TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Onyeka Kelvin Onyema 214201IVCM

Designing an e-Learning Application for Phishing Attack Recognition Based on Cialdini's Persuasion Principles

Master's thesis

Supervisor: Kaido Kikkas
PhD,
Associate professor

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Onyeka Kelvin Onyema 214201IVCM

E-õpperakenduse kavandamine õngitsusrünnete tuvastamiseks Cialdini veenmisprintsiipide abil

Magistritöö

Juhendaja: Kaido Kikkas

Tehnikateaduste doktor
Kaasprofessor

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Onyeka Kelvin Onyema

17.04.2023

Abstract

Phishing attacks are a prevalent form of cybercrime that seeks to deceive people into divulging sensitive information. To address this issue, this study aimed to develop an e-Learning course based on principles of persuasion to help learners identify and avoid phishing attacks. The course was designed using the ADDIE methodology and incorporated Cialdini's seven principles of persuasion: authority, scarcity, consistency, liking, consensus, reciprocity and unity. The study found that the e-Learning course is an effective method of teaching phishing recognition, and the application of persuasion principles increased learners' ability to recognize and avoid phishing attacks. Furthermore, the course addressed gaps in knowledge that users have regarding phishing attacks, such as the importance of checking links and awareness of persuasion tactics. This study generally contributes to the development of effective anti-phishing education and provides insights into the application of persuasion principles with ADDIE approach in e-Learning design.

Keywords: phishing, social engineering, persuasion principles, ADDIE.

Annotatsioon

E-õpperakenduse kavandamine õngitsusrünnete tuvastamiseks Cialdini veenmisprintsiipide abil

Andmepüügirünnak on levinuim küberkuritegevuse viis, mille kaudu peibutatakse inimesi avaldama tundlikku informatsiooni. Teema käsitlemiseks on sell uurimuse eesmärgiks arendada veenmisprintsiipidel põhinev e-õppe kursus, mis aitab õppijatel tuvastada ja vältida andmepüügirünnakuid. Kursus disainiti ADDIE mudeli põhjal ning sisaldab Cialdini seitset veenmisprintsiipi: autoriteetsus, nappus, järjekindlus, meeldivus, üksmeel, vastastikkus ja ühtsus. Uurimus leidis, et e-õppe kursus on tõhus viis andmepüügi äratundmise õpetamiseks ning et veenmisprintsiipide rakendamine suurendas õppijate võimet ära tunda ja vältida andmepüügirünnakuid. Lisaks käsitles kursus kasutajate lünklikke teadmisi andmepüügirünnakute kohta nagu linkide kontrollimise tähtsus ja veenmistaktikate teadlikkus. See uurimus annab panuse tõhusa andmepüügivastase hariduse edendamisse ja ülevaate veenmisprintsiipide rakendamisest e-õppe disainimisel ADDIE mudeli põhjal.

Märksõnad: andmepüük, sotsiaalne manipuleerimine, veenmisprintsiibid, ADDIE

List of abbreviations and terms

ADDIE	Analysis, Design, Development, Implementation, Evaluation
MVP	Minimum Viable Product
NLP	Natural Language Processing
PHP	PHP Hypertext Preprocessor
TPR	Ratio of the number of phishing emails correctly detected in the sample to the total number of phishing emails

Table of contents

List of figures

1 Introduction

Phishing attacks have been consistently increasing and serious threat to individuals and organizations in recent years. These attacks are designed to trick users into providing sensitive information, such as usernames, passwords, and financial data by mimicking legitimate and trusted sources [1]. Despite the growing awareness of phishing attacks, they continue to be successful due to their sophisticated and convincing nature.

1.1 Motivation

Despite the advancements in cybersecurity, every system has its vulnerabilities that can be exploited. In most cases, it is the human factor of the system that is the weakest link and easiest to compromise. Attackers often resort to manipulating and deceiving people by instilling panic, using persuasive tactics, or exploiting trust to put their victims at ease [2].

The need for effective anti-phishing education is more important than ever. Existing approaches to anti-phishing education, such as classroom-based training and online tutorials, have limitations in terms of accessibility, effectiveness, and scalability. Developing an e-Learning course on anti-phishing that is based on the principles of persuasion can be an innovative and effective way to improve users' ability to detect and avoid phishing attacks. Such a course can be designed to be engaging, interactive, and adaptable, and can reach a wide audience, including individuals with varying levels of experience and knowledge.

1.2 Scope

The scope of the research is withing developing and implement an e-learning course that is specifically designed to help learners identify and avoid phishing attacks using the knowledge from principles of persuasion. This will require a comprehensive understanding of the various types of phishing attacks, their characteristics, and the strategies that attackers use to exploit vulnerabilities in human cognition and behaviour. By gaining a deep understanding of the tactics and techniques used in phishing attacks, the e-learning course can be designed to provide learners with practical skills and strategies for recognizing and avoiding these attacks.

The course will be developed using instructional design principles and e-learning technologies, and will incorporate a variety of interactive learning activities, multimedia, and assessment methods to enhance engagement and promote effective learning. The implementation of the course will involve the delivery of the course to a sample of participants, with the aim of evaluating the effectiveness of the course in achieving its learning outcomes.

It is not within the scope of this thesis to develop a sophisticated admin backend or to add advanced security features to the e-learning platform. The e-learning will focus on the instructional design of the e-learning platform for teaching anti-phishing attacks using persuasion principles through the ADDIE model. Other technical aspects such as hosting, server maintenance, and database management will also not be within the scope of this thesis.

1.3 Research Questions

This research aims to design an e-learning course based on the principles of persuasion by Dr. Robert Cialdini for phishing recognition. The course will be designed to help users recognize the most common types of phishing attacks, identify the psychological tactics used by attackers, and develop effective strategies for avoiding phishing attempts. Hence, this research aims to address the following research questions:

i. How can we effectively teach phishing recognition, and what methods, rationale, and approaches should be considered?

ii. What are the key principles of persuasion that can be applied to anti-phishing education, and how effective are they in improving users' ability to recognize phishing attacks?

iii. What are the gaps in knowledge that users have regarding phishing attacks, and how can an e-learning course based on persuasive principles be designed to address these issues?

1.4 Research Contribution

Despite the availability of numerous anti-phishing tools and technologies, phishing attacks continue to succeed by exploiting human vulnerabilities such as curiosity, fear, and urgency. Therefore, there is a growing need for effective training programs that can help individuals recognize and resist phishing attempts.

The purpose of this study is to develop an e-course based on the principles of persuasion for phishing recognition and evaluate its effectiveness in improving users' ability to recognize and avoid phishing attacks. The proposed e-course is designed to leverage persuasive communication strategies to enhance users' awareness of phishing tactics, foster critical thinking and decision-making skills, and promote behavioural change.

The potential contribution of this e-course is threefold. First, it offers a novel approach to phishing education by incorporating persuasive principles that have been shown to be effective in influencing behaviour using e-Learning. By combining the insights from the fields of psychology, communication, and cybersecurity, the proposed e-course provides a comprehensive and interdisciplinary framework for understanding and combating phishing attacks.

Second, the e-course has the potential to be scalable and cost-effective, enabling a broad range of users to access and benefit from the training. The use of technology-based delivery platforms, such as learning management systems, makes it possible to reach a large and diverse audience while also facilitating continuous and personalized learning experiences.

Finally, the evaluation of the e-course's effectiveness can contribute to the development of evidence-based best practices for phishing education. By measuring users' pre- and post-training knowledge, attitudes, and behaviours, this study can provide valuable insights into the effectiveness of the e-course in improving users' ability to recognize and avoid phishing attacks.

In conclusion, the proposed e-course based on the principles of persuasion for phishing recognition has the potential to contribute to the development of effective and scalable phishing education programs. By leveraging persuasive strategies and technology-based delivery platforms, the e-course can offer a novel and interdisciplinary approach to

combating phishing attacks, while also providing valuable insights into the best practices for cybersecurity education.

1.5 Limitation and Challenges

A potential limitation of this thesis could be time constraints. Developing an e-Learning application requires a significant amount of time and resources, and the quality of the application may be impacted by limited time. Also, user engagement with the application and the effectiveness of the persuasive principles used may be difficult to measure and evaluate in a short amount of time.

Another potential limitation would be technical constraints. The e-learning application intended to be designed for phishing attack recognition may not be compatible with certain devices or have limited functionality on smaller screens.

1.6 Research Approach and Methodology

This section will kick-off our first question ***How can we effectively teach phishing recognition, what methods, rationale, and approaches should be considered?***

As mentioned earlier, the aim of this research is developing an e-Learning course to teach phishing recognition. This section further explains how and why we've chosen the approach we intended.

According to C. Hadnagy, the act of influencing and practicing persuasion involves a set of methods that aim to motivate another person to adopt a particular behaviour, attitude, thought or belief in a manner that aligns with the persuader's intention. Unfortunately, social engineers and malicious scammers use the art of persuasion everyday [2]. By teaching learners how to recognize the tactics used by attackers to influence and persuade their targets, they can develop the skills to detect and avoid phishing attacks in various scenarios. Principles of persuasion will be discussed further in chapter 2.

There are several reasons why teaching phishing recognition through e-Learning with ADDIE methodology can be beneficial. e-Learning allows for flexibility in terms of time and location, as learners can access the course material at their convenience. Additionally, the ADDIE methodology provides a structured approach to the design and development

of the e-Learning course, ensuring that all aspects are thoroughly planned and executed. This can lead to a more effective and efficient learning experience for the learners.

ADDIE is a common methodology used in instructional design to guide the development of effective learning materials [3, 4]. ADDIE stands for Analysis, Design, Development, Implementation, and Evaluation as seen in Figure 1.

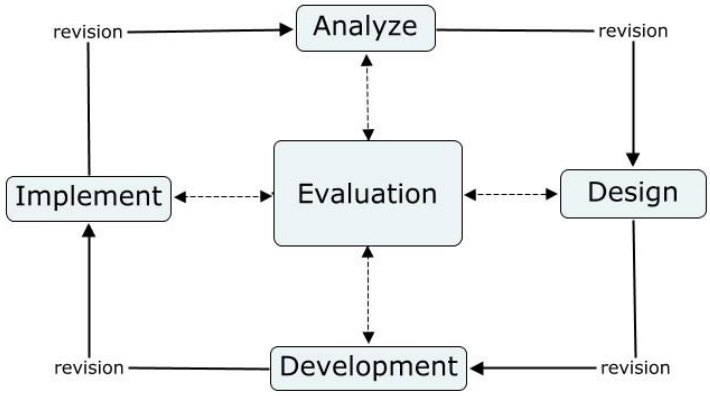


Figure 1: The ADDIE model consists of five distinct components [3].

Here is a brief overview of each phase:

Analysis: This phase involves gathering information about the learners and the context in which the learning will take place. This includes identifying the goals of the instruction, the learners' needs and characteristics, and the learning environment.

Design: In this phase, instructional designers create a blueprint for the instruction, including learning objectives, assessment strategies, and instructional methods. This phase also involves selecting appropriate instructional materials and resources.

Development: In this phase, the actual learning materials are created, including lesson plans, handouts, presentations, and multimedia resources. This phase involves developing the content and creating a prototype of the learning materials.

Implementation: This phase involves the actual delivery of the instruction. The learning materials are tested and refined, and the instruction is delivered to the learners.

Evaluation: In this phase, the effectiveness of the instruction is evaluated. This includes evaluating the learning outcomes and the instructional methods. The results of the evaluation are used to make improvements to the instruction for future use.

1.7 Thesis Structure

The following sections of the paper are structured as: Chapter 2 provides an overview of the history and evolution of phishing attacks, explains the principles of persuasion in the context of phishing attacks, and explores different e-learning methods that have been used to educate users on anti-phishing techniques. Chapter 3 focuses on the research approach employed in this study, which involved gathering, describing, and analysing the information to help design the e-Learning application. Chapter 4 of the thesis will concentrate on the comprehensive evaluation of the e-Learning application and the learners who have interacted with it. This phase of the research will aim to assess the effectiveness and efficiency of the e-Learning platform in meeting the learning objectives that were established in the earlier phases. On the other hand, Chapter 5 will present the conclusive remarks and recommendations drawn from the findings of the research, highlighting the strengths and offering suggestions for future research in this field.

2 Theoretical Background

This section will provide an analysis of the key concepts and factors related to phishing attacks, including their history, types, techniques, indicators, and the principle of persuasion in the context of phishing. It will also examine the various e-Learning methods that are employed in trainings. The section will review the existing literature in these areas and identify the research gaps. Moreover, it will answer the research question of ***What are the key principles of persuasion that can be applied to anti-phishing education, and how effective are they in improving users' ability to recognize phishing attacks?***

2.1 Definition and History of Phishing

The internet, since its invention, has brought significant changes to human existence and transforming several industries, such as e-Healthcare and e-commerce, amongst other sectors. Although the internet makes life more comfortable, it also makes security precautions more necessary, a fact that brings in the aspect of digital phishing attacks, among other related facets that imperil cybersecurity. "Phishing" first appeared in the 1990s [5]. Considering that they typically hacked using their phones, the earliest and first attackers frequently substituted the letter "f" with the letters "ph" to create new terminologies within the hacking fraternity, according to [5]. Phishing attacks typically involve the use of fraudulent emails, websites, or other forms of digital communication that are designed to look legitimate in order to deceive the victim [6]. Nishad, in [5] adds that phishing is regarded as a kind of cybercrime or fraud, and those that engage in it are referred to as cybercriminals. He explains that a group of individuals (victims) receive phishing emails urging them to update their information accounts and passwords, among other similar or related kinds of mischief. He also states that phishers employ traditional social engineering methods, such as making phone calls to their victims.

2.1.1 Phishing in the 1990s

Arshad et al. revealed that on 2nd January 1996, the phrase "phishing" first came into its initial use [7]. They continue by saying that throughout the 1990s, hacking communities and cybercriminals would pose as AOL officials and admins. At the same time, they were phishing for login information to gain free internet usage and connectivity. They clarify that to obtain an AOL identity or account, an organization known as the Warez

community primarily made up of fraudsters and pirates would collect users' login information and randomly produce credit card and account numbers. Despite being quite simple, this fraud was successful as nobody knew the dangers of phishing. As per Chate et al., a popular fraudster and spammer are credited with coining the word "phishing" in the middle of the 1990s [8]. They clarify that the phishing hacking program AOHell, which had the capability for trying to illegally obtain the financial data or passwords of America Online members, is where the name is initially reported. Phishing, nevertheless, would merely stay among the most common issues businesses today deal with.

Another notable case of phishing in the 1990s was the "Nigerian Prince" scam, also known as the "419" scam. This scam involved an email from someone claiming to be a wealthy Nigerian prince who needed help transferring large sums of money out of the country. The scammer requested the recipient's banking information to facilitate the transfer, but in reality, the scammer was attempting to steal the recipient's money [9].

2.1.2 Phishing in the 2000s to 2010s

In Tariq's opinion, the phishing industry developed quickly from the 2000s through the 2010s. Individuals who lived through the beginning of the 2000s were still largely ignorant of phishing [10]. He continues by saying that it is not generally known that con artists pose as officials in order to win big. Throughout this time, phishers began to focus on digital payment channels like E-gold and PayPal. For instance, when there were many PayPal consumers, criminals sent emails instructing people to modify their credit card information while stealing it [10]. According to him, the end of 2008 saw the emergence of cryptocurrencies, which fraudsters implement to work together and blackmail their targets, besides securely withdrawing the proceeds of their latest crimes. Since 2013, Cryptolocker ransomware and subsequent worms like Petra and WannaCry ransomware, which is primarily spread via phishing of emails, remains prevalent [10]. A ransomware outbreak also results in a large loss. Even without accounting for the extortion, the majority incurred big financial losses.

The implementation of phishing scams by social engineers changed toward the beginning of the 2010s, resulting in a greater percentage of cybercriminals adopting them for purposes other than traditional money-related ones. He mentions, for instance, how John Podesta, the director of Hillary Clinton's presidential campaign race, was the target of a phishing attempt that may have been politically initiated in 2016 [10].

2.1.3 Phishing today

Phishing attacks continue to be a prevalent threat in recent days, with cybercriminals constantly evolving their tactics to deceive victims. According to Burda et al., cybersecurity experts and cybercriminals are engaged in endless competition as they aim to outdo each other by utilizing cutting-edge tools, situations, and offensive strategies [11]. Cybercriminals discovered a new informational gold mine through the rise of social media sites such as Facebook and LinkedIn, where they may conduct studies and craft increasingly convincing and specific phishing emails, among other forms of online communication [11]. Unrestrained access to private data enables attackers to create customized trident phishing online messages that depend on acquaintance and render it more difficult for consumers to recognize a phishing effort, according to their statement. Since the epidemic drove many businesses to operate remotely, anti-phishing movements have become more effective [11]. Cybercriminals made use of the fact that small firms do not have as much protection as bigger enterprises to target more of them to increase their reward while corporates and workers adjusted to the fresh virtual office security requirements [11]. According to INTERPOL, there have been 589% higher phishing assaults in March 2020 than in February 2020. It represents approximately a 600% spike beyond one month, as Burda et al. stated, which only highlights the degree to which cybercriminals are profiting from the terror brought about by the epidemic. Also, they note that whereas electronic messages have dominated phishing for the last ten years, the year 2020 saw an increase in frauds involving phone conversations (vishing) alongside text messages (SMSs) (smishing) [11].

2.2 Types of Phishing Attacks and Techniques

Phishing attacks can be categorized in many ways considering the facets or circumstances under which cybercriminals perpetrate them. According to Rastenis et al., for instance, the taxonomy of phishing attacks may be based on electronic mail (Emails), which encompasses all the stalemates of every phishing category known to have been in existence [12]. It is presumed that the implied taxonomy assumes a vaster range of classifications. This aspect relies on various classes, which are twice as much in numbers when contrasted with the taxonomy of the already occurring classes [12]. Phishing attacks can take on several different forms, and attackers use various techniques to trick users

into divulging sensitive information. Here are some common types of phishing attacks and their techniques.

2.2.1 Email Phishing

Research by Priyanka et al defines email phishing as a type of phishing attack where an attacker sends a fraudulent email, appearing to be from a legitimate source, to trick the recipient into sharing sensitive information, such as login credentials or financial information. This technique is widely used by cybercriminals due to its ease of implementation and high success rate [13]. Their research aimed at providing an extensive overview of how natural language processing (NLP) concepts can be utilized for the classification of phishing emails. The paper presented the application of NLP concepts to classify emails and calculates the accuracy rate of various classifiers.

Gaoqing et al elaborated that phishing emails typically display their content in HTML format and contains a lot of resources, including hyperlinks, images, CSS, and JavaScript code. These features are used to create false identities, gain users' trust, and persuade victims to click malicious links, enter their username and password, or download and run malicious attachments [14].

According to the 2019 Internet Crime Report by the FBI's Internet Crime Complaint Center (IC3), part of the information that was made public was that they recorded 467,361 complaint and $3.5 billion losses to both individuals and business victims and part of the financial loss was due to email spoofing [15]. Email spoofing is when a message is sent with a falsified sender address and other parts of the email header to make it look like it came from a trustworthy source. This method is often used by attackers to deceive recipients and gain their confidence in order to carry out harmful actions. Email spoofing is commonly employed in phishing and spam campaigns [16].

Email phishing attacks can take on several different techniques, including spear phishing, whaling and clone phishing.

2.2.2 Spear Phishing

Spear phishing is a type of phishing attack that is directed towards a specific organization or individual and is highly customized for the targeted recipient(s) [17]. Unlike traditional phishing attacks, which often involve mass-sent, generic emails, spear phishing attacks

are carefully crafted to appear legitimate and are often based on detailed research about the targeted individuals or organizations. This type of attack often relies on social engineering techniques, such as posing as a trustworthy individual or organization, to trick the recipient into divulging confidential information or clicking on a malicious link or attachment.

Whaling

The use of spear-phishing attacks against high-level targets, such as corporate executives or government officials, is also known as “whaling”. Whaling is a highly targeted and risky form of spear phishing that is directed at high-level executives within organizations [18]. These executives often have access to highly confidential and sensitive information about their company, making them a valuable target for attackers seeking to steal this information for financial gain or other nefarious purposes. Due to the level of access that these individuals have, successful whaling attacks can have a significant impact on a company's reputation, financial stability, and overall security posture.

Clone phishing

This type of phishing attack involves the creation of a replica of an existing email, which is then used by the attacker to include malicious content or links with the intention of stealing personal information or committing fraud. The email containing the malicious content is subsequently sent to the victim, who may be deceived into believing that it was sent from the original sender [13].

2.2.3 Vishing

Vishing is a type of cyberattack that uses voice communication, usually over the phone, to trick people into divulging sensitive information such as credit card numbers, passwords, or personal identification numbers (PINs). The term "vishing" is a combination of "voice" and "phishing," which refers to a similar type of cyberattack that is carried out via email or instant messaging [19]. Vishing attacks can be carried out using a variety of techniques, such as using automated voice messages or impersonating a trusted person or organization.

Vishing attacks often use principles of persuasion to manipulate victims into divulging sensitive information. The research by Keith et al, examined samples of real-world

vishing attacks to identify the various persuasion principles present on them. The persuasion principles most commonly utilized in the vishing attacks samples were authority, social proof, and distraction, liking, similarity, and deception. Commitment, reciprocation, and consistency were not frequently observed in vishing attacks. They concluded that the principle of persuasion discovered in the samples were the main persuasion principles used in vishing attacks [20].

In a vishing attack, the attacker might impersonate a legitimate organization, such as a bank or a government agency, and ask the victim to provide sensitive information or to make a payment. The attacker might also use scare tactics, such as claiming that the victim's account has been compromised or that they owe money to the government.

Vishing attacks can be difficult to detect, as the attackers may use sophisticated techniques to make their calls appear legitimate.

2.2.4 Smishing

Smishing is a type of cyberattack that uses text messages (SMS) or messaging apps to trick people into giving out sensitive information or downloading malware onto their device. The term "smishing" is a combination of "SMS" and "phishing" [20].

According to [21], Text messaging, also known as Short Message Service (SMS), is widely used by mobile phone users. This communication method is particularly popular due to its affordability, making it a preferred option for reaching large numbers of people. As a result, it is extensively employed to promote purchase points of interest and serve as an advertising medium.

Attackers favour using SMS over email for phishing due to the high response rates of text messages, the cost-effectiveness of bulk messaging through affordable SMS packages, and users' difficulty in differentiating between genuine and phishing URLs within SMS links [21].

2.2.5 Domain Spoofing

Domain spoofing is a technique used by cybercriminals to falsify the email sender's domain name or website domain to appear legitimate. This technique is often used in phishing attacks to deceive the recipient into believing that the message or website is from a trusted source when it is actually from a malicious entity [15]. The attacker can change

the "From" email address to a domain that is similar to a legitimate organization's domain, making it look like the email came from that organization. For example, they can use a domain name that is one or two letters off from the real domain, such as "g00gle.com" instead of "google.com" [16].

The lack of appropriate email anti-spoofing schemes or their misconfiguration may lead to successful phishing attacks or spam dissemination. The research in [15] assesses the global implementation rate of SPF and DMARC in two extensive campaigns, examining 236 million domains and high-profile domains from 139 countries. The authors introduce a novel algorithm that utilizes SPF check_function emulation to detect defensively registered domains and enumerate domains with SPF rules that are misconfigured. Based on our measurements, it appears that a significant proportion of domains have inadequate SPF and DMARC configurations. This vulnerability allows cybercriminals to effectively send fraudulent emails to recipients' inboxes.

2.3 Indicators of Phishing Attacks

Phishing attacks are becoming increasingly sophisticated, and it can be challenging for users to distinguish between legitimate emails and phishing attempts. One way to identify potential phishing attacks is to look for specific indicators or red flags that suggest that an email or message may not be legitimate. Here, we will review the various indicators of phishing attacks as identified by researchers in the field.

2.3.1 Suspicious URL Links or Attachments

Malicious actors often use URL manipulations to deceive users into clicking on a harmful link. A popular technique is called "mangle," where the attacker replaces letters in a company or brand name with similar-looking characters or uses misspelled versions of the name to make the URL appear legitimate. This manipulation can be challenging to spot, making it a common tactic in phishing attacks [22].

2.3.2 Email Specific Indicators

Phishing attacks can vary in sophistication and consequently, the email-specific indicators can differ as well. In less sophisticated attacks, common indicators that people are familiar with include poor spelling and grammar. However, more advanced spear

phishing attacks utilize tactics like email spoofing, where the message appears to originate from a legitimate source, making it difficult to detect the attack [23].

2.3.3 Domain Indicator

Domain indicator refers to the part of an email address that follows the "@" symbol and identifies the domain name associated with the email address.

By examining the domain name within a URL, metadata can be accessed to identify potential indicators of phishing. One such indicator is the age of the domain, which can be obtained through WHOIS, a database for domain registration information. The domain's creation date can be compared to established thresholds for phishing sites to determine if the site is suspicious [23].

2.3.4 Suspicious Sender Email Address

Phishers may use variations of legitimate email addresses or domain names to make the email appear more convincing. For example, they may use an email address that looks like it is from a reputable company by using a slightly altered version of the company's name or domain name, such as @goggle.com instead of @google.com. A suspicious sender email address is an email address that appears to be fake, illegitimate or suspicious, and is often used in phishing attacks. These email addresses are designed to trick recipients into believing that the email is from a legitimate source, such as a reputable company or organization, when in fact it is not.

2.4 Principles of Persuasion in the Context of Phishing Attacks

According to Dr. Robert Cialdini, a renowned expert in the field of social psychology and author of the best-selling book "Influence: The Psychology of Persuasion," there are seven fundamental principles of persuasion (figure 2) that can be used to influence others. And these principles are namely reciprocity, consistency, consensus, liking, authority, scarcity and Unity [24, 25]. These principles are based on the fundamental principles of human behaviour and can be effectively applied in various contexts to influence others. Phishing attacks continue to happen because cybercriminals understand how people think and hence, use this knowledge to achieve their goals. The principles of persuasion play a crucial role in the success of the attacker's attempt to deceive the target.

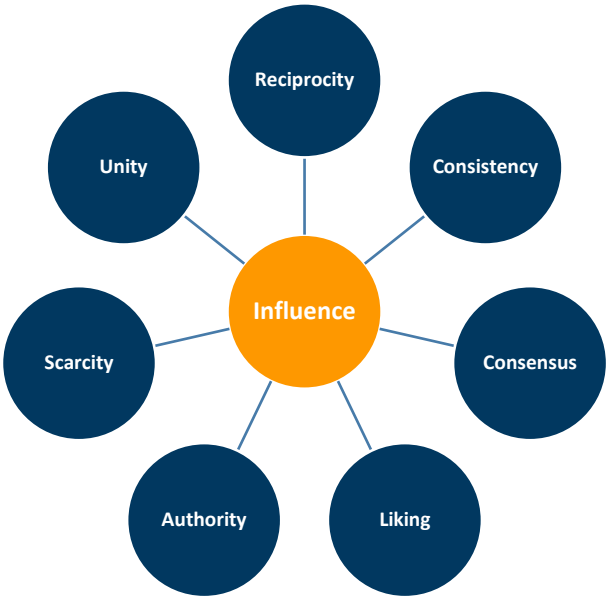


Figure 2: Principles of persuasion, adapted by the author from Cialdini (2016) [25] by Dr. Robert Cialdini

2.4.1 Principle of Reciprocity

From Dr. Cialdini's lessons, reciprocity is a principle of persuasion that suggests that people are more likely to comply with a request or favour if they feel that they owe something in return [26]. The concept of reciprocity has been studied extensively in social psychology, and it has been found that people tend to feel a sense of obligation to repay favours or kindness that have been shown to them. In the context of phishing attacks, attackers may use reciprocity to trick victims into revealing sensitive information or performing an action by offering something in return, such as a free gift or service.

The Principle of Reciprocity can be observed in various phishing campaigns and scams where the attacker offers something for free to the victim, such as a coupon or a gift, and then requests the victim to perform a certain action, like signing up for an account or providing personal information [27].

2.4.2 Principles of Scarcity

Scarcity in principle of persuasion that suggests people are more likely to want something if they believe it is rare, limited in availability, or will soon become unavailable [26]. Phishing attackers exploit people's attraction to items that appear rare by imposing deadlines on deals in emails. Alternatively, in a frequent strategy, they inform individuals

that their account will be disabled within 24 hours if they do not click on a link to resolve it [27]. This can pressure the recipient into clicking on a link or giving away their personal information without taking the time to carefully evaluate the legitimacy of the email or its contents.

2.4.3 Principle of Authority

People who are regarded as authoritative and knowledgeable in a particular area are often viewed as more influential, perhaps because credibility and authority are important components of trust. The more we trust someone, the more likely we are to comply with their suggestions. As a result, when we want to make good decisions, we tend to rely on advice given by experts in the field [28].

The utilization of authority figures to deceive users is a widespread and potent tactic. In some spear phishing campaigns, malicious actors impersonate the Chief Executive Officer (CEO) and compel the Chief Financial Officer (CFO) to wire money promptly. This technique, when combined with urgency, can create fear in individuals, who may be hesitant to refuse their superior's request [27].

2.4.4 Principle of Consistency

People are more likely to comply with requests if they believe they have already made a commitment to the behaviour or action. This commitment can be verbal, written, or even just a mental commitment. Once someone has made a commitment, they are more likely to stick with it to remain consistent with their previous behaviour or decision [28].

Fraudsters exploit people's tendency to remain consistent by requesting something minor in an initial email and then gradually escalating their demands in subsequent messages [27].

One example of the principle of consistency in the context of a phishing attack could be when an attacker sends an initial email asking the victim to fill out a survey. The victim completes the survey, providing personal information such as their name and email address. Later, the attacker sends a follow-up email posing as a trustworthy organization and asks the victim to enter their credit card information to complete a purchase, citing their previous completion of the survey as evidence of their interest. The victim may be

more likely to comply with this request due to the principle of consistency, as they have already taken a small step towards providing personal information.

2.4.5 Principle of Liking

The principle of liking in persuasion suggests that people are more likely to comply with requests from individuals they like or who share common interests with them [28].

A typical example of the principle of liking in the context of phishing attack is when attackers create fake social media profiles that appear to be from someone the victim knows and trusts, such as a friend or colleague. They then use these profiles to send messages or emails to the victim, attempting to trick them into clicking on a link or providing sensitive information. The victim is more likely to comply with the request because they believe it is coming from someone they know and like.

2.4.6 Principle of Consensus

The principle of consensus also known as social proof suggests people are more likely to take a specific action if they believe many others are already doing it. Essentially, when people are unsure of what to do, they tend to look to others for guidance on how to behave [28].

An example of the principle of consensus in the context of a phishing attack is when attackers use social engineering tactics to create a sense of urgency in the victim by suggesting that many other people have already taken advantage of a particular offer or clicked on a certain link. This implies that the victim should also act in the same way to avoid missing out on something valuable or important. The attackers may also create fake social media posts or reviews that make it seem like many other people have already interacted with the fraudulent message or link, which can increase the victim's confidence in the legitimacy of the message.

2.4.7 Principle of Unity

This is the idea that people are more likely to be persuaded by those who they perceive as being part of the same group or sharing similar characteristics or identity [25].

Phishing attackers can use the principle of unity to create a false sense of shared identity with their target. For example, an attacker may send a phishing email to an employee of

a company and pretend to be a member of the same department or team, using language and jargon that would be familiar to the employee. This can create a sense of unity and shared identity, making the employee more likely to trust the attacker and follow the instructions in the phishing email, such as clicking on a link or entering login credentials.

Alternatively, attackers may use the principle of unity by pretending to be a member of a group or organization that the target belongs to, such as a social media platform or a charity. They may then send a phishing email or message that claims to be from the group, asking the target to click on a link or provide personal information to verify their account. The false sense of shared identity can make the target more likely to comply with the request, leading to a successful phishing attack.

2.5 e-Learning Methods for Trainings

Traditional methods of cybersecurity training are often insufficient in preparing users to recognize and respond to these attacks. As such, e-learning has emerged as a promising platform for anti-phishing training due to its flexibility and cost-effectiveness. This approach involves the use of online tools and resources to educate users about the various indicators of phishing attacks, how to avoid falling victim to them, and how to respond appropriately when encountering suspicious emails. There are various e-learning methods for anti-phishing training are being reviewed.

Gamification and Simulations: article [29] referred gamification as the use of game design elements and principles in educational environments to enhance engagement, motivation, and learning outcomes. It involves incorporating game-like features such as points, badges, leader boards, challenges, and rewards into the learning process to make it more interactive, fun, and immersive. The research work by Ondrejicka reviewed and improve upon an existing anti-phishing game prototype, with the goal of creating a production-ready application [30].

One type of simulation is a software work simulator, which replicates the user interface and functionality of a program, allowing learners to practice using the software in a safe environment. Another type of simulation is process modelling, which presents complex models in an interactive form, allowing learners to explore and manipulate various scenarios [31].

Video-based e-Learning involves the use of videos as a primary means of delivering educational content. These videos can be created with a variety of techniques and may include supporting elements such as illustrations, diagrams, and text overlays to enhance understanding. In addition, videos can also include computer-generated graphics that can simulate real-world situations and scenarios, making the learning experience more immersive and engaging [31]. Video-based e-Learning could also incorporate interactive elements, allowing learners to engage with the content in a more dynamic way. For example, learners may be asked to answer questions or complete tasks based on the content presented in the video, providing a more personalized learning experience [31].

Video-based e-Learning can also be tailored to specific learning objectives and can be used to teach a wide range of subjects, from complex technical concepts to soft skills and communication strategies. It is a flexible and scalable learning method that can be used across a variety of industries and contexts.

Text-based learning - according to Zdanevych et al refers to the use of written materials as the primary means of delivering content to learners. This method can include various types of text-based resources such as online articles, eBooks, digital documents, and written assignments [31]. In this type of e-Learning, the learner is expected to read and comprehend the written material to gain knowledge and understanding. The text may be accompanied by visual aids, such as images or infographics, to enhance the learning experience [31].

One advantage of text-based e-Learning is that it allows for self-paced learning, as learners can progress at their own speed and revisit the content as needed. However, text-based e-Learning may not be suitable for all learners, particularly those who have difficulty with reading or prefer more interactive forms of learning. Therefore, it is important to consider the needs and preferences of the target audience when designing e-Learning courses using text-based resources.

2.6 Review of Related Works

This phase aims to provide a summary of previous research studies that have investigated the principles of persuasion as they relate to phishing attacks. It involves examining the

existing literature to identify the various persuasion principles that have been studied in the context of phishing attacks, the research methodologies used, and the findings.

In 2014, N. Akbar conducted a study to investigate the role of persuasion principles in phishing emails. The study examined the use of six persuasion principles (reciprocity, scarcity, social proof, authority, liking, and commitment/consistency) in over 200 phishing emails collected from a security organization. The results of the study showed that the most commonly used persuasion principle in phishing emails was Authority, followed by scarcity and likability. The least commonly used principle was social proof. The study also found that the phishing emails that contained more persuasion principles were more effective in tricking users into disclosing sensitive information. Overall, the study concluded that the use of persuasion principles plays a significant role in the effectiveness of phishing attacks [32].

In the study conducted by Ferreira et al., the researchers aimed to address the gap in previous studies by utilizing a relational method to generate a distinct list of Principles of Persuasion in social engineering, which builds on the foundational work of Cialdini, Gragg, and Stajano and Wilson. They selected phishing emails randomly from various phishing archives, conducted further analysis on them, and demonstrated the relationships among all the persuasion principles present on the phishing emails. This study was a further step in understanding the use of persuasion principles in phishing emails and suggested future applications for automated recognition of these principles [33].

In Xue et al's 2020 journal article, they investigated a detection method for phishing emails that relied on the principles of persuasion. The scientists applied persuasion principles often utilized in phishing emails to train a dataset. They conducted experiments using three machine learning classification algorithms: KNN algorithm, DecisionTree algorithm, and Bayes algorithm. Comparing the outcomes of the experiment, it was observed that the detection method based on persuasion principle significantly improved TPR and Precision in comparison to other detection methods. [34].

In a study conducted by Burda et al., a traditional phishing experiment was conducted in both an institutional and corporate setting to examine the relationship between phishing persuasion techniques and their success rate in tailored environments. Two phishing campaigns were launched targeting both the university and the Indian organization, with

a total of 1320 employees. The campaigns utilized persuasion principles such as Authority, Liking, Scarcity, and Consistency. The results indicated that the success rate in India was higher compared to that of the university, suggesting that India is more susceptible to phishing attacks. Furthermore, attacks exploiting Authority were found to be more effective on university employees. [35].

In 2021, Garcia suggested the use of a video game to evaluate the effectiveness of persuasion principles in enhancing information security awareness among university students. The game comprises visual content and presents various scenarios to the player, prompting them to make decisions. Each decision leads to another scenario, and this continues until the game is complete. The study findings align with earlier research, indicating that the assessed persuasion principles exhibited high scores for susceptibility [36].

Majority of the studies focusing on persuasion techniques and phishing attacks aim to either demonstrate the effectiveness of persuasion techniques in phishing attacks, or utilize persuasion principles to train datasets for the purpose of machine learning. These studies seek to understand the various tactics and strategies employed by attackers to influence their targets and exploit their psychological vulnerabilities. Additionally, some of the studies aim to enhance the ability of machines to detect and mitigate such attacks by developing algorithms that are trained on persuasive patterns.

Overall, the review emphasizes the need for a deeper understanding of the principles of persuasion in the context of phishing attacks and the development of effective training programs to educate individuals on how to recognize and avoid phishing scams.

3 Analysis, Design, Development, and Implementation

The focal point of this section revolves around elaborating on the techniques and procedures that we will utilize to accomplish the intended goal of this research. This section will also provide answer to the research question "***What are the gaps in knowledge that users have regarding phishing attacks, and how can an e-learning course based on persuasive principles be designed to address these issues?***"

The success of e-Learning largely depends on several factors, which include the learner's achievement, attitude, knowledge base, socioeconomic level, and learning strategy. The aspect of achievement in e-Learning refers to the level of progress that learners make in acquiring the necessary skills and knowledge. This progress is usually assessed through various forms of evaluation, including tests, assignments, and projects.

In this research work, we will apply the ADDIE as described in the first chapter. The ADDIE method is a widely used instructional design framework that consists of five phases: Analysis, Design, Development, Implementation, and Evaluation. The method provides a systematic approach for creating effective and efficient instructional materials and is used by instructional designers, trainers, and educators to ensure that learning experiences are relevant, engaging, and impactful.

To conduct this research, a bank in Nigeria was chosen due to some reasons. First, the bank's employees are expected have achieved a certain level of education, which can contribute to the quality of data collected. Additionally, the employees come from different educational fields, which provides a diverse perspective. Furthermore, banks are often targeted by phishing attacks, making them suitable research setting for studying users' knowledge gaps and designing effective e-learning courses to address these gaps.

3.1 Analysis Phase

The analysis phase of the ADDIE model is a crucial step in the instructional design process. It involves identifying the learning needs and goals of the target audience, as well as assessing the resources and constraints that affect the design and development of the e-learning course. This analysis phase will be divided into four subcategories, namely instructional goals, instructional analysis, learner analysis, and learning objectives.

3.1.1 Instructional Goals

The instructional goal is to design and develop an e-learning application that can effectively teach learners how to recognize and avoid phishing attacks leveraging on principles of persuasion. The goal is to provide learners with the necessary knowledge, attitudes, and skills to recognize and respond appropriately to phishing attacks.

To achieve this goal, the instructional strategy will include brief lectures in different phases, interactive questions in between lectures to keep the learners active, and a final quiz to evaluate the learners' understanding and retention of the material. The instructional design will also incorporate assessment instruments and technology to track and measure learners' progress throughout the course.

The ultimate goal of this instructional design is to ensure that learners are able to apply the principles of persuasion to recognize and avoid phishing attacks in a real-world setting.

3.1.2 Instructional Analysis

To successfully achieve the instructional goals, it is essential to identify and outline all the necessary steps involved. Teaching recognition of phishing attacks based on the knowledge from principles of persuasion following ADDIE model, we had to consider the following steps:

- We first had to identify the key principles of persuasion that are relevant to phishing attacks as mentioned in the literature review, and that will be covered in the e-learning course.

- The author conducts an analysis of the target learners, their needs, characteristics, and e-Learning preferences, which is discussed in the leaners analysis.

- Appropriate instructional strategies and methods that are aligned with the learners' needs and the selected principles of persuasion will be developed.

- Detailed learning objectives that are specific, measurable, achievable, relevant, and time-bound will be created.

- The author will develop the e-learning course content, materials, and assessments that are aligned with the instructional strategies, methods, and learning objectives.

- The author will implement the e-learning course and evaluate its effectiveness based on the learning objectives and feedback from the learners.

- Revise and refine the e-learning course as needed based on the evaluation results and feedback.

3.1.3 Learner Analysis

This study involved the use of a questionnaire (Appendix 1) to collect data from a sample of employees who work in a specific department of a financial institution located in Nigeria. Our objective was to assess the level of awareness among the respondents regarding phishing attacks, to investigate their preferences for e-Learning, and to explore the diversity present in their demographic characteristics.

From our observation of the data collected, it was found that more than 50% of the respondents expressed uncertainty about the persuasion principles that are commonly used in phishing attacks. Additionally, 46% of the respondents either agreed or strongly agreed that they had undergone phishing training, while the remaining respondents were either neutral or disagreed that they had received such training. Approximately 66% of the respondents acknowledged that they sometimes and rarely check the links before clicking them, whereas the remaining 34% reported that they always and often examine the links before clicking on them. The majority of the respondents, precisely 92%, agreed and strongly agreed that detecting phishing attacks can be a challenging task.

With respect to their learning style, a significant proportion of the participants indicated their comfort in using a computer as a medium for learning. Additionally, they expressed a preference for interactive learning, which involves active engagement. They also indicated their willingness to learn using graphics, audio, and animations. Furthermore, the participants showed a preference for a story-based approach to learning complex ideas.

We distributed the questionnaire to around 70 individuals, out of which 54 persons actively participated. The gender distribution showed that 52% of the participants were male and 48% were female, and the age range was between 20 to 50 years old. 7% of the

participants were between 40 to 60 years of age. The majority of the participants (94%) held a B.Sc degree, while 4% had an M.Ba and 2% held an M.Sc degree. The academic fields of the participants were diverse, ranging from arts, science, social sciences, management science, engineering, and technology.

3.2 Design Phase

In the design phase, the primary goal is to identify the learning objectives, assessment tools, and resources needed to evaluate the performance. The process includes subject matter analysis, exercise, lesson planning, and media selection, which are essential in achieving the desired learning outcomes. Additionally, this stage involves the development of assessment instruments and content to ensure that learners acquire the necessary knowledge and skills to combat anti-phishing attacks [3].

3.2.1 Learning Objective

In the course of designing the e-learning, it's important to keep the learning objectives in mind. The learners' objectives provide the direction for the course and help ensure that it meets their needs. Understanding the learners' goals is essential to creating a course that is effective and engaging. By aligning the course content and activities with the learners' objectives, the course can be designed to help learners achieve their objectives in a meaningful way.

The focus of the e-Learning course will be to educate learners about the seven persuasion principles of influence and how they are utilized in phishing attacks. Akin to Akbar's research in [32], some studies indicate that a significant proportion of phishing emails incorporate persuasive tactics.

Persuasion principles are often used by attackers to trick and deceive individuals into divulging sensitive information in a phishing attack. By leveraging social engineering techniques, attackers can manipulate their targets into believing they are trustworthy or in a position of authority.

For example, the principle of authority can be used to create the illusion of credibility and legitimacy. An attacker may impersonate a trusted source, such as a bank or government agency, and request that the victim provide personal information or login credentials. By

using the authority principle, the attacker is able to exploit the victim's natural inclination to comply with perceived authority figures.

Similarly, the principle of scarcity can be used to create a sense of urgency and scarcity to pressure victims into taking immediate action. For instance, an attacker may claim that the victim's account has been compromised and that they need to act quickly to avoid potential financial loss or other negative consequences.

The principle of liking can also be used to build a sense of rapport and trust with the victim. Attackers may use personal information or details to create a sense of familiarity with their targets, which can make them more likely to comply with requests for sensitive information.

These objectives will guide the design and development of the course and ensure that learners are able to acquire the necessary knowledge, skills, and attitudes which the objectives will be based upon. The learning objectives when teaching recognition of phishing attacks using knowledge from persuasion principles will include:

- Developing an understanding of different types of phishing attacks and their impact: This objective focuses on building knowledge of different types of phishing attacks such as spear phishing, whaling, and social engineering attacks. It also aims to create awareness of the potential impact of these attacks on individuals and organizations.

- Recognize common phishing techniques: This objective focuses on developing the skill to identify common phishing techniques used by attackers, such as baiting, pretexting, and spoofing. It also aims to build the ability to identify phishing attacks across different communication channels such as email, social media, and messaging platforms.

- Evaluate suspicious emails and messages: This objective aims to build the skill to evaluate the credibility of emails and messages received, and determine whether they are legitimate or suspicious. It focuses on developing critical thinking skills to identify inconsistencies in the content, formatting, and language used in messages.

- Apply the knowledge of persuasion principles to recognize and respond to phishing attacks: This objective focuses on applying knowledge of persuasion principles such as authority, scarcity, social proof etc. to recognize and respond to phishing attacks. It aims to build the skill to analyse the content and context of messages to identify the presence of persuasion techniques, and respond appropriately to mitigate the risk of an attack.

Overall, the learning objectives focus on building knowledge, skills, and attitudes necessary to recognize and respond to phishing attacks using knowledge of persuasion principles.

3.2.2 Instructional Strategy

The instructional strategy for the e-learning app for teaching phishing recognition will involve a combination of different techniques to ensure effective learning. The strategy will include brief lectures delivered in different phases, designed to cover various aspects of phishing attacks and the principles of persuasion used in these attacks. The lectures will be designed to be engaging and interactive, with examples and case studies used to illustrate concepts.

To keep the learners actively engaged, questions will be inserted in between the lectures to test their understanding and reinforce their knowledge. The questions will be designed to encourage the learners to think critically and apply the concepts they have learned.

At the end of the lectures, a quiz will be administered to evaluate the learners' understanding of the subject matter. The quiz will be designed to be comprehensive, covering all aspects of phishing recognition and the principles of persuasion. It will be a combination of multiple-choice and short-answer questions, to test the learners' knowledge and application of the concepts.

The instructional strategy will also include the use of technology, such as interactive multimedia and gamification, to enhance the learning experience. Interactive multimedia will be used to provide visual aids and interactive simulations that will help learners understand the concepts better.

The instructional strategy will aim to provide a comprehensive and engaging learning experience that will equip the learners with the knowledge and skills to recognize and avoid phishing attacks.

3.2.3 Minimum Viable Product of the e-Learning

Based on the scope of your thesis and the MVP (minimum viable product) approach, the focus will be on creating a simple, user-friendly e-Learning platform that effectively teaches learners to recognize and prevent phishing attacks applying the knowledge from principles of persuasion. The MVP will include the core components of the instructional design, such as interactive multimedia content, quizzes, and assessments. It will also have a basic user interface with easy navigation and access to the necessary materials.

The MVP will be functional and accessible on web browser using a PC which is okay to accommodate the learners' needs. Additional features and improvements can be added to the application based on feedback and evaluation from the learners and the assessment results.

3.3 Development Phase

This phase details the actual creation of the e-Learning. It involves the development of the instructional design, creation of the content, design of assessments and learning activities, and the production of the multimedia or other instructional materials, following the instructional strategy.

Firstly, the author was required to establish the framework of the course and generate a written document detailing the content and structure of the course, commonly known as the transcript (appendix 2). The transcript acts as the blueprint for the development phase of the ADDIE methodology, guiding the author in creating the necessary materials for the course. The transcript includes welcoming words which set the tone for the learners, follow by instructions/guidance for better learning experience. Upon logging into the portal, this information is presented on the initial page as seen in figure 2.

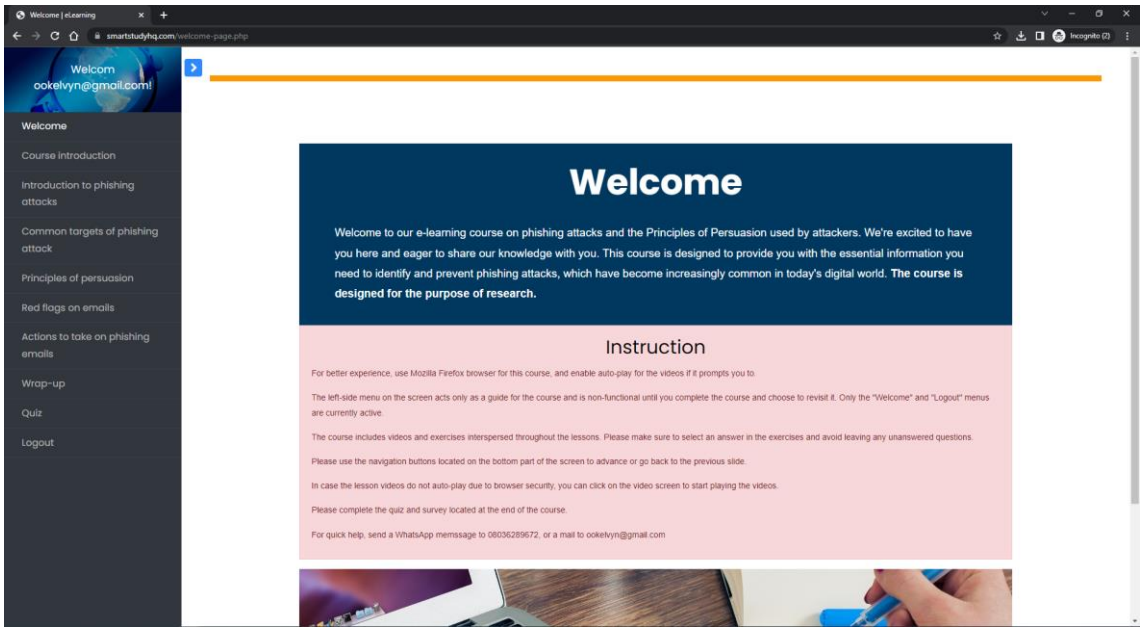


Figure 3: Welcome page of the e-Learning course

The majority of the textual content included in the transcript is transformed into an audio format with the assistance of the Naturalreader AI web application as seen in Figure 4. This audio content will subsequently be utilized to generate video resources that can be easily accessed and comprehended by the learners.

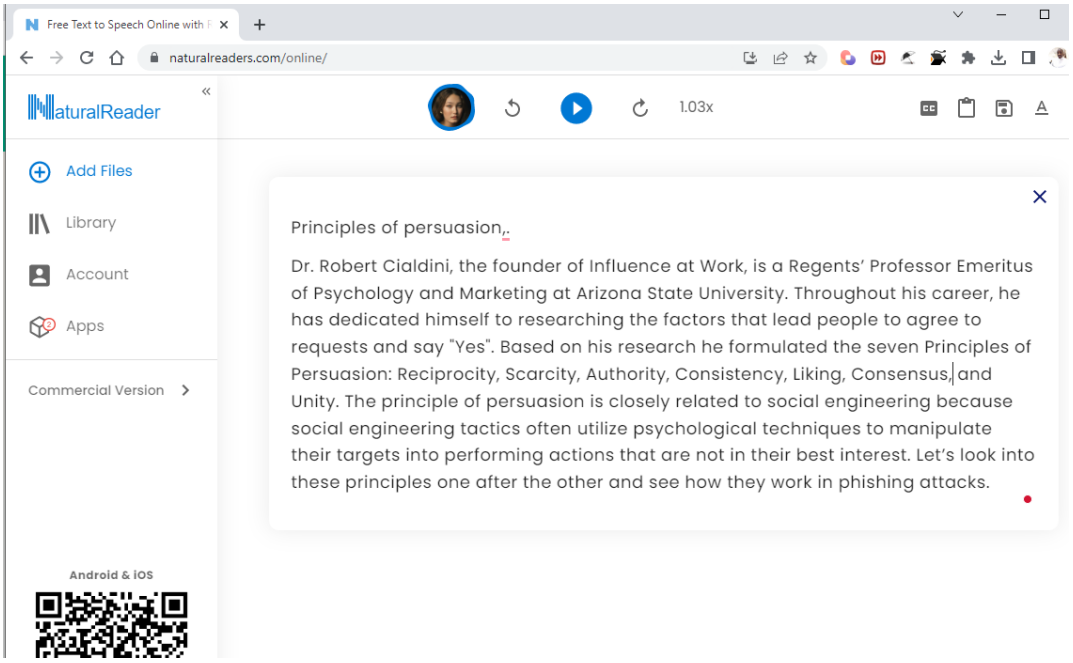


Figure 4: Converting text to speech with Naturalreader

Based on the findings from our previous survey, it was revealed that a majority of the learners expressed their preference for multimedia elements such as graphics, audio, animations, and images. Therefore, in order to cater to their learning needs, the author had to download free images from the Pixabay website which are relevant and relatable to the scenarios being presented in the course. After obtaining images, the author combines them with the previously converted text to speech. This combination of visual and audio components is then used to create videos through the use of the Clipchamp platform as seen in Figure 5. In consideration of those who may not have optimal listening capabilities, subtitles were meticulously crafted and added to all the videos using app.animaker.com.

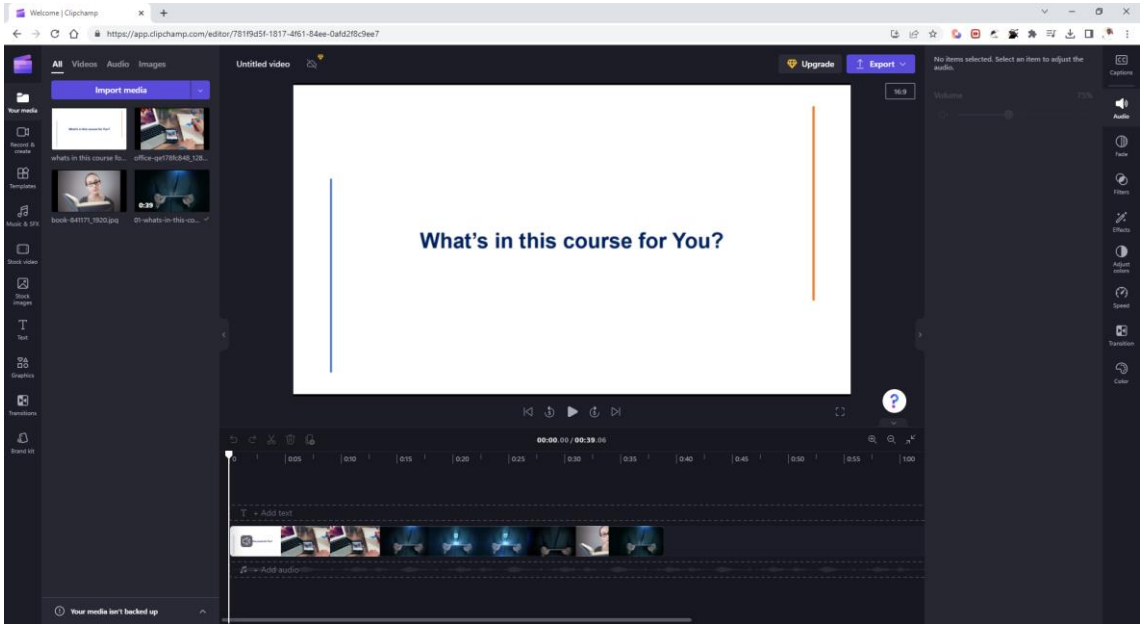


Figure 5: Clipchamp website used for video creation.

The introductory section of the e-Learning course, displayed on the second web page, features the first video which clearly articulates the motivation and purpose of the course. It goes on to expound on the course objectives and goals, thus providing a comprehensive overview of what learners can expect to gain from taking the course. The course then incorporated various tasks and questions to be completed at intervals between lessons. Some of the questions presented to the learners are related to the preceding lessons, and this approach is aimed at encouraging active participation in the learning process. An example of questions asked can be seen in figure 6, the question relating to data breach

leading to exposure of personal data in a company was asked before introducing the next slide that speaks to phishing attack which is the related answer for the question.

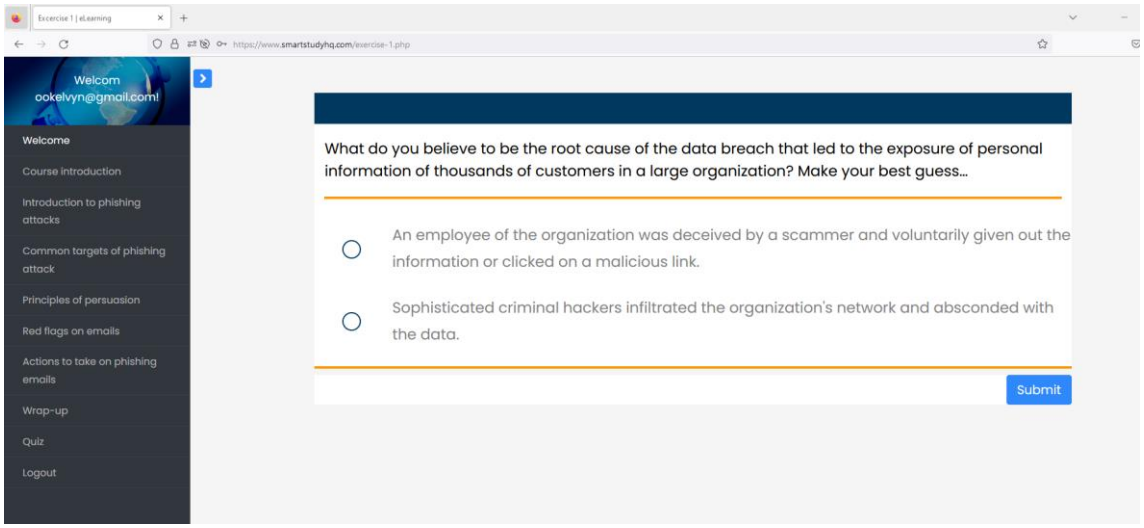


Figure 6: Example of question asked be commencing the related lesson.

In order to provide a better learning experience for the learners, the author developed a task which focuses on teaching the skills required to effectively check the links on URLs and buttons as depicted in figure 7. This task was included with the intention of improving the practical skills of the learners and enabling them to confidently apply the theoretical knowledge they have acquired during the course.

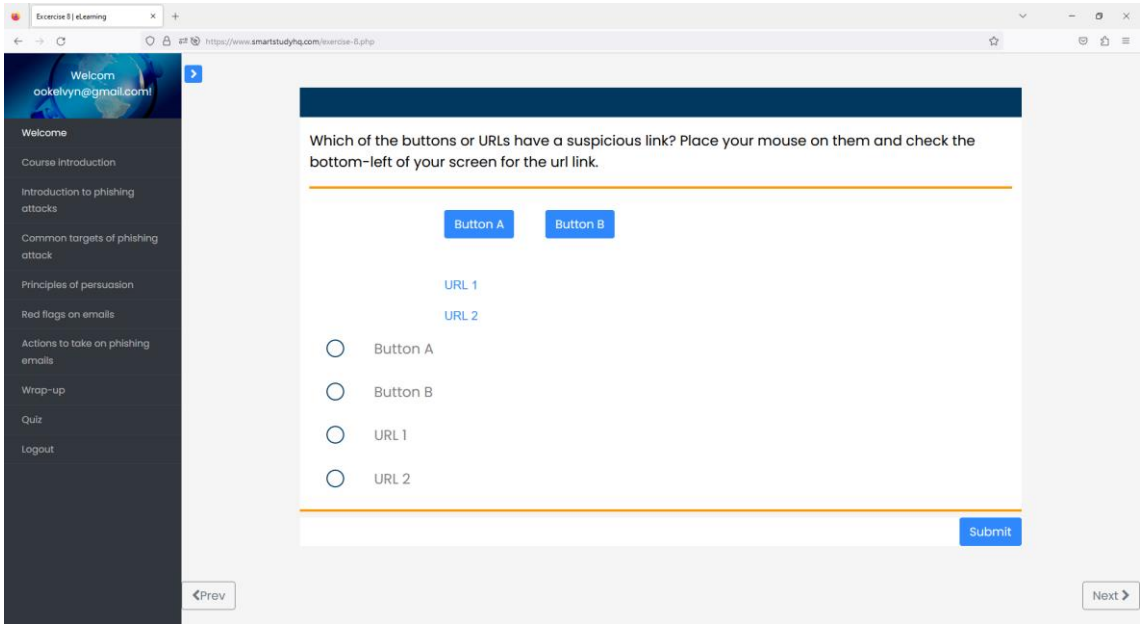


Figure 7: Exercise for checking URLs.

The quiz section of the course was thoughtfully developed, taking inspiration from real-world phishing examples observed on various websites, as well as incorporating exercises from the reputable resource https://phishingquiz.withgoogle.com. An example of part of the quiz is seen in figure 8.

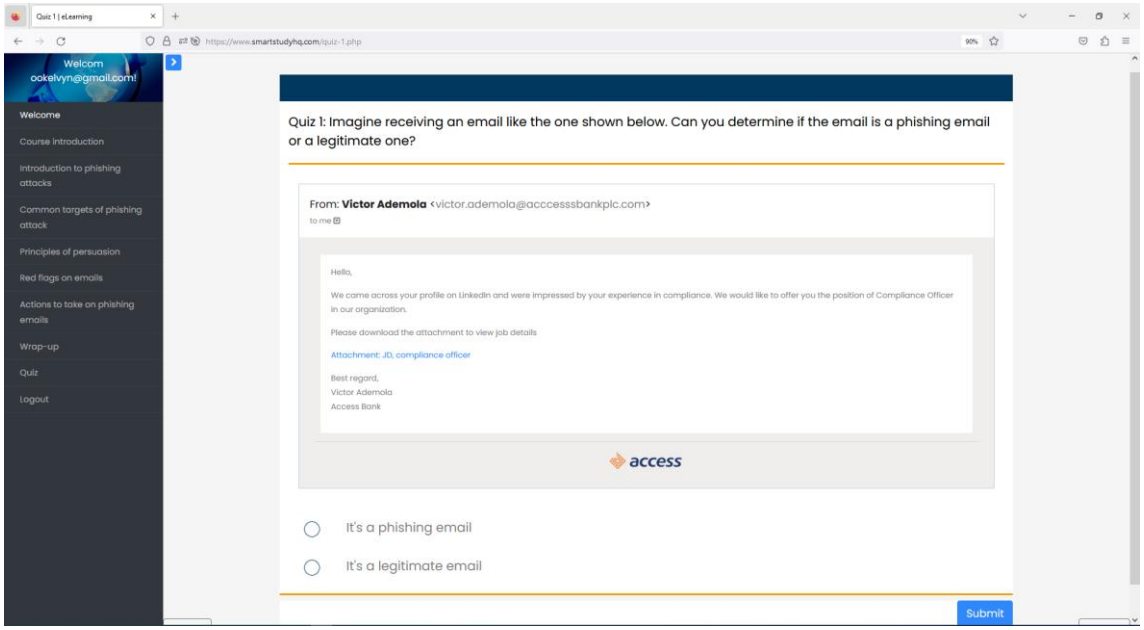


Figure 8: Sample of the first quiz

The entire e-Learning course is developed as a series of webpages, which are designed with HTML code to establish the structure. Additionally, CSS is utilized to style the pages to make them more visually appealing to the learners. The author also incorporated JavaScript code to initiate specific events within the e-Learning course.

To make the e-Learning site more dynamic and capable of handling data, the author utilized a server-side scripting language known as PHP - PHP Hypertext Preprocessor, a web programming language. This allowed for the creation of interactive elements on the site and provided the ability to process and manage data input from learners.

The design of the course is optimized for compatibility with a majority of web browsers typically accessed via desktop or laptop computers. Although it can be accessed through smaller devices like smartphones, but the user experience may be somewhat compromised due to the limited screen space.

3.4 Implementation Phase

After the web content was developed on local computer, the next step was to make it available online. To achieve this, the content was uploaded to a web hosting service, and a domain name was registered. As a result, the e-Learning course could be accessed through the domain name https://www.smartstudyhq.com. The process expected of the users involves creating a personalized account that has a unique identification, followed by logging in to the account before proceeding to take the course. The e-learning website that was developed has a layout that is illustrated in figure 9.

The e-learning course is scheduled to be taken within a period of 4 days, starting from the 11th of April and ending on the 14th of April, allowing learners to complete the course at their own pace. The coordination of this schedule was carried out by the group's Lead, and technical support was provided by the author to ensure a smooth learning experience.

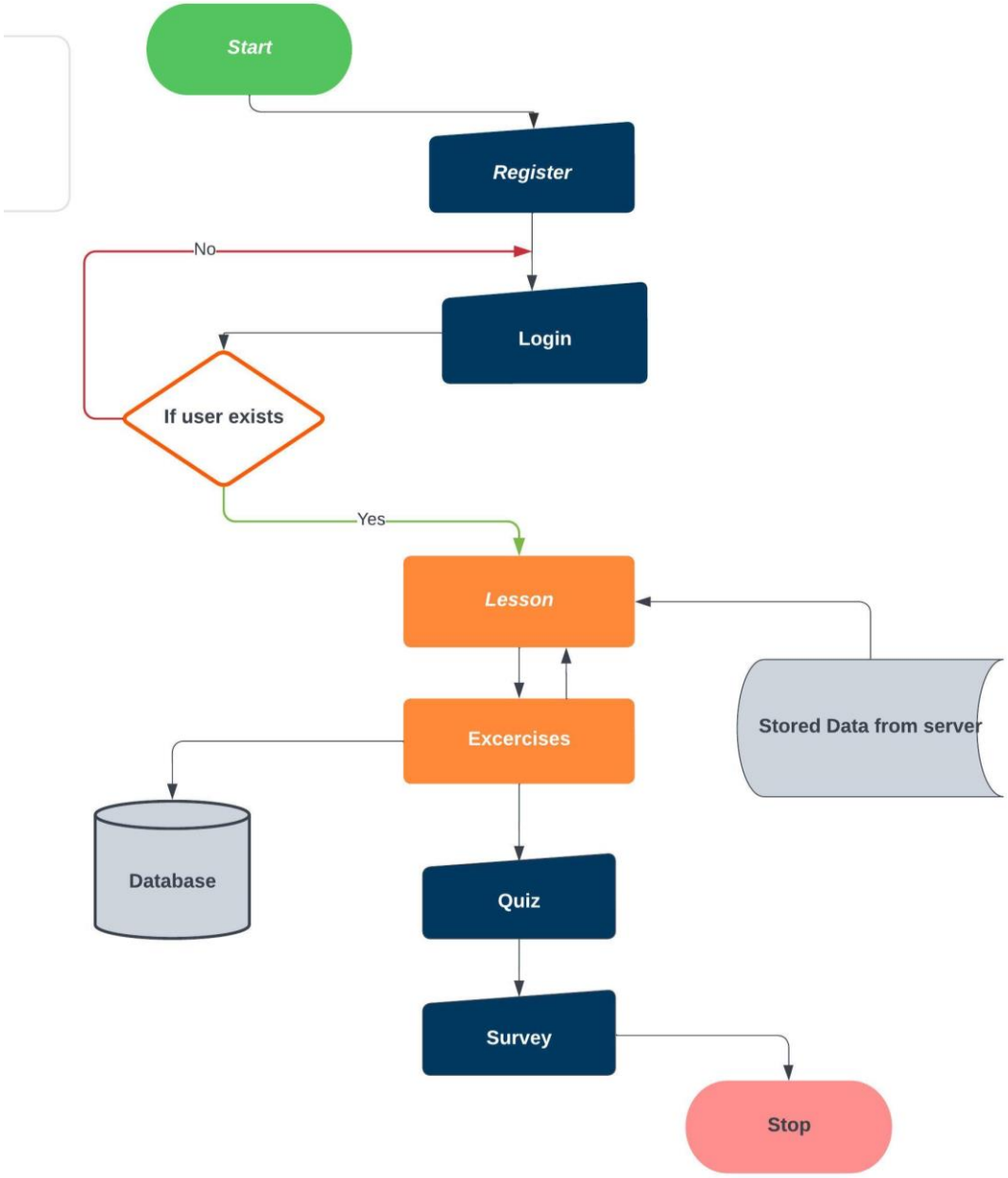


Figure 9. A flowchart illustrating the user's activity on the e-learning portal.

4 Evaluation

The evaluation phase of this thesis focuses on assessing the effectiveness of the e-learning course developed using the ADDIE model. The course was designed to improve the cybersecurity knowledge and awareness of learners, and learning persuasive principles on phishing attacks. The purpose of this evaluation is to determine whether the course achieves its intended learning objectives and to identify any areas where improvements can be made.

The evaluation was a continuous process that took place during the entire duration of the e-Learning course. The evaluation process of the e-learning course encompassed the learners' inputs which were gathered from their responses to the exercises and quizzes during the course. Additionally, a survey was conducted using a questionnaire after the learners had completed the training. The survey aimed to gather feedback on the effectiveness of the course and provide insights into areas that could be improved in future iterations. The learners' inputs and feedback were vital in assessing the overall quality and effectiveness of the course.

46 out of the 57 registered participants successfully completed the e-learning course, which included completing exercises, quizzes, and providing feedback through a survey. There were 21 male participants and 25 female participants.

4.1 Assessment of Learners' Performance

The course employs a strategy where some exercises were given prior to the related lesson with the aim of stimulating the recall of prior knowledge, promoting comprehension, and developing critical-thinking skills. The first exercise presented a scenario where the learner was prompted to identify the root cause of a data breach that resulted in the compromise of personal data belonging to thousands of customers within a large organization. 30 respondents, accounting for 65% of the total, answered the question correctly, while the remaining 16 respondents, making up 35% of the total, selected an incorrect answer. This question was followed by introducing the course and the content to be learnt.

The second exercise featured a question that asked the learners to identify what a phishing attack is, with the correct option being "a type of social engineering". The correct option was chosen by 74% (34) of the respondents. Upon reflecting on the analysis phase of our learners, it was discovered that approximately 19% of them reported not having received any prior training on phishing. However, the question was asked to help the learners to recall and retrieve prior knowledge, which can aid in the comprehension and retention of new information presented during the course.

After providing an explanation about phishing attacks and the potential consequences, the learners were presented with a question that aimed to test their understanding of a specific type of phishing attack. The question asked, "What is the type of phishing attack that involves the creation of a fraudulent email address that appears similar to a genuine email of a trusted organization, with the intent of deceiving users into clicking on a harmful link?" 78% (36 respondents) answer the question correctly while 22% (10 respondents) chose a wrong answer.

The fourth exercise presented five options to identify the common targets of phishing attacks, including the correct option "all of the above". 39 out of 46 learners, which is equivalent to 85%, answered the question correctly, while 7 learners, which is 15%, chose the wrong answer. This gives an idea that that they have a good understanding of the types of targets that cybercriminals typically use to launch phishing attacks.

Prior to introducing the seven persuasion principles by Cialdini, the learners were asked if they were already familiar with them. Subsequently, a follow-up question was presented, specifically "Which persuasion principle pertains to being influenced by an individual due to a shared tribal affiliation?" Exercise 5 and exercise 6 comprised these questions. Out of the total participants, 46 learners, 54% (25 learners) answered negatively as they were not acquainted with the principles of persuasion. On the other hand, 45% (21 learners) of the participants responded positively, claiming to be familiar with the principles of persuasion. And regarding the follow-up question, 4 options were presented to the learners to select from, only 28% (28 learners) of the participants chose the correct option. The outcome here suggests that they may not have a strong understanding or knowledge of the persuasion principles. Lessons on the seven principles of persuasion began after these questions.

Following the summary of the seven persuasion principles, a lesson on "identifying red flags in emails" was presented, which was followed by a practical exercise where learners were required to hover over a button and correctly choose the URL it revealed. A set of three options were provided, out of which one was the correct response. The correct option was selected by 56% of the participants, while the remaining participants evenly distributed their choices among the other two incorrect options with 22% each.

The final exercise 8, similar to the previous one, provided additional details on where learners could find the URL by hovering their mouse over the buttons. The learners were presented with four options to choose the correct one from. The correct option was chosen by 87% (40 participants), while the remaining 13% (6 participants) chose the wrong option.

Following the lessons and exercises, a quiz was administered to evaluate the learners' comprehension of the course content. The quiz is a form of assessment that allows learners to demonstrate their understanding of the concepts covered in the course. The quizzes were presented in the form of web-based emails, with elements such as sender's address, company logos, links with assumed attachments, buttons, and an email body, designed to closely resemble typical email formats. The quizzes presented consisted of four examples designed to test the learners' ability to identify phishing emails and one example that required them to identify the persuasion principle used in a phishing email. 87% (40 participants) of the learners correctly identified the first quiz as a phishing email, while 13% (6 participants) of the learners selected the wrong answer. The second quiz presented a phishing email, with 93% (43 participants) of the learners selecting the correct answer, while 7% (3 participants) chose the wrong answer. The third quiz presented a genuine email, and 74% (34 participants) of the learners selected the correct answer, while 26% (12 participants) of the learners chose the wrong answer. The fourth quiz presented a phishing email, and 89% (41 participants) of the learners correctly identified it as such, while 11% (5 participants) selected the wrong answer. And for the last quiz, an email was drafted using the principle of consensus, the learners were asked to identify the persuasion principle used in the email. They were presented with four options, one of which was correct. Out of the participants, 91% (42 learners) chose the correct option, while the remaining 9% (4 learners) chose the wrong option.

4.2 Feedback Data Analysis

A questionnaire using Likert scale was used through Google Form to get feedback from the learners, aimed at assessing the course based on four categories: the content of the course, the structure and design of the course, the exercises and quizzes and knowledge gained. The learners were also provided with an opportunity to offer general feedback as well.

The learners' email addresses, which they used to register for the e-learning course, were collected along with the feedback. This was done to facilitate the analysis of feedback received only from learners who had fully participated in the course.

4.2.1 Feedback on the Course Content

The first section of the questionnaire was aimed at getting feedback about the content of the course as it helps to evaluate if the course met the learners' expectations and if the information provided was useful, relevant, and engaging. And also provides insights into areas that may require improvement or further development.

The questionnaire began by asking whether the course had a clear purpose. Out of 46 participants, 33 (72%) strongly agreed and 11 (24%) agreed that "the course had a clear purpose." Only 2 (4%) participants were neutral, while no one disagreed or strongly disagreed with the statement. The high percentage of agreement suggests that most participants felt that the course had a clearly defined purpose, which likely contributed to their overall positive perception of the course as seen in figure 10.

The second statement 'The aim of the course and tasks were achievable' was strongly agreed upon by 25 participants (54%) and agreed upon by 20 participants (44%). Only one participant (2%) strongly disagreed, while no participants were neutral or disagreed (figure 10). This indicates that the majority of participants found the course goals and tasks to be realistic and feasible.

Out of the 46 participants who took the survey, a majority of 56% (26 participants) strongly agreed that the e-learning course used relevant examples and scenarios, while 37% (17 participants) agreed. Only a small minority of 7% (3 participants) were neutral, and none of the participants disagreed or strongly disagreed with the statement (figure

10). This suggests that the use of relevant examples and scenarios in the course was effective in engaging the learners and enhancing their understanding of the subject matter.

The next statement "The course content was presented in a way that was engaging and kept my attention" received responses from 46 participants. Out of these, 25 (54%) strongly agreed, 16 (35%) agreed, 4 (9%) were neutral, 1 (2%) disagreed, and 0 strongly disagreed. This suggests that a majority of the participants found the course content to be engaging and able to keep their attention, although a small portion did not agree with this statement.

Following the last statement in this category, "the course content provided enough depth and detail on the subject matter" received 25 (54%) strong agreements, 17 (37%) agreements, 4 (9%) neutral responses, 0 disagreements, and 0 strong disagreements from the participants.

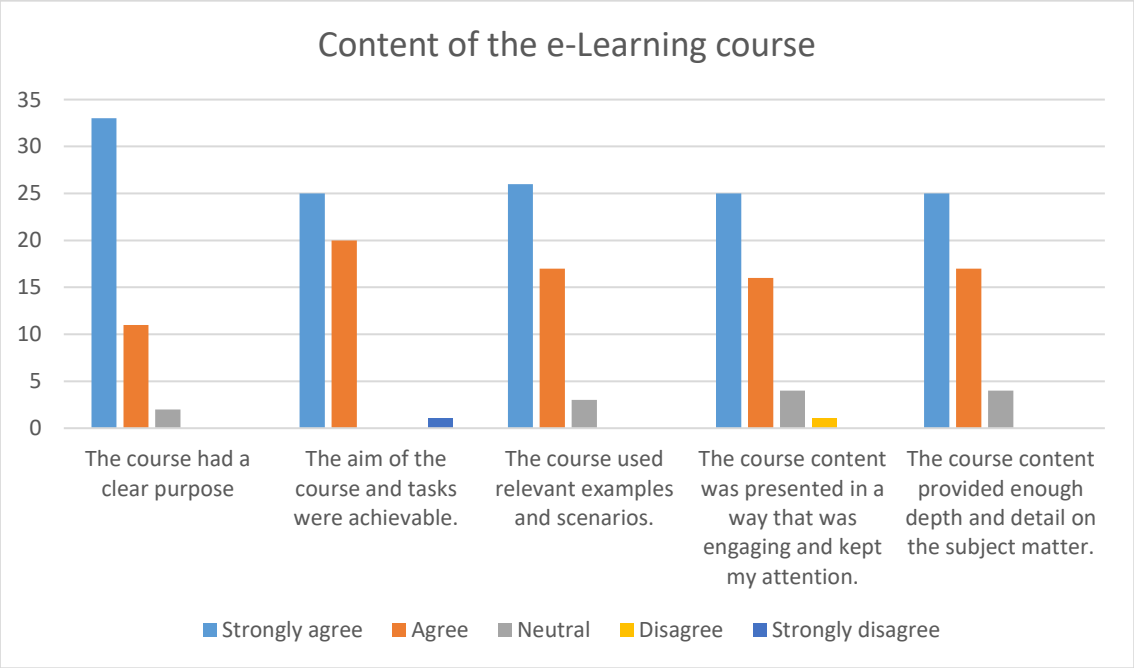


Figure 10: Response on content of the e-learning course

4.2.2 Feedback on the Structure and Design of the Course

The participants provided feedback on the overall structure and design of the e-learning course. This feedback focused on aspects such as the organization of content, ease of navigation, visual and pace of the course.

The statement 'The course had a straightforward structure and was not difficult to follow" received feedback from 28 (61%) participants who strongly agreed, 15 (33%) participants who agreed, 3 (6%) participants who were neutral, 0 participants who disagreed, and 0 participants who strongly disagreed as seen in figure 11. This suggests that the majority of participants found the structure of the course to be easy to follow and straightforward, with only a small number expressing uncertainty or disagreement. This positive feedback indicates that the course was well-organized and presented in a clear and concise manner.

Out of the 46 participants, 17 (37%) strongly agreed and 28 (61%) agreed that the course was visually appealing. Only 1 participant (2%) was neutral, and no participants disagreed or strongly disagreed with the statement (figure 11). This indicates that a majority of the learners found the course visually appealing, which must have contributed to their engagement and motivation to learn.

The statement "The use of multimedia elements (e.g, video, pictures, sound) was effective" was responded to by 25 (39%) participants who strongly agreed, 18 (57%) participants who agreed, 3 (7%) participants who were neutral, 0 participants who disagreed, and 0 participants who strongly disagreed (figure 11). This indicates that the majority of the participants found the use of multimedia elements in the e-learning course to be effective in enhancing their learning experience. However, a small percentage of participants remained neutral on the statement. For future course, it would be useful to explore further why they did not have a strong opinion on the effectiveness of the multimedia elements.

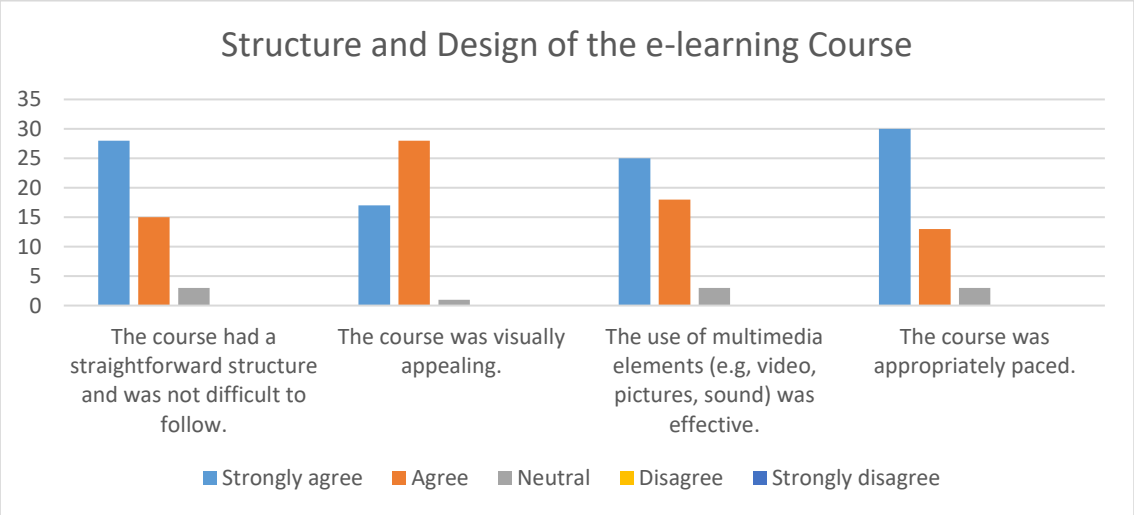


Figure 11: Feedback on the structure and design of the course

The statement "The course was appropriately paced" received feedback from the 46 participants. Out of these, 30 (65%) strongly agreed, 13 (28%) agreed, and 3 (7%) were neutral (figure 11). None of the participants disagreed or strongly disagreed with the statement. This indicates that a majority of the learners felt that the course was taught at a suitable pace, while a smaller percentage had a neutral opinion.

4.2.3 Feedback on Exercises and Quiz

It was necessary to ask for feedback on the exercises and quizzes given in order to assess their relevance and effectiveness for the learners. This information helps to determine whether the course content was being effectively communicated and whether the learners were able to grasp the key concepts being taught.

The statement 'There were enough tasks in the course' received feedback from 46 participants, with 44 participants (44%) agreeing and 20 participants (44%) strongly agreeing. Only 6 participants (12%) were neutral, while no participants disagreed or strongly disagreed with the statement. This indicates that a majority of the participants found the number of tasks to be adequate, while a small percentage had a neutral opinion.

The following statement was presented; 'The tasks and exercises were effective in reinforcing my learning' received positive feedback from the participants. Out of 46 participants, 27 (59%) strongly agreed, 16 (35%) agreed, and 3 (6%) were neutral as seen in Figure 12. No participants disagreed or strongly disagreed with the statement. This indicates that the tasks and exercises in the course were perceived to be helpful in consolidating the participants' understanding of the course material.

The statement "The tasks and quiz were relevant to the course content" was strongly agreed by 32 participants (69%), agreed by 9 participants (20%), and had 5 neutral participants (11%). No participants disagreed or strongly disagreed with the statement (figure 12). This indicates that the majority of the participants found the tasks and quiz to be closely related to the course content and were able to reinforce their learning effectively. However, it's worth noting that a small percentage of participants were neutral, which could suggest that there is room for improvement in terms of ensuring the relevance of tasks and quizzes for all learners.

As seen in Figure 12, of the total 46 participants, the majority of the participants, 28 (61%), strongly agreed that the tasks and quiz provided feedback or explanations for correct and incorrect answers, while 14 (30%) agreed. Only 4 (9%) participants were neutral, and there were no participants who disagreed or strongly disagreed with this statement. The result indicates that the majority of the participants found the feedback and explanations provided by the tasks and quiz to be helpful in reinforcing their learning and understanding of the course content. This feedback can be used to improve the design and implementation of future e-learning courses to ensure that they provide adequate feedback to learners.

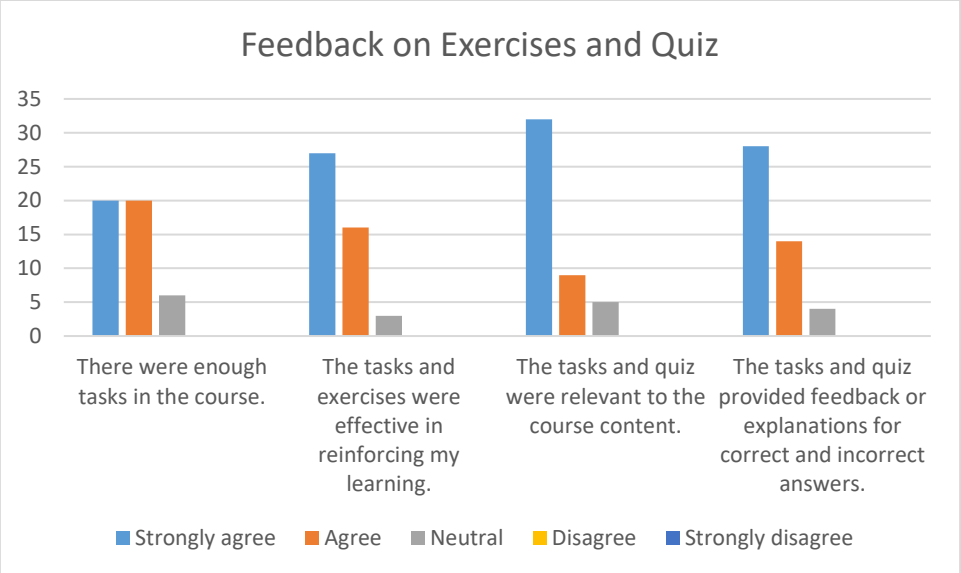


Figure 12: Feedback on Exercises and Quizzes

4.2.4 Feedback on Knowledge Gained

To assess the extent to which the course accomplished its learning objectives, the author conducted a survey to evaluate the knowledge acquired by the learners. The goal is to assess the learners' comprehension of persuasion principles and their application in phishing attacks, as well as their confidence in defending against such attacks.

This section began with the statement "The course helped me to better understand how persuasion works in real-world scenarios and in phishing attacks", and feedback as from 46 participants. Out of these, 35 (76%) strongly agreed, 9 (20%) agreed, and 2 (4%) were neutral as seen in Figure 13. No participant disagreed or strongly disagreed with the statement. This indicates that a large majority of the learners found the course effective

in enhancing their understanding of persuasion in real-world scenarios and its connection to phishing attacks.

As seen in Figure 13, 50% of participants (23) strongly agreed that they feel more confident in their ability to apply the knowledge of principles of persuasion to prevent phishing after taking the course. 41% of participants (19) agreed with the statement while 9% of participants (4) were neutral. No participant disagreed or strongly disagreed with the statement. This suggests that the course was effective in increasing participants' confidence in applying the principles of persuasion to prevent phishing. However, 4 (9%) participants were neutral, indicating that the course may not have had a significant impact on their confidence in this area.

A total of 46 participants provided their feedback on the statement "The course has increased my knowledge and awareness of the risk of phishing attacks." Out of these, 31 participants (68%) strongly agreed, 13 participants (28%) agreed, and 2 participants (4%) were neutral. No participant disagreed or strongly disagreed with the statement. The majority of the participants (96%) agreed or strongly agreed that the course increased their knowledge and awareness of the risk of phishing attacks. This suggests that the course was effective in achieving its objective of educating the learners on the risks associated with phishing attacks. The high percentage of participants who strongly agreed with the statement also indicates that the course content was well-received by the learners and was effective in conveying the necessary information.

As seen in Figure 13, the statement "The course provided practical strategies to avoid falling victim to phishing attacks" was strongly agreed by 31 (67%) participants, 14 (31%) participants agreed, and 1 (2%) participant was neutral. No participants disagreed or strongly disagreed. This indicates that the majority of the participants found the course to be effective in providing practical strategies to avoid falling victim to phishing attacks. The high percentage of strong agreement suggests that the strategies provided were particularly useful and actionable.

The statement "The course adequately covered the main topics and concepts related to persuasion and phishing attacks" was strongly agreed by 27 (59%) participants, while 15 (32%) participants agreed, and 4 (9%) participants were neutral. No participant disagreed or strongly disagreed (Figure 13). This feedback suggests that the majority of participants

found the course to be comprehensive in its coverage of the main topics and concepts related to persuasion and phishing attacks. However, the presence of some neutral responses indicates that there may be room for improvement in terms of further elaborating on certain topics or clarifying certain concepts. Overall, this feedback is positive and indicates that the course was generally effective in providing a comprehensive overview of the subject matter.

The final statement on the questionnaire "Overall, I feel that the course met my expectations and was beneficial to my learning" reveals that 24 (52%) participants strongly agreed, 18 (39%) participants agreed, and 4 (9%) participants were neutral in their response to the course meeting their expectations and being beneficial to their learning. This feedback indicates that a majority of the participants (91%) felt that the course met their expectations and was beneficial to their learning. Only a small proportion (9%) were neutral in their response. While it's positive that the majority of the participants found the course beneficial, the feedback from the neutral participants could be used to identify areas for improvement or to gather more specific feedback on what they felt could have been improved. Overall, the feedback suggests that the course was successful in meeting the expectations of most participants and was helpful in enhancing their learning.

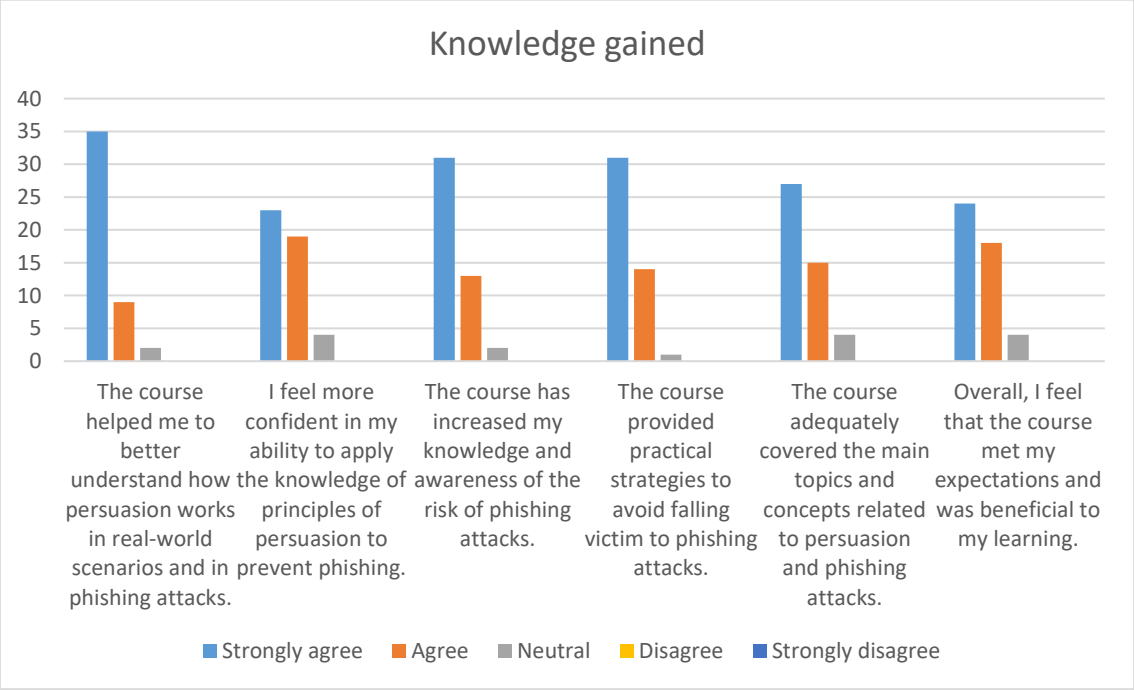


Figure 13: Feedback on knowledge gained on the course.

4.2.5 General Feedback from Learners

After completing the survey, the learners were provided with an opportunity to provide any supplementary feedback or comments. Some examples of the feedback/comments received are as follows:

- Nice course
- It will really help in our day-to-day work life.
- Going through the course was educating and brought more awareness to me about the types of persuasions.
- Satisfactorily
- The course was helpful
- Nice work keep it up. I have gained knowledge about cyber security.
- Educative task
- Very Educative
- Informative
- Great job
- Positive thinking
- When questions are raised within the course and answers picked, whenever you log on again it should continue from where you stopped last. It should not take you back to the beginning with the same questions you had earlier done otherwise it should represent the question in another format if you must start all over again.
- Made me have more knowledge about phishing emails.
- Thanks for this course.
- The course is very interesting and educative.

- Very Informative
- I found the course to be useful, however, I believe that additional practical training is necessary.
- The course helped me refresh the knowledge I had on principles of persuasion. I never knew there are now 7 of them.
- I couldn't track my progress, and whenever login again, I start afresh. Overall, i learnt something new, which is persuasion principles.
- Maybe a real-life phishing email would be good for a test.
- The course met my expectations and should be recommended to people, generally.

In addition to the positive feedback, there were a few comments pointing out flaws in the course that need to be addressed.

5 Conclusion and Future Work

This chapter provides a concise overview of the thesis, presents the findings that address the research questions, and offers recommendations for future research.

In this research, we aimed to develop an e-Learning course for anti-phishing education that is based on principles of persuasion to help learners identify and avoid phishing attacks. The introduction section outlines our strategy for accomplishing this goal by presenting the driving force behind it and the proposed approach. ADDIE (Analysis, Design, Development, Implementation and Evaluation) is briefly introduced as the approach proposed for this research.

The subsequent chapter (2) of this study provides a theoretical framework by first defining phishing attacks and tracing their history. The chapter also provides an explanation of different types of phishing attacks and discusses indicators that can be used to recognize phishing attacks. It then delves into different persuasion principles, such as authority, scarcity, consistency, and likability, and elucidates on how these principles can be leveraged to trick victims into revealing confidential information. The chapter also discusses various e-learning methods, including text presentations, video-based e-Learning, educational games, and simulations, which can be used to deliver anti-phishing training. And finally review studies related to persuasion principles and phishing attack.

Exploring the ADDIE phases in chapter 3, survey conducted to gather information about the demographics and computer usage habits of potential course participants. Using the ADDIE model, we designed an e-Learning course framework and created a course prototype that incorporates persuasive techniques to improve participants' ability to recognize and avoid phishing attacks.

We evaluated the course prototype by conducting a pilot study with a group of participants, and found that the course had a positive impact on participants' ability to recognize and avoid phishing attacks. The evaluation results indicate that the e-Learning course is effective in improving participants' knowledge and awareness of phishing attacks, and in providing them with the necessary skills to protect themselves against such attacks.

In conclusion, our research has demonstrated the potential effectiveness of an e-Learning course for anti-phishing that is based on the principles of persuasion. By designing a course that incorporates persuasive techniques, we have been able to improve participants' ability to recognize and avoid phishing attacks.

Our findings suggest that e-Learning courses can be a valuable tool for educating users about online security threats, and that principles of persuasion can be effectively employed to enhance their efficacy.

5.1 Answer to Research Questions

This section provides answers to the research questions stated in Section 1.

- ***How can we effectively teach phishing recognition, and what methods, rationale, and approaches should be considered?***

  One common method of teaching phishing recognition is by many research work is by conducting phishing exercises. However, we found the method explored in this study, developing an e-learning course to be effective. Teaching phishing recognition through e-Learning can be utilized to cover every aspect of phishing attacks, both practically and theoretical. Teaching learners about the tactics used by attackers to influence and persuade their targets, can develop their skills to detect and avoid phishing attacks in various scenarios. Moreover, it has been proven that persuasion principles cover these tactics. Applying ADDIE approach to developing e-learning is useful as it provides a structured approach to the design and development of a course.

- ***What are the key principles of persuasion that can be applied to anti-phishing education, and how effective are they in improving users' ability to recognize phishing attacks?***

  The key principles of persuasion that can be applied to anti-phishing education include authority, reciprocity, consensus (social proof), consistency, liking, scarcity and unity. In this study, the principles mentioned are elaborated in section 2. These principles have been shown to be effective in improving users' ability to recognize phishing attacks by increasing their awareness and skepticism of

suspicious messages, promoting critical thinking and analysis of message content, and encouraging users to seek out additional information before taking action. Many studies have established the prevalence of persuasion principles in phishing attacks. Therefore, integrating these principles into anti-phishing education programs, especially e-learning courses, can offer a well-organized and captivating learning approach to increase awareness and understanding of phishing and its potential risks. The use of e-learning courses incorporating persuasion principles is a promising approach to improve the effectiveness of anti-phishing education.

- ***What are the gaps in knowledge that users have regarding phishing attacks, and how can an e-learning course based on persuasive principles be designed to address these issues?***

  Based on the results of this study and the participants' performance in the exercises, it was found that a considerable number of individuals fail to check links concealed in URLs and lack awareness of persuasion tactics. Phishing involves the use of social engineering tactics in which attackers aim to trick individuals into revealing sensitive information. This deception is accomplished by utilizing various tactics that often involve the application of one or more of the principles of persuasion. The efficacy of developing an e-learning course using the ADDIE method for teaching phishing attacks has been demonstrated in this study, supported by the outcomes of feedback and exercises. Using the ADDIE method to develop an e-Learning course on the principles of persuasion in phishing attacks could help address these issues if applied repeatedly.

5.2 Future Work

Future research could explore additional ways to leverage persuasive techniques to further improve the effectiveness of e-Learning courses for anti-phishing, and to examine the generalizability of our findings across different populations and contexts. Overall, our research contributes to the development of effective and accessible tools for online security education and awareness. In addition to the potential future research on the effectiveness of anti-phishing e-Learning courses based on Cialdini's persuasion principles, it may also be worthwhile to explore the impact of administering phishing

exercises after the completion of the e-Learning course. These exercises could serve as a practical application of the knowledge and skills learned in the course and may further improve the ability of users to recognize and avoid phishing attacks. Additionally, it may be useful to investigate the long-term retention of the knowledge and skills gained through such e-Learning courses and exercises, as well as the potential for customization of the e-Learning content based on the specific needs and vulnerabilities of different user groups.

References

[1] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy". *Frontiers in Computer Science, 3*, p.563060, 2021.

[2] C. Hadnagy, "Social engineering: The art of human hacking," 2010.

[3] D. S. Kurt, "ADDIE Model: Instructional Design - Educational Technology", 2017 Retrieved from https://educationaltechnology.net/the-addie-model-instructional-design/ [Accessed: 18-Feb-2023].

[4] R. M. Branch, "Instructional design: The ADDIE approach" (Vol. 722). *New York: Springer*, 2009.

[5] M. Nishad, "A Review Paper on Phishing through Email". *International Journal of New Technology and Research*, 4(1), p.263164, 2018.

[6] Y. Wang, Y. Liu, T. Wu, and I. Duncan, "A Cost-Effective OCR Implementation to Prevent Phishing on Mobile Platforms". *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-8). IEEE, 2020.

[7] A. Arshad, A.U. Rehman, S. Javaid, T. M. Ali, J. A. Sheikh and M. Azeem, "A systematic literature review on phishing and anti-phishing techniques". arXiv preprint arXiv:2104.01255, 2021.

[8] P. P. Chate, M. S. Maske, and M.S. Maske, "The Advance Techniques used in Cyber Security for Phishing Detection", 2021.

[9] O. Okosun, and U. Ilo, "The evolution of the Nigerian prince scam". *Journal of Financial Crime*, 2022.

[10] N. Tariq, "Impact of cyberattacks on financial institutions". *Journal of Internet Banking and Commerce, 23(2),* pp.1-11, 2018.

[11] P. Burda, T. Chotza, L. Allodi, and N. Zannone, "Testing the effectiveness of tailored phishing techniques in industry and academia: a field experiment". In

Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-10), 2020.

[12] J. Rastenis, S. Ramanauskaitė, J. Janulevičius, A., Čenys, A. Slotkienė and K. Pakrijauskas, "E-mail-based phishing attack taxonomy". *Applied Sciences*, 10(7), p.2363, 2020.

[13] P. Verma, A. Goyal, and Y. Gigras, "Email phishing: Text classification using natural language processing". *Computer Science and Information Technologies*, 1(1), 1-12, 2020.

[14] G. Yu, W. Fan, W. Huang and J. An, "An Explainable Method of Phishing Emails Generation and Its Application in Machine Learning," IEEE 4th *Information Technology, Networking, Electronic and Automation Control Conference (ITNEC),* Chongqing, China, 2020, pp. 1279-1283, doi: 10.1109/ITNEC48623.2020.9085171, 2020.

[15] S. Maroofi, M. Korczyński, A. Hölzel, and A. Duda, "Adoption of email anti-spoofing schemes: A large scale analysis. IEEE Transactions on Network and Service Management", 18(3), 3184-3196, 2021.

[16] Internet Crime Report, 2019, [online] Available: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120. [Accessed: 22-Feb-2023].

[17] A. Hutchings, "Theory and Crime: Does It Compute?", *Griffith University*, 2013.

[18] 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) (pp. 337-343). IEEE, 2020.

[19] E. O. Yeboah-Boateng, and P. M. Amanor, "Phishing, SMiShing & Vishing: an assessment of threats against mobile devices". *Journal of Emerging Trends in Computing and Information Sciences,* 5(4), 297-307, 2014.

[20] K. S. Jones, M. E. Armstrong, M. K. Tornblad, and A. S. Namin, "How social engineers use persuasion principles during vishing attacks". *Information & Computer Security*, 29(2), 314-331, 2021.

[21] S. Mishra, and D. Soni, "Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis". *Future Generation Computer Systems*, 108, 803-815, 2020.

[22] M. Volkamer, K. Renaud, and B. Reinheimer, "TORPEDO: tooltip-powered phishing email detection". In *ICT Systems Security and Privacy Protection: 31st IFIP TC 11 International Conference, SEC 2016, Ghent, Belgium,* Proceedings 31 (pp. 161-175). Springer International Publishing, 2016.

[23] S. Waddell, "CatchPhish: A URL and Anti-Phishing Research Platform". *Doctoral dissertation, Master's thesis*. University of Edinburgh, 2020.

[24] O.A. Zielinska, A.K. Welk, C.B. Mayhorn, and E. Murphy-Hill, "A temporal analysis of persuasion principles in phishing emails". In *Proceedings of the human factors and ergonomics society annual meeting* (Vol. 60, No. 1, pp. 765-769). Sage CA: Los Angeles, CA: SAGE Publications, 2016.

[25] A. Birkett, "Cialdini's 7th Persuasion Principle: Using Unity in Online Marketing." *Conversionxl. Geraadpleegd van https://bit.ly/2fYFIZl*, 2016.

[26] D. R. Cialdini, "The Principles of Persuasion Aren't Just for Business. Retrieved from https://www.influenceatwork.com/principles-of-persuasion-are-not-just-for-business/, 2016. [Last retrieved 09-Mar-2023].

[27] D. Kelley, "The psychology of social engineering—the "soft" side of cybercrime" *Microsoft Security Blog*. Retrieved from https://www.microsoft.com/en-us/security/blog/2020/06/30/psychology-social-engineering-soft-side-cybercrime/, 2020. [Last retrieved 09-Mar-2023].

[28] S. Chiriatti, "Fogg and Cialdini's persuasive principles present in different types of e-services' web pages." 2021.

[29] D. Strmecki, A. Bernik, and D. Radosevic, “Gamification in E-Learning: Introducing Gamified Design Elements into E-Learning Systems”. *J. Comput. Sci.*, *11*(12), 1108-1117, 2015.

[30] B. Ondrejička, “Gamification of Phishing Resiliance Training”, *Master’s Thesis, Masaryk University* 2022.

[31] L. Zdanevych, K. Kruty, O. Demianenko, N. Pakhalchuk, L. Perminova, and O. Garachkovska, “E-Learning Methods in Students’ Education”, 2019.

[32] N. Akbar, “Analysing persuasion principles in phishing emails” *Master's thesis, University of Twente,* 2014.

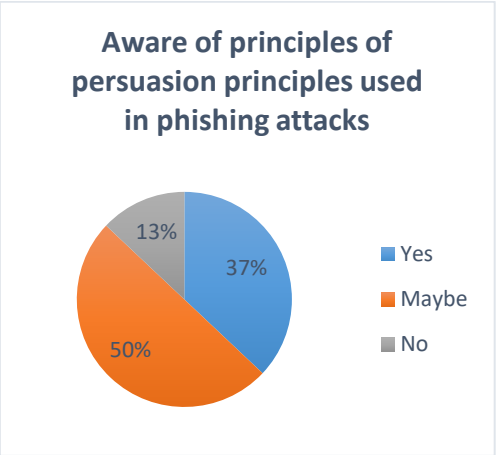
[33] A. Ferreira, and S. Teles, “Persuasion: How phishing emails can influence users and bypass security measures”. *International Journal of Human-Computer Studies*, 125, pp.19-31, 2019.

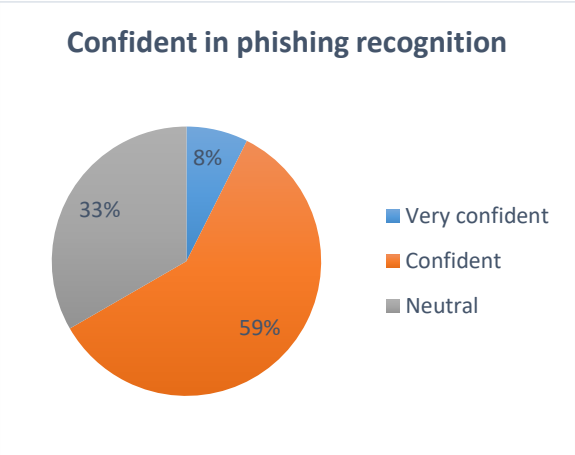
[34] X. Li, D. Zhang and B. Wu, “Detection method of phishing email based on persuasion principle”. In IEEE 4th Information Technology, *Networking, Electronic and Automation Control Conference* (ITNEC) (Vol. 1, pp. 571-574). IEEE, 2020.

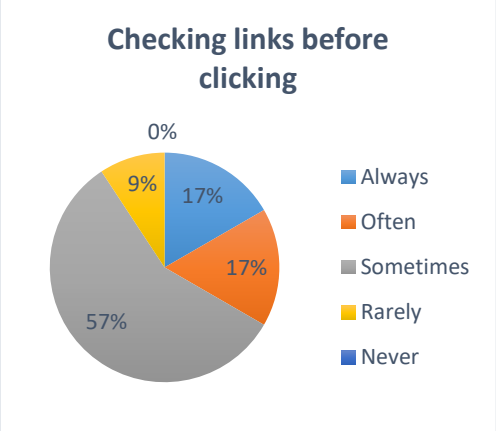
[35] P. Burda, T. Chotza, L. Allodi, and N. Zannone, “Testing the effectiveness of tailored phishing techniques in industry and academia: a field experiment”. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-10), 2020.

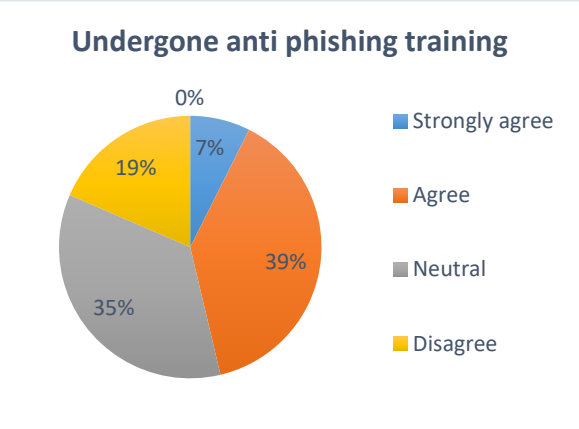
[36] V. A. Garcia and R. D. Parra, “Phishing video game to validate the principles of persuasion in university students”. In *AMCIS*, 2021.

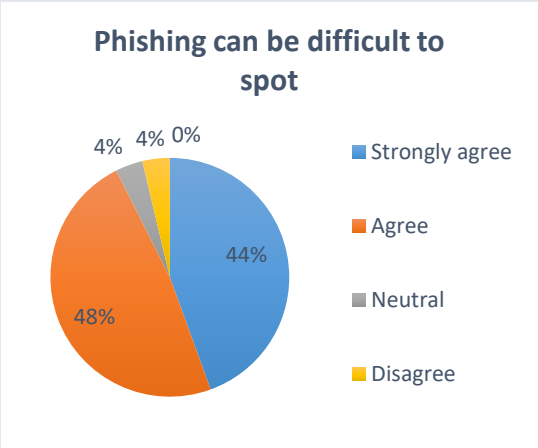
Appendix 1 - Questionnaire result



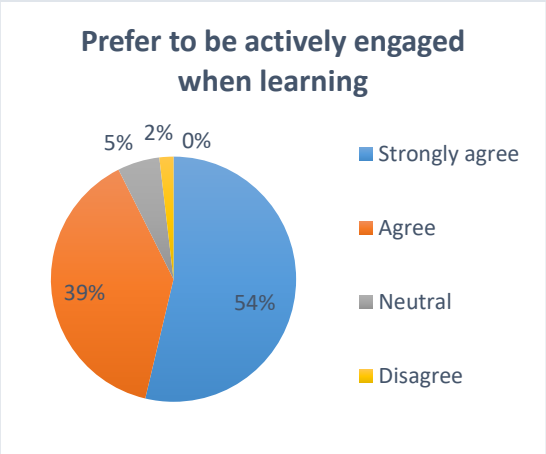


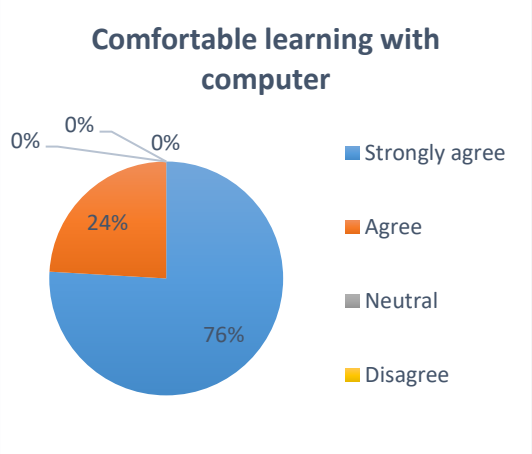


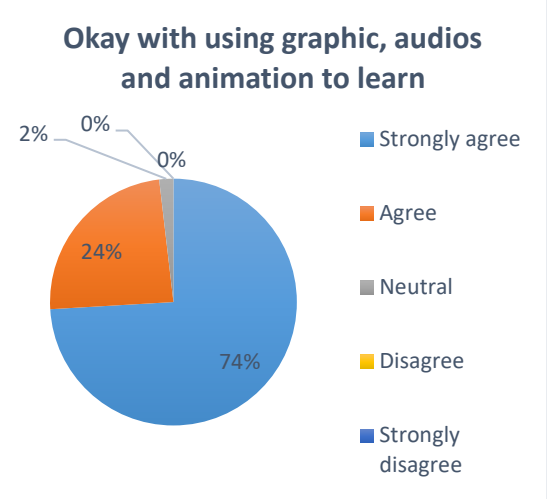




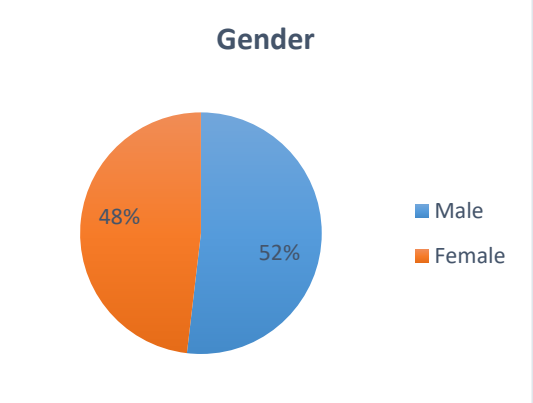
Learning preferences

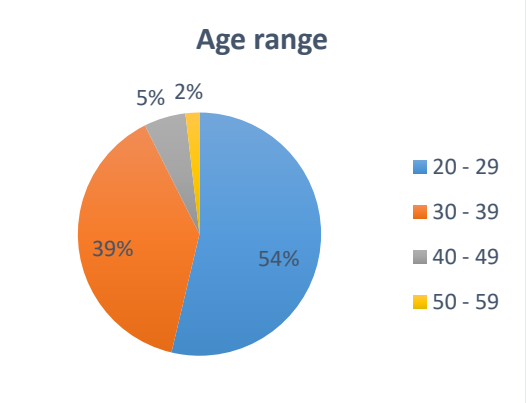


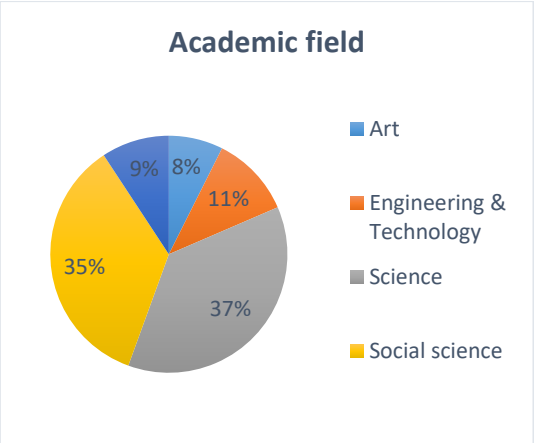


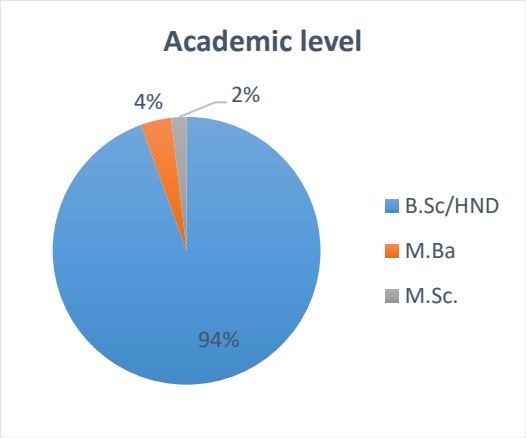


Demographic

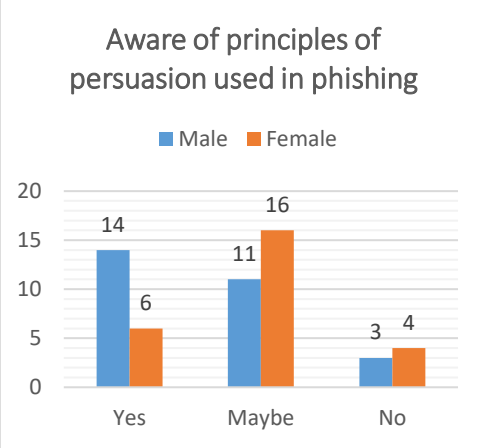


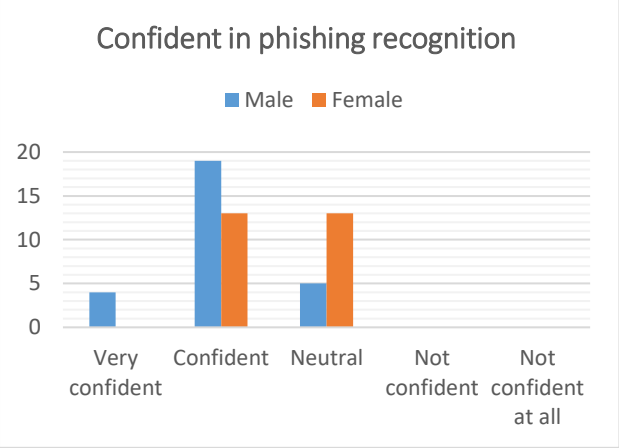


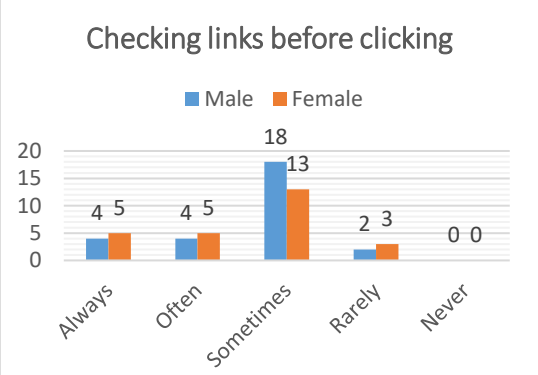


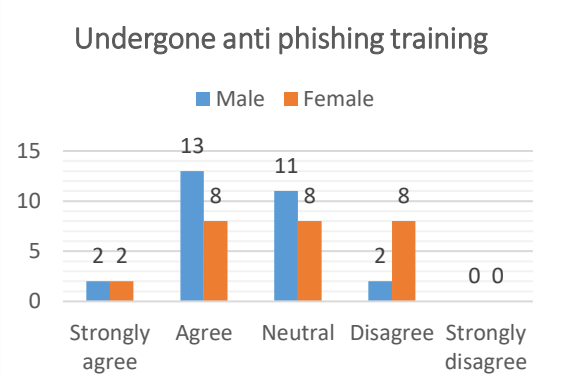


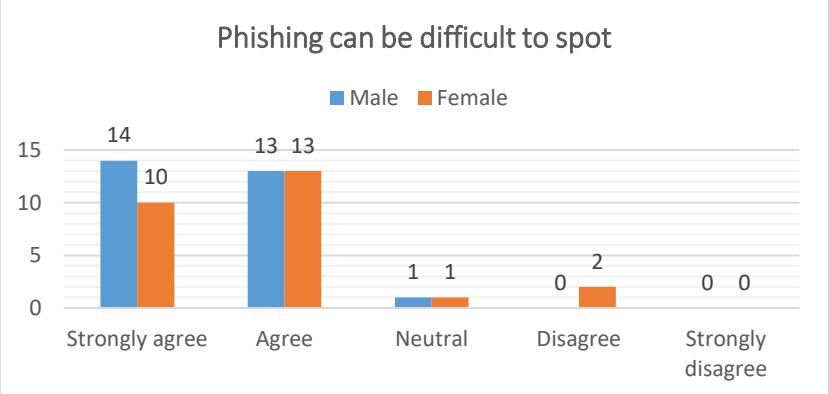
Comparison between male and female











Appendix 2 – e-Learning course transcript

Page 1 – Welcome

Welcome to our e-learning course on phishing attacks and the principles of persuasion used by attackers. We're excited to have you here and eager to share our knowledge with you. This course is designed to provide you with the essential information you need to identify and prevent phishing attacks, which have become increasingly common in today's digital world.

Instruction

For better experience, use Mozilla Firefox browser for this course, and enable auto-play for the videos if it prompts you to.

The left-side menu on the screen acts only as a guide for the course and is non-functional until you complete the course and choose to revisit it. Only the "Welcome" and "Logout" menus are currently active.

The course includes videos and exercises interspersed throughout the lessons. Please make sure to select an answer in the exercises and avoid leaving any unanswered questions.

Please use the navigation buttons located on the bottom part of the screen to advance or go back to the previous slide.

In case the lesson videos do not auto-play due to browser security, you can click on the video screen to start playing the videos.

Please complete the quiz and survey located at the end of the course.

For quick help, send a WhatsApp memssage to 08036289672, or a mail to ookelvyn@gmail.com

Page 2 - What's in this course for you?

Before commencing this training, let's establish its purpose. It is plausible that you have prior knowledge of several of the topics that we will discuss. However, since the cybersecurity environment is consistently evolving, we must periodically update our knowledge and continuously enhance our security awareness skills. The goal here is to provide you with the necessary knowledge, attitudes, and skills to recognize and

respond appropriately to phishing attacks. We request that you approach this with an open mindset and utilize this opportunity to refine your strategies that can enhance your overall security.

Page 3 – Exercise 1:

What do you believe to be the root cause of the data breach that led to the exposure of personal information of thousands of customers in a large organization? Make your best guess…

A) An employee of the organization was deceived by a scammer and voluntarily given out the information or clicked on a malicious link.
B) Sophisticated criminal hackers infiltrated the organization's network and absconded with the data.

Page 4 - Introduction to phishing attack

In today's digital age, phishing attacks have become increasingly common and sophisticated. Cyber criminals use a variety of techniques to manipulate people into giving out their personal information, often relying on persuasion principles and social engineering tactics to trick victims. This course is designed to provide you with a comprehensive understanding of the persuasion principles used in phishing attacks and how to identify and protect yourself from such attacks. Through this course, you will gain valuable insights into the psychology of phishing attacks, recognize common red flags, and learn best practices for protecting your personal information online.

Page 5 - Exercise 2

1. What is phishing?

A) A type of physical security B) A type of malware C) A type of social engineering attack D) A type of denial-of-service attack

Page 6 - What is phishing attack?

Phishing attack is a type of cyberattack where an attacker attempts to trick victims into revealing sensitive information such as login credentials, credit card details, or other personal information by posing as a trustworthy entity in electronic communication, such as email, instant messages, or text messages. Phishing attacks often use social engineering techniques to manipulate and persuade victims into divulging their personal information, such as creating a sense of urgency or appealing to their emotions.

In 2017, the man, Evaldas Rimasauskas, was pleaded guilty for scamming google and facebook. Rimasauskas operated by using a company he set up that employed a name similar to Quanta, a reputable provider of data center hardware products. Between 2013 – 2015, he was sending emails that looked like they were sent from quanta to both Google and Facebook, and demanding payment for alleged services and products. According to reports, he is accused of scamming $23 million from Google and $100 million from Facebook. Ref. https://www.zdnet.com/article/lithuanian-man-pleads-guilty-to-scamming-google-and-facebook-out-of-123-million/

Page 7 - Exercise 3

Which type of phishing attack involves the creation of a fake email address that looks similar to a legitimate email of a trusted company, with the goal of tricking users into clicking a malicious link?

A) Spear phishingB) Clone phishing C.) Duplicate phishing D.) Pharming

Page 8 - Examples of phishing attacks

Now that we have a grasp on what a phishing attack entails, let's delve into the different types of phishing attacks.

Page 9 - Deceptive Phishing:

This involves an attacker sending an email or message that appears to be from a legitimate company or organization, often with a sense of urgency, and requesting the user to click on a link or provide sensitive information.

Page 10 - Spear Phishing:

This is a targeted form of phishing where the attacker researches the victim's background and customizes the attack to appear more convincing. The attacker may use personal information, such as the victim's name, job title, or employer, to make the message seem more legitimate.

Page 11 - Clone Phishing:

Clone phishing is a type of phishing attack where an attacker creates a nearly identical copy of a legitimate email, such as from a trusted company or colleague, with the intent of tricking the recipient into clicking on a malicious link or opening a malware-infected attachment. The clone email often looks convincing with similar logos, sender names,

and formatting, but may have slight changes in the content, such as a different sender email address or a sense of urgency to take action.

Page 12 - Smishing:

Smishing is a type of cyberattack that uses text messages (SMS) or messaging apps to trick people into giving out sensitive information or downloading malware onto their device. The term "smishing" is a combination of "SMS" and "phishing".

Page 13 - Vishing:

This is a common type of phishing that uses voice calls to trick the victim into providing sensitive information such as credit card numbers, passwords, or personal identification numbers. The attacker may impersonate a legitimate organization or use social engineering tactics to gain the victim's trust.

Page 14 - Whaling:

This is a form of spear phishing that targets high-profile individuals, such as executives or politicians, and attempts to trick them into divulging sensitive information or transferring money to the attacker.

Page 15 – Exercise 4

What groups of individuals or organizations are targeted by phishing attacks?
Select all the options that may be correct.

a) Individual consumers

b) Small businesses

c) Large corporations

d) Financial institutions (banks, credit unions, etc.)

e) Healthcare organizations

f) All of the above

Page 16 - Common Target of Phishing attacks

Phishing attacks can target anyone who uses digital devices and online services, but some common targets include individuals, small businesses, enterprises, and government organizations. Attackers use a range of tactics, such as impersonation, social engineering, and malware, to trick their victims into divulging sensitive

information or gaining access to systems. It is important to remain vigilant and take appropriate security measures to protect against these attacks.

Page 17 – Exercise 5

1. Prior to now, do you know the seven (7) principles of persuasion?

A) Yes B) No

Page 18 - Exercise 6

2. What is the persuasion principle that describes being influenced by someone due to sharing the same tribal affiliation?

A) Principle of liking B) Principle of tribe C) Principle of unity D) Principle of consensus

Page 19 - Principles of persuasion

Dr. Robert Cialdini, the founder of Influence at Work, is a Regents' Professor Emeritus of Psychology and Marketing at Arizona State University. Throughout his career, he has dedicated himself to researching the factors that lead people to agree to requests and say "Yes". Based on his research he formulated the seven Principles of Persuasion: Reciprocity, Scarcity, Authority, Consistency, Liking, Consensus and Unity. The principle of persuasion is closely related to social engineering, because social engineering tactics often utilize psychological techniques to manipulate their targets into performing actions that are not in their best interest. Let's look into these principles one after the other and see how they work in phishing attacks.

Page 20 - Principle of reciprocity

The concept of reciprocity has been studied extensively in social psychology, and it has been found that people tend to feel a sense of obligation to repay favours or kindness that have been shown to them. For example, if someone shares valuable information with you, you may feel the need to reciprocate by sharing something useful with them in return. Another example is If someone gives you a small gift, you may feel compelled to reciprocate by doing something nice for them in return.

In the context of phishing attacks, attackers may use reciprocity to trick victims into revealing sensitive information or performing an action by offering something in return, such as a free gift or service.

Page 21 - Principle of Scarcity

If news of an impending fuel shortage were to circulate, then fuel stations would be flooded with people buying fuel, even if the news turned out to be false.

The principle of scarcity is of the idea that people are more motivated to act when they perceive a limited availability or scarcity of an opportunity or product. Phishing attackers exploit people's attraction to items that appear rare by imposing deadlines on deals in emails.

In a frequent strategy, an attacker informs individuals that their account will be disabled within 24 hours if they do not click on a link to resolve it. This can pressure the recipient into clicking on a link or giving away their personal information without taking the time to carefully evaluate the legitimacy of the email or its contents.

Page 22 - Principle of Authority

People who are regarded as authoritative and knowledgeable in a particular area are often viewed as more influential, perhaps because credibility and authority are important components of trust. The more we trust someone, the more likely we are to comply with their suggestions. As a result, when we want to make good decisions, we tend to rely on advice given by experts in the field.

The utilization of authority figures to deceive users is a widespread and potent tactic. In some spear phishing campaigns or emails, the malicious actors impersonate the Chief Executive Officer (CEO) and compel the Chief Financial Officer (CFO) to wire money promptly. This technique, when combined with urgency, can create fear in individuals, who may be hesitant to refuse their superior's request.

Page 23 - Principle of consistency

Do you have a friend or colleague who repeatedly asks for small favors, such as financial assistance or other forms of help, and because the requests are not too demanding, you feel obligated to comply with their requests? If such individuals eventually request a more significant favor, you are more likely to grant their request. Fraudsters exploit people's tendency to remain consistent by requesting something minor in an initial email and then gradually escalating their demands in subsequent messages.

One example of the principle of consistency in the context of a phishing attack could be when an attacker sends an initial email asking the victim to fill out a survey. The victim

completes the survey, providing personal information such as their name and email address. Later, the attacker sends a follow-up email posing as a trustworthy organization and asks the victim to enter their credit card information to complete a purchase, citing their previous completion of the survey as evidence of their interest. The victim may be more likely to comply with this request due to the principle of consistency, as they have already taken a small step towards providing personal information.

Page 24 - Principle of Liking

The principle of liking in persuasion suggests that people are more likely to comply with requests from individuals they like or admire. When a friend asks for assistance, it can be challenging to decline, whereas it is more straightforward to reject a request from a stranger. Also, many individuals would go above and beyond to fulfill a request from their loved ones.

But how is liking used in phishing? Here is an example. When an attacker hacks someone's email account, the attacker may use principles of liking by impersonating someone the victim knows and trusts, such as a colleague, friend, or family member. This increases the likelihood that the victim will comply with their request for sensitive information or payment.

Page 25 - Principle of consensus.

The principle of consensus is also known as social proof, and this suggests that people are more likely to take a specific action if they believe many others are already doing it. Which simply means that your actions are determined by the actions of other people. Has there ever been an instance where you decided to attend an event based on the fact that your friends, whom you asked about the event, confirmed their attendance? Or have you ever supported a colleague or a friend because people around you are do so? That's principle of consensus at influence.

An example of the principle of consensus in the context of a phishing attack is when attackers use social engineering tactics to create a sense of urgency in the victim, and suggesting that many other people have already taken advantage of a particular offer or clicked on a certain link.

Page 26 - Principle of unity

Unity is the idea that people are more likely to be persuaded by those who they perceive as being part of the same group or sharing similar characteristics, identity or even tribe. During a study on a college campus, a young woman solicited donations from people in traffic for a good cause. The study revealed that when she added the statement, "I'm a student here too," prior to making the request, the rate of donations increased by 400%. Phishing attackers can use the principle of unity to create a false sense of shared identity with their target. For example, an attacker may send a phishing email to an employee of a company and pretend to be a member of the same department or team, using language and jargon that would be familiar to the employee. This can create a sense of unity and shared identity, making the employee more likely to trust the attacker and follow the instructions in the phishing email, such as clicking on a link or entering login credentials.

Page 27 – Summary of Persuasion principles

- Persuasion principle refers to the principles and techniques used to influence or convince someone to change their attitudes, beliefs, or behaviors towards a particular idea, product, or service.
- Reciprocity: People tend to feel obligated to give back to others who have first given to them.
- Scarcity: People tend to perceive items or opportunities that are scarce as being more valuable, and are more motivated to acquire them.
- Authority: People tend to follow the lead of credible and knowledgeable experts.
- Consistency: People tend to align their actions with their prior commitments and statements.
- Liking: People tend to be more easily persuaded by people they like, admire, or find attractive.
- Consensus: People tend to look to the actions of others in order to determine their own behaviour, especially in uncertain or ambiguous situations.
- Principle of Unity: People are more likely to say yes to someone who they perceive as being similar to them in some way, such as sharing common interests, backgrounds, or identities.

Page 28 - Red Flags to Look Out for in emails.

To protect yourself against phishing attacks, it's essential to be able to identify the red flags on emails. This includes recognizing suspicious sender addresses, links, and attachments, among other indicators. Here are common ones:

Page 29

- Suspicious sender: Check the sender's email address and see if it looks genuine. Sometimes, phishing emails may use an email address that looks similar to a legitimate one but has a small difference. For example , "support@google.com" may become "support@goooogle.com".
- Urgent or threatening language: Phishing emails often contain language that creates a sense of urgency, such as "urgent action required" or threats like "your account will be closed if you don't respond immediately." They may also use scare tactics, such as threatening legal action or account suspension, to pressure the recipient into taking action.
- Grammatical errors: Many phishing emails contain grammatical errors and typos, indicating that they are not from a legitimate source.
- Unfamiliar sender: If you receive an email from an unknown sender, it's important to take a moment to examine the email before responding or taking any action. Check the sender's email address to ensure that it matches the sender's name and any email signatures...
- Suspicious attachments or links: Be wary of links or attachments in emails, especially if they are asking you to provide sensitive information or redirecting you to a different site. It is recommended to hover over any buttons within an email to reveal the URL.
- Requests for personal information: Legitimate companies and organizations rarely ask for personal information via email, so be wary of any request for such information.

Page 30 – Exercise 7

1. Hover on these buttons and type the URL links discovered on them in the textboxes…

   “There will be a few buttons created with html which will reveal URL links”

Page 31 - Exercise 8

2. Which of the buttons have a fake link?

"One of them will have a suspicious looking URL"

Page 32 - Actions to take when you suspect a phishing email.

Here, will outline the actions to take when you suspect a phishing email, helping you stay safe and secure in the digital world.

- Do not click on any links or download any attachments in the email.
- Mark the email as spam or junk to help your email provider better filter such messages in the future.
- Delete the email from your inbox and trash folder.
- If you provided any sensitive information, such as your password or credit card details, immediately change your password and notify your bank or credit card company.
- Consider reporting the phishing attempt to the relevant authorities, such as your company's IT department or the Anti-Phishing Working Group

Page 33 - Wrap-up

I hope this e-learning course on phishing attacks and the principles of persuasion has been informative and helpful to you. By now, you should have a better understanding of the various types of phishing attacks, the strategies cybercriminals use to deceive their targets, and how to protect yourself and your organization from falling victim to these malicious schemes.

Page 34 – Quiz 1

Page 35 – Quiz 2

Page 36 – Quiz 3

Page 37 – Quiz 4

Page 38 – Quiz 5

Page 40 – survey link/End course

Page 41 - exit window

Appendix 2 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Onyeka Kelvin Onyema

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "[Thesis title]" , supervised by [Supervisor's name]
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

15.05.2022

Onyeka Kelvin Onyema

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.