UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

DIEGO AUGUSTO DE ARAUJO MADEIRA

INVESTIGATING FACTORS AND GOOD PRACTICES TO IMPROVE THE EFFECTIVENESS OF PHISHING AWARENESS

Recife
2024

DIEGO AUGUSTO DE ARAUJO MADEIRA

INVESTIGATING FACTORS AND GOOD PRACTICES TO IMPROVE THE EFFECTIVENESS OF PHISHING AWARENESS

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de mestre em Ciência da Computação. Área de Concentração: Engenharia de Software e Linguagens de Programação

Orientadora: Carina Frota Alves

Recife

2024

.Catalogação de Publicação na Fonte. UFPE - Biblioteca Central

Madeira, Diego Augusto de Araujo.
Investigating Factors and Good Practices to Improve the Effectiveness of Phishing Awareness / Diego Augusto de Araujo Madeira. - Recife, 2025.
12f.: il.

Universidade Federal de Pernambuco, Centro de Informática, Programa de Pós-Graduação em Ciência da Computação, 2024.
Orientação: Carina Frota Alves.
Inclui referências e apêndices.

1. Phishing; 2. Cibersegurança; 3. Segurança da Informação. I. Alves, Carina Frota. II. Título.

UFPE-Biblioteca Central

Diego Augusto de Araujo Madeira

“INVESTIGATING FACTORS AND GOOD PRACTICES TO IMPROVE THE EFFECTIVENESS OF PHISHING AWARENESS”

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação. Área de Concentração: Engenharia de Software e Linguagens de Programação.

Aprovado em: 16/12/2024.

BANCA EXAMINADORA

_____

Prof. Dr. Hermano Perrelli de Moura
Centro de Informática / UFPE

_____

Profa. Dra. Flávia Maria Santoro
Instituto de Matemática e Estatística / UERJ

_____

Profa. Dra. Carina Frota Alves
Centro de Informática / UFPE
(**orientadora**)

ACKNOWLEDGMENTS

I am grateful to my wife, Renata, for her infinite encouragement and support, and to my family for their understanding and patience throughout this journey. To my son, Miguel, I owe my deepest thanks for his patience and for inspiring me to aspire to be a better person so that I may be an example to him. I also thank my colleagues who inspired me to get on this path: Iveruska, Moises, and Marcelo. I am especially thankful to Carina, who guided and illuminated my way during this process.

AGRADECIMENTOS

Sou grato à minha esposa, Renata, por seu incentivo e apoio infinitos, e à minha família pela compreensão e paciência ao longo desta jornada. Ao meu filho, Miguel, agradeço profundamente por sua paciência e por me inspirar a aspirar ser uma pessoa melhor, para que eu possa ser um exemplo para ele. Agradeço também aos meus colegas, Iveruska, Moises e Marcelo, que me motivaram a trilhar este caminho. Sou especialmente grato à Carina, que guiou e iluminou meu percurso durante todo esse processo.

RESUMO

Phishing é um ataque direcionado que utiliza mensagens fraudulentas para enganar usuários, com o objetivo de obter informações restritas ou instalar softwares maliciosos, tornando-se uma das principais ferramentas utilizadas por cibercriminosos no ambiente digital. Funcionários de diversas organizações são frequentemente alvos desses ataques, representando uma ameaça significativa tanto para si mesmos quanto para suas organizações. Como resposta, as organizações investem recursos, tempo e esforço em Treinamento de Conscientização em Segurança (SAT) voltado para a prevenção de *phishing*. Os programas de SAT incluem simulações de ataques de *phishing* e treinamentos para ajudar os indivíduos a reconhecerem tentativas de *phishing*. No entanto, a efetividade real dessas iniciativas permanece pouco explorada. Para investigar os fatores que contribuem para a eficácia dos programas de SAT, realizamos um estudo de caso em uma organização pública, investigando como a utilização de simulações de *phishing* e a aplicação de treinamentos impacta a capacidade dos colaboradores de identificar essas ameaças. O estudo de caso foi realizado em quatro fases. Na primeira fase, planejamos os processos de design, implementação e avaliação da intervenção. Na segunda fase, conduzimos um estudo quantitativo com 4.457 participantes para medir a suscetibilidade dos indivíduos a ataques de *phishing* e seu engajamento com o SAT voltado à prevenção de *phishing*, utilizando a plataforma KnowBe4. Na terceira fase, realizamos entrevistas qualitativas com 20 participantes da organização estudada para analisar suas experiências, percepções e motivações relacionadas aos esforços de prevenção de *phishing* no âmbito do programa de SAT. Na quarta fase, propusemos um conjunto de boas práticas fundamentadas nos achados dos estudos quantitativo e qualitativo. Nosso estudo de caso destaca os principais fatores que influenciam a eficácia do SAT e apresenta boas práticas projetadas para melhorar as estratégias de prevenção contra *phishing*.

Palavras-chave: Phishing, Cibersegurança, Programas de Conscientização, Segurança da Informação.

ABSTRACT

Phishing is a targeted attack that uses fraudulent messages to deceive users to obtain restricted information or install malicious software, making it one of the main tools cybercriminals use in the digital environment. Employees from various organizations are often the target of phishing attacks, representing a significant threat to themselves and their organizations. In response, organizations invest resources, time, and effort in structured initiatives aimed at enhancing users' ability to identify and respond to such threats, described as Security Awareness Training (SAT), which includes simulated phishing attacks and training to help individuals recognize phishing attempts. However, the actual effectiveness of these initiatives remains underexplored. To investigate the factors contributing to the effectiveness of SAT programs, we conducted a case study at a public organization, allowing us to assess the impact of the intervention on users' ability to recognize phishing attempts. The case study was performed in four phases. In the first phase, we planned the design, implementation, and evaluation processes of the intervention. In the second phase, we conducted a quantitative study with 4,457 participants to measure individuals' susceptibility to phishing attacks and their engagement with Security Awareness Training designed for phishing prevention using the KnowBe4 platform. In the third phase, we conducted qualitative interviews with 20 participants from the studied organization to analyze their experiences, perceptions, and motivations regarding phishing prevention efforts within the SAT program. In the fourth phase, we proposed a set of good practices informed by the findings from both the quantitative and qualitative studies. Our case study highlights the main factors influencing SAT effectiveness and presents good practices designed to improve phishing prevention strategies.

Keywords: Phishing, Cybersecurity, Awareness Programs, Information Security.

LIST OF FIGURES

Figure 1 - Number of Malicious URLs 15
Figure 2 - Victims by age group. 19
Figure 3 - Phishing Classification Techniques 21
Figure 4 - A Basic Flow of Social Engineering-Based Cyberattacks 22
Figure 5 - Example Homograph Attack Technique 22
Figure 6 - Steps of a Scareware Attack 24
Figure 7 - Training and Generation of Deepfake Content 26
Figure 8 - Growth in Previously Unknown Zero-Hour Attacks 28
Figure 9 - Conscious Competence Ladder 31
Figure 10 - Example of Feedback in a Simulated Phishing 34
Figure 11 - Challenges in Phishing Awareness Programs 35
Figure 12 - Case Study Phases 40
Figure 13 - Knowbe4 Platform 42
Figure 14 - Participants Selection 43
Figure 15 - Phishing for the campaign with Instant Feedback 45
Figure 16 - Phishing Landing Page with Instant Feedback 47
Figure 17 - *Redflags* in the landing page with instant feedback 48
Figure 18 - Phishing for the Campaign without Feedback 49
Figure 19 - Landing page without feedback 49
Figure 20 - Knowbe4 User Training Panel 50
Figure 21 - Data analysis and refinement process 57
Figure 22 - Coding Process Using *Atlas.ti* Platform 58
Figure 23 - Illustration of open coding 59
Figure 24 - Building categories with open coding 59
Figure 25 - Themes, Categories and Codes 60
Figure 26 - Failures in the first hours. 65
Figure 27 - Daily Failures Throughout the Phishing Campaign 65
Figure 28 - Phishing Propensity by Age Group 66
Figure 29 - Training Completion Rate by Group 67
Figure 30 - Training Completion by Group and Approach Type 67
Figure 31 - Training Completion Rate: No Feedback x Instant Feedback 68

Figure 32 - Phishing Propensity after Training.....69
Figure 33 - Age distribution of participants 72
Figure 34 - Forgetting Curve.....94
Figure 35 - Overcoming the Forgetting Curve 94

LIST OF TABLES

Table 1 - Real-life examples of Punycode 24
Table 2 - Qualitative Interviews Overview..... 55
Table 3 - Codes Frequency 61
Table 4 - Types of Phishing 64
Table 5 - Phishing Propensity..... 66
Table 6 - Overall Performance in Phishing Simulations and Training 69
Table 7 - Relationship Between Findings and Proposed Practices 80

SUMMARY

1. INTRODUCTION 12
1.1. RESEARCH CONTEXT 12
1.2. PROBLEM STATEMENT AND RESEARCH QUESTIONS 13
1.3. DOCUMENT STRUCTURE 14
2. BACKGROUND 15
2.1. PHISHING OVERVIEW 15
2.2. PHISHING CONCEPTS AND DEFINITIONS 16
2.3. MOTIVATION OF ATTACKERS 18
2.4. CONSEQUENCES OF PHISHING FOR INDIVIDUALS 19
2.5. CONSEQUENCES OF PHISHING FOR ORGANIZATIONS 20
2.6. PHISHING ATTACK TECHNIQUES 21
2.6.1. Social Engineering 21
2.6.2. Technical subterfuge 25
2.7. COGNITIVE DECEPTION IN PHISHING ATTACKS 28
2.8. Phishing Prevention in Security Awareness Programs 30
2.8.1. Mandatory Training Approach 32
2.8.2. Timing of Feedback 33
2.9. KEY CHALLENGES IN PHISHING AWARENESS 35
2.10. RELATED WORK 37
3. METHODOLOGY 38
3.1. PHASE 1 - PLANNING 40
3.2. PHASE 2 - QUANTITATIVE STUDY 41
3.2.1. Participant Selection 42
3.2.2. Data Collection 44
3.2.3. Data Synthesis 52
3.3. PHASE 3 - QUALITATIVE STUDY 53
3.3.1. Participant Selection 53
3.3.2. Data Collection 54
3.3.3. Data Synthesis 56
3.4. PHASE 4 - GOOD PRACTICES PROPOSAL 61
4. RESULTS 64
4.1. QUANTITATIVE STUDY 64
4.1.1. Initial Simulated Phishing Campaign 64
4.1.2. Training Engagement Measurement 66
4.1.3. Post-Training Simulated Phishing Campaign 68
4.2. QUALITATIVE STUDY 71
4.2.1. Phishing Awareness 72
4.2.2. Training Effectiveness 75
4.3. GOOD PRACTICES PROPOSAL 80
4.3.1. Practice 1 - Adjust Training Content to Different Roles and Knowledge Levels 81
4.3.2. Practice 2 - Implement Strategic Feedback and Continuous Reinforcement 82
4.3.3. Practice 3 - Use Realistic and Scenario-Based Simulations 83
4.3.4. Practice 4 - Link Training to Career Development Initiatives 83
4.3.5. Practice 5 - Optimize the Invitation Process 84
4.3.6. Practice 6 - Adopt a Multi-Channel Communication Strategy 85
4.3.7. Practice 7 - Use Engaging Learning Elements 86

5. DISCUSSION **87**
5.1. MAIN FACTORS 88
5.2. GOOD PRACTICES 91
6. CONCLUSIONS **100**
6.1. THEORETICAL AND PRACTICAL CONTRIBUTIONS 100
6.2. THREATS TO VALIDITY 101
6.3. FUTURE WORK 103
7. REFERENCES **105**
8. APPENDIXES **115**
A - RESEARCH PROTOCOL - SEMI-STRUCTURED INTERVIEW 115
B - SEMI-STRUCTURED INTERVIEW GUIDE 119
C - INFORMED CONSENT FORM 121

1. INTRODUCTION

We introduce the foundation of the research, providing context for understanding phishing as a continuously evolving cybersecurity threat. We explore the psychological and technical tactics employed in phishing attacks and their significant impact on individuals and organizations, emphasizing the importance of addressing human vulnerabilities through targeted security awareness initiatives. Furthermore, we identify critical gaps in the current understanding of phishing prevention strategies, setting the stage for the research questions and objectives of this study.

1.1. RESEARCH CONTEXT

Phishing is a type of cyberattack in which an adversary deceives users into revealing sensitive information, such as passwords or financial details, by posing as a legitimate entity through fraudulent emails or websites (TAIB, 2019). As a form of social engineering, it exploits psychological principles to manipulate user behavior, using tactics like urgency, authority, or familiarity to lower suspicion and trick victims into either installing malicious software or disclosing confidential personal or organizational data (KHERUDDIN, 2024). Social engineering is an art of manipulating people who have less knowledge about information security, phishing attacks and its techniques. This manipulation is done with the aim of acquiring sensitive information or compelling people to undertake specific actions (GUPTA, 2016).

Cognitive distortions are frequently coupled with technical subterfuge in social engineering, as elucidated by Leonov (2021). It serves as an attack mechanism to compromise vital systems within organizations, ultimately aimed at monetary gain, as articulated by ProofPoint (2021). Furthermore, Baig (2021) highlights that perpetrators capitalize on an array of human vulnerabilities, including the pursuit of swift rewards, the inclination to aid others, and a susceptibility to flattery by fraudsters. Additionally, a lack of emotional control emerges as a contributing factor rendering certain individuals more susceptible to becoming easy targets for such schemes.

In 2021, the cost of cybercrime damage was already projected to reach $6 trillion, making it more profitable than the illicit drug trade (METCLOUD, 2021), with expectancy to surge to $23.84 trillion by 2027, up from $8.44 trillion in 2022, according to WORLD ECONOMIC FORUM (2023). In recent years, phishing has emerged as one of the primary vectors of cyberattacks, intensified by its increasing use by cybercriminals. In 2023, the Anti-Phishing Working Group (APWG) recorded nearly 5

million phishing attacks, marking a 6.3% increase compared to the previous year, being the highest number ever recorded. These attacks were responsible for over 91% of data breaches, emphasizing the urgency of effective approaches to mitigate these threats. The most critical aspect of protecting any system lies in human vulnerability, often exploited through social engineering and cognitive biases.

The significance of this study arises from the need to understand and improve phishing prevention in the context of security awareness training programs. With the growing prevalence of phishing attacks and their devastating consequences, it is imperative to develop effective methods to educate and protect users against such threats. Given the direct influence of security awareness on the effectiveness of protective measures, this study aims to provide insights for strengthening security policies within organizations.

1.2. PROBLEM STATEMENT AND RESEARCH QUESTIONS

Despite the recognized importance of phishing prevention in the context of security awareness training programs (BAUER, 2015; ALSHAIKH, 2020; ASSENZA, 2020; KWEON, 2021) there is a significant gap in understanding how these programs are structured and their effectiveness in preventing phishing attacks. Currently, little is known about the specific characteristics of these programs, their implementation strategies, and methods for evaluating their effectiveness (KÄVRESTAD, 2021). This dissertation aims to fill this gap by providing a thorough analysis of current information security awareness training practices, including program structures, delivery methods, and evaluation techniques, and by suggesting improvements to increase their effectiveness in preventing phishing attacks.

This dissertation aims to investigate the following research questions:

RQ1: What are the main factors that contribute to the effectiveness of phishing prevention strategies in security awareness training programs?

RQ2: What are the good practices to improve the effectiveness of phishing prevention strategies in security awareness training programs?

We seek to investigate the key aspects that influence the effectiveness of phishing prevention strategies in security awareness training programs, focusing specifically on how the inclusion of mechanisms like feedback impacts participants' engagement in the training and their knowledge retention. Our objective is to determine

whether providing immediate feedback when participants fall for a simulated phishing attempt enhances their learning experience and thereby improves their ability to recognize and respond to real phishing threats. Furthermore, this research aims to explore how the structure of the training—whether delivered through mandatory or non-mandatory formats—affects the willingness of participants to engage meaningfully with the content.

We aim to identify effective practices that enhance the effectiveness of phishing awareness training programs. We explore how factors such as training frequency, content relevance, communication, and the inclusion of practical exercises influence their engagement and learning. The findings highlight which approaches result in improved training performance, building a set of recommendations that can help organizations optimize their strategies in preventing phishing attacks.

1.3. DOCUMENT STRUCTURE

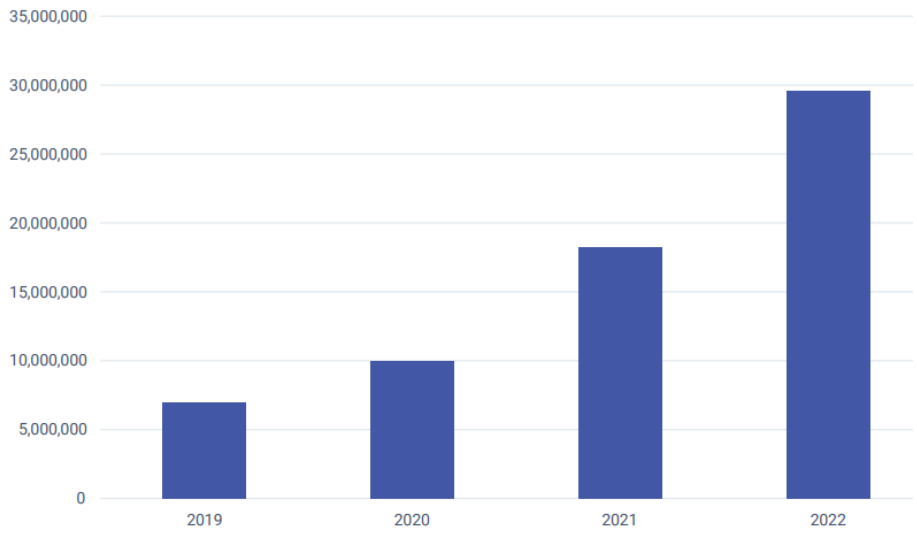
This dissertation is divided into six chapters. Chapter 2 describes the theoretical background of the literature on phishing and its consequences, discusses email-based socio-technical attacks, cognitive deception in phishing attacks, awareness programs, and key challenges. Chapter 3 explains the research methodology adopted to conduct the study, the research planning to investigate the research questions, presents the quantitative and qualitative studies. Chapter 4 presents the results of the quantitative study based on the phishing simulations and training deployed, and we also present the findings from the semi-structured interviews within the qualitative study. Chapter 5 presents a discussion about main factors for security awareness training designed to prevent phishing and good practices proposed by the study. Finally, Chapter 6 concludes the dissertation, summarizing the main findings, explaining how the study contributes to security awareness programs, and discussing the limitations and insights for future research.

2. BACKGROUND

2.1. PHISHING OVERVIEW

Phishing stands as one of the principal vectors of cyber-attacks and has emerged as the most widely utilized attack vector by cybercrime recently, as highlighted by the FBI. In 2022 alone, there were over 255 million recorded instances of phishing, marking a substantial 61% surge compared to the preceding year, as reported by SlashNext. This alarming escalation resulted in over 91% of data breaches (KNOWBE4b, 2022). The efficacy of phishing hinges upon cybercriminals' ability to deceive individuals and compel them to act against their own best interests.

Figure 1 - Number of Malicious URLs



Source: SlashNext (2022)

The most significant vulnerability in safeguarding any system resides within its users. The human mind is not infallible, attributable in part to cognitive distortions, commonly referred to as "*human thinking errors*" (LEONOV, 2021). Attackers skillfully take advantage of these distortions in different combinations to create strategies for launching attacks by carefully examining the vulnerabilities and susceptibilities of individuals or groups who have access to the restricted information. Through the exploitation of these pinpointed "weak points," hackers can obtain specific data or confidential information. This practice forms the foundation of what is known as social engineering.

For JARI (2022), phishing constitutes a sophisticated form of social engineering attack aimed at illicitly acquiring victim data, encompassing personal information and even relevant credentials such as credit card numbers. This malicious activity is

engendered when a malicious actor falsely assumes the identity of a trusted entity, whether individual or organization, skillfully persuading the victim to engage by responding to a message or accessing a malicious website. Opening this communication exposes the vulnerability of the individual target's information, thereby compromising the security of their device and data.

Phishing exploits a variety of human weaknesses, including the desire for quick rewards, the willingness to assist others, and the longing for approval from criminals (BAIG, 2021). Lack of emotional control is a factor that can make individuals more inclined to become victims. While organizations allocate resources to meet their technological requirements, processes contingent on human actions are often overlooked. Within this context, the policies adopted by organizations regarding their user awareness programs in information security have a significant impact on the effectiveness of security measures. As such, these programs represent preventive measures and prove indispensable in fostering a robust organizational culture (SAS, 2021).

2.2. PHISHING CONCEPTS AND DEFINITIONS

Phishing poses an escalating threat to information security and personal privacy in the digital realm, representing a malicious form of social engineering that combines diverse techniques to achieve its objectives. However, despite its widespread prevalence and societal relevance, it is intriguing to note that the term "phishing" can assume various meanings and interpretations according to authors and subject matter experts. These conceptual divergences may be linked to technical, contextual, and even cultural nuances, rendering the study and comprehension of this phenomenon more complex. In this context, different perspectives on phishing are explored, seeking to understand its variations and implications for this research.

According to the Federal Trade Commission (FTC), a U.S. government agency investigating unfair or fraudulent business practices to enforce the law and protect consumer rights, phishing is a cyber-attack technique that involves attempting to deceive individuals into revealing confidential information, such as passwords, credit card numbers, or personal data. Cybercriminals masquerade as trustworthy entities like banks, companies, or government organizations, sending fake messages via

email, instant messaging, or phone calls to persuade people to share sensitive information (FTC, 2022).

The term phishing is commonly used in literature (LASTDRAGER, 2014). In many instances, the phenomenon is explicitly defined, while in others, it is conveyed through examples, assuming prior reader familiarity with the concept. Consequently, the author offers a conceptual definition after conducting a systematic review that incorporates 113 predefined criteria. The systematic review leads to the conclusion that "*phishing is a scalable act of deception whereby impersonation is used to obtain information from a target*." This definition serves to provide an understanding of the term, including its various dimensions and characteristics as revealed through a rigorous evaluation of existing literature and criteria.

The most adopted definitions of phishing emphasize the use of social engineering and technical subterfuge, such as malware infection, as primary strategies. In contrast, classic definitions focus on the theft of personal information online without specifying the method used. These conclusions were reached through a systematic analysis of 100 articles written between 2006 and 2022, which aimed to clarify the concept of phishing by examining Natural Language Processing (NLP) techniques for its detection (SALLOUM 2022).

Phishing is a socio-technical attack that exploits vulnerabilities to achieve specific goals by introducing a threat into the victim's system through a determined method, often using social engineering to persuade the victim to act in a way that results in harm. Current definitions primarily focus on mechanisms and countermeasures, neglecting the phishing lifecycle. To address this, a detailed phishing anatomy was proposed, considering attack phases, attacker types, threats, targets, and techniques (ALKHALIL, 2021).

The definition of phishing can be approached from various perspectives, considering the techniques employed in different attack stages and strategies to exploit system vulnerabilities or deceive users. However, at its core, phishing is consistently characterized as a threat that exploits the combination of system and human vulnerabilities to acquire resources from victims, which involves communication, whether via email, text, audio, video, conferencing, AI-generated simulations of people, or any other forms of electronic communication that appear legitimate, often mimicking well-known brands, organizations, or individuals, with the intent to deceive victims into

providing confidential information such as passwords, credit card numbers, personal data, system or service credentials, access authorizations, or any form of personal or restricted access resource.

2.3. MOTIVATION OF ATTACKERS

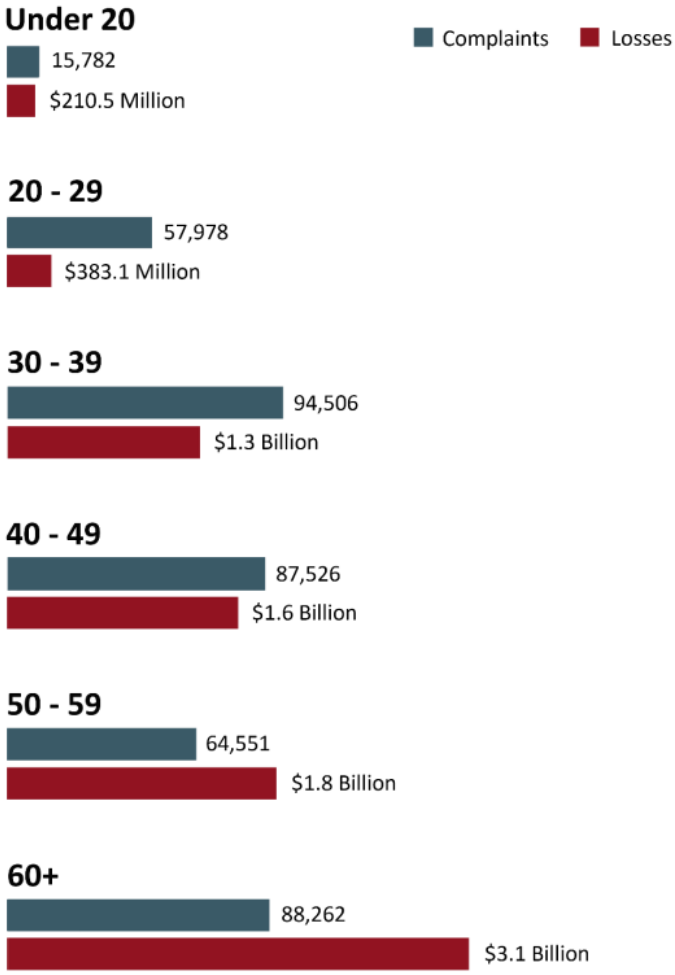
Phishers exploit individuals' tendency to overlook critical warning messages, taking advantage of society's lack of awareness about phishing attacks, which has greatly contributed to their success. Despite researchers' efforts to develop techniques to combat these attacks, phishers continuously seek out vulnerabilities to maintain their effectiveness (GUPTA, 2017). While financial gain remains a primary motive for phishing, other factors also incentivize these criminals:

- **Theft of login credentials**: phishers steal login details for online services like eBay, Amazon, and Gmail by sending deceptive emails posing as warnings, urging users to alter passwords via provided hyperlinks.
- **Theft of banking credentials:** online banking credentials and credit card specifics, including card numbers, expiry dates, cardholder names, and CVV numbers, are targeted from reputable institutions like PayPal, OnlineSBI, HDFC, and Citibank.
- **Capture of personal information:** personal data, such as addresses and phone numbers, hold considerable market value and are eagerly sought after by direct marketing companies.
- **Theft of trade secrets and confidential documents:** employing spear-phishing tactics, perpetrators specifically target organizations to acquire proprietary information that can be utilized directly or sold to interested parties.
- **Fame and notoriety:** an intriguing psychological facet of phishing involves obtaining information not for monetary gain, but for the sake of recognition and infamy within their peer circles.
- **Exploiting security vulnerabilities:** individuals driven by curiosity to test the resilience of certain systems might develop programs to breach others' systems, launching phishing attacks or selling compromised systems to fellow phishers.
- **Attack propagation:** phishers can leverage a single compromised host as an internal "jump point" within an organization, facilitating future attacks through a combination of spear-phishing and the installation of bot agents.

2.4. CONSEQUENCES OF PHISHING FOR INDIVIDUALS

Phishing results in the highest financial losses among individuals aged 60 and older, totaling $3.1 billion and affecting 88,262 victims, highlighting the significant impact of phishing scams on senior citizens and emphasizes the urgent need for stronger cybersecurity measures and targeted educational initiatives to reduce these risks (FBI, 2022), as shown in Figure 2.

Figure 2 - Victims by age group.



Source: FBI Internet Crime Report (2022)

This form of cyberattack poses a serious risk not only because of its prevalence but also because of its widespread impact. Understanding these risks is a pre-active measure that is essential to guard against this threat. Below are some of the most common impacts for individuals associated with phishing:

- **Identity theft:** phishing can result in several consequences for its victims, such as identity theft, where criminals exploit stolen data for

financial fraud, opening fraudulent accounts, compromising an individual's reputation, or gaining advantages such as extorting money (FTC, 2022).

- **Financial loss:** another ramification, involving fraudulent activities like obtaining banking data, such as credit card numbers or credentials in electronic payment services, leading to monetary repercussions (The United States Department of Justice).
- **Compromised online security:** arises as phishing infiltrates online user services, enabling fraudulent activities, unauthorized access to various platforms, including social networks, email, financial services, and shopping, or even acquiring privileged access to sensitive data for targeted attacks (KASPERSKY, 2024).

2.5. CONSEQUENCES OF PHISHING FOR ORGANIZATIONS

In 2022, phishing reached unprecedented levels, with over 4.7 million attacks documented by the APWG (2022). Notably, October 2022 marked a significant milestone, with a staggering 101,104 distinct email subjects, representing the highest monthly sample ever observed. The consequences of falling victim to phishing attacks are multifaceted and pose significant challenges for organizations. As phishing continues to evolve as a sophisticated threat, understanding and mitigating these multifaceted risks are imperative for organizations seeking to safeguard their assets and reputation. We present some of the most common impacts for organizations caused by phishing attacks:

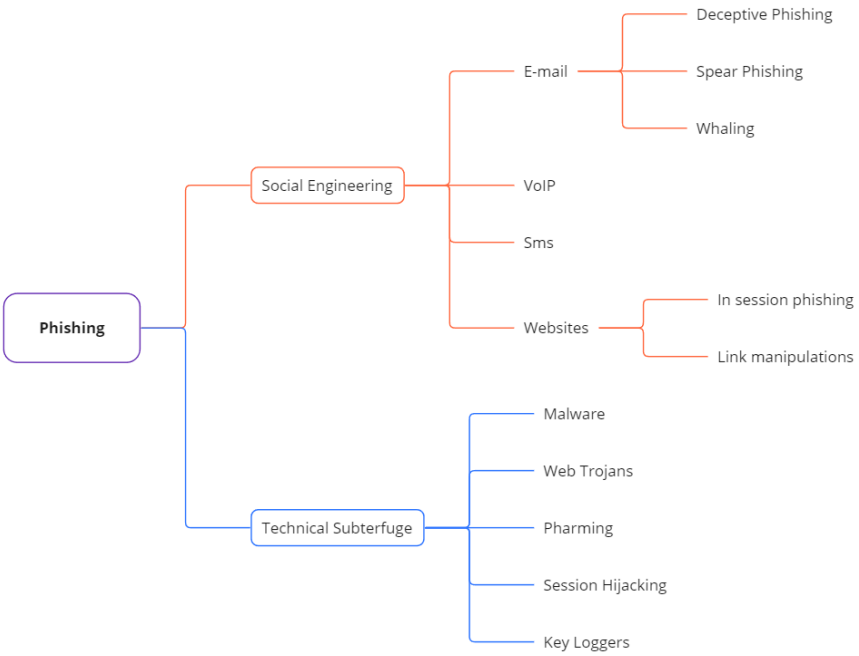
- **Data loss:** through successful phishing attempts can potentially result in the compromise of sensitive information, leading to financial losses through extortion, data breaches, loss of intellectual and commercial property, and the sale of classified data to criminal organizations (VERIZON, 2019).
- **Reputation damage:** whereby the erosion of customer trust can tarnish an organization's standing and impact its relationships with partners, potentially resulting in loss of customer trust, which may also negatively impact business relationships with partners and the organization's overall image (IBM, 2020).

- **Financial losses:** extend to encompass both direct monetary losses from fraudulent activities and the costs associated with recovering from these attacks, coupled with potential legal penalties, such as fines or breaches of contractual clauses with clients and partners, or those imposed by data protection authorities due to data breaches (BROADCOM, 2019).

2.6. PHISHING ATTACK TECHNIQUES

Phishing attacks employ a variety of techniques to achieve their goals. Athulya (2020) categorizes these techniques into two groups: Social Engineering and Technical Subterfuge. Figure 3 depicts this classification.

Figure 3 - Phishing Classification Techniques



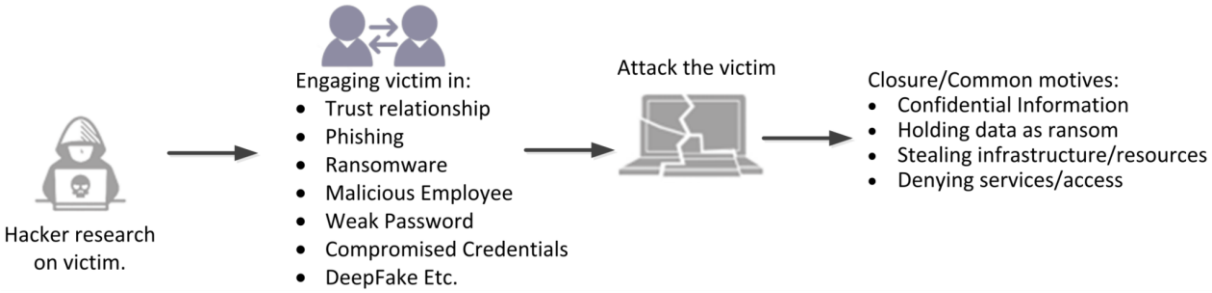
Source: Adapted from Athulya (2020)

2.6.1. Social Engineering

The concept of social engineering is closely related to the field of information security, where it is recognized as a powerful means of gaining information by exploiting individuals' weaknesses (CORRADINI, 2020). It is often regarded as the art of persuading individuals to reveal confidential information (MOUTON, 2018). Social engineering attacks often rely on psychological and mental manipulation to deceive individuals into revealing sensitive data (KHIDZIR, 2019).

Security experts face a significant challenge in responding to social engineering attacks because of their unpredictable nature. Targets often remain unaware of manipulation. Despite technological advancements, humans remain exploitable in organizational security (SIDDIQI, 2022). Figure 4 depicts common resources, and the basic flow of social engineering cyber-attacks:

Figure 4 - A Basic Flow of Social Engineering-Based Cyberattacks

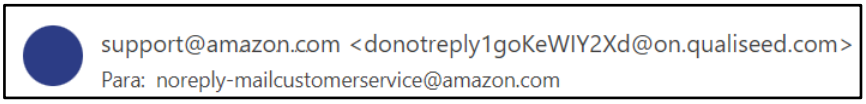


Source: SIDDIQI (2022)

We present various types of phishing attacks that demonstrate the diverse strategies employed by cybercriminals to deceive users and compromise security. Below are some common phishing attack variants, illustrating the range of tactics used to manipulate victims into revealing sensitive information or taking harmful actions:

1) **Deceptive phishing:** involves sending emails that mimic the logos or websites of trusted financial institutions and other reputable entities, aiming to induce users to click on them (ATHULYA, 2020). Within these attack scenarios, users might be deceived by the structure of the domain name. It can be combined with other techniques, for instance *support@am.azo.n.c,.om* was written using Unicode characters that mimic ASCII to deceive a user, enabling the attacker to acquire data. This technique is called homograph attack, as shown in Figure 5.

Figure 5 - Example Homograph Attack Technique



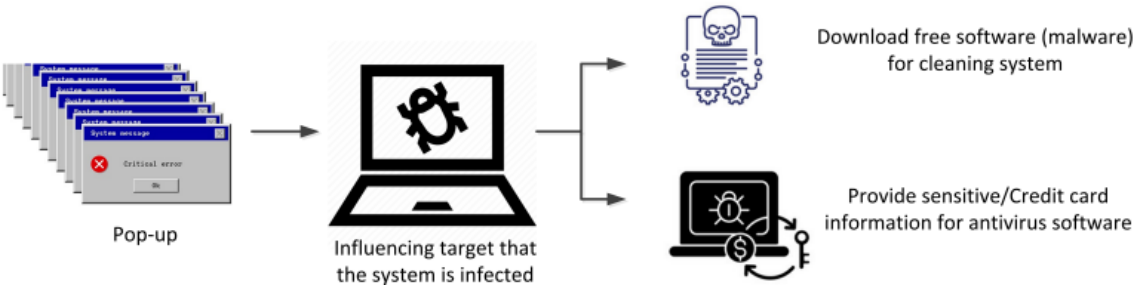
Source: The Author (2023).

2) **Spear phishing:** often adapted to target individuals or small groups, are characterized by iterative phases of reconnaissance and attack engineering, coupled with the sophistication of the artifacts employed in the endeavor

(ALLODI, 2020). This type of attack can be difficult for detection and response solutions to identify, as the usual components of phishing may be spread across various communication vectors such as email, text messages, websites, instant messaging, and password-encrypted files.

3) **Whaling:** attacks target high-level executives like head of HR, C-level executives such as CISO, CTO, CFO or board members. These attacks are highly risky as executives have access to the most confidential company information (BHARDWAJ, 2020).
4) **VoIP:** or Vishing - phishing with Voice over IP - is a form of phishing conducted through phone calls. In this scheme, the attacker poses as a legitimate caller, fabricates a problem, and pressures the target to swiftly resolve it by divulging account details. Upon initiating the call, the attacker guides users to input sensitive bank account information like PIN, account number, One Time Password, and more (YEBOAH, 2014).
5) **In Session phishing:** exploits the credibility of a genuine website by using pop-up messages that appear during an ongoing session. These pop-ups might display messages like *'session timed out*,' *'reset your password*,' or *'log in again*.' Since these messages appear to originate from the legitimate site, users tend to provide their information, inadvertently sending their login credentials to the attackers instead of the legitimate servers (EISEN, 2009).
6) **Scareware:** a form of social engineering attack leveraging human emotions like anxiety and shock. This manipulation exploits users' feelings to coerce them into installing malicious software.. Once clicked, misinformation prompts panicked actions, such as sharing sensitive data or purchasing a supposed solution. The hacker's aim is to convince the victim to click a link, utilizing diverse techniques to manipulate them. The graphical interface of scareware is vital in deceiving victims, often mimicking trusted brands' appearances for credibility, incorporating color schemes, fonts, and logos resembling renowned antivirus or software products like Microsoft and Norton antivirus. Figure 6 outlines the steps in a scareware attack, wherein hackers employ pop-up alerts on various sites to engage targets.

Figure 6 - Steps of a Scareware Attack



Source: SIDDIQI (2022)

7) **Link manipulation:** known as Homograph phishing attacks, involve URLs that appear legitimate, with the page content mimicking the original, but leading to a distinct website designed to steal sensitive data or compromise the user's device. This manipulation is achieved using puny codes. A puny code is a method of transforming words that cannot be represented in ASCII into Unicode ASCII-encoded characters. Attackers can create a domain name that substitutes certain ASCII letters with Unicode letters. Many web browsers utilize the *xn*— prefix, an ASCII encoding indicator, to signify puny code domains. This precautionary measure helps guard against Homograph phishing attacks. However, not all browsers display the puny code prefix, creating an opening for hackers to exploit this vulnerability. This technique is shown in Table 1.

Table 1 - Real-life examples of Punycode

Brand	What the user sees	The Punycode
Adidas	adıdas.de	http://xn--addas-o4a.de/
Aerlingus	aerl̨ingus.com	xn--aerlngus-j80d.com
Aerlingus	aer̨lingus.com	xn--aelingus-of0d.com
Air France	airfr̨ance.com	xn--airfrnce-rx0d.com
British Airways	britishairẇays.com	xn--britishairays-541g.com
British Airways	britisha̧irways.com	xn--britishirways-of2g.com
Google	gooǵle.com	xn--googe-95a.com

Source: www.jamf.com/blog/punycode-attacks/

8) **Business Email Compromise (BEC):** a sophisticated form of cyber fraud targeting businesses conducting wire transfers. Fundamentally, BEC involves utilizing social engineering tactics or hacking to illicitly gain access to corporate

email accounts and then using these accounts to induce company employees to execute fund transfers to criminal-controlled accounts. These scams are notoriously difficult to detect as they often involve emails that appear legitimate, originating from known superiors or colleagues (FBI, 2022).

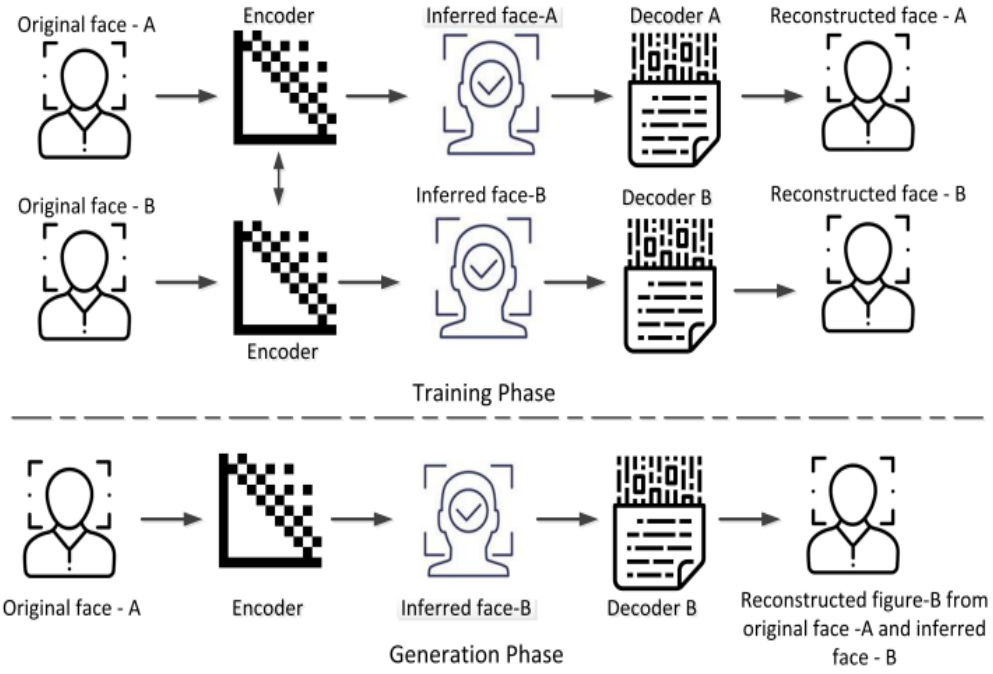
2.6.2. Technical subterfuge

These Technical subterfuge attacks involve the installation of malicious software on the victim's device, with the primary objectives of stealing credentials and manipulating local and remote network traffic to redirect users to fake websites controlled by phishers (ATHULYA and PRAVEEN, 2020). We discuss the following types of phishing that fit into this category:

1) **Malware:** designed to compromise computer systems, can spread through various methods, such as email attachments or hidden in multimedia files on websites. It can also exploit security vulnerabilities in outdated software that hasn't been patched, allowing attackers to infiltrate systems and carry out malicious activities (ZAHRA, 2022).
2) **Web trojans:** operate by surreptitiously appearing when users initiate login procedures. These insidious elements covertly amass the entered credentials from the user, subsequently relaying this sensitive information to the phishing perpetrator.
3) **Pharming:** entails the transmission of code to the target either via email or links, which subsequently alters the entire system's *localhost* data. This manipulation involves converting URLs into numeric strings, which the system uses to reach web pages. Consequently, the target's redirection to the malevolent site occurs, even if the correct URL is entered. Another avenue for pharming involves DNS Poisoning, wherein the local host files of the network remain unchanged, but the domain name system's table is altered. This manipulation results in redirecting the target to malicious websites (SHANKAR, 2019).
4) **Session hijacking:** refers to an attack that involves monitoring a user's activities until they log into a specific account or initiate a transaction. Attackers then acquire legitimate user credentials. Subsequently, they gain control over the session and wield malicious software to execute unauthorized actions, such as fund transfers, without the user's awareness (VILELA, 2022).

5) **Keyloggers:** Keyloggers and Screen loggers represent distinct forms of malware designed to monitor keystrokes and capture valuable data, which is then sent to the hacker via the Internet. These specialized utilities integrate into user browsers, initiating automatically upon browser launch, and embedding themselves within system files, device drivers, and related components (VILELA, 2022).
6) **Deepfake:** is a highly convincing technique employed in social engineering attacks by cybercriminals. This emerging cybersecurity threat utilizes generative adversarial networks (GANs), a combination of two artificial neural networks - detectors and synthesizers - trained on real image, audio, and video datasets. The synthesizer ANN creates deceptive content, while the detector ANN strives to determine authenticity. This iterative process aims to produce undetectable forged content. An illustrative overview of the deepfake creation process involves training a network with different faces and generating images with blended expressions or audio to confuse victims. Notably, deepfakes have been notably exploited for scams, blackmail, reputation damage, fake news, misinformation, and causing mass panic in various criminal activities (SIDDIQI, 2022). This technique is shown in Figure 7.

Figure 7 - Training and Generation of Deepfake Content



Source: Siddiqi et al (2022)

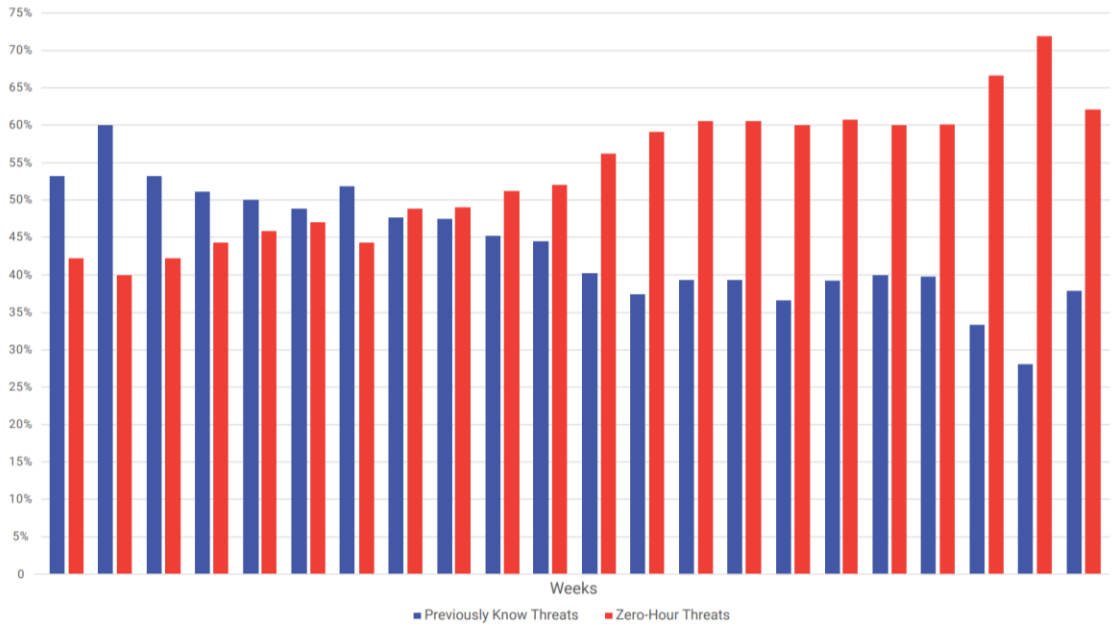
7) **ZERO-HOUR THREAT**

The urgency of raising user awareness is critical when confronting zero-hour threats, which are designed to cause significant harm before conventional security measures can detect and mitigate them. These attacks are particularly concerning due to their effective exploitation of credential theft (SLASHNEXT, 2022).

A staggering 76% of the zero-hour attacks detected were focused on spear phishing, with the sole purpose of stealing credentials. This distressing statistic underscores the pivotal role that credential harvesting plays in initiating a chain reaction of malicious activities—ransomware extortion, data exfiltration, and insidious cyber espionage. However, the most striking revelation of 2022 lies in the meteoric surge of zero-hour threats, those that materialize from the shadows without any precedent. For example, in the zero-hour threat landscape, attackers exploit ChatGPT's cost-effectiveness and user-friendliness to swiftly enhance rapid deployment phishing attacks, complicating large-scale detection and mitigation by security vendors. Moreover, ChatGPT's simplicity empowers attackers with varying technical skills to create evasive phishing tactics, encompassing techniques like text encoding, browser fingerprinting, and clickjacking, evading standard anti-phishing protocols (ROY, 2023).

The escalating sophistication of attackers is evident, with 54% of the threats identified in 2022 falling into the elusive zero-hour category, marking a 48% increase from the end of 2021. This surge highlights how cybercriminals are developing tactics that go undetected until they strike. The gap between threats uncovered through threat intelligence and those intercepted by real-time scanning underscores the adaptability of these attackers (SLASHNEXT, 2022). Figure 8 illustrates the weekly distribution of previously known threats versus zero-hour threats, showing a clear dominance of zero-hour threats throughout the observed period, with a significant upward trend in the later week:

Figure 8 - Growth in Previously Unknown Zero-Hour Attacks



Source: SlashNext (2022)

Phishing attacks exploit gaps in user awareness to achieve their objectives (MAHAJAN, 2018). As threat actors continuously refine techniques to bypass existing security measures (DIVAKARAN, 2023), developing targeted awareness programs becomes critical essential for enhancing the resilience of organizations (SUTTER, 2022). The effectiveness of these programs relies on aligning training content with the dynamic threat landscape, ensuring users can recognize and respond to new and sophisticated phishing strategies. Establishing a security-aware culture not only minimizes the risk of successful attacks but also transforms users into active participants in the organization's security posture. This is particularly important for defending against zero-hour threats, which exploit vulnerabilities before traditional security measures can react, making user aware of the critical frontline defense in such scenarios.

2.7. COGNITIVE DECEPTION IN PHISHING ATTACKS

Mental models refer to the cognitive representations that individuals construct to comprehend and interpret the world around them. These models are based on an individual's learning, experience, skills, and knowledge, enhancing the thought process, and resulting in specific behaviors or outcomes. In simple terms, it is an

individual's thought process regarding how a particular phenomenon functions in a real-life scenario (JARI, 2022).

Cybercriminals capitalize on victims' beliefs, expectations, and pre-existing knowledge to make their attacks more effective. They craft phishing messages that align with what people expect to see from legitimate sources, thus exploiting users' mental models. For instance, a phishing email might impersonate a bank and claim that the user's account is compromised, leading them to believe the message is genuine and prompting them to provide personal information.

Cognitive models play a pivotal role, and various models can be employed to counter phishing. However, as emphasized by Jari (2022), none of these models can address the issue in isolation. In this context, phishing attacks succeed when attackers manipulate users into forming inaccurate mental models of an online interaction (DOWNS, 2006).

Despite numerous studies on mental models aimed at enhancing detection and response mechanisms in phishing combat, the numbers of successful attacks increase each year. To achieve this outcome, criminals have employed more sophisticated techniques to circumvent system security safeguards. Additionally, they employ social engineering techniques using contextualized personal data to persuade users into undesirable actions or divulging confidential information (BURDA 2020).

Cognitive biases, which are mental shortcuts that simplify information processing but may not always align with reality, play a significant role in influencing thoughts, behaviors, and decision-making. Hackers exploit these biases by using deceptive information to manipulate decisions, such as enticing employees with fake coupons or messages appearing to be from managers, leading them to click on malicious links or reveal sensitive company information. This manipulation is based on nine common biases that subtly shape human judgment (KNOWBE4a, 2022), which often exploit the habits of human psychology:

1. **Hyperbolic Discounting**: preferring immediate rewards (e.g., "*Free coupon*") over delayed ones.
2. **Habit**: exploiting users' routines, using regular communications like a "*Daily delivery report*."
3. **Recency Effect**: focusing on recent events, such as the "*COVID-19 vaccination*" lure.

4. **Halo Effect**: leveraging trust in familiar entities, like "*Apple*" messages.
5. **Loss Aversion**: urging action to avoid losses, such as "*Save your credit score*."
6. **Ostrich Effect**: prompting fear-driven quick fixes, e.g., "*Clean up your computer*."
7. **Authority Bias**: manipulating by impersonating authority figures, like a "*CEO*."
8. **Optimism Bias**: overestimating positive outcomes, as in a "*30% pay raise*."
9. **Curiosity Effect**: exploiting the desire to resolve uncertainty, even if risks are expected, such as a "*Secret offer - click here*."

2.8. Phishing Prevention in Security Awareness Programs

In the digital era, phishing poses a significant and pervasive threat, targeting both individuals and organizations through various channels such as emails, social media messages, and fraudulent websites (APWG, 2023). These attacks rely heavily on social engineering, making them particularly challenging to detect. This complexity highlights the need for thorough prevention strategies. One of the most effective approaches is Security Awareness Training (SAT), which equips users with the knowledge to identify phishing tactics and raises a proactive attitude, reducing the likelihood of falling victim to such exploits (SIDDIQI, 2022; WANG, 2021).

Security Awareness Training programs are structured initiatives aimed at enhancing users' ability to identify and respond to security threats effectively (ALYAMI, 2023). SAT programs are designed to cultivate a proactive cybersecurity culture, promoting shared responsibility for maintaining information security across the organization. According to KRUGER & KEARNEY (2006), SAT involves using various communication methods, such as posters, simulations, and interactive modules, to keep employees informed about evolving threats and safe practices.

No comprehensive data is available regarding the total number of Security Awareness Training (SAT) programs implemented worldwide. However, individual initiatives from major organizations like Microsoft provide an understanding into the growing adoption of these programs. Microsoft has launched extensive cybersecurity training addressing the increasing demand for professionals in the field. To date, the company has trained over 400,000 individuals worldwide (Microsoft, 2024).

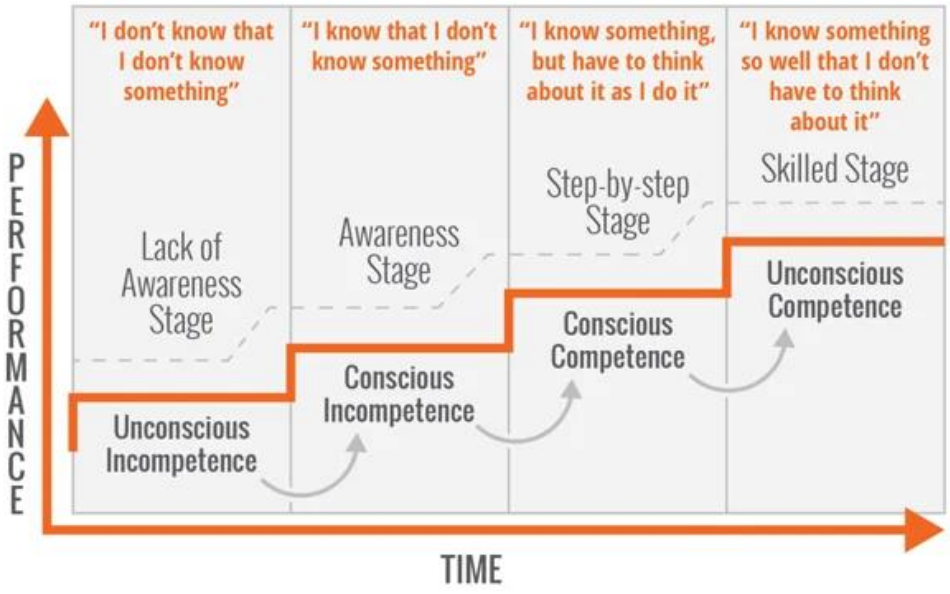
At a more advanced level, SAT programs include specialized training modules focusing on practical scenarios that reinforce skills like identifying phishing emails,

recognizing social engineering attempts, and adhering to secure practices in daily activities (AMANKWA, 2014). The success of SAT programs depends on clear objectives, ongoing reinforcement, and continuous evaluation to adapt the training content to emerging threats.

Through structured SAT programs, users learn to identify phishing indicators such as misspellings, unusual grammar, and suspicious URLs (ARDUIN, 2021). HADNAGY and FINCHER (2021) emphasize that raising awareness strengthens users' ability to detect sophisticated attacks, while HAGEN. (2011) found that SAT also improves digital hygiene, lowering the likelihood of falling for phishing attempts by promoting safer online behavior.

To further develop the effectiveness of SETA programs, it is important to examine how individuals evolve in their understanding and application of cybersecurity measures through the lens of the Four Stages of Competence (KNOWBE4c, 2024) described by Noel Burch in the 1970s, which remains a robust framework for understanding skill acquisition and personal development within educational and professional settings. This psychological model represented in Figure 13 provides a structured pathway that not only complements the theoretical and practical training efforts of SAT but also maps the gradual transformation from unawareness to skillful competence in security practices.

Figure 9 - Conscious Competence Ladder



Source: Knowbe4C (2024)

In the context of the Competence Ladder, At the *Unconscious Incompetence* stage, users are unaware of phishing risks and their own lack of security knowledge, making them highly susceptible to attacks. Introducing targeted awareness content and running initial phishing simulations allows SAT programs to create a "wake-up call," moving users into the *Conscious Incompetence* stage, where they begin to recognize their vulnerabilities and the need for improvement. Continuous exposure to realistic scenarios and feedback then helps users progress into the *Conscious Competence* stage, where they become capable of identifying phishing attempts but must still actively think through each decision.

As users engage in more frequent and varied simulated phishing exercises, they build confidence and proficiency, eventually reaching the *Unconscious Competence* stage, where recognizing phishing attempts becomes an automatic response. At this final stage, SAT programs achieve their goal of transforming users into vigilant defenders who can respond to phishing without deliberate effort.

Simulated phishing exercises not only facilitate this progression but also serve as effective tools for assessing employees' current stage of competence. Analyzing responses to these exercises allows organizations to identify specific areas of weakness and adjust their training strategies, certifying that personnel evolve from being unaware of security risks to becoming adept at preventing real-world phishing attacks, and reinforcing the organization’s overall security culture.

Security culture is a central element of information security awareness programs, directly influencing employees’ behaviors toward threats like phishing. Carpenter and Roer (2022) emphasize that security culture comprises seven dimensions: attitudes, behaviors, cognition, communication, compliance, norms, and responsibilities. Integrating these dimensions into training programs not only enhances individual capabilities to recognize threats but also creates an organizational environment where security becomes a shared value.

2.8.1. Mandatory Training Approach

Phishing prevention within SAT programs faces significant challenges and limitations that reduce their effectiveness. Systemic problems in design and implementation often cause these programs to fall short of their goals. Research by Gavett (2017) shows that some educational interventions can reduce vulnerability to

phishing attacks. However, many organizations still rely on mandatory phishing awareness training as a solution (MOSSANO, 2020). Yet, the success of these programs is frequently hindered by various challenging factors.

Mandatory training, often implemented through policies and compliance requirements, ensures that all individuals within an organization receive a baseline level of education and awareness (GO-GLOBE, 2018). Mandatory training can serve as a foundational step, educating employees on the characteristics and tactics of phishing attacks, as well as the importance of information security vigilance (LAIN, 2022).

Non-mandatory training programs play a crucial role in enhancing phishing prevention within SAT programs. These training types, such as voluntary training, opt-in training, gamified training, and awareness campaigns, offer employees the opportunity to engage in learning activities without compulsion. Voluntary training allows employees to participate at their discretion, while opt-in training requires active engagement from participants who are genuinely interested in security awareness (ABAWAJY, 2012). Gamified training, although not exclusively non-mandatory, incorporates elements of play to increase engagement and participation (THOMPSON, 2022). Awareness campaigns, on the other hand, utilize informal methods like newsletters and quizzes to enhance awareness without formal participation requirements (BAGUI, 2023). These non-mandatory approaches are effective in raising a proactive security culture by encouraging voluntary engagement and learning, potentially leading to higher retention and practical application of knowledge (NAGYFEJEO & SOLMS, 2020).

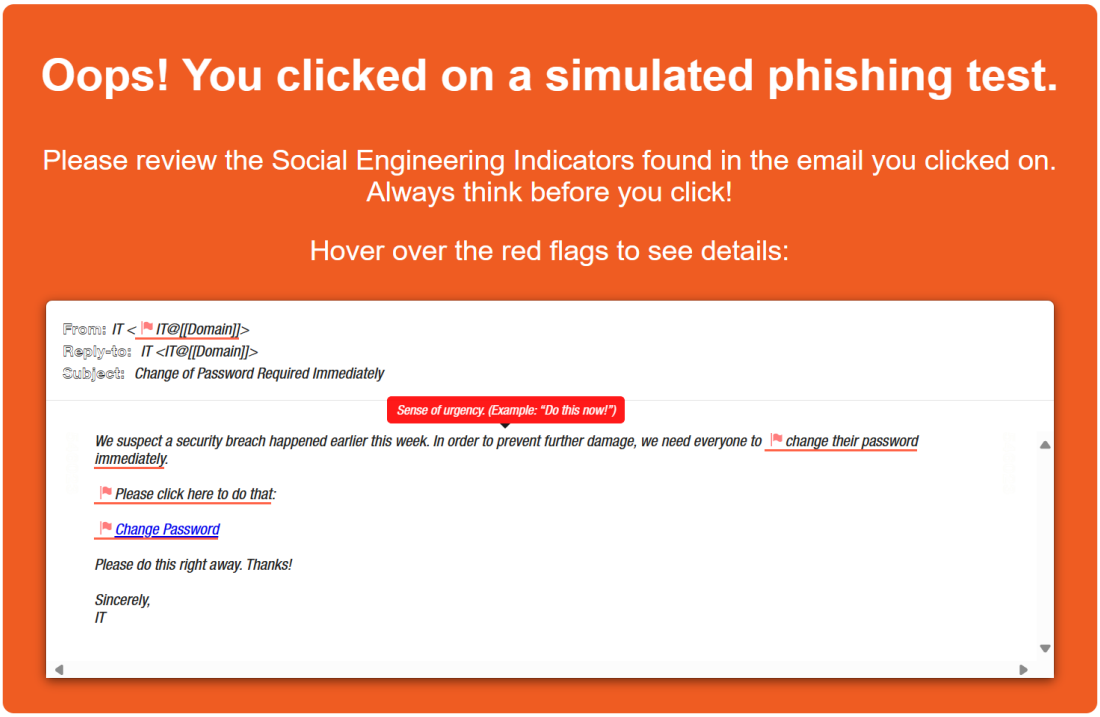
A strategic approach to training that combines mandatory and non-mandatory elements can be highly effective in addressing the nuances of complex issues like phishing prevention (KNOWBE4c, 2024). Organizations that encourage a culture of collaboration build collective knowledge and skills of their workforce, leading to innovative problem-solving and a stronger sense of community.

2.8.2. Timing of Feedback

In simulated phishing campaigns, the literature outlines the use of immediate feedback as an effective strategy to enhance learning outcomes. Immediate feedback involves alerting users right after they interact with a simulated phishing email,

informing them that they fell for the attempt and explaining the characteristics of the phishing message that made it suspicious (CANHAM, 2021). This method seeks to correct the behavior in real-time, leveraging the "*teachable moment*" to reinforce recognition patterns and improve the user's response to similar threats in the future. Vishwanath (2016) supports that providing timely feedback right after the mistake occurs significantly improves the ability of users to internalize the lesson and reduces the likelihood of repeating the same error in subsequent simulations. Figure 10 presents an example of a landing page used in simulated phishing, providing immediate feedback.

Figure 10 - Example of Feedback in a Simulated Phishing



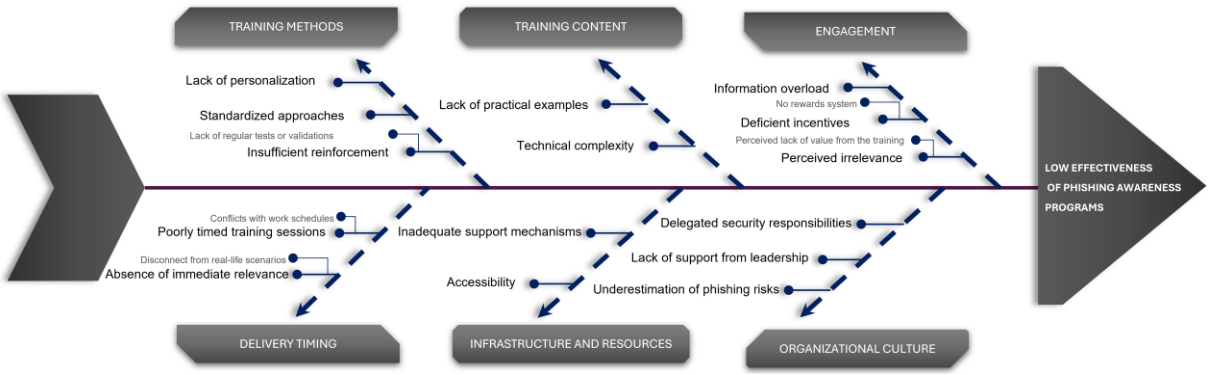
Source: Knowbe4 Platform (2024)

Immediate feedback emphasizes instant correction and reinforcement, focusing on addressing mistakes as they happen, while delayed training concentrates on long-term educational impacts and reinforcement at a later stage. Both approaches offer distinct advantages and can be employed based on the specific objectives of the phishing awareness program. Immediate feedback is effective for immediate correction and learning reinforcement, while delayed training is beneficial for assessing long-term training retention and the sustained effectiveness of training initiatives (VISHWANATH, 2016).

2.9. KEY CHALLENGES IN PHISHING AWARENESS

Understanding the factors that limit the success of phishing awareness programs in organizations is fundamental. We used an Ishikawa diagram to determine key aspects affecting participants engagement and learning. The main factors include training methods, content relevance, timing, infrastructure, and organizational culture. Common obstacles include for example overly generic content, complex terminology, and lack of support. Figure 11 shows these dimensions and barriers, offering a summary and suggestions for addressing each issue to improve the overall effectiveness of training programs.

Figure 11 - Challenges in Phishing Awareness Programs



Source: the author (2024)

Phishing awareness programs often struggle with low effectiveness due to poor **training methods**. Generic content that doesn't consider specific risks faced by different departments and employees reduces relevance (JAMPEN, 2020). Additionally, the lack of continuous testing and reinforcement weakens long-term retention (HARRISON, 2016). To address these issues, it is essential to tailor training to users' profiles and specific threat scenarios, ensuring sustained engagement and meaningful learning outcomes (TSCHAKERT, 2019; ZAHARON, 2021).

Training content must be practical and easy to understand to be effective. Programs that use complex terminology and lack real-life examples often fail to prepare users for real phishing threats (STEVES, 2019). Research highlights the importance of incorporating practical simulations and real-time feedback to enhance training outcomes (SUTTER, 2022). Simplifying content and using realistic examples help bridge the gap between theory and practice, making it easier for employees to apply their learning in real scenarios (DAREM, 2021).

Engagement is a major barrier to effective training. Overloading employees with information or presenting irrelevant content often leads to disinterest and low participation (DOWNS, 2007). Providing incentives, linking training to real job responsibilities, and using interactive methods can significantly increase engagement and retention (BAYL-SMITH, 2021). It is essential to consider the diverse needs of employees and develop strategies that maintain interest and motivation throughout the training program (ZIELINSKA, 2014).

The **timing of training delivery** is critical for its effectiveness. Sessions conducted during busy work hours or unrelated to ongoing threats are often poorly attended and less impactful (JAMPEN, 2020). Scheduling training when it aligns with current security issues and using short, focused sessions has been shown to enhance participation and retention (VOLKAMER, 2018). Additionally, providing immediate feedback to users, by redirecting them to a landing page that informs them they have fallen for a simulated phishing attempt and identifies the red flags they missed, can be effective. The instant feedback mechanism not only offers real-time learning but also helps users quickly recognize their mistakes, reinforcing key security behaviors. Tailoring training schedules based on users' availability and current organizational needs, along with immediate feedback mechanisms, can greatly improve outcomes (ALIYU, 2023).

The accessibility of **training resources** directly affects participation rates. Complicated access procedures or a lack of available resources can discourage employees from engaging in training (KROMBHOLZ, 2015). Ensuring easy access through multiple platforms and providing IT support can remove these barriers. Strong management and IT support are also critical to securing necessary resources and promoting a culture that prioritizes security training (SAWAYA, 2017).

Organizational culture significantly influences the success of phishing awareness programs. A lack of support from leadership or underestimation of phishing risks can undermine training initiatives (D'ARCY, 2009). Establishing clear security roles, encouraging reporting, and integrating security into business strategies are essential steps to building a security-aware culture (HADNAGY, 2015). Active involvement from executives reinforces the importance of security and ensures these initiatives receive the attention and resources needed for success (KRAEMER, 2007).

2.10. RELATED WORK

A case study conducted within a credit union by Pires (2023) in an institution in southern Santa Catarina serving over 50,000 members through 29 service points has shown that proactive awareness training can pivot the organization's cybersecurity posture from reactive to strategic. The data collected through questionnaires reflects a positive assessment of the awareness program using KnowBe4. Most employees affirmed the training led to increased confidence in handling high-risk information, translating into improved practices both professionally and personally. Additionally, the cooperative reported a decrease in security incidents, indicating a successful application of the platform's training modules.

Another analysis titled "*Examining factors impacting the effectiveness of anti-phishing trainings*" by Sumner, Yuan, and Anwar (2022) employs a case study methodology to investigate the impact of KnowBe4's training on improving users' ability to detect phishing attempts. The research addresses two primary questions: the extent to which KnowBe4 training influences phishing detection and the overall training effectiveness. Results indicated an improvement in phishing detection rates. The detection rate of phishing attempts increased by 45% after users completed the KnowBe4 training program.

Following these insights, Alshaikh et al., (2019) investigated the effectiveness of cybersecurity training programs using an action research methodology. The study identified deficiencies in traditional SETA programs, which often fail to drive significant behavioral changes in employees. While involving participants in the evaluation process, the research improved cybersecurity behaviors, resulting in a 35% increase in phishing detection rates after training program adjustments.

3. METHODOLOGY

We describe the methodological approach adopted to investigate phishing prevention strategies in the context of security awareness training (SAT) programs, beginning with an introducing to the research design, which included a case study methodology and the organizational context in which the study was conducted. We detail the use of mixed-methods approach, combining quantitative and qualitative data collection, highlighting how the integration of these methods offered a thorough understanding of the research questions. Each phase of the research is outlined, from the initial planning and design to the execution of phishing simulations, training interventions, and participant interviews.

We also explain the procedures for participant selection, data collection, and analysis for both the quantitative and qualitative components, and discuss the use of a SAT platform for phishing simulations and a specific tool for thematic analysis. Finally, we introduce the structure of the subsequent sections, detailing how each research phase contributes to addressing the study's objectives and informing the proposed set of good practices to improve phishing prevention efforts in SAT programs.

3.1 **Study Overview and Organizational Context**

We aim to address the following research questions:

RQ1: What are the main factors that contribute to the effectiveness of phishing prevention strategies in security awareness training programs?

RQ2: What are the good practices to improve the effectiveness of phishing prevention strategies in security awareness training programs?

To investigate these questions, we adopted a case study methodology, as recommended by Merriam (2009). Case studies are suitable for understanding complex phenomena within their real-world context and allow for a deep examination of security awareness strategies aimed at preventing phishing.

The research setting involves a large public organization in Pernambuco, Brazil, comprising approximately ten thousand employees distributed across more than 150 cities throughout the state. The workforce is divided into two main levels: employees, who are public servants responsible for various operational and administrative functions, and C-Levels, who are senior officials holding high-level decision-making roles within the organization. The organization had been frequently targeted by

phishing attacks, leading to credential theft and disruptions to critical systems, highlighting the need for enhanced security awareness initiatives. These incidents highlighted the urgent need for a more robust security posture, prompting the organization to invest in a Security Awareness Training (SAT) platform aimed to systematically reduce participants vulnerability to phishing through structured simulations and training interventions.

Given this context, the organization provided an ideal context to explore the factors influencing the effectiveness of phishing prevention strategies within SAT programs. The organization's prior lack of structured phishing simulations or formal training initiatives created a natural setting for examining the impact of the SAT program. To achieve an understanding of its effectiveness, a mixed-methods approach was adopted. We performed a quantitative study, focused on collecting data through the SAT platform and assessing participant responses to simulated phishing emails and engagement with training modules. Then, we performed a qualitative study, conducting semi-structured interviews with a selected group of participants using thematic analysis to understand participant perceptions, learning experiences, and suggestions for improvement.

The organization offers a valuable context for studying the factors that influence the effectiveness of phishing awareness training, given its size, diversity, and prior exposure to phishing threats. The findings from the case study are expected to enhance both the theoretical understanding of phishing awareness and the practical design of more effective training interventions. Drawing on the results from both the quantitative and qualitative studies, a set of good practices was proposed to improve phishing prevention within SAT programs, providing practical recommendations for the design and delivery of these programs. Figure 12 describes the phases of the case study.

Figure 12 - Case Study Phases

Source: the author (2024)

Figure 16 illustrates the four phases of the research methodology adopted in this investigation: Planning, Quantitative Study, Qualitative Study, and Good Practices Proposal. In the subsequent sections, each phase is detailed, explaining how it was conducted and its role in addressing the research questions.

3.1. PHASE 1 - PLANNING

In this phase, we established a structure for investigating user awareness strategies to prevent phishing attacks, defining the design, implementation, and evaluation processes. The simulated phishing campaigns and security awareness training (SAT) interventions were central components of the quantitative study, aimed at measuring participant propensity, engagement, and training effectiveness. Then, semi-structured interviews were conducted as part of the qualitative study, focusing on exploring participants' perceptions, experiences, and insights related to the different phishing simulations and trainings invitations. These combined efforts were designed to generate both measurable results and deeper understanding, ultimately resulting in the proposal of good practices, which synthesized findings from both the quantitative and qualitative phases.

Given the need to understand the measurable outcomes of the quantitative and qualitative studies, it was crucial to employ a methodological approach capable of capturing these complexities. The integration of quantitative data, which reveals trends and patterns, with qualitative insights, which provide context and depth, enabled a more comprehensive analysis of the factors influencing the effectiveness of phishing prevention within a SAT program. This dual focus was necessary to not only determine

what strategies worked better but also to explain why they were effective or ineffective within the specific organizational context.

Consequently, the use of case study methodology with mixed methods emerged as a natural choice for this research. It allowed us to examine complex interactions within a real-world setting, capturing nuances that could be overlooked in a purely quantitative or qualitative approach (MERRIAM, 2009; YIN, 2018). The approach provided a holistic view of the phenomena through the integration of both measurable outcomes and participant insights, facilitating a deeper understanding of what works and why, as recommended in studies dealing with complex organizational processes (FLYVBJERG, 2006).

We began by designing structured phishing simulations and security awareness training (SAT) interventions to systematically measure and enhance user awareness regarding phishing prevention. The SAT program followed a sequential process, starting with a simulated phishing campaign to assess the initial susceptibility of participants to phishing attacks. This was followed by a training intervention aimed at increasing awareness and security behavior. A subsequent phishing simulation was then conducted to evaluate the effectiveness of the training in reducing susceptibility.

To investigate the impact of different strategies, we employed varied configurations within the phishing simulations. Some phishing emails included feedback mechanisms, such as a landing page displayed after clicking a phishing link, while others were sent without feedback. This method aimed to evaluate how the presence or absence of feedback influenced user behavior, particularly in terms of engagement with subsequent training interventions. Additionally, the training phase explored different invitation methods, evaluating user engagement based on a more direct approach versus a friendlier, less formal invitation. This allowed us to quantitatively measure user adherence to training and the influence of invitation style on engagement.

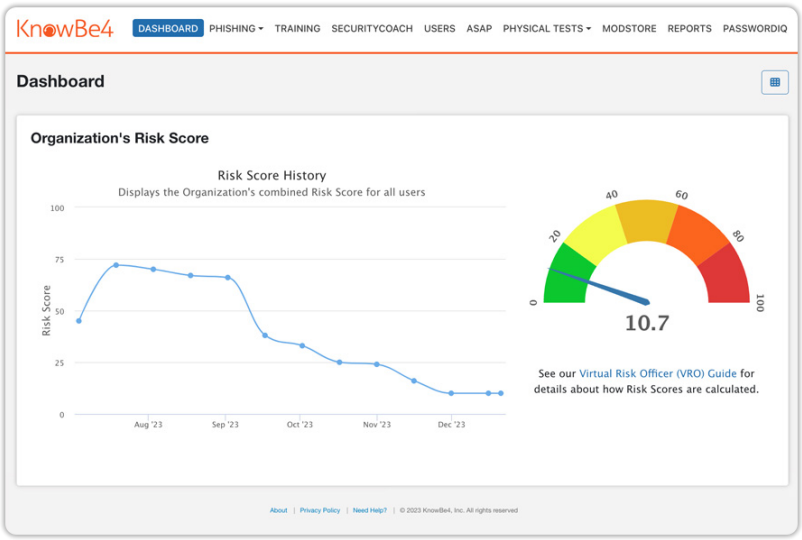
3.2. PHASE 2 - QUANTITATIVE STUDY

The quantitative study was designed to measure participants' susceptibility to phishing attacks and their engagement with security awareness training (SAT). We

used the KnowBe4[1] platform, a specialized tool for simulating phishing attacks and managing SAT programs in organizational environments.

The KnowBe4 platform is used for security awareness initiatives, offering features to both simulate phishing attacks and deliver training content. It enables us to create customized phishing campaigns that mimic real-world threats, allowing us to test participants responses to various social engineering tactics. In addition to phishing simulations, the platform provides an extensive library of training materials, including interactive modules, videos, and quizzes. The platform also measures user risk based on behavioral history, as illustrated in Figure 13, where the risk score dashboard displays the combined risk level for all users in the organization over time.

Figure 13 - Knowbe4 Platform



Source - Knowbe4.com

Using the platform, security administrators can create customized phishing campaigns to measure participant responses, such as whether they clicked on the phishing links and how quickly they reacted; and then invite participants to complete SAT modules. The tool also enabled the delivery of instant feedback to participants when they click in a simulated phishing, which was one of the variables tested in this study.

3.2.1. Participant Selection

In this section, the criteria for participant selection are described. The study included 4,457 collaborators from a public organization in the State of Pernambuco, Brazil. Participants were divided into groups based on their location, categorized as

[1] www.knowbe4.com

either from the Metropolitan Region of Recife or the interior of the state, as well as by role, including 498 C-Levels distributed across Pernambuco. Most participants were concentrated in the Metropolitan Region of Recife, reflecting the organization's employee distribution. The selection of participants was independent of their previous experience with phishing.

The study began with a simulated phishing campaign. Participants were initially divided into two groups:

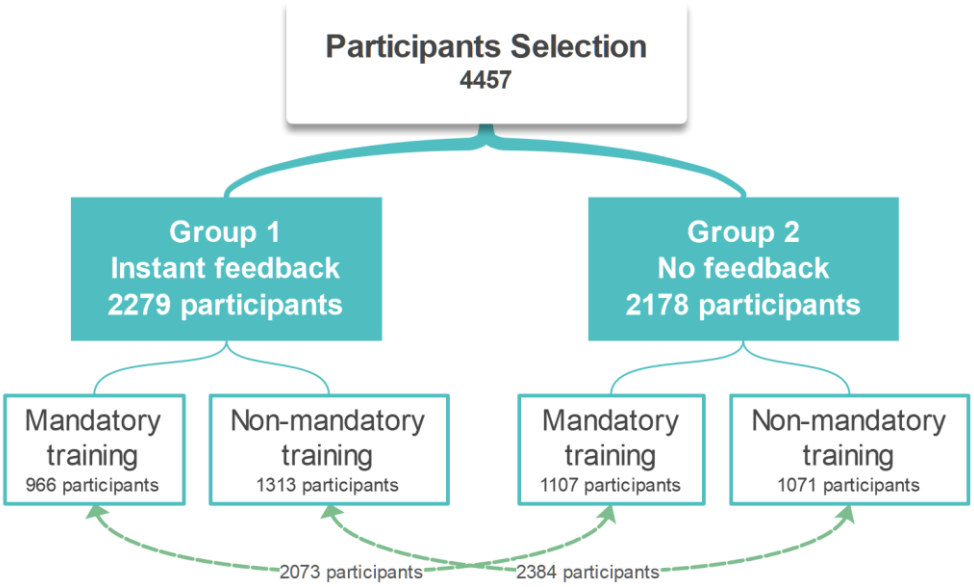
- **Group 1**: received instant feedback after clicking on a simulated phishing link.
- **Group 2**: received no feedback after clicking on a simulated phishing link.

Following this, participants in each group were invited to participate in the training intervention. The invitation to the training was conducted using two different methods:

- **Mandatory training**: delivered with a more direct and formal invitation.
- **Non-mandatory training**: delivered with a friendlier and less formal invitation.

The participant selection is represented in Figure 14.

Figure 14 - Participants Selection



Source: the author (2024)

The selection criteria for participants were designed to ensure a representative sample from all the personnel from the organization, which aims to obtain insights that are reflective of the broader community. Importantly, the Metropolitan Region of Recife is emphasized due to its higher concentration of collaborators, aligning the participant base with the regional density of potential cybersecurity threats. According to Creswell

(2018), ensuring a diverse and representative sample is important for creating balanced and controlled conditions that support the credibility of case studies.

3.2.2. Data Collection

The quantitative data collection was organized into three stages:

- **Initial Simulated Phishing Campaign**: to establish a baseline of participant susceptibility.
- **Training Engagement Measurement**: to evaluate how participants interacted with training modules following the phishing simulations.
- **Post-Training Simulated Phishing Campaign**: to assess changes in behavior and training effectiveness.

3.2.2.1. Initial Simulated Phishing Campaign

In the initial stage, we used the KnowBe4 platform to simulate the latest phishing tactics and deliver phishing emails to 4,457 participants. The aim was to establish a baseline for participant susceptibility, while tracking and analyzing their real-time responses and interactions with the emails. The specific metrics collected using the platform were:

- **Failures in the First Hours**: track the number of participants who fall for a phishing attempt within the first hours of the campaign, providing insights into initial vulnerability.
- **Daily Failures Throughout the Campaign**: monitor daily failures helped in understanding how susceptibility to phishing changes over the course of the campaign.
- **Phishing Propensity**: measure the percentage of participants who respond to phishing attempts, reflecting the overall susceptibility (in percentage) of the group.
- **Clicks Recorded**: the total number of clicks on links within the phishing emails were tracked to measure the direct interaction with potentially malicious content.
- **Types of Phishing Deployed**: different types of phishing emails were sent to participants, with four types designated for immediate feedback and four for delayed feedback. The goal is to assess the failure rate for

each type of campaign, both with and without feedback, and to evaluate the adherence of individuals to training after receiving feedback, compared to those who did not receive feedback.

To assess participant susceptibility and response behaviors, we designed eight different simulated phishing attacks, which were distributed across two groups, allowing us to capture a broader range of responses and ensure a more accurate analysis of participant behavior:

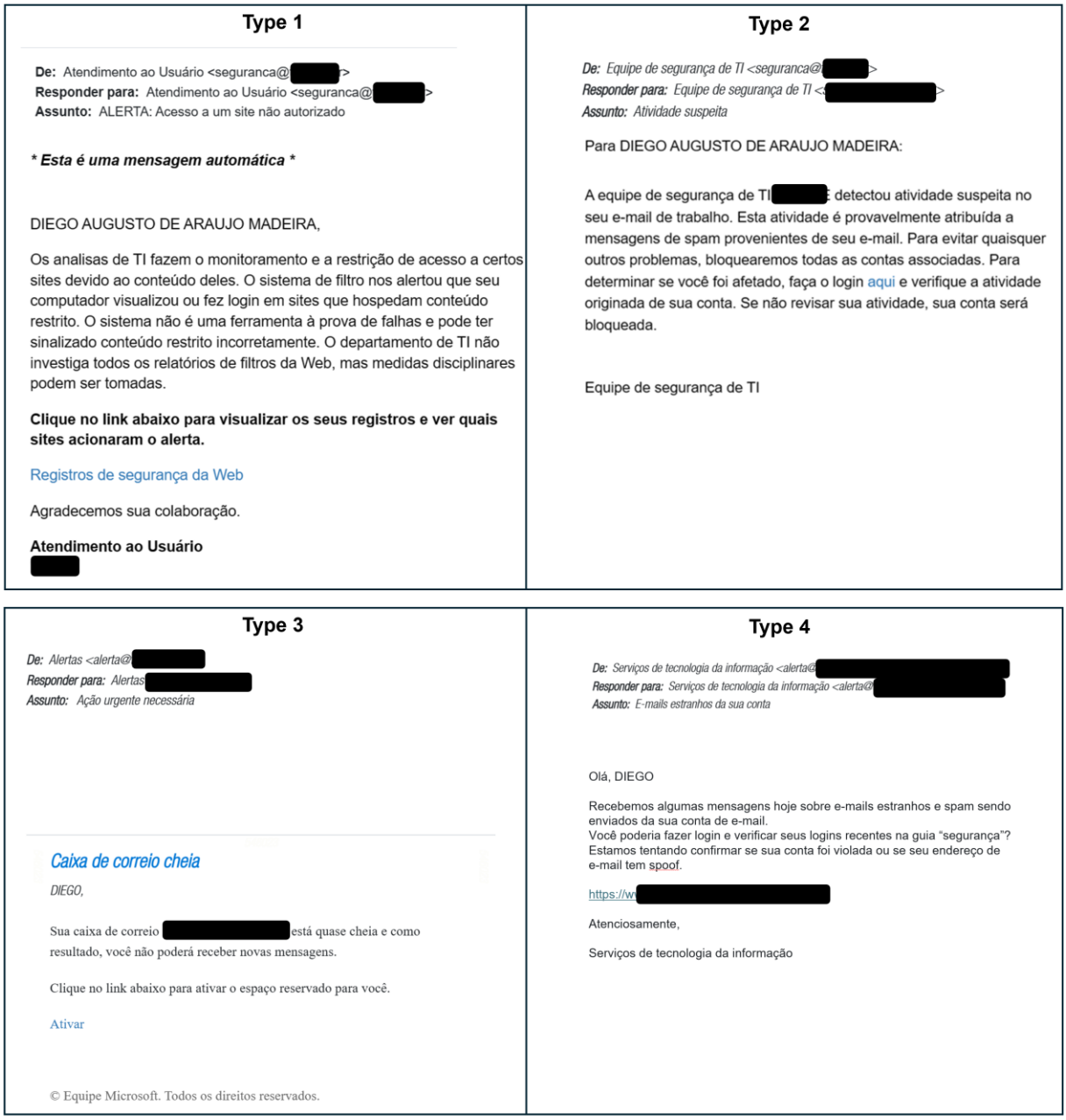
- **Four types with instant feedback**: participants received immediate feedback after clicking on a phishing link, informing them that it was a simulated attack.
- **Four types without feedback**: participants received no feedback, leaving them unaware that the email was part of the simulation.

The decision to include both feedback and no-feedback variations aimed to analyze how feedback presence or absence affects user behavior and training engagement, providing insights into how instant feedback influences participant responses and subsequent engagement with training.

All simulated phishing emails leveraged the same cognitive bias called sense of urgency, creating an approach that aims to reduce the likelihood that users would carefully analyze the email before responding, thereby increasing the chances that they would click on the phishing link. The urgency bias exploits the human tendency to react quickly to situations that seem urgent or threatening, often bypassing critical analysis or verification of the message's authenticity (KHERUDDIN, 2024). The same bias was used for all campaigns to ensure they can be analyzed fairly.

The specific types of phishing simulations with **instant feedback** are presented in Figure 15.

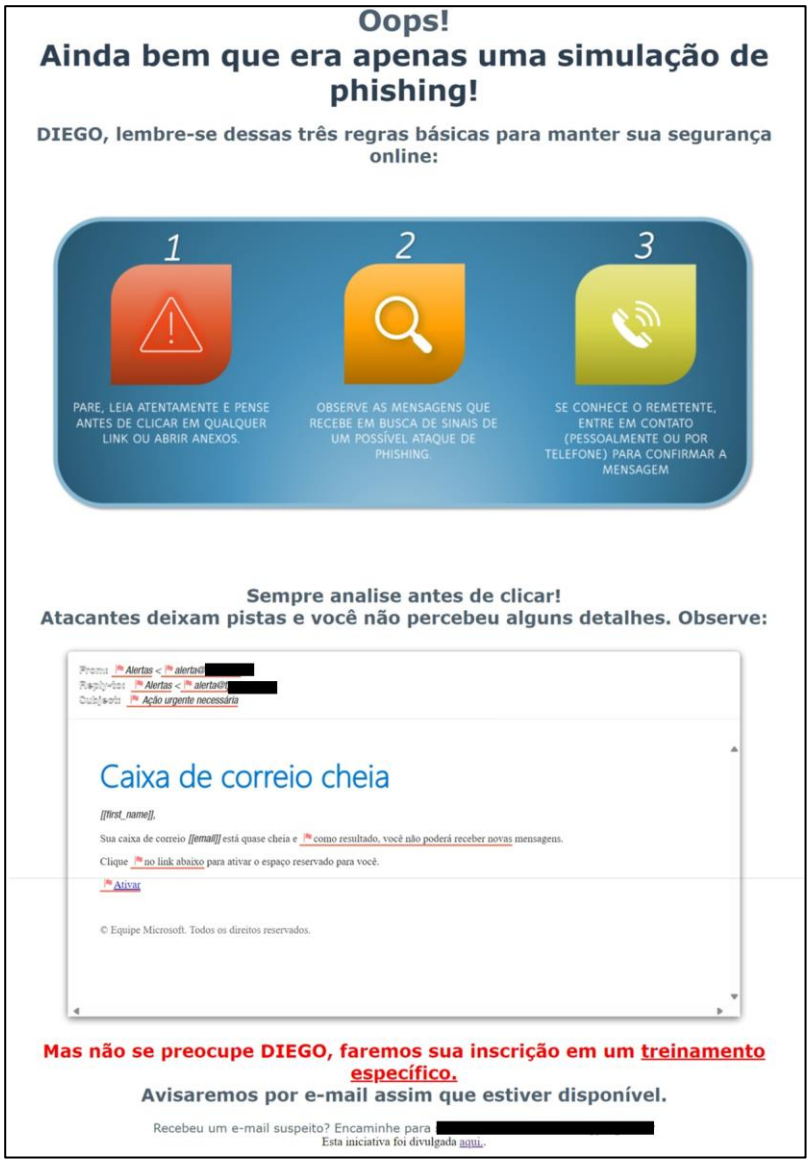
Figure 15 - Phishing for the campaign with Instant Feedback



Source - The Author (2024)

In Figure 15, four types of phishing simulations are presented. Each simulation used a typical cognitive bias commonly found in real-world phishing attacks to create a sense of urgency, which contain warnings about account suspensions, alerts regarding suspicious activities, messages about full inboxes, and notifications of potential security breaches. If users clicked on the link provided, they were redirected to a landing page that provided instant feedback, indicating that the email was a simulated phishing attempt, as shown in Figure 16.

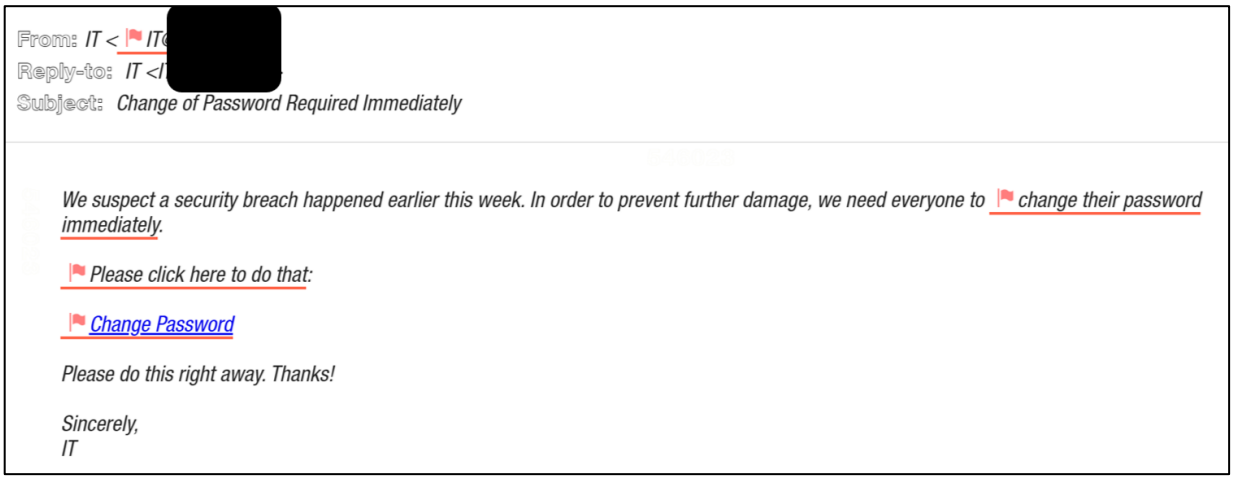
Figure 16 - Phishing Landing Page with Instant Feedback



Source: the author (2024)

The response page for **instant feedback** was provided with "Red flags", that were warning signs or indicators pointing to potential problems or threats. These signs were clues or suspicious characteristics that helped users identify phishing attempts, fraud, or other malicious activities. Examples of red flags include emails from unknown senders, urgent messages requesting personal or financial information, suspicious links, grammatical or spelling errors, and unusual requests for quick action (ΖΑΧΑΡΙΆΔΗ, 2023). These red flags were displayed on the landing page for the simulated phishing campaign with instant feedback, helping users to immediately understand what they missed and how to avoid such threats in the future, as shown in Figure 17.

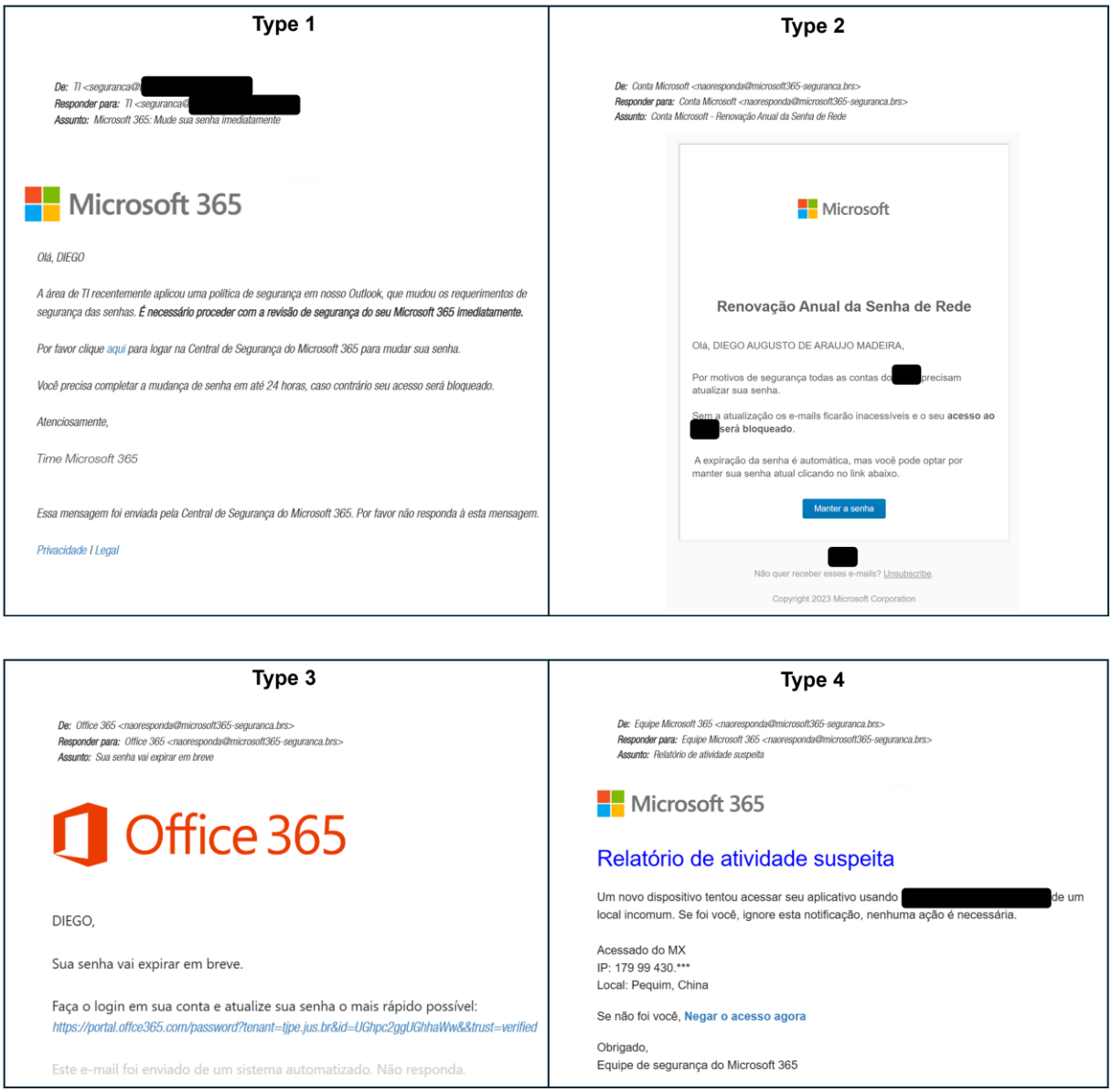
Figure 17 - *Redflags* in the landing page with instant feedback



Source: the author (2024)

Similarly, we present the messages sent to phishing simulations **without feedback**. In Figure 18, another four types of phishing simulations are displayed, representing campaigns without immediate feedback. Each simulation also employs a typical cognitive bias commonly used in real-world phishing to create a sense of urgency. The tactics include prompts to change passwords due to security policies, notifications of account renewal requirements, warnings of password expiration, and alerts about suspicious login activities. Unlike the previous set of simulations, these phishing emails do not redirect users to a landing page for instant feedback, leaving participants unaware that the email was part of a simulation.

Figure 18 - Phishing for the Campaign without Feedback



Source: the author (2024)

The response page **without feedback** simulated phishing is provided with a "*404 Not Found*" error message, as described in Figure 19.

Figure 19 - Landing page without feedback

Source - The Author (2024)

The "*404 Not Found"* page is loaded without providing any additional information to the user, leaving them with no indication that the interaction was part of a simulated phishing.

3.2.2.2. Training Engagement Measurement

After the initial simulated phishing campaign, participants were invited to engage with educational content delivered through video modules on the KnowBe4 platform. The training phase was designed to start three days after the phishing simulation campaign, to ensure a seamless transition from phishing exposure to learning. The video modules included a series of episodes focused on Social Engineering, Phishing Attacks and Social Networks, as illustrated in Figure 20.

Figure 20 - Knowbe4 User Training Panel

Source: Knowbe4 (2024)

Figure 20 shows the video episodes:

- *Internal Threat: Season 1, Episode 1 - The Newcomer (Social Engineering*), 8 minutes.
- *Internal Threat: Season 1, Episode 2 - Socializing (Social Networks),* 7 minutes.
- *Internal Threat: Season 1, Episode 3 - On Our Team (Phishing Attacks),* 7 minutes.

The video episodes selected for the training are structured to maintain participant engagement by presenting information in short, focused segments. Each

episode lasts no more than 8 minutes, making it easier for learners to absorb the content without feeling overwhelmed. The videos were available in Brazilian Portuguese, the native language of the participants. Additionally, data on the number of participants who completed, did not complete, or partially completed the training was recorded, capturing completion statistics.

The decision to utilize video content exclusively was made for several reasons. Videos require less interaction from the users, allowing them to absorb the information more passively and conveniently, which contributes to reduced user interaction. Additionally, video ensures a consistent delivery of content, providing all participants with the same quality and form of information, thereby maintaining consistency and quality of delivery. Furthermore, the engaging nature of well-produced video content can significantly enhance information retention and maintain participant interest, leading to enhanced engagement and learning outcomes (MAYER, 2014).

The training component exclusively utilizes video content selected from KnowBe4's *The Inside Man* series, specifically the first three videos of Season 1. This decision is based in the series' engaging narrative format, which leverages high-quality filmmaking to present information security concepts in an accessible and relatable way. Unlike traditional training methods such as text-based materials or static presentations, "*The Inside Man*" provides a compelling storyline that unfolds across various episodes, maintaining viewer interest and engagement. This narrative approach not only makes complex information security issues more understandable but also enhances retention by embedding educational content within the context of relatable scenarios faced by characters in the series. The use of video also standardizes the delivery of content, ensuring that all participants received the same information in the same format, which is critical for comparing the effectiveness of the training across the different groups of study participants, and maximizing engagement and learning outcomes through high-impact, modern educational techniques.

In addition, participants received daily reminders via email to complete the training modules, which were designed using a similar as the initial training invitation, maintaining consistency in tone and structure. The reminders aimed to reinforce the importance of the training and encourage adherence by keeping it top of mind for participants during the campaign period.

3.2.2.3. Post-Training Simulated Phishing Campaign

In this final part of the quantitative study, we focused on participants who failed the initial simulated phishing test but completed the training. The objective was to evaluate the effectiveness of the training by comparing the metrics collected during the post-training phishing simulation with those from the initial phase. These metrics include:

- Failures in the first hours of the campaign,
- Daily failures throughout the campaign,
- Phishing propensity,
- Recorded clicks.

However, unlike the initial simulation, in this phase we used three new types of phishing emails, each employing the same cognitive bias of urgency, which were selected based on the highest failure rates in previous tests and were not repeated to ensure variety. Additionally, the simulated phishing campaign was structured in a way that prevented participants from receiving the same phishing email they had encountered previously.

3.2.3. Data Synthesis

The synthesis of the quantitative study aimed to identify patterns and trends in participants' responses to phishing simulations and their engagement with the training modules, focusing on different feedback types and training modalities to evaluate the effectiveness of the phishing prevention within a SAT program.

We utilized descriptive statistics to summarize key metrics collected at different stages of the study:

- **Failures in the first hours of the campaign:** collected during the initial hours of each phishing simulation, providing insights into participants' immediate reaction times and initial susceptibility to phishing attempts.
- **Daily failures throughout the campaign**: tracking daily failures allowed us to observe changes in participant behavior over time.
- **Phishing propensity**: measured as the likelihood of participants clicking on phishing links, providing an overall indication of the effectiveness of the SAT program designed to prevent phishing attacks.

- **Recorded clicks**: the total number of clicks on phishing links offered a direct measure of participant responses and the effectiveness of the training in altering user behavior.

Trend analysis was used to examine how participant susceptibility changed over time, especially after the training interventions. To achieve this, we conducted a targeted simulated phishing campaign for participants who initially failed but completed the training, assessing their ability to recognize and respond to phishing attempts after the training phase.

To analyze the training data, we used descriptive statistics to analyze the completion rate, focusing only on participants who watched all three videos in full to understand overall engagement patterns. We then compared participants who received immediate feedback with those who did not, assessing how feedback influenced their engagement. Additionally, we compared engagement between mandatory and non-mandatory training to identify differences in motivation and completion rates.

The quantitative study provided data to answer both RQ1 and RQ2, allowing us to identify key factors that influence phishing prevention within SAT programs and offer insights into their effectiveness.

3.3. PHASE 3 - QUALITATIVE STUDY

In this phase, we conducted qualitative semi-structured interviews to gain a comprehensive understanding of participants' experiences, perceptions, and motivations within phishing prevention efforts in SAT programs. The interviews explored how the presence or absence of user feedback, along with different training approaches, influenced participant engagement, training relevance, and susceptibility to phishing, contributing to answer RQ2. Additionally, the interviews aimed to identify factors that impact readiness to engage in security training, uncovering elements that could enhance interaction with training content and support the development of good practices.

3.3.1. Participant Selection

Participants for the semi-structured interviews were selected through convenience sampling, a common approach in qualitative research to gain in-depth

insights into specific topics (ETIKAN, 2016). This method involves choosing individuals who are readily available and willing to participate, allowing researchers to gather detailed information from those who are most accessible (MARSHALL, 1996). Convenience sampling is effective for exploratory studies, as it helps generate initial assumptions and deeper understanding of the subject (PATTON, 2002).

Participants were invited to take part in the interviews through phone calls and in-person requests, ensuring direct communication and confirmation of availability. A total of 20 individuals were selected based on their willingness to participate and availability during the data collection period. The interviews took place between May 21, 2024, and May 23, 2024.

3.3.2. Data Collection

Individual interviews were conducted in a controlled and confidential environment to ensure participants felt comfortable sharing their experiences and perceptions. Depending on participants' availability and preferences, the interviews were conducted either in person or via telephone communication. The environment was structured to minimize distractions and maintain confidentiality throughout the process.

To guide the data collection, a semi-structured interview protocol was developed to guide the data collection, as outlined in Appendix A. The protocol was created with the following steps:

- **Informal Literature Review**: a review of existing studies on phishing prevention strategies within a SAT program was conducted, aiming to identify key themes and questions that are commonly explored.
- **Alignment with Research Questions**: focus on RQ2, which aims to propose good practices to improve the effectiveness of phishing prevention strategies.
- **Iterative Refinement**: to ensure the protocol could prompt meaningful responses from participants.
- **Pilot Testing**: a pilot interview was conducted to test the effectiveness of the questions and the flow of the conversation. Adjustments were made based on this test, refining the wording and sequence of questions to improve participant engagement.

The protocol included open-ended questions designed to encourage participants to share their experiences freely, covering topics such as personal experiences with phishing, perceptions of the training content and format, and feedback on simulated phishing activities when applicable. To establish a stronger connection with participants, the protocol began with a more personal question, asking whether they had ever fallen victim to a phishing attempt and prompting them to self-assess their ability to detect phishing. This procedure aimed to create a comfortable environment for open discussion, designed to capture context-rich information. Table 2 provides an overview of the interview data, including participant demographics, interview duration, and transcript details.

Table 2 - Qualitative Interviews Overview

ID	Age	Function	Years of Service	Date of Interview	Transcript Pages	Duration (min)
I1	40-49	Employee	22	21/05/2024	5	08 min 01 secs
I2	30-39	Employee	11	22/05/2024	8	13 min 59 secs
I3	50-59	Employee	26	21/05/2024	9	23 min 37 secs
I4	40-49	Employee	22	21/05/2024	4	07 min 09 secs
I5	40-49	Employee	22	22/05/2024	4	06 min 03 secs
I6	50-59	C-Level	15	21/05/2024	3	05 min 05 secs
I7	50-59	Employee	27	22/05/2024	4	07 min 12 secs
I8	50-59	Employee	26	22/05/2024	8	16 min 56 secs
I9	30-39	C-Level	21	23/05/2024	13	19 min 43 secs
I10	40-49	C-Level	29	23/05/2024	3	05 min 49 secs
I11	40-49	Employee	12	22/05/2024	5	09 min 00 secs
I12	40-49	Employee	15	22/05/2024	10	19 min 55 secs
I13	50-59	C-Level	10	22/05/2024	7	11 min 28 secs
I14	20-29	Employee	10	22/05/2024	7	13 min 15 secs
I15	30-39	Employee	25	21/05/2024	5	09 min 10 secs
I16	60+	Employee	2	22/05/2024	2	03 min 40 secs
I17	50-59	Employee	12	21/05/2024	4	05 min 55 secs
I18	60+	C-Level	21	21/05/2024	4	05 min 22 secs
I19	20-29	Employee	22	21/05/2024	3	05 min 12 secs
I20	40-49	Employee	18	22/05/2024	3	03 min 55 secs

Source: the author (2024)

All interviews were recorded with participants' informed consent to capture the complete content of each conversation. The recordings were transcribed to ensure an accurate representation of the discussions, with all transcriptions securely stored to protect participants' privacy and used solely for research purposes. On average, the interviews lasted 10 minutes.

3.3.3. Data Synthesis

The qualitative data were analyzed using Thematic Analysis, a synthesis method that enables the identification of patterns and themes within the data (BRAUN, 2006), allowing for the documentation of good practices based on participants' actual experiences and perceptions of phishing prevention within SAT programs. The first step in data preparation involved transcribing all recorded interviews to ensure that every detail of the conversation is captured accurately. The transcriptions then were read thoroughly multiple times to immerse the researcher in the data.

In open coding, data were fragmented, analyzed, compared, and categorized. According to Merriam (2009), open coding involves labeling any unit of data relevant to the study. Flick (2004) states that open coding is the analytical process through which concepts are identified and developed in terms of their properties and dimensions, with the aim of expressing data and phenomena in the form of concepts. Data are segmented and classified by unit of meaning in short word sequences, and the researcher explores the data meticulously due to intensive text reading.

In axial coding, relationships between categories forming the propositions of substantive theory are examined. Merriam (2009) describes axial coding as the process of relating categories and properties to each other, refining the category scheme. Axial coding involves procedures performed after open coding, where data are restructured through relationships between categories, considering conditions, context, action/interaction strategies, and their consequences (STRAUSS et al, 1998). According to Flick (2004), axial categories are enriched as they fit as many segments as possible.

Finally, selective coding refines the entire process by identifying the central category of the theory to which all other categories are related. In summary, the research will examine the conditions, interactions, and consequences related to each category, providing a deeper understanding of how different factors influence user perceptions and consequently increase user engagement of SAT programs designed to prevent phishing. In the selective coding phase, the focus shifts to identifying the central category that integrates all other categories. This core category represents the main theme or storyline emerging from the data. The core category and related subcategories are then integrated to form a coherent theoretical framework that

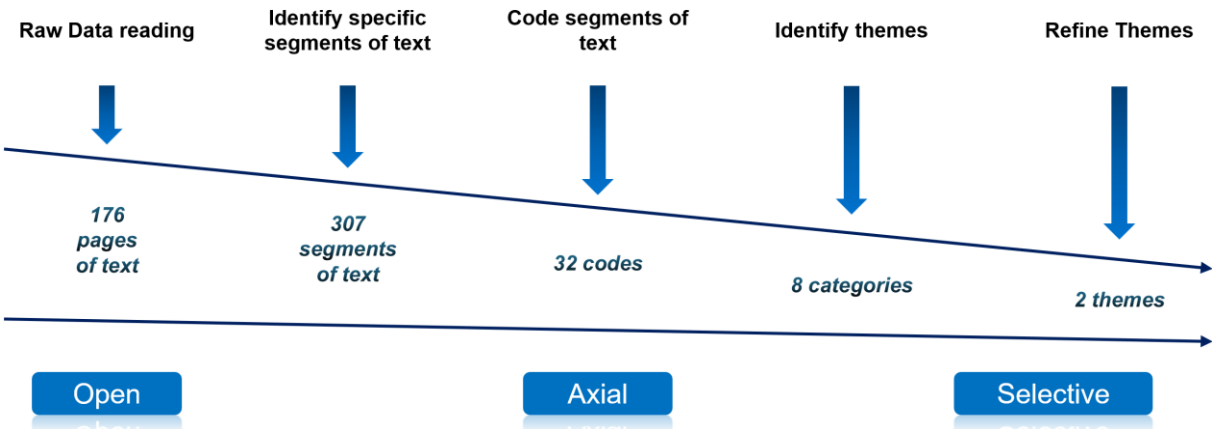
explains participants' experiences and perceptions regarding phishing awareness training.

According to Merriam (2009), thematic synthesis is a variation of content analysis, identifying, analyzing, and recording patterns (themes or categories) from data, divided into five steps:

- **Extract data**: extract data from interview transcripts, focusing on research objectives, context, and results, including primary study information and bibliographic details.
- **Code data**: identify and code relevant concepts, categories, findings, and systematically organize results into a database.
- **Translate categories**: translate and organize into themes, sub-themes, and higher-order themes.
- **Create a hierarchical model of themes**: explore relationships between themes and create a model with higher-order themes.
- **Evaluate synthesis reliability**: assess and validate the reliability of the interpretation from basic data to the final thematic synthesis.

To support the credibility of our findings, triangulation was used by adopting multiple sources of data, such as the mentioned interview transcripts and observation notes, to corroborate findings and enhance the validity of the results. An audit trail was kept, documenting records of the data analysis process, coding decisions and theoretical memos.

Figure 21 - Data analysis and refinement process



Source: the author (2024)

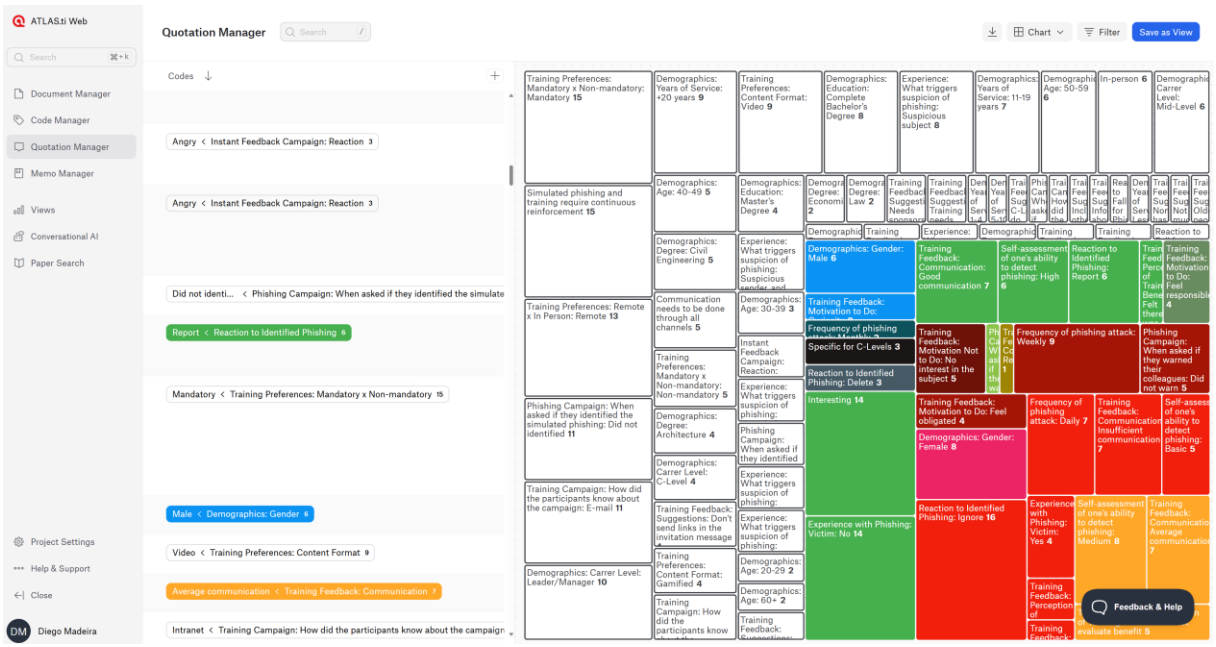
As shown in Figure 21, the process of data analysis and synthesis can be identified, beginning with the initial reading of the transcribed interviews. This process

continues with the identification of specific segments, followed by the coding of these segments. Once the segments are identified, they allow for the grouping of codes into categories, which ultimately enables the refinement of themes.

The findings of the thematic analysis are presented in a structured format, highlighting the main themes and categories. Figure 21 presents the themes, categories, and codes generated from the analysis of interview transcriptions, providing an understanding of the factors that influence the effectiveness of phishing prevention within SAT programs.

To conduct the thematic analysis, the *Atlas.ti*[2] platform was utilized for its capabilities in coding and organizing information. The platform enabled the systematic identification of patterns and the construction of categories directly from qualitative data. It also facilitated the organization and management of large volumes of data, allowing us to draw connections between codes and memos. Additionally, the platform's support for graphical visualization of relationships between categories and subcategories aided in structuring the analysis cohesively.

Figure 22 - Coding Process Using *Atlas.ti* Platform



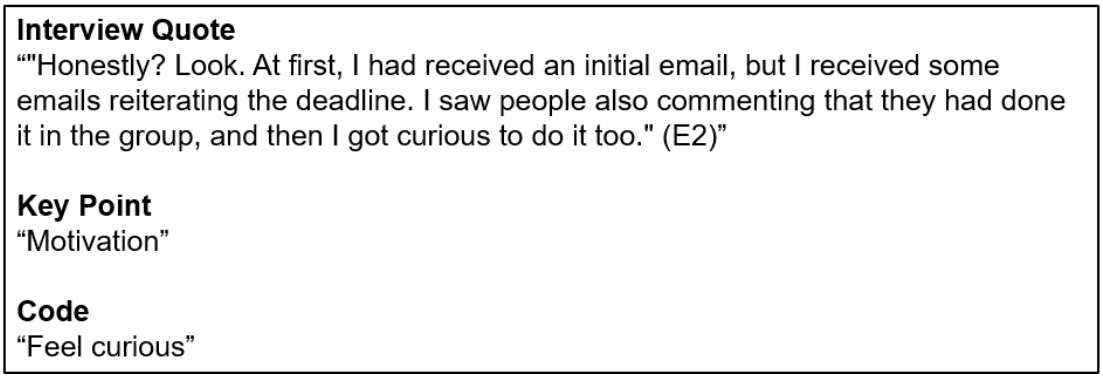
Source - web.atlasti.com (2024)

As shown in Figure 22, we followed the steps recommended by Braun (2006). Research documents such as transcribed interviews were imported into the software. The texts were then read, with relevant segments highlighted and labeled with codes

[2] https://atlasti.com/

representing specific themes or categories. These codes were organized hierarchically and interrelated, providing a detailed view of the data.

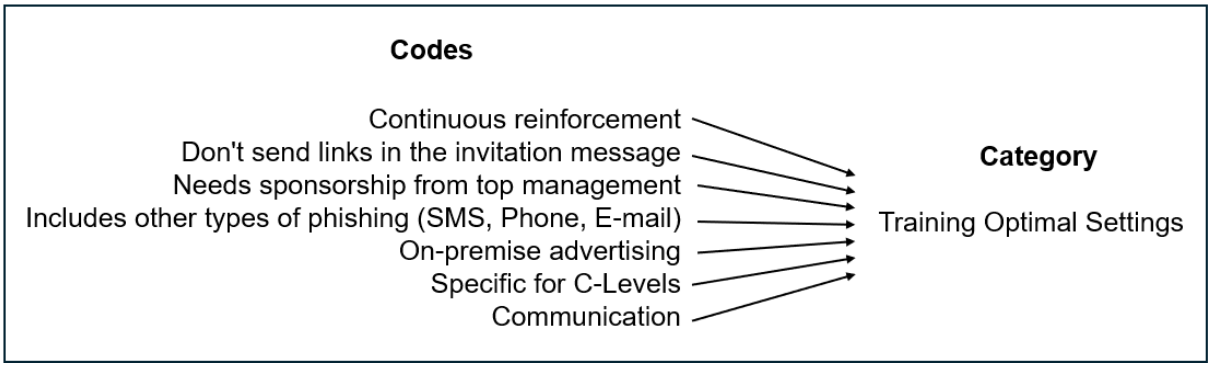
Figure 23 - Illustration of open coding



Source - The Author (2024)

Figure 23 provides an example of the open coding process, showcasing how specific quotes from interview transcripts are analyzed and coded. An interview quote is examined to identify key points, which in this example is identified as "*Motivation*," and the code assigned is "*Feel curious*."

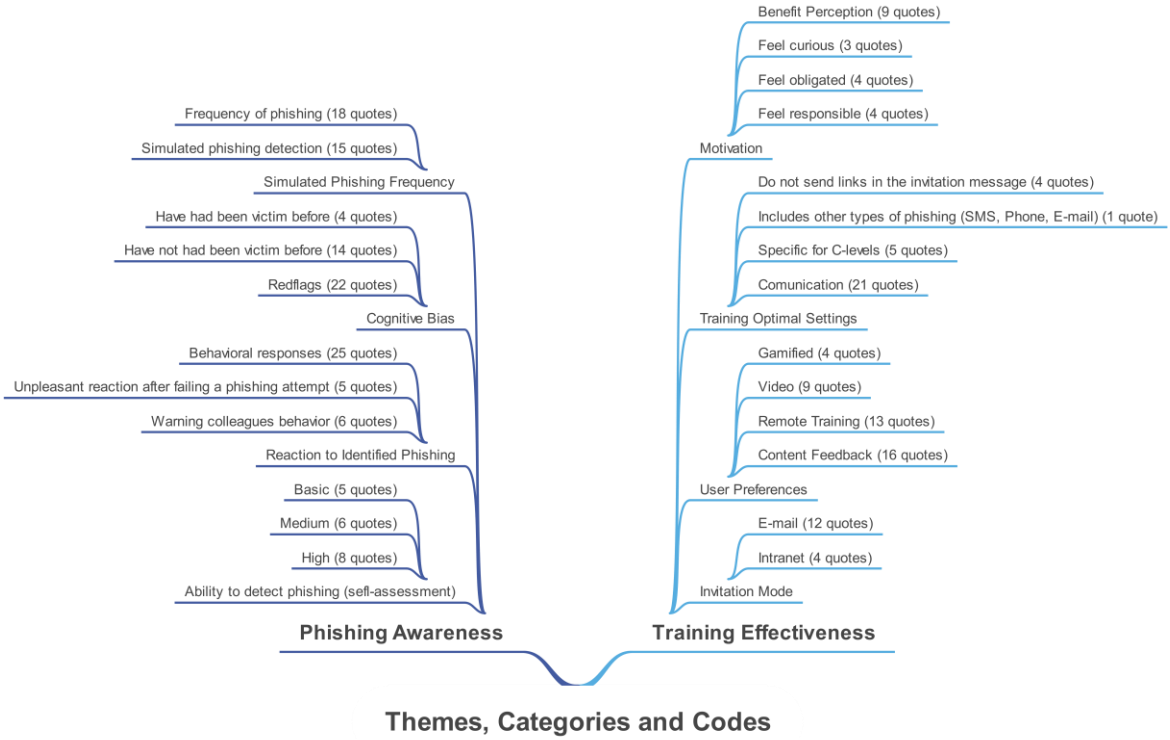
Figure 24 - Building categories with open coding



Source - The Author (2024)

The process of open coding, as shown in Figure 24 consists in identifying and categorizing key themes from the qualitative data. Codes were applied to specific segments of the text that illustrate these themes. These codes are then grouped into a broader category, in this case, "*Training Optimal Settings*.”

Figure 25 - Themes, Categories and Codes



Source - The Author (2024)

Figure 25 was created to visually represent the thematic analysis conducted in this study. It organizes the key themes, categories, and codes that emerged from the data in a structured way, helping to illustrate the connections and patterns discovered during the analysis, making the findings easier to understand.

We obtained 32 codes derived from 307 text segments, which were organized into two main themes: ***Phishing Awareness*** and ***Training Effectiveness***. The ***Phishing Awareness*** theme comprehends categories such as the frequency of phishing, detection of simulated phishing, cognitive biases, behavioral responses, and the ability to detect phishing. The ***Training Effectiveness*** theme includes categories like motivation, training optimal settings, user preferences, and invitation mode. Each category is further broken down into sub-categories, reflecting the analysis of the data.

We distributed the 32 codes into 8 categories. The most frequent codes reflect the main themes that emerged from the interviews, indicating areas of greater emphasis in participant responses. In contrast, the less frequent codes represent more specific or less common insights, which may still be relevant to the qualitative analysis. Table 3 details the frequency of each code:

Table 3 - Codes Frequency

Codes	Frequency	Percentage
Behavioral responses	25	7,82%
Red flags	22	7,17%
Communication	21	6,84%
Ability to detect phishing	19	6,19%
Frequency of phishing	18	5,86%
Employee	16	5,21%
Simulated phishing detection	15	4,89%
Continuous reinforcement	14	4,56%
Mandatory approach	14	4,56%
Haven't had been victim before	14	4,56%
Content feedback	13	4,23%
Prefers remote training	13	4,23%
On-premises advertising	11	3,58%
E-mail	11	3,58%
Video	9	2,93%
Benefit perception	9	2,93%
Warning colleagues' behavior	6	1,95%
Prefers in-person training	6	1,95%
Unpleasant reaction after failing a phishing attempt	5	1,63%
Non-mandatory approach	5	1,63%
Specific for C-levels	5	1,63%
No interest in the subject	5	1,63%
Don't send links in the invitation message	4	1,30%
Feel responsible	4	1,30%
Feel obligated	4	1,30%
Have had been victim before	4	1,30%
Gamified	4	1,30%
Intranet	4	1,30%
Feel curious	3	0,98%
Needs sponsorship from top management	2	0,65%
Career progression	2	0,65%
Includes other types of phishing (SMS, Phone, E-mail)	1	0,33%
	307	**100%**

Source - The Author (2024)

3.4. PHASE 4 - GOOD PRACTICES PROPOSAL

In this phase, we proposed good practices to enhance phishing awareness, addressing RQ2, based on insights from both the quantitative and qualitative studies. To frame the recommendations appropriately, we opted for the term "Good Practices" instead of "Best Practices." While "Best Practices" suggests universally optimal solutions, we recognize the variability of organizational contexts, user behaviors, and resource constraints that may influence the effectiveness of phishing prevention strategies.

These recommended practices combine technical measures with human-centered approaches. The following aspects are explored as potential components of an effective strategy:

- **Tailored Content Delivery**: we propose to investigate whether tailoring training content to the specific needs of different employee groups within the organization could enhance engagement and retention. The effectiveness of such tailored training should be assessed, but it is posited that relevance to the individual's work context may improve the overall impact of the program. This aligns with findings from Steves (2019), who emphasize the importance of contextually relevant training.
- **Different Feedback Mechanisms**: the role of feedback in learning processes is well-documented, and its application in phishing awareness programs warrants further exploration. We investigated whether providing immediate feedback after phishing simulations, as opposed to no feedback, could enhance learning outcomes. Vishwanath (2016) suggest that immediate feedback could help employees correct their mistakes promptly and better retain the lessons learned.
- **Incorporate Real-world Scenarios**: another area of interest is the use of real-world scenarios in SAT programs. Simulated phishing attempts that closely mimic the types of attacks employees are likely to encounter in their daily work may prove more effective in preparing them for real threats. We explored how closely aligning training content with actual phishing tactics could influence the program's success (SUTTER, 2022).
- **Multi-Channel Communication**: Effective communication is essential in phishing awareness campaigns, and the use of multiple channels may help reach a wider audience within the organization. We investigated whether user preferences regarding communication methods, such as emails, intranet posts, webinars, and in-person workshops, can improve engagement. Hagen (2011) found that diverse communication strategies help reinforce awareness messages across an organization.

These proposed good practices are exploratory in nature, and their effectiveness will be subject to further investigation and analysis. The aim is to develop

a thorough strategy that addresses the identified challenges and improves the overall resilience of the organization against phishing attacks.

4. RESULTS

In this chapter we present an integrated analysis of the case study findings, derived from both the quantitative and qualitative studies, followed by the development of good practices for phishing prevention within SAT programs. The results are organized to reflect the distinct phases of the case study:

- **Quantitative Study**: which includes the initial simulated phishing campaign, the training campaign, and the post-training simulated phishing,
- **Qualitative Study:** focusing on participant perceptions, engagement, and experiences gathered through semi-structured interviews,
- **Good Practices Proposal:** developed based on the synthesis of both quantitative and qualitative findings.

4.1. QUANTITATIVE STUDY

This section synthesizes the findings from the quantitative study, integrating data from the **initial simulated phishing campaign**, the **training campaign**, and the **post-training simulated phishing**. The goal is to evaluate the effectiveness of various phishing prevention strategies, focusing on participants' responses to simulated phishing, engagement with the training modules, and changes in behavior following the interventions. The analysis is structured into the following key areas: click-through rates during the simulated phishing campaigns, effectiveness of different feedback mechanisms, participant adherence to mandatory versus non-mandatory training, and overall impact on phishing susceptibility.

4.1.1. Initial Simulated Phishing Campaign

In the first stage, 4,457 participants were exposed to simulated phishing emails using the KnowBe4 platform to measure their initial susceptibility to phishing attacks. The simulation was designed to capture participants' immediate responses to various phishing tactics. Table 4 shows the overall failure rate across the different phishing emails used in the simulation.

Table 4 - Types of Phishing

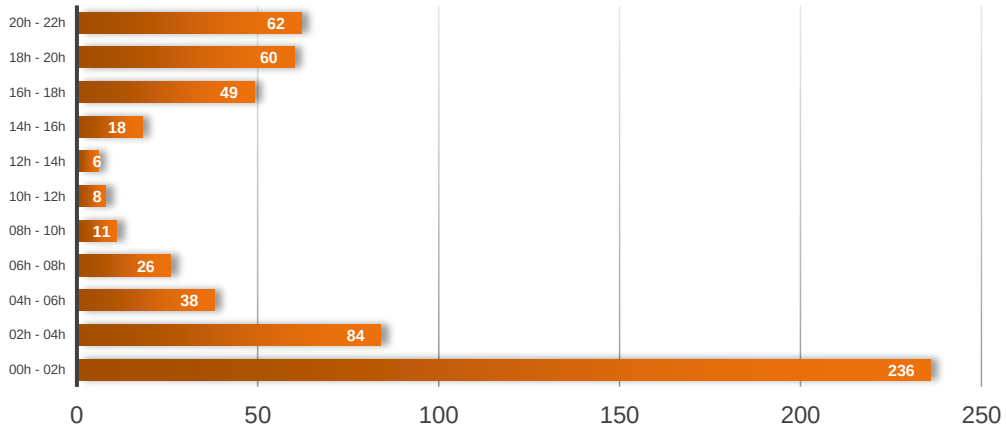
Types of Phishing	Fail Rate
(With Feedback) ALERT: Unauthorized Website Access	25,43%
(With Feedback) Suspicious Activity	19,93%
(No Feedback) Microsoft Account	16,82%

(With Feedback) Strange Emails from Your Account	14,48%
(With Feedback) Microsoft: Mailbox Full	14,84%
(No Feedback) Microsoft 365: Suspicious Activity Report	13,34%
(No Feedback) Microsoft/Office 365: Your Password Will Expire Soon	11,27%
(No Feedback) Microsoft 365: Change Your Password Immediately	8,57%

Source - The Author (2024)

Table 4 reveals differences in fail rates between phishing emails that provided feedback and those that did not. The average fail rate for phishing emails with feedback is 18.24%, whereas for those without feedback, the average fail rate is 12.26%.

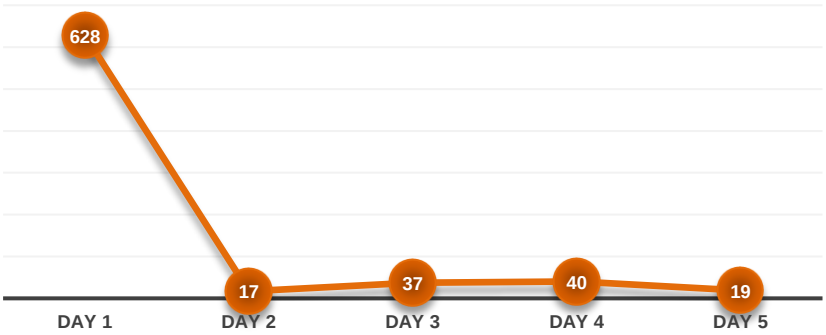
Figure 26 - Failures in the first hours.



Source - The Author (2024)

As shown in Figure 26, the highest concentration of failures occurred within the first two hours, with 236 participants failing during this period.

Figure 27 - Daily Failures Throughout the Phishing Campaign



Source - The Author (2024)

Figure 27 illustrates the daily distribution of failures throughout the campaign. The highest number of failures, 628, was recorded on Day 1, indicating a strong initial impact of the phishing attempt.

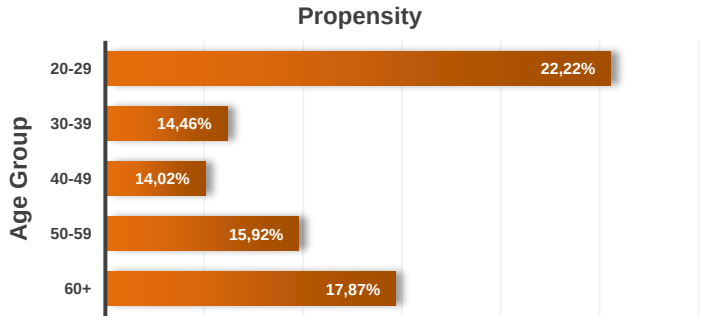
Table 5 - Phishing Propensity

Years of service	Propensity
Less than 1 year	26,04%
1 - 5 years	16,04%
5-10 years	13,08%
10+	15,30%

Source - The Author (2024)

Table 5 shows that participants exhibited varying susceptibility to phishing attempts based on their years of service, as illustrated in the following table, participants with less than one year of service had the highest click-through rate at 26.04%, indicating a significant vulnerability among newer employees. In contrast, those with 1-5 years of service had a click-through rate of 16.04%, while those with 5-10 years and over 10 years of service had rates of 13.08% and 15.30%, respectively. These initial findings highlight the necessity for targeted training interventions for newer employees who are more prone to phishing attacks.

Figure 28 - Phishing Propensity by Age Group



Source - The Author (2024)

In terms of age group, Figure 28 reveals that younger employees are more susceptible to phishing attempts. As illustrated, people aged 20-29 years had the highest failure rate at 22.22%, followed by those aged 30-39 years at 14.46%, 40-49 years at 14.02%, 50-59 years at 15.92%, and 60+ years at 17.87%.

4.1.2. Training Engagement Measurement

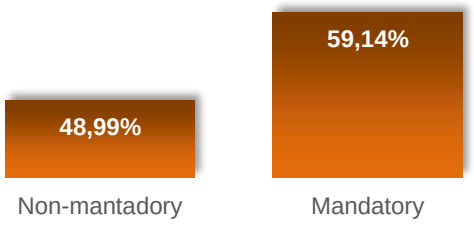
After completing the initial phishing simulation, participants were invited to engage in SAT modules in Knowbe4 platform. The training consisted of three short videos, each lasting between 7 to 8 minutes, covering essential topics such as social engineering tactics and phishing awareness. The objective was to assess how different

training approaches influence participant engagement and completion rates. Overall, 2,073 participants (46.5%) completed the training. However, completion rates varied significantly between the two groups:

- **Mandatory Training**: which achieved a completion rate of 59.14% (1,226 participants). In this group, participants were informed that the training was required, emphasizing the importance of completion.
- **Non-Mandatory Training**: which reached a lower completion rate of 48.99% (1,168 participants). In this group, participants were encouraged to complete the training voluntarily.

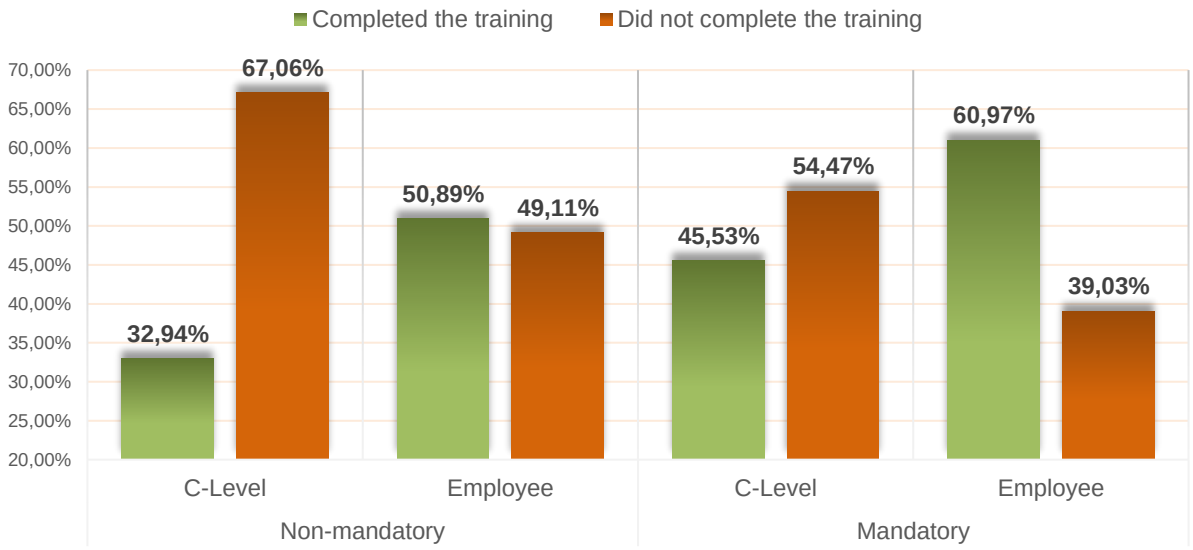
As illustrated in Figure 29, these differences highlight the impact of training requirements on participant engagement and adherence to the training program.

Figure 29 - Training Completion Rate by Group



Source - The Author (2024)

Figure 30 - Training Completion by Group and Approach Type



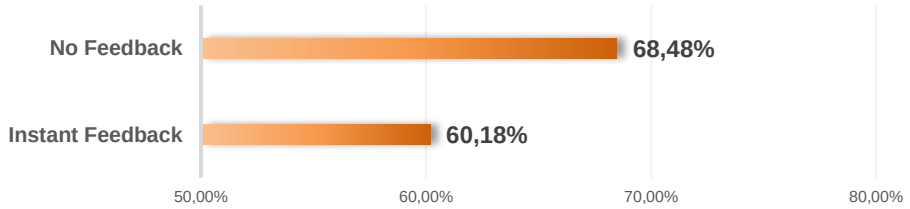
Source - The Author (2024)

As shown in Figure 30, the training completion rates also varied based on participant roles:

- Employees: 60.97% completed the mandatory training, while 50.89% completed the non-mandatory training.
- C-Level Executives: 45.53% completed the mandatory training, while only 32.94% completed the non-mandatory training.

We then investigated the impact of instant feedback on training completion rates. Figure 31 shows that the participants who received no instant feedback had a higher percentage of the training completion rate at 68.48% (266 participants) compared to those with instant feedback at 60.18% (189 participants). This divergence may suggest that while instant feedback can provide immediate corrective information, it may also have unintended consequences that affect overall training adherence.

Figure 31 - Training Completion Rate: No Feedback x Instant Feedback



Source - The Author (2024)

4.1.3. Post-Training Simulated Phishing Campaign

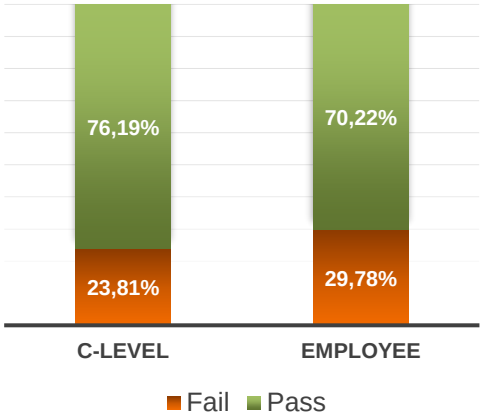
In the final part of the quantitative study, a follow-up simulated phishing campaign was conducted to assess the impact of the security awareness training (SAT) on participants' susceptibility to phishing attacks. We targeted only those participants who had initially failed the first phishing simulation and subsequently completed the training. The objective was to determine whether the training reduced participants' likelihood of falling for phishing attempts and to compare performance between those who received feedback and those who did not.

The participants were divided into the same two feedback groups established in the initial simulation: Group 1 consisted of participants who received immediate feedback after failing the first phishing attempt, while Group 2 included those who did not receive feedback after failing the initial attempt.

The outcomes were further analyzed based on feedback conditions:

- Participants who received **instant user feedback**: Out of 233 participants, 54 (23.18%) failed the phishing attempt again.
- Participants who **did not receive instant user feedback**: Out of 222 participants, 70 (31.53%) failed the phishing attempt again.

Figure 32 - Phishing Propensity after Training



Source - The Author (2024)

Figure 32 shows the results of the post-training simulation, including 455 participants who failed the initial simulation and completed the training. Among C-Level participants, 76.19% (128 participants) avoided the phishing attempt, while 23.81% (40 participants) failed the phishing attempt again. For employees, 70.22% (194 participants) passed the retest, while 29.78% (82 participants) failed again.

Table 6 - Overall Performance in Phishing Simulations and Training

Results after Post-Training Simulated Phishing	C-Levels (Feedback)	C-Levels (No feedback)	Employees (Feedback)	Employees (No Feedback)
Failed and did not complete the training	6,88%	2,02%	7,57%	4,14%
Failed, completed the training, but failed again	1,38%	3,54%	2,61%	3,34%
Failed, completed the training, and passed in the retest	6,88%	3,03%	8,70%	5,43%
Did not fail and completed the training	28,44%	34,85%	38,79%	45,49%
Did not fail and did not complete the training	56,42%	56,57%	42,33%	41,60%

Source - The Author (2024)

Table 6 presents a summary of performance in phishing simulations and subsequent training completion for C-Levels and employees, segmented by whether they received instant feedback after failing a phishing attempt. The feedback mechanism involved redirecting users who failed to a page informing them that they had clicked on a phishing link.

Analyzing the results within the groups, for C-Levels, those who **failed and did not complete the training** had a higher failure rate among those who received

feedback (6.88%, 26 participants) compared to those who did not receive feedback (2.02%, 8 participants). A similar trend is observed among employees, where 7.57% (148 participants) of those who received feedback, failed and did not complete the training, compared to 4.14% (81 participants) of those who did not receive feedback.

In the group of participants who **failed, completed the training, but failed again**, C-Levels who did not receive feedback showed a higher failure rate (**3.54%**, 14 participants) compared to those who received feedback (**1.38%**, 5 participants). The same trend applies to employees, with **3.34%** (65 participants) of those who did not receive feedback failing again, compared to **2.61%** (51 participants) of those who received feedback.

For participants who **failed, completed the training, and passed in the retest**, the success rate was higher among C-Levels who received feedback (**6.88%**, 26 participants) compared to those who did not receive feedback (**3.03%**, 12 participants). This trend is also evident among employees, where **8.70%** (170 participants) of those who received feedback passed the retest, compared to **5.43%** (106 participants) of those who did not receive feedback.

The percentage of participants who **did not fail and completed the training** was higher among those who did not receive feedback, for both C-Levels (**34.85%**, 132 participants) and employees (**45.49%**, 890 participants). For those who received feedback, the completion rate was lower: **28.44%** (108 C-Levels) and **38.79%** (759 employees).

Finally, the percentage of participants who **did not fail and did not complete the training** was similar between the groups. Among C-Levels, the difference was minimal, with **56.42%** (214 participants) among those who received feedback and **56.57%** (214 participants) among those who did not. Among employees, the percentages were **42.33%** (827 participants) for those with feedback and **41.60%** (814 participants) for those without feedback.

To conclude, we recalculated the overall reduction in phishing susceptibility considering all participants of the SAT program. While the initial phishing simulation and training campaign targeted everyone, the retest was conducted only for those who failed the first simulation and completed the training, totaling 455 participants.

After the training, the failure rate among these participants dropped from 100% to approximately 27.25%, as 124 out of 455 participants failed the phishing attempt

again. Using these post-training failure rates, we estimated the global impact of the training on phishing susceptibility. We applied the reduced failure rates among trained participants to estimate a global reduction in phishing susceptibility, resulting in an overall decrease of approximately 7.47% across the entire group.

We presented the quantitative results, which provided empirical evidence on the effectiveness of different training strategies, such as feedback mechanisms, mandatory versus non-mandatory training approaches, and participants' responses across multiple scenarios. This phase addresses RQ1, which aims to identify the main factors that influence phishing prevention strategies.

In the next section, the Qualitative Study, we presented deeper insights into participant perceptions of the training and simulated phishing experiences. The qualitative findings contribute to addressing RQ2, focusing on identifying good practices that improve the effectiveness of security awareness training to prevent phishing.

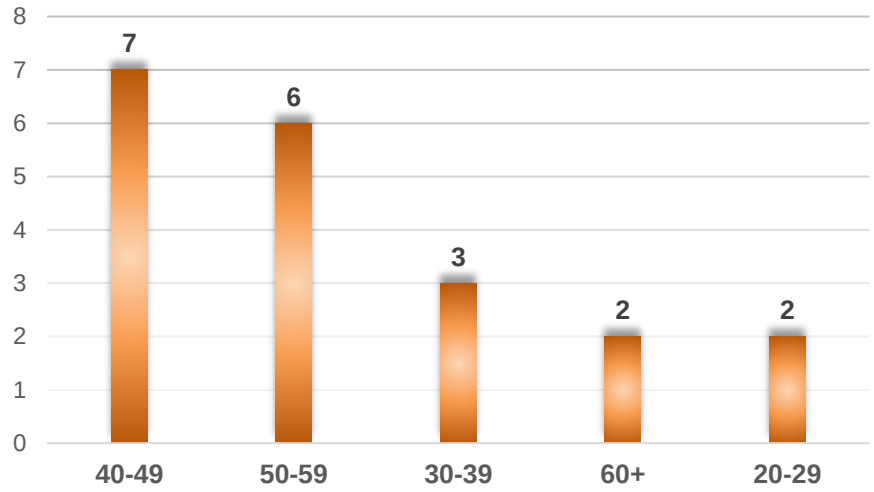
4.2. QUALITATIVE STUDY

In this section, we present the results of the qualitative study that explored participants' experiences and perceptions of phishing prevention within SAT programs. Through semi-structured interviews with 20 collaborators of the studied organization, we analyzed how various aspects of the SAT program influenced user engagement and the perceived effectiveness of training strategies. The interviews addressed topics such as personal encounters with phishing, the relevance of the training content, participant motivation, preferred delivery formats (e.g., video, gamification), and overall impressions of the SAT program.

We aimed to understand how participants perceive and interact with the training content, suggesting insights that contribute to the development of effective strategies for phishing prevention, as outlined in RQ2.

10 interviewees completed the SAT program designed for phishing prevention, while the other 10 interviewees did not participate in the program. Figure 33 presents the age distribution of the interviewees. 7 participants are in the 40-49 age group, representing the largest portion of the sample. This is followed by 6 participants in the 50-59 age group. The 30-39 age group included 3 participants, while the 20-29 and 60+ age groups each had 2 participants.

Figure 33 - Age distribution of participants



Source - The author (2024)

The analysis of the age distribution reveals a predominance of professionals in intermediate age groups, indicating their maturity in the field. This insight could be valuable for tailoring training approaches to meet the specific needs of each age group.

As discussed in the Data Synthesis section, we used Thematic Analysis to identify patterns and categorize the results into two main themes: **Phishing Awareness** and **Training Effectiveness**. Under the **Phishing Awareness** theme, we examined participants' insights on the detection of phishing attempts, their understanding of phishing risks, and the role of cognitive biases in influencing behavior. The **Training Effectiveness** theme focused on how training formats, feedback mechanisms, and user preferences impact engagement and learning outcomes. In the following sub-sections, we discuss both themes.

4.2.1. Phishing Awareness

We present our findings on participants' perspectives related to phishing awareness within the SAT program. We start by categorizing their self-assessed phishing knowledge to understand how it relates to training completion and motivation. Then, we examine personal experiences to understand engagement and responses to the training. Finally, we focus on participants' suggestions for improving phishing prevention efforts.

4.2.1.1. Knowledge Level

Participants' self-assessed knowledge of phishing was categorized in three levels: low, medium, and high. Then we analyzed the relationship between knowledge

levels and training completion. Six participants considered to have a low phishing knowledge level, in which three completed the training. Participants who completed the training, such as E7 and E8, were mainly driven by **feelings of obligation**, as expressed by E7: "*I felt obligated to complete it."* Conversely, E11 and E13, who did not complete the training, indicated a **lack of interest** as the main reason. E13 mentioned, "*no interest in the subject*," but suggested that "*older people prefer more visual (*physical*) communication*," highlighting potential improvements in content delivery to enhance engagement.

Five participants considered themselves to have medium phishing knowledge, of whom two completed the training, resulting in a 40% completion rate. **Feelings of responsibility** were the predominant motivators among those who completed the training, such as E2 and E20. E17, who did not complete the training, cite a **lack of interest**, while also emphasizing the need for **ongoing reinforcement**, stating, "*The training content needs more continuous reinforcement; otherwise, we forget the key points.*"

Among the nine participants with high phishing knowledge, five completed the training, leading to a 55.6% completion rate. Participants like E3 and E9 were **motivated by curiosity** and a **sense of responsibility**. However, participants like E14 and E18, who did not complete the training, found it less relevant due to their existing expertise. E14 commented, "*The training felt less necessary*," indicating a need for more advanced or **tailored content** to maintain engagement among participants with higher knowledge levels.

4.2.1.2. Personal Experiences with Phishing

Personal experiences with phishing played a significant role in shaping participants' engagement with the training. Some participants had previously fallen **victim to phishing** attacks, which influenced their approach to training. All the participants shared their direct experiences with phishing. For example, E8 stated, "*I receive these types of messages regularly, at least once or twice a week."*

Some participants had been directly affected by real phishing, while others managed to recognize and avoid attempts. E1, for example, described a past incident where she was a victim of phishing, leading to a **more cautious approach**: "A*fter that incident, I became much more attentive. Nowadays, I don't even open unfamiliar emails, even if they appear to be from a bank or another institution I'm associated with.*"

E7 noted **frequent exposure to phishing** messages but highlighted her ability to identify them based on specific patterns: "I've never fallen for it, but I receive phishing emails almost daily." E9 mentioned a **proactive approach**, saying, "*I check the sender's address. If it doesn't match the organization, I immediately delete it*," suggesting a more detailed verification process compared to other participants who primarily ignore or delete suspicious messages without further inspection.

However, not all participants showed the same level of alertness. E2 mentioned a past incident: "I *once almost clicked on a link because it looked very convincing. It had the right logo and language, but something fell off, so I stopped*." This participant's experience demonstrates how visual and **content-related** signs can influence susceptibility to phishing, emphasizing the need for better training on recognizing subtle signs. On the other hand, E10 highlighted the importance of experience and context in avoiding phishing attacks, stating, "*Having dealt with many phishing attempts before, I can spot them more easily now. I think curiosity can sometimes be risky*."

4.2.1.3. Suggested Improvements for Phishing Awareness

Participants offered numerous suggestions aimed at improving phishing awareness initiatives within the SAT program. One recurring suggestion was the need for **continuous reinforcement** of training content. For instance, E6 emphasized, *"Phishing awareness campaigns should be a monthly activity, not limited to October or other specific periods,"* stressing the importance of ongoing awareness efforts throughout the year.

Participants also suggested expanding the use of **diverse communication channels** to enhance the reach of awareness messages. E6 recommended using all available channels, such as the **official organization's website**, intranet, email, and even social media, to ensure better dissemination of phishing awareness information. She further suggested placing visual displays in high-traffic areas like hallways or elevators, making it more likely for employees to engage with the content.

Many participants highlighted the need for **clearer communication** and **more engaging content**. E7 noted that the campaign emails often lacked appealing language and visuals, which could contribute to lower engagement rates. She proposed adding **visual aids and clear instructions** to make the content more

engaging, explaining that this process would help employees understand that the training videos are designed to be both informative and interactive.

Several participants mentioned that the training content should be more **contextually relevant**. E7 suggested, *"The training should include scenarios that reflect real work situations,"* to make phishing simulations more relatable and effective. She believed that presenting **phishing attempts similar to emails** commonly seen by employees would enhance their ability to recognize threats in their everyday work environment.

Gamification was another popular suggestion, particularly emphasized by E16, who stated, *"I think a gamified approach with quizzes and leaderboards would make the training more engaging and less monotonous, helping us retain what we've learned better,"* advocating for a more interactive learning environment that could help creating phishing awareness.

E9 proposed improving the **timing and delivery** of training. He suggested that the training should be scheduled during non-peak work hours to avoid conflicts with employees' workloads, thereby increasing participation rates. Additionally, E9 advocated for more **personalized invitations**, highlighting the importance of creating messages that emphasize the training's relevance to the employee's specific role, potentially boosting motivation to participate.

E2 recommended integrating the training with **career progression plans**, arguing that linking training completion to professional growth could serve as a stronger motivator. She also emphasized the need for **simple and clear messaging** in both the training invitations and simulated phishing attempts, suggesting that avoiding complex terminology would ensure broader understanding and engagement among employees.

4.2.2. Training Effectiveness

In this section, we explored interviewees' perspectives on the effectiveness of the SAT program, examining factors that influenced their engagement, completion rates, and overall satisfaction with the training content and format. The analysis focuses on participants' feedback regarding motivation, training delivery modes, content format preferences, and the impact of the invitation process. Their suggestions for improvements are also included.

4.2.2.1. Motivation Factors

Participants showed varying levels of motivation to engage in the training, which influenced their completion rates. The primary motivators included feelings of obligation (E2, E7, E12), professional responsibility (E6, E9, E10), and curiosity (E3, E20).

Participants with lower phishing knowledge levels primarily reported a **sense of obligation** as their main motivation for completing the training. For instance, E2 and E12 mentioned feeling compelled to participate, with E7 explicitly stating, "*I felt obligated to complete it*."

Among those with medium knowledge levels, professional responsibility was a more prevalent motivator. For example, E6 shared that "*it felt like a professional duty to participate*," while E20 also cited a **sense of responsibility** as a driving factor.

Participants with higher phishing knowledge levels were largely driven by **curiosity**. E3 explained, "*I was curious to see how the training aligned with what I already knew*." E20 also echoed this sentiment, demonstrating that curiosity might play a key role in engaging those already familiar with phishing concepts.

4.2.2.2. Training Delivery Modes

The delivery mode of the training had a distinct impact on participant engagement and completion rates. Out of the 20 interviewees, 13 preferred **remote training** (E1, E2, E3, E6, E7, E8, E9, E12, E13, E14, E17, E18, E20), mainly due to its flexibility and convenience. For instance, E8 noted, "*Remote training works better for my schedule*." Despite the convenience, some participants found remote sessions less engaging, citing the lack of interaction.

On the other hand, seven interviewees preferred **in-person training** (E4, E5, E10, E11, E15, E16, E19), emphasizing the benefits of direct interaction and immediate feedback. E4 explained, "*In-person training sessions make it easier to ask questions and clarify doubts*." This suggests that face-to-face training could be more effective in encouraging a clearer understanding of the content.

4.2.2.3. Content Format Preferences

The format of the training content was a key factor in shaping participants' engagement. They expressed preferences for **video-based content**, **gamification**, and other interactive formats. The majority of interviewees (15 out of 20) preferred

video-based content for its clarity and structured format (E1, E2, E3, E4, E5, E6, E7, E8, E9, E10, E11, E12, E17, E20). E9 mentioned, "*Video training was clear and easy to follow, making it suitable for all knowledge levels*." This preference highlights the effectiveness of videos in delivering information across various knowledge levels.

Although less common, five participants specifically recommended **gamified content** to create a more interactive experience (E10, E15, E16, E18, E19). E16 suggested, "*A gamified approach with quizzes and leaderboards would make it more engaging and less monotonous*," indicating that gamification could enhance participant engagement and retention.

Analyzing the training format preferences by function reveals distinct patterns between employees and C-Level executives. Employees show a strong preference for **video-based training**, with 80% (12 out of 15) indicating this choice. On the other hand, C-Level executives have a more balanced distribution: 40% (2 out of 5) prefer videos, 20% (1 out of 5) prefer gamified content, and another 40% (2 out of 5) have no specific preference. This suggests that, while video training is the dominant format among employees, C-Level executives tend to value diverse approaches, possibly due to an interest in more interactive or **flexible methods**.

Additionally, interviewees provided positive feedback on the video content, appreciating the dynamic and varied approaches used. E20 remarked, "*I liked it because it was quick. So, even though it was mandatory, even though it took that extended period where you have to look at it for a long time*." E2 commented, "*I think it is explored in a… clearer way, I think it is more dynamic. Even for us to watch, it catches our attention, I think it's better*."

Several participants (8 out of 20) emphasized the need for the training to reflect **real-life scenarios** (E2, E4, E6, E7, E10, E11, E13, E17). For instance, E7 proposed, "*The training should mimic actual emails we receive at work to be more relatable*," underscoring the importance of **realistic simulations** in improving phishing awareness.

4.2.2.4. Invitation Process and Engagement

Participants suggested that the training invitations could be more personalized to improve engagement. For instance, E2 remarked, "*The email invitations were often too generic; a more personalized approach could help*," highlighting the potential of **tailored messages** to increase participation rates.

Ten interviewees recommended using **clearer language** in training invitations to enhance understanding and motivation (E3, E4, E6, E7, E8, E10, E11, E13, E17, E20). E11 emphasized, “*Avoiding complex terminology would make the training more accessible*,” suggesting that simplifying the language could make the training more inclusive and effective across different knowledge levels.

Participants reported varied levels of satisfaction with the organization’s communication about the training. Out of the 20 interviewees, 7 rated the communication as good (E2, E7, E10, E11, E14, E16, E19), indicating that they found the information clear and accessible. Nine participants rated it as regular (E3, E4, E5, E8, E13, E15, E17, E20), suggesting that the communication was adequate but could benefit from improvements in clarity and engagement. Four participants expressed dissatisfaction, labeling it as bad (E1, E6, E9, E12), emphasizing issues such as unclear messaging and **lack of personalization**. These responses indicate that while communication was generally effective, there is room for enhancement.

4.2.2.5. Benefit Perception

Participants' perception of training benefits emerged in the qualitative study as a key factor influencing engagement. Our qualitative findings reveal that participants’ perception of the training's benefits influenced their motivation to engage with phishing awareness programs. While a portion of the participants, such as E7 and E20, recognized the value of understanding phishing risks and felt that the training enhanced their vigilance, others, like E4 and E8, saw limited personal relevance or tangible benefit from the sessions.

For instance, E8 remarked, "*It didn't change anything.*" E4 simply stated, "*I don't think so*.", when asked if there was a perceived benefit of the training. One participant, E7, emphasized the nature of the training, stating, "*The message about not clicking on phishing links must be conveyed. All the information, from the concept to the consequences of falling victim, is important and was well-presented in the training material*." This underscores the importance of covering all aspects of phishing awareness, from understanding what phishing is to learning how to avoid it and recognizing the potential consequences.

E7 also reflected on their pre-training knowledge, saying, "*Before the training, it was more of a tacit understanding. I had access to the information but couldn't always*

recall specific details." This suggests that the training helped solidify and clarify their existing knowledge.

E6 found the training enjoyable and acknowledged its contribution, stating, *"It was enjoyable, but you don't know what it is until you do it. I think it contributed positively.*" Similarly, E12 expressed gaining new knowledge, "*Yes, there were some things about phishing I didn't know. It was good to learn about them*."

E20 observed an increase in vigilance, noting, "*It even helps people remember better. They become more alert to those types of messages asking to click here or do something. You become more attentive.*" Clearly communicate the benefits of phishing awareness training and demonstrate its impact on improving detection skills to enhance user buy-in and perceived value.

4.2.2.6. Suggested Improvements for Training

Finally, we gathered several suggestions from interviewees to improve phishing awareness training. Their proposals centered around three main areas: continuous reinforcement, varied training formats to suit different learning styles, and stronger incentives linked to career progressions.

- **Continuous Reinforcement**: seven interviewees (E2, E4, E6, E7, E8, E10, E17) emphasized the importance of **regular reinforcement** to maintain phishing awareness. E6 suggested implementing "*monthly campaigns*" rather than confining efforts to specific periods of the year, to keep the topic consistently in focus, enhancing long-term retention and readiness.
- **Variety in Training Delivery**: ten interviewees (E1, E3, E4, E5, E6, E8, E11, E13, E16, E19) recommended diversifying training formats to offer different learning possibilities. E3 proposed a mix of videos, quizzes, and hands-on simulations, believing that this strategy could better engage a wider range of participants by addressing diverse learning styles.
- **Linking Training to Career Progression**: five interviewees (E2, E4, E7, E9, E13) suggested that associating training completion with career progression could serve as a stronger motivator. E2 commented, "*If it were tied to career progression, more people would take it seriously*."

This strategy could encourage higher participation rates and reinforce the importance of training within the organization.

4.3. GOOD PRACTICES PROPOSAL

In this section, we present seven actionable recommendations, referred to as “good practices”, which were developed by synthesizing the insights gained from both the quantitative and qualitative components of this research. These practices aim to address key gaps and opportunities identified during the analysis, offering strategies to enhance phishing awareness and improve the effectiveness of SAT programs. We identified key areas where adjustments to simulated phishing deployment, training content, delivery, and engagement methods could improve participants’ responsiveness to phishing threats.

Table 7 presents the association between the quantitative and qualitative studies with the proposed practices, demonstrating how they emerged from our findings. Quantitative data reveal measurable trends, while qualitative findings add depth through participant experiences and perspectives, supporting the development of the proposed practices to improve phishing awareness and training effectiveness.

Table 7 - Relationship Between Findings and Proposed Practices

Evidence from Quantitative Study	**Evidence from Qualitative Study**	**Proposed Practice**
Participants with less experience (1-5 years) and younger employees (20-29 years) demonstrated higher phishing susceptibility, highlighting the need for demographic-specific adjustments.	• Participants with high knowledge levels found the training too basic. E14: "*The training felt less necessary*." C-Level participants emphasized the need for more strategic scenarios relevant to their roles. E9: "*Having dealt with many phishing attempts before, I can spot them more easily now*." • E12: "*There were some things about phishing I didn't know. It was good to learn about them*," supporting the need for varied content based on knowledge levels.	Adjust Training Content to Different Roles and Knowledge Levels
Participants who received no feedback had a higher failure rate in the post-training phishing simulation (31.53%) compared to those who received immediate feedback (23.18%).	• Frustration was reported after failing in a phishing simulation. E3: "*[…] don't these people have anything better to do? I am in the middle of an activity*." • Participants recommended continuous reinforcement. E17: "*The training content needs more continuous reinforcement; otherwise, we forget the key points*." E6: "*Security awareness training should be a monthly activity*."	Implement Strategic Feedback and Continuous Reinforcement
More realistic phishing scenarios showed higher initial failure rates (e.g., 25.43% for the "*Unauthorized Website Access*" simulation).	• Realistic scenarios were perceived as more relevant. E7: "The training should mimic actual emails we receive at work to be more relatable." • Generic simulations were considered less impactful. E9: "*I check the sender's address. If it doesn't match the organization, I immediately delete it*."	Use Realistic and Scenario-Based Simulations

Participants without immediate feedback showed higher training completion rates than those who received feedback after failing a simulated phishing.	• Linking training to career progression was suggested to increase motivation. E2: "*If it were tied to career progression, more people would take it seriously*." • Participants saw career-related incentives to align training relevance with personal and professional growth.	Link Training to Career Development Initiatives
Completion rates were higher when invitations emphasized mandatory participation.	• Participants found generic invitations less engaging. E2: "*The email invitations were often too generic; a more personalized approach could help*." • Clarity in messaging was highlighted as important. E11: "*Avoiding complex terminology would make the training more accessible*."	Optimize the Invitation Process
Participants received daily reminders	• Suggestions included hallways, elevators, and intranet as communication spaces. E7: "Using multiple platforms can ensure broader engagement." • E6: "Using all available channels, like intranet, email, and even social media, can improve awareness	Adopt a Multi-Channel Communication Strategy
Video content was widely accepted and had good completion rates.	• Video content was preferred by most participants. E3: "*The video training was clear and easy to follow*." • Gamification was suggested to increase engagement. E16: "*A gamified approach with quizzes and leaderboards would make it more engaging and less monotonous*."	Use Engaging Learning Elements

Source - The Author (2024)

The evidence from the quantitative and qualitative studies revealed both strengths and challenges that shaped the proposed practices. Positive aspects, such as the effectiveness of immediate feedback and video content, were balanced against issues like frustration following simulation failures and lower training adherence among certain groups.

Our insights guided the development of practices aimed at addressing gaps while leveraging successful strategies. The proposed practices also incorporate suggestions directly from participants, who offered perspectives on improving the effectiveness and engagement of phishing awareness efforts. In the following subsections, we describe seven good practices to improve SAT programs designed to prevent phishing.

4.3.1. Practice 1 - Adjust Training Content to Different Roles and Knowledge Levels

To adjust training to reflect participant's roles and knowledge levels we propose the following actions:

- **Develop Role-Specific Scenarios**: create training modules that address phishing threats relevant to specific departments or job functions, helping participants relate training content to their responsibilities.

- **Offer Knowledge-Based Modules**: provide basic training for participants with lower phishing knowledge while offering advanced topics for those with higher familiarity to ensure relevance and engagement.

The recommendation to tailor phishing awareness training to employees' roles and knowledge levels emerged from findings in the quantitative and qualitative analyses. The study revealed distinct engagement patterns tied to participants' knowledge levels: those with low phishing knowledge showed higher completion rates when training was mandatory, driven by feelings of obligation. Participants with higher knowledge levels, however, were more likely to complete the training if they perceived it as relevant and challenging, indicating that a "one-size-fits-all" approach may reduce effectiveness across diverse groups.

In the qualitative study, interviewees emphasized the importance of content relevance, expressing a desire for scenarios that reflect their specific responsibilities. For example, C-Level participants expressed a need for training that acknowledges the strategic risks they meet. Additionally, interview responses highlighted that participants with higher familiarity with phishing felt the standard content was too basic, suggesting a need for advanced material to maintain their engagement.

4.3.2. Practice 2 - Implement Strategic Feedback and Continuous Reinforcement

We propose the following actions to implement strategic feedback and continuous reinforcement:

- **Provide Immediate Feedback**: deliver instant feedback after phishing simulations to allow employees to understand and learn from their mistakes.
- **Schedule Monthly or Quarterly Refreshers**: regular refresher simulations and modules to reinforce phishing awareness and help employees retain critical concepts.

The recommendation to incorporate strategic feedback and continuous reinforcement in SAT Programs designed for phishing prevention stems from both quantitative and qualitative research findings that emphasize the positive impact of immediate feedback and continuous exposure on training effectiveness. The quantitative study indicated that participants who received immediate feedback after failing a phishing attempt demonstrated a higher awareness and recall in subsequent simulations, showing an improvement in phishing detection skills.

Qualitative insights further reinforced this practice, with participants expressing a need for regular reminders to maintain their awareness over time. Participants highlighted the value of periodic phishing campaigns and reminders, which they felt would sustain awareness and keep security practices fresh in their minds.

4.3.3. Practice 3 - Use Realistic and Scenario-Based Simulations

The recommendation to develop realistic, scenario-based phishing simulations is grounded in findings from qualitative findings. The interviewees emphasized the need for realism, stating that simulations that closely were aligned with their daily responsibilities felt more impactful, based on their experiences. For example, employees mentioned that scenarios involving typical email communication patterns were more engaging and helped them apply what they learned in the training to real-world situations. This sentiment was especially prevalent among those in roles that involved frequent email communication, as well as among C-Level participants, who expressed a preference for simulations that highlighted scenarios relevant to their strategic decision-making responsibilities.

We propose the following actions to implement realistic, scenario-based simulations:

- **Create Authentic Phishing Scenarios**: design simulations to reflect real-world phishing tactics, fostering more realistic responses.
- **Incorporate Role-Based Simulations**: deploy phishing simulations according to specific job roles, making the subsequent training directly relevant to participant's everyday work.

4.3.4. Practice 4 - Link Training to Career Development Initiatives

We suggest the following actions to link phishing awareness training with career development initiatives:

- **Incorporate Training into Career Milestones**: link completion of specific training modules to career progression requirements, such as eligibility for promotions or participation in advanced projects, providing tangible incentives and aligning training with participants' professional aspirations.
- **Offer Both Mandatory and Optional Advanced Modules**: include a core set of mandatory training for all employees, complemented by optional advanced

modules for those seeking additional knowledge or skill enhancement, allowing participant's to further specialize in areas relevant to their roles and interests.

The recommendation to integrate phishing awareness training into career development programs derives from key findings in both the quantitative and qualitative studies, which highlighted motivation as a critical factor in training engagement. The quantitative analysis revealed that mandatory training achieved higher completion rates among participants, particularly those with lower phishing knowledge levels, who often completed the training out of a sense of obligation. However, the qualitative study shed light on a potential improvement: participants suggested that linking training to career progression would create a more compelling reason for engagement, making it feel beneficial rather than simply obligatory.

Qualitative feedback further underscored this point, with participants expressing that connecting training to career growth could increase motivation, recommending that training could be recognized as part of their professional growth journey, reinforcing both their skills and their commitment to organizational security.

4.3.5. Practice 5 - Optimize the Invitation Process

We propose the following actions to optimize the training invitation process:

- **Personalize and Make Role-Relevant Invitations**: design invitations that emphasize the training's relevance to each participants' specific role, reinforcing the value of the training and helping employees connect it to their daily responsibilities.
- **Use Clear, Accessible Messaging**: create invitations in simple, direct language to make the training's purpose easy to understand. Avoid jargon and complex terminology to ensure that the training's objectives are clear to all recipients, regardless of their familiarity with security terms.
- **Emphasize Mandatory Nature for Core Modules**: for essential training modules, communicate the mandatory nature clearly, setting clear expectations for participation, particularly among employees and C-Levels.

The quantitative study highlighted a noticeable difference in completion rates between mandatory and non-mandatory training modules, suggesting that clear communication about training requirements influences engagement levels. Meanwhile,

the qualitative study revealed that many participants found the invitations too generic, noting that a more personalized approach could boost engagement.

Feedback from participants emphasized that invitations should be relevant to their roles and use straightforward language. Interviewees mentioned that tailored, role-specific messaging could help emphasize the importance of the training for their daily responsibilities, making it feel directly applicable. Additionally, some participants pointed out that clear, straightforward messaging would make the purpose of the training more engaging.

4.3.6. Practice 6 - Adopt a Multi-Channel Communication Strategy

To adopt a robust multi-channel communication strategy, we recommend the following actions:

- **Utilize Diverse Communication Platforms**: deliver phishing awareness content through a variety of channels, such as emails, intranet posts, social media, and even physical displays in common areas. Utilizing multiple platforms enables the organization to ensure that all participants encounter awareness messages regularly, regardless of their preferred mode of communication.
- **Conduct Ongoing Awareness Campaigns**: schedule regular in-local SAT trainings to reinforce training concepts and keep security top of mind, helping sustain participants' awareness and encouraging proactive behavior against phishing threats.

The recommendation to implement a multi-channel communication strategy arises from findings in both the qualitative study, which showed, accordingly to interviewees, that regular exposure to security awareness content can significantly improve retention. The post-training simulated phishing sent in the quantitative study highlighted the effectiveness of reinforcement in reducing failure rates over time, while the qualitative feedback emphasized the importance of consistent reminders and diverse communication formats.

Interviews revealed that participants were more likely to engage with security awareness messages when they also encountered them in their everyday work environments, rather than only through a single channel. For example, participants recommended leveraging high-traffic areas, such as hallways or elevator screens, to display key security awareness reminders. Others highlighted the value of digital

channels like email and intranet, with some suggesting that the use of social media could increase engagement, specifically among younger employees. These insights emphasize the need to reach employees where they are, both physically and digitally, to strengthen security awareness within phishing prevention continuously.

4.3.7. Practice 7 - Use Engaging Learning Elements

We propose the following actions to implement diverse and engaging learning elements:

- **Focus on Video Content as a Core Element**: utilize video as the primary format for SAT to prevent phishing, given its approachability, allowing straightforward explanations that resonate with participants across varying levels of phishing knowledge.
- **Add Gamification and Interactive Elements**: introduce quizzes, and other interactive features to create a more dynamic learning environment. Gamified elements encourage active participation and serve as an alternative for participants who benefit from hands-on, scenario-based learning, serving to those who may find traditional training formats less engaging.

The recommendation to integrate engaging learning elements, such as video-based content and gamification, is based on participant feedback highlighting their preferences for varied, interactive formats in phishing awareness training. Interviewees in the qualitative study responded positively to the clarity and engaging approach of video content, noting that it made the training easy to understand. This appreciation was attributed to the quality of the video material, which allowed participants to engage meaningfully with the content without feeling overwhelmed.

Additionally, participants with more advanced knowledge or those in higher-level positions indicated that while they valued the clarity of videos, they also desired interactive elements like quizzes and gamified components to keep the training dynamic, suggesting a balanced approach that could improve engagement across all levels.

5. DISCUSSION

We assess findings from the mixed-method case study, providing a comprehensive view of the study's contributions, while also situating them within the broader context of existing literature on phishing prevention within SAT programs.

We conducted a case study using a mixed-methods approach to investigate strategies for improving phishing awareness within SAT programs through an integrated analysis of quantitative and qualitative data. We adopted a combination of simulated phishing campaigns, targeted training modules, and semi-structured interviews.

Quantitative findings revealed the importance of mandatory training in achieving higher completion rates. Additionally, immediate feedback following phishing simulations proved effective in enhancing participants' knowledge retention and reducing failure rates in the subsequent simulation, highlighting the value of real-time corrective actions. Further analysis showed that phishing susceptibility correlated with variables like years of service and age group, with newer and younger employees showing a higher propensity to click on phishing links.

The qualitative study provided a deeper understanding of these findings by analyzing participants' personal experiences and preferences. Participants expressed a need for training content tailored to their roles and knowledge levels, highlighting that a standardized approach might not be sufficient for effective SAT outcomes. Moreover, they identified realistic, scenario-based simulations as essential for creating a meaningful connection with the training. Participants also emphasized the importance of continuous reinforcement and multi-channel communication, suggesting that regular, diverse exposure to phishing awareness content could help them better recognize and respond to threats. Building on these insights, we developed a set of good practices aimed at improving phishing awareness within SAT programs. These practices were derived from the synthesis of both quantitative and qualitative findings and address common challenges in phishing prevention.

Reflecting on the study's findings, it becomes clear that effective phishing awareness training demands more than conventional methods. Our research highlights the importance of addressing participants' distinct motivations, knowledge levels, and engagement needs, which collectively influence their interaction with SAT programs. Data from both quantitative and qualitative studies highlight those strategies

such as tailored feedback, scenario-based simulations, and aligning training relevance with participants' roles improve effectiveness. Furthermore, incorporating career development elements into phishing prevention initiatives provides a compelling incentive for better engagement, indicating a shift from traditional approaches. Our findings advocate for a strategic, multi-faceted approach to SAT programs, emphasizing the need for adaptability to meet dynamic organizational needs. With this context, we now turn to the research questions to analyze how they were addressed through this study’s integrated findings.

5.1. MAIN FACTORS

We examined which factors contribute to the effectiveness of phishing prevention strategies within SAT programs to answer RQ1 by analyzing the application of immediate feedback versus no feedback after phishing simulation failures and the impact of mandatory versus non-mandatory training invitations. Although the methodology initially focused on these factors, our findings identified an additional key factor: participants' benefit perception. Our analysis revealed that mandatory invitations increased training completion rates, and immediate feedback improved phishing detection skills, both improving the effectiveness of the SAT program. We discuss these findings, including the role of benefit perception, in this section.

The quantitative analysis revealed a significant difference in phishing detection success between participants who received **immediate feedback** and those who did not. Among the participants who received instant feedback, 207 out of 266 (77.8%) avoided phishing in subsequent simulations, whereas only 115 out of 189 (or 60.8%) of those who received no feedback were able to avoid phishing., demonstrating a notable improvement in detection accuracy associated with immediate feedback, and suggesting a direct correlation between timely corrective feedback and enhanced phishing detection skills.

The positive influence of immediate feedback aligns with findings from Vishwanath et al. (2016) and Steves et al. (2019), who underscore the role of timely feedback in reinforcing training retention. However, these results also point to potential challenges: while feedback supports skill acquisition, it must be carefully managed to prevent over-reliance on corrective input, which may diminish vigilance when real-world cues are subtler, or feedback is absent.

Another factor is negative and positive implications of **no feedback for baseline assessment**. Participants who did not receive feedback after failing phishing simulations offered valuable insights into their unassisted detection capabilities. Of this group, only 115 out of 189 participants avoided phishing in subsequent simulations, reflecting a 17% less success rate compared to those who received instant feedback. This provided a useful baseline for evaluating intrinsic phishing awareness levels. While this feedback-free approach was less effective for immediate skill enhancement, it allowed us to assess employees' natural detection abilities without external guidance, revealing areas where additional reinforcement may be necessary for long-term awareness. This finding aligns with research indicating that withholding feedback can expose persistent vulnerabilities by simulating real-world conditions in which such guidance is unavailable (SOSAFE, 2023).

While withholding feedback provides a baseline for assessing intrinsic phishing awareness, it also introduces quite a few challenges. First, the absence of feedback led to an increase in user complaints to the IT Service Desk, as participants expressed frustration over receiving a suspicious e-mail. Although none of the participants expressed any concerns, we suggest that the absence of feedback in phishing simulations could lead to distrust in the organization's automated phishing detection and blocking systems, potentially causing administrators to question whether these solutions are sufficient to protect against threats. Consequently, it is imperative to align the decision to withhold feedback with organizational leadership to ensure a clear communication strategy and avoid unintended effects. A collaborative approach can help mitigate negative user perceptions and maintain trust in the organization’s overall information security strategy.

Another factor is the effectiveness of **mandatory invitations** on completion rates. Our analysis of training completion rates reveals notable differences in engagement between participants invited through mandatory and non-mandatory approaches, particularly when segmented by organizational role. For C-Level participants, mandatory invitations resulted in a 57.44% completion rate, which is significantly higher than the 42.56% completion rate observed among those receiving non-mandatory invitations. This outcome suggests that a mandatory approach is more effective in driving training engagement among senior management, likely because C-Level individuals recognize the organizational importance attached to mandatory

directives. This finding aligns with the literature, which indicates that training framed as mandatory can resonate more strongly with higher-level employees who may feel a heightened sense of responsibility and accountability (JOHNSON, 2021).

For general employees, however, the difference in completion rates between mandatory and non-mandatory groups is minimal. Mandatory invitations led to a completion rate of 50.66%, while the non-mandatory group achieved a similar rate of 49.34%. This close percentage suggests that, unlike C-Level participants, employees are less influenced by the mandatory nature of the invitation alone. Our results here align with findings by Smith (2020), who noted that lower-level employees often respond more to practical and intrinsic motivators rather than formal obligations, resulting in similar engagement levels regardless of whether training is mandatory or optional.

We suggest that the limited influence of mandatory invitations on the Employee group's completion rates may also been reduced due to cultural factors within the organization. Because the invitation originates from the IT department that is not directly above them in the organizational hierarchy, employees may not feel a strong sense of responsibility to comply. In this context, it becomes necessary to secure sponsorship from senior leadership for mandatory training initiatives. When employees see that training has the support and endorsement of upper management, they are more likely to perceive it as essential, increasing their likelihood of participation.

However, this strategy comes with a potential drawback. Relying solely on mandatory invitations backed by upper management may not lead to meaningful engagement over the medium and long term. Employees might complete the training simply out of obligation, without genuine interest or motivation. Over time, this compliance-driven approach can limit the effectiveness of the training, as participants may not fully absorb or apply the knowledge gained. Finally, while mandatory invitations with executive sponsorship can increase initial compliance, fostering an intrinsic motivation to participate remains essential for long-lasting impact, which leads us to the following section.

Another factor is the **benefit perception** of the security awareness training, which is a motivational factor that aligns with self-determination theory, emphasizing that individuals are more motivated to engage in activities they view as personally valuable (DECI, 2000). When employees understand the relevance of the training to

their own roles and see it as a tool for protecting themselves and the organization, their intrinsic motivation increases. Studies indicate that this sense of perceived benefit leads to higher engagement and better retention of information (COMPEAU, 1999).

In light of these findings, we recommend incorporating clear explanations of how phishing awareness contributes to both personal and organizational security, tailored to each department's unique needs. Additionally, presenting data on the financial and reputational costs of phishing attacks can help underscore the importance of training for all employees, not just those in IT. Ultimately, although benefit perception of the security awareness training serves as a strong motivational factor, sustaining it over time necessitates continuous reinforcement. We recommend implementing periodic refreshers and regularly updating training content to ensure that employees continue to perceive the training as relevant and valuable.

In conclusion, our analysis of the main factors influencing the effectiveness of phishing prevention strategies within SAT programs highlights the relationship between the use of feedback in phishing simulations, mandatory invitations, and participants' benefit perception. Immediate feedback proved effective in improving phishing detection skills, while the absence of feedback allowed for baseline assessments but introduced challenges in user experience and organizational trust. Mandatory invitations increased engagement, mostly among C-Level participants, but demonstrated limited long-term impact on intrinsic motivation. Benefit perception emerged as a key factor, aligning with motivational theories and emphasizing the need to communicate the value of training continuously.

5.2. GOOD PRACTICES

The proposed good practices were developed by synthesizing findings from both the quantitative and qualitative studies, addressing RQ2. In this section, we examine each recommendation, drawing on insights gathered from participant responses, data analysis, and existing literature on phishing awareness strategies. Our goal is to critically evaluate the potential benefits, implementation challenges, and broader implications of each practice, considering how personalized approaches in phishing prevention may address specific organizational needs and participant characteristics. Furthermore, we assess the effectiveness and practicality of each proposed practice in strengthening organizational resilience against phishing threats.

In **Practice 1** we proposed **Adapting training content** to match participants' knowledge levels and roles, offering several benefits. Studies indicate that contextually relevant content increases retention and engagement. Hamari (2014) highlights that personalized content tends to be more engaging and encourages active participation, which can lead to sustained reductions in phishing susceptibility.

However, customizing training poses operational challenges and may require considerable investment. Developing distinct content for each knowledge level and role demands substantial resources, both in terms of creation and ongoing updates. Furthermore, organizing employees into knowledge or role-based groups can complicate training management. Guidance from institutions like the National Institute of Standards and Technology (NIST, 2024) notes that while personalization offers benefits, the managerial complexity and associated costs may limit this approach's feasibility in large organizations.

Another challenge is ensuring that tailored training does not inadvertently create perceptions of inequality among employees. Segmenting training by knowledge and role, if not managed carefully, could lead to discomfort among participants who feel undervalued if they receive basic training.

We suggest a gradual and focused approach to personalization, starting with basic adaptations for specific groups, such as departments more vulnerable to phishing attacks, and expanding as the program’s effectiveness is validated.

In **Practice 2**, que present the **Use of feedback** represent another practice we shed light for discussion. Some interviewees expressed negative emotions after falling for simulated phishing attempts. For example, E3 stated, "*How did I not check this thing before? And secondly, the person keeps thinking: don't these people have anything better to do? I am in the middle of an activity [...] The security people should be full of tasks.*" indicating that failing phishing simulations can elicit strong emotional responses. Another participant, E6, mentioned, "*It's a horrible experience.*" Similarly, E11 noted, "*I think a lot of people get angry with this.*" These statements illustrate the frustration and irritation experienced by participants when they realize they have been tricked by a simulated phishing attempt.

Considering these emotional responses and their effects in subsequent training engagement, feedback shall be used strategically, as it can be a valuable tool for raising a constructive learning environment. Studies have shown that immediate

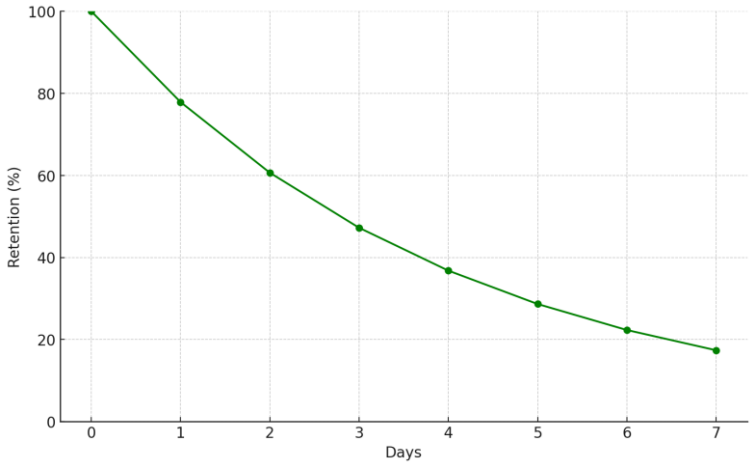
feedback after phishing simulations allows employees to recognize and correct their errors quickly, leading to better retention of phishing identification skills (VISHWANATH, 2016; STEVES, 2019). Feedback enables users to gain insights into their mistakes and improve their awareness without feeling overly discouraged. Furthermore, it reinforces correct behavior, helping employees to become more vigilant over time.

However, there are strategic reasons for choosing **not to provide feedback** in certain phishing simulations. For instance, simulations without feedback can better replicate real-world phishing scenarios where feedback is not given, thereby testing an employee's "true" resilience over time without influencing their actions after each failed attempt. Research suggests that withholding feedback in some cases may reveal baseline awareness levels and highlight persistent vulnerabilities, as it prevents employees from anticipating corrective guidance (SOSAFE, 2023). This method allows organizations to assess the natural detection rates and weaknesses in employee responses to phishing attempts, offering an authentic measure of susceptibility.

Ultimately, the choice between providing or withholding feedback in phishing simulations should align with the training objectives. When the goal is to educate and build skills over time, feedback can be instrumental. Conversely, when the aim is to assess baseline resilience or gauge long-term awareness without immediate corrective influence, withholding feedback can provide clearer insights. Balancing both approaches may offer comprehensive insights into employee susceptibility while progressively enhancing phishing awareness and resilience across the organization.

Another relevant aspect we highlight for discussion in **Practice 2** is **continuous reinforcement**. While it might be convincing to conduct phishing simulations frequently, studies indicate that sending more than three simulated phishing emails per month can lead to decreased effectiveness (SOSAFE, 2023; LAIN, 2022).

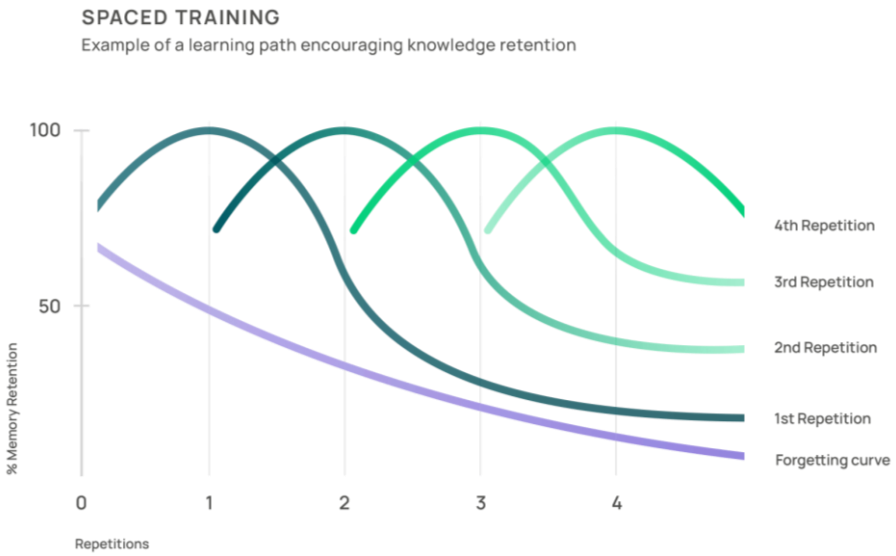
Figure 34 - Forgetting Curve



Source - Adapted from SOSAFE (2023)

As shown in Figure 34, a large-scale study found that regular simulated phishing helps reinforce employees' memory and skills in identifying real phishing attacks (PROOFPOINT, 2024), effectively combating the “forgetting curve” described by Hermann Ebbinghaus in 1885, sustaining that information is forgotten at an exponential rate if not reviewed or reinforced. A research study by JAMPEN (2020) revealed that the training knowledge retention period is estimated to fall between 7 days and five months.

Figure 35 - Overcoming the Forgetting Curve



Source - SOSAFE (2023)

As demonstrated in Figure 35, considering that SAT programs are designed for phishing prevention involve phishing simulations followed by training, it is important to emphasize the need for regular training. General recommendations suggest conducting phishing campaigns once a month. This interval helps avoid employee saturation and maintains training effectiveness. (SOSAFE, 2023).

In **Practice 3** we explore the practice of **scenario-based simulations** in our discussion. The recommendation to develop scenario-based phishing simulations tailored to participants' specific roles arose from qualitative findings in which participants reported that realistic simulations made the training more relevant and engaging.

Research supports that scenario-based training can lead to improved retention and practical application (HAMARI, 2016; CARPENTER AND ROER'S; 2022), as aligning phishing simulations with realistic situations can encourage employees to engage more deeply, and strategic interventions should be integrated into employees' daily practices, fostering continuous learning and adaptation to changes in the threat landscape.

However, implementing realistic, role-based simulations with instant feedback introduces a critical concern. Vishwanath (2011) suggests that when participants receive immediate feedback after simulated phishing failures, their perception of phishing risks can diminish over time, potentially undermining the effectiveness of real-world detection efforts. Knowing they will receive corrective feedback may reduce users' sense of urgency or risk when confronted with real phishing threats, leading to a false sense of security.

We also focus on **Practice 4** in this discussion**,** which proposed **linking training to career development**. The suggestion to link training to career development as a practice emerged from insights indicating that participants, especially those with lower phishing knowledge levels, were more likely to complete mandatory training out of a sense of obligation. Additionally, participants in the qualitative study expressed that connecting training to career progression could increase motivation, shifting it from a compliance-based activity to a growth-oriented experience.

Johnson (2021) studies suggest that incorporating information security skills into professional development milestones raises a sense of relevance around the

training, encouraging employees to view these skills as a part of their career growth. Similarly, Smith (2019) argues that aligning training with career development objectives boosts retention of content, as employees come to see the training as an investment in their own professional advancement.

On the other hand, some studies criticize this approach. Harris (2020) found that organizations implementing career-linked training requirements may see employees completing the minimum necessary to pass, rather than engaging deeply with the material. Additionally, Zhao (2018) argue that linking training to career objectives can distract from the primary goal of true security awareness, as employees might prioritize meeting the requirement over applying security practices meaningfully in their daily work.

An additional key aspect we focus on for discussion is the **invitation process** proposed in **Practice 5**. Comparing engagement levels between mandatory and non-mandatory training approaches provided valuable insights for creating a more effective SAT program. Among the 4,457 training sessions conducted, 59.14% (1,226 out of 2,073) were completed as mandatory, while 48.99% (1,168 out of 2,384) were completed as non-mandatory. These results show that mandatory training sessions achieved a higher completion rate, suggesting that requiring employees to participate increases their likelihood of doing so. Mandatory training helps ensure broad participation, which is essential for establishing a basic level of awareness across the organization. In contrast, non-mandatory training depends on voluntary participation, which may not achieve the same level of coverage. Overall, the higher completion rates for mandatory training sessions suggest that organizations should consider implementing mandatory training policies to ensure that all employees receive essential training. However, there are negative effects that must be considered.

As Gordon (2019) investigated, mandatory training may increase completion rates, but it has the potential to build resistance and demotivation among employees because employees may view the program as the imposition of something they are forced to do, not an opportunity for them to grow. Moreover, since the training is mandatory, frequent or lengthy sessions may end up causing an information overload, and thus, knowledge of the employees gets stored superficially, as they will only do enough training to get done with it without understanding most of the contents. These weaknesses demand the creation of training programs that must be mandatory but

engaging and should not be exhaustive in their delivery and the number of times delivered.

In **Practice 6 - Adopt a Multi-Channel Communication Strategy,** our study suggests that using various communication channels may enhance participant engagement and knowledge retention, as participants are more likely to interact with security messages presented consistently across different platforms.

In the quantitative study, participants received daily email reminders emphasizing the need to complete the training. Since the training campaign was conducted only once, with no additional experiments and without daily reminders, it is not possible to assess the specific impact of these reminders on user engagement. However, we believe that the mandatory invitation format, combined with daily reminders, played an important role in encouraging adherence to the training. Additionally, in the qualitative study, participants suggested using non-digital channels for communication, such as posting reminders in hallways and elevators. We consider this approach to be valuable, as it can effectively reach individuals in certain age groups or roles who may not frequently check email.

In **Practice 7** we focused on **using engaging learning elements**. The preference for video-based training among 80% of participants aligns with research highlighting video as an effective medium for delivering clear, structured, and easily digestible information across various knowledge levels. Vishwanath (2016) found that video content is particularly advantageous in security training due to its visual appeal and capacity to simplify complex information, making it accessible to both IT and non-IT staff. This aligns with participant statements in this study, such as E3's and E8's appreciation for video format, which they found straightforward and effective for varied levels of knowledge. E3 mentioned, "*I liked the experience of this format. The video, right? I had never done training like this before*." Similarly, E8 stated, "*I think a video is always a good thing*."

However, the study also found that while gamified content appeals to some participants (20%), it did not necessarily translate to completion rates. Only 25% of those who favored gamified training completed it, suggesting potential barriers in gamified content that may detract from actual engagement. Research by Hamari et al. (2014) emphasizes that while gamification enhances engagement by incorporating interactive elements, it may not universally appeal to all learners. Instead, Hamari et

al. suggest that the appeal of gamification often depends on individual learning preferences and motivations, which could explain why participants who preferred gamified training often did not engage with the video-based modules.

Additionally, participants who favored gamified training often displayed a lack of interest in video content, suggesting divergent learning preferences. E15 and E16's comments reflect a common theme in educational psychology: learners with a preference for interactive, hands-on content may find static video formats less engaging. This insight resonates with findings from Schmid (2014), who observed that learners with high kinesthetic tendencies are more likely to engage with gamified, interactive content than with passive formats like video. For example, E15 stated, "*And I never participated in any specific training for this, no*." E16 mentioned, "*I just gave an okay, that I was aware of it, but actually, I didn't watch the training. I was not given any training. I gave okay, read everything there, but I didn't do the training*."

The study also explored training delivery modes, revealing a preference for remote training (65%) due to flexibility and convenience. This finding is supported by NIST (2024), which suggests that remote training enhances accessibility, particularly in large or dispersed organizations. Remote training, as mentioned by participants like E3 and E5, provides the flexibility to complete training at one's own pace, which can enhance engagement. However, 35% of participants expressed a preference for in-person training, valuing the immediacy of direct interaction and feedback. This aligns with findings from the Infosec Institute (2023), which emphasize that in-person training can foster a more immersive learning experience, supporting better information retention.

While this study identifies and proposes seven good practices to enhance phishing awareness and improve the effectiveness of Security Awareness Training (SAT) programs, it is relevant to acknowledge that these practices do not encompass the entirety of potential strategies for phishing prevention. For instance, although the proposed practices address critical elements such as tailored training, feedback mechanisms, and engaging learning methods, additional measures may be necessary to strengthen organizational resilience, including the integration of advanced threat detection tools and aligning SAT programs with broader risk management frameworks. Furthermore, the adoption of real-time monitoring and adaptive training systems could complement the practices proposed in this study.

Another consideration is the variability in organizational contexts. The effectiveness of SAT programs can be influenced by factors such as organizational size, employee demographics, and available resources. Future research should explore how these contextual differences impact the applicability and outcomes of SAT practices, potentially leading to the development of additional strategies tailored to specific environments.

In summary, we found both the advantages and limitations of different training formats. While video content offers broad accessibility, gamification requires careful implementation to avoid barriers that may prevent completion. Similarly, while remote training provides flexibility, in-person sessions remain valuable for participants who prioritize real-time interaction.

In sum, the seven proposed good practices focus on encouraging a balanced and strategic approach to phishing awareness within SAT programs. Findings from both quantitative and qualitative studies were synthesized into actionable recommendations to improve engagement, retention, and overall effectiveness. These practices proposed emphasize tailoring content to participants' knowledge levels and roles, using feedback strategically, ensuring continuous reinforcement through regular simulations and trainings, and incorporating realistic, scenario-based training.

Finnaly, linking training to career development and refining the invitation process increases participation and sustains interest over time. And multi-channel communication strategies and engaging learning formats, such as video content and gamification, demonstrate potential for effectively reaching diverse audiences. While these approaches present operational challenges, the benefits of cultivating a proactive security culture outweigh the complexities.

6. CONCLUSIONS

The aspects of phishing awareness and prevention have been examined across measurable areas, such as phishing concepts, socio-technical email attacks, consequences for individuals and organizations, and decreasing susceptibility rates through simulations and training. Participants receiving immediate feedback demonstrated less engagement but a stronger learning curve regarding their mistakes, despite some negative reactions reported in interviews. Consequently, immediate feedback should be carefully aligned with the objectives of the phishing awareness campaign to maximize its benefits.

Our findings show that phishing prevention training significantly improves participants' ability to recognize and respond to phishing attempts. Key factors include participants' benefit perception, mandatory participation, strategic feedback, video-based training, and continuous reinforcement. Additionally, qualitative insights highlight the importance of communicating the training’s benefits engagingly to maximize effectiveness.

6.1. THEORETICAL AND PRACTICAL CONTRIBUTIONS

In our case study, through a mixed-methods approach, we investigated main factors that influence training effectiveness, such as the strategic use of feedback, mandatory and non-mandatory training invitations, and participants' perception of benefit. Then, the insights gathered from both quantitative and qualitative findings served as the foundation for developing our proposed good practices for phishing prevention within SAT programs.

With these findings, we extend the knowledge based on SAT effectiveness, advancing both the theoretical framework and practical strategies of SAT programs designed to prevent phishing attacks, bridging the gap between theory and practice. Our study aimed at identifying the main factors that influence the effectiveness of phishing awareness programs. Theoretical contributions emerge from a detailed examination of elements such as instant feedback—given immediately after a participant interacts with a simulated phishing email—and the impact of mandatory versus non-mandatory training formats. These factors are analyzed in terms of how they affect user engagement, knowledge retention, and behavioral responses. The results will enrich existing theories on feedback effectiveness, motivation, and user

compliance within security contexts, offering an understanding of how these factors interact in successful security awareness programs.

The study also provides insights into the structure of SAT programs, exploring how different combinations of training approaches and feedback strategies contribute to participant's motivation and adherence, offering a perspective on the theoretical dynamics of training design, moving beyond traditional compliance-based approaches to focus on genuine user engagement.

The integration of quantitative findings from phishing simulations and training, and qualitative insights from participant interviews establishes a background for understanding and improving the effectiveness of security awareness training programs focused on phishing prevention.

This study also reinforces Carpenter and Roer's (2022) perspective that organizational security should transcend technical measures and reach cultural integration while proposing good practices aligned with the strengthening of security culture, creating an environment where security becomes an intrinsic value. Thus, the practices discussed in our study can be implemented as part of a broader strategy for cultural transformation, aligned with the organization's long-term security goals.

From a practical perspective, we developed a set of good practices derived from our integrated analysis of quantitative and qualitative data to improve the effectiveness of security awareness training programs focused on phishing prevention. We applied semi-structured interviews to gather participants' perceptions and experiences, uncovering important details that are often overlooked in quantitative studies. These interviews highlight key aspects such as the perceived benefit of the training content, the effect of feedback on user behavior, and how mandatory versus voluntary participation impacts engagement. The findings support the creation of a set of training strategies that can be adjusted to fit different organizational needs, ensuring that security awareness programs designed to prevent phishing are not only conceptually strong but also effective in practice.

6.2. THREATS TO VALIDITY

Addressing potential threats to validity is necessary to strengthen the conclusions of our study. We discuss in this section the threats to validity identified in our case study, applying data triangulation to improve the reliability of our results

through the combination of insights from simulated phishing tests results and semi-structured interviews, helping us to provide an understanding of the research problems, as we cross-check data from different sources to confirm patterns and findings.

In the quantitative study, a key threat to internal validity is selection bias. To address statistical validity and quantitative representativeness in our sample selection, we referenced Creswell (2014), who emphasizes the importance of a sufficiently large sample to ensure the validity of quantitative research results. Using a large number of participants reduces selection bias and enhances the generalizability of findings. In this case, we aimed for a statistically valid sample that represents a diverse range of experiences and perspectives within the organization, selecting half of the employees to participate. Additionally, Creswell advocates for purposive sampling in cases where certain subgroups may have unique perspectives that are critical to the research. Following this, we included all C-level executives in our sample.

Another potential threat to internal validity in the quantitative study is non-response bias, which occurs when the characteristics of participants who chose not to respond or complete the training differ significantly from those who participated, potentially skewing the results (MERRIAM, 2009). For instance, employees who opted out might have lower motivation or awareness of phishing risks, leading to an overestimation of the SAT program's effectiveness. Conversely, highly aware individuals may have avoided the training, perceiving it as redundant. To mitigate this, participation rates were closely monitored, and measures were implemented to address potential gaps. Specifically, communication efforts were intensified by increasing the frequency of reminder emails, reinforcing the importance of the training, and ensuring that participants were aware of their enrollment.

In the qualitative study, researcher bias is an inherent concern during participant selection and analysis of the collected data. The semi-structured interviews provided flexibility but also introduced the possibility of researcher influence through question phrasing or interpretation. To reduce this risk, we strictly adhered to the interview protocol and employed independent coding by two researchers to ensure consistency (MERRIAM, 2009).

Another potential threat to validity in the qualitative study is recall bias. Participants’ ability to accurately recall and report their experiences with phishing attempts and training programs may affect the reliability of the data, leading to either

underreporting or exaggeration (MERRIAM, 2009). To address this, interview questions were crafted to be specific, assisting participants in accurately remembering and describing their experiences. Additionally, the interviews began with more personal questions related to real phishing attempts, as these are commonly encountered by most individuals, helping contextualize the discussion, and situating participants in a relevant and familiar scenario before moving on to more structured questions about the simulated phishing and training programs.

Lastly, considering that the study was conducted within a single organizational context, external validity may be limited. The unique structure and culture of this organization could influence the effectiveness of security awareness training designed to prevent phishing differently than in other settings. To address this, we compared our findings with existing literature and studies from varied organizational contexts to identify common patterns.

6.3. FUTURE WORK

We point out future research directions that may extend our understanding of phishing awareness and prevention. Future work may need longitudinal research studies to capture the long-term effectiveness of different phishing awareness programs, shedding light on the longevity of training effects and identify highly effective strategies to sustain behavioral change. Additionally, more research is needed to understand the effectiveness of various types of training, such as gamified approach, and other types of simulated phishing attacks (Instant messaging, phone, SMS and USB Drives). Understanding the relative effectiveness of these approaches can inform the design of more impactful training programs.

Future studies could also look at the design and effects of individual differences in demographics and cognitive styles on phishing awareness training. Tailored training might help drive engagement and effectiveness. Further research may identify unique cognitive biases that increase vulnerability to phishing. Knowing which biases, such as urgency, familiarity, and authority, affect decision-making can result in more sophisticated anti-phishing implementations.

Another direction is to explore how incorporating state-of-the-art technologies like artificial intelligence and machine learning can design more adaptive and

responsive phishing detection systems. These technologies could also customize and deliver content in real time.

Moreover, another possible future work is to validate the proposed good practices in different organizational contexts. We may implement these practices in various organizational backgrounds, such as small businesses, large companies, universities, and government agencies. We aim to assess the suitability of the proposed good practices across different scenarios, leading to more effective implementation and tailoring the good practices to specific organizational needs, such as industry-specific threats or demographic profiles of employees.

7. REFERENCES

ATHULYA, A. A.; PRAVEEN, K. Towards the detection of phishing attacks. In: *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 2020. Anais [...]. Tirunelveli: IEEE, 2020. p. 337-343. Disponível em: https://doi.org/10.1109/ICOEI48184.2020.9142967.

ABAWAJY, J. User preference of cyber security awareness delivery methods. *Behavior & Information Technology*, v. 33, n. 3, p. 237-248, 2012. Disponível em: https://doi.org/10.1080/0144929x.2012.708787.

ALIYU, M.; BAGARAWA, M. U.; MU'AZU, A. N.; UMAR, M. Understanding phishing awareness among students in tertiary institutions and setting-up defensive mechanisms against the attackers. *Caliphate Journal of Science and Technology*, v. 5, n. 1, p. 22-31, 2023. Disponível em: https://doi.org/10.4314/cajost.v5i1.4.

ALKHALIL, Z. Phishing attacks: a recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, v. 3, p. 563060, 2021.

ALLODI, Luca et al. On the need for new antiphishing measures against spear phishing attacks. *IEEE Security & Privacy*, v. 18, n. 2, p. 23-34, 2020.

ALSHAIKH, M. Toward sustainable behaviour change: an approach for cyber security education training and awareness. 2019.

ALSHAIKH, M.; MAYNARD, S. B.; AHMAD, A. Security education, training, and awareness: incorporating a social marketing approach for behavioural change. In: *International Information Security Conference*. Cham: Springer International Publishing, 2020. p. 81-95.

ASSENZA, G. A review of methods for evaluating security awareness initiatives. *European Journal for Security Research*, v. 5, p. 259-287, 2020.

APWG. *Phishing activity trends reports*. Disponível em: https://www.antiphishing.org/trendsreports/.

BAGUI, L.; LUSINGA, S.; PULE, N.; TUYENI, T. T.; MTEGHA, C. Q.; CALANDRO, E.; SOLMS, B. v. The impact of COVID-19 on cybersecurity awareness-raising and mindset in the Southern African Development Community (SADC). *The Electronic Journal of Information Systems in Developing Countries*, v. 89, n. 4, 2023. Disponível em: https://doi.org/10.1002/isd2.12264.

BAIG, M. S.; AHMED, F.; MEMON, A. M. Spear-phishing campaigns: link vulnerability leads to phishing attacks. In: *2021 4th International Conference on Computing & Information Sciences (ICCIS)*. Anais [...]. IEEE, 2021. Disponível em: https://ieeexplore.ieee.org/document/9676394/.

BAUER, S.; BERNROIDER, E. W. N. The effects of awareness programs on information security in banks: the roles of protection motivation and monitoring. In:

Human Aspects of Information Security, Privacy, and Trust: Third International Conference. Cham: Springer International Publishing, 2015. p. 154-164.

BAYL-SMITH, P.; TAIB, R.; YU, K.; WIGGINS, M. Response to a phishing attack: persuasion and protection motivation in an organizational context. *Information and Computer Security*, v. 30, n. 1, p. 63-78, 2021. Disponível em: https://doi.org/10.1108/ics-02-2021-0021.

BEER, M.; FINNSTROM, M.; SCHRADER, D. The great training robbery. *Harvard Business School Research Paper Series*, n. 16-121, 2016.

BHARDWAJ, A.; SAPRA, V.; KUMAR, A.; KUMAR, N.; ARTHI, S. Why is phishing still successful? *Computer Fraud & Security*, v. 2020, n. 9, p. 15-19, 2020.

BROADCOM INC. Symantec 2019 Internet security threat report. Disponível em: https://docs.broadcom.com/docs/istr-24-2019-en.

BURDA, P.; ALLODI, L.; ZANNONE, N. Don't forget the human: a crowdsourced approach to automate response and containment against spear phishing attacks. In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2020. p. 471-476.

CARPENTER, P.; ROER, K. *The security culture playbook: an executive guide to reducing risk and developing your human defense layer*. Hoboken: Wiley, 2022.

CLARKE, V.; BRAUN, V. *Successful qualitative research: a practical guide for beginners*. Thousand Oaks: Sage, 2013.

COMPEAU, Deborah; HIGGINS, Christopher A.; HUFF, Sid. Social cognitive theory and individual reactions to computing technology: a longitudinal study. *MIS Quarterly*, p. 145-158, 1999.

CORRADINI, Isabella. Redefining the approach to cybersecurity. *Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology*, p. 49-62, 2020.

CRESWELL, John W.; CRESWELL, J. David. *Research design: qualitative, quantitative, and mixed methods approaches*. Thousand Oaks: Sage Publications, 2017.

D'ARCY, J.; HOVAV, A.; GALLETTA, D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, v. 20, n. 1, p. 79-98, 2009. Disponível em: https://doi.org/10.1287/isre.1070.0160.

DAREM, A. Anti-phishing awareness delivery methods. *Engineering Technology & Applied Science Research*, v. 11, n. 6, p. 7944-7949, 2021. Disponível em: https://doi.org/10.48084/etasr.4600.

DECI, Edward L.; RYAN, Richard M. *Intrinsic motivation and self-determination in human behavior*. Springer Science & Business Media, 2013.

DIVAKARAN, D. M.; OEST, A. Phishing detection leveraging machine learning and deep learning: a review. *arXiv preprint*, 2022. Disponível em: https://arxiv.org/abs/2205.07411.

DOWNS, J.; HOLBROOK, M.; CRANOR, L. Behavioral response to phishing risk. *Communications of the ACM*, v. 50, n. 11, 2007. Disponível em: https://doi.org/10.1145/1299015.1299019.

DOWNS, Julie S.; HOLBROOK, Mandy B.; CRANOR, Lorrie Faith. Decision strategies and susceptibility to phishing. In: *Proceedings of the Second Symposium on Usable Privacy and Security*, 2006. p. 79-90.

EISEN, O. In-session phishing and knowing your enemy. *Network Security*, v. 2009, n. 3, p. 8-11, 2009.

ETIKAN, Ilker. Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, v. 5, n. 1, p. 1-4, 2016.

FBI. Internet Crime Complaint Center (IC3) 2022 Internet Crime Report. Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

FEDERAL TRADE COMMISSION (FTC). How to recognize and avoid phishing scams. *Consumer Information*. Disponível em: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing.

FLICK, Uwe; VON KARDOFF, Ernst; STEINKE, Ines (Ed.). *A companion to qualitative research*. Thousand Oaks: Sage Publications, 2004.

GAMISCH, L. A study of different awareness campaigns in a company. *Proceedings of the ACM*, 2023. Disponível em: https://doi.org/10.1145/3600160.3605006.

GAVETT, B. E.; ZHAO, R.; JOHN, S. E.; BUSSELL, C.; ROBERTS, J. R.; YUE, C. Phishing suspiciousness in older and younger adults: the role of executive functioning. *Plos One*, v. 12, n. 2, e0171620, 2017. Disponível em: https://doi.org/10.1371/journal.pone.0171620.

GO-GLOBE. The importance of employee training: statistics and trends. 2018. Disponível em: https://www.go-globe.com/the-importance-of-employee-training-statistics-and-trends/. Acesso em: 11 maio 2024.

GORDON, W.; WRIGHT, A.; GLYNN, R.; KADAKIA, J.; MAZZONE, C.; LEINBACH, E.; LANDMAN, A. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association*, v. 26, n. 6, p. 547-552, 2019. Disponível em: https://doi.org/10.1093/jamia/ocz005.

GUPTA, B. B.; TEWARI, A.; JAIN, A. K.; AGRAWAL, D. P. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, v. 28, p. 3629-3654, 2017.

GUPTA, Surbhi; SINGHAL, Abhishek; KAPOOR, Akanksha. A literature survey on social engineering attacks: phishing attack. In: *2016 International Conference on Computing, Communication and Automation (ICCCA)*. Anais [...]. IEEE, 2016. p. 537-540.

HADNAGY, Christopher; FINCHER, Michele. *Phishing dark waters: the offensive and defensive sides of malicious emails*. Hoboken: John Wiley & Sons, 2015.

HAGEN, J.; ALBRECHTSEN, E.; HOVDEN, J. Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, v. 16, n. 4, p. 377-397, 2008. Disponível em: https://doi.org/10.1108/09685220810908796.

HAMARI, Juho; KOIVISTO, Jonna; SARSA, Harri. Does gamification work?—a literature review of empirical studies on gamification. In: *2014 47th Hawaii International Conference on System Sciences*. Anais [...]. IEEE, 2014. p. 3025-3034.

HARRIS, L.; NGUYEN, P. Compliance vs. engagement in security training: a critical analysis. *Cybersecurity and Behavioral Studies*, v. 7, n. 4, p. 89-105, 2020.

IBM. Cyber resilience organization report 2020. Disponível em: https://www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report. Acesso em: 21 set. 2023.

INFOSEC INSTITUTE. 10 factors for implementing successful and effective security awareness training. 2023. Disponível em: https://www.infosecinstitute.com/blog/10-factors-for-implementing-successful-and-effective-security-awareness-training/. Acesso em: 22 jun. 2024.

JAMPEN, D.; GÜR, G.; SUTTER, T. S.; TELLENBACH, B. Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*, v. 10, n. 1, 2020. Disponível em: https://doi.org/10.1186/s13673-020-00237-7.

JARI, Mousa. An overview of phishing victimization: human factors, training and the role of emotions. *arXiv preprint*, 2022. Disponível em: https://arxiv.org/abs/2209.11197.

JOHNSON, A.; BROWN, T. The role of cybersecurity skills in career development. *Journal of Security Awareness*, v. 5, n. 2, p. 145-160, 2021.

KÄVRESTAD, Joakim; NOHLBERG, Marcus. Evaluation strategies for cybersecurity training methods: a literature review. In: *Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021*. Anais [...]. Springer International Publishing, 2021. p. 102-112.

KASPERSKY. What is phishing and how to spot a phishing attempt. Disponível em: https://www.kaspersky.com/resource-center/threats/phishing. Acesso em: 06 out. 2024.

KHERUDDIN, Muhammad Syafiq; ZUBER, Muhammad Adam Emir Mohd; RADZAI, Muhammad Mukhlis Mohamad. Phishing attacks: unraveling tactics, threats, and defenses in the cybersecurity landscape. *Authorea Preprints*, 2024.

KHIDZIR, Nik Zulkarnaen; AHMED, Shekh Abdullah-Al-Musa. Viewpoint of probabilistic risk assessment in artificial enabled social engineering attacks. *Journal of Contemporary Issues and Thought*, v. 9, p. 12-17, 2019.

KNOWBE4a. 9 cognitive biases hackers exploit the most. Disponível em: https://info.knowbe4.com/wp-nine-cognitive-biases-hackers-exploit-most.

KNOWBE4b. What is spear phishing? Disponível em: https://www.knowbe4.com/spear-phishing.

KNOWBE4c. Security awareness training. Disponível em: https://www.knowbe4.com/security-awareness-training. Acesso em: 11 maio 2024.

KRAEMER, Sara; CARAYON, Pascale. Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. *Applied Ergonomics*, v. 38, n. 2, p. 143-154, 2007.

KROMBHOLZ, K.; HOBEL, H.; HUBER, M.; WEIPPL, E. Advanced social engineering attacks. *Journal of Information Security and Applications*, v. 22, p. 113-122, 2015.

KWEON, Eunkyung. The utility of information security training and education on cybersecurity incidents: an empirical evidence. *Information Systems Frontiers*, v. 23, p. 361-373, 2021.

LAIN, Daniele; KOSTIAINEN, Kari; ČAPKUN, Srdjan. Phishing in organizations: findings from a large-scale and long-term study. In: *2022 IEEE Symposium on Security and Privacy (SP)*. Anais [...]. IEEE, 2022. p. 842-859.

LASTDRAGER, Elmer E. H. Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, v. 3, n. 1, p. 1-10, 2014.

LEONOV, P. Y. The main social engineering techniques aimed at hacking information systems. In: *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*. IEEE, 2021. p. 471-473.

MAHAJAN, R.; SIDDAVATAM, I. Phishing website detection using machine learning algorithms. *International Journal of Computer Applications*, v. 181, n. 23, p. 45-47, 2018.

SAS, Marlies; RENIERS, Genserik; PONNET, Koen; HARDYNS, Wim. The impact of training sessions on physical security awareness: measuring employees' knowledge,

attitude and self-reported behaviour. *Safety Science*, v. 144, 2021. Disponível em: https://doi.org/10.1016/j.ssci.2021.105447.

MARSHALL, Martin N. Sampling for qualitative research. *Family Practice*, v. 13, n. 6, p. 522-526, 1996.

MAYER, Richard E. Incorporating motivation into multimedia learning. *Learning and Instruction*, v. 29, p. 171-173, 2014.

METCLOUD. Targeting your business is worth more to cartels than drug trade. Disponível em: https://www.metcloud.com. Acesso em: 27 jun. 2024.

MERRIAM, S. Qualitative research: a guide to design and implementation. San Francisco: John Wiley & Sons Inc., 2009.

MERRIAM, Sharan B.; TISDELL, Elizabeth J. *Qualitative research: a guide to design and implementation*. 4. ed. San Francisco: John Wiley & Sons, 2015.

MICROSOFT. Microsoft expande iniciativas de treinamento em cibersegurança no Brasil. Disponível em: https://news.microsoft.com/pt-br/microsoft-expande-iniciativas-de-treinamento-em-ciberseguranca-no-brasil/. Acesso em: 20 dez. 2024.

MITNICK, Kevin D.; SIMON, William L. *The art of deception: controlling the human element of security*. Hoboken: John Wiley & Sons, 2003.

MOSSANO, M.; VANIEA, K.; ALDAG, L.; DÜZGÜN, R.; MAYER, P.; VOLKAMER, M. Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector. In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2020. Disponível em: https://doi.org/10.1109/eurospw51379.2020.00026.

MOUTON, Francois; LEENEN, Louise; VENTER, Hein S. Social engineering attack examples, templates and scenarios. *Computers & Security*, v. 59, p. 186-209, 2016.

NAGYFEJEO, E.; SOLMS, B. v. Why do national cybersecurity awareness programmes often fail? *International Journal of Information Security and Cybercrime*, v. 9, n. 2, p. 18-27, 2020. Disponível em: https://doi.org/10.19107/ijisc.2020.02.03.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook. Gaithersburg, MD: NIST, 1995. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-12.pdf. Acesso em: 22 jun. 2024.

NORTONLIFELOCK. The cost of cybercrime. Disponível em: https://www.nortonlifelock.com/cybersecurity-insights/reports/threat-report.

RAVULA, P.; KUMAR CH, S.; GOPISETTY, S.; PEDHAMALLU, H.; MISHRA, V. K.; BADAL, T. VoIP spam detection using machine learning. In: *2022 6th International*

Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, 2022. p. 1251-1258. Disponível em: https://doi.org/10.1109/ICICCS53718.2022.9788233.

PARSONS, Kathryn. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, v. 42, p. 165-176, 2014.

PATTON, Michael Quinn. *Qualitative research & evaluation methods*. Thousand Oaks: Sage Publications, 2002.

PIRES, Érica de Souza. Análise do uso da plataforma KnowBe4 para conscientização da segurança da informação em uma instituição financeira: um estudo de caso. 2023. Trabalho de Conclusão de Curso (Graduação em Tecnologias da Informação e Comunicação) – Universidade Federal de Santa Catarina, Araranguá, 2023. Disponível em: https://repositorio.ufsc.br/handle/123456789/248975. Acesso em: 20 dez. 2024.

PROOFPOINT. State of the phish report reveals ransomware and phishing attack trends. Disponível em: https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-state-phish-report-reveals-ransomware-and-phishing-attack-trends.

PROOFPOINT. 2023 Human factor report: analyzing the cyber attack chain. Disponível em: https://www.proofpoint.com/us/resources/threat-reports/human-factor. Acesso em: 24 jun. 2024.

PROOFPOINT. 2024 State of the phish - today's cyber threats and phishing protection. Disponível em: https://www.proofpoint.com/us/resources/white-papers/state-of-phish. Acesso em: 23 jun. 2024.

JAMF. Punycode attacks: the fake domains that are impossible to detect. Disponível em: https://www.jamf.com/blog/punycode-attacks/.

RIZZONI, F.; MAGALINI, S.; CASAROLI, A.; MARI, P.; DIXON, M.; COVENTRY, L. Phishing simulation exercise in a large hospital: a case study. *Digital Health*, v. 8, 2022. Disponível em: https://doi.org/10.1177/20552076221081716.

ROWLEY, E.; BURNS, L.; BURNHAM, G. Research review of nongovernmental organizations' security policies for humanitarian programs in war, conflict, and postconflict environments. *Disaster Medicine and Public Health Preparedness*, v. 7, n. 3, p. 241-250, 2013. Disponível em: https://doi.org/10.1001/dmp.2010.0723.

ROY, S. S.; NARAGAM, K. V.; NILIZADEH, S. Generating phishing attacks using ChatGPT. *arXiv preprint*, 2023. Disponível em: https://arxiv.org/abs/2305.05133.

SALLOUM, S.; GABER, T.; VADERA, S.; SHAALAN, K. A systematic literature review on phishing email detection using natural language processing techniques. *IEEE Access*, v. 10, p. 65703-65727, 2022.

SAWAYA, Y.; SHARIF, M.; CHRISTIN, N.; KUBOTA, A. Self-confidence trumps knowledge: a cross-cultural study of security behavior. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2017. p. 2202-2214.

SHAHBAZNEZHAD, H.; KOLINI, F.; RASHIDIRAD, M. Employees' behavior in phishing attacks: what individual, organizational, and technological factors matter? *Journal of Computer Information Systems*, v. 61, n. 6, p. 539-550, 2020. Disponível em: https://doi.org/10.1080/08874417.2020.1812134.

SHANKAR, Akarshita; SHETTY, Ramesh; NATH, B. A review on phishing attacks. *International Journal of Applied Engineering Research*, v. 14, n. 9, p. 5, 2019.

SIDDIQI, Murtaza Ahmed; PAK, Wooguil; SIDDIQI, Moquddam A. A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, v. 12, n. 12, p. 6042, 2022.

SMITH, R.; DOE, J. Enhancing employee engagement through career-linked security training. *International Journal of Cybersecurity Education*, v. 8, n. 3, p. 203-217, 2019.

SLASHNEXT. The state of phishing 2022. Disponível em: https://slashnext.com/the-state-of-phishing-2022/.

SOSAFE AWARENESS. How often should phishing simulations be done? 2023. Disponível em: https://www.sosafe-awareness.com. Acesso em: 23 jun. 2024.

STEVES, M.; GREENE, K.; THEOFANOS, M. A phish scale: rating human phishing message detection difficulty. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2019. Disponível em: https://doi.org/10.14722/usec.2019.23028.

STRAUSS, Anselm; CORBIN, Juliet. *Basics of qualitative research techniques*. Thousand Oaks: Sage Publications, 1998.

Sumner, A., Yuan, X., Anwar, M., & McBride, M. (2022). Examining Factors Impacting the Effectiveness of Anti-Phishing Trainings. Journal of Computer Information Systems, 62(5), 975–997. https://doi.org/10.1080/08874417.2021.1955638

SUTTER, T. S.; BOZKIR, A. S.; GEHRING, B.; BERLICH, P. Avoiding the hook: influential factors of phishing awareness training on click-rates and a data-driven approach to predict email difficulty perception. *IEEE Access*, v. 10, p. 100540-100565, 2022. Disponível em: https://doi.org/10.1109/access.2022.3207272.

TAIB, Ronnie. Social engineering and organizational dependencies in phishing attacks. In: *IFIP Conference on Human-Computer Interaction*. Cham: Springer International Publishing, 2019. p. 564-584.

UNITED STATES DEPARTMENT OF JUSTICE. Phishing. Disponível em: https://www.justice.gov/criminal-ccips/ccips-cyber-crime-unit. Acesso em: 06 out. 2024.

THOMPSON, L.; MELENDEZ, N.; HEMPSON-JONES, J.; SALVI, F. Gamification in cybersecurity education: the RAD-SIM framework for effective learning. *European Conference on Games Based Learning*, v. 16, n. 1, p. 562-569, 2022. Disponível em: https://doi.org/10.34190/ecgbl.16.1.504.

TSCHAKERT, K.; NGAMSURIYAROJ, S. Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, v. 5, n. 6, e02010, 2019. Disponível em: https://doi.org/10.1016/j.heliyon.2019.e02010.

VERIZON. 2019 Data breach investigations report. Disponível em: https://enterprise.verizon.com/resources/reports/dbir/.

VILELA, Erica; UEDA, Eduardo Takeo; GAVA, Vagner Luiz. Phishing and social engineering: concept, modalities, techniques of detection and prevention of fraud. A systematic review of the literature. In: *19th CONTECSI-International Conference on Information Systems and Technology Management*. Anais [...]. São Paulo, 2022.

VISHWANATH, A.; HARRISON, B.; NG, Y. J. Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, v. 45, n. 8, p. 1146-1166, 2016. Disponível em: https://doi.org/10.1177/0093650215627483.

VOLKAMER, M.; RENAUD, K.; REINHEIMER, B.; RACK, P. D.; GHIGLIERI, M.; MAYER, P.; GERBER, N. Developing and evaluating a five-minute phishing awareness video. In: *Trust, Privacy, and Security in Digital Business*. Cham: Springer, 2018. p. 119-134. Disponível em: https://doi.org/10.1007/978-3-319-98385-1_9.

WORLD ECONOMIC FORUM. 2023 was a big year for cybercrime - here's how we can make our systems safer. Disponível em: https://www.weforum.org. Acesso em: 27 jun. 2024.

YEBOAH-BOATENG, E. O.; AMANOR, P. M. Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Cybersecurity*, v. 4, p. 1-9, 2014.

ZAHARON, N.; ALI, M.; HASNAN, S. Factors affecting awareness of phishing among Generation Y. *Asia-Pacific Management Accounting Journal*, v. 16, n. 2, p. 409-444, 2021. Disponível em: https://doi.org/10.24191/apmaj.v16i2-15.

ZAHRA, S. R.; CHISHTI, M. A.; BABA, A. I.; WU, F. Detecting COVID-19 chaos-driven phishing/malicious URL attacks by a fuzzy logic and data mining-based intelligence system. *Egyptian Informatics Journal*, v. 23, n. 2, p. 197-214, 2022.

ZHAO, Y. et al. Limitations of career-driven security training programs. *Global Journal of Information Security*, v. 10, n. 1, p. 50-63, 2018.

ZIELINSKA, O.; TEMBE, R.; HONG, K.; GE, X.; MURPHY-HILL, E.; MAYHORN, C. One phish, two phish, how to avoid the internet phish. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, v. 58, n. 1, p. 1466-1470, 2014. Disponível em: https://doi.org/10.1177/1541931214581306.

ZAXAPIÁΔH, X. Building societal resilience against phishing attacks. *Kypseli*, 2023.

8. APPENDIXES

A - RESEARCH PROTOCOL - SEMI-STRUCTURED INTERVIEW

INTRODUCTION

This form aims to inform respondents about the use of data for academic purposes of the Master's in Computer Science by student Diego Augusto de Araujo Madeira at the UFPE's Informatics Center.

RESEARCH PROTOCOL - SEMI-STRUCTURED INTERVIEW

INVESTIGATING FACTORS AND GOOD PRACTICES TO IMPROVE THE EFFECTIVENESS OF PHISHING AWARENESS

RESEARCH OBJECTIVE

The primary objective of this research is to evaluate the effectiveness of information security awareness programs, with a particular focus on the prevention of phishing attacks. This study aims to understand the efficacy of the approaches adopted, known as Security Awareness Training (SAT), and to identify factors that contribute to the success or failure of these programs.

Specifically, the research seeks to achieve the following objectives:

1. **Analyze the Approaches Used in Awareness Programs**: assess user perceptions of different approaches and techniques employed in information security awareness programs. This involves identifying the most effective approaches, whether imposing or not, and the timing of content delivery—prior to or following a simulated phishing attack, either before falling for a simulated phishing attack or after experiencing it.
2. **Evaluate the Effectiveness of Awareness Programs**: investigate the impact of awareness programs on users' perceptions regarding the detection of phishing attacks and their behavior in adopting recommended security practices within the organization.
3. **Identify Critical Success Factors**: explore the factors that contribute to the effectiveness of awareness programs. This includes analyzing aspects such as the frequency and approach used in training, the relevance of the training material presented, and how security recommendations are perceived by different user groups.
4. **Propose Recommendations for Improving Awareness Programs**: based on the research findings, provide recommendations to enhance the approaches and timing of training content delivery. Suggestions may focus on increasing the effectiveness of the programs, tailoring training approaches for specific user groups to strengthen awareness and prevention of phishing attacks.

Through this study, it is expected to contribute to the field of information security by providing valuable insights into how awareness programs can be structured and implemented more effectively, aiming to better protect individuals and organizations against phishing attacks.

PROBLEM STATEMENT

Phishing has emerged as one of the primary vectors of cyberattacks, exacerbated by its increasing use by cybercriminals. In 2023, the Anti-Phishing Working Group (APWG) recorded nearly 5 million phishing attacks, marking a 6.3% increase compared to the previous year. This figure represents the highest number ever recorded. These attacks were responsible for over 91% of data breaches, underscoring the urgency of effective approaches to mitigate these threats. The most critical aspect of protecting any system lies in human vulnerability, often exploited through social engineering and cognitive biases.

The significance of this study stems from the need to understand and improve information security awareness strategies, specifically regarding phishing prevention. With the growing prevalence of phishing attacks and their devastating consequences, it is imperative to develop effective methods to educate and protect users against such threats. Given the direct influence of security awareness on the effectiveness of protective measures, this study aims to provide valuable insights for strengthening security policies within organizations.

Despite the recognized importance of information security awareness programs, there is a significant gap in understanding how these programs are structured and their effectiveness in preventing phishing attacks. Currently, little is known about the specific characteristics of these programs, their implementation strategies, and methods for evaluating their effectiveness. This study aims to fill this gap by providing a detailed analysis of current practices and suggesting improvements.

The objective of this study is to evaluate information security awareness programs, with a focus on preventing phishing attacks. Through semi-structured interviews with individuals across various age groups, the study seeks to analyze the effectiveness of approaches and timing of content delivery used in these programs from the perspective of phishing attack prevention.

RESEARCH QUESTIONS

- What are the main factors that contribute to the effectiveness of phishing prevention strategies in security awareness training programs?
- What are the good practices to enhance the effectiveness of phishing prevention strategies in security awareness training programs?

METHODOLOGY

RESEARCH TYPE

This research adopts a qualitative approach, utilizing semi-structured interviews to collect data on participants' perceptions and experiences related to information security awareness programs, with the aim of evaluating the factors that influence the effectiveness of these programs in preventing phishing attacks.

DATA COLLECTION METHOD

The proposed research aims to evaluate the approaches and timing of information security awareness programs with a focus on phishing attack prevention, analyzing individuals' perceptions of the approaches and delivery methods used by these programs. To achieve this objective, a semi-

structured interview protocol was chosen, justified by its potential to provide a contextualized view of participants' experiences and perceptions regarding information security awareness strategies (MERRIAM, 2009).

The data collection method will involve conducting individual semi-structured interviews with individuals who have direct experience with information security awareness programs. This method allows for the adaptation of questions based on participants' responses and enables in-depth investigation of participants' experiences while maintaining the flexibility to explore emerging topics during the interview. Content analysis will be employed to extract detailed information from the collected data (MERRIAM, 2009).

TARGET POPULATION

The study focuses on employees and C-Levels who are directly involved in information security awareness programs. The target population includes individuals aged 18 and over, from both the capital and interior regions, covering a diverse range of profiles, such as varying levels of experience, areas of expertise, and organizational contexts.

PARTICIPANT SELECTION AND DATA COLLECTION PROCEDURES

Participants will be selected using a purposive sampling approach to ensure a representative variety of profiles. The selection criteria will include individuals who have actively participated in information security awareness programs.

- **Preparation for Interviews:** develop a semi-structured interview guide that addresses the central themes of the study and allows for in-depth exploration based on participants' responses.
- **Conducting the Interviews**: interviews will be conducted individually in a controlled and confidential environment, either in person or via online communication platforms, according to the participants' availability and preference.
- **Recording and Transcription**: with the participants' consent, the interviews will be recorded and subsequently transcribed for analysis.

ETHICAL CONSIDERATIONS

The data collected through the interviews will be analyzed using thematic analysis. This process will involve a thorough reading of the transcripts to identify patterns, themes, and relevant categories. The analysis will focus on extracting relevant information about awareness strategies, their effectiveness, and the factors influencing their success or failure.

VALIDITY AND RELIABILITY

The research will adhere to ethical standards, ensuring the confidentiality and anonymity of participants. Informed consent will be obtained from all participants, clarifying the purpose of the research, how the data will be used, and the guarantee of privacy.

To ensure validity and reliability, thematic analysis will be conducted on the data collected through semi-structured interviews, ensuring that the emerging themes are directly derived from the data, reflecting participants' perspectives. Reliability will be assured through a systematic analysis process, where the data will be reviewed to ensure consistency and accuracy in theme identification. The integration of critical reflection on the researcher's biases and assumptions will strengthen

objectivity, contributing to the robustness of the findings and the foundation of conclusions regarding the effectiveness of phishing awareness programs.

LIMITATIONS

The interpretation of semi-structured interviews can be subjective, and there is a potential for researcher bias in data selection and analysis. The results may not be applicable to all contexts, limiting the generalizability of the findings. The potential lack of face-to-face interaction might affect the learning dynamics and engagement in fully online awareness programs.

Additionally, the online collaborative approach may not fully capture the nuances of non-verbal communication, which are essential for building shared understanding. The selection and motivation of participants for online engagement might introduce bias, limiting the generalization of results to a broader population.

To mitigate these limitations, the training programs will be designed to be brief and low-interaction, prioritizing multimedia content such as videos over lengthy texts. To reinforce motivation, a group of users will be informed after failing for phishing simulations, highlighting the importance of knowledge on the topic.

B - SEMI-STRUCTURED INTERVIEW GUIDE

- **Research Theme**: investigating factors and good practices to improve the effectiveness of phishing awareness.
- **Objective:** to evaluate information security awareness training programs, with a particular focus on preventing phishing attacks, and to assess the effectiveness of the adopted approaches, identifying factors that contribute to the success or failure of the programs.
- **Profile of Interviewees**: employees and C-levels of a specific public organization in Pernambuco who are directly involved in information security awareness training programs. The target population includes individuals aged 18 and over, from both the capital and interior regions, with varying levels of experience and areas of expertise.
- **Estimated Duration**: 30 minutes

Introduction

- Introduction of the interviewer.
- Explanation of the research and its importance.
- Reiteration of confidentiality and obtaining informed consent.

Section 1: Interviewee Qualifications

1. Years of Service
2. Position
3. Do you hold a leadership role or position?
4. Education
5. Age
6. Gender

Section 2: Context and Personal Experience

7. Have you ever been a victim of phishing?
8. How would you rate your level of knowledge about phishing?
9. How do you identify a phishing attempt?
10. What do you do when you identify a phishing attempt?
11. How often do you encounter suspicious messages?

Section 3: Perception of Program Content and Format

12. How did you learn about the organization's information security awareness training?
13. What was your motivation to participate in the training?
14. Do you think participation should be mandatory for everyone?
15. What did you think of the content presented in the training?
16. Do you prefer remote or in-person training?
17. **For better training, which format do you prefer:**
    a. Video
    b. Gamified
    c. Explanatory text

Section 4: Experiences with Activities and Simulations

18. Have you recently identified any suspicious emails in the organization?
19. For users who identified the phishing:
    a. Did you click on the email link?
20. **For users who fell for the simulated phishing**
    a. What was your reaction when you were notified that you fell for a simulated phishing attempt?

b. After being notified about clicking on a simulated phishing attempt, did you feel more prepared to identify phishing attempts?
c. Did you suspect the email might be phishing before clicking?
d. What factors influenced you to click the link or open the file?
e. Do you think you might have taken a risk by clicking the link or opening the file provided in the email?

21. **For users who identified the simulated phishing**
a. When you identified a phishing attempt, what characteristics caught your attention?
b. After identifying a phishing attempt, what actions did you take immediately?
c. Did you share your experience of identifying the phishing attempt with colleagues or information security personnel in your organization? If so, how was that conversation?
d. Do you believe that the information and training you received previously adequately prepared you to identify and respond to the phishing attack? Please justify your answer.

Section 5: Feedback on the Programs

22. For users who completed the training:
a. How would you rate your level of knowledge about phishing before and after the training?
23. For users who did not complete the training:
a. Why did you not participate in the training?

Section 6: Overall Impact and Recommendations

24. Could you provide suggestions for improving phishing awareness programs?
25. How do you evaluate the organization's communication regarding the provided training?

Conclusion

Thank you for your participation.

Opportunity for final comments or additional clarifications.

C - INFORMED CONSENT FORM

Introduction

This form aims to inform respondents about the use of data in a safe and private way, for academic purposes of the master's in computer science by student Diego Augusto de Araujo Madeira at the UFPE's Informatics Center.

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

Pesquisa: INVESTIGATING FACTORS AND GOOD PRACTICES TO IMPROVE THE EFFECTIVENESS OF PHISHING AWARENESS

Pesquisador: Diego Augusto de Araujo Madeira

Instituição: UFPE

Contato do Pesquisador: 81997552530 / daam@cin.ufpe.br

Prezado(a) Participante,

Você está sendo convidado(a) a participar da pesquisa intitulada "*Investigando Fatores e Boas Práticas para Melhorar a Eficácia da Conscientização sobre Phishing*," conduzida por Diego Augusto de Araújo Madeira, sob orientação da Professora Dra. Carina Frota Alves. Antes de decidir participar, é importante que você entenda os objetivos, procedimentos e riscos associados a este estudo.

1. Objetivo da Pesquisa

O objetivo desta pesquisa é investigar as estratégias utilizadas em programas de conscientização em segurança da informação, com foco na prevenção de ataques de phishing, e avaliar a efetividade desses programas.

2. Procedimentos da Pesquisa

Como participante, você será convidado(a) a responder a uma série de perguntas durante uma entrevista semiestruturada. Esta entrevista deverá durar aproximadamente 30 minutos e será conduzida pelo pesquisador em um local de sua escolha ou por meio de uma plataforma online.

3. Confidencialidade

Todas as informações que você fornecer serão mantidas confidenciais. Seus dados serão anonimizados, e apenas os pesquisadores terão acesso às informações coletadas. Os resultados da pesquisa poderão ser publicados em artigos ou apresentados em conferências, mas sua identidade será sempre preservada.

4. Riscos e Benefícios

Não há riscos físicos ou emocionais previstos na participação deste estudo. O benefício esperado é contribuir para o aprimoramento de estratégias de conscientização em segurança da informação, beneficiando a comunidade como um todo.

5. Voluntariedade e Retirada do Consentimento

Sua participação é totalmente voluntária. Você tem o direito de retirar seu consentimento e desistir da pesquisa a qualquer momento, sem penalidades ou perda de benefícios aos quais você possa ter direito.

6. Contato para Perguntas ou Preocupações

Se você tiver quaisquer dúvidas ou preocupações relacionadas a esta pesquisa, pode entrar em contato com o pesquisador responsável através do e-mail daam@cin.ufpe.br.

Ao assinar este termo, você concorda voluntariamente em participar desta pesquisa, tendo compreendido as informações acima.

Assinatura do participante: _____ Data:_____

Assinatura do pesquisador: _____ Data:_____