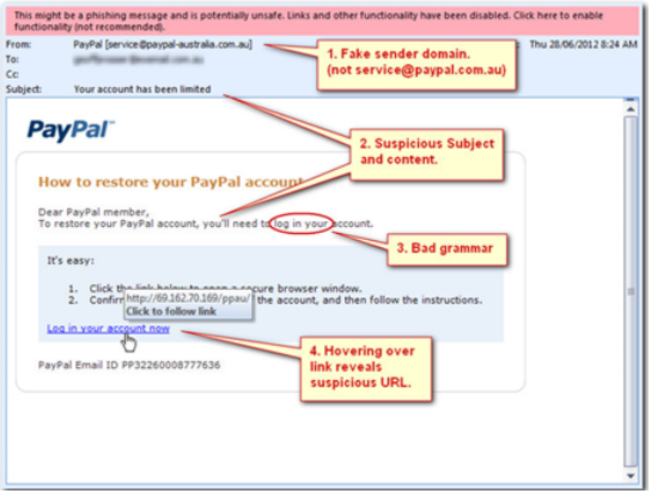


Fig. 13 Do security awareness education campaigns help attendees become more conscious about cyber security?


This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au] Thu 28/06/2012 8:24 AM
To:
Cc:
Subject: Your account has been limited

How to restore your PayPal account

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm the account, and then follow the instructions.

Log in your account now

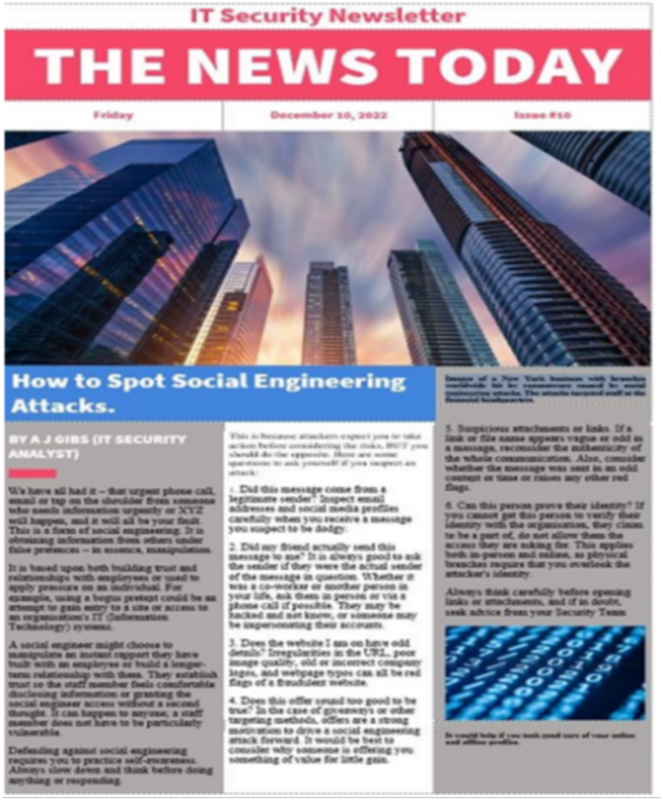
PayPal Email ID PP32260008777636

PayPal
http://69.162.70.169/ppau/
Click to follow link
1. Fake sender domain. (not service@paypal.com.au)
2. Suspicious Subject and content.
3. Bad grammar
4. Hovering over link reveals suspicious URL.

Fig. 14 A screenshot with an example of a phishing email [26].

4.4 Scam and phishing simulation exercises

The final phase of the PoC was a series of phishing simulations deployed to target all participants invited at the start of the study. 3 simulations were deployed over 3 weeks. The authors' choice or preference for phishing trials was informed by studies from Alkhalil et al.



IT Security Newsletter

THE NEWS TODAY

Friday | December 10, 2022 | Issue #10

How to Spot Social Engineering Attacks.

BY A J GIBS (IT SECURITY ANALYST)

We have all had it – that urgent phone call, email or tap on the shoulder from someone who needs information urgently or XYZ will happen, and it will all be your fault. This is a form of social engineering. It is obtaining information from others under false pretences – in essence, manipulation.

It is based upon both building trust and relationships with employees or used to apply pressure on an individual. For example, using a bogus pretext could be an attempt to gain entry to a site or access to an organisation's IT (Information Technology) systems.

A social engineer might choose to manipulate an instant rapport they have built with an employee or build a longer-term relationship with them. They establish trust so the staff member feels comfortable disclosing information or granting the social engineer access without a second thought. It can happen to anyone, a staff member does not have to be particularly vulnerable.

Defending against social engineering requires you to practice self-awareness. Always slow down and think before doing anything or responding.

This is because attackers expect you to take action before considering the risks, BUT you should do the opposite. Here are some questions to ask yourself if you suspect an attack:

1. Did this message come from a legitimate sender? Inspect email addresses and social media profiles carefully when you receive a message you suspect to be dodgy.

2. Did my friend actually send this message to me? It is always good to ask the sender if they were the actual sender of the message in question. Whether it was a co-worker or another person in your life, ask them in person or via a phone call if possible. They may be hacked and not know, or someone may be impersonating their accounts.

3. Does the website I am on have odd details? Irregularities in the URL, poor image quality, old or incorrect company logos, and webpage typos can all be red flags of a fraudulent website.

4. Does this offer sound too good to be true? In the case of giveaways or other targeting methods, offers are a strong motivation to drive a social engineering attack forward. It would be best to consider why someone is offering you something of value for little gain.

Images of a New York business with branches worldwide hit by [illegible] caused by social engineering attacks. The attacks targeted staff at the financial headquarters.

5. Suspicious attachments or links. If a link or file name appears vague or odd in a message, reconsider the authenticity of the whole communication. Also, consider whether the message was sent in an odd context or time or raises any other red flags.

6. Can this person prove their identity? If you cannot get this person to verify their identity with the organisation, they claim to be a part of, do not allow them the access they are asking for. This applies both in-person and online, as physical breaches require that you overlook the attacker's identity.

Always think carefully before opening links or attachments, and if in doubt, seek advice from your Security Team.

It would help if you took good care of your online and offline profiles.

Fig. 15 Screenshot of the security newsletter used in the PoC

[27], which found that phishing emails with links, attachments, and spelling errors are increasingly becoming a primary attack vector. The study submitted that nowadays, phishing is considered one of the most pressing cyber security threats for all internet users, regardless of their technical understanding and how cautious they are. Phishing attacks can lead to severe losses for victims, including sensitive information, identity theft, companies, and government secrets. Al-Qahtani & Cresci in [28] concur that phishing messages that appealed to authority were among the most frequent cyber threats experienced during the COVID-19 pandemic. The theory is supported by Mahadevan [29], who insisted that criminal gangs used phishing emails during the pandemic to attack victims' businesses, especially healthcare organizations. Malicious actors designed emails using logos copied from the World Health Organisation (WHO) website, for example. They used them in fake emails with embedded links and attachments to convince some people they came from authentic senders. This appeal to authority created a sense of trust in victims, making them more likely to click on the links.

The first was a message with suspicious hyperlinks embedded, and the second had a suspicious attachment. The final test was a message with spelling, grammar, and punctuation errors. Table 2 below shows the results of the outcomes of the individual simulation campaigns.

5 Discussion

The survey that kicked off the PoC uncovered several observations. To begin, it highlighted that employees have different levels of knowledge and understanding regarding cyber security. For example, while phishing is relatively well-known and topical, 13.6% of participants were unsure of what phishing was. As strange as it may appear, this discovery aligns with research by Alsharnouby et al. [30], which found that phishing remains a significant threat because users are unaware and cannot verify the authenticity of the links to a website asking for their credentials. Equally, the high number of respondents who indicated that they could identify spam and phishing appeared to suggest that most users could deal with it. Should that be the case, then it is very positive, given that spam and phishing have been described as the most widely used technique that leads to a compromise in cyber security by sending fraudulent emails to users and compelling them to act [31]. While this is encouraging, just having the knowledge or awareness about a specific risk does not mean one has the skills needed to address challenges caused by the threat. Abawajy in [14] corroborated this argument by establishing that though users may be aware of threats such as spam and phishing, they might not have the knowledge and skills to protect themselves against such threats.

A key observation from the survey data is that 16% out of all 50 respondents said they were unsure or did not know about social engineering. The lack of knowledge in this area substantiates the results of a recent study by Sharma et al. [32], which argued that a lack of awareness is among the main factors that lead to successful phishing and social engineering attacks. Because of observations like these, security education and awareness providers like CybSafe (2023) advocate for regular SAECs and maintain that security awareness training is essential for businesses to ensure that their employees are knowledgeable about the latest security threats and best practices.

Another observationis the fact that many respondents also confirmed that they had been targeted by scams and phishing while working remotely. This data corroborates the views of Ahmad [33], who established that coronavirus-themed phishing scams have bombarded people working from home since the pandemic. He maintained that these scams leveraged psychological factors such as fear and the uncertainty surrounding COVID-19, hooking vulnerable people, and taking advantage of

Table 2 Results of the 3 email simulation tests conducted during the PoC, the actions taken by respondents and a breakdown of the numbers.

Type of scam or phishing emails	Participants' response action	Number of respondents
Emails with suspicious links		
	Found and reported the suspicious link	36
	Clicked on the suspicious hyperlink	14
Emails with suspicious attachments		
	Identified and reported attachment	40
	Did not identify or report attachment	10
Emails with spelling and grammar errors		
	Identified spelling and grammar errors	45
	Did not Identify spelling and grammar errors	5

workplace disruption to trick staff with personal information or business secrets.

In a similar study, Price Waterhouse Cooper in [34] advanced that employees working remotely during the pandemic were susceptible to social engineering attacks. They stated that threat actors used phishing attacks crafted to exploit potential alarms around COVID-19 to trick victims into giving away company data and other priced information. The fact that most participants stated their organisations did not offer regular security awareness training and that they had not participated in a SAEC session recently is no surprise.

These statistics align with recent studies such as Furnell in [23], Furnell & Shah in [24], which found that there was a lack of cyber security awareness training for remote workers during the pandemic [12]. They argue that the failure to offer cyber awareness education to staff working remotely during the COVID-19 pandemic will likely increase staff susceptibility to cyber-attacks.

Another observation from the survey is that more than 90% of respondents believed SAECs are essential in building a cyber-conscious culture. This is important because studies like CybSafe [15] insist that businesses should invest in staff security awareness training. They advanced that when employees are provided with the proper security awareness training regularly, it influences them to develop specific security behaviors, ensuring that the business remains secure against cyber threats.

To assist users in understanding and, most importantly, applying knowledge gained from SAECs practically, we employed resources like a newsletter article on social engineering to assist participants in understanding what spam, phishing, and social engineering are. The session used real-life phishing simulation exercises aimed at helping participants apply the knowledge and understanding they have acquired in a practical, real-life scenario. The exercise alerted participants to the growing number of email or text message-based phishing attempts targeting remote users. It urged participants to remain alert to potential spam, phishing emails, or text messages to reduce the business' susceptibility to cyber threats, especially phishing attempts.

The desire to encourage staff to build skills that can help them become more involved in organizational security protection is in line with research by Reegård et al. (2019), who stated that individuals must also take responsibility for maintaining a secure and vigilant culture at work as security should not be seen as solely the responsibility of the IT department. That explains why Ahmad [33] highlighted that spam and phishing posed significant risks to remote workers, especially during and post-COVID-19, when remote working became the norm. The study insisted that helping participants understand and tackle spam and phishing is vital, given that threat actors used COVID-19-related names in malicious file titles or fake hyperlinks to trick users into opening them. Additionally, businesses are responsible for ensuring remote staff know how to detect and react to phishing fraud and other cyber-attacks. The authors in [12] share the same views, maintaining that it is essential for businesses to educate staff, helping them acquire good cyber security skills needed to deal with the cyber challenges of remote working to minimize risks to businesses and their staff.

Additionally, the SAEC PoC provided specific guidance to participants. It used examples like the inconsistencies highlighted in Figure 10 to show participants what to look for in scam and phishing messages. The exercise demonstrated checking for inconsistencies or 'red flags' in email addresses, attachments, and hyperlinks deemed suspicious. The PoC advised that most malicious emails could look legitimate, but there are usually indicators when something is not quite right. Participants were advised to check for spelling and grammatical mistakes, as most generic phishing emails may have incorrect spelling or grammar. Besides that, they should take time to verify if the email originates from an organization they regularly correspond with. If so, they should crosscheck the sender's address against previous emails from the same organization. Participants were taught to be skeptic and ask themselves if they expected an email from the reported sender. For example, they were taught that unless they have registered their work email address with PayPal, they should not receive an email from PayPal asking them to restore an account that they never created. They were also advised to report emails they are unsure about or deem suspicious to IT Support or IT Security for investigation.

The outcomes and results of all three spam and phishing simulation exercises conducted in the PoC have some positive indicators. In the first simulation containing a suspicious hyperlink, 19 out of 25 recruits, 76%, participated in the challenge. 14 out of 19, 73.6%, identified and reported the link as suspicious, while 3, 15.7%, clicked first before reporting it. A further 2, 10.5%, clicked the link but did not report it. In the second simulation with a suspicious attachment as payload, 22, which makes 88% out of 25 participants responded to the challenge. 19, 86% of respondents immediately identified and reported the suspicious attachment. 2 participants, 9% of all respondents, opened the attachment before reporting it as suspicious, while 1, 4% opened but failed to report it. In the last challenge with a spam, phishing message with spelling, grammar, and punctuation errors, 21 participated, making it 84% of respondents. All 21, 100% of participants spotted the spelling, grammar, and punctuation errors and immediately flagged the message as suspected spam or phishing. While the study is relatively small, the high number of respondents who recognized the threats indicates that regular and varied SAECs could effectively control phishing. Equally, the fact that participants gradually got better at identifying and reporting suspicious messages and links indicates that regular, varied, bite-sized SAECs could effectively promote a good security culture for remote workers.

Following on from the observations discussed above, it is clear that despite the minor differences in respondents' attitudes, there was an improvement in the number of participants who could identify and flag potentially malicious messages over time. As the simulations progressed, better spam and phishing detection rates by staff indicate that regular SAECs, especially those with practical examples that enable staff to identify what to look out for, could benefit remote workers. This discovery is significant because, in a study of why awareness campaigns failed to increase awareness amongst employees, Bada et al. in [13] argued that staff needed to find relevance with the training, to accept that information in SAECs is appropriate and understand how to apply it in responding to threats before campaigns can be meaningful to them. In the same light, Aldawood & Skinner in [19] assert that for training to be practical, it has to help employees to develop the skills and aptitudes to recognise, flag, or deal with malicious attempts and potential attacks. Following this research evidence, our PoC sought to make the information meaningful to participants and offered them opportunities to demonstrate their understanding of the knowledge and skills taught through the exercises.

Another positive observation worth emphasizing is that 3 participants, or 15.7% of respondents, in the first test and 2 participants, or 9%, in the second test, reported the link and attachment as suspicious.Recognising and reporting possible breaches by victims is laudable and necessary in building a cyber security culture change within organisations. Users need to recognise that they are essential in the fight against cyber threats. To make this possible, businesses must create enabling environments with policies and procedures that encourage users to report breaches even when they are responsible for the offense.

6 Conclusion and Limitations

This study elaborated on the literature on the changing working conditions of several businesses and their staff since COVID-19. It featured some human factors threats to remote working and highlighted challenges of delivering security awareness education to remote staff pre- and post-COVID-19. The study also recognized the importance of SAECs as a vital control to mitigate some threats that remote workers encounter. It insisted that scams and phishing messages are familiar yet effective threats to remote workers. They should be addressed using standard methods that allow trainees to experience and demonstrate real-time steps to protect the business's data and systems.

Moreover, the study implies that securing the remote office requires a robust SAEC approach that encourages remote staff to be open and transparent, reporting potential or suspicious breaches without fear of being blamed. It concludes that successful SAECs help staff protect business systems and data. To be effective, these awareness campaigns must be regular and varied, providing opportunities for staff to understand what to look for in suspicious scams and phishing emails. Furthermore, it highlights that SAECs must provide opportunities for staff to practice their knowledge and understanding through practical exercises such as spam and phishing simulation exercises, which could help staff to avoid falling victim to such threats.

As this is an initial study, it is essential to point out that it has some limitations, a key one of which is the small number of respondents. The sample size was based on numbers from several small and medium-sized businesses with which the researchers had previously interacted. To improve the study's robustness, it is necessary to widen the scope to include participants from bigger businesses with more significant staff numbers over a prolonged period. Another limitation is that the study concentrated mainly on spam, phishing, and social engineering, just a few of the many common risks remote workers experience regularly. Future studies should widen the scope to involve most, if not all, of the threats highlighted in Figure 2.

Availability of data and materials. The results data/figure in this manuscript have not been published elsewhere, nor are they under consideration by another publisher. The data that support the findings of this study are available on request from the corresponding author.

Declarations

Conflict of interest. The authors declare no competing interests.

Compliance with Ethical Standards The authors declare full compliance with ethical standards. This article does not contain any studies involving humans or animals performed by any of the authors.

References

1. Anna Georgiadou, Spiros Mouzakitis, and Dimitris Askounis. Working from home during covid-19 crisis: a cyber security culture assessment survey. *Security Journal*, 35(2):486–505, 2022.
2. Iva Tasheva. Cybersecurity post-covid-19: Lessons learned and policy recommendations. *European View*, 20(2):140–149, 2021.
3. Bernardi Pranggono and Abdullahi Arabo. Covid-19 pandemic cybersecurity issues. *Internet Technology Letters*, 4(2):e247, 2021.
4. Mohammad Hijji and Gulzar Alam. Cybersecurity awareness and training (cat) framework for remote working employees. *Sensors*, 22(22):8663, 2022.
5. Grigoris Tzokatziou, Leandros Maglaras, and Helge Janicke. Insecure by design: Using human interface devices to exploit scada systems. In *3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015) 3*, pages 103–106, 2015.
6. Glorin Sebastian. A descriptive study on cybersecurity challenges of working from home during covid-19 pandemic and a proposed 8 step wfh cyber-attack mitigation plan. *Communications of the IBIMA*, 2:2–7, 2021.
7. Yahya Lambat, Nick Ayres, Leandros Maglaras, and Mohamed Amine Ferrag. A mamdani type fuzzy inference system to calculate employee susceptibility to phishing attacks. *Applied Sciences*, 11(19):9083, 2021.
8. Christian Kagerl and Julia Starzetz. Working from home for good? lessons learned from the covid-19 pandemic and what this means for the future of work. *Journal of Business Economics*, 93(1):229–265, 2023.
9. Longqi Yang, David Holtz, Sonia Jaffe, Siddharth Suri, Shilpi Sinha, Jeffrey Weston, Connor Joyce, Neha Shah, Kevin Sherman, Brent Hecht, et al. The effects of remote work on collaboration among information workers. *Nature human behaviour*, 6(1): 43–54, 2022.
10. Lidong Wang and Cheryl Ann Alexander. Cyber security during the covid-19 pandemic. *AIMS Electronics and Electrical Engineering*, 5(2):146–157, 2021.
11. Jose Maria Barrero, Nicholas Bloom, and Steven J Davis. 60 million fewer commuting hours per day: How americans use time saved by working from home. *University of Chicago, Becker Friedman Institute for Economics Working Paper*, (2020-132), 2020.
12. Giddeon Njamngang Angafor, Iryna Yevseyeva, and Leandros Maglaras. Scenario-based incident response training: lessons learnt from conducting an experiential learning virtual incident response tabletop exercise. *Information & Computer Security*, 2023.
13. Maria Bada, Angela M Sasse, and Jason RC Nurse. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*, 2019.
14. Jemal Abawajy. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3):237–248, 2014.
15. CybSafe. 7 reasons why security awareness training is important in 2023, Mar 2023. URL `https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/`.
16. Malcolm Pattinson, Marcus Butavicius, Meredith Lillie, Beau Ciccarello, Kathryn Parsons, Dragana Calic, and Agata McCormac. Matching training to individual learning styles improves information security awareness. *Information & Computer Secu-*

rity, 28(1):1–14, 2020.

17. Ana Kovačević and Sonja D Radenković. Sawit—security awareness improvement tool in the workplace. *Applied Sciences*, 10(9):3065, 2020.
18. Ana Kovačević, Nenad Putnik, and Oliver Tošković. Factors related to cyber security behavior. *IEEE Access*, 8:125140–125148, 2020.
19. Hussain Aldawood and Geoffrey Skinner. Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues. *Future Internet*, 11(3):73, 2019.
20. Predrag Tasevski. It and cyber security awareness-raising campaigns. *Information & Security*, 34(1): 7–22, 2016.
21. Donna J Middaugh. Cybersecurity attacks during a pandemic: It is not just it's job! *Medsurg Nursing*, 30(1):65–66, 2021.
22. Mohammed ALotibi and Abdulrahman Abdullah Alghamdi. The effect of applying information security awareness concept of moh employees on cybersecurity department–ministry of health-riyadh. *Journal of Information Security and Cybercrimes Research*, 5(2):144–163, 2022.
23. Steven Furnell, Network Research Group, et al. Securing the home worker. *Network Security*, 2006 (11):6–12, 2006.
24. Steven Furnell and Jayesh Navin Shah. Home working and cyber security–an outbreak of unpreparedness? *Computer fraud & security*, 2020(8):6–12, 2020.
25. Hossein Siadati, Sean Palka, Avi Siegel, and Damon McCoy. Measuring the effectiveness of embedded phishing exercises. In *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)*, 2017.
26. Student guide to phishing: What to do if you click (but don't click!), Aug 2021. URL `https://www.onlineeducation.com/features/student-guide-to-phishing-attacks`.
27. Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3:563060, 2021.
28. Ali F Al-Qahtani and Stefano Cresci. The covid-19 scamdemic: A survey of phishing attacks and their countermeasures during covid-19. *IET Information Security*, 16(5):324–345, 2022.
29. Prem Mahadevan. Cybercrime. *Threats during the COVID*, 2019.
30. Mohamed Alsharnouby, Furkan Alaca, and Sonia Chiasson. Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82:69–82, 2015.
31. Michael JA Miranda. Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, 14(2):5–10, 2018.
32. Pawankumar Sharma, Bibhu Dash, and Meraj Farheen Ansari. Anti-phishing techniques–a review of cyber defense mechanisms. *IJARCCE*, 11(7):153–160, 2022.
33. Ahmad T. Pandemic and work from home: Challenges of cybercrimes and cybersecurity. *Available at SSRN*, 2020.
34. URL `https://www.pwc.nl/nl/themas/assets/pdf/impact-of-covid-19-on-cyber-security-nl.pdf`.

Appendix A: Questionnaire

Security Awareness Education Campaigns
PoC Initial Survey

1. Which business sector are you in?
   (a) Customer Services
   (b) Information Technology
   (c) Government including local councils
   (d) Financial Industry
   (e) Health and care sector
   (f) Commercial sector
2. What department do you work in?
   (a) Human Resources
   (b) Service Desk
   (c) IT
   (d) Finance
   (e) Learning and Development
   (f) Project Management
3. What is your highest qualification?
   (a) GCSE
   (b) Advanced Level
   (c) Diploma
   (d) Degree
   (e) Masters or MBA
   (f) PhD
   (g) other
4. Do you know what phishing is?
5. Do you know what spam is?
6. Do you know what social engineering is?
7. Which one of the following best describes your working status?
   (a) Office Based
   (b) Hybrid
   (c) Remote
8. If your work is remote, when did you start?

   (a) Before COVID'19
   (b) During COVID'19
   (c) After COVID'19

9. Have you been exposed to scams or phishing email threats while working remotely?
   (a) Scam emails
   (b) Phishing emails
   (c) All of the above
10. Select the most relevant statement from the list below
   (a) I can confidently identify scam and phishing emails
   (b) I may be able to recognize scam and phishing emails
   (c) i am not able to recognize scam and phishing emails
11. Select all the options that apply to you.
   (a) I understand what cyber security awareness education campaigns are
   (b) My company carries out regular cyber security awareness education campaigns
   (c) I have recently attended a cyber security awareness education campaign
12. I believe that regular security awareness campaigns encourage users to be conscious of cyber security threats.
   (a) Yes
   (b) No
   (c) Don't Know