TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Ayooluwa Samuel Ayoola 215124 IVCM

PHISHING CAMPAIGNS AND SECURITY AWARENESS TRAINING IN A SPORT BETTING COMPANY

Master's Thesis

Supervisor: Prof. Olaf Maennel

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Ayooluwa Samuel Ayoola 215124 IVCM

ÕNGITSUSKAMPAANIATE JA TURVATEADLIKKUSE KOOLITUSED SPORDIKIHLVEO ETTEVÕTTES

Magistritöö

Juhendaja: Prof. Olaf Maennel

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: Ayooluwa Samuel Ayoola

May 29, 2023

Abstract

Cyber-attacks cost the world as much billions of dollars every year. Phishing is a type of social engineering cyber-attack that exploits human weaknesses instead of flaws in digital or technical infrastructure. The impacts may include but not limited to financial losses, damage to reputation, loss of customer trust, unemployment, legal repercussions, and reduced productivity due to the need for increased security measures, and the time and resources required to address the aftermath of an attack. Therefore, to mitigate the multifaceted impact of phishing attacks on organizations and their employees as well as stakeholders, there is a need for robust prevention and response strategies. Security awareness training (SAT) has been said to be the prevention and response strategy with the most likelihood of success in averting phishing attacks, as users and employees are the last line of protection against many cyber risks.

This study collected retrospective data over the duration of 15 month from a sport betting company to assess the effectiveness of the security awareness training in reducing the number of employees that would fall victim of phishing, and increasing the number of employees reporting suspicious mail. The study also mapped real phishing email received in the sport betting industry to the MITRE ATT&CK framework for context.

The findings of this study suggests that security awareness training is neither effective in reducing the number of employees that fell victim of phishing, nor increasing the number of employees that report suspicious mail. The study mapped real phishing emails to the ATT&CK framework and concluded that the three email categories of the real phishing activities are all connected to the initial access and reconnaissance tactics of the framework.

This thesis was written in the English language, and there are 57 pages, including 11 figures and 8 tables.

List of Abbreviations and Terms

SAT	Security Awareness Training
MAF	MITRE ATT&CK Framework
PC	Phishing Campaign

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Introduction

The sports betting industry is a competitive multibillion-dollar business sector with a large number of educated and uneducated users. The sensitive nature of all personal and financial data involved in its day-to-day operations, as well as the constant attempts to uncover competitive advantage of competitors make the sector a perpetual target for cyber threats such as phishing attacks [1]. In information and communication technology (ICT), the act of phishing refers to attempts to get sensitive information from an internet user by masquerading as a different person, organization, or government. Such information may a user's name, password, credit card details, or medical records [2].

According to [3], common attack areas include mis-configured servers, software not updated, password reuse, social engineering, remote access services, etc. Phishing is very often used to obtain access to corporate or governmental networks in order to plant malware, download malicious software, transfer assets to individuals who should not have received them, or steal sensitive information [4] [5]. Phishing is a type of social engineering attack because it mostly takes advantage or exploits human weaknesses instead of flaws in digital or technical infrastructure [2][5]. The direct and indirect significant impacts of phishing have been extensively discussed in literature as it affects organizations and their stakeholders [6] [7], employees [8] [9], and organizational operations [10] [11]. These impacts may include but not limited to financial losses, damage to reputation, loss of customer trust, unemployment, legal repercussions, and reduced productivity due to the need for increased security measures, and the time and resources required to address the aftermath of an attack. Therefore, to mitigate the multifaceted impact of phishing attacks on organizations and their employees as well as stakeholders, there is a need for robust prevention and response strategies.

According to the findings of a number of studies, security awareness training (SAT) is the prevention and response strategy with the most likelihood of success in averting phishing attacks, as users and employees are the last line of protection against many cyber risks [12] [13][14] [15]. Security awareness trainings (SATs) on information security is a critical component in securing organisations against threat, and it plays a pivotal role in equipping individuals with knowledge about the existing risks and threats, and how to respond. Consequently, there is a need to access the effectiveness of these training among employees who are the last lines of defense in an organization. Usually, the effectiveness of security awareness training underwent by employees are evaluated through the success rate in failing to fall victim to phishing attacks from phishing campaigns. Phishing campaigns are simulated phishing attacks implemented by an organization's cybersecurity department to evaluate SAT effectiveness. But as much as literature have documented the effectiveness of SATs in reducing susceptibility to phishing attacks, little has been reported on the effectiveness of security awareness training in increasing employee reporting rate of phishing attacks.

As highlighted by [16] in their research, monitoring and quantifying the number of phishing emails accessed by employees within an organization can provide valuable insights into the level of information security. A higher number of accessed phishing emails may indicate a lower level of security and awareness, as security-conscious users are less likely to fall prey to such attacks. Similarly, high reporting rate of phishing activities can help organizations to fortify their security awareness training curriculum to cover emerging threats and technique, by mapping them to the components of MITRE Detection, Denial, and Disruption Framework Empowering Network Defense (MITRE D3FEND). These emerging threats may be globally emerging threats or threats already existing in the cybersecurity framework but new to the organization. Additionally, phishing attacks are a type of coordinated cyber-attack as outlined in the MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) framework for understanding and categorizing all cyber-attacks. However, there is a dearth of evidence to show how real phishing activities relates to the component of the MITRE ATT&CK framework.

Therefore, the main purpose of this study is to evaluate the effectiveness of security awareness training in reducing susceptibility to phishing attacks, and increasing employee reporting rate of phishing activities. This study will further analyze the real reported phishing emails in a sport betting company over the study duration and map the real phishing emails to the MITRE ATT&CK framework and technique.

1.2 Rationale of the study

According to [17], Google records about 17 million phishing emails on a monthly basis and most of them involve people utilizing false identities. This depicts the volume of cyber-attacks that organizations may experience in a month depending on its size and value. Frequent success of these cyber-attacks can result in poor outcomes for any high value industry. The financial worth of the sports betting industry and the vast number of users who share sensitive information on the platforms during registration demand continuous effort in protecting their organizations, stakeholders, employees, and customers.

But the continuity of this protection cannot be guaranteed if the effectiveness of the methods is not tested, or the ever-changing dynamics of the attacks is missed. Hence, to continuously expose the different crafts, tactics, and techniques used by attackers to deceive employees to phishing sites, and to improve the compliance of employees with the guidance provided during security awareness training, this study is necessary. Furthermore, there are also new start-ups in the industry that need information from available evidences that can be used in formulating their standard operating procedures and protect them from cyber-attacks. This type of study provides such evidence that can protect newbies from falling prey to attacks.

Also, the growing competition in the industry means that companies often strive to keep their operations and strategies secret from competitors, and this increases the number of possible attacks targeted at each organization. However, this study provides evidences that can be harnessed as a competitive advantage by any company.

1.3 Research Questions

To help achieve the overall purpose of this study, the following research questions were identified.

RQ 1: How effective are the security awareness training in reducing the percentage of clickers during phishing campaigns?

RQ 2: Were there repeat clickers during subsequent phishing campaigns after the first?

RQ 3: What percentage of phishing activities of the phishing campaigns were reported by employees?

RQ 4: What percentage of the reported phishing activities were real threats?

RQ 5: How do the reported real phishing emails relate to the MITRE ATT&CK framework and technique?

1.4 Novelty of the study

The MITRE ATT&CK framework is generic for all cyber-attacks, with very little evidence to show where phishing activities belong in the framework. This study extracts the real phishing emails reported by employees of a sport betting company over the period of a year and maps them to the MITRE ATT&CK framework tactics and techniques.

Secondly, the security awareness trainings conducted by members of the cybersecurity team of the sport betting company would be evaluated to know if it has any effect on employee reporting rate of phishing activities. This is not a commonly reported activity as against measuring the effectiveness of SAT in reducing susceptibility to phishing attacks.

Lastly, studies about phishing in sports betting industries have rarely been conducted, and by analyzing the connection between the reported incidents and the framework, this study will provide a distinctive contribution to the field of cybersecurity.

1.5 Scope

The scope of this thesis is limited to one sports betting company in Europe. The phishing activities are limited to the emails reported as suspicious by employees and those confirmed by the security team to be real phishing emails, while the cybersecurity awareness training and phishing campaigns to be considered will only cover those conducted within the duration of a year.

2. Literature Review

2.1 Introduction

The increasing number of phishing campaigns targeting organizations and the continuous rise in the number of attacks reported by various researchers and organizations have made "phishing attacks" one of the most recognized terms in the field of cybercrime[18]. Phishing attacks involve the use of fraudulent emails and websites to deceive people into disclosing confidential data, such as login credentials or financial information. These kinds of cyber-attacks can result into serious consequences such as financial or reputation harm for both individuals and organizations[2]. To address this growing threat, it is crucial for organizations to take steps that mitigate the risks.

According to [19], user security education and training is crucial for organizations to strengthen their overall security posture. As a result, one effective approach is the implementation of security awareness training programs for employees. These awareness programs should be aimed at providing cyber security education about the dangers of phishing, alongside the necessary skills and knowledge to recognize and respond to such phishing attacks. Consequently, studies have been conducted to assess the effectiveness of phishing training in improving employees' level of information security awareness. This type of training involves sending out simulated phishing emails to educate end-users on how to avoid falling for actual phishing attacks. The work of [20] compared the outcomes of a simulated phishing exercise before and after employees received information security awareness training, and found that the percentage of employees who clicked on phishing URLs decreased from 31% to 12% after the training, while the proportion of employees affected by phishing decreased from 24% to 4%.

As much as organisations are now trying to provide security awareness training to employees, studies have indicated that conventional phishing training programs and tools are not very effective against targeted social engineering attacks. To address this problem, [21] propose a toolkit for implementing tailored, large-scale phishing campaigns to train employees within an organization. The toolkit includes customizable email templates that can be personalized with detailed target information and a semi-automated process for selecting a phishing domain name. The result provided a more effective approach to training against tailored social engineering attacks by enhancing the credibility of phishing emails.

A MITRE ATT&CK framework exists for understanding and categorizing all cyber-attacks, and the framework is a database that provides knowledge on security threats by analyzing how attackers infiltrate and propagate through computer systems, with a focus on the data obtained from real breaches. The framework categorizes cyber adversary behavior into tactics, techniques, and procedures (TTPs), which are not limited by any specific order [22]. However, little is known about how phishing mails relate to the MITRE attack framework..

2.1.1 Purpose of the literature review

Email is a widely used communication channel for both business and personal purposes. But it is increasingly being exploited by malicious actors for phishing attacks. To address this growing threat, many organizations have introduced anti-phishing training programs for their employees. However, there is a need for continuous improvement in the design of sustainable and effective trainings to protect employees from phishing attacks [23].

Therefore, the purpose of this literature review is to evaluate the impact of phishing campaigns and security awareness trainings in organizations and investigate the relationship between phishing mails and the MITRE attack framework, in order to offer insights into how organizations can better protect themselves against phishing attacks. More specifically, this literature review seeks to answer questions such as:

1. What are the current trends and practices in phishing campaigns and security awareness trainings in organizations?
2. What are the factors that influence the effectiveness of security awareness trainings in mitigating the impact of phishing attacks?
3. How do phishing mails relate to the MITRE attack framework, and what implications does this have for organizations?

2.2 Phishing

Phishing is a widely discussed topic in science journals, newspapers, and among organizations such as banks and law enforcement agencies, with various definitions proposed by different scholars [24]. A phishing attack is one of the most serious threats for any organization [25]. Understanding the definition and history of phishing is important in developing effective security awareness trainings and measures to protect against phishing attacks. The term "phishing" emerged in the mid-1990s, as a result of scammers using email as a bait to trick people into disclosing their sensitive information such as usernames and passwords. The term was created from the analogy of the act of fishing, and is thought to have originated from "phreaking". Specifically, in 1996, criminals began "phishing" passwords from American Online (AOL) users to gain unauthorized access to their accounts [24] [26].

According to PhishTank, phishing is a fraudulent attempt, often via email, to illicitly obtain personal information [27]. Similarly, [28] describes phishing as a term referring to a criminal activity where a person sends a fake email to random people with the aim of obtaining personal information. And [29] also define phishing as a social engineering method that manipulates people into providing sensitive information or gaining unauthorized access to a system. However, while these definitions are applicable to many phishing attacks, they may not necessarily cover all scenarios, as phishing attacks can involve other motives beyond personal data theft [24].

Phishing can be further explained using the step-by-step methods below [2]:

1. The attacker drafts and sends an email to the potential victim.
2. The potential victim clicks and is redirected to the phishing site.
3. The potential victim enters sensitive information on the phishing site.
4. The attacker harvests the victim's credentials from the phishing site.
5. The attacker uses the harvested victim's credentials for personal use.

2.2.1 Tactics and techniques used in phishing attacks

Different tactics and techniques have been developed for carrying out phishing attacks, and these techniques can be described as follows:

1. **Email spoofing:** This tactic is a type of phishing technique in which fake emails are made to look like they originate from trusted senders, with the intention of convincing recipients to trust the message and comply with its instructions.
2. **Web scooping:** this technique involves creating a fake website that closely resembles a legitimate website, thereby, tricking victims into thinking it's genuine and prompting them to enter their personal information.
3. **Malware installation:** this technique uses programmed contents (software, code, script, etc.) to disrupt computer operations and extract sensitive data. Malware encompasses various types of malicious software such as viruses, worms, trojan horses, keyloggers, spyware, and adware. While client security products are capable of detecting and removing malware, phishers can employ techniques to make their malware undetectable [30].

2.2.2 Prevalence and Impact of Phishing Attacks

Phishing attacks have become a pervasive threat in the digital landscape, with significant implications for individuals, organizations, and society at large. Numerous studies have examined the prevalence and impact of phishing attacks, shedding light on the scope, scale, and consequences of this type of cybercrime. With as much as 5.6% of organization's IT budget been spent on cybersecurity and IT risks, the IBM security report as highlighted by [31] recorded that a cyber-attack cost an average of $3.3 million, while [32] reported that the cost of cyber-attacks in 2020 alone ran into billions of dollars. According to [27], phishing attacks are increasingly prevalent and are becoming more sophisticated and frequent over time. One valid evidence is Google recording as much as 17 million phishing emails monthly [17]. The work of [33] noted that phishing attacks are also widely recognized as a more prevalent method of identity theft compared to other techniques, such as hacking, physical data retrieval, shoulder surfing, insider threats, and malicious software installation. However, the study further explained that the attack can only occur when a number of variables come together. These factors are: the interest of a phisher, and a rewarding target whose security system is not effective. Susceptibility to phishing attack is higher for individuals who engage in frequent routine activities involving computer use and online banking. Another study observed the psychological anchoring effect in phishing attacks, and with only a quarter of the participants achieving a detection score above 75%, it can be concluded that many individuals are still at risk of falling victim to phishing attacks [34].

The impact of phishing attacks extends beyond financial losses to include reputational damage, loss of trust, legal and regulatory implications, and psychological distress for victims. Several research have examined the financial costs of phishing attacks to organizations, the consequences of data breaches resulting from successful phishing attacks, and the challenges of recovering from a phishing attack. One study [35] conducted an assessment of the severity of phishing attacks by evaluating their risk levels and the potential impact on the market value of targeted organization. The study analyzed a dataset of 1,030 phishing alerts from a public database, along with financial data associated with the targeted firms, and discovered a number of variables that associates with the severity of attack. The approach utilized a hybrid method that combined text phrase extraction and supervised classification, resulting in a prediction accuracy of up to 89% for severity of the attacks.

2.3 Security Awareness Training

Phishing tactics have continued to evolve, and businesses need to consider effective strategies to protect themselves against potential threats as suggested by [36]. The work of [36] further explained that employees play a crucial role as an important line of defense in cybersecurity and mitigating their vulnerability to attacks is of utmost importance. This necessitates comprehensive education and security awareness training efforts. In a bit to control the prevailing attacks, [37] outline various features that can be employed to differentiate between phishing URLs and legitimate ones. The features were used in the development of an effective and accurate logistic regression filter which quantifies the prevalence of phishing attacks on the internet with high precision.

2.3.1 Definition and objectives of security awareness training

Awareness programmes on information security is a critical component in securing organisations against threat. In the realm of information security, awareness plays a pivotal role as it involves equipping individuals with knowledge about the existing risks and threats. According to the findings of a number of studies, awareness training has the highest likelihood to avert phishing attacks [12] [14] [13] [15].

While awareness is a fundamental requirement, training is what sets the stage for effectively safeguarding an organization or individual's sensitive information. Without proper guidance, it is unrealistic to expect individuals to naturally grasp these risks and respond to them appropriately. Training aims to impart skills for specific functions such as identifying phishing mails, while awareness serves to draw attention to such specific issues [38]. As highlighted by [16] in their research, monitoring the number of phishing emails accessed by employees within an organization can provide valuable insights into the level of information security awareness. A higher number of accessed phishing emails may indicate a lower level of awareness.

According to [39], security awareness training is a proactive approach employed by IT and security experts to mitigate user risk and prevent information security breaches. They further describe that such programs are specifically designed to educate users and employees about their role in safeguarding against security threats. [40] recommends that when developing a comprehensive security awareness training program, companies should highlight to employees the importance of safeguarding the organization. This should include providing an overview of corporate policies and procedures that outline secure work practices and the appropriate channels to report potential threats. In addition, by providing training on cyber hygiene, identifying security risks associated with actions, and recognizing potential cyber-attacks through email and the web, effective security awareness programs empower employees with the knowledge and skills needed to contribute to the overall security posture of the organization [39].

Proactively implementing security awareness involves educating end users and employees on how to safeguard personal and organizational information through the application of information security best practices [38]. The overarching objectives of cybersecurity awareness training are multi-faceted and encompass several key purposes. It is imperative to understand the specific purposes of security training in order to appreciate its significance. The primary benefits and objectives of security awareness training is to empower employees as a First Line of defense and to prevents social engineering attacks [31]. An effective security awareness training program must take into account the business objectives and mission of the organization and ensure that these goals are met as safely and securely as possible, because reinforcing these objectives will make the program more acceptable to the employee base [41].

Marlies and Genserik [42] analyzed the impact of training sessions amongst 170 staff members of a Belgian university in 2018 with the training focusing on terrorism, reporting of incidents, and university staff responsibilities. The method implemented was sharing questionnaires before and 2 weeks after the training. The result of the study showed that the employees' level of security knowledge as well as their attitudes towards security improved as a direct result of the training session as 83.6% were more aware and 85% had a better understanding of the methods used for reporting radicalization inside the organization.

2.3.2 Importance of security awareness training in organizations

In today's ever-evolving cybersecurity landscape, organizations face relentless threats from cyber-attacks that can result in severe consequences, including data breaches, financial losses, and reputational damage. To effectively combat these risks, security awareness training for employees is of paramount importance. User education is recognized as a crucial and commonly employed strategy in combating phishing attacks. Numerous organizations have implemented awareness campaigns to educate users about the concept of phishing attacks, how to detect them, and how to prevent falling victim to them [43]. Studies have shown that human errors account for 95% of incidents, underscoring the importance and need of prioritizing information protection as a critical organizational objective [31] [32]. Developing awareness programs for most people will prevent these types of attacks. [44] in their paper describes how promoting awareness of AI-based cybersecurity can potentially lead to a decrease in phishing attacks by highlighting the effectiveness of AI-based cybersecurity awareness training and its potential impact on cyber-attacks.

2.3.3 Types of security awareness training programs

According to [45], traditional security awareness training can be delivered in one of the following three ways:

1. **Classroom-based training program:** This type of training is one which attendee are temporarily removed from their regular duties for a few hours, during which an instructor guides them through the intricacies of a security topic such as phishing, malware, or social engineering attacks. This approach allows employees to actively participate and receive detailed instruction from an experienced instructor, providing them with valuable insights into these security threats and how to effectively address them. It is best preferred for its interactive nature which promote a culture of security [45].
2. **Visual aids (including video):** These are informative tools that utilize visual elements to convey concise security advice. These aids, often in the form of posters, handouts, or videos, cover various topics such as secure passwords, phishing scams, password security, and the risks associated with public Wi-Fi. They provide bite-sized information that is easy to understand and serve as a visual reminder to employees about important security practices [45].
3. **Simulated attacks:** These are also known as cybersecurity awareness simulations, and are mock attacks that are conducted to test how individuals respond to threats in real-world scenarios. These trainings often involve simulated phishing emails, phishing text messages, or other deceptive tactics, such as fake text messages or USB sticks labeled with enticing titles. The goal of these simulations is to replicate the tactics used by malicious actors and assess the level of awareness and preparedness of individuals in identifying and handling potential cyber threats [45].

2.3.4 Factors that affect the effectiveness of security awareness training

Studies have shown that security awareness training can be an effective tool in reducing the risks associated with phishing attacks based on the MITRE ATT&CK framework [46]. For example, a study conducted by [47] explore the potential of MITRE ATT&CK framework in security assessment and defensive design. The study proposed a cyber-security culture framework that incorporates various applications, including the organization of security procedures and the provision of information to employees about security risks and threats to enhance security awareness. Security training should be taken into account as a non-technical solution that can supplement the efficiency of anti-phishing technical tools [16]. However, as much as security awareness training appears to be a common strategy for organizational security governance, the work of [48] has shown that only few organizations claimed that their security awareness training programs are effective. One possible reason for this is the lack of a systematic understanding of the nature of the programs, how they impact employees' security-related beliefs and behavioral intentions, and the conditions that influence such a relationship. The development is supported by the conclusion of [46] that the effectiveness of security awareness training in preventing phishing attacks varies depending on several factors, including the training materials and method, the frequency of training, and the level of employee engagement.

Similarly, [49] highlighted ways to make security awareness trainings effective and it include top-down awareness, thoroughness, frequency, and variation of training methods. In top-down awareness, just like any other aspect of an organization's culture, the importance of security awareness is set by the leadership, including the CEO, President, or Director. When top-level executives demonstrate a strong attitude towards cybersecurity as a critical element of the company's success, employees take notice. However, it's not just about attitude, but also about providing training to these executives, just like any other employee in the organization. For instance, "whaling" is a type of spear-phishing that specifically targets c-level employees with the aim of gaining access to sensitive data. This form of phishing poses the highest level of threat and requires adequate attention in security awareness training programs. Thorough security awareness training is very crucial for new employees during onboarding and for all staff members through annual re-training. Cybercriminals are always changing tactics, however, staying updated with evolving cyber threats and incorporating them into thorough training sessions for employees is essential for effective risk mitigation.

According to CEO of KnowBe4, Stu Sjouwerman regular security awareness training, conducted at least once a quarter, results in a significant decrease in risk, with further drops in risk observed when training and simulated phishing tests are conducted monthly [50]. This refresher training does not need to be as comprehensive as initial onboarding and annual training, but rather serves as reminders of best practices. Supplementing training with periodic cybersecurity awareness emails, handouts, posters, and simulated phishing tests can provide insights into the organization's overall awareness level, allowing for adjustments in training to enhance effectiveness. Finally, individuals have diverse learning preferences, with some employees preferring videos, others preferring reading, and some benefiting from interactive classes or gamified training. It is important to recognize that what may be effective for one employee may not work for another. As a result, it is recommended to mix up the training methods to accommodate different learning styles and keep the training engaging and interesting for everyone.

2.3.5 Challenges and limitations of security awareness training

Despite the provision of security awareness training by many organizations to their employees, there are still numerous obstacles and limitations that can leave institutions susceptible to security threats like phishing attacks. These challenges may encompass the rapid obsolescence of security content, low employee participation, waning interest and retention of training material, administrative burdens associated with security programs, and a compliance-centric focus rather than emphasizing actual results [51].

2.4 Repeat Clickers In Organizations

Most of the challenges and limitation of security awareness training can lead to inefficiency in term of repeat clicks. The definition adopted for a repeat clicker in this study is an employee who falls victim of phishing attacks in two consecutive phishing campaigns, even after participating in a security awareness training in-between those phishing campaigns. Ronald et.al [19] conducted research that studies how organizations treat repeat clickers during simulated phishing campaigns, a thematic analysis approach was used to analyze responses to 3 open-ended questions - *"Your organisation discovers that an employee is repeatedly clicking on simulated phishing emails. What would your company currently do (if anything) and why?”*. The responses were gathered from data collected from 45 participants via Qualtrics which was used to select security awareness professionals. The result of this research showed that 36% identified tailored trainings to individuals as a fix. The result also concluded that a combination of strategies, including the use of positive incentives (also known as "carrots") and negative consequences (sometimes known as "sticks"), may be required to successfully promote long-term behavior change.

According to the research by [52] which employs a mixed-methods design, employees repeatedly clicked on phishing sites despite attending security awareness training, because of job pressure, curiosity, lack of expertise, and limited cybersecurity resources. The study proposes that hospitals provide regular and extensive cybersecurity training to personnel, establish a clear system for reporting and addressing phishing attempts, and invest in technical solutions to limit phishing risks. The limitation of this study also relied in the specific context of hospital settings which may limit the generalizability of the findings.

2.5 MITRE ATT&CK Framework

2.5.1 Overview and history of the MITRE ATT&CK Framework

In 2013, the MITRE ATT&CK framework was initiated as an attempt to use all previous cyber-attack tactics, techniques, and procedures (TTPs) that have been targeted at Microsoft Windows systems to categorize all categorize cyber-attacks [47]. So, MITRE ATT&CK is a body of knowledge for all cyber adversaries based on past and present real-world observations. The framework has been used in the development of software and processes because it has both research and industrial acceptance. The objective of MITRE ATT&CK is to serve as a baseline to develop adaptive models and methodologies for various identified threats [53]. The framework is a comprehensive tool intended for cybersecurity professionals at all levels within an organization, ranging from analysts to executives. It provides valuable insights for making informed decisions on detection, prevention, and response strategies. Moreover, the framework can be utilized to benchmark an organization's security posture against specific adversaries, assess the effectiveness of security controls, and identify potential gaps in defenses [54]. The MITRE ATT&CK framework is based on observations from the real world, and corporate sectors, government, and the cybersecurity product and service industry all use this body of knowledge as a springboard for the creation of targeted threat protection models and techniques [55].

2.5.2 Components and elements of the framework

The MITRE ATTACK framework consists of three core components [56], and a dynamic one:

1. **Tactics:** The actions used by an adversary to accomplish their objectives. It practically addresses the "why" [55] [57]. Tactics are contextual categories that encompass individual techniques and provide standardized, higher-level notations for actions carried out by adversaries during an attack, such as data exfiltration, privilege escalation, and defense evasion [58].
2. **Techniques:** The specific methods or tools employed by an adversary to execute a tactic. In other words, they address the "how" and, in some cases, the "what" an adversary gains by performing an action [58]. Techniques may be divers in one tactic category [57].These are usually single steps in a process and they have unique identifiers (ID). For example T1566 for phishing and T1110 for Bruteforce. There may also be sub-techniques showing specificity in how adversaries use techniques [55] [58].

3. **Sub-techniques / Procedures:** The detailed steps taken by an adversary to carry out a technique [38]. They are being used to describe in-the-wild use of techniques or sub-techniques while exhibiting several additional behaviors in the way they are performed [59]. e.g spear phishing link as a subtechnique has the ID T1566.002 which falls under the tactic phishing with the ID T1566. [55]
4. **Mitigation:** This involves defining countermeasures that can thwart adversaries from achieving their tactical objectives by utilizing specific techniques. Mitigations are ever changing and they provide guidance on "what to do" in response to Tactics, Techniques, and Procedures (TTPs) used by adversaries [60].

To tackle security concerns in enterprise systems, [55] suggests a proactive approach by introducing a threat modeling language based on the MITRE ATT&CK Matrix. The language described organization's defenses, system assets, attack steps, and asset associations. The understanding of the relationship between phishing emails and the MITRE ATT&CK framework created by the language can help organizations develop effective defense strategies. For example - the following can be gotten from the framework [55]

2.5.3 Use of the framework in cybersecurity threat analysis and response

The use of the MITRE ATT&CK framework can provide numerous benefits for organizations. Such benefits as highlighted by [56] are processes including adversary emulation, red teaming, behavioral analytics development, defensive gap assessment, security operation center (SOC) maturity assessment, and cyber threat intelligence enrichment. Adversary emulation is a process where the security of an organization is evaluated by utilizing knowledge about the tactics used by potential attackers to simulate a threat. The MITRE ATT&CK framework is employed to design scenarios that imitate the behavior of adversaries and assess the effectiveness of defense mechanisms. Red teaming is the use of the ATT&CK framework to simulate an attacker to illustrate the consequences of a security breach.

It helps to formulate red team strategies and coordinate actions. Behavioral analytics development is the process of using the ATT&CK framework to simplify, organize, and associate patterns of suspicious activity deemed malicious, for monitoring of attacker's activities. Defensive gap assessment involves using the MITRE ATT&CK framework to evaluate the adequacy of defenses and visibility across an organization. This includes assessing existing security tools and testing new ones to identify potential gaps, thereby, helping to prioritize investments in security.

Similarly, SOC maturity assessment evaluates the efficiency of a security operations center (SOC) in terms of identifying, analyzing, and responding to security breaches using the ATT&CK framework. Finally, the cyber threat intelligence enrichment is a process to evaluate an organization's capability to protect against various Advanced Persistent Threats (APT) and patterns of activity shared by multiple threat actors, in order to improve knowledge about threats and the actors.

2.5.4 Relationship Between Phishing and the MITRE ATT&CK Framework

Knowing about various kinds of cyber-attacks and their attack vectors is an essential ingredient for prevention [31]. The understanding of the core of the MITRE-ATT&CK sequence provides an opportunity to anticipate a phisher's next move and intercept it. [61] utilized MITRE ATT&CK framework and analyzed tactics, techniques, and procedures (TTPs) employed in different phishing campaigns. They proposed a framework that offers significant contributions to assist organizations in effectively mitigating the malicious threats of phishing.

The MITRE ATT&CK framework provides a useful tool for understanding how phishing attacks fit into the overall cyber-attack landscape. With phishing emails classified as a type of social engineering attack in the framework, specifically under the initial access tactics, the framework is of valuable importance in addressing phishing.

Youngsup et al. [61] conducted an extensive analysis of the phishing campaigns carried out by three country-based threat groups - Kimsuky, Lazarus group and APT37. Part of what was analyzed was the phishing campaigns performed by these APT groups to know the critical tactics. The methodology used for the research was using a similarity analysis approach to gather incidents in the form of reports, extract certain information such as victims, IoCs and time duration from these incidents and extract the TTPs of these campaigns. It was concluded that most of these phishing campaigns make use of TA0007 (Discovery) tactic, while tactic TA0008 (Lateral movement) was not used by the Kimsuky group, they used TA0003 (persistence) and TA0006(credential access) tactics. The study mapped group activities but not the real phishing email gotten at the target side of industries.

To tackle security concerns in enterprise systems, [55] when further and suggested a proactive approach by introducing a threat modeling language based on the MITRE ATT&CK Matrix. The language described organization's defenses, system assets, attack steps, and asset associations. The understanding of the relationship between phishing emails and the MITRE ATT&CK framework created by the language can help organizations develop effective defense strategies. Table 1 shows some part of the mapping extracted from [55]. However, the work did not map real industry phishing activities to the MITRE framework as proposed by this current study.

Excerpts from the MITRE ATT&CK Framework			
S/N	**Tactic**	**Technique [Tactic ID]**	**Sub-techniques**
1	Reconnaissance	Gather Victim Identity Information [T1589]	T1589.001, T1589.002, T1589.003
2	Reconnaissance	Phishing for Information [T1598]	T1598.001,T1598.002, T1598.003
3	Initial Access	Phishing [T1566]	T1566.001, T1566.002,T1566.003
4	Credential Access	Adversary-in-the-Middle [T1557]	T1557.001,T1557.002,T1557.003

Table 1. Mitre Att&ck Tactics & Technique Example

2.5.5 Limitations and criticisms of the framework

The basic problem of ATT&CK is that hierarchical structures are missing or inconsistent. The techniques lack linearity, grouping or hierarchy [62]. This means that there is no exclusivity in the use of techniques, and one can oftentimes be used in different tactics and in different phases of an attack. More so, the identifiers are not traceable for both tactics and techniques.

There is also the limitation of false positives where some behaviours registered as attacks are not malicious. Example of such is documented in [63] where a normal file deletion cannot be differentiated from an attacker's action.

2.6 Summary and Gaps in the Literature

2.6.1 Recap of the key findings and insights from the literature review

The literature review delves into the impact of phishing campaigns and security awareness trainings in organizations, with little or no information on how phishing mails relate to the MITRE ATT&CK framework. The key findings and insights from the literature review shed light on the significance of phishing campaigns as a prevalent and persistent cybersecurity threat that can lead to devastating consequences for organizations. The review identifies various tactics and techniques employed in phishing campaigns, such as spear phishing, whaling, and social engineering, and their potential impacts on organizational security. Additionally, the review highlights the importance of security awareness trainings in mitigating the risks posed by phishing campaigns by educating employees on how to recognize and respond to phishing attempts.

2.6.2 Identification of gaps and limitations in the literature

The literature review has identified several gaps and limitations in the existing research study. Firstly, while there have been studied that have evaluated the effectiveness of security awareness training in reducing susceptibility of organizations' employees to phishing attacks, the effectiveness of security awareness training has been rarely discussed as it relates to increasing employee reporting rate of phishing activities.

Secondly, the literature review indicates that there is limited research on the alignment of phishing mails with the MITRE ATT&CK framework. While the MITRE ATT&CK framework is widely used in cybersecurity, there is limited literature that specifically examines how phishing activities align with the various stages of the framework. This gap underscores the need for additional research to better understand the relationship between phishing mails and the MITRE ATT&CK framework, and how this alignment can inform strategies for detecting and responding to phishing attacks.

Lastly, there are millions of people all around the world who take part in various sports betting activities, making the sector of sports betting a market that is expanding at a rapid rate. However, despite the magnitude and significance of the sector, study of phishing activities in the sport betting industry is scarce.

3. Methodology

3.1 Introduction

This chapter discusses the research methodology of this thesis. The methodology outlines the approach, design, and procedures used to investigate the impact of phishing campaigns and security awareness trainings in organizations, as well as the alignment of phishing mails with the MITRE attack framework. This chapter details how the gaps and limitations identified in the literature review will be addressed. The data collection method explaining how the data was gathered and analyzed through descriptive quantitative comparison. The chapter is concluded by highlighting the ethics and limitations of this study.

3.2 Research Design and Study Population

The research employs a retrospective study design which uses data from a previous year to answer the research questions as much as the data permits. The study duration was fifteen months (February 2022 - April 2023), and it was conducted among the employees of a sport betting company based in Europe. The company was established within the last decade and has a staff capacity between 300 and 500.

The company has an in-house cybersecurity team which was assembled over 2 years ago. The cybersecurity team secures the cyber space of the company and conducts cybersecurity awareness trainings to her employees. The team also runs phishing campaigns to track the effectiveness of the security awareness training. Data from security awareness training and phishing campaigns are stored on database ‘X’.

3.3 Data Collection and Analysis

Data was extracted from database ‘X’ used to store information from the different security awareness training conducted and the phishing campaigns ran over the study period (February 2022 to April 2023). The data was disaggregated by the month when the security awareness training was conducted and when the phishing campaigns were implemented. Information on real phishing incidents (external phishing emails) was also collected from the emails reported to members of the security team by employees of the sport betting company in the same period. Descriptive analysis was done to compare a number of variables from the extracted data, while real phishing emails were mapped to the MITRE

ATT&CK framework using technical similarity index. The components of the security awareness training were also mapped with MITRE D3FEND to show the frameworks counters the ATT&CK.

To answer RQ 1 which queries how effective the security awareness training were in reducing the percentage of clickers during phishing campaigns, a quantitative analysis of training information obtained from the database ‘X’ was done and the percentages of clickers in successive training were descriptively compared for increased or reduced.

To answer RQ 2 which queries if there were repeat clickers during subsequent phishing campaigns after the first, clickers in the first, second, and third phishing campaigns were used to identify repeat clickers in the second, third and fourth phishing campaigns respectively.

To answer RQ 3 which queries the percentage of phishing activities of the phishing campaigns reported by employees, the total number of phishing mails and the reported mails in each campaign were analyzed and described for all the phishing campaigns.

To answer RQ 4 which queries the percentage of RQ 3 that were real threats, the percentage of real threats confirmed and recorded by the cybersecurity team was calculated from the reported suspicious emails.

To answer RQ 5 which seeks to establish how the component of RQ 4 relates to the MITRE ATT&CK framework and technique, all real phishing emails confirmed by the cybersecurity team were analyzed to determine the attackers’ approaches. The approaches were first specifically grouped into procedures or sub-techniques, then further grouped into techniques, and finally into tactics of the MITRE ATT&CK framework.

3.4 Ethical Consideration

This study is compliant with popular ethical principles of confidentiality, informed consent, beneficence, and non-maleficence. Confidentiality was maintained as the name of the sporting betting company, the country of operation, and the name of the database was withheld or anonymized. Informed consent is crucial to the development of morally sound studies [16][17], so this study sort consent from the head of the security team of the sport betting company before the commencement of the research. Finally, the nature of this study guarantees that it will bring no harm to the participants or the company, and findings from this study serves to benefit the sport betting industry.

4. Results

4.1 Introduction

This section highlights the results of the study by analyzing the outcome of all security awareness trainings, all phishing campaigns and the emails reported to the security team. These findings are used for further discussions as they relate to existing literature.

4.2 Security Awareness Trainings

Four security awareness training was conducted for all available staff members within the study period. As shown in tables 2, the content of the first training was structured to discuss the company's security policies, and the content of the subsequent ones varied from time to time depending on the outcome of the previous phishing campaigns. The first training which started on the 6th of February 2022 and lasted for 2 weeks, had 387 staff enrollees and approximately 99% completion rate.

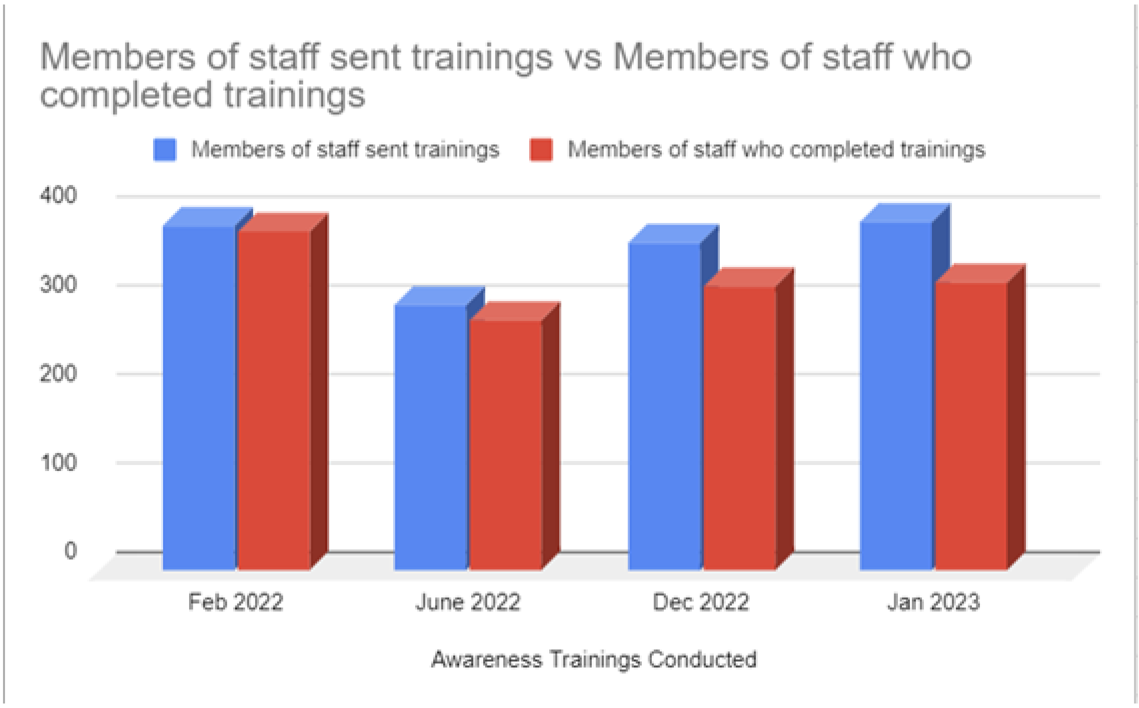


Figure 1. Enrollment and completion rates for all security awareness training

The second training rolled out on the 1st of June 2022 and also lasted two weeks, with 298 enrollees and about 95% completion rate. The third training opened from the 7th of November 2022 till 2nd of December, 2022. The training had 369 members of staff enrolled and about 80% completion rate. The final security awareness training consisted of 2 sub-trainings and an assessment afterwards. The training commenced from the 6th of January till 27th of March, 2023, with a total of 393 enrollees and 82% completion rate. Each security awareness training had a set of notifications and reminders prompting enrollees at successful enrolment, five days after enrolment for enrollees who have not started the training, every three days after, three days to the end of the training for those who have not completed the training, on the last day of the training for managers, and a completion notification to all those who complete the training.

S/N	**Training Month**	**Training Title**	**Training Content**
1	February 2022	Security Policies Summary	Reporting an incident - different steps and contacts
			Acceptable Use policies
			Account and password policies - related to different platforms.
			Policies on remote working - maintaining security while working from home.
2	June 2022	Taking Security Home: Working Remotely	Organizational policies still apply even when working from home.
			Think before you click; separating work and personal data.
			Securing home networks.
			Not forgetting physical security
		Your Role: Internet Security and You - version 1	Facts about cyberattacks
			Different strategies and examples of social engineering.
			Phishing, Smishing and different examples related to these attacks.
3	November -December 2022	Security Awareness Training	Social Engineering Red Flags
			Recognizing that cybercrime is very prevalent, and that every employee is a target.
			Developing a greater awareness of social engineers, social engineering and warning signs that point to a phishing attack.
			Demonstrating security awareness skills through choosing actions that minimize the risks from cyberthreats.

Table 2. Training months and curriculum/content 1/2

S/N	Training Month	Training Title	Training Content
4	January - March 2023	Your Role: Internet Security and You - version 2	Understanding that individual actions directly impact the organization's safety i.e. clicking on a malicious link in email might have consequences on the organization at large.
			Able to identify the most common types of red flags when browsing and in emails - cybercriminals use information from social media accounts to know about employees.
			Be able to use the achieved knowledge to protect the organization and personal life.
		Safe browsing	Sources of risk e.g. public hotspots, shoulder surfers, fake URLs etc.
			Best practices of data download and information sharing.

Table 3. Training months and curriculum/content 2/2

4.3 Phishing Campaigns

Similar to the number of security awareness training, four phishing campaigns were conducted in the study period. In the first phishing campaign conducted in March 2022, 300 phishing emails were sent to employees and 290 were delivered. Of the 290 emails delivered, 80% were opened and only 19% were reported as suspected phishing or suspicious activities, while 12% of those who opened the emails fell victim by clicking on the phishing links. The second phishing campaign conducted July 2022 sent out 334 emails and 273 were delivered.

Phishing Campaigns				
Metric	**First Campaign**	**Second Campaign**	**Third Campaign**	**Fourth Campaign**
Total Number of mails sent out	300	334	367	388
Number of mails delivered	290	273	336	316
Number of mail opened	233	231	272	60
Number of mails reported	55	33	39	7
Number of Clickers	28	29	37	40

Table 4. Summary of the phishing campaign activities

Of those delivered, about 85% were opened and only 12% were reported as suspicious, while approximately 13% of those who opened the email clicked the phishing link. For the third phishing campaign conducted in December 2022, the total number of emails sent were 367, and 336 got delivered. Employees opened 81% of the emails delivered and reported only about 12% of the emails as suspicious. Out of the number who opened the emails, about 14% failed the campaign by clicking the phishing link. The final phishing campaign in the study period conducted April 2023 sent out 388 emails and 316 were delivered. Approximately 19% of the delivered emails were opened and 2% were reported. However, of those who opened the email, 67% failed the campaign by clicking on the phishing link.

The four phishing campaigns were conducted independently, and the following were the types of phishing emails they contain: social networking, phishing for sensitive information, current ongoing events, and attachment inclusion. Social networking spoofs the managers address to impersonates the manager, and crafts phishing mail with the sense of urgency. It could also use invitation from professional social media platform like LinkedIn. Phishing for sensitive information provides a link to a platform where it convinces users to test if their credentials have been compromised or not. The link does not collect users' information but only records the number of clickers. Current ongoing events take into cognizance any current event, trend or happenings either at the workplace or around, and drafts a mail related to that. Attachment inclusion uses emails with attachments and prompts the user to respond quickly.

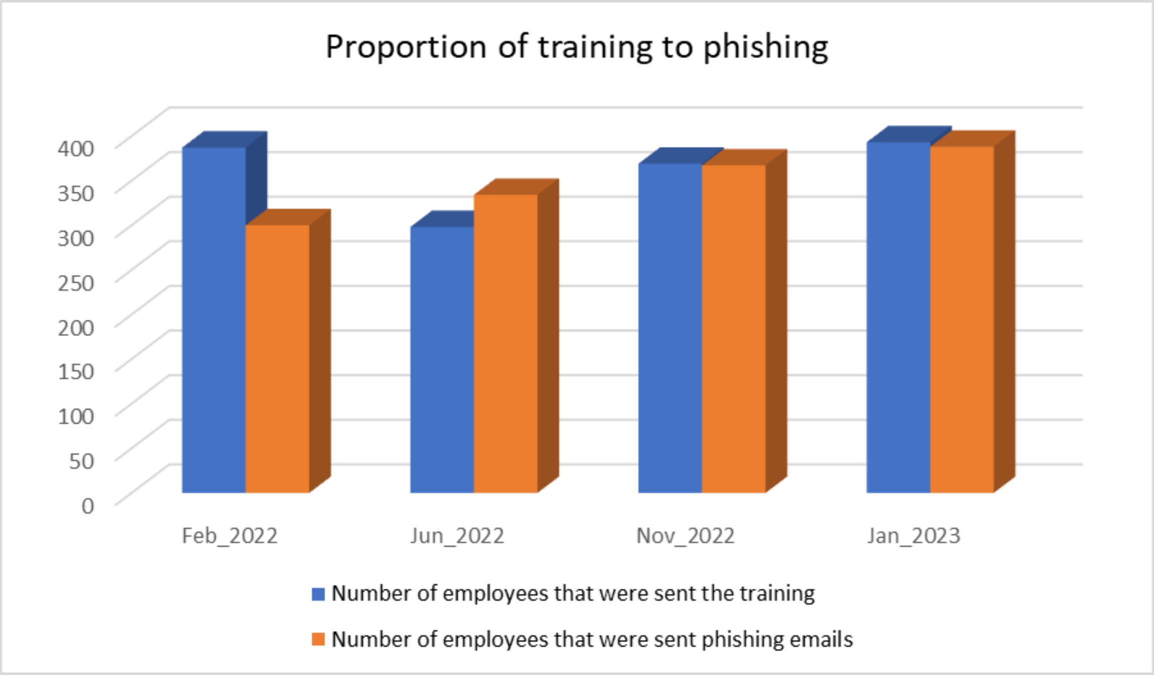


Figure 2. Employees who were aware of the training and those who participated in the campaign.

Although the phishing emails were related to multiple things such as urgent deadlines, automatic Microsoft updates, Microsoft teams and workflow approval, fake google attachments and links signing documents digitally, enrolling from a trial application, LinkedIn requests, Adobe collaboration links, and Adobe reader updates, findings from the study showed that employees did not click all but some specific types such as those relating to responding to urgent deadlines, Microsoft teams and workflow approval, signing documents , LinkedIn requests, and Adobe updates. Falling victim was not because the employees were not prompted to take the training or they were not trained, as figure 2 below shows the proportion of employees that were sent the security awareness training, to the employees that were sent the phishing emails. This suggests that approximately all the members of staff who were aware of the training also participated in the campaign.

4.3.1 Trends of clickers repeater clickers

According to the definition of repeat clickers adopted in this study, employees who fall victim of phishing attacks in two consecutive phishing campaigns, even after participating in a security awareness training in-between those phishing campaigns are in this category. The 28 clickers in March 2022 phishing simulations, were neither classified as unique clickers nor repeat clickers because it is unclear whether they have attended a security awareness training or not as stipulated in the definition of repeat clickers.

Therefore, the number of clickers in June was set as baseline for repeat clickers in the subsequent campaigns as shown in table 4. At the second phishing campaign, 28% of the clickers were repeat clickers from the first phishing campaign who partook of the security awareness training in June 2022. In the third phishing campaign, 19% of the clickers were repeat clickers from the second phishing campaign who partook of the security awareness training in November to December 2022. In the last phishing campaign, 10% of the clickers were repeat clickers from the fourth phishing campaign who also partook of the security awareness training in January to March 2023.

Phishing Campaigns				
S/N	**Phishing Campaigns**	**Clickers**	**Unique Clickers**	**Repeat Clickers**
1	March 2022	28	-	-
2	July 2022	29	72%	28%
3	December 2022	37	81%	19%
4	April 2023	40	90%	10%

Table 5. Unique and repeat clickers in all phishing campaigns

The findings of this study showed that the sport betting company has a special procedure for ensuring that repeat clickers get the required skills needed to respond to phishing attacks. The procedure is represented in figure 3 and broken down into simple steps as shown below:

1. Upon completion of a campaign, the emails of clickers are collated and disaggregated into unique and repeat clickers.
2. The unique clickers among the employees are then added to a group called the “unique clickers” group on the security awareness training platform.
3. The users who are repeat clickers are also added to another group called “repeat clickers” group on the security awareness training platform.
4. A targeted training with contents highlighted in table 5 is assigned to users in the “repeat clickers” group and reminders are sent to ensure the training is completed.
5. A refresher course of the previous training is also assigned to users in the “unique clickers” group and reminders are sent to ensure the training is completed.
6. These users are then studied and monitored in the next phishing campaign to ensure that they don’t fail the test.

Training Name	**Training Content**
Phishing Fundamentals	The basics of phishing
	How criminals use phishing.
	How you can avoid falling for phishing scams.
	Examples of phishing emails and how it looks.

Table 6. Content of targeted training for repeat clickers

4.3.2 Reported Phishing Mails

The reported phishing emails contain all emails reported by the employees to be suspicious, including the phishing emails sent out during phishing campaigns organized by the security team. A total of 264 emails were reported to be suspicious during the study period. Upon analysis by the security team, it was realized that not all reportedly suspicious emails were phishing emails. Only about 11% of all suspicious emails were real phishing emails, and 51% were phishing emails from the phishing campaigns. Therefore, there were five categories of emails in the suspicious emails reported by employees of the sport betting company. This includes:

1. **Real Phishing:** These are the real phishing email threats reported, and examples were CEO impersonation emails for approval or requests, or emails sent to users to click malicious links.
2. **Phishing campaign:** This category includes all phishing emails sent out during phishing campaigns and reported by employees
3. **Marketing emails:** This category shows legitimate marketing emails from third-party clients or from vendors willing to advertise their products

4. **Legitimate emails:** All internal mails sent from legitimate employees to other members of staff were put in this category.
5. **Spam:** All unsolicited emails were added to the spam bucket list.

As much as it would not have caused any harm if employees failed to report the phishing emails from phishing campaigns, reporting those emails is a sign of the level of security awareness in the organization. The number of suspicious emails reported by employees and their categories over the study period has been summarized in table 6 below. The real phishing percentage was calculated by dividing the number for the real phishing email by the total number of suspicious emails reported, and multiplied by 100.

Real phishing (%) = (no of real phishing email / total suspicious email reported) * 100

PERCENTAGE OF REAL PHISHING OVER TIME		
Metric	**Number**	**Percentage**
Total Suspicious email reported	264	100%
Real Phishing Email	29	11%
Phishing Campaign	134	51%
Legitimate	42	16%
Marketing	50	19%
Spam	9	3%

Table 7. Suspicious email types in the study period

As shown by figure 4, the highest number of reported incidents occurred in months where phishing campaigns were run internally by the security team because the number of phishing emails employees got increased in March 2022, July 2022, December 2022 and April 2023 when phishing campaigns were conducted. On average, the number of real phishing emails reported decreased significantly from the initial 10 recorded in March 2022. There were several months during which no real phishing emails were reported at all. Additionally, a substantial percentage of marketing and legitimate emails were reported over time with September 2022, October 2022 and January 2023 reporting only those two types.

4.3.3 Reported Real Phishing Mails vs MITRE Frameworks

After excluding the false positive from the reported suspicious emails, 29 real phishing emails were recorded.

These real phishing emails were analyzed individually to know the email category it belongs to, before continuing to map it to the MITRE ATT&CK framework and the respective technique. The MITRE ATT&CK framework consists of 14 different tactics and each of

REPORTED EMAILS BY CATEGORY	
Email Category	**Count**
Phishing Links	20
CEO Impersonation Emails	6
Phishing Link with Attachment	3

Table 8. Email category of real phishing emails

these tactics have respective techniques. Some of these tactics include reconnaissance, initial access, execution, credential access, lateral movement, command and control, etc. This study went further by mapping the component of each of the security awareness trainings to the MITRE D3FEND in order to understand how each training address the phishing threats. The table 7 below summarizes the email categories before mapping.

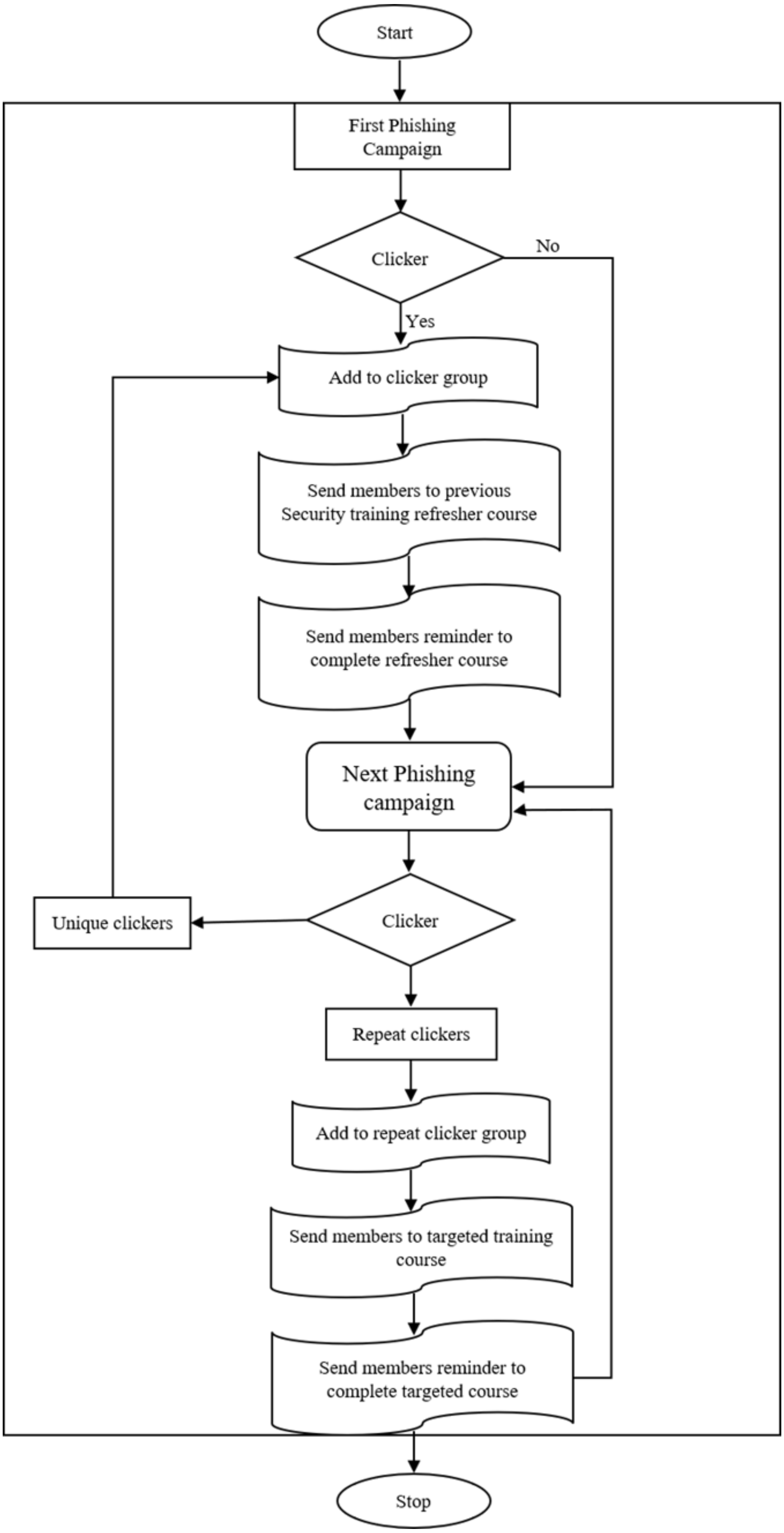

Start
First Phishing Campaign
Clicker
No
Yes
Add to clicker group
Send members to previous Security training refresher course
Send members reminder to complete refresher course
Next Phishing campaign
Unique clickers
Clicker
Repeat clickers
Add to repeat clicker group
Send members to targeted training course
Send members reminder to complete targeted course
Stop

Figure 3. Internal procedure to handle clickers (unique and repeat)

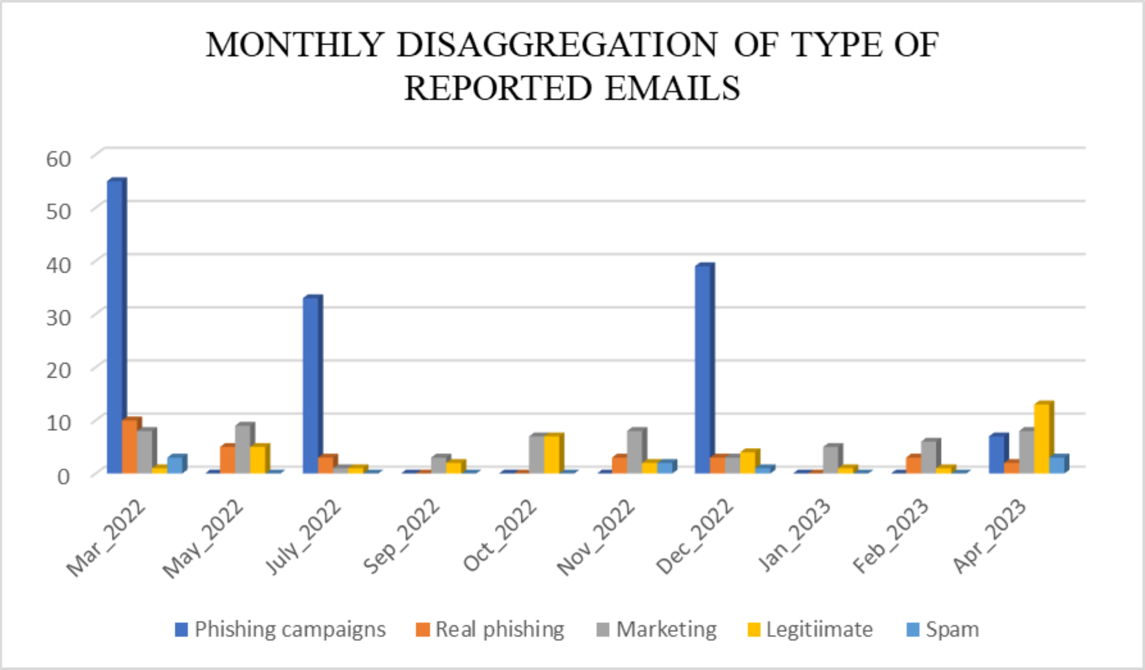


Figure 4. Suspicious emails reported monthly

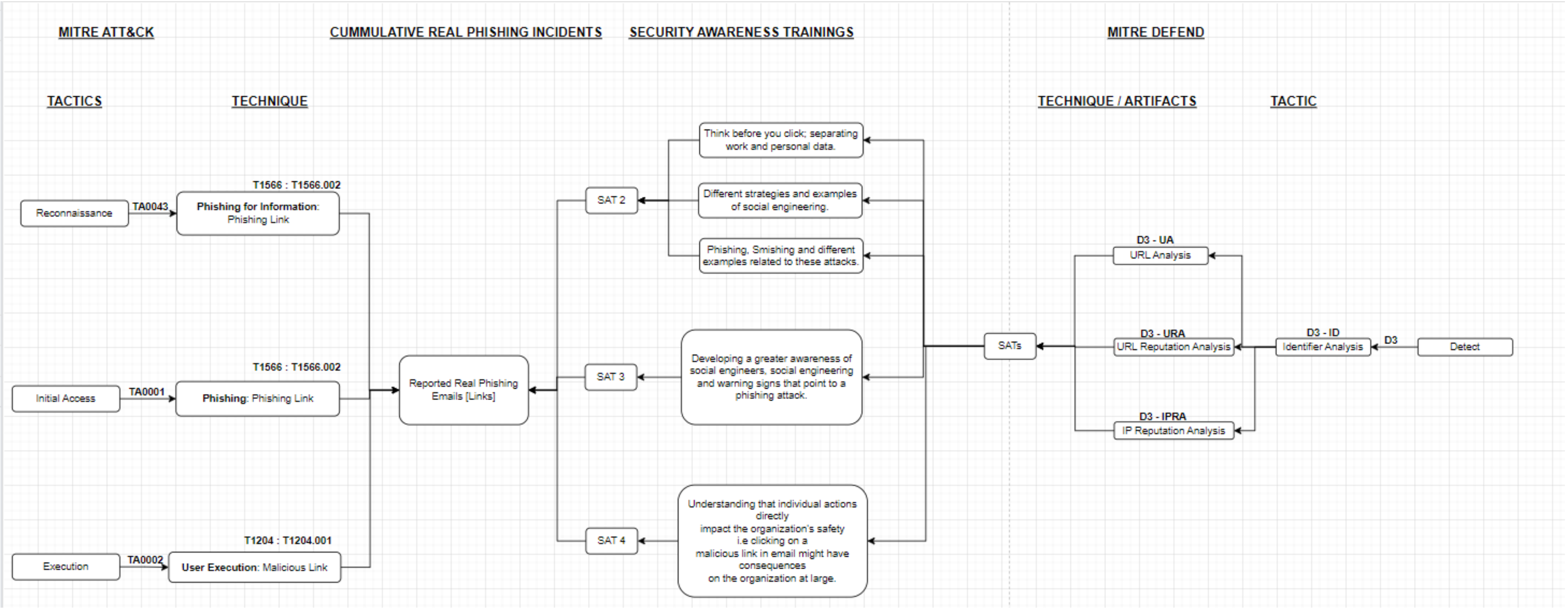

MITRE ATT&CK
CUMMULATIVE REAL PHISHING INCIDENTS
SECURITY AWARENESS TRAININGS
MITRE DEFEND
TACTICS
TECHNIQUE
TECHNIQUE / ARTIFACTS
TACTIC
Think before you click; separating work and personal data.
Different strategies and examples of social engineering.
Phishing, Smishing and different examples related to these attacks.
T1566 : T1566.002
Reconnaissance
TA0043
Phishing for Information: Phishing Link
SAT 2
D3 - UA
URL Analysis
D3 - URA
URL Reputation Analysis
D3 - ID
Identifier Analysis
D3
Detect
SATs
T1566 : T1566.002
Initial Access
TA0001
Phishing: Phishing Link
Reported Real Phishing Emails [Links]
SAT 3
Developing a greater awareness of social engineers, social engineering and warning signs that point to a phishing attack.
D3 - IPRA
IP Reputation Analysis
Understanding that individual actions directly impact the organization's safety i.e clicking on a malicious link in email might have consequences on the organization at large.
T1204 : T1204.001
Execution
TA0002
User Execution: Malicious Link
SAT 4

Figure 5. Mapping phishing links email categories to the MITRE ATT&CK framework

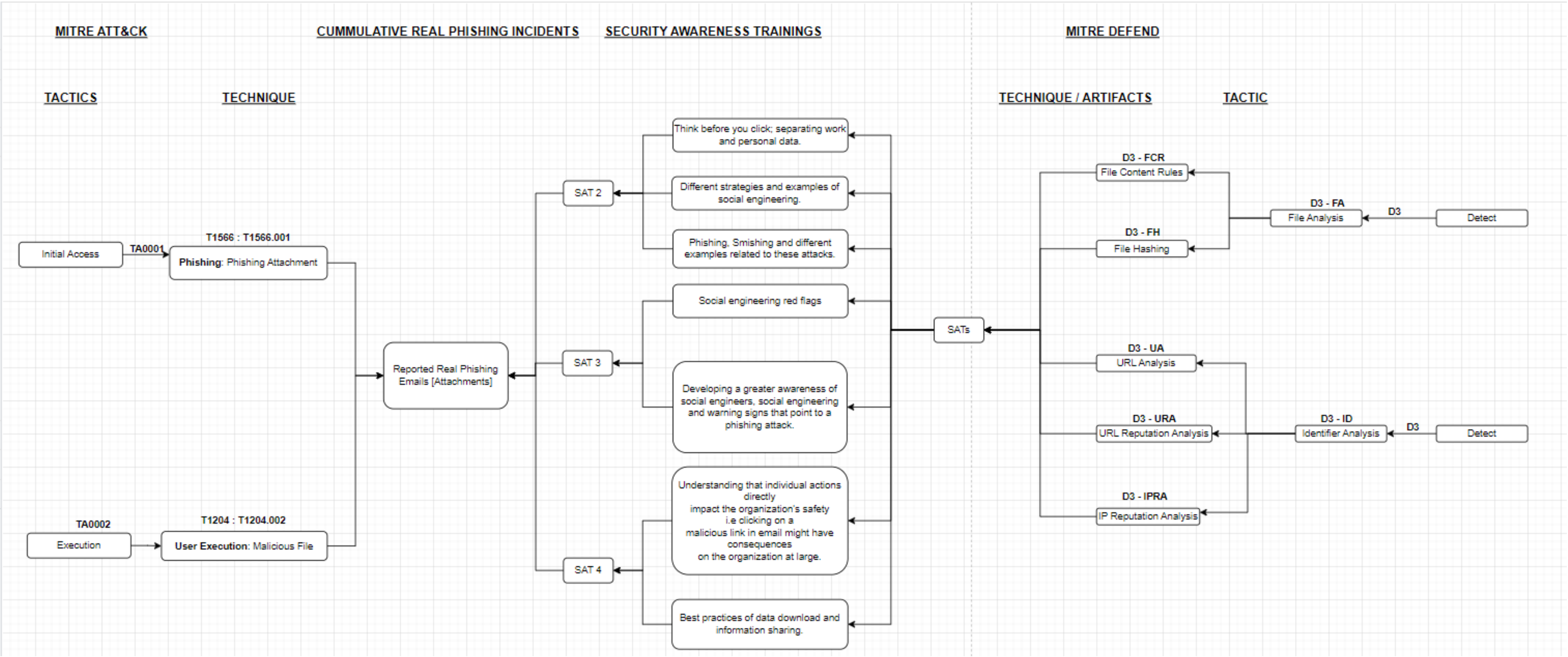

MITRE ATT&CK
CUMMULATIVE REAL PHISHING INCIDENTS
SECURITY AWARENESS TRAININGS
MITRE DEFEND
TACTICS
TECHNIQUE
TECHNIQUE / ARTIFACTS
TACTIC
Initial Access
TA0001
T1566 : T1566.001
Phishing: Phishing Attachment
TA0002
Execution
T1204 : T1204.002
User Execution: Malicious File
Reported Real Phishing Emails [Attachments]
SAT 2
SAT 3
SAT 4
Think before you click; separating work and personal data.
Different strategies and examples of social engineering.
Phishing, Smishing and different examples related to these attacks.
Social engineering red flags
Developing a greater awareness of social engineers, social engineering and warning signs that point to a phishing attack.
Understanding that individual actions directly impact the organization's safety i.e clicking on a malicious link in email might have consequences on the organization at large.
Best practices of data download and information sharing.
SATs
D3 - FCR
File Content Rules
D3 - FH
File Hashing
D3 - FA
File Analysis
D3
Detect
D3 - UA
URL Analysis
D3 - URA
URL Reputation Analysis
D3 - IPRA
IP Reputation Analysis
D3 - ID
Identifier Analysis
D3
Detect

Figure 6. Mapping attachment email categories to the MITRE ATT&CK framework.

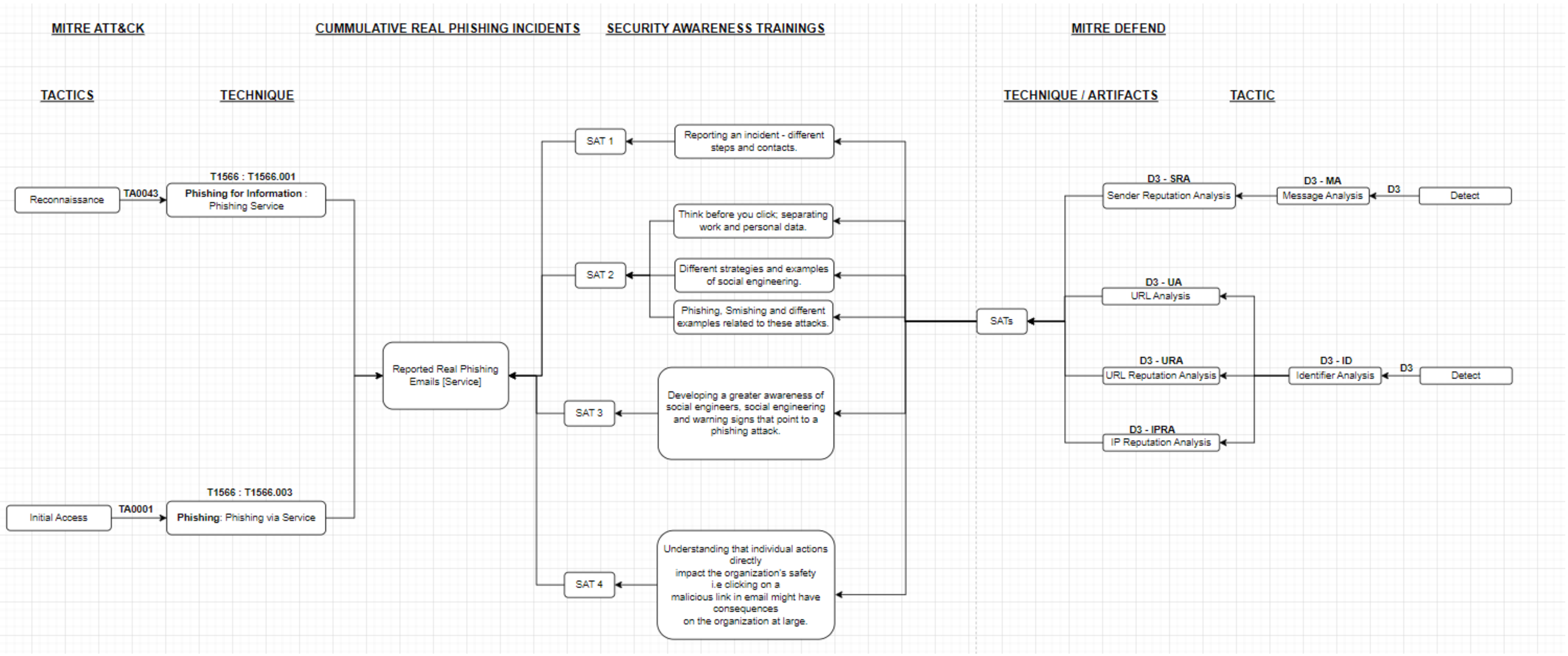

MITRE ATT&CK
CUMMULATIVE REAL PHISHING INCIDENTS
SECURITY AWARENESS TRAININGS
MITRE DEFEND
TACTICS
TECHNIQUE
TECHNIQUE / ARTIFACTS
TACTIC
Reconnaissance
TA0043
T1566 : T1566.001
Phishing for Information : Phishing Service
Initial Access
TA0001
T1566 : T1566.003
Phishing: Phishing via Service
Reported Real Phishing Emails [Service]
SAT 1
SAT 2
SAT 3
SAT 4
Reporting an incident - different steps and contacts.
Think before you click; separating work and personal data.
Different strategies and examples of social engineering.
Phishing, Smishing and different examples related to these attacks.
Developing a greater awareness of social engineers, social engineering and warning signs that point to a phishing attack.
Understanding that individual actions directly impact the organization's safety i.e clicking on a malicious link in email might have consequences on the organization at large.
SATs
D3 - SRA
Sender Reputation Analysis
D3 - UA
URL Analysis
D3 - URA
URL Reputation Analysis
D3 - IPRA
IP Reputation Analysis
D3 - MA
Message Analysis
D3 - ID
Identifier Analysis
D3
Detect
D3
Detect

Figure 7. Mapping service email categories (CEO impersonation) to the MITRE ATT&CK framework.

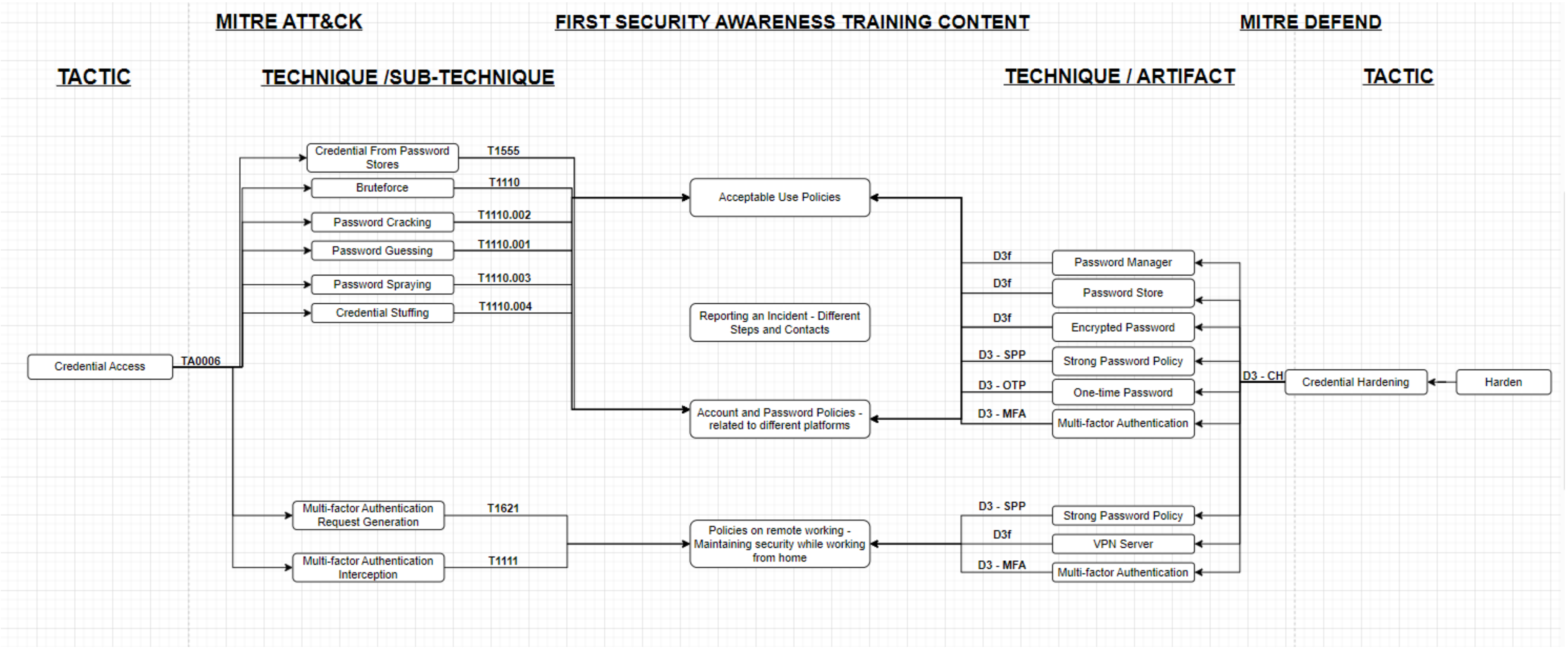


Figure 8. Mapping the first security awareness training to MITRE frameworks

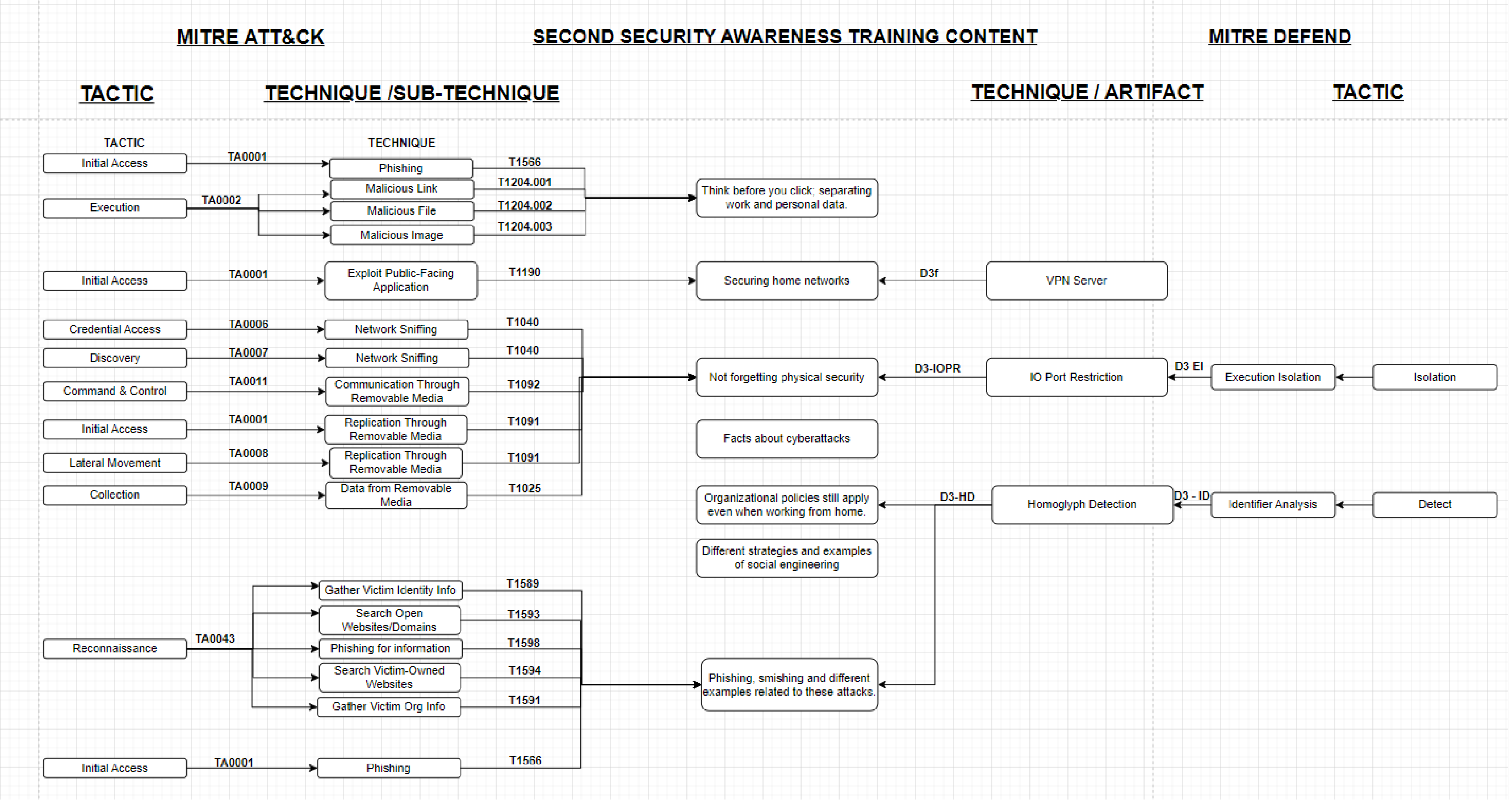


Figure 9. Mapping the second security awareness training to MITRE frameworks

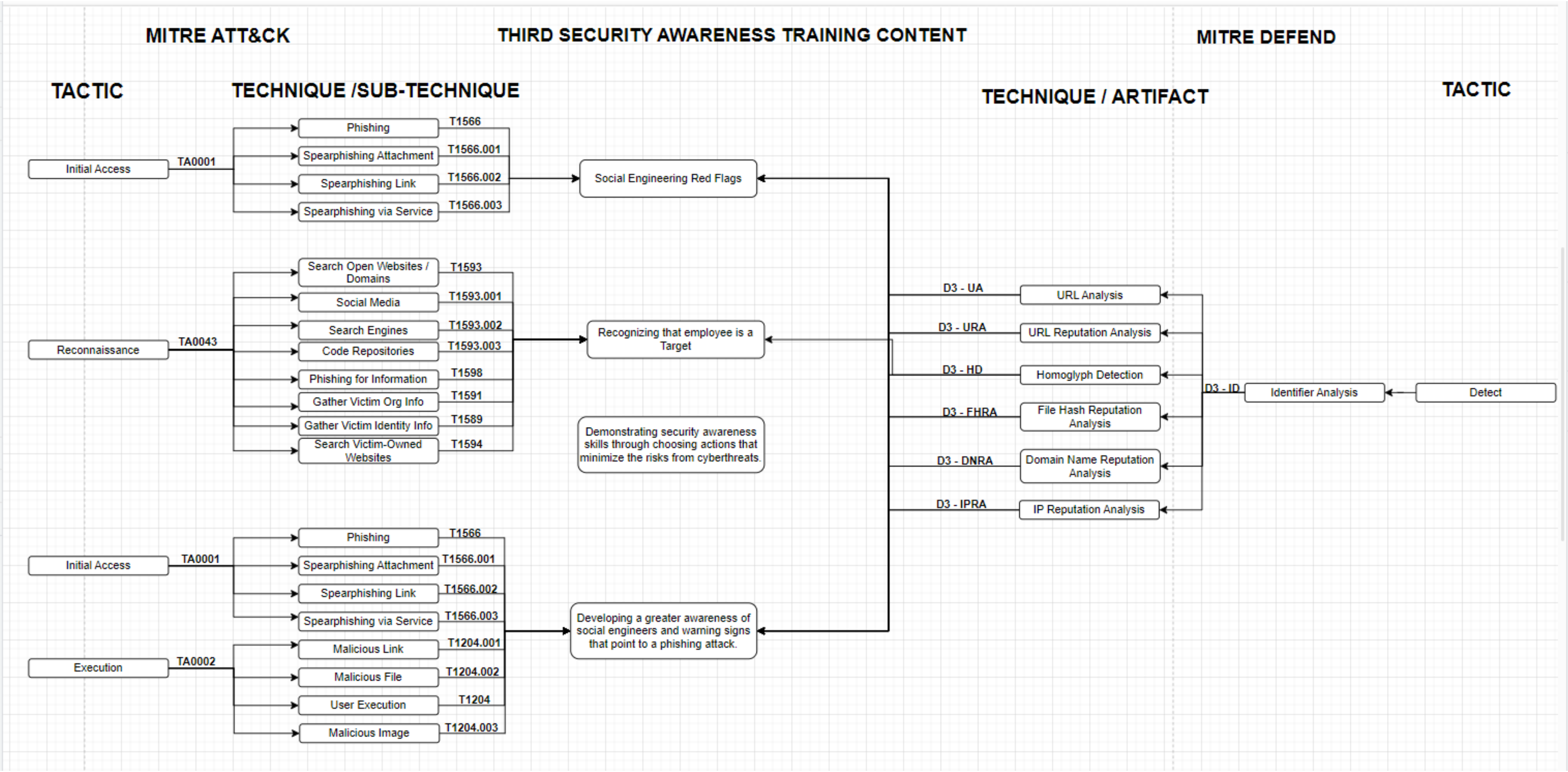


Figure 10. Mapping the third security awareness training to MITRE frameworks

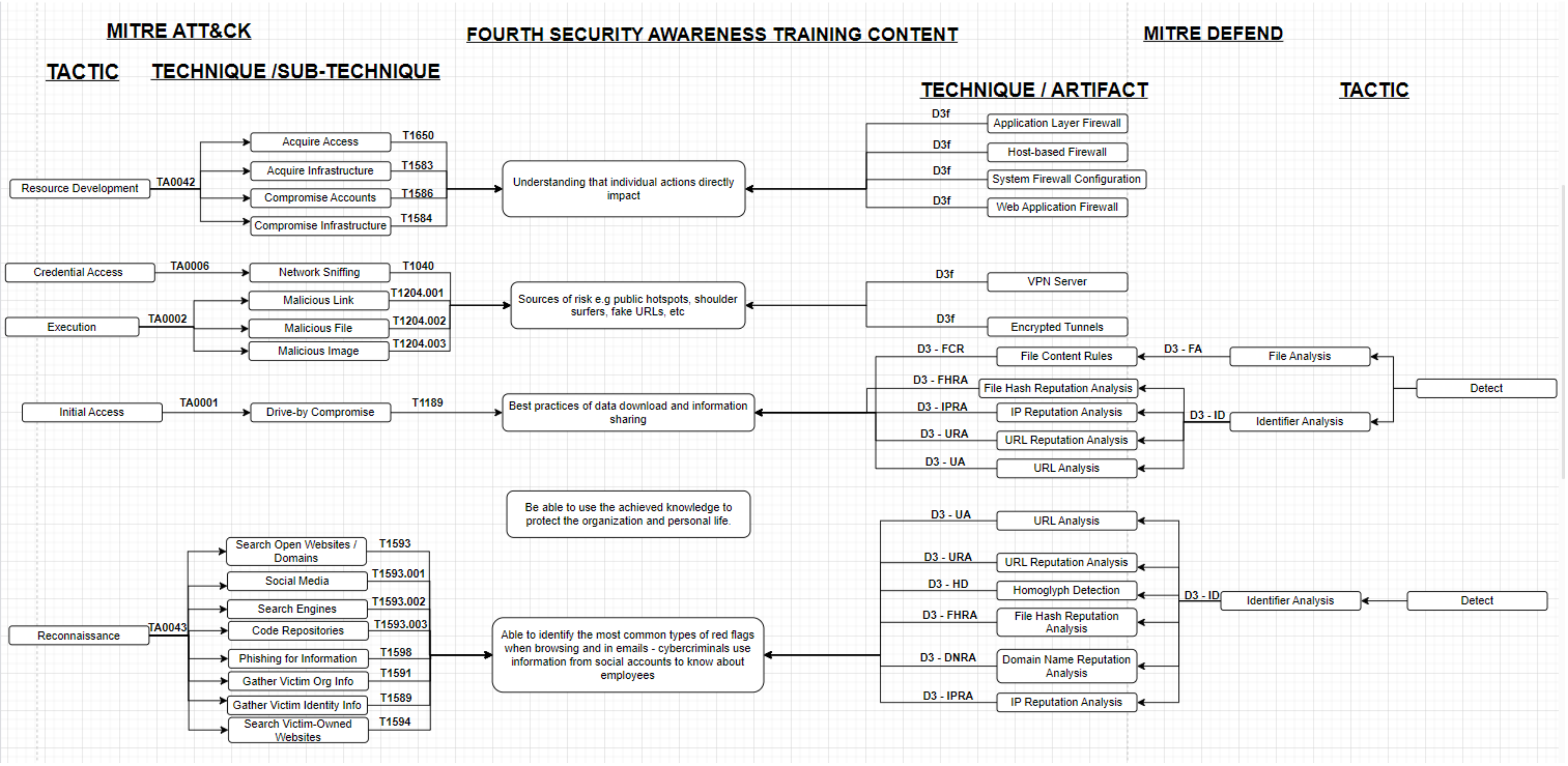


Figure 11. Mapping the fourth security awareness training to MITRE frameworks

5. Discussion and Conclusion

5.1 Discussion

The number of security awareness training conducted in this study corroborates existing literature that have shown that companies and organizations have been prioritizing security awareness training. Similarly, the very high completion rates ranging from 80-99% across the training programme is in tandem with what was recorded by [50]. A study by the National Institute of Standards and Technology (NIST) that measured the effectiveness of U.S. Government Security Awareness Programs had earlier concluded that organizations place emphasis on compliance metrics such as training completion rates [64], and that accounts for most high completion rates of security awareness training. Although the finding of this study supports the work of [64], there was no information to determine whether the company involved in the study mandated training completion. However, the high completion rates recorded in this study suggests that security awareness training program is effective in engaging employees and promoting awareness of security issues.

As much as it has been recorded that security awareness training are effective in protecting companies, their stakeholders, employees and customers against phishing attacks [12][14], the finding of these study was not consistent with such. Recent study by [65], [66] and [67] found that a high number of organizations said that regular security awareness training had reduced their staffs' susceptibility to phishing attacks within the first 12 months. But the percentage of employees who failed phishing campaign gradually increased from 12% after the first training to 14% after the third training, while it peaked at 67% after the fourth training. More so, the ineffectiveness of the security awareness training was more evident in the employee reporting rate for phishing activities during the campaign. Reporting rate dropped from 19% among those who open phishing emails at the first campaign to 2% at the fourth campaign. This sparks a major concern because participating in a security awareness training should empower employees to best respond to phishing activities by failing to click the links and reporting the activities to the security team.

As highlighted by [16], monitoring phishing emails accessed by employees within an organization can provide valuable insights into the level of information security awareness. But the employees' low reporting rate would not afford the security team that opportunity. Contrary to the ineffectiveness of the security awareness training, it is important to note that while the number of unique repeat clickers increase, the number of repeat clickers reduced over time. The increase in unique clickers is a common finding in phishing studies, as attackers continue to adapt and improve their tactics to trick users into clicking on malicious links. Evidences on phishing attacks found that phishing has evolved into a more sophisticated attack vector [27], and online fraudsters have adapted their tactics to exploit the rising cost of living by targeting those in difficult financial situations with phishing attacks [68]. The continuous reduction in the number of repeat clickers in this study however suggests that the targeted training that repeat clickers are mandated and prompted to take have a positive effect in protecting against phishing. The ineffectiveness of the security awareness training in reducing the number of clickers could be because the type of phishing common to the industry have not been identified and the training components were not targeted at those specific phishing activities.

Therefore, the use of the MITRE ATT&CK framework in this study has shown that the framework is useful in identifying and mitigating cyber threats because it covers most types of cyber-attacks, but it lacks the specificity to describe all. Previous studies have highlighted the importance of focusing on the types of phishing attacks that are most prevalent in order to improve training effectiveness. For example, a comprehensive study on phishing attacks proposed a detailed anatomy of phishing which involves attack phases, attacker's types, vulnerabilities, threats, targets, attack mediums, and attacking techniques. The proposed anatomy can help readers understand the process lifecycle of a phishing attack in developing a holistic anti-phishing system which in turn will increase the awareness of these phishing attacks and the techniques being used [27]. The mapping of this study serves the same purpose for the sport betting industry, and opines that most phishing techniques used in the sport betting industry are of initial access and reconnaissance tactics.

5.2 Conclusion

As against popular opinion, security awareness training was not effective in reducing the number of employees who fail victim of phishing threats. This supports the work of [48] that stated that only few organizations claimed that their security awareness training programs are effective. The development is supported by the conclusion of [46] that the effectiveness of security awareness training in preventing phishing attacks varies depending on several factors, including the training materials and method, the frequency of training, and the level of employee engagement.

Therefore, the possible reason for the ineffectiveness of the training could be the lack of a systematic understanding of the nature of the threats that is peculiar to the sector, how they impact employees' security-related beliefs and behavioral intentions, and the conditions that influence such a relationship. The number of repeat clickers showing continuous reduction in this study cannot be attributed to the main security awareness training but the targeted course. Also, the training did not improve the reporting rates of phishing activities in the company as contrary to what most studies believe.

5.3 Limitations

The limitations of these study include the sampling frame of a single organization, which may not be representative of other organizations in the sport betting industry. This limits the generalizability of the findings to other contexts in and outside the EU. Also, the study was conducted over a period of fifteen month, which may not be sufficient to determine the long-term effectiveness of the training.

Another limitation of this study is that it relied on self-reported data from employees, which may not be entirely accurate. This is because employees may not have reported all suspicious emails or may have misreported some legitimate emails as suspicious. The last limitation is that this study did not take into account the potential impact of external factors such as changes in the threat landscape, advances in phishing techniques, or changes in the organization's technology or policies. It is possible that these factors affect the effectiveness of the proposed procedure over time.

5.4 Recommendations

All employees should first take the targeted course for repeat clickers, and continually trained using the framework to identify vulnerabilities and create focused training programs to increase staff knowledge and skills. Modern cyber threats might not be defeated using conventional training techniques.

The MITRE DEFEND metric, which offers a framework of active defense measures to assist organizations detect and respond to cyberattacks, should therefore be a major component of security awareness training. Additionally, regular phishing simulations should be employed to help organizations assess their employees' susceptibility to phishing attacks. These regular phishing exercises can also instill a culture of caution among staff members, making them more likely to see and report strange emails or other security risks.

References

[1] K. R. L. Rand and S. A. Light, “Sports betting and data security: Cybersecurity, data protection, and privacy rights in gaming law practice.” https://www.americanbar.org/groups/business_law/publications/blt/2021/02/sports-betting/.

[2] V. Bhavsar, A. Kadlak, and S. Sharma, “Study on phishing attacks,” *Int. J. Comput. Appl*, vol. 182, pp. 27–29, 2018.

[3] H. Target, “Modern threats the attack surface. a whitepaper.,” *Hacker Target*, 2021.

[4] “Phishing in depth (attacks mitigations)..” https://bit.ly/3N8iQ7x, 2020.

[5] “What is an attack surface?.” https://www.ibm.com/topics/attack-surface#:~:text=An%20organization′s%20social%20engineering,prevalent%20social%20engineering%20attack%20vector. Accessed: 2023-04-12.

[6] S. A. Chaudhry, J. A.and Chaudhry and R. G. Rittenhouse, “Phishing attacks and defenses.,” *International journal of security and its applications*, vol. 10(1), pp. 247–256, 2016.

[7] P. Sharma, B. Dash, and M. F. Ansari, “Anti-phishing techniques–a review of cyber defense mechanisms,” vol. 11(7), pp. 153–160, 2022.

[8] J. T. Okpa, B. O. Ajah, and J. E. Igbe, “Rising trend of phishing attacks on corporate organisations in cross river state, nigeria,” *International Journal of Cyber Criminology*, vol. 14(2), pp. 460–478, 2020.

[9] H. J. Parker and S. V. Flowerday, “Contributing factors to increased susceptibility to social media phishing attacks,” *South African Journal of Information Management*, vol. 22(1), pp. 1–10, 2020.

[10] S. Unchit, P.and Das, A. Kim, and L. Camp, “Quantifying susceptibility to spear phishing in a high school environment using signal detection theory.,” 2020.

[11] A. J. Burns, M. E. Johnson, and D. D. Caputo, “Spear phishing in a barrel: Insights from a targeted phishing campaign,” *Journal of Organizational Computing and Electronic Commerce*, vol. 29, no. 1, pp. 24–39, 2019.

[12] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue participation and collective reflection. an intervention study," *Comput. Secur.*, vol. 29, no. 4, pp. 432–445, 2010.

[13] M. Alshaikh, S. B. Maynard, A. Ahmad, and S. Chang, "An exploratory study of current information security training and awareness practices in organizations," *Proc. 51st Hawaii Int. Conf. Syst. Sci*, pp. 5085–5094, 2018.

[14] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Comput. Secur.*, vol. 98, Nov. 2020.

[15] N. S. Safa, R. V. Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput. Secur.*, vol. 56, pp. 70–82, Feb 2016.

[16] B. Khan, K. S. Alghathbar, S. I. Nabil, and M. Khan, "Effectiveness of information security awareness methods based on psychological theories," *African Journal of Business Management*, vol. 5, no. 26, pp. 10862–10868, 2011.

[17] M.Liapustin, "Why do employees continue to fall for phishing attacks?." `https://trustifi.com/why-do-employees-continue-to-fall-for-phishing-attacks/`. Accessed: 2023-04-12.

[18] B. Wardman, "Assessing the gap: Measure the impact of phishing on an organization," *Annual ADFSL Conference on Digital Forensics, Security and Law*, 2016.

[19] C. Ronald, J. Dodge, C. Carver, and A. Ferguson, "Phishing for user security awareness," *Elsevier: computers security*, vol. 26, pp. 73–80, 2007.

[20] E. Subagyo and K. Ramli, "Analyzing the impact of information security awareness training to the employees of telco company xyz," *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, vol. 5, pp. 8799–8808, 2022.

[21] S. Pirocca, L. Allodi, and N. Zannone, "A toolkit for security awareness training against targeted phishing," *International Conference on Information Systems Security, ICISS 2020: Information Systems Security*, pp. 137–159, 2020.

[22] Y. Jo, O. Choi, J. You, Y. Cha, and D. Lee, "Cyberattack models for ship equipment based on the mitre attck framework," *Sensors*, vol. 22, no. 1860, pp. 24–39, 2020.

[23] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, "Don't click: towards an effective anti-phishing training. a comparative literature review," *Springer Open: Human Centric Computing and Information Science*, vol. 10, no. 33, 2020.

[24] S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, "Phishing email detection using natural language processing techniques: A literature survey," *Elsevier: Procedia Computer Science*, vol. 189, no. 2021, pp. 19–28, 2021.

[25] A. Basit, M. Zafar, X. Liu, A. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of ai-enabled phishing attacks detection techniques," *Springer Nature: Telecommunication Systems (2021)*, vol. 76, no. 2021, pp. 139–154, 2021.

[26] A. S. Martino and X. Perramon, "Phishing secrets: History, effects, and countermeasures," *International Journal of Network Security*, vol. 12, no. 1, pp. 37–45, 2011.

[27] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," *Frontiers in Computer Science*, vol. 3, no. 563060, 2021.

[28] I. Vayansky and S. Kumar, "Phishing–challenges and solutions.," *Computer Fraud Security*, 2018.

[29] A. Rader and S. Rahman, "Exploring historical and emerging phishing techniques and mitigating the associated security risks," *International Journal of Network Security Its Applications (IJNSA)*, vol. 5, no. 4, 2013.

[30] M. Banu and S. Banu, "A comprehensive study of phishing attacks," *International Journal of Computer Science and Information Technologies*, vol. 4, no. 6, 2013.

[31] Threatcop, "Benefits and purpose of security awareness training." `https://threatcop.com/blog/benefits-and-purpose-of-security-awareness-training/`, 2020.

[32] J. Terra., "The importance of security awareness training." `https://www.simplilearn.com/importance-of-security-awareness-training-article`, 2023.

[33] A. Hutchings and H. Hayes, "Routine activity theory and phishing victimisation: Who gets caught in the 'net'?," *Current Issues in Criminal Justice*, vol. 20, no. 3, pp. 433–452, 2009.

[34] C. Iuga, J. Nurse, and A. Erola, "Baiting the hook: factors impacting susceptibility to phishing attacks," *Springer Open: Human Centric Computing and Information Science*, vol. 6, no. 8, 2016.

[35] X. Chen, I. Bose, and C. G. A. Leung, “Assessing the severity of phishing attacks: A hybrid data mining approach,” *Elsevier: Decision Support Systems*, vol. 50, pp. 662–672, 2011.

[36] R. Rutherford, “The changing face of phishing,” *Computer Fraud Security*, 2018.

[37] S. Garera, N. Provos, and M. Chew, “A framework for detection and measurement of phishing attacks”, worm’07, alexandria, virginia, usa,” 2007.

[38] R. Damodaram, “Study on phishing attacks and antiphishing tools,” *International Research Journal of Engineering and Technology*, vol. 3, 2016.

[39] Mimecast, “What is security awareness training and why is it important?,” 2022.

[40] M. K. P. (2021), “What is cyber hygiene and why is it important?,” 2021.

[41] T. R. Peltier, “Implementing an information security awareness program,” *Information Systems Security*, vol. 14, no. 2, pp. 37–42, 2005.

[42] M. Sas, G. Reniers, K. Ponnet, and W. Hardyns, “The impact of training sessions on physical security awareness: Measuring employees’ knowledge, attitude and self-reported behaviour,” *Safety Science*, vol. 144, p. 105447, 2021.

[43] F. A. Alou, “The need for effective information security awareness,” *Journal of Advances in Information Technology*, vol. 3, no. 3, 2012.

[44] M. Ansari, P. K. Sharma, and B. Dash, “Prevention of phishing attacks using ai-based cybersecurity awareness training,” *International Journal of Smart Sensor and Adhoc Network*, vol. 3, no. 3, 2022.

[45] Cybsafe, “Top 4 types of security awareness training and the pros and cons of each.,” 2021.

[46] A. R. M. Asri and I. E. Khairuddin, “A theoretical framework for the awareness of phishing attack,” *Journal of Information and Knowledge Management (JIKM)*, vol. 1, pp. 126–135, 2022.

[47] A. Georgiadou, S. Mouzakitis, and D. Askounis, “Assessing mitre att&ck risk using a cyber-security culture framework.,” *Sensors*, vol. 21, no. 3267, 2021.

[48] A. Jayatilaka, “Evaluation of security training and awareness programs: Review of current practices and guideline,” *IEEE Computer Society*, 2021.

[49] J. Bilodeau, “Four factors for effective security awareness training,” 2021.

[50] J. J, “What is a good completion percentage for security and compliance training? knowbe4..” https://blog.knowbe4.com/good-completion-percentage-for-security-compliance-training, 2022, January 26. Accessed: April 28, 2023.

[51] S. Buege, “Security awareness training: Top challenges and what to do about them. security magazine.,” 2021.

[52] M. S. Jalali, M. Bruckes, D. Westmattelmann, and G. Schewe, “Why employees (still) click on phishing links: Investigation in hospitals,” *J Med Internet Res*, vol. 22, p. e16775, Jan 2020.

[53] ECcouncil, “Mitre attck: Meaning, benefits and mitre attack framework.,” 2022.

[54] VMWare, “What is mitre attack?.” https://bit.ly/3N8iQ7x, 2021.

[55] T. M. Corporation’, “Mitre att&ck. the mitre corporation.” https://attack.mitre.org, 2016.

[56] Trellix, “What is the mitre attck framework?.” https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html, 2021.

[57] B. Strom, “Att&ck101.” https://medium.com/mitre-attack/att-ck-101-17074d3bc62, 2021.

[58] B. Strom, A. Applebaum, D. Miller, K. Nickels, A. Pennington, and C. Thomas, “Mitre attck: Design and philosophy,” *The MITRE Corporation, Bedford, MA, USA,*, 2018.

[59] B. Strom, J. Battaglia, M. Kemmerer, W. Kupersanin, D. Miller, C. Wampler, S. Whitley, and R. Wolf, “Finding cyber threats with attck-based analytics,” *The MITRE Corporation, Bedford, MA, USA,*, 2017.

[60] S. Caimi, “Mitre attck: The magic of mitigations; cisco: San jose, ca,,” 2020.

[61] Y. Shin, K. Kim, J. Lee, and K. Lee, “Focusing on the weakest link: A similarity analysis on phishing campaigns based on the attck matrix,” *Hindawi Security and Communication Networks*, vol. 2022, 2022.

[62] M. Schneider, “Mitre att&ck flaws of the standardization..” https://www.scip.ch/en/?labs.20210204, 2021.

[63] M. Buckbee, “Mitre attck framework: Everything you need to know.,” 2022.

[64] J. L. Jacobs, J. M. Haney, and S. M. Furman, “Measuring the effectiveness of u.s. government security awareness programs,” *A Mixed-Methods Study. National Institute of Standards and Technology.*, 2022.

[65] D. Jordan, “How effective is security awareness training? [blog post]..” `https://blog.usecure.io/does-security-awareness-training-work`, 2022, January 26.

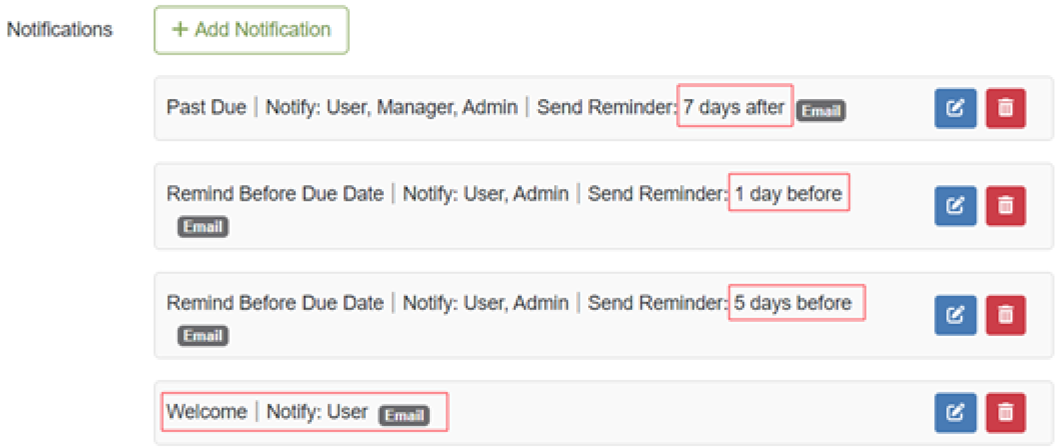
[66] S. Alder, “Study confirms security awareness training significantly reduces susceptibility to phishing attacks,” *HIPAA Journal.* Accessed: April 28, 2023.

[67] Rapid7, “Why you should let your security team go phishing - a guide for executives on the value, cost, risk, and execution of a phishing awareness program,”

[68] G. Jamie, “Online fraudsters adapt tactics to exploit uk cost of living crisis..” `https://www.theguardian.com/business/2022/sep/26/online-fraudsters-adapt-tactics-to-exploit-uk-cost-of-living-crisis` Accessed: April 28, 2023.

A. Appendices

Appendix 1



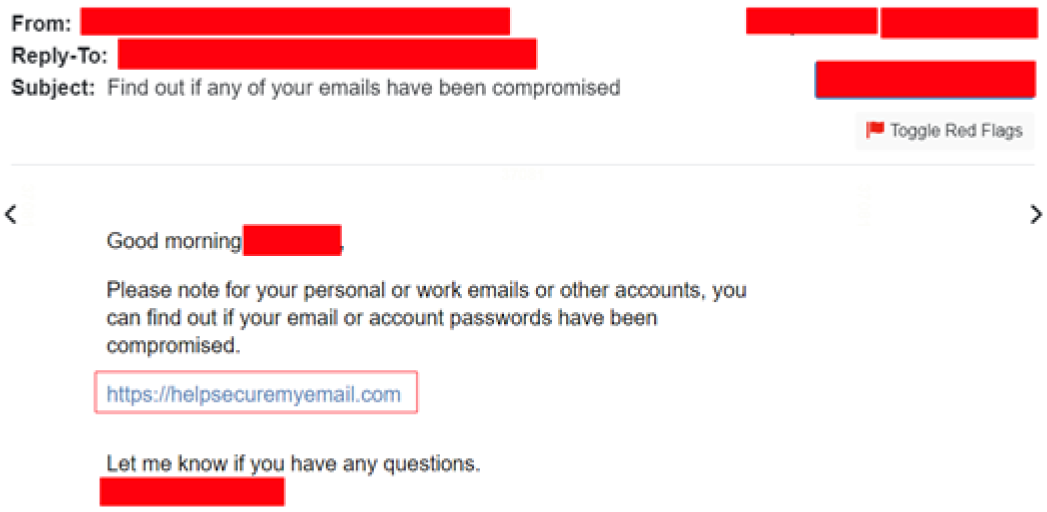
Past Due | Notify: User, Manager, Admin | Send Reminder: 7 days after Email

Remind Before Due Date | Notify: User, Admin | Send Reminder: 1 day before Email

Remind Before Due Date | Notify: User, Admin | Send Reminder: 5 days before Email

Welcome | Notify: User Email

Figure 12. Notification set to remind users of trainings



From: [redacted] [redacted] [redacted]
Reply-To: [redacted]
Subject: Find out if any of your emails have been compromised [redacted]

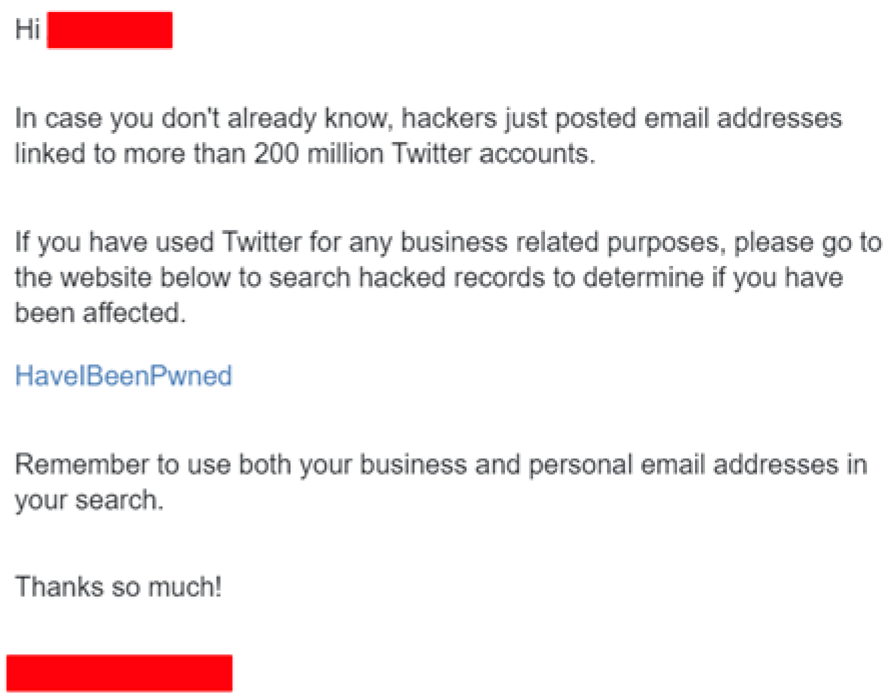
Good morning [redacted],

Please note for your personal or work emails or other accounts, you can find out if your email or account passwords have been compromised.

https://helpsecuremyemail.com

Let me know if you have any questions.
[redacted]

Figure 13. Suspicious email sample



Hi [redacted]

In case you don't already know, hackers just posted email addresses linked to more than 200 million Twitter accounts.

If you have used Twitter for any business related purposes, please go to the website below to search hacked records to determine if you have been affected.

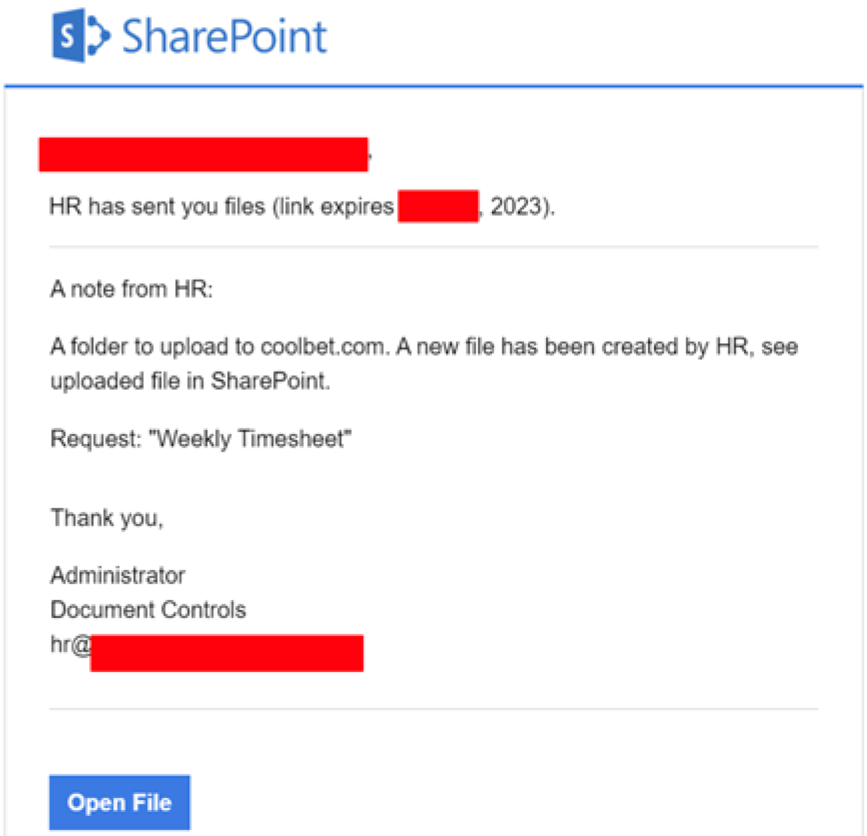
HaveIBeenPwned

Remember to use both your business and personal email addresses in your search.

Thanks so much!

[redacted]

Figure 14. Suspicious email sample



[redacted],

HR has sent you files (link expires [redacted], 2023).

A note from HR:

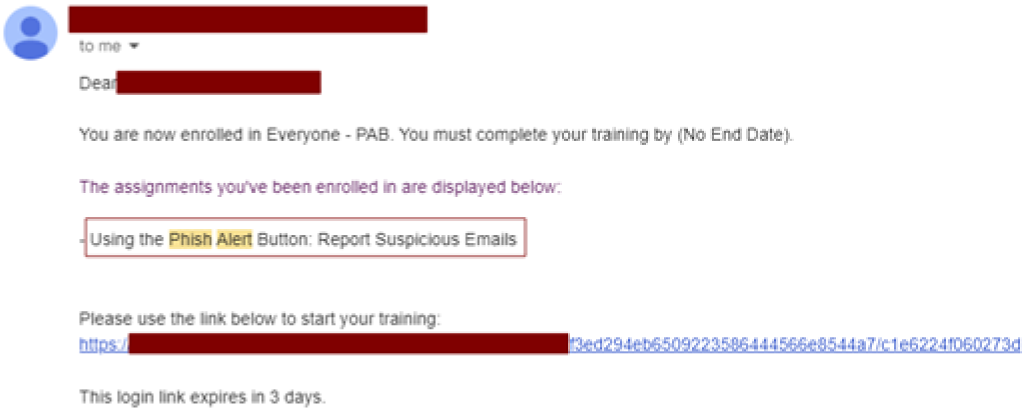
A folder to upload to coolbet.com. A new file has been created by HR, see uploaded file in SharePoint.

Request: "Weekly Timesheet"

Thank you,

Administrator
Document Controls
hr@[redacted]

Figure 15. Suspicious email sample



[redacted]

to me ▾

Dear [redacted]

You are now enrolled in Everyone - PAB. You must complete your training by (No End Date).

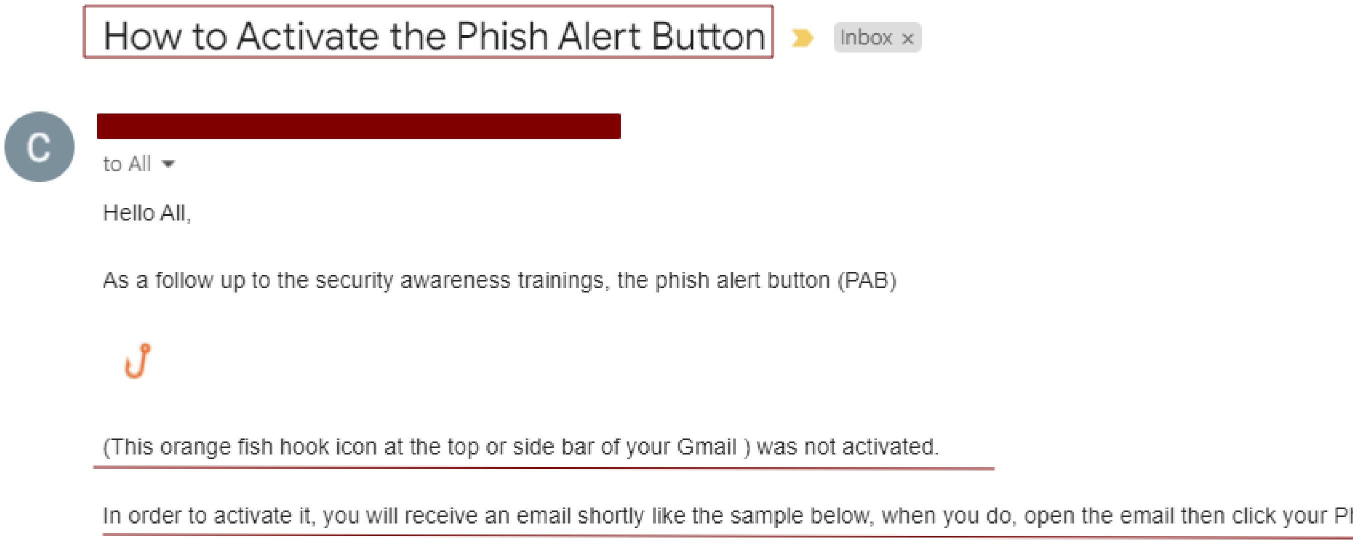
The assignments you've been enrolled in are displayed below:

- Using the Phish Alert Button: Report Suspicious Emails

Please use the link below to start your training:
https:/[redacted]f3ed294eb6509223586444566e8544a7/c1e6224f060273d

This login link expires in 3 days.

Figure 16. Email sent to employee to activate the reporting button



How to Activate the Phish Alert Button

[redacted]

to All ▾

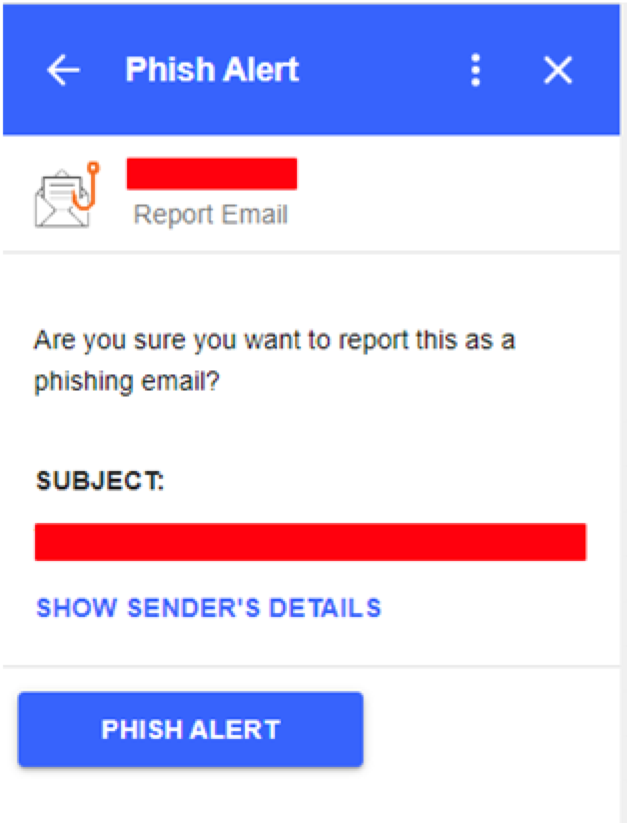
Hello All,

As a follow up to the security awareness trainings, the phish alert button (PAB)

(This orange fish hook icon at the top or side bar of your Gmail) was not activated.

In order to activate it, you will receive an email shortly like the sample below, when you do, open the email then click your Pl

Figure 17. Email sent to employee to activate the reporting button



[redacted]

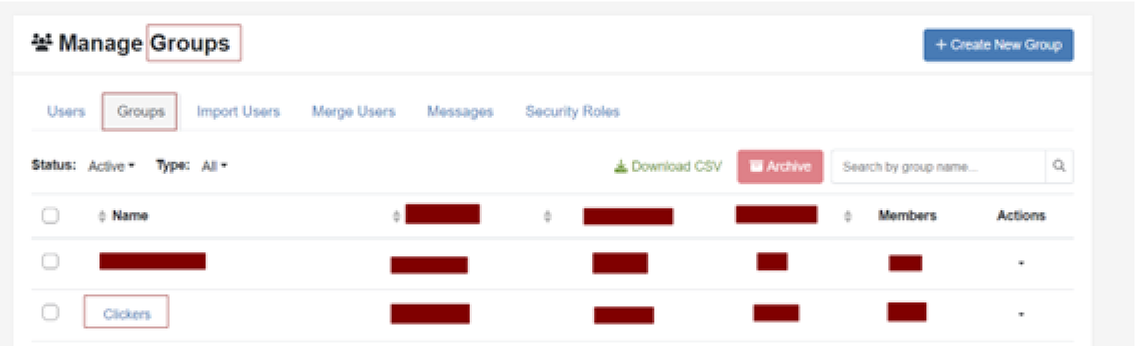
Report Email

Are you sure you want to report this as a phishing email?

SUBJECT:

[redacted]

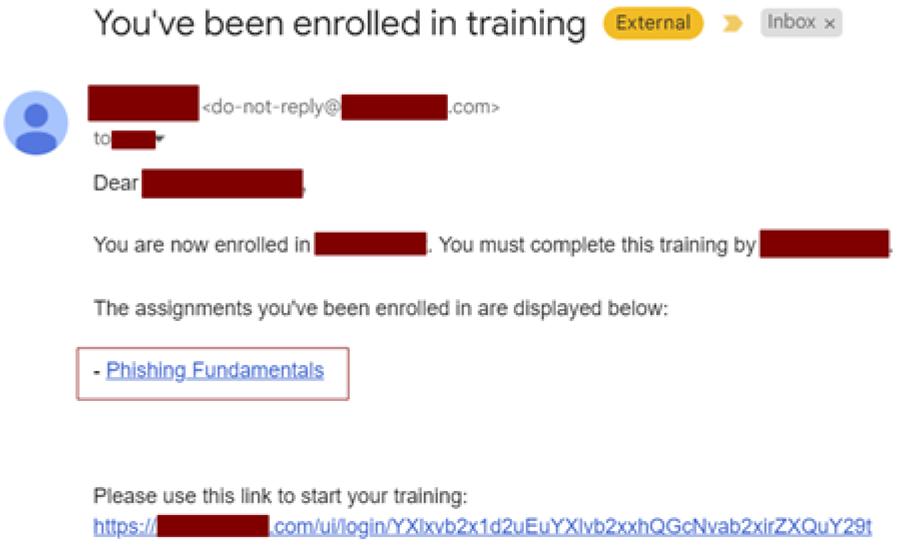
Figure 18. Phish alert button to report suspicous emails



Status: Active ▾ Type: All ▾

□	Name	[redacted]	[redacted]	[redacted]	Members	Actions
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	▾
□	Clickers	[redacted]	[redacted]	[redacted]	[redacted]	▾

Figure 19. Repeat Clickers Group



You've been enrolled in training

[redacted] <do-not-reply@[redacted].com>
to [redacted]

Dear [redacted].

You are now enrolled in [redacted]. You must complete this training by [redacted].

The assignments you've been enrolled in are displayed below:

- Phishing Fundamentals

Please use this link to start your training:
https://[redacted].com/ui/login/YXlxvb2x1d2uEuYXlvb2xxhQGcNvab2xirZXQuY29t

Figure 20. Link to the Email Training sent to repeat clickers