UNIVERSITY OF TARTU
Institute of Computer Science
Cybersecurity Curriculum

Temilola Esther Olorunshe

Recognition of Phishing Attacks and its Impact: A Case Study

Master's Thesis (24 ECTS)

Supervisor: Prof Raimundas Matulevicius,PhD

Tartu 2021

Recognition of Phishing Attacks and its Impact: A Case Study

Abstract: A phishing attack is a cyber-attack that uses social engineering to steal sensitive information or plant malware in the target machine. The attack can also serve as a backdoor for an attacker to carry out another cyber attack. Phishing attack has changed within the past years. One can deploy phishing attacks in various ways, such as emails, SMS, calls, etc. As phishers develop ways to improve phishing attacks, these attacks may pass through security technology. Hence, safeguarding against phishing attacks may depend on humans identifying these attacks. This paper studies how to train people to recognise phishing attacks and their impact. The recognition could help to safeguard against an attack because humans will be able to detect these attacks. This thesis used an experimental ATTF (Awareness, Training, Testing, Feedback) approach. Firstly, we have carried out a simulation to know how aware staff is of recognising phishing emails. Next, we have distributed a questionnaire to explore how humans understand phishing attacks. In the last step, we performed a post-simulation to see whether the participants learnt to recognise the phishing attacks. With humans being able to recognise phishing attacks, it reduces the probability of attack victims. In these cases where security technology fails to detect phishing attacks, the human trained to recognise these attacks can identify them and carry out the steps required to safeguard against them. The recognition of phishing is a good practice because of the changes with the phishing attacks. If attackers continue to be creative with their attacks and humans are continuously trained on the trends and indicators of phishing, targets will prevent themselves from being victims of the attack.

Keywords:
Phishing, social engineering, phishing recognition.

CERCS: T120-Systems engineering, computer technology.

Andmepüügirünnakute äratundmine ja nende mõju: Juhtumianalüüs

Lühikokkuvõte:

Andmepüügirünnak on küberrünnak, mis kasutab tundliku teabe varastamiseks või pahavara installeerimiseks sotsiaalset manipuleerimist. Ründaja võib rünnakut kasutada ka süsteemi tagauksena, et korraldada veel küberrünnakuid.Andmepüügirünnak on viimaste aastate jooksul muutunud. Andmepüügirünnakuid saab rakendada mitmel viisil, näiteks meilide, SMS-ide, kõnede jms abil. Kuna andmepüüdjad töötavad välja viise õngitsemisrünnakute parandamiseks, võivad need rünnakud läbida turbetehnoloogia. Seega võib andmepüügirünnakute kaitse sõltuda inimesest, kes neid rünnakuid tuvastab. Selles lõputööds uuritakse, kuidas treenida inimesi ära tundma andmepüügirünnakuid ja nende mõju. Tunnustus võib aidata rünnaku eest kaitsta, sest inimesed suudavad need rünnakud avastada. Selles lõputöös kasutati eksperimentaalset ATTF-meetodit (teadlikkus, koolitus, testimine, tagasiside). Esiteks oleme läbi viinud simulatsiooni, et teada saada, kui teadlik on personal andmepüügimeilide tuvastamisest. Järgmisena oleme välja jaganud küsimustiku, et uurida, kuidas inimesed andmepüügirünnakuid mõistavad. Viimases etapis viisime läbi simulatsiooni, et näha, kas osalejad õppisid andmepüügirünnakuid ära tundma. Kuna inimesed suudavad andmepüügirünnakuid ära tunda, vähendab see rünnaku ohvrite tõenäosust. Sellistel juhtudel, kui turvatehnoloogia ei tuvasta andmepüügirünnakuid, suudab nende rünnakute tuvastamiseks koolitatud inimene need tuvastada ja teha nende eest kaitsmiseks vajalikud sammud. Andmepüügi tunnustamine on hea tava, kuna andmepüügirünnakud muutuvad. Kui ründajad jätkavad loovate rünnakute loomisega ja inimesi koolitatakse pidevalt andmepüügi suundumuste ja näitajate osas, takistavad sihtmärgid ennast rünnaku ohvritetks langevat.

Võtmesõnad:
Andmepüük, sotsiaalne manipuleerimine, andmepüügi tuvastamine

CERCS: T120 Süsteemitehnoloogia, arvutitehnoloogia

Contents

List of Figures

List of Tables

1 Introduction

1.1 Motivation

Over the years, information technology has evolved [Shw16]. With this evolution comes a variety of security threats [Pra16]. Attackers have become creative, and the attack methods have changed over time. As the worth of data and information kept in infrastructure grows, it becomes a target for attack. With the importance of data in infrastructures, there is a need to implement security measures based on possible attacks.

A phishing attack is a cyber-attack that uses social engineering to steal user data such as login details or personal information. It is considered a successful attack when the target trusts the attacker, which is masked as a trusted entity. The user is deceived into clicking malicious links which prompt the installation of malware [Imp20]. This attack is a threat to data confidentiality and can also negatively affect data integrity and availability

The attack can be problematic to an individual or organisation if not detected. This is because, apart from the attack being used to steal sensitive information, it can also lead to another cyber-attack called ransomware, which prevents affected machines from accessing resources. A successful phishing attack negatively affects the confidentiality, integrity, and availability of assets and can lead to reputation damage or financial losses.

1.2 Problem Description

As phishing attacks have changed over time, technical security measures have been put in place to prevent the attack. Some of these include ant-virus tools, anti-malware tools, etc. Nevertheless, attackers become creative, and some of the phishing attacks have been engineered to pass these security implemented tools.

Since the attack is carried out by deceiving humans, safeguarding against the attack if it passes through implemented security tools will have to be done by the people being targeted. In the long run, humans recognising the attack will help them decide how to react to the attack.

1.3 Scope

The scope of the research is limited to how to raise awareness on the attack, its impact and its recognition. However, raising awareness will require discussing the attack, understanding how the attack can be carried out, the impact of a successful phishing attack, how the attack can be recognised and the importance of recognition in safeguarding against the attack.

The paper focuses on raising awareness of phishing attacks, their impact and their recognition based on the case study. This is done to provide a way to safeguard against

the attack. The research is not limited to creating awareness of the attack. However, it is expanded to ensure the awareness created can be applied such that individuals can confirm the ability to identify phishing attacks.

The research applies the ATTF (Awareness, Training, Testing, Feedback) cycle for the case study. This is proposed as a means to improve phishing awareness and recognition by people. We will use the ATTF cycle to train people and test how much they know and recognise phishing attacks and their impacts to find areas for improvement. A simulated attack will be carried out to see if people can recognise the attack. However, during the research, vulnerabilities discovered will be reported to the appropriate personnel in the organisation used for the case study.

1.4 Research Question

This research aims to find a way to raise awareness on phishing recognition using the case study. So the main research question to be answered is: **How to raise people's awareness of phishing attacks and their impacts?** If awareness on the types of attack with the attack methods can be raised and people can be trained to recognise the attack, this will help to prevent the targets from being victims should the phishing attack pass through implemented security tools. Hence, to address the main research question, the following sub-questions will need to be answered:

SQ1 - What are phishing attacks, and how are they executed in different organisations? We will identify the different types of phishing attacks and the methods for which these attacks are carried out.

SQ2-What is the impact of phishing attacks on an organisation's business process? Based on the information collected in SQ1, the impact of the attack can be analysed with information gathered on the attack methods. The company's business process for the case study will also be collected and represented in BPMN. With this, possible risks can be identified in a phishing attack on the business process assets. We will also simulate an attack to come up with practical impacts of the attack on the business process based on the simulation result.

SQ3-How to carry out awareness of the phishing attack in the organisation? After the simulation is carried out, reactions such as clicks or responses are collected. Possible reasons as to why there were victims to the attack will be used to design a questionnaire. The questionnaire will explain the phishing types, attack methods and indicators with pictorial examples. Finally, training will be carried out to create more awareness on improving phishing recognition.

1.5 Research Approach

As people recognising phishing can go a long way in safeguarding from the attack, they need to be trained on recognising the indicators of phishing. In order to improve

knowledge of phishing recognition, the ATTF process cycle can be used (see Figure 1).

The cycle was designed based on the four R's of deep learning (Receive, Retrieve, Rate, Reflect) [Car14]. However, the different stages can also be seen to be similar to core activities described, on how to train people on phishing attacks, in the research by Michael [Mir16]. This cycle will be applied to the selected company for the case study.

Figure 1. Improving Phishing Recognition

- Awareness: This stage involves creating a general awareness of what phishing is, how it is carried out and how to safeguard against it. It could be done in various ways, such as using images, videos, etc., to communicate what people need to be aware of. Creating awareness of phishing will involve sharing ideas on what phishing attacks are and possible ways they can be carried out. The different types of phishing should be discussed so the audience can understand why knowledge of phishing is essential.
- Training: In this stage, the focus is on training on recognizing phishing by looking out for indicators. This will help individuals to identify phishing emails from legitimate emails. The stage differs from the first stage since, within training, the audience can ask questions for clarification.
- Testing: This stage requires testing individuals to apply the knowledge the people have on phishing. This can be done by simulating an attack or using games for results. This stage continues to put people in the position to test the knowledge they believe they have on phishing.
- Feedback: In this stage, feedback is requested from individuals to see why they failed the testing and from individuals who passed the testing to see how they

recognized the attack. This feedback is then used to prepare for the next awareness and training.

1.6 Contribution

The thesis contributes to existing knowledge on protecting against phishing attacks by giving the following results:

1. Proposing a method that can be used to raise awareness. The ATTF cycle is proposed and used to test if it will be reliable for raising awareness on phishing recognition.

2. The case study, its results and lesson learnt contribute to future research on phishing.

1.7 Structure

The remainder of the paper is structured as follows: Chapter 2 gives an overview of past research on phishing attacks. It discusses previous research related to phishing types, the attack methods, and suggested means of preventing the attacks based on existing research. Chapter 3.1 describes the experimental approach used for the study. It gives an overview of how the information is gathered to carry out a phishing attack simulation based on the organisation's assets. Chapter 4 discusses the experimental approach used for the study. Chapter 5 discusses the ATTF usability on carrying out phishing awareness and training to improve phishing recognition. Chapter 6 gives a summary of the entire thesis by answering the research questions, limitations, recommendations for future works, and concludes the research.

2 Literature Review

In this section, an overview of phishing will be discussed, previous related works will be analysed in the literature, and the research gaps will be identified. A systematic review of the previous research work was carried out as most of them discussed **SQ1 - What are phishing attacks, and how are they executed in different organisations?**. In the section, we will also discuss phishing attack methods and suggested countermeasures for the attack.

2.1 Phishing Attack

Phishing is a type of cyber-attack in which fake communication is masked to be received from a trustworthy source to compromise data sources [Cis20]. The goal of the phishing attack is to ensure the target undertakes actions which they usually would not do [Was20]. These actions can lead to sharing personal information with an attacker, who can then use the information to access accounts for which monetary values can be stolen. The attack has been seen to be the primary source of many other cyber-attacks. According to Verizon technical report in 2018, phishing attacks were identified as one of the top threat action varieties of both incidents, and breaches [Ver19]. The report further explains that 32% of breaches were as a result of a successful phishing attack, and 94% of malware delivery was done via email.

The 2018 PhishLabs Trend report stated that some of the ransomware threats of 2017 were delivered through phishing emails [Phi18]. Some of these ransomware threats include Locky, Globeimposter, Jaff, Wannacry Trojan, and Petya/NotPetya. According to Kristen et al., a significant impact on the economy has resulted from phishing attacks as the attack captures credentials and delivers malware which leads to other security breaches [GST18].

Robin and Michael discussed phishing from the sociological point of view and explained how attackers could exploit many targets at the same time by classifying them into segments [GL15]. The research further analysed how the attack can be exploited in three different ways; computational, sociological, and psychological. Nevertheless, phishing attacks have been identified as the most associated with Social Engineering as they disguise as trustworthy sources to acquire victims' personal or private information [SY19].

2.2 Types of Phishing Attacks

As phishing attack depends on its channel, mechanism, and number of targets, it can be categorised based on social engineering, and technical subterfuge [AP20]. Phishing attacks are carried out using social engineering. The attacker uses factors such as fear, urgency, e.tc. to influence victims to carry out actions they usually would not.

There are common phishing types of which its indicators can be detected, such as vishing, SMiShing, link manipulations, spear-phishing e.t.c. However, some of the phishing attacks are carried out using technical subterfuge where tools are set up on a target computer to steal information directly. Some examples of phishing attacks done by technical subterfuge are keyloggers, session hijacking, malware-based phishing, pharming, Trojans, e.t.c. Below is a detailed description of the phishing attack types based on the reviewed literature.

Domain Spoofing

Research by Rabab et al. defined domain spoofing as a phishing attack in which an attacker tricks a victim to visit a fake website masqueraded to look authentic, whereby the victim is prompted to provide sensitive information or install malware on the machine [HRJA19]. In the research, a project was carried out focusing on detecting an attachment file of a phishing website using a decision tree algorithm. An application was designed to detect, identify and block phishing websites and emails leading to phishing websites.

Zuochao et al. explained that the phishing attack is influenced by the social engineering approach performed on a victim and carried out by an attacker in order to harvest the website users' personal information [DKK+17]. According to the research, the attack is carried out in five stages which are reconnaissance, weaponisation, distribution, exploitation, and exfiltration.

The research carried out by Juan, and Chuanxiong defined the domain spoofing attack as a phishing attack in which a phisher provides a link to a victim in order to redirect the victim to a malicious website that has been set up to steal user information and perform business crime [CG06]. They explained that the attack is made by a phisher setting up a counterfeit website that looks legitimate. He then sends many spoofing emails to targets stating to perform some action as the email sender is masked to look like it is being sent from a legitimate source. The victim opens the email, clicks the spoofed hyperlink, and inputs required information; the phisher then proceeds to perform a fraudulent act such as transferring money from the victims' account. Juan and Chuanxiong studied certain features of the hyperlinks embedded in the phishing emails and designed an anti-phishing algorithm called LinkGuard, which helps prevent the attack at the stage of spoofing emails being sent out as LinkGuard detects up to 96% real-time phishing attacks.

According to Dhamija et al., the attack is carried out by directing targets to fraudulent websites and is carried out by a phisher [DTH06]. The research explains the attack is by presenting an impressive presence, which would lead a victim to fail to recognise security measures installed in the web browser. Dhamija et al. concluded three reasons why the attack is successful be; lack of computer system knowledge, visual deception, and bounded attention as the victim fails to pay attention to security indicators of web browsers. Based on the experiment carried out by Dhamija et al. on 22 participants, which involved distinguishing legitimate websites from a total of 20 websites, 23% of

the participants were not aware of browser-based security indicators, which led to 40% of incorrect answers.

Athulya and Praveen described domain spoofing as a phishing attack where the attacker creates a website that is almost identical to the legitimate website in order to deceive a victim, to steal the user's confidential information [AP20]. The research explained that the websites are designed so that a user will be unable to distinguish the fake from the legitimate website. However, this attack can be identified by observing the Uniform Resource Locator (URL). Athulya and Praveen further explained that the phishing attack is successful because many users of the internet fail to inspect the URL of websites being visited, and many also ignore indication of protection provided by the machine used to visit the websites.

According to the phishing activity trends report for July-September, attackers use encryption to deceive victims [APW19]. The report explains that the HTTPS encryption protocol protects many sites used for phishing attacks. This is deceitful, as HTTPS is important on websites that require password protection on accounts.

Email phishing

Daniel et al. explained in an article how email is of great importance in communication for personal matters and business operations [JGST20]. The research explains that the most common phishing attacks are initiated by email phishing, as the attacker attaches links in the email to achieve the goal. Daniel et al. described that the attack is carried out so that an attacker tricks a victim into believing that the email was sent from a legitimate source to persuade the victim into performing certain actions. The attacker can then access the victim's personal information.

According to Imperva, one of the ways the spear-phishing attack begins is by researching the names of various employees of an organisation's marketing department and gaining access to their latest projects. The attacker then poses as a member of the marketing department and emails the project manager and provides a formulated update on the project, and attaches a link that is supposedly password protecting the document [Imp20]. Imperva further explains that the email content is formatted to look like it was legitimately sent from within the company to deceive the project manager, who then logs in to view the document. At the same time, the attacker steals his credentials and gains access to the organisation's sensitive information.

Research by Blythe et al. explained how email phishing is one of the most common types of phishing attacks and how very often these scam emails originate from Nigeria [BPC11]. Blythe et al. explain that the attack is carried out by a phisher sending fake emails designed to look legitimate. However, the attack can be identified using premise, spelling, grammar, logos, and style. The research explains that emails with easy-to-copy logos are more challenging to identify as phishing emails than emails without logos. The compelling visual design is used when deceiving targets for phishing attacks. According

to the simulation analysed by Blythe et al. on 224 participants on distinguishing phishing emails from 10 emails, 56.9% recognised genuine emails as phishing emails, and 28.1% failed to identify the phishing emails.

Research by Rick explained that the email phishing attack is an attack where an attacker sends an email posing to be who they are not in order to ensure the victim takes actions which they usually would not do [Was20]. He discussed how the attack is carried out by the attacker taking advantage of how humans interpret the content of what they see or hear. An interview carried out by Rick explained how failure to engage in enough sense-making and discrepancies in email lead to a successful email phishing attack. According to Rick, certain IT experts have a process that is followed in identifying phishing emails. He explained the stages as the first stage is to make sense of the email and understand its relation. If discrepancies are seen in the content of the email, they proceed to the next stage, which is to look for technical details to confirm their suspicions of phishing. The final stage is to deal with the email by either deleting or reporting the email.

Research by Kristen et al. explains how the email phishing attack affects an organisation and how some organisations have implemented technological solutions to prevent the attack. Kristen et al. explained that email users could not be prevented from falling for email scams. However, as phishing emails can bypass technological defences, users might be the only option to safeguarding against the attack [GST18]. The article further advises not penalising but engaging users by providing phishing awareness training to educate users on how to spot real-world phishing emails.

Masayuki et al., in research, explained how email phishing is carried out by a phisher who makes use of social engineering and computer technology, pretends to be a trusted entity to steal a victims' valued information such as personal identity information and credentials. The research further explains that defending against phishing attacks will require not only to depend on information security systems such as firewalls but to create awareness of information security for an organisation's staff [HKOK19].

Spear-phishing

The spear-phishing attack is a phishing attack in which a specific individual, business, or organisation is targeted as an email is received from a source that seems trustworthy, but unknowingly, clicking any link contained in the email will lead to a download of malware [Kasb].

According to Symantec internet security threat report for 2017, 71.4% of attacks on organisations in 2017 were initiated by spear-phishing emails [Sym18]. In 2018, Symantec internet security threat reported that 65% of attacks used spear-phishing as the primary infection vector [Sym19].

According to research carried out by Alex and Xiaohong, a phishing attack is an attack that has been identified to be the most associated with social engineering as an

attacker is disguised as a trustworthy source in order to acquire victims' personal or private information [SY19]. The research explains that spear phishing is personally designed for a specific target and is time-consuming. The attacker, called a phisher, gathers information regarding the victim to plan an effective attack. The research further explains how education and training is the best way to mitigate the attack as individuals are taught how to identify and deal with the attack.

Another spear-phishing attack is the whaling attack, where the target is an executive member of an organisation. The attack method is the same as a spear-phishing attack, but in this case, the target is someone with access to more confidential information. A whaling attack is risky as individuals in executive positions have access to highly confidential information of the organisation [AP20].

QR Code

SMS phishing, otherwise known as smishing, is a form of phishing. Short messaging services (SMS) or text messages are masked to originate from a trusted source asking for details or requiring them to perform some actions. Research carried out by Sandhya and Devpriya explained that the attack is carried out by an attacker called a smisher. This attacker sends a text message prompting the user to visit a fake website and perform a specific action, which the attacker can then use to steal the user's personal information [MS19]. The research further explains that the content of the message can also contain a phone number. In the phone number, the victim is pressured to make the call to the number presented to resolve a fake urgent situation that the smisher has presented. When the call is made, the smisher will ask for personal information, which the smisher claims to be necessary to resolve the issue, but instead steals the provided information and uses it for certain fraudulent activities. Sandhya and Devpriya concluded that the attack is successful because of the lack of knowledge of security options among mobile phone users. The research also explains that users have a habit of installing applications without thinking about the possibility of the application being malicious.

The QR code is considered a two-directional bar-code as it allows more data to be stored significantly compared to the standard bar-code [Kasa]. Katharina et al. explained that the QR code is used to encode certain information such as a link or other textual information to make it instantly available instead of manually typing the link URL [KFR+15]. The research further explains how an attacker modifies a QR code to redirect a user to a malicious setup site, disguised to look legitimate, where the victim provides personal information. The attacker then steals this information to use for fraudulent activities. Katharina et al. further explained the failure of the majority of QR code scanners as they cannot identify altered QR codes and investigate web content for malicious purposes.

Research carried out by Kelvin et al. explained how it had made access to the digital world convenient as it has been adapted by various applications to point to digital

information and authentication [YCT19]. The research explains the QR code phishing attack to be one in which the code is manipulated as certain code features are changed, so when used by a victim, the victim is redirected to a malicious site. This attack is not easy to identify, as victims will not validate the codes visually. Kelvin et al. concluded that technical countermeasures are more effective in preventing the attack. However, education and awareness on detecting QR code phishing is a better option long term.

SMS and Voice Phishing

SMS phishing, otherwise known as smishing, is a form of phishing. Short messaging services (SMS) or text messages are masked to originate from a trusted source asking for details or requiring them to perform some actions. Research carried out by Sandhya and Devpriya explained that the attack is carried out by an attacker called a smisher. This attacker sends a text message prompting the user to visit a fake website and perform a specific action, which the attacker can then use to steal the user's personal information [MS19]. The research further explains that the content of the message can also contain a phone number. In the phone number, the victim is pressured to make the call to the number presented to resolve a fake urgent situation that the smisher has presented. When the call is made, the smisher will ask for personal information, which the smisher claims to be necessary to resolve the issue, but instead steals the provided information and uses it for certain fraudulent activities. Sandhya and Devpriya concluded that the attack is successful because of the lack of knowledge of security options among mobile phone users. The research also explains that users have a habit of installing applications without thinking about the possibility of the application being malicious.

Voice phishing is also called vishing. It is an attack where the attacker disguises himself using a fake caller ID as a trusted entity. He makes a phone call appearing to be from the local area or a trusted organisation to a target offering to provide certain services, which will require the target first to provide some personal information [Dro19]. A research by Athulya and Praveen said a phone call is placed to the target under the pretence of being a representative of a trusted organisation such as a bank offering help in making instant corrections to critical mistakes noticed on the target's account [AP20]. The research explained that the target will have to provide personal information such as a bank account number, which the attacker will then use to perform fraudulent activities.

Session Hijacking and In-Session Phishing

According to research by Athulya and Praveen, phishing attacks can also be performed by technical subterfuge [AP20]. The research explains one of these types of phishing attacks as session hijacking. The attacker monitors the target's actions until an account is logged in to or a transaction is made whereby the attacker will acquire the credentials of the target. In this attack, the target is unaware that he is being monitored.

According to Zbigniew, performing the attack will require the attacker to know the target's session ID, which can be acquired by persuading the target to click a malicious link that contains a primed session ID [Ban19]. According to Athulya and Praveen, the In-session attack is another type of phishing deployed using technical subterfuge. The attacker takes advantage of the trust of the legitimate website and displays a pop-up such as 'session timed out' or 'reset your password ', and the user who believes the website is trusted will go-ahead to submit information, thereby sending login credentials to the attacker.

Business Email Compromise

Business email compromise (BEC) is one of the common security issues for businesses. Research by Songpon et al. described the BEC attack as the attacker is disguised as someone associated with the business to gain trust, sends an email, requesting payment for specific services into a fraudulent bank account, thereby deceiving the target [TYU20]. The research explains that the attack targets companies that do business with partners overseas because the verification of overseas transactions takes some time and is complicated.

According to the Agari threat intelligence brief report for 2020, 60% of BEC attackers were located in Africa, of which 83% of the African attackers, as well as 50% of global BEC actors, are from Nigeria. The attack, if successful, could be catastrophic for the organisation. According to the APWG report in 2020, the COVID-19 phishing was used in the BEC attacks [APW20]. The report explained how an email was received from a source masked to be trusted. This email stated, "Due to the news of the CoronaVirus disease (COVID-19), we are changing banks and sending payments directly to our factory for payment, so please let me know the total payment ready to be made, so I can forward you our updated payment information.". Further investigation revealed the new account to be in Hong Kong, where the criminal could collect the funds via money mules [APW20]. Many more COVID-19 attacks were reported to have taken place using the BEC.

Zoom Phishing

Zoom Phishing is a phishing attack where targets receive emails from joining a Zoom meeting concerning a supposed termination. Due to the urgency, the target will attempt to join the meeting by login into the zoom phishing page whilst their credentials are being stolen [Sec20]. The attack was first reported to APWG in March 2020 as the emails contained links which, when clicked, redirected victims to websites set up to steal Zoom account credentials [APW20]. According to the APWG report, attackers can then use the stolen credentials to log in to conferencing accounts and harvest passwords of other sites and services.

Table 1. Phishing Attack Review Summary

Attack	Domain spoofing		Email phishing	Spear phishing/Business Email Compromise
Business assets	Human Sensitive data.		Human Sensitive data	Human Sensitive data, Monetary Value
System assets	Human, Machine, Email		Human, Email	Human, Email
Vulnerability	1. Human can be visually deceived. 2. Human fails to recognize security measures installed on machine and web browser. 3. Human fails to inspect URL of website being visited.	Machine is not protected with information security systems.	1. Human can be deceived to believe email is being sent from reliable source. 2. Human fails to recognize discrepancies in the content of the email.	1. Human can be deceived to believe email is being sent from reliable source. 2. Human fails to recognize discrepancies in the content of the email.
Threat	A phisher steals human sensitive data by deceiving the human to visiting a fake website.	An attacker installs malware on human machine and steals human sensitive data by deceiving the human to visiting a fake website.	A phisher steals human sensitive data by deceiving the human with the content of email to believe the data is being shared with a reliable source.	1. A phisher steals human sensitive data by doing a detailed study of a particular human to deceive the human with the content of email to believe the data is being shared with a reliable source. 2. An attacker steals monetary value from a business by deceiving the human with the content of email to believe the payment is being made to a reliable source such as a business partner.
Impact	1. Loss of confidentiality of human sensitive data. 2. Loss of availability of resources linked to stolen human sensitive data.	1. Loss of confidentiality of human sensitive data. 2. Loss of availability of resources linked to stolen human sensitive data 3. Loss of integrity of machine. 4. Loss of availability of machine	1. Loss of confidentiality of human sensitive data. 2. Loss of availability of resources linked to stolen human sensitive data.	1. Loss of confidentiality of human sensitive data. 2. Loss of availability of resources linked to stolen human sensitive data 3. Loss of availability of monetary value.
Countermeasure	Train human to detect, identify and make decision on phishing attacks.	Use of application to detect, identify, and block phishing websites and emails	1. Application of information security systems. 2. Educate humans by carrying out phishing awareness training.	Train human to detect, identify and make decision on phishing attacks.
Reference	[DKK+17], [DTH06], [AK20], [APW19b].	[HRJA19], [CG06].	s[JGST20]. t[Imp20]. a[BPC11]. o[Was20]. k[GST18]. f[HKOK19].	e[Kasb]. n[SY19]. T n[AK20].

Table 2. Phishing Attack Review Summary (b)

Attack	SMS and Voice Phishing		QR Code	Zoom Phishing
Business asset	Human Sensitive data		Human Sensitive data	Human Sensitive data
System assets	Human, SMS, Phone	Human, Phone	Human, QR code	Human, Email, Zoom application.
Vulnerability	1. Human can be deceived to believe the SMS is being sent from a reliable source. 2. Human fails to inspect URL of website being visited. 3. Humans lack knowledge on mobile security options.	1. Human can be deceived to believe the phone call is being placed from a reliable source. 2. Human can be put under pressure to believe the situation presented by attacker is critical.	1. QR code can be modified. 2. Many QR code scanners fail to identify altered QR codes. 3. Humans cannot validate QR codes visually.	1. Human can be deceived to believe email is being sent from reliable source to join a zoom call. 2. Human fails to recognize discrepancies in the content of the email.
Threat	A smisher steals human sensitive data by deceiving human to visiting a fake website presented in the SMS.	An attacker steals human sensitive data by deceiving human to believe the situation presented by attacker is critical and that attacker is a trusted entity helping to resolve the situation.	An attacker modifies QR code used by human, thereby redirecting human to malicious site to steal human sensitive data.	An attacker steals human sensitive data by deceiving the human to login to the Zoom application to join an urgent call.
Impact	1. Loss of confidentiality of human sensitive data. 2. Loss of availability of resources linked to stolen human sensitive data.	1. Loss of confidentiality of human sensitive data. 2. Loss of availability of resources linked to stolen human sensitive data.	1. Loss of confidentiality of human sensitive data. 2. Loss of availability of resources linked to stolen human sensitive data.	1. Loss of confidentiality of human sensitive data. 2. Loss of availability of resources linked to stolen human sensitive data.
Countermeasure	Train human to detect, identify and make decision on phishing attacks.		1. Making use of technical applications to prevent the attack. 2. Fortifying QR code scanners to be able to detect and identify altered QR codes. 3. Create human awareness on detecting QR code phishing attack.	Train human to detect, identify and make decision on phishing attacks.
Reference	n[MS19]. [Dro19]. t[AK20].		[KFR+15]. [YCT19]	[TYU20], [APW20]

2.3 Phishing Attack Process

The phishing attack is usually carried out in various stages, depending on the type of attack. Hossein et al. explained in research that an email phishing attack is carried out in 3 steps; the user opens the phishing emails, the user clicks on the link, and the user submits sensitive information [ADPL21]. The research focused on the step 'clicking the link' as the paper discusses demographic factors and psychological traits influencing targets to fall for the attack. The risk-taking behaviour and decision-making style were compared against demographic factors to determine the attitude of phishing targets when they receive a phishing message.

In the research carried out by Zuochao et al., he explained that phishing attack is carried out in 5 stages [DKK+17]. Many of the reviewed research explains the attack beginning with the attacker getting information on his targets, planning the attack, and then deploying the attack. From the research, it can be said that the attack stages can be summarized into 6 phases (see Figure 2). This could sometimes be more or less depending on the type of phishing attack. These phases are explained below:

1. Information gathering: In this phase, the attacker gets the details of the victim. This includes but is not limited to a phone number, email address, social media contact, e.t.c. This information can be collected using social engineering.

2. Design phishing attack: The attack is then designed. This could be a composed SMS, email, or designed domain. It could also be a programmed malware or popup designed to take advantage of browser cookies.

3. Deploy attack: The attack is deployed taking advantage of SMS, email, phone calls, websites, or cookies. After the attack is deployed, the attacker waits for the reaction of the target.

4. Receive phishing message: The designed message gets to a possible technical phishing security system. Depending on the design of the attack, the phishing message may stop at this stage. However, more sophisticated phishing attacks pass-through this technical security system and can only be stopped if the target identifies the message as a phish.

5. Perform action or provide sensitive information: Target sees the message and makes a decision. If the message is recognised as a phish, the attack will fail, as the target will not fall for it. However, if the target fails to recognise the email, the target can then carry out the requested action in the message. This action can be to click a link/attachment/button on a website (whereby malware is planted on the system) or provide sensitive information directly. The recipient then becomes a victim of phishing.

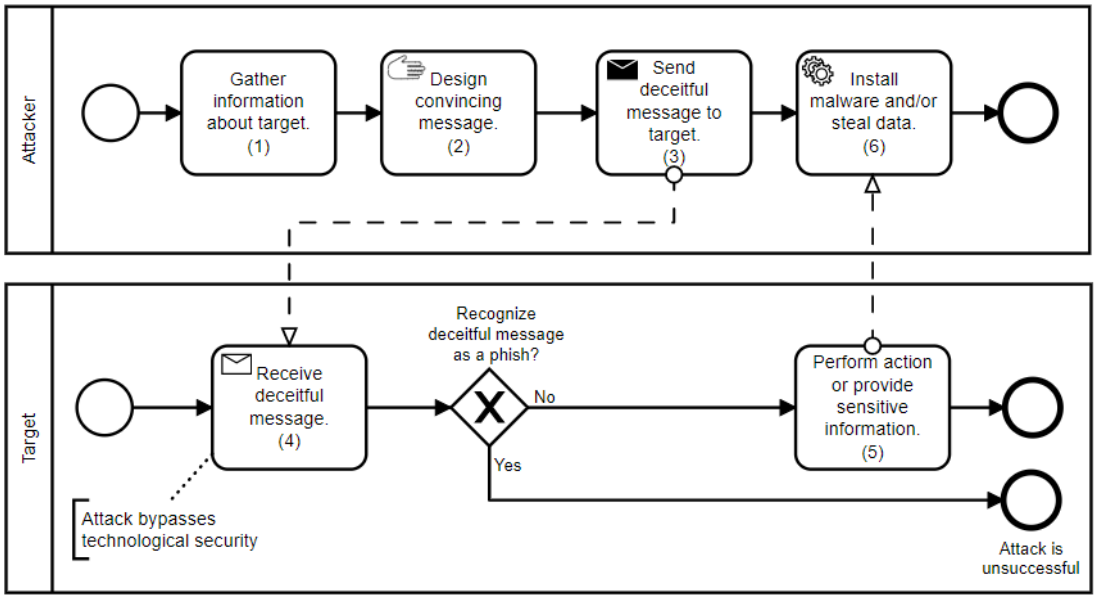


Figure 2. Phishing Attack Process

6. Install malware or steal data: The attacker waits for feedback based on the target's decision. If the malware installation is initiated, the attacker will be aware as he will be prompted depending on how the malware is designed. However, if the attack was designed to have the target provide the sensitive directly, this will also be received on the attacker's end.

2.4 Phishing Attack Simulation in Different organisations

A few companies have carried out phishing attack simulations on their employees. The goal was to test the employee's level of awareness of phishing attacks. Different approaches have been used to carry out the simulation. However, the most common approach is using monetary incentives to lure the employees into falling for the attack, and many indeed fell for the simulation attack. In some simulations, there were complaints about the simulation not being ideal, as the phishing emails did come from email addresses of the company domain.

In 2020, a web domain registrar called GoDaddy carried out a phishing attack simulation on its employees [Lon20]. The domain registrar sent emails to its employees, informing them that they had received a holiday bonus of $650. The email was designed to be a form of appreciation for the hard work done by the employees. Contained in the email was a link to the bonus, of which many of the employees clicked. Two days after the email was sent, employees received another email from the security chief of

GoDaddy stating, "You are receiving this email because you failed our recent phishing test,". This attack was considered brutal because the employees believed the email was legitimate, as roughly 500 employees clicked and failed the test. The email from the security chief further stated that "You will need to retake the Security Awareness Social Engineering training.". This email from the security chief indicates that security training of the employees will help prevent the employees from falling for such attacks in the future.

Another company called Tribune Publishing tested its employees with the phishing attack [Pic20]. An email was sent out to its employees offering a monetary bonus of $5,000-$10,000. The email was designed as a form of gratitude to the employees for their commitment. The email contained links to the bonus and a breakdown of the tax. On clicking the link, a message was received informing the employee that they had clicked a simulated phishing test.

Table 3. Phishing Attack Simulation Different Industries

Company	**No. of Target**	**The attack**	**No. of Victims**	**Purpose**
GoDaddy	>100	Phishing email using money incentive	Not stated	To test employee level of phishing awareness
Tribune Publishing	Not stated	Phishing email using money incentive	Not stated	To test employee level of phishing awareness
Telecommunication sector (unknown)	39	Phishing email using money incentive Phishing email about security update	None 12	To determine level of phishing awareness To determine level of phishing awareness

A simulation was carried out by Ahmad and Masniza on an organisation under the telecommunication and defence sub-sector [AM19]. The simulation aimed to determine the level of awareness of phishing attacks in the sector, where 39 participants were involved. The simulation was carried twice with a 4-month lag between each. In the first simulation, an email was sent out on monetary incentives; however, none of the targets fell for the spear-phishing emails. The questionnaire reviewed after the attack showed that respondents were able to identify signs of phishing emails.

However, the second simulation was carried out using a different approach, as the email mentioned some security updates required. In this second simulation, 12 participants responded to the email by clicking on the link attached to the email content. When the link was clicked in the second simulation, it directed the users to a fake website. On the fake website, a hyperlink was included, which then redirected the victim to the legitimate website. This way, the victims would not deduce that they have fallen for a phishing attack, as the final website to which they were redirected is a legitimate website. Ahmad and Masniza further concluded that the spear-phishing attack was successful and further proved that the attack could work in the telecommunication and defence sub-sector using the second simulation procedure.

2.5 Phishing Awareness Training

With the possibility of attacks being able to pass through security implemented tools, people would need to be trained on phishing attacks. Michael, in his research, described a way to enhance phishing awareness training [Mir16]. He provided core activities required to carry out the training. According to Micheal, the core processes are; train on phishing detection and incident response, obtaining leadership approval, developing the training scenarios, selecting and deploying the phishing tool, implementing and testing exercise scenarios, developing and implementing exercise response, and initiating the exercise report on the metrics. These processes explained the steps to carry out before training and how to train people. He also explained that sending a phishing email to the people to be trained can test them on phishing recognition. The research explains in-depth how to go about the training, but the processes were not carried out with a case study to see the possible outcome.

Another research by Steven et al. [MMS18] presented that different organisations use different approaches to simulate phishing programs. He explained that the various results could be used to focus training on the security education program. He explored various ways phishing simulations can reduce the susceptibility of phishing attacks and concluded that behaviour-based controls were more successful in reducing vulnerability to phishing attacks. The behaviour-based controls required carrying out generic and targeted training on phishing attacks using simulations.

2.6 Summary

Many researchers have studied phishing attacks and their types. Some have delved further into providing possible ways to protect against the attacks. A few research stated the best way to reduce the risk of phishing attacks is to create awareness of the attack, whilst others suggested applying technical security systems. More research has covered protecting against these attacks by implementing specific tools and machine language to filter phishing emails from getting into the system.

Based on the research on different types of phishing (see Table 1 and Table 2), it can be seen that humans are the most vulnerable assets when it comes to performing phishing attacks. Also, as phishing attacks are evolving, being designed to pass through the implemented tools, human detection of phishing attacks will be the best way to prevent attacks from being successful. Some research provided details on awareness creation to reduce the risk of phishing. However, awareness alone has been proven not to be enough.

This section explains the types of phishing attacks and how the attacks are simulated in various organisations. We also described the processes required to carry out the attack based on reviewed research. The next chapter will use the described phishing and the attack process to simulate an attack. This is done to describe the impact of the attack on the organisation's business process.

3 Research Approach

This chapter discusses the method used to carry out the research. The research by Hossein et al. studied the human behaviour and demographics during a phishing process [ADPL21]. He discussed to what extent being a victim of phishing is influenced by people risk-taking and decision-making styles. If people can be trained to recognise phishing attacks, this can help improve the risk-taking styles, thereby affecting their decision-making regarding phishing attacks. In this section, we will answer the **SQ2-What is the impact of phishing attack on an organisation's business process?** This thesis applies the ATTF cycle to members of staff within an organisation for the case study.

For this case study, we will apply the ATTF cycle described in section 1.5, beginning at the testing stage of the cycle. This is done to know how if staff can recognise phishing. The reaction and feedback to the phishing message are used to plan the awareness and training stages of the cycle. This ATTF cycle is applied to a telecommunication company for the case study. A telecommunication company is selected because of its infrastructure and the fact that it serves many customers.

3.1 Testing

The impacts of phishing attacks on the organisation business process will require knowing the assets and risks of the attack based on the business process. Understanding the impacts of phishing attacks will shed light on the importance of recognising the attack if this penetrates through the security systems put in place. To fulfil the testing stage, we will simulate a phishing attack using email phishing and domain spoofing on the company. This is because most of the information of the company business process is shared over email, and email addresses are used to access various resources within the company.

3.1.1 Data Collection

The company used for the case study is one of the major telecommunication companies on its continent with many competitors. The business process of the organisation will be reviewed to define the business and system assets. This will help to understand the possible risks and impact of the attack on the business process.

During the simulation, required data will be provided and validated by a member of staff. This staff will collect and share details such as emails and reactions to the simulation based on what was reported.

3.1.2 Protected Assets

The company's business process begins with a customer requesting a service from the sales unit, and the sales unit confirms the availability of the service and informs the customer. The customer then decides to purchase the service. The project management and engineering team are then engaged to take the actions required to ensure the service can be delivered. A survey of the customer's location is carried out to generate requirements for the service to be delivered. A bill is then generated into a purchase order, which is sent to the customer. The customer reviews the bills and decides if to carry on with the service at the cost. Once the customer decides to proceed, the service is then deployed, tested, and handed over to the customer for use. A job completion certificate (JCC) is given to the customer to sign after the service has been used for five working days. After this is signed, the project is handed over to the engineering team to monitor the service and ensure quality assurance (see Figure 3).

During various stages of service provisioning, certain documents are collected and generated. These documents are stored on the network drive. The network drive contains various data, including customer's private information, bills for the provisioning, survey report on customer's location, customer's purchase order, and signed JCC. There is a considerable risk of an attacker gaining access to the network drive data. For the purpose of this case study, we shall be referring to any data contained in the network drive as **network drive data**. The business process is represented using the BPMN (see Figure 3).

3.1.3 Attack Method

In the organisation, log in to most of the resources are accessed with the same credentials for emails, so gaining access to email addresses will create a path for attacking the business asset.

A number of the email addresses can be gotten by an attacker, taking time to put scraps together to get emails. The company website has three emails that can be reached out to ask for information, which can lead to getting other emails. This method will require social engineering when making inquiries.

An attacker creates a fake domain and sends a legitimate email to email address A (sales), asking for a detailed explanation of how the service offered by the company is carried out from beginning to end. This information is claimed to be what the attacker needs to know before he invests his money into the service, and the sales team will be happy to acquire a new customer. The attacker sends a new email to customer service email B requesting that they provide an email address of someone in the project management team as they want inquiries to request a service.

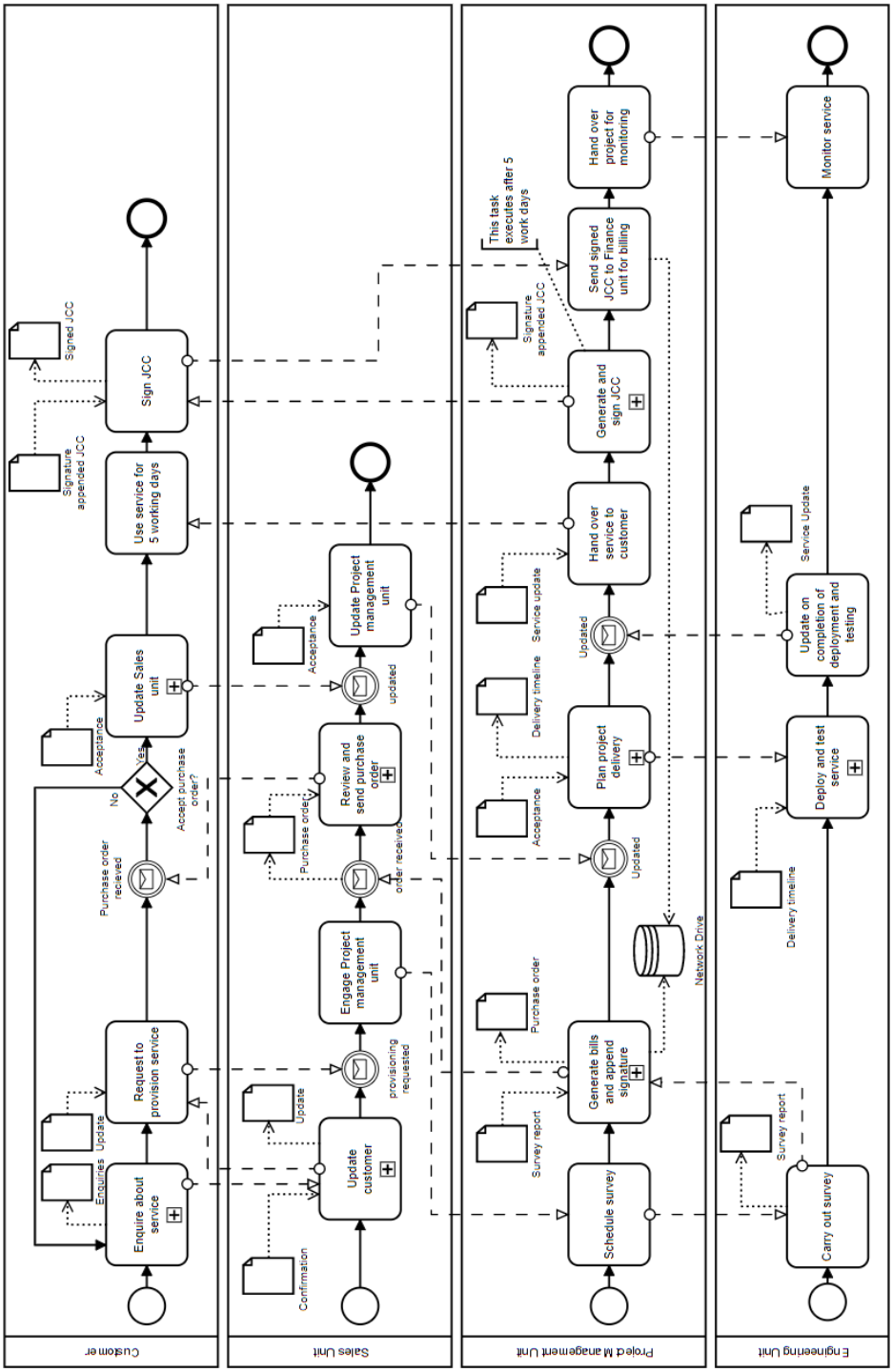


Figure 3. Company Business Process

The attacker reviews the company's profile page on LinkedIn and sees various accounts of staff. He then calls a number from the company website mentioning that he was trying to email Staff A (who has been confirmed is a staff member from LinkedIn), but he could not locate the email address. He then asks for the head of the department's email address as he claims to want to copy the head of the department in the email.

The attacker goes ahead to write to the WhatsApp number contained on the company website to ask for the email address of the engineering team, sales team, and project management team. He claims he is an existing customer and wants to refer a new customer, but the new customer would like to ask questions from each team member listed before he proceeds with requesting the service. After some days, the attacker goes around with the same process until he has gotten a substantial number of email addresses to carry out the phishing attack.

3.1.4 Security Risks

There are several risks associated with an attacker gaining access to the network drive data. These risks can be possible with a successful phishing attack being carried out on a member of staff of the organisation and acquiring credentials required to access the network drive. Phishing attacks are sometimes overlooked as some people think, 'as long as I do not reply to the phishing email, I am safe.'. Unknowingly to many, phishing emails can contain malware embedded in links/attachments in the email. A target can click this link and see nothing happen, but unfortunately, malware has been deployed into the computer. Depending on the strain of malware, it can also spread to other computers connected to the same network as the infected computer. Below are examples of possible risks with accessing the network drive data using a phishing email attack as the attack source. These possible risks are similar to what was described in the literature reviewed (see Table 1 and Table 2)).

Table 4. Risk 1

Business asset	Network drive data
System assets	Network drive, Project management unit, Sales unit, Staff, Engineering Units, Email, Computers.
Security criteria	1. Integrity of network drive data 2. Confidentiality of network drive data
Risk	An expert hacker, hired by a competitor company, inspired by personal gain, deceives staff into installing malware on the computer by clicking a link/attachment contained in an email, which steals credentials to access the network drive and steals the network drive data, leading to loss of integrity of network drive data and loss of confidentiality of network drive data. This thereby affects the organisation's business and results in financial losses.
Impact	1. Loss of confidentiality of network drive data. 2. Loss of integrity of network drive data.
Threat	An expert hacker deceives staff into installing malware on the computer and steals credentials to access the network drive data.
Vulnerability	1. Staff in the project management unit, Sales Unit, or Engineering unit can be deceived into reviewing clicking links/attachments contained in malware compromised email. 2. Staff fail to recognise compromised email as a phishing email. 3. Malware can be installed on computers.
Threat agent	An expert attacker with the means to install malware on computers deceives staff into clicking on links/attachments contained in the email to steal credentials needed to access network drive data.
Attack method	Get staff email and deceive staff into clicking a link/attachment embedded with malware used to steal credentials contained in the email.

Table 5. Risk 2

Business asset	Network drive data
System assets	Network drive, Project management unit, Sales unit, Staff, Engineering Units, Email, Computers.
Security criteria	1. Availability of Network drive data 2. Integrity of Network drive data 3. Confidentiality of network drive data
Risk	A malicious former worker, with the aim of revenge, installs ransomware on the network drive because staff can be deceived into providing credentials required to access network drive data, leading to the loss of availability of network drive data, loss of confidentiality of network drive data and loss of integrity of network drive data which will lead to poor services offered by the company within the period of the attack.
Impact	1. Loss of confidentiality of network drive data. 2. Loss of integrity of network drive data. 3. Loss of availability of network drive data.
Threat	A malicious former worker installs ransomware on the network drive by deceiving staff into providing credentials required to access network drive data.
Vulnerability	1. Staff can be deceived into sharing credentials required to access a network drive with an attacker. 2. Malware can be installed on computers.
Threat agent	A malicious former worker, with the means to install ransomware on a network drive, deceives staff into providing credentials required to access network drive data.
Attack method	Deceive staff into providing credentials required to access network drive data.

Table 6. Risk 3

Business asset	Network drive data
System assets	Network drive, Project management unit, Sales unit, Staff, Engineering Units, Email, Computers.
Security criteria	1. Integrity of Network drive data 2. Confidentiality of network drive data
Risk	An expert hacker hired by a competitor company, inspired by personal gain, deceives staff into installing malware on the computer which steals credentials to access the network drive data, makes modifications to network drive data leading to loss of Integrity of network drive data and loss of confidentiality of network drive data thereby ruining the business.
Impact	1. Loss of confidentiality of network drive data. 2. Loss of integrity of network drive data.
Threat	An expert hacker deceives staff into installing malware on the computer and steals credentials to access the network drive and make modifications of the network drive data.
Vulnerability	1. Staff in the project management unit, Sales Unit, or Engineering unit can be deceived into reviewing clicking links/attachments contained in malware compromised email. 2. Staff fails to recognise compromised emails as phishing emails. 3. Malware can be installed on computers.
Threat agent	An expert attacker with the means to install malware on computers deceives staff into clicking on links/attachments contained in the email to steal credentials needed to access the network drive and make modifications to network drive data.
Attack method	Get staff email and deceive staff into clicking link/attachment embedded with malware used to steal credentials.

3.2 Attack Plan

Sub-research question (SQ2) can be answered by simulating a phishing attack on the organisation. The possible impacts of the attack will be collected based on the feedback from the attack. The simulation will be carried out in 6 phases (see Figure 4) based on the attack method discussed in Figure 2. The feedback will be identified as clicks or responses to the phishing email.

1. Get staff email: In this phase, information is gathered and email addresses of employees will be collected. This will be provided by an internal staff assigned so email is delivered to all staff.

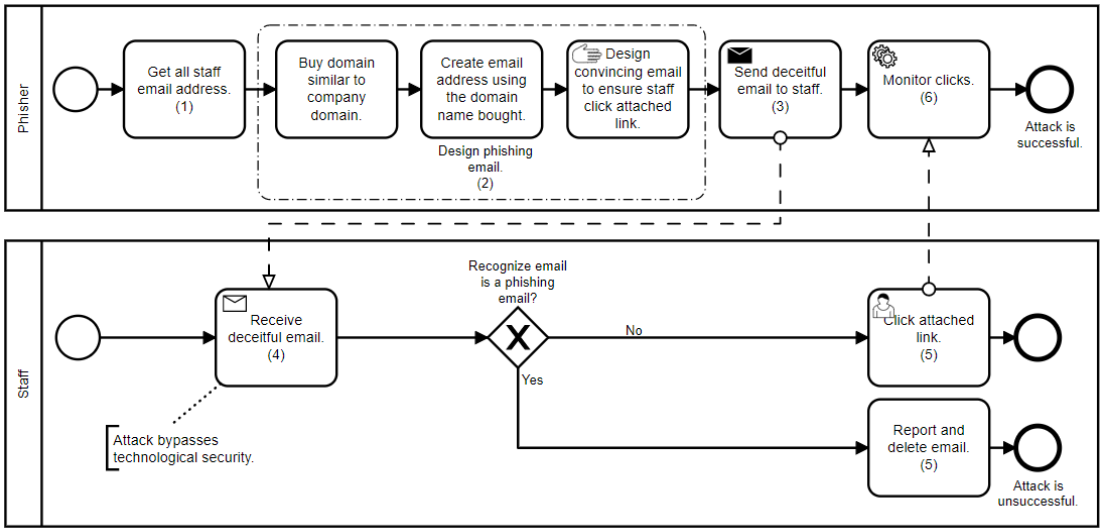


Figure 4. Attack Plan

2. Design phishing email: This phase described the design of the attack, which is the first step to deceiving the staff. The phase is broken into three steps.

   - Buy domain: A domain name very similar to the company's domain will be bought. A character in the domain name will be changed to deceive the staff. The character 'l' from the company's legitimate domain will be changed to the character 'I' to have the email address convincing. A staging website is then built using the domain name bought. This website will contain a 'Maintenance' page (see Figure 5)
   - Create email address: An email address will be created with the identity BBS. The choice for BBS was suggested because from the information gathered, the broadband solution (also known as BBS) is in charge of security updates within the organisation. However, there is no such email address with the identity BBS in the company. When the false email address is sent out, the identity BBS is used to make believe that the security update email being sent is legitimate.
   - Design convincing email: The final step is to design the email. The email is to contain a required security update which contains a link. The link is

stated to be the path to updating credentials, as explained in the email content. However, when the link is clicked, it redirects the user to the staging website earlier built using the domain name bought (see Figure 6). The email is also designed with the company logo in the signature.

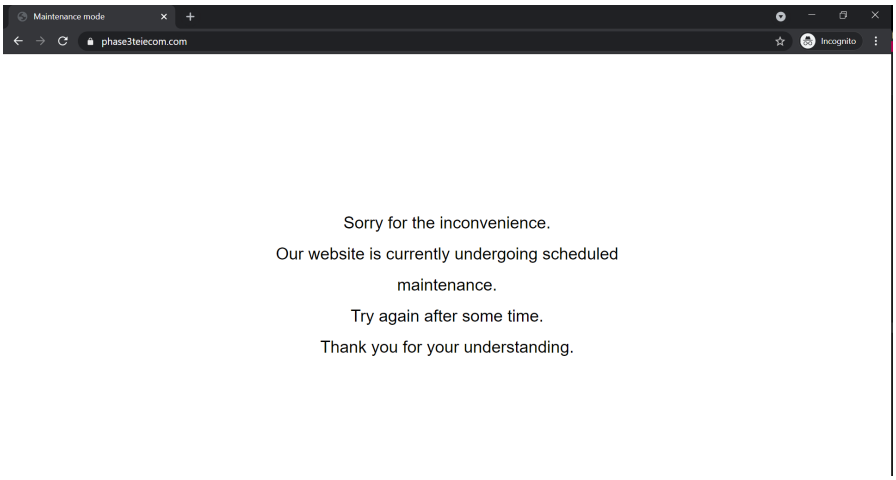


Figure 5. Staging Website

3. Send Deceitful email: In this phase, the email is sent out to staff with the attached link. The email content gives a deadline for which the update is to be carried out.

4. Receive email: The email is then received by the staff in their inbox based on the email client being used for emails.

5. Make a decision: In this phase, the staff knowledge of phishing recognition will be tested. If the email is recognised as a phish, the staff will know to report this. However, if the email is not recognised as a phish, the staff will click the link.

6. Monitor clicks: The accurate number of clicks will be gotten from the access log of the staging website. The access logs give a list of IP addresses with the number of times the device with the IP visited the website.

   The internal staff assigned will collate the number of staff who reached out to confirm if the email sent was legitimate or a phish. The staff assigned will also collect the number of staff who reached out to complain that the link did not work, as it redirected to a maintenance page. This will therefore indicate a higher vulnerability, as not only did the staff fail to recognise the email as a phish, but they also complained about the site being under maintenance.

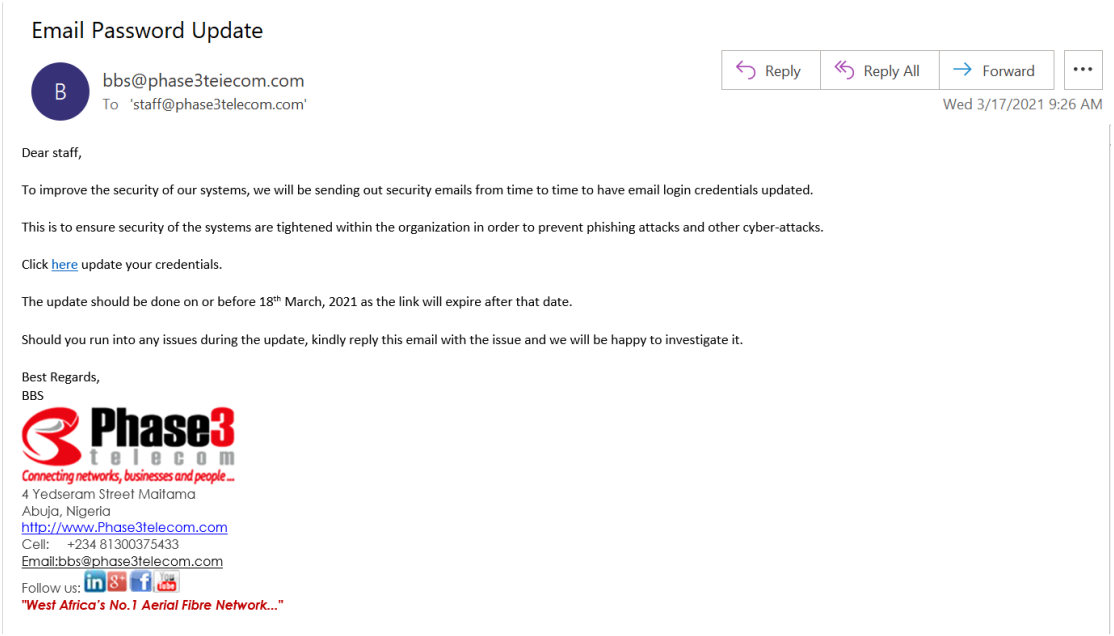


Figure 6. The Phishing Email

3.3 Attack Deployment

The simulation was carried out in the early hours of the day on the 17th of March, 2021. The email required an update to be done between the 17th of March 2021 and the 18th of March 2021. The phishing email was sent to staff at 9:26 am EST (which translates to 8:26 am, Central African Time). The purpose of selecting the time was to get the employees off-guard as that will be one of the first emails which will be received for the day.

The phishing email content required a security update, which contained a link. The link is stated to be the path to updating credentials, as explained in the email content. However, when the link is clicked, it redirects the user to the staging website built using the domain name bought. Several calls were made to the BBS team on verifying the email and its content. Some other calls were made to report the email as a phish. The email included indicators of phishing (see Figure 7) as it had the features; fake domain, sense of urgency, attached link, different style of writing, and generic email signature.

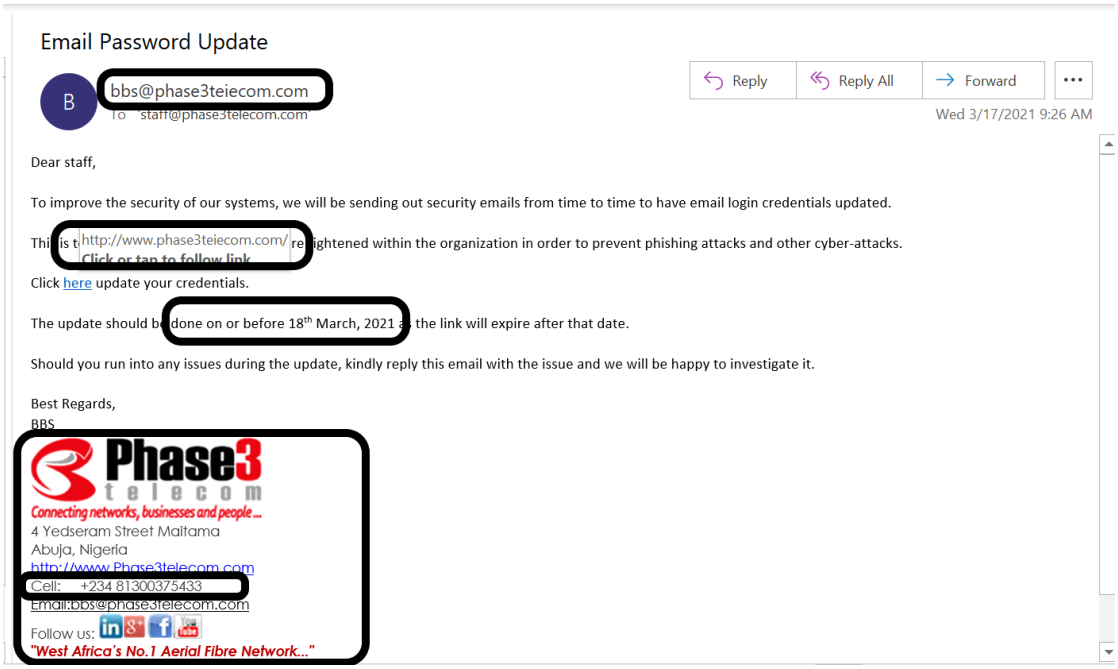


Figure 7. The Email analysis

3.4 Result

The simulation targeted an average of 250 employees. The result was gathered at the end of the second day of the simulation. The time of the phishing email caught some of the staff unawares.

3.4.1 Email Feedback

After the email was sent out within the first few minutes, the first reply was received from a staff member concerning the email content. More responses were received between that day and the next.

1. First Reply

   This reply was received a few minutes after the phishing email was sent out. The respondent is a member of the finance team. The reply indicates that the respondent clicked the link attached to the email, thereby failing to recognise the email as a phish. The respondent identified the link to be incorrect after clicking and replied to the email to have the link corrected but failed to see the email was sent from an incorrect domain name. With the attack failing to be recognised, malware embedded in the attachment or domain contained will successfully be installed on

the computer to gain access to the network drive data accessible by the finance team. The data gotten from the network drive, accessed through the vulnerability in the finance team, can be modified, sold to other cyber attackers, or sold to a competitor, thereby leading to loss of integrity, loss of availability, and loss of confidentiality of the network drive data. Client data can be stolen, and payment processes such as the account to make payment for services can be modified, causing a loss of monetary value to the organisation.

2. Second Reply

   The second reply was from a different team. This time around, the email signature of the respondent indicates the email was from the head of a unit. The head of units in the organisation have access to multiple data within the network drive. This vulnerability gives an attacker access to more data within the network drive. The data can then be altered, sold, or restricted, leading to loss of confidentiality, loss of integrity, and loss of availability of the network drive data, causing damage to the reputation of the company.

3. Third Reply

   The third reply is from staff in the non-engineering team. This staff is in a team that has access to staff information. The respondent failed to identify the email as a phish and clicked the attached link. With this vulnerability, an attacker can access the network drive data accessible by the team to which this respondent belongs and steal information on staff members within the organisation. This data can be sold to other cyber attackers, which can then use this data to carry out cyber-attacks in the future. The data can also be sold, and the identities of staff can be stolen and sold in illegal cyber black market.

4. Fourth Reply

   The last reply on the first day was received from a staff member in the engineering unit in a different region. This staff work in the office in a different state. The staff fails to recognise the email as a phish, and clicking the link attached can result in a successful attack. The attacker who has embedded malware in the attachment or the domain redirected to upon clicking the link will gain access to the engineering data in the network drive and data on the processes being carried out in that region. The data can then be changed, sold, or access to the data can be blocked, leading to loss of availability, loss of integrity, and loss of confidentiality of network drive data, thereby disrupting services provided by the organisation.

   The site's access logs were reviewed for this day, and 161 clicks were observed to have come from the company's IP address. This indicates that the link in the email was clicked multiple times, thereby falling for the attack. Some clicks were also

seen from Afrinic IP addresses, which shows some staff attempted to access the link using their mobile data. Some others called the department (BBS) to complain about the link in the attachment leading to a maintenance page. A few calls were made to the BBS department to inform them of a phishing email received and tell the BBS team to send out an email to staff to inform them about it.

5. Fifth Reply

   On the second day of the simulation, one staff member replied to the maintenance page's phishing email. The respondent is a member of the engineering team. With this vulnerability, the attacker can verify the data accessed as he has gained access to the network drive data accessible by the engineering team from two staff. He may then expand the attack with malware such as ransomware to spread the malware and restrict access to the network drive data, causing loss of availability, loss of integrity, and loss of confidentiality of the network drive data.

   The number of clicks dropped to 18 from the company IP, with fewer clicks from Afrinic IP addresses on the second day. Staff communicating among themselves about a phishing email being received and being warned to not click on the link in the email may have resulted in fewer clicks on the second day.

3.4.2 Attack Summary

After the end of the day on the 18th of March 2021, a total of 179 clicks were seen from the company IP, and over 40 clicks were seen from IP addresses of Afrinic (see Table 7). These numbers were collected from the access logs of the staging website.

Table 7. Phishing Attack Simulation Response

Day	**Number of clicks from company network.**	**Number of clicks from external network.**	**Number of email replies.**
1	161	>30	4
2	18	>10	1
Total	**179**	**> 40**	**5**

Few people reported the email as a phish, while some others either confirmed if the email was legitimate or made a complaint about the link in the email not working. This shows that some staff were not able to detect if the email was legitimate or a phish (see Table 8).

Table 8. Phishing Attack Simulation Reporting

Day	**Number of reports on phishing email.**	**Number of calls to confirm if email is legitimate.**	**Number of calls to complain that attached link was not working.**
1	3	4	2
2	-	-	-
Total	**3**	**4**	**2**

There was a total of five replies to the phishing email (see Figure 9). The network drive contains data accessible by different units, and access to various sections can lead to access to all sections as sections are linked. A click from various units gives an attacker access to the network drive data. The attacker may then modify data, steal data, steal identity, sell data leading to loss of confidentiality, integrity, and confidentiality of network drive data. The risk level of the staff who replied to the email is shown in figure 8 based on the access they have to the network drive data. The risk with the engineering unit staff clicking individual is medium. However, the risk increases when both clicks are combined as the attacker has access to more data within the engineering unit.

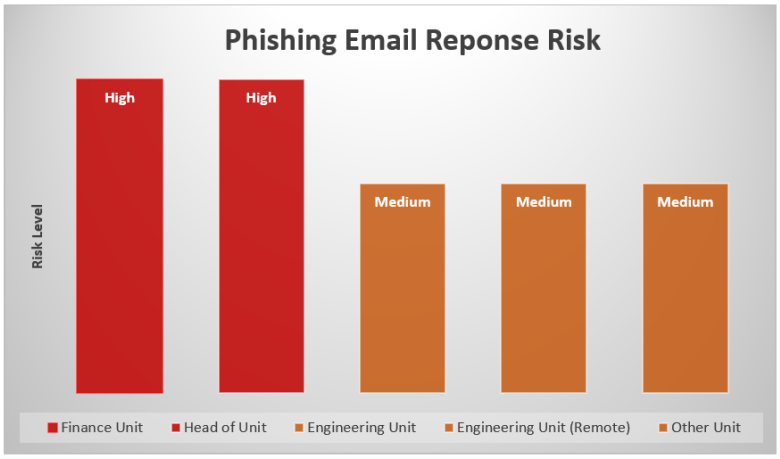


Figure 8. Risk Level Based on Email Responses

With these losses, the company will experience impacts to its business process that can damage the company. Adverse effects such as identity theft can also impact the attack, thereby leading to loss of monetary values in the event of managing the impact of the attack.

From the simulation carried out, the number of clicks is relatively high. (see Figure 10). It shows that some of the staff cannot recognise a phishing attack when faced with one. An attacker can embed malware on the system via the link which was clicked to gain access to the network drive of various departments and get data from the network drive, thereby leading to the risk of loss of availability, confidentiality, and integrity of network drive data.

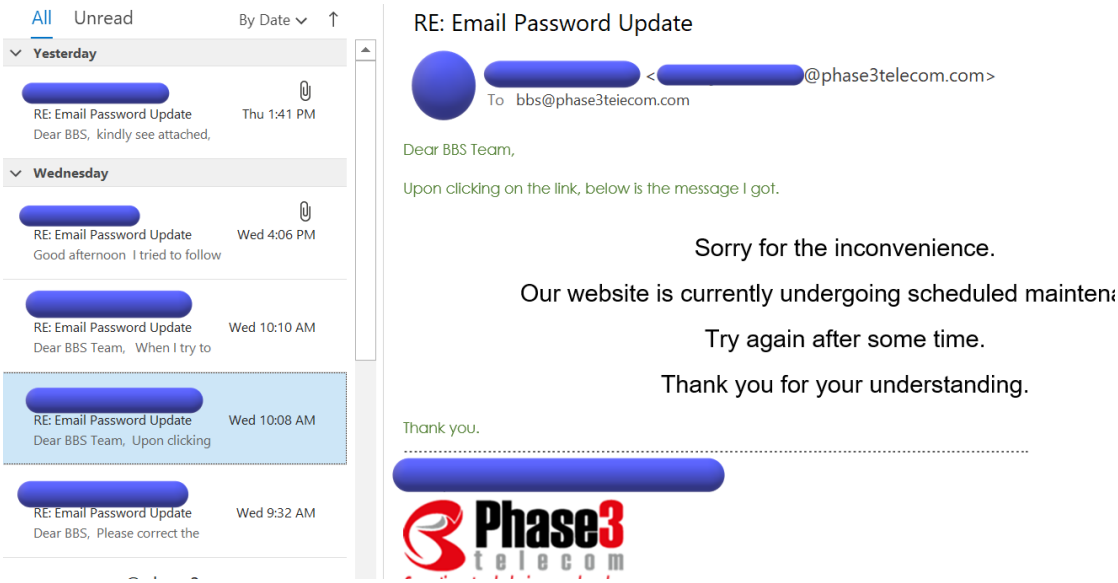


Figure 9. Total Responses

The responses to the email were from different departments within the organisation. There is considerable risk with this as a response to a phishing email proves higher vulnerability within the organisation. With the responses, an attacker can exploit the people who responded further to get more information.

Comparing the number of clicks from within the company IP and the email respondents with the total number of emails sent, the values are high, indicating multiple failure points. Having only four email suspects and three reports on the email being a phish is not enough to prevent a successful attack. When it comes to phishing in an organisation, a single point of failure could damage the company's reputation or loss of monetary value.

The simulation proved that visual deception is indeed one of the reasons why people fail to recognise phishing. One of the respondents to the phishing email discovered the link was incorrect after clicking it but failed to see the email was from the wrong domain name. The company logo, which was used as the email signature when the phishing email was sent, deceived the employees into assuming the email was legitimate.

The email containing a link to updating email login credentials indicates that this email is a phish. The reason is that email credentials can be changed in the email clients being used to view emails. Alternatively, the email credentials can be changed by directly contacting the team managing the email server to make the changes. This proves that the level of security awareness among members of staff is relatively low.

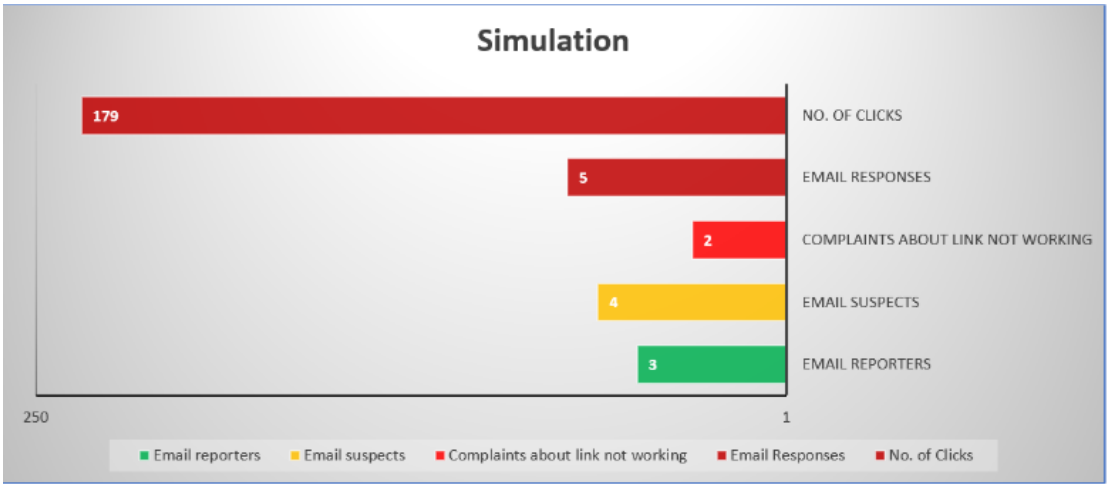


Figure 10. Total Responses

3.4.3 Impact to Business Process

From the reply to the phishing email by a member of a unit that has access to staff personal data, the attacker can now access the emails of members of the sales team. He may intercept the communication between prospective clients at the very first stage of the business process by redirecting emails sent to the sales team to himself. That way, when a prospective client asks about the availability of a service, he then updates the client by telling them that the service is unavailable, leading to the negation of the integrity of network drive data (See point V1 of Figure 11). The growth of the business will be affected because there will be a fall in the number of new clients coming into the organisation.

Based on the reply from the engineering team members, the attacker can confirm they clicked the link. From the network drive data accessible by the engineering unit, an attacker can get the end-to-end design of the service being provisioned, thereby negating the confidentiality of the network drive data (See point V2 of Figure 11). He may then sell this to business competitors or an individual with bad intentions for the organisation. The design gives the fibre optics layout used for the service. A person with intentions may go to the location and damage the fibre during the test phase (five working days before the customer signs JCC) or after the service is provisioned, thereby causing disruption of

service for the client, leading to mistrust in service provided by the organisation. This also affects the organisation financially as they will need to fix or change the fibre.

Through the click from the unit that has access to staff data, an attacker may access and use the credentials of the project management team members to change the details of the service being provisioned. He may assign more or less than the amount of service requested. This is then appended on the purchase order sent to the prospective client, leading to a negation of the integrity of network drive data (See point V3 of Figure 11). This indicates incompetence of the organisation, as the service requested is not what is in the purchase order shared with the prospective client. As s result of this, the prospective client may get upset, thereby giving the organisation a bad name, leading to a harmful effect on the company's reputation and loss of a prospective client.

With access to the network drive data accessible by the Head of a unit, an attacker may extract client personal information, leading to the negation of confidentiality of network drive data (See point V4 of Figure 11). He then uses the data to carry out phishing attacks on the client to exploit them for monetary value. This is a risk as the client may not know how the data may have leaked or if the data leaked, and then the client falls for phish, leading to other issues for the client.

Since the attacker has access to staff data, the attacker can access the network drive data and get the personal information of staff. The data may include work emails and the corresponding roles in the organisation, thereby negating the confidentiality of network drive data (See point V5 of Figure 11). He may then carry out a brute-force attack to get the passwords for the emails. That way, he will be able to access data on the network drive. He can then use the data for any attack, leading to catastrophic effects if not noticed immediately. He may carry out another attack and request a ransom from the organisation since he now has access to data in the network drive.

With this attack requesting the ransom, the organisation may decide to pay the ransom to reduce the risk. However, an attacker may have modified some data within the network drive or stolen some information to sell to business competitors before releasing the data to the organisation, which negates the availability and integrity of network drive data (See point V5 of Figure 11).

Based on the clicks from the engineering team members, the attacker can exploit the malware he may have embedded. He then goes ahead to extract information on the third party used to deploy services, leading to the negation of confidentiality of network drive data (See point V6 of Figure 11). An attacker may then use this information to compromise the business, leading to loss of co-operation between the3rd party and the organisation, which then affects offering business services where third parties are needed.

From the reply to the phishing email by a finance team member, an attacker can confirm that the finance member clicked the link. He may then access the data accessible by the finance team by using the embedded malware which he may have planted in the link attached.

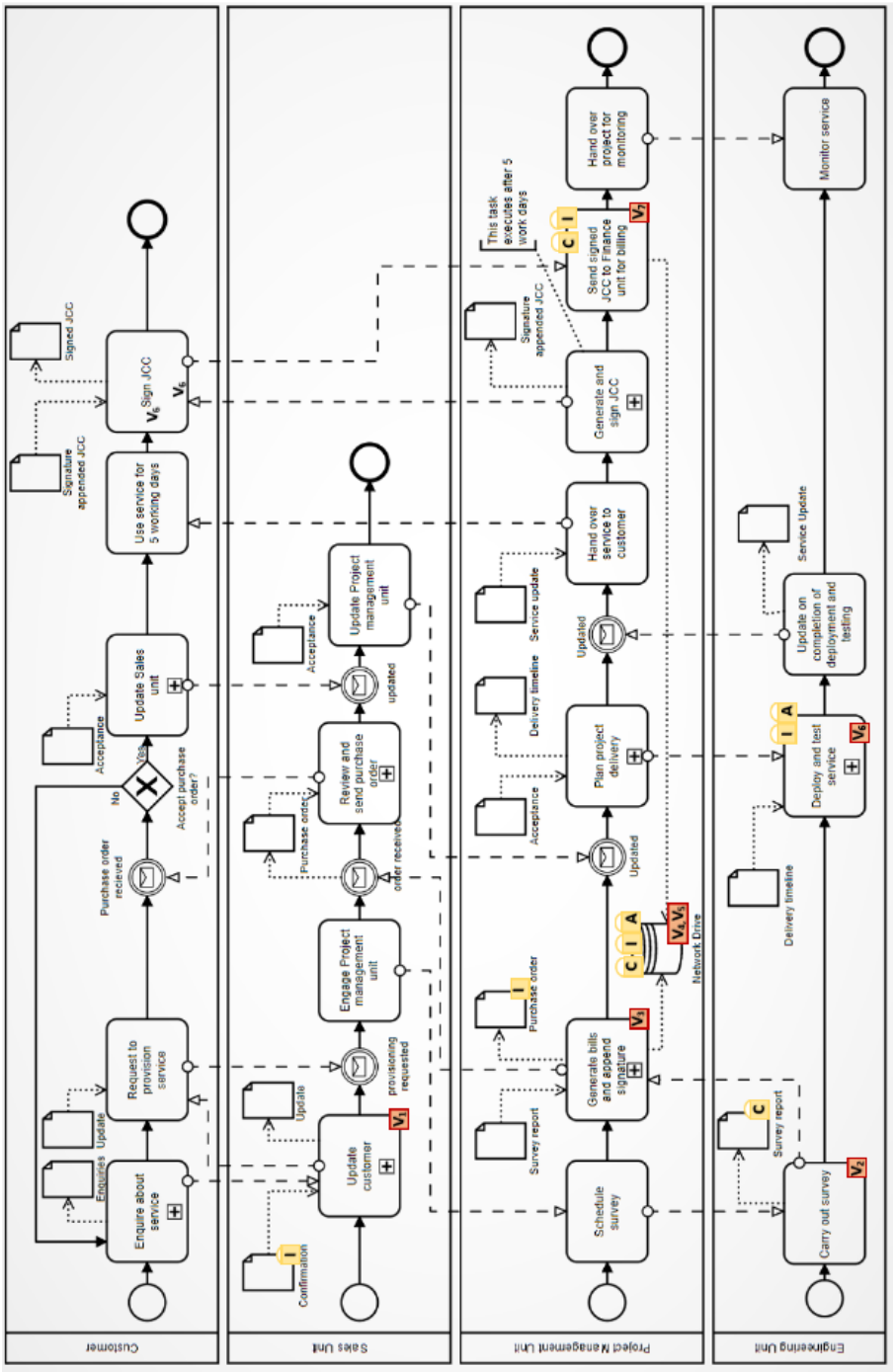


Figure 11. Risk with Clicks

This can be used to get credentials of employees and intercept the communication between the staff and client at the final stage of the business process, leading to the

negation of confidentiality and integrity of network drive data (See point V7 of Figure 11).

He gets the clients' contact details and then provides different account details to the client to have the client make payment wrongly, which leads to complications in the business between the client and the organisation, thereby affecting the business image, leading to loss of monetary value and client.

From the number of clicks monitored between the two days of the simulation, an attacker can exploit the network drive using the embedded malware to see what data he can access from each click. He may come to find out that he has access to other data within the network drive apart from what he has already accessed based on the email respondents.

However, the email respondents are members of crucial departments in the organisation when it comes to carrying out the business process. An Attacker can already have data from the network drive data based on the confirmation of the clicks from the staff members of those significant departments. With this access, an attacker can negate confidentiality, integrity and availability of network drive data.

3.5 Summary

The simulation required gathering information. The business process can be attacked with some knowledge of the business process. The information gathered on the business process and its assets can then be used to carry out the attack.

In this simulation, knowing fully well that information is shared via emails and access to network drive data is accessed using the email addresses of staff, email phishing is used. With staff clicking on the link to update email credentials, malware can be planted on the computer or network to get passwords required to access the network drive data from the clickers.

Clicks from some units have medium risks attached to them. An example is the engineering unit since both of the staff from the units are in different locations with different access. However, having both members click the link and reply to the phishing email, the combination of both clicks yields a high risk. The reason is that the attacker will now have access to engineering data from both locations.

In the same way, a high number of clicks combined with the email respondents would have resulted in a successful attack. Fewer clicks or responses to email may have given attackers access to limited network drive data.

In this section, we simulated a phishing attack based on the organisation's business process information. The steps used to carry out the simulation were described, and the impact on the business process was discussed based on the multiple points of failure. The number of clicks and responses to emails proves that the staff need training on recognising phishing. The next chapter will discuss how to train the staff on phishing. This is done to improve the level of phishing recognition.

4 Awareness and Training

In this section, we shall be answering **SQ3-How to carry out awareness of the phishing attack in the organisation?** The discussion will be based on **SQ1** and **SQ2**. A phishing awareness was carried out using a questionnaire format, and training was scheduled after this.

4.1 Questionnaire

After the simulation was carried out, a questionnaire was sent on phishing to gather details on their level of phishing attack awareness and how they recognise the attack. The questionnaire results will be used to prepare the training on phishing (see Figure 13). The questionnaire included questions on the following areas; general knowledge of phishing, types of phishing, probability of clicking links/attachments in a message, phishing experience, and phishing recognition.

The questionnaire was sent out, and it was communicated that many staff were sceptical about clicking the link to the questionnaire. This may have been because the staff were scared that the email with the questionnaire may have been phishing. The questionnaire was sent from an internal email address from the department in charge of system security in the company. This email was not sent from a group but was directly sent from an internal email address. This indicates that many of the staff do not know how to recognise a legitimate email from a phishing email. With this fear, some staff will begin to ignore legitimate emails as they do not know how to recognise phishing emails from legitimate emails. The questionnaire had a total of 55 responses.

Knowledge on Phishing

The questionnaire indicated that 91% of respondents know about phishing (see Figure 12).

Figure 12. Knowledge on Phishing

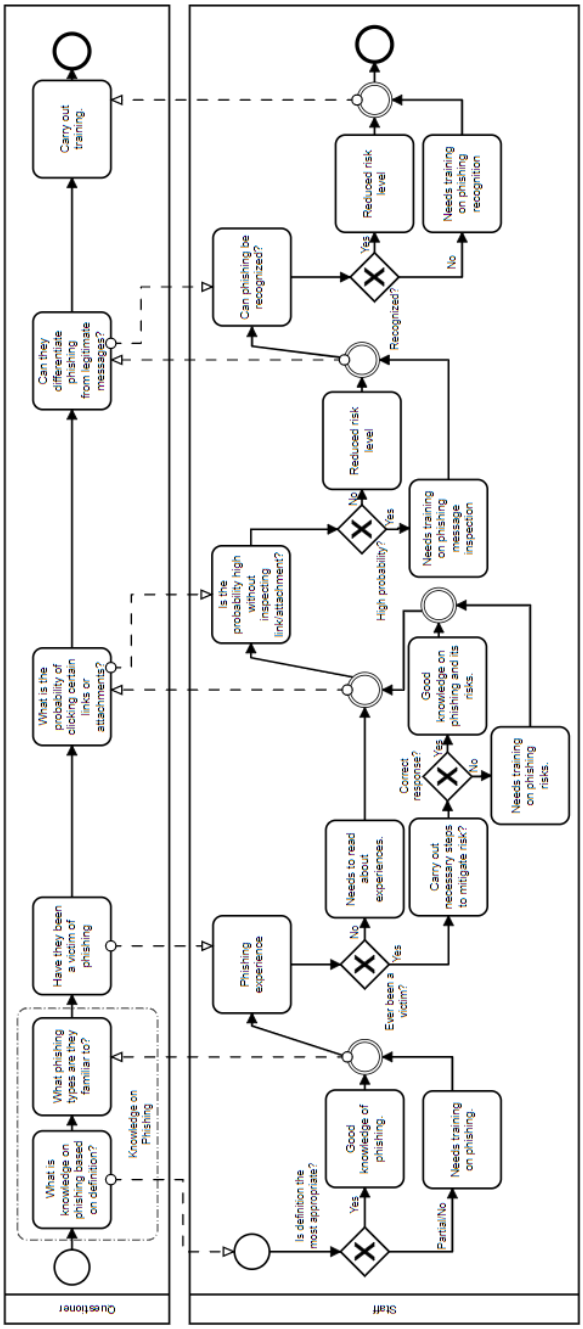


Figure 13. Questionnaire Plan

Based on the percentage, it can be perceived that they know what phishing is and how the attack is carried out. Another question was asked to estimate how well the

respondents know how the attack is carried out. A total of 43 people selected the option which best describes the attack, while four people selected the option which least explains the attack (see Figure 14).

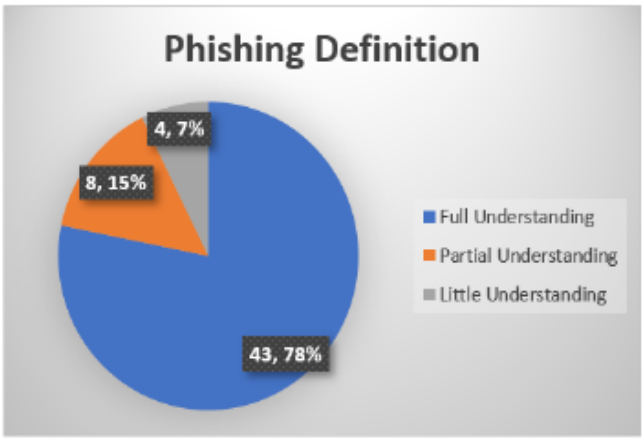


Figure 14. Phishing Definition

This can mean that some people who claim to know what phishing is can partially describe the attack, as there is an intersection with the values. This questions what they believe they know is a phishing attack or how confident staff is with the knowledge they have on phishing. Seven people out of the 50 who claim to know phishing did not select the best definition of the attack from the options provided.

According to the responses to the knowledge of types of phishing attacks, it shows that the most known type of phishing is Email phishing, while the least known type of phishing is QR phishing (See Figure 15). Based on the response to known types of phishing, it can be said that many of the respondents do not know about some types of phishing attacks. Some respondents understand the definition of the attack and know that the attacker aims to deceive the target into providing information. However, they do not know how an attacker can deliver deceiving messages to the targets. They are aware it can be done through emails and calls, but the QR phishing seemed to be not known by many of the questionnaire respondents.

Phishing Experience

A question was asked to know if staff has ever been scared to open an email because they were not sure if it was legitimate. The responses make it seem like most of the respondents fear opening emails because they are scared it may be phishing.

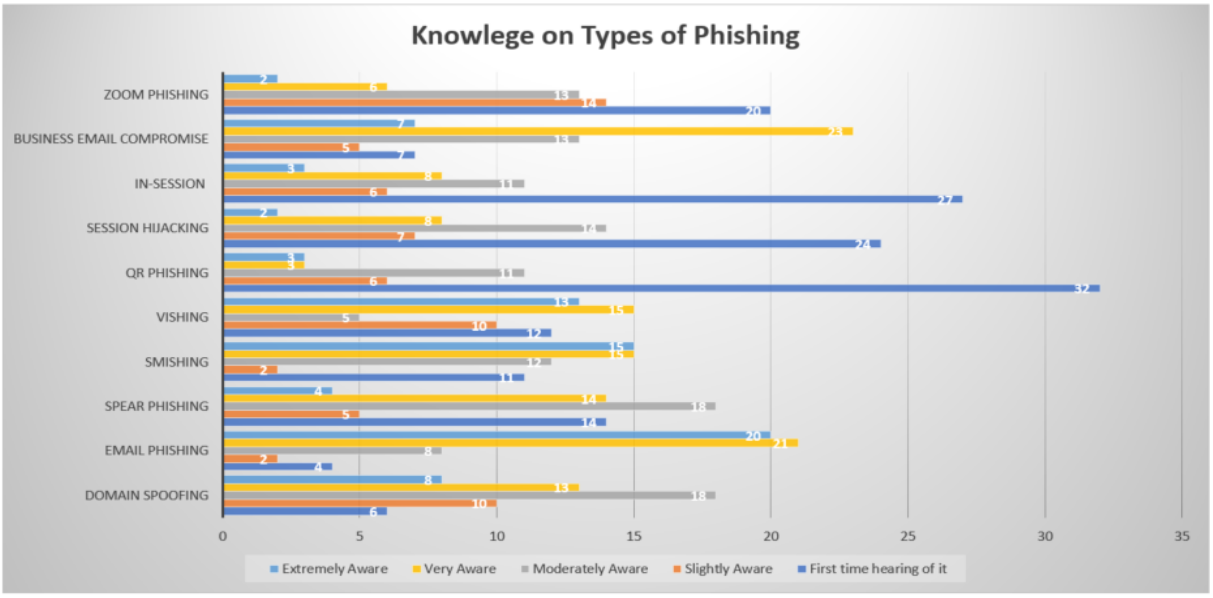
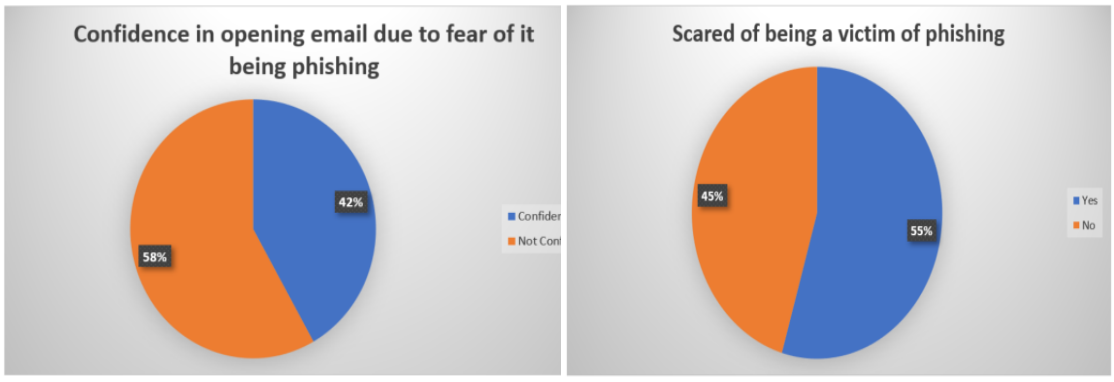


Figure 15. Types of Phishing

However, some of the respondents who say they are not scared to open emails because they are not sure if it is legitimate fall into the category of those scared of being victims of phishing (see Figure 16). In this case, it can be assumed that if they are not scared of opening emails but are scared of being victims of the attack, they should have some understanding of recognizing phishing indicators.



(a) Confidence with opening emails (b) Phishing Victim

Figure 16. Phishing Experience

Reason People Fall for Phishing Attacks

The respondents were asked to select the top five reasons they believed people fell for the attack in the questionnaire. The most selected reason was ignorance (see Figure 17). Irrespective of what is perceived in the questionnaire response to be why people fall for phishing, creating awareness of phishing and training on how to recognise the attack will help staff not depend entirely on security tools. This thereby helps prevent a targeted staff in the organisation from being a victim of the attack.

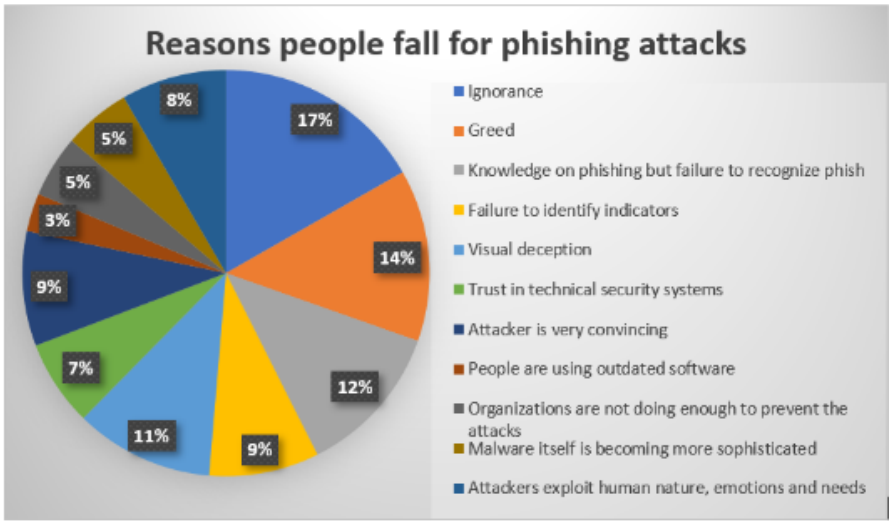


Figure 17. Reasons people fall for phishing attacks

Phishing Recognition

A series of images were displayed in the questionnaire to have staff indicate if email/SMS was phishing or legitimate. Some of the images were correctly identified, while others were not. The total percentage of correctly recognised phishing/legitimate messages to incorrectly identified messages is shown in figure 18.

A section of the questionnaire was focused on what the respondents inspect when an email is received. The essential features of the emails inspected based on the responses are the following; sender's email address, attachment/Link, signature, and contact details. These are indeed indicators to be monitored. However, it is advisable to inspect the email as a whole for indications of phishing.

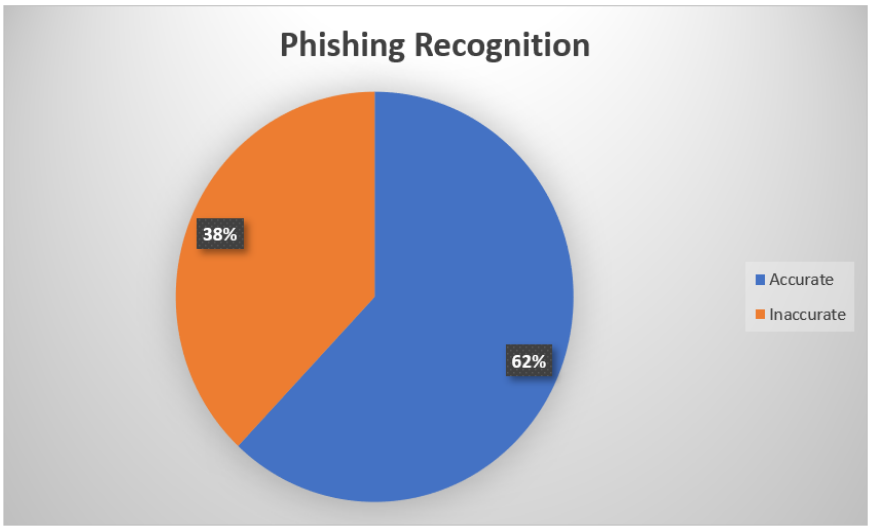


Figure 18. Phishing Recognition

4.2 Questionnaire Limitations

A limitation to the result of the questionnaire is that not all staff responded to the questionnaire. Also, it can not be verified if most of the respondents to the questionnaire were the victims of the simulated attack. Nevertheless, there were 55 respondents to the questionnaire, which gives approximately 22% of the staff population.

4.3 Training

The training was carried out based on the questionnaire result and the simulated phishing attack. Indicators of the simulated phishing attacks were discussed. Types of phishing that were listed in the questionnaire were also talked discussed. The training focused on general phishing awareness and visual examples of phishing attacks to explain the common indicators of phishing. This is done to help improve the level of recognition of phishing.

There were over 120 participants at the training, and the participants were indulged in the training. It lasted for 45 minutes as the training itself took 30 minutes, and the last 15 minutes was focused on answering questions and listening to opinions.

During the training, questions were asked about clarification of recognizing phishing attacks. Participants were also asked about the steps to carry out when they are not sure an email is a phish. Some questions asked are listed below.

- What measures should be taken when you realise you have fallen for a phishing attack?

- How can an attack on an individual affect the entire organisation?
- What if I am not sure the email or SMS is a phish? Do I just ignore it if I suspect it and see few indicators?
- As the department managing email, what should be done when an individual reports that he was a victim of phishing with his official email?

The training session was interactive, which means the staff were very well involved and interested in the phishing attacks. Some participants were able to answer questions asked by their colleagues. Unfamiliar phishing attack types based on the questionnaire were explained during the training, and some participants mentioned how they have sometimes experienced in-session phishing. However, they were not sure if it was phishing. It was explained further that when it comes to in-session phishing when a pop-up is seen concerning the session time out, it is safer to refresh the page and go to the site again and login legitimately. This is done rather than logging in directly from the pop-up.

As requested by the staff members, the training material was shared and some other documents to help improve knowledge of phishing. This means that the participants found the training material clear, valuable and resourceful.

The training was very informative, and participants learned a lot. When comparing some questions asked during the training with the responses in the questionnaire, it can be said that the trainees were able to improve in areas where they wrongly answered in the questionnaires. In general, the awareness carried out via the questionnaire and the training can be concluded to have been a very effective process. However, to verify the training efficiency, another phishing attack was carried out. This was done some weeks after the training.

4.4 Post-Training Phishing Attack

The second simulation was carried out three months after the first simulation. The timing is to give the employees ample time to relax after the first simulation and see if they will remember what was taught during the last two months after the first simulation. This simulation is going to take advantage of the Covid-19 situation worldwide.

4.4.1 Attack Deployment

The phishing email was sent out in the early hours of the day. This was done to play upon the vigilance of the staff. The email content contained a link that requested staff to provide personal information. The information was requested as a requirement to register for the COVID-19 vaccine.

The indications of phishing (see Figure 19) in the email include; fake domain, sense of urgency, attached link, inconsistency with the domain name, the email signature is generic, email content did not specify vaccine offered and grammar error.

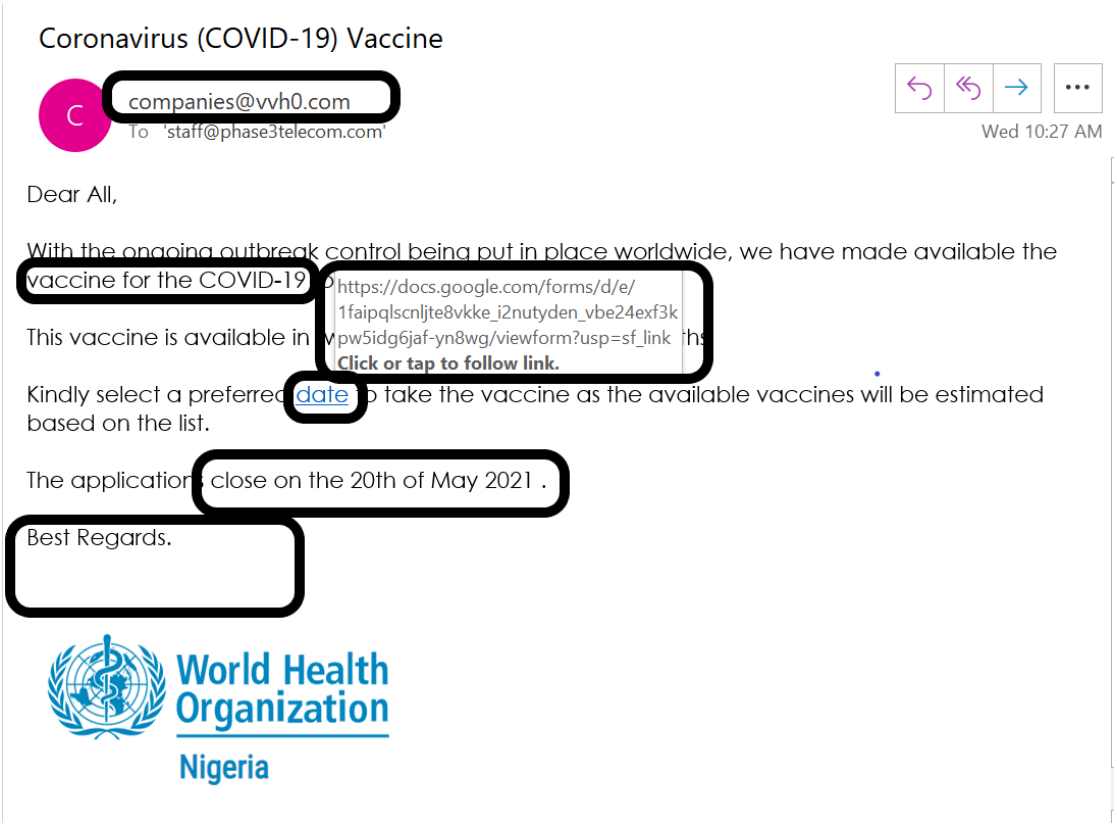


Figure 19. The Email analysis

4.4.2 Result

The second simulation was targeted at the same number of employees. The email was sent under the same condition as the first simulation. However, after the two days of the simulation period, there was no victim.

There are three possible reasons why the second simulated attack was not successful. These are elucidated below:

1. Awareness: The most probable reason is that the training on phishing carried out effectively improved staff awareness and recognition of phishing.

2. The Email: Another reason may be that the attack was not convincing enough. This could lead to staff easily identifying the email as a phish.

3. Timing: The final reason may be that the time-lapse between the first simulated attack, training, and second simulated attack was close, and staff were still vigilant before the second simulation.

Since there was no victim of the attack, the next step was to determine if the training was entirely successful by the number of reports on the email. It was recorded that nine people reached out to the department in charge of managing email to report the email as phishing. These reports were made on the first day of the attack. However, there was no report on the second day of the attack.

During the training phase of the research, staff was advised on steps to take when an email is suspected or confirmed to be phishing. The first step was to inspect the email for phishing indicators. If found and are still unsure, they can reach out to the team in charge of email to investigate further. However, if they are sure the email is a phish, they were told to inform the department in charge of email security. Having nine people report the email as a phish means the email was not suspected. This confirms that the nine reporters were sure the email was phishing.

4.5 Summary

The questions asked during the training show that participants were more enlightened on different aspects of phishing. The simulation result further confirmed that the staff could recognise the indicators of phishing in the email. Some also followed the necessary steps required to handle a suspicious email.

The result from the second simulation proves the method used for increasing phishing recognition is effective, as this was carried out after some time. The awareness and training also proved to be efficient as staff became more aware of phishing indicators, which helped them recognise phishing attacks better.

In this section, we have looked into how a phishing attack can be recognised. The questionnaire and training carried out were resultful in explaining how to recognise the phishing attack correctly. The second simulation was also carried out to have staff test the knowledge acquired during the training. In the next chapter, we shall be discussing how people can be trained to recognise phishing attacks and their impacts.

5 Discussion

This section discusses the ATTF cycle usability. The research contributes academically by implementing the ATTF cycle on the case study to raise awareness on phishing, its impact and its recognition.

5.1 Lessons Learnt

The case study using the selected telecommunication company resulted in the following lessons learnt:

- The ATTF cycle seemed to have effectively raised awareness of phishing attacks and their impact in this case study.
- Recognising phishing attacks and their impact has a positive effect on safeguarding the business assets based on the case study.
- There are few major indicators of phishing emails/messages based on the existing phishing attack types and the implemented attack in the case study.
- Phishing attacks in various organisations can be carried out in similar ways; however, the impact may vary depending on the business process or the attacker's end goal.

5.1.1 Training on Phishing Recognition

As described in section 2.2, many of the research on phishing believe that safeguarding against phishing attacks can be done by training people on the attack (see Table 1 and 2). In this research, the ATTF cycle was used for training staff on phishing recognition. Some of the core activities described by Michael in his research was covered while using the ATTF cycle [Mir16]. The research, however, followed the order below:

- Testing: In this phase, the simulation described in section 3.1 was carried out. The process involved gathering information on the company and understanding the business process to test the staff. The rest was carried out to understand how familiar phishing is to staff.

  This stage was carried out using the attack process described in section 2.3. The security update idea with a staging website was from the simulation carried out by Ahmad, and Masniza [AM19]

- Feedback: The results and observations were collected from the simulation result. The number of clicks as shown in section 3.4.2 proved staff failed to recognize

phishing. This means the phishing recognition level is low. The email respondents (see section 3.4.1) also indicate vulnerability. This information indicated that the training to be carried out would need to focus on recognizing phishing.

- Awareness: The questionnaire was sent out to fulfil this phase. The goal of the questionnaire was to deduce how much staff believe they know about phishing attacks, as explained in section 4.1. Also, the questionnaire introduced staff to other types of phishing attacks. Phishing recognition was a focus in the questionnaire, as many questions had to do with if staff could differentiate legitimate messages from phishing based on images. Based on the responses to the questions, the training was planned.

- Training: In this phase, the staff was trained on phishing and how to recognise phishing in order to distinguish a legitimate email from phishing, as explained in section 4.3. During the training, the staff asked multiple questions, which means they acquired knowledge. The training section was interactive, as some participants were able to answer questions asked by their colleagues.

- Testing: Finally, the second simulation was deployed to test the effect of the training. The approach to the simulation was different from the first simulation. From the result described in section 4.4.2, there was no victim to the second phishing simulation. This proves the training was helpful as the staff was able to identify the message as a phish.

From the result of the second simulation in this case study, this proposed cycle proves to have been effective for this case study. With this process cycle repeated, staff will constantly improve on recognising the attacks. As the repeated cycle requires keeping up to date on the updated trends of the attack, the human factor in the case study will be fortified based on the knowledge acquired, thereby safeguarding against the attack.

5.1.2 Effect of Phishing Recognition on Business Assets

The recognition of phishing attacks is essential as it helps maintain the confidentiality, integrity, and availability of valuable assets. For the case study, we used email phishing and domain spoofing where visual deception was used to influence the target to carry out actions as described in section 2.2. Below are some positive effects the recognition will have against the attack.

1. Avoid catastrophe: As many cyber-attacks are initiated by phishing, safeguarding against phishing attacks goes a long way in safeguarding against many cyber attacks.

Based on the number of clicks shown in table 7 from the first simulation, a successful phishing attack can lead to another cyber attack. This may not result in an immediate effect on the business process.

Therefore, in the long run, a future attack, when investigated, can identify the source of the attack to be the clicks. The phishing attack can create back doors with installed malware over the period before the catastrophic attack may be noticed.

The long-term effect may damage the reputation, financial losses, legal cases due to data breach, e.t.c. The result can be damaging to the company as, depending on the attack and attacker goal, the company may have to close down as they may not recover from the losses.

However, if staff awareness of phishing recognition is improved, this can be avoided. The risk of chaos can be reduced to a level that the organisation can manage.

2. Reduce risk level: Identifying phishing attacks to prevent being a victim will help reduce the risk associated with the attack. With clicks from various departments, the phishing attack risk can be reduced with fewer clicks.

   If there are only victims of the phishing attack from two units, the attacker will be limited to the network drive data accessible from those two units. Although, this will also depend on the position held by the victim of the attack and the vulnerable units.

   From the responses to the phishing emails explained in section 3.4.1, all positions held by the respondents are essential, as they all have access to valuable data. If there was a response from the unit that manages cleaning services, there would be no effect of that victim on the business process.

   Nevertheless, an attacker can still be creative and use the data from the cleaning services team to come up with another attack plan. This is why training all staff to recognise phishing attacks is essential, as it will help reduce the risk attached to the attack.

3. Reduce financial loss: Being able to identify the attack will prevent the financial expenses required to mitigate the risk attached to the attack.

   As shown in section 3.4.1, there were email responses from the finance unit and the head of another unit. This confirms there were clicks from those units. Provided that there were clicks from the units, the probability of an attacker getting vital data that can cost the organisation money is increased.

   The attack based on the vulnerability of these email responses and clicks can result in an attacker redirecting payment or restricting access to specific data. Suppose

access is restricted to this critical data, an attacker can ask a company to pay a massive sum before he can release the data to them, as discussed in section 3.4.3.

Nonetheless, if the attack can be recognised by these units with access to classified data, the financial loss can be reduced or eliminated. This also applies to members of all units, as an attacker can make use of any information he deems valuable to request for a ransom.

4. Protect reputation: A successful phishing attack on an organisation affects the business's reputation as the attack steals data, which leads to trust in the business being reduced.

   If an attacker can access business partners, customers, and private organisation data based on the clicks from various units, this information can be disclosed or sold to the black market. The information on such a breach will affect the organisation's image.

   As discussed in table 5, a successful attack based on the clicks and responses in section 3.4, the reputation of the company will be tarnished, and the business will be affected.

   Notwithstanding, if the attack can be recognised, the data may not be accessible by the attacker. With the attacker being unable to access data that can damage the company's reputation, the impact is managed.

5.1.3 Recognizing Phishing Attacks

Recognising phishing attacks can only be done by identifying the phishing indicators. This makes the explanation of phishing indicators important during the training on phishing. During the training, most of the phishing examples had common indicators. It is important to note that phishing attacks evolve, and new indicators will need to be discovered over time. Some of the common indicators of phishing are explained below:

1. Sender identity: In the case of email phishing, the email address should be inspected. Sometimes, the attacker uses a legitimate name but a fake domain for email. This name could be a member of the organisation or a business partner.

   In the simulation carried out in section 4.4.1, this was an obvious indication of phishing. The domain name used was similar to the organisations' domain but was not the same. The second simulation aimed to deceive staff into thinking the email was from the World Health Organisation (WHO), but the domain name was incorrect.

   When it comes to vishing or smishing, unknown phone numbers should be suspected, and if the caller does not give a proper introduction (name) or organisation, this should be suspected as a phish.

2. Generic greeting: Many legitimate emails are not sent out with generic greetings. This indicator is significant in identifying spear-phishing emails.

   An example of a generic greeting is 'Dear user'. A legitimate email from a legitimate source will identify the user by name and not the identity 'user'. An attacker tends to use a generic greeting as, most times, phishing messages are sent to multiple people at a time in order to get feedback from as many as possible.

   In the case where some organisations use greetings such as 'Dear all ',' Dear staff'. e.t.c, it is crucial to be familiar with the terms used by the organisation.

3. Subject: If the subject of the email/SMS is too good to be true or has some sense of urgency, the email should be inspected.

   In many cases, the attacker uses interesting email subjects to lure victims' attention to what he has to communicate. Sometimes, the subject may be about a sale or something more critical, such as an update on the business, work, or health-related topics used in the simulations carried out in this research.

   Email subjects give a clue whether an email is legitimate or not. Some email clients, such as Microsoft Outlook, identify spam messages based on the email subject.

4. Sense of urgency: Phishing email/SMS and calls always have a sense of urgency. A time frame is communicated to have certain activities carried out.

   Many of these phishing messages or calls always require action to be taken within a short period. The reason is that the attacker most likely wants to carry out the attack and be able to track the process.

5. Attachment/Link: Attachments and links should be inspected for inconsistencies. If the link attached does not match a legitimate link or the domain of the sender of the SMS/email or caller, this should be investigated further.

   For the simulation in this research, the links used were consistent with the domain name used. However, if the domain name had not been recognised as fake from the email address, the link would have been another sellout for the phishing attack. Sometimes, the domain name used in email is correct, but the link/attachment is redirecting to a spoofed domain.

6. Grammar or spelling mistakes: Grammar or spelling mistakes in the message content are sometimes an indication of phishing. However, with attacks evolving, this indicator will not always be seen.

5.2 Contributions

The contribution of the thesis has been reflected through the various sections. These contributions are as follows:

1. Proposing a method that can raise awareness on recognising phishing attacks and their impact. Since attacks can pass through security tools, raising awareness of attack recognition can help safeguard against the attack. The ATTF cycle was applied to the case study to raise awareness of phishing attack recognition and its impact. During the case study, the different stages of the cycle were practised and then testing was repeated. For this case study, the ATTF cycle showed a positive outcome with no victim to the second simulated phishing attack, which was done for testing.

2. The case study, its results and lesson learned contributes to future research on phishing. The case study applied the ATTF cycle for raising awareness on phishing recognition and its impact on a telecommunication company. The result from the case seemed to show how much staff within this company perceive their knowledge on phishing. Having many clicks and few responses to the phishing email shows vulnerability. One click can cause damage depending on what privilege the clicker has when accessing the network drive data. It can be perceived that staff did not know how to differentiate a phishing email from a legitimate email since the staff was sceptical about opening the questionnaire sent from an official internal email address. Nevertheless, carrying out the training on phishing recognition and its impact seemed to have raised the ability for staff to recognise phishing emails as there was no victim to the second phishing attack.

3. The stages of the ATTF cycle are similar to steps that Michael has proposed for carrying out training on phishing [Mir16]. The cycle further employed a simulation for testing as the research by Steven et al. [MMS18] presented that phishing simulations can be used to reduce the susceptibility of phishing attacks. The simulations used in the case study was done based on phishing attack processes described by Hossein et al. [ADPL21]. Zuochao et al. research which explained the five stages of phishing attacks, was also used for designing the attack process for the simulation [DKK+17]. The research applied existing researches for the case study.

4. The lesson learnt from this case study can be generalised. Many phishing attacks are carried out with similar end goals. However, the attack method and its impact may varydepending on the target and what the attacker stands to gain. The research used the ATTF cycle for training staff of a telecommunication organisation on phishing attacks and their impact. The end goal was to train staff to recognise the

phishing attack and its impact. The method used in the different stages of the cycle may vary depending on the training audience. In this case study, email phishing and domain spoofing were used because the business process and assets revolve around emails. The ATTF cycle can be applied to different types of the audience using different approaches at each stage.

6 Conclusion

This chapter gives a summary of the thesis paper. It explains the research limitations, answers the research questions, provides recommendations for future work and concludes the research.

This paper analysed phishing attack recognition and its impact on the business process using a telecommunication company for the case study. To train the staff of this organisation to recognise phishing attacks and their impacts, we researched what the attack is and how they are carried out.

To proceed with the research, we implemented the ATTF cycle. A phishing attack was simulated in the testing phases to see if staff can recognise phishing attacks. The simulation was done using the information gathered on email phishing and domain spoofing. This experiment was carried out on people who seem to be learned and conversant with technology evolution.

After the simulation was done, we used the result to generate a questionnaire and plan the training to improve how to recognise phishing attacks and their impacts.

6.1 Limitation

The limitations of the research work is explained below:

1. Case Study: A telecommunication company was used for this case study. The simulated attack results impact the phishing attack, and training results are for this particular company. As the phishing attack methods are similar, the impact on various organisations will vary depending on their business processes. The training approach and result may also differ depending on the company.

2. Time Factor: As the research was approached using the ATTF cycle discussed in section 5.1.1, a time gap is required between each phase of the cycle. In this research, the entire ATTF cycle was concluded within three months. With more time being available, more data will be collected. Also, with time, the results may be different because staff may have forgotten what they have learned between each stage of the cycle. Therefore, staff will show more vulnerability, and with the indicators remembered or forgotten, we can repeat the ATTF cycle more times.

3. Types of Phishing: For this case study, email phishing and domain spoofing were used. Unfamiliar phishing types such as QR code or In-session phishing were not used. Email phishing and domain spoofing were used because the company used for the case study carries out processes using emails. In this case, selected phishing types were more relatable to the simulation.

4. Monitor Clicks: For this case study, the website's access log was used to monitor the number of clicks during the simulation. Clicks from within the company networks were recorded in the access log as a single IP, the company's external IP address. This did not help identify the uniqueness of clicks. However, a more effective method can be using a C&C (command and control) malware which will be installed on devices of clickers to get the total number of unique clicks. Nevertheless, this will depend on what the company to be used for the case is convenient with using.

5. Evolution of Phishing: During the research, existing phishing types were studied. The attack methods and indicators were gathered. However, attackers seem always to get creative and could work on known indicators to mislead targets. Over time, the indicators may change, and this will need to be learned.

6.2 Answer to Research Question

This section answers the research questions in Section 1.

- SQ1. *What are phishing attacks and how are they executed in different organisations?*

  As discussed in section 2.2, there are multiple types of phishing attacks of which include email phishing, domain spoofing, QR phishing, In-session phishing e.t.c. Many of these phishing types are not familiar to people; however, the goal of most phishing attacks is the same. All phishing attacks aim to make the target act, which they usually would not. Also, the attack methods are similar as the attack plan requires the target to click on a link/image/attachment or button, with the goal being to get sensitive data from the target.

  Various organisations have carried out simulations using email phishing on their employees. In most cases, monetary incentives are used to deceive the employees into carrying out the actions required. These actions involve clicking on a link or attachment and then claiming the reward. As explained in table 3, many employees from different organisations failed to recognise the emails as a phish. Some of these victims were then advised to take phishing awareness programs.

- SQ2. *What is the impact of a phishing attack on organisation's business process?*

  The impact of phishing on an organisation's business processes varies depending on the organisation. The impact may also depend on other factors such as the worth of an organisation based on monetary values, the end goal of the attack, or if the attack is only a backdoor for another attack.

  During the simulation described in section 3.1, the results of the clicks can result in impacts described in the possible risk discussed in table 4, table 5 and table 6.

The impact based on the email respondents, as explained in section 3.4.3, can also cause more harm such as monetary loss, tarnish to business reputation, e.t.c.

- SQ3. *How to carry out awareness of the phishing attack in the organisation?*

  Many research works have stated that safeguarding against phishing attacks can be done by creating awareness and training people on phishing attacks. However, awareness of phishing goes beyond informing people about phishing attacks, the types of phishing attacks, and how to recognise phishing attacks.

  The ATTF cycle proved to be somewhat efficient in this case study. The process involved informing staff on the basics of phishing. These basics included its types, how it is performed, and its impact. It also put staff in the position to practise what they had learned while combining what they knew. Carrying out phishing awareness should always include having participants practise what they learn.

6.3 Concluding Remarks

This primary research question, **"How to raise people's awareness of phishing attacks and their impacts?"** served as a guide for this research. Training on phishing attacks should not be limited to teaching terms and processes. It should involve some practice using simulations or games, as practice makes a person better at what they do.

Based on the simulations and questionnaire used in this case study, it was perceived that some staff did not know how to recognise phishing. From the inspection of emails, the staff was able to identify a few features of emails to be inspected for phishing. With inadequate knowledge of phishing recognition, a successful phishing attack could be launched against this company, thereby disrupting its business process. The impact on the business process of this company can result in damage. This damage includes, but is not limited to, loss of monetary value, reputation damage, identity theft, legal issues.

Training the staff on the types, trends of phishing attacks and identifying these attacks will go a long way in preventing a successful attack. The ATTF cycle described in section 1.5 was used as a guide to carry out this research. For this case study, the ATTF cycle seemed to have been a good way to raise awareness on phishing attacks, their impact and how to recognise the attack. This is said because there was no victim to the second simulated attack. However, this cycle should be done with a time spacing of months, so the time factor serves to remind them of what has been learned so far. At each stage of the cycle, information was collected on how staff already recognised phishing and how to train them on areas they seemed to lack.

6.4 Future Work

As discussed in section 6.1, the time factor is essential with training using the ATTF cycle as a guide. Although the paper focused on the case study using email phishing and domain spoofing, other phishing attacks may be used for the testing stage of the cycle. Based on the knowledge of different types of phishing, the least known phishing types can be used to carry out further studies on phishing. As a proposal for future work, the ATTF cycle can be attempted using other phishing types over a better spread of time.

Also, for this case study, a telecommunication company was used, and the training results are limited to this particular company. The ATTF cycle can be applied in training people in other industries or companies. The process of the cycle will remain the same; however, the approach may vary. If a simulation is to be used, it is recommended to use a more reliable option to monitor the clicks on links/attachments.

Finally, as attackers become creative with phishing attack methods, the indicators may change over time. Phishing attacks based on technical subterfuge do not have known apparent indicators. For future work, these types of phishing can be researched thoroughly to find indicators, which can then be used to carry out awareness training.

References

[ADPL21] H. Abroshan, J. Devos, G. Poels, and E. Laermans. Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. *IEEE Access*, 9:44928–44949, 2021.

[AM19] A. S. Abdullah and M. Mohd. Spear phishing simulation in critical sector: Telecommunication and defense sub-sector. In *2019 International Conference on Cybersecurity (ICoCSec)*, pages 26–31, 2019.

[AP20] A. A. Athulya and K. Praveen. Towards the detection of phishing attacks. In *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, pages 337–343, 2020.

[APW19] APWG. Phishing activity trends report: 3rd quarter 2019. `https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf`, 2019. Last accessed 25-Jan-2021.

[APW20] APWG. Phishing activity trends report: 1st quarter 2020. `https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf`, 2020. Last accessed 25-Jan-2021.

[Ban19] Z. Banach. What is session hijacking: Your quick guide to session hijacking attacks. `https://www.netsparker.com/blog/web-security/session-hijacking/`, August 2019. Last accessed 12-Feb-2021.

[BPC11] M. Blythe, H. Petrie, and J. A. Clark. F for fake: Four studies on how we fall for phish. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, page 3469–3478, New York, NY, USA, 2011. Association for Computing Machinery.

[Car14] R. Carpenter. The four rs of deep learning. `https://newforums.com/four-rs-deep-learning/`, 2014. Last accessed 22-Dec-2020.

[CG06] J. Chen and C. Guo. Online detection and prevention of phishing attacks. In *2006 First International Conference on Communications and Networking in China*, pages 1–7, 2006.

[Cis20] Cisco. What is phishing? *Email Security*, 2020.

[DKK+17] Z. Dou, I. Khalil, A. Khreishah, A. Al-Fuqaha, and M. Guizani. Systematization of knowledge (sok): A systematic review of software-based web phishing detection. *IEEE Communications Surveys Tutorials*, 19(4):2797–2819, 2017.

[Dro19] M. Drolet. Smishing and vishing: How these cyber attacks work and how to prevent them. https://www.csoonline.com/article/3411439/, August 2019. Last accessed 5-Feb-2021.

[DTH06] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, page 581–590, New York, NY, USA, 2006. Association for Computing Machinery.

[GL15] R. Gonzalez and M. E. Locatso. An interdiscplinary study of phishing and spear-phishing attacks. https://cups.cs.cmu.edu/soups/2015/papers/eduGonzales.pdf, 2015. Last accessed 25-Feb-2021.

[GST18] K. Greene, M. Steves, and M. Theofanos. No phishing beyond this point. *Computer*, 51(6):86–89, 2018.

[HKOK19] M. Higashino, T. Kawato, M. Ohmori, and T. Kawamura. An anti-phishing training system for security awareness and education considering prevention of information leakage. In *2019 5th International Conference on Information Management (ICIM)*, pages 82–86, March 2019.

[HRJA19] R. A. A. Helmi, C. S. Ren, A. Jamal, and M. I. Abdullah. Email anti-phishing detection application. In *2019 IEEE 9th International Conference on System Engineering and Technology (ICSET)*, pages 264–267, 2019.

[Imp20] Imperva. Phishing attacks. https://www.imperva.com/learn/application-security/phishing-attack-scam/, 2020. Last accessed 28-Jan-2021.

[JGST20] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach. Don't click: towards an effective anti-phishing training. a comparative literature review. *Human-centric Computing and Information Sciences*, 10(1), 2020. Cited By :1.

[Kasa] Kaspersky. A guide to qr codes and how to scan qr codes. https://www.kaspersky.com/resource-center/definitions/what-is-a-qr-code-how-to-scan. Last accessed 2-Feb-2021.

[Kasb] Kaspersky. What is spear phishing? https://https://www.kaspersky.com/resource-center/definitions/spear-phishing. Last accessed 25-Jan-2021.

[KFR+15] K. Krombholz, P. Frühwirt, T. Rieder, I. Kapsalis, J. Ullrich, and E. Weippl. Qr code security – how secure and usable apps can protect users against malicious qr codes. In *2015 10th International Conference on Availability, Reliability and Security*, pages 230–237, 2015.

[Lon20] L. Longhi. Godaddy employees were told they were getting a holiday bonus. it was actually a phishing test. https://coppercourier.com/story/godaddy-employees-holiday-bonus-secruity-test/, December 2020. Last accessed 28-Feb-2021.

[Mir16] J. A. M. Miranda. Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, 14, 2016.

[MMS18] S. McElwee, G. Murphy, and P. Shelton. Influencing outcomes and behaviors in simulated phishing exercises. In *SoutheastCon 2018*, pages 1–6, 2018.

[MS19] S. Mishra and D. Soni. Sms phishing and mitigation approaches. In *2019 Twelfth International Conference on Contemporary Computing (IC3)*, pages 1–5, 2019.

[Phi18] PhishLabs. 2018 phishing trends & intelligence report: Hacking the human. https://info.phishlabs.com/, 2018. Last accessed 22-Dec-2020.

[Pic20] A. Picchi. Tribune workers got an email dangling a bonus — but it was a hoax from their employer. https://www.cbsnews.com/news/tribune-bonus-email-hoax-cybersecurity-test/, September 2020. Last accessed 2-Mar-2021.

[Pra16] S. Prashin. W.a.d beyond global. https://www.wad.net/assets/Newsletters/vol66.pdf, 2016. Last accessed 25-June-2021.

[Sec20] Abnormal Security. Zoom phishing. https://abnormalsecurity.com/blog/abnormal-attack-stories-zoom-phishing/, 2020. Last accessed 12-Feb-2021.

[Shw16] K. Shwab. The Fourth Industrial Revolution: what it means, how to respond. *Fourth Industrial Revolution*, 2016.

[SY19] A. Sumner and X. Yuan. Mitigating phishing attacks: An overview. In *Proceedings of the 2019 ACM Southeast Conference*, ACM SE '19, page 72–77, New York, NY, USA, 2019. Association for Computing Machinery.

[Sym18] Symantec. Internet security threat report (isrt). https://docs.broadcom.com/doc/istr-23-executive-summary-en, 2018. Last accessed 12-Jan-2021.

[Sym19] Symantec. Internet security threat report (isrt) - 2019. https://www.phishingbox.com/news/phishing-news/

internet-security-threat-report-irst-2019, 2019. Last accessed 12-Jan-2021.

[TYU20] S. Teerakanok, H. Yasuki, and T. Uehara. A practical solution against business email compromise (bec) attack using invoice checksum. In *2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 160–167, 2020.

[Ver19] Verizon. 2019 data breach investigations report. https://www.phishingbox.com/assets/files/images/Verizon-Data-Breach-Investigations-Report-DBIR-2019.pdf, 2019. Last accessed 24-Jan-2021.

[Was20] R. Wash. How experts detect phishing scam emails. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW2), October 2020.

[YCT19] K. S. C. Yong, K. L. Chiew, and C. L. Tan. A survey of the qr code phishing: the current attacks and countermeasures. In *2019 7th International Conference on Smart Computing Communications (ICSCC)*, pages 1–5, 2019.

Appendix

A. Search Process

For the purpose of the research, digital libraries such as Scopus, ACM and IEEE were used. Papers and reports were also reviewed from other sources. Included in the search queries are ("Phishing" OR "Email Phishing") AND ("Social Engineering") AND ("Attacks" OR "Simulations")AND ("Attack Process"), ("Phishing attack") AND ("Telecommunication Industry" OR "organisation").

Selected Search Sources for Literature Review

Table 9. Criteria on selected papers

Sources	IEEE	Scopus	ACM	APWG	Other sources
	14	2	4	4	22

B. Experimental Phase

I. The Business Process

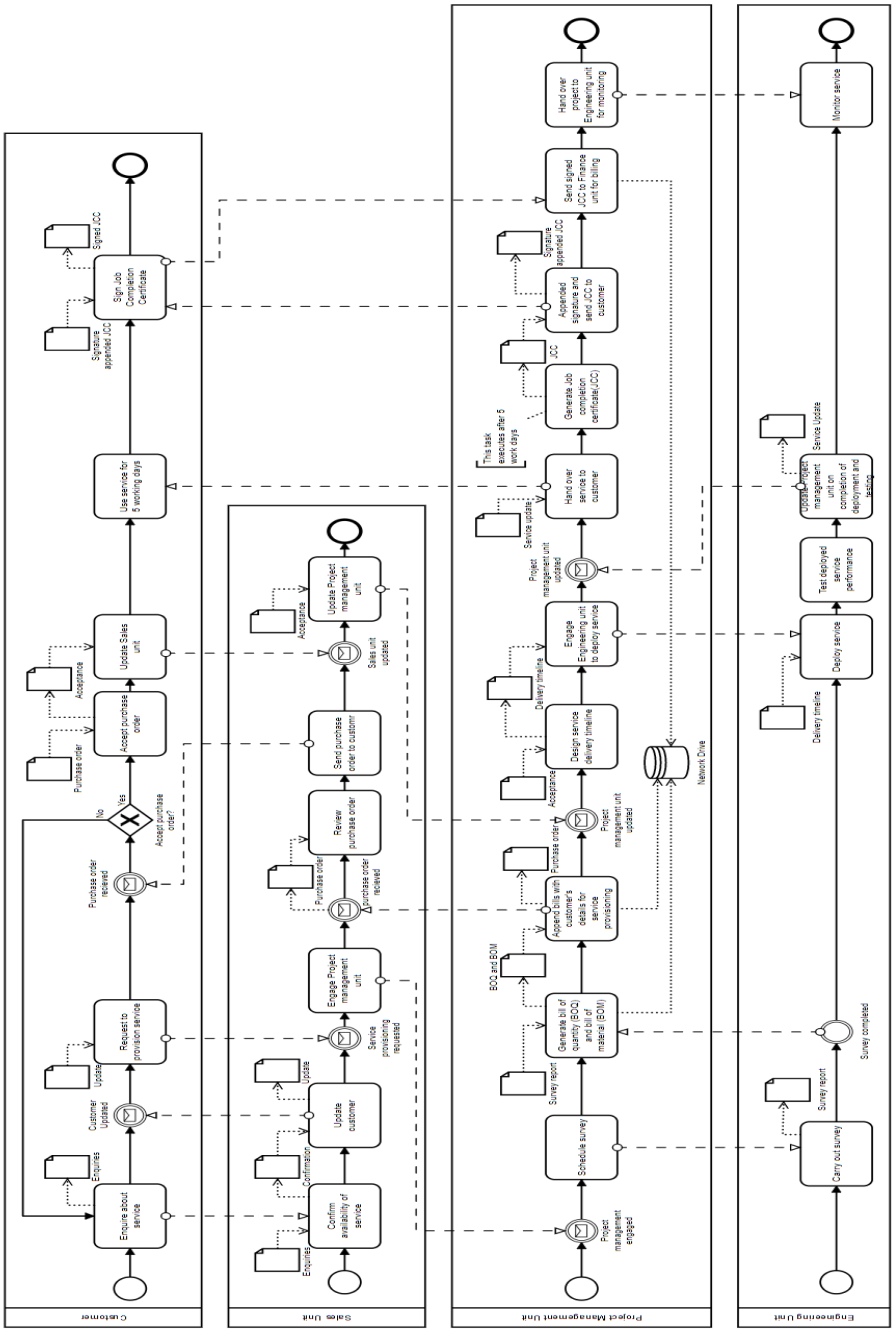
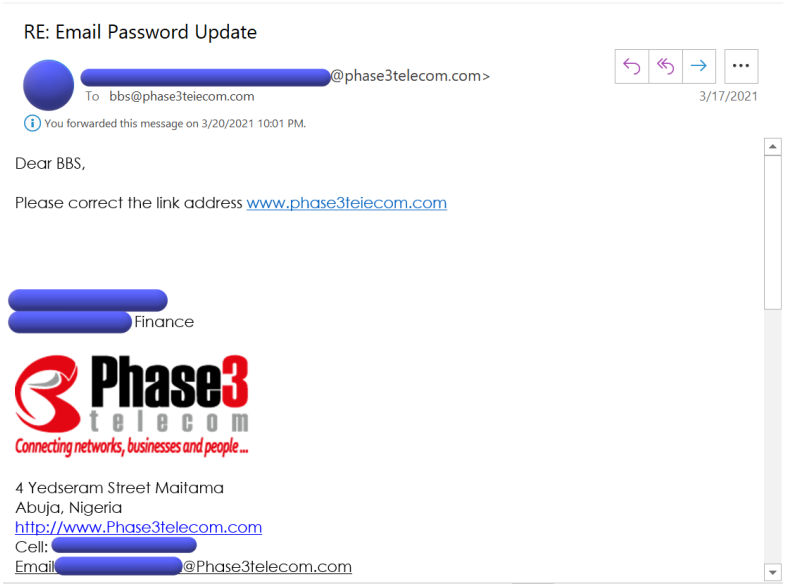


Figure 20. Business process expanded.

II. The Email Responses


RE: Email Password Update

[redacted]@phase3telecom.com>

To bbs@phase3teiecom.com

3/17/2021

You forwarded this message on 3/20/2021 10:01 PM.

Dear BBS,

Please correct the link address www.phase3teiecom.com

[redacted]

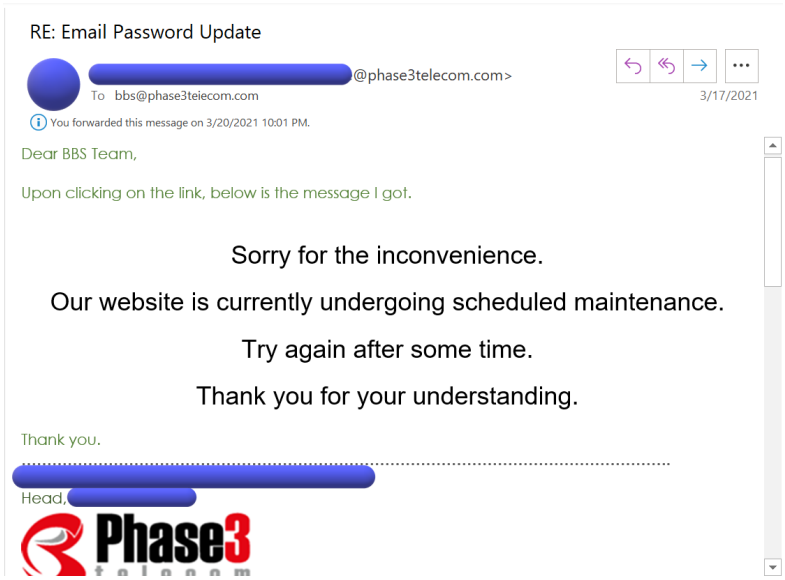
[redacted]Finance

Phase3 telecom

Connecting networks, businesses and people...

4 Yedseram Street Maitama
Abuja, Nigeria
http://www.Phase3telecom.com
Cell: [redacted]
Email[redacted]@Phase3telecom.com

Figure 21. Reply from finance staff.


RE: Email Password Update

[redacted]@phase3telecom.com>

To bbs@phase3teiecom.com

3/17/2021

You forwarded this message on 3/20/2021 10:01 PM.

Dear BBS Team,

Upon clicking on the link, below is the message I got.

Sorry for the inconvenience.

Our website is currently undergoing scheduled maintenance.

Try again after some time.

Thank you for your understanding.

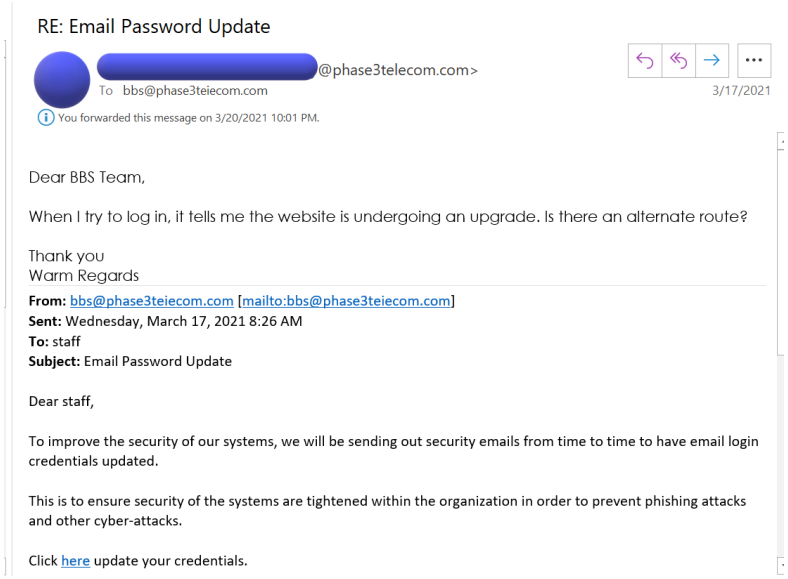
Thank you.

[redacted]

Head, [redacted]

Phase3 telecom

Figure 22. Reply from head of unit



RE: Email Password Update

[redacted]@phase3telecom.com>

To bbs@phase3teiecom.com

3/17/2021

You forwarded this message on 3/20/2021 10:01 PM.

Dear BBS Team,

When I try to log in, it tells me the website is undergoing an upgrade. Is there an alternate route?

Thank you
Warm Regards

From: bbs@phase3teiecom.com [mailto:bbs@phase3teiecom.com]
Sent: Wednesday, March 17, 2021 8:26 AM
To: staff
Subject: Email Password Update

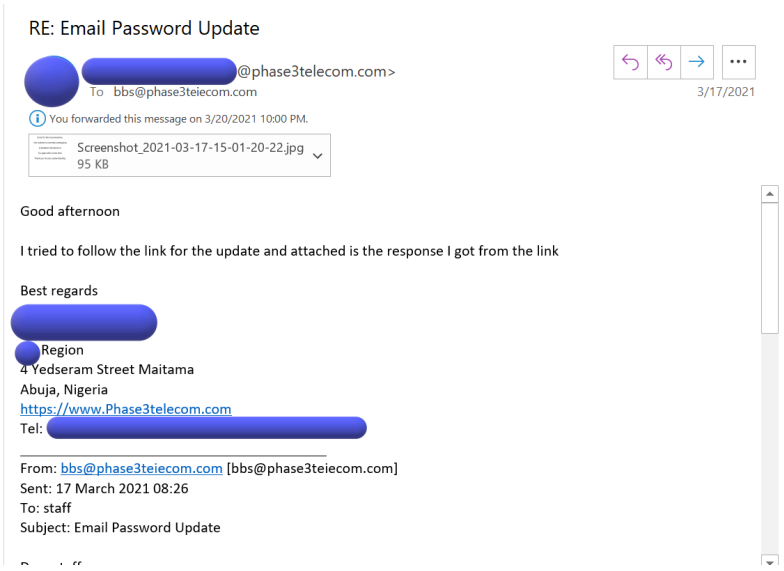
Dear staff,

To improve the security of our systems, we will be sending out security emails from time to time to have email login credentials updated.

This is to ensure security of the systems are tightened within the organization in order to prevent phishing attacks and other cyber-attacks.

Click here update your credentials.

Figure 23. Reply from department with access to staff data.



RE: Email Password Update

[redacted]@phase3telecom.com>

To bbs@phase3teiecom.com

3/17/2021

You forwarded this message on 3/20/2021 10:00 PM.

Screenshot_2021-03-17-15-01-20-22.jpg
95 KB

Good afternoon

I tried to follow the link for the update and attached is the response I got from the link

Best regards

[redacted]
[redacted] Region
4 Yedseram Street Maitama
Abuja, Nigeria
https://www.Phase3telecom.com
Tel: [redacted]

From: bbs@phase3teiecom.com [bbs@phase3teiecom.com]
Sent: 17 March 2021 08:26
To: staff
Subject: Email Password Update

Figure 24. Reply from engineering staff.

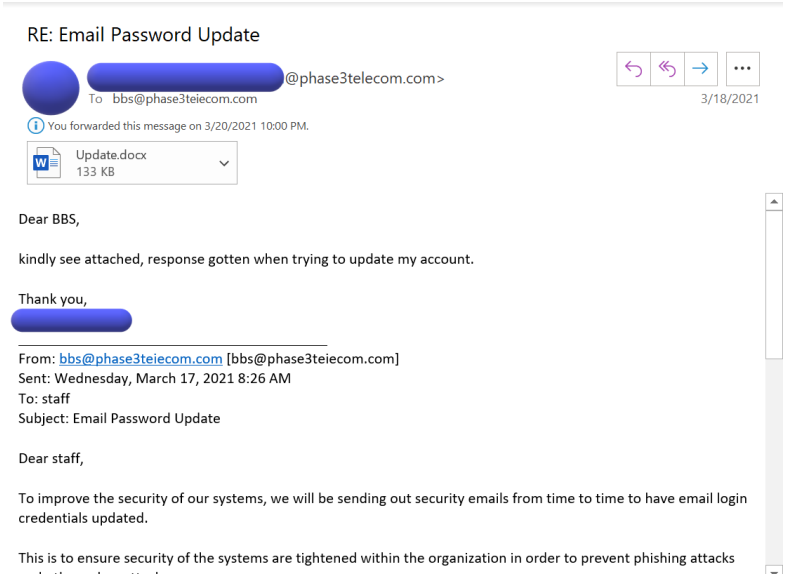


Figure 25. Reply from engineering staff.

III. Impact of clicks to the Business Process

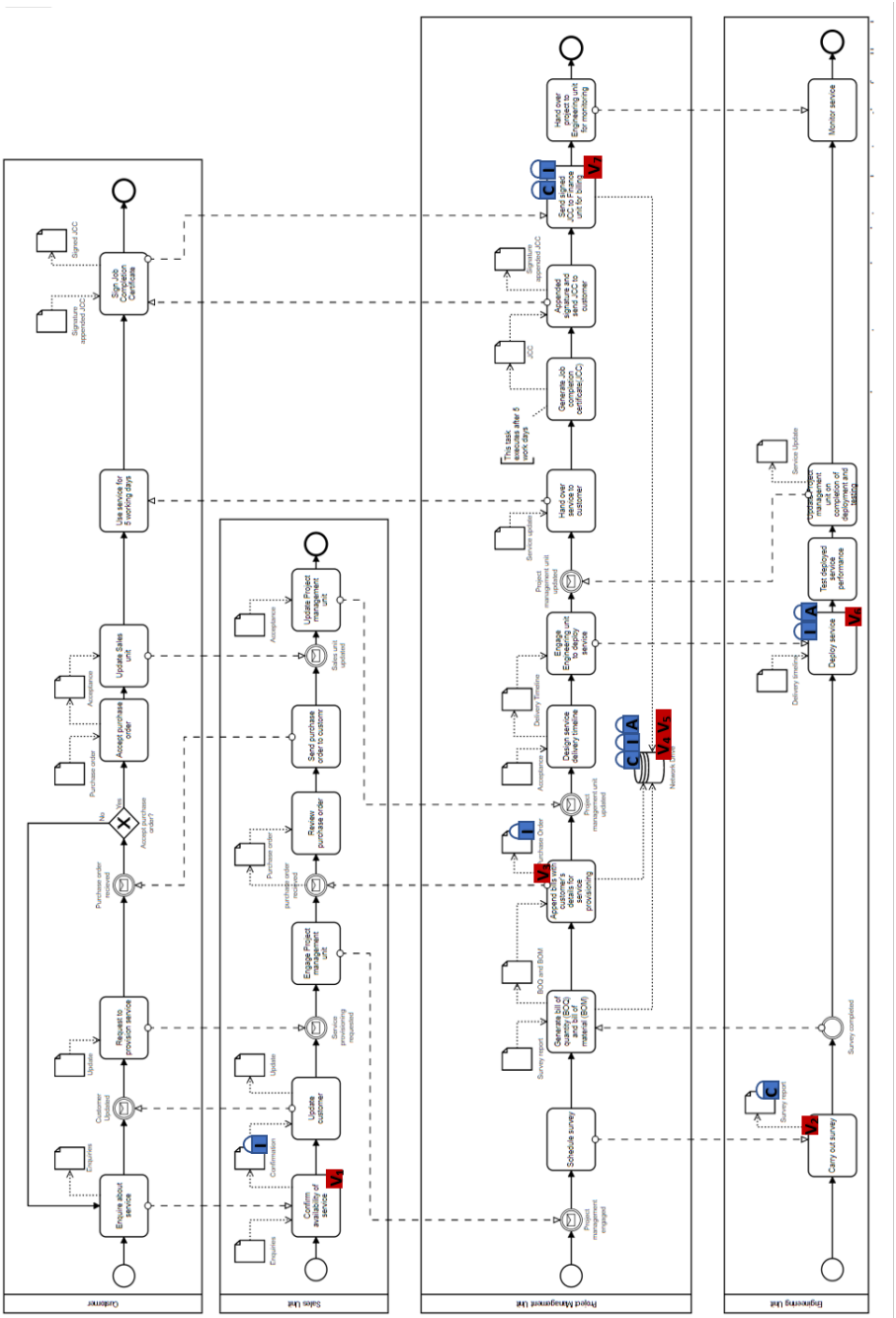
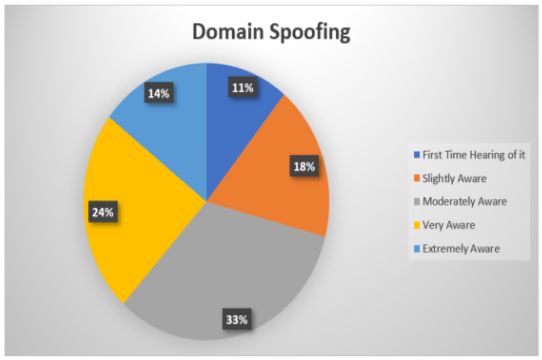
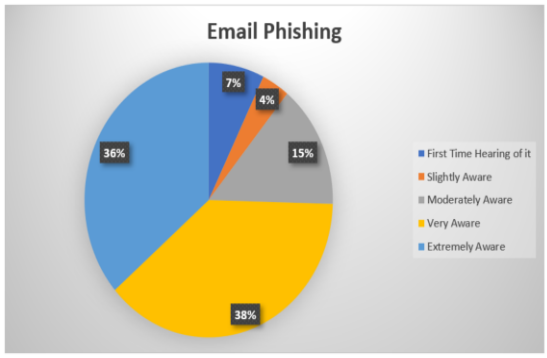


Figure 26. Impact of clicks to the business process expanded.

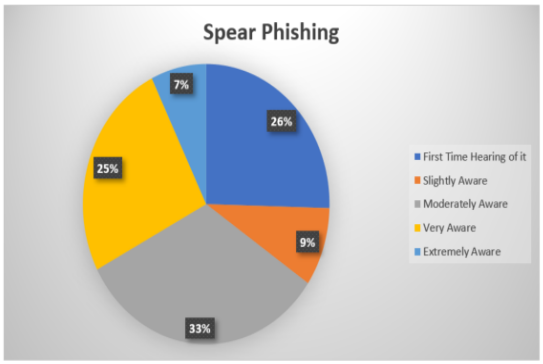
IV. Questionnaire Result



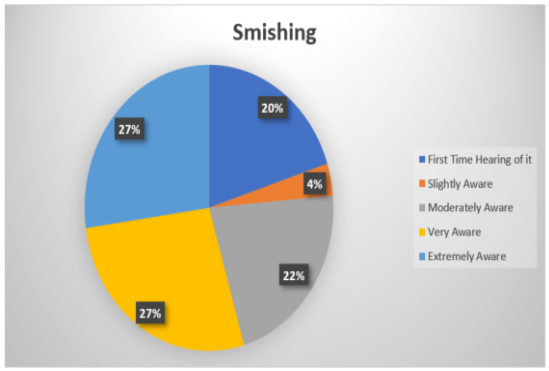
(a) Domain Spoofing



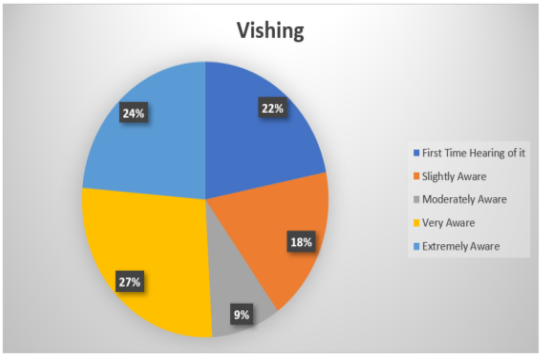
(b) Email Phishing



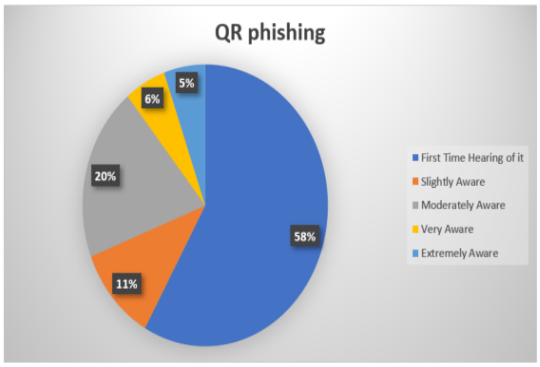
(c) Spear Phishing



(d) SMS Phishing

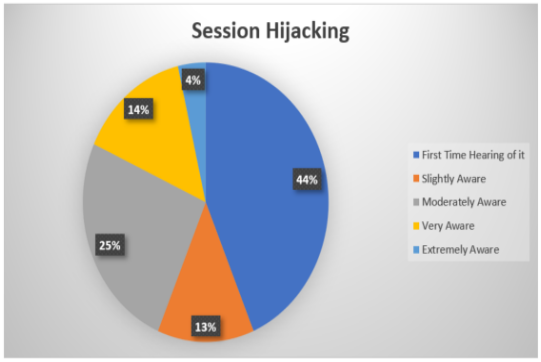


(e) Voice Phishing

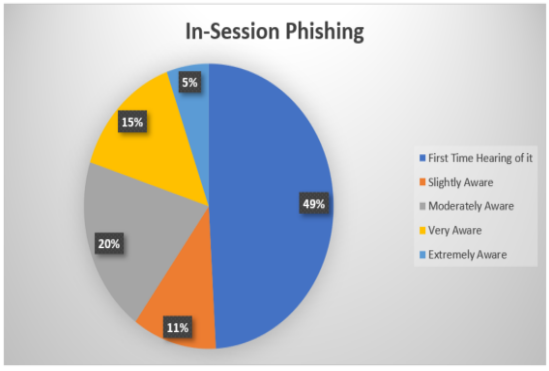


(f) QR Phishing

Figure 27. Knowledge on Phishing Types (I)

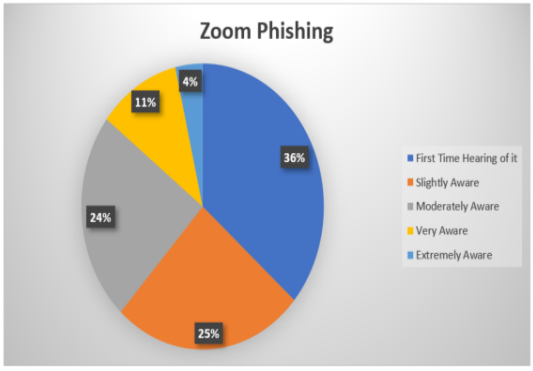


(a) Session Hijacking



(b) In-Session

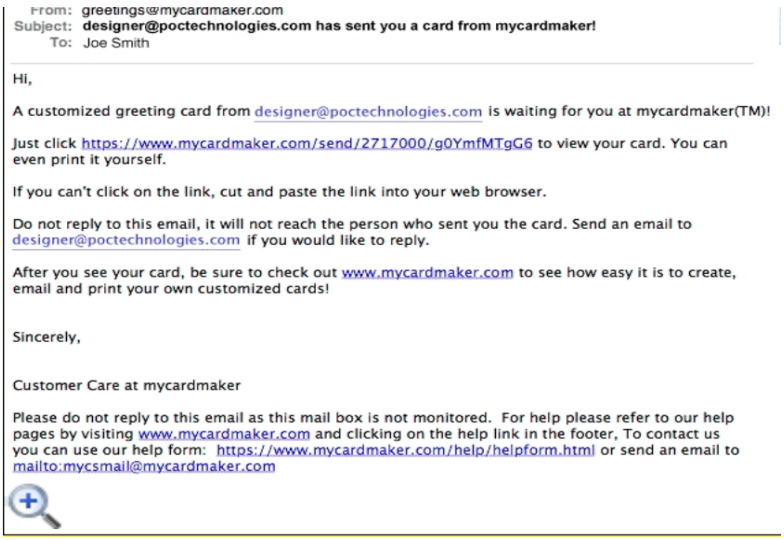
(c) BEC Phishing



(d) Zoom Phishing

Figure 28. Knowledge on Phishing Types (II)

IV. Phishing Recognition Images



From: greetings@mycardmaker.com
Subject: **designer@poctechnologies.com has sent you a card from mycardmaker!**
To: Joe Smith

Hi,

A customized greeting card from designer@poctechnologies.com is waiting for you at mycardmaker(TM)!

Just click https://www.mycardmaker.com/send/2717000/g0YmfMTgG6 to view your card. You can even print it yourself.

If you can't click on the link, cut and paste the link into your web browser.

Do not reply to this email, it will not reach the person who sent you the card. Send an email to designer@poctechnologies.com if you would like to reply.

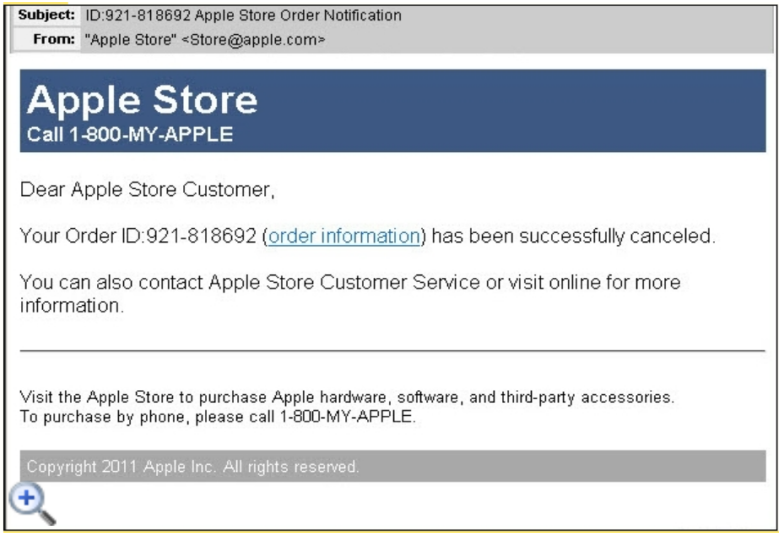
After you see your card, be sure to check out www.mycardmaker.com to see how easy it is to create, email and print your own customized cards!

Sincerely,

Customer Care at mycardmaker

Please do not reply to this email as this mail box is not monitored. For help please refer to our help pages by visiting www.mycardmaker.com and clicking on the help link in the footer, To contact us you can use our help form: https://www.mycardmaker.com/help/helpform.html or send an email to mailto:mycsmail@mycardmaker.com

(a) Image 1



Subject: ID:921-818692 Apple Store Order Notification
From: "Apple Store" <Store@apple.com>

Apple Store
Call 1-800-MY-APPLE

Dear Apple Store Customer,

Your Order ID:921-818692 (order information) has been successfully canceled.

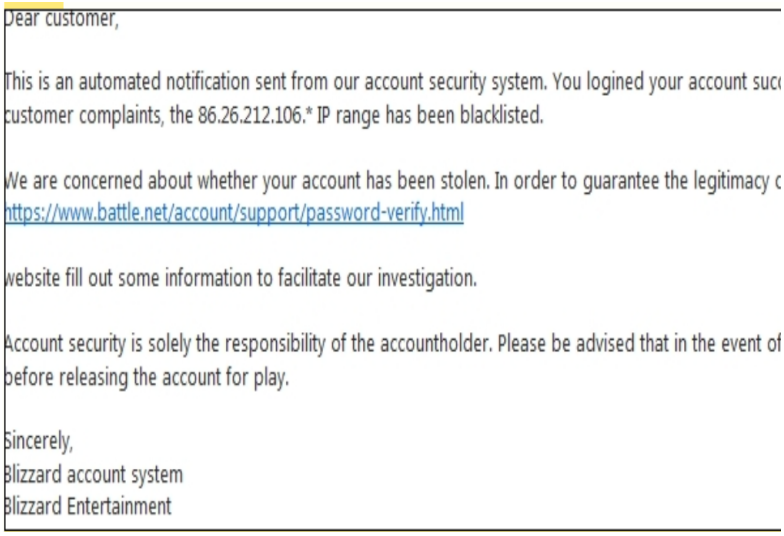
You can also contact Apple Store Customer Service or visit online for more information.

Visit the Apple Store to purchase Apple hardware, software, and third-party accessories.
To purchase by phone, please call 1-800-MY-APPLE.

Copyright 2011 Apple Inc. All rights reserved.

(b) Image 2

Figure 29. Questionnaire Images (I)



Dear customer,

This is an automated notification sent from our account security system. You logined your account suc
customer complaints, the 86.26.212.106.* IP range has been blacklisted.

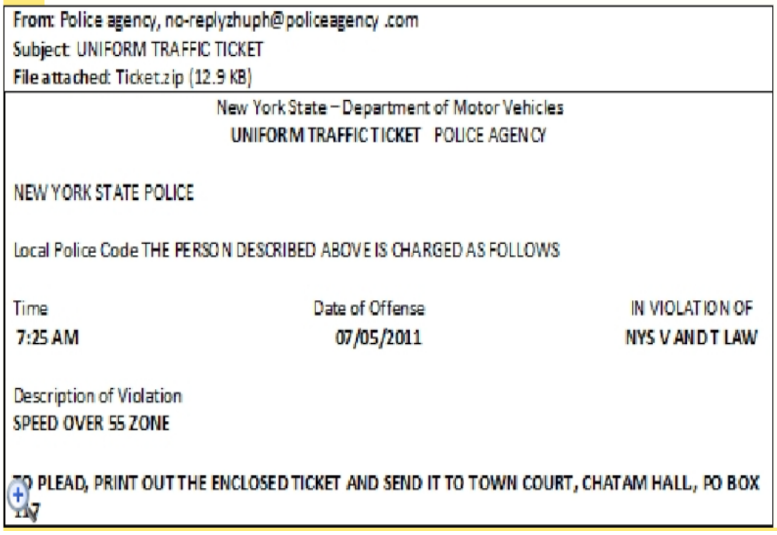
We are concerned about whether your account has been stolen. In order to guarantee the legitimacy c
https://www.battle.net/account/support/password-verify.html

website fill out some information to facilitate our investigation.

Account security is solely the responsibility of the accountholder. Please be advised that in the event of
before releasing the account for play.

Sincerely,
Blizzard account system
Blizzard Entertainment

(a) Image 3



From: Police agency, no-replyzhuph@policeagency .com
Subject: UNIFORM TRAFFIC TICKET
File attached: Ticket.zip (12.9 KB)

New York State – Department of Motor Vehicles
UNIFORM TRAFFIC TICKET POLICE AGENCY

NEW YORK STATE POLICE

Local Police Code THE PERSON DESCRIBED ABOVE IS CHARGED AS FOLLOWS

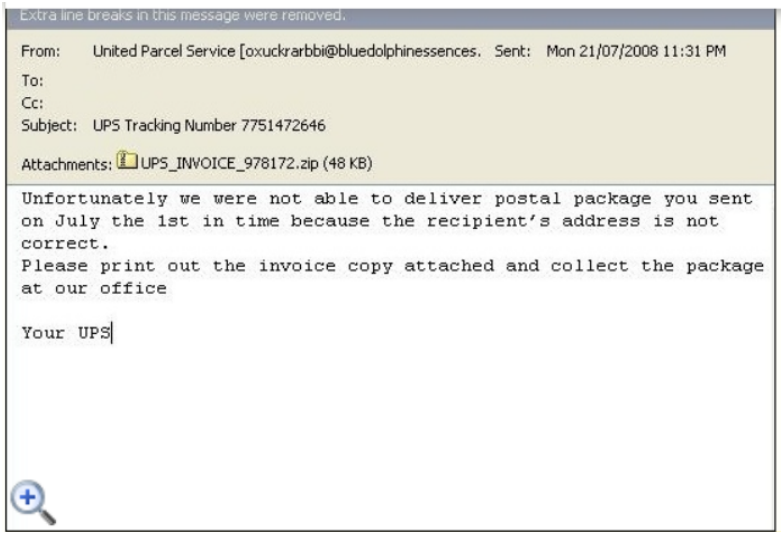
Time	Date of Offense	IN VIOLATION OF
7:25 AM	07/05/2011	NYS V AND T LAW

Description of Violation
SPEED OVER 55 ZONE

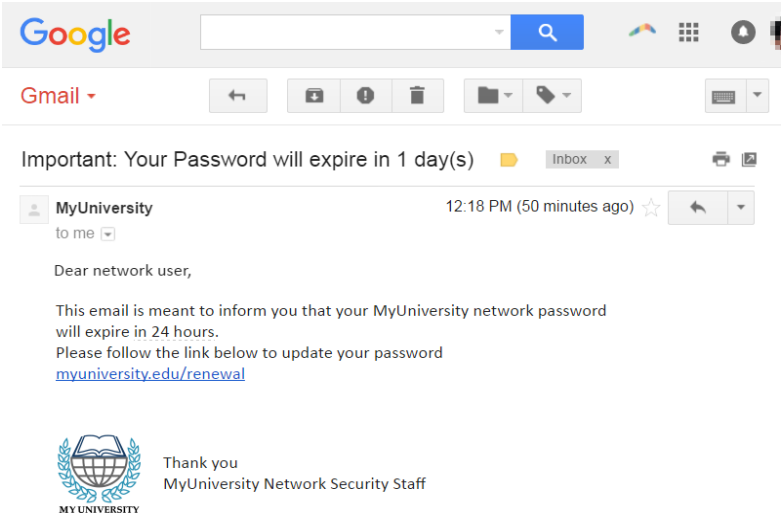
TO PLEAD, PRINT OUT THE ENCLOSED TICKET AND SEND IT TO TOWN COURT, CHATAM HALL., PO BOX 117

(b) Image 4

Figure 30. Questionnaire Images (II)

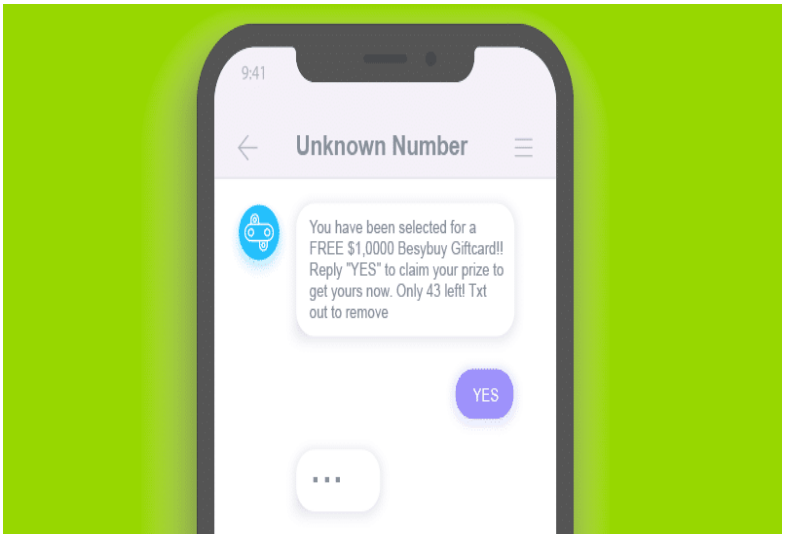


(a) Image 5

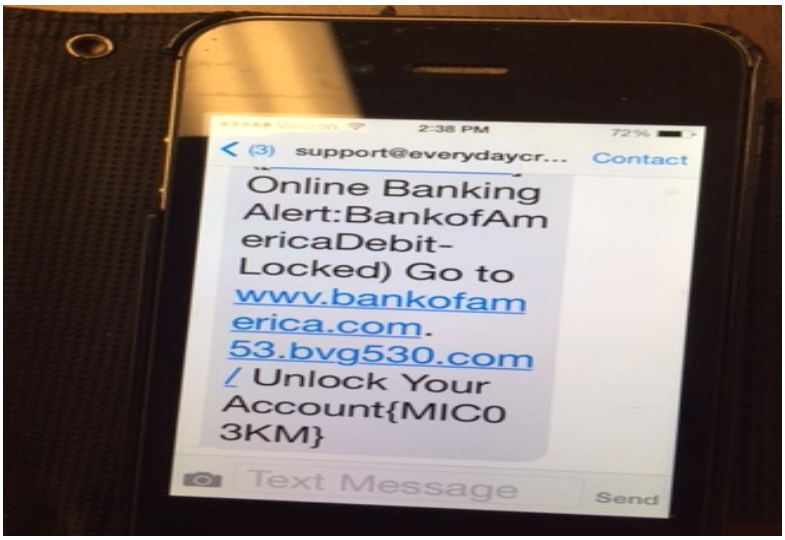


(b) Image 6

Figure 31. Questionnaire Images (III)



(a) Image 7



(b) Image 8

Figure 32. Questionnaire Images (IV)

V. Second Simulation

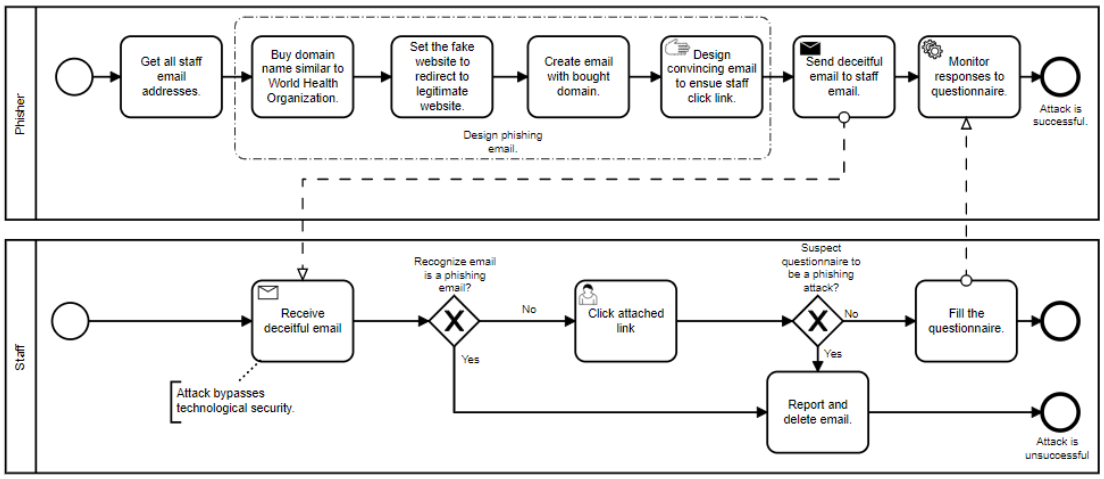


Figure 33. Second Simulation Attack Plan

Phase 1: Get staff email.

In this phase, information is gathered and email addresses of employees will be collected. This will be provided securely by an internal staff assigned to ensure the email is delivered to all staff.

Phase 2: Design Phishing email

This phase described the design of the attack which is the first step to deceiving the staff. The phase is broken into 4 steps.

Figure 34. The Phishing Email

1. Buy domain:The domain name **vvh0.com** will be bought to impersonate world health organisation.
2. Setup website: A website will be created with the domain name and set to redirect to the legitimate world health organisation website.
3. Create email address: The email address will **companies@vvh0.com** will be created and used to send the email.
4. : Design convincing email: The email is designed with two available dates to take the Covid vaccine. This email will contain a link which leads to a questionnaire asking personal details required to be submitted alongside the preferred date for the vaccine to be taken.

Phase 3: Send Deceitful email.

The email is sent out to staff with the attached link. The email content gives a deadline for which the form should be filled.

Phase 4: Receive email.

The email is then received by the staff in their inbox based on the email client being used for emails.

Phase 5: Make a decision

In this phase, the staff knowledge on phishing recognition will be tested. If the email is recognised as a phish. the staff will know to report this. However, if the email is not recognised as a phish, the staff will click the link.

Phase 6:Make a second decision.

If the staff clicks the link, a second decision will need to be made. Based on the content of the questionnaire, will the staff be able to finally recognise that the attack is phishing?

Phase 7: Monitor responses.

The responses will be monitored for within the two dates provided in the email.

Table 10. Second Phishing Attack Simulation Reporting

Day	**Number of reports on phishing email.**	**Number of calls to confirm if email is legitimate.**	**Number of calls to complain that attached link was not working.**
1	9	-	-
2	-	-	-
Total	**9**	**-**	**-**

C. Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Temilola Esther Olorunshe**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   Recognition of Phishing Attacks and its Impact: A Case Study,

   supervised by Raimundas Matulevicius.
   (supervisor's name)

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Temilola Esther Olorunshe
28/07/2021