Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Engineering

Bachelor Thesis

Cyber Security: Effect of Social Engineering in Cyber Attacks – Risks, Vulnerabilities and Countermeasures

Cagdas Baran Bilim

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Cagdas Baran Bilim

Informatics

Thesis title

Cyber Security: Effect of Social Engineering in Cyber Attacks – Risks, Vulnerabilities and Countermeasures

---

Objectives of thesis

The bachelor thesis deals with cyber security attacks furthermore focuses on various forms of Social Engineering techniques and tactics and how social engineers exploit human vulnerabilities, various methods to counteract such cyber attacks, and emphasizing the importance of being conscious to prevent such attacks. The partial goals of the bachelor thesis are:

- to identify the effect of social engineering on cyber attacks,
- to develop critical literature review for damage caused by social engineering attacks,
- to distinguish methods and approaches which are commonly used in social engineering attacks,
- to evaluate the role of human factors and psychological variables on cybercrimes,
- to determine methods of prevention of social engineering attacks.

Methodology

The methodology of the bachelor's thesis will be based on the study and analysis of professional information sources. In the first section of the thesis; cyber security, its terminology and approaches used in cyberattacks will be provided. Secondly, the human vulnerability factor and psychological aspect of cyber attacks will be evaluated. Later, social engineering attacks in relation with human factors will be analyzed in detail. Socio-Technical Attack Examples will be given as a real-life simulation. In addition to this, statistical informations and previous surveys will be provided for recommendations and implementation proposals to increase IT security.

Based on the combination of theoretical knowledge and the results of the analysis, the bachelor thesis will be concluded.

The proposed extent of the thesis

30 – 40 pages

Keywords

cybersecurity, social engineering, risks, cyberattacks, cybercrimes, threats

---

Recommended information sources

Andreea Bendovschi, Cyber-Attacks – Trends, Patterns and Security Countermeasures, Procedia Economics and Finance, Volume 28, 2015, Pages 24-31, ISSN 2212-5671, https://doi.org/10.1016/S2212-5671(15)01077-1.

Bakhshi, T., Papadaki, M. and Furnell, S. (2009), "Social engineering: assessing vulnerabilities in practice", Information Management & Computer Security, Vol. 17 No. 1, pp. 53-63. https://doi.org/10.1108/09685220910944768

David Tayouri, The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages, Procedia Manufacturing, Volume 3, 2015, Pages 1096-1100, ISSN 2351-9789, https://doi.org/10.1016/j.promfg.2015.07.181.

Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl, Advanced social engineering attacks, Journal of Information Security and Applications, Volume 22, 2015, Pages 113-122, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2014.09.005.

Salahdine, Fatima, and Naima Kaabouch. 2019. "Social Engineering Attacks: A Survey" Future Internet 11, no. 4: 89. https://doi.org/10.3390/fi11040089

Expected date of thesis defence

2021/22 SS – FEM

The Bachelor Thesis Supervisor

doc. Ing. Jan Tyrychtr, Ph.D.

Supervising department

Department of Information Engineering

Electronic approval: 1. 11. 2021

Ing. Martin Pelikán, Ph.D.

Head of department

Electronic approval: 23. 11. 2021

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 14. 03. 2023

Declaration

I declare that I have worked on my bachelor thesis titled "Cyber Security: Effect of Social Engineering in Cyber Attacks – Risks, Vulnerabilities and Countermeasures" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break any copyrights.

In Prague on 15.03.2023 _____

Acknowledgement

Hereby I would like to thank all those who supported me in preparing my bachelor's thesis. I would especially like to thank my supervisor doc. Ing. Jan Tyrychtr, Ph.D and statistics tutor Ing. Zuzana Pacáková, Ph.D. for their professional guidance, assistance, and valuable comments throughout this work. Last but not least, I would like to thank to my family and friends for their material and spiritual support during my bachelor studies.

Cyber Security: Effect of Social Engineering in Cyber Attacks – Risks, Vulnerabilities and Countermeasures

Abstract

Social engineering attacks are increasingly used by cybercriminals to deceive individuals and organizations into disclosing sensitive information. As the use of social engineering attacks continues to rise, it is crucial to understand the different social engineering tactics and the impact of human factors on these attacks. This study aims to explore the level of social engineering awareness and knowledge among a sample of 100 participants, consisting of 57 males and 43 females, in order to identify any differences in awareness and knowledge between male and female participants. A 30-item questionnaire was developed to assess the participants' knowledge of social engineering, and the data collected were analysed using the Pearson Chi-Square Test. The findings suggest that there is no significant difference in the level of awareness of social engineering concepts and potential risks associated with social engineering attacks between males and females. However, there is a significant difference in the level of education and training on how to identify and protect against social engineering attacks between males and females, with females being less likely to have received training or education on this topic. The study highlights the need for organizations to provide gender-inclusive training on preventing social engineering attacks to increase awareness and reduce the risk of successful attacks.

In conclusion, this study highlights the importance of understanding social engineering tactics, and the impact of human factors on these attacks. By identifying gender differences in social engineering awareness and knowledge, educators and policymakers can tailor cybersecurity education programs to address these differences. Moreover, this study provides guidance on countermeasures that organizations can implement to mitigate social engineering attacks. Overall, this research contributes to the understanding of social engineering attacks and the measures that can be taken to protect against them.

Keywords: Cybersecurity, social engineering, risks, cyberattacks, cybercrimes, threats.

Kybernetická bezpečnost: Vliv sociálního inženýrství na kybernetické útoky - rizika, zranitelnosti a protiopatření

Abstrakt

Útoky sociálního inženýrství jsou stále častěji využívány kyberzločinci k oklamání jednotlivců a organizací, aby prozradili citlivé informace. Vzhledem k tomu, že využívání útoků sociálního inženýrství stále roste, je nezbytné porozumět různým taktikám sociálního inženýrství a vlivu lidského faktoru na tyto útoky. Cílem této studie je prozkoumat úroveň povědomí a znalostí o sociálním inženýrství u vzorku 100 účastníků, který tvoří 57 mužů a 43 žen, s cílem zjistit případné rozdíly v povědomí a znalostech mezi účastníky a účastnicemi. K posouzení znalostí účastníků o sociálním inženýrství byl vytvořen 30položkový dotazník a shromážděná data byla analyzována pomocí Pearsonova chí-kvadrát testu. Zjištění naznačují, že mezi muži a ženami není významný rozdíl v úrovni povědomí o pojmech sociálního inženýrství a potenciálních rizicích spojených s útoky sociálního inženýrství. Existuje však významný rozdíl v úrovni vzdělání a školení o tom, jak identifikovat útoky sociálního inženýrství a chránit se před nimi, mezi muži a ženami, přičemž u žen je méně pravděpodobné, že absolvovaly školení nebo vzdělávání na toto téma. Studie zdůrazňuje, že je třeba, aby organizace poskytovaly školení o prevenci útoků sociálního inženýrství zohledňující pohlaví, aby se zvýšila informovanost a snížilo riziko úspěšných útoků.

Závěrem tato studie zdůrazňuje důležitost pochopení taktik sociálního inženýrství a vlivu lidského faktoru na tyto útoky. Díky identifikaci genderových rozdílů v povědomí a znalostech o sociálním inženýrství mohou pedagogové a tvůrci politik přizpůsobit vzdělávací programy v oblasti kybernetické bezpečnosti tak, aby tyto rozdíly zohledňovaly. Kromě toho tato studie poskytuje návod na protiopatření, která mohou organizace zavést ke zmírnění útoků sociálního inženýrství. Celkově tento výzkum přispívá k pochopení útoků sociálního inženýrství a opatření, která lze přijmout na ochranu před nimi.

Klíčová slova: kybernetická bezpečnost, sociální inženýrství, rizika, kybernetické útoky, kybernetická kriminalita, hrozby.

Table of Contents

List of Abbreviations

API	Application Programming Interface
CLD	Causal Loop Diagram
IBM	International Business Machines Corporation
IRL	The Internal Revenue Service
ISACA	The Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	The International Organization for Standardization
IT	Information Technology
NLP	Neuro-linguistic programming
PC	Personal Computer
RAT	The FBI Internet Crime Complaint Center's Recovery Asset Team
U.S.	The United States of America
VoIP	Voice Over IP
VPN	Virtual Private Network

1 Introduction

This thesis aims to provide an in-depth analysis of the different aspects of social engineering attacks. Specifically, it will explore how, where, when, and why these attacks occur, as well as the methods used by social engineers to select their victims, gather information, and launch the attack. The structure of social engineering attacks will also be dissected and examined, with the goal of developing effective countermeasures against such attacks. Although, according to Kevin Mitnick, a renowned cybersecurity professional, "You can never protect yourself 100%. What you do is protect yourself as much as you can and reduce the risk to an acceptable level. You can never eliminate all risk" [1].

The thesis is structured as follows: Chapter 2 presents the objectives and methodology of the research. The objectives of the study are outlined in Section 2.1, followed by a description of the methodology used in Section 2.2.

Chapter 3 discusses the current state of the art in cyber security and social engineering. Section 3.1 provides an overview of cyber security, while Section 3.2 delves into the concept of social engineering. Section 3.3 examines the attributes of a social engineer, and Section 3.4 explores the cycle of social engineering attacks, including information gathering, developing relationships, exploitation, and execution. Section 3.5 discusses various social engineering approaches, including physical, social, reverse, technical, and socio-technical approaches. Section 3.6 highlights the methods of social engineering attacks, such as the impact of human factors and psychological manipulation techniques like lying, partial truth, providing a reason, avoidance and diversion, interrelation, and humor. In Section 3.7, different types of social engineering attacks are examined, such as pretexting, reverse social engineering, piggybacking, whaling, dumpster diving, social media network attacks, neuro-linguistic programming, honey trapping, shoulder surfing, quid pro quo, watering hole, and scareware. Section 3.8 focuses on advanced social engineering attacks, including phishing, voice phishing, spear phishing, and baiting.

Chapter 4 examines countermeasures for social engineering attacks. Section 4.1 provides an overview of defense mechanisms, such as cyber security and social engineering awareness and training, creating an effective security policy, physical security, digital security, and

password security policy. In Section 4.2, fundamental corporate security measures to be taken against social engineering attacks are discussed, such as spreading information security awareness in organizations, implementing fundamental corporate security measures.

Chapter 5 of this thesis focuses on the practical part of the study. Section 5.1 provides an introduction to the practical part and outlines the purpose and scope of the study. Section 5.2 details the design and implementation of the survey, including information on the target population, sample size, survey instrument, data collection procedure, and data analysis techniques used in the study. Section 5.3 presents the survey evaluation and includes 4 subsections: demographic analysis, social engineering exposure analysis, social engineering knowledge analysis, and attitudes towards social engineering analysis. The demographic analysis examines the characteristics of the survey respondents, while the social engineering exposure analysis investigates their experience with social engineering attacks. The social engineering knowledge analysis assesses respondents' awareness of social engineering concepts, and the attitudes towards social engineering analysis explores their perceptions and attitudes towards social engineering attacks. Section 5.4 presents the statistical analysis of the hypothesis of the study. The study investigated three hypotheses related to social engineering attacks, and the Chi-Square Test was used to test each hypothesis. The first hypothesis examined the differences in awareness of social engineering concepts between males and females. The second hypothesis investigated the differences in awareness of potential risks associated with social engineering attacks between males and females. The third hypothesis analyzed the differences in the level of education and training on how to identify and protect against social engineering attacks between males and females. The results of the analysis are presented and discussed in this section.

Finally, Chapter 6 provides the conclusion of the study. This section summarizes the main findings of the research and their implications for social engineering attacks. The chapter also discusses the contributions of the study and provides recommendations for future research.

2 Objectives and Methodology

2.1 Objectives

The bachelor thesis deals with cyber security attacks furthermore focuses on various forms of Social Engineering techniques and tactics and how social engineers exploit human vulnerabilities, various methods to counteract such cyber-attacks, and emphasizing the importance of being conscious to prevent such attacks. The partial goals of the bachelor thesis are:

- to identify the effect of social engineering on cyber-attacks,
- to develop critical literature review for damage caused by social engineering attacks,
- to distinguish methods and approaches which are commonly used in social engineering attacks,
- to evaluate the role of human factors and psychological variables on cybercrimes,
- to determine methods of prevention of social engineering attacks.

2.2 Methodology

This study employed a quantitative research design to investigate social engineering awareness among participants. The study involved administering a questionnaire to a sample of participants, which was used to collect data for the study.

2.2.1 Participants

Participants were recruited through convenience sampling from various online channels, such as social media groups and university groups. The sample included 100 participants, with 57 male and 43 female participants. Participants were required to be at least 18 years old.

2.2.2 Instrumentation

The instrument used for this study was a self-administered questionnaire that consisted of 30 items. The questionnaire was developed based on previous literature on social engineering and covered various aspects of social engineering, including knowledge of social engineering tactics, exposure to social engineering attacks, and attitudes towards

social engineering. The questionnaire also included four demographic questions, which were used to gather information about participants' age, gender, educational level, and occupation.

2.2.3 Data Collection

Data collection for this study was conducted solely through an online survey via Google Forms. Before starting the survey, participants were asked to provide informed consent. The online survey was designed to be self-administered, allowing participants to complete the questionnaire at their own pace and convenience. No identifying information was collected from the participants, ensuring the anonymity of their responses.

2.2.4 Data Analysis

The data collected in this study were analysed using descriptive statistics and Pearson Chi-Square tests. Descriptive statistics were used to summarize the data collected on each variable, including the mean, standard deviation, and range. Pearson Chi-Square tests were used to determine whether there were significant differences in social engineering awareness between male and female participants. The statistical analyses were conducted using the IBM SPSS Statistics software version 28.

2.2.5 Hypothesis

The hypothesis of this study involved collecting data through a survey instrument to assess the level of awareness and education on social engineering attacks between males and females. The data collected and analysed in this study indicated that there was no significant difference in the level of awareness of social engineering concepts and potential risks associated with social engineering attacks between males and females. This suggests that both genders have a similar understanding of the risks associated with social engineering attacks. However, the study did find a significant difference in the level of education and training on how to identify and protect against social engineering attacks between males and females. Males were found to be more educated and trained on this topic than females.

2.2.6 Ethical Considerations

This study was conducted in accordance with ethical guidelines for research involving human subjects. Participants were provided with informed consent forms that described the

purpose of the study, the voluntary nature of participation, and their rights as research subjects. Participants were also assured of the confidentiality of their responses and were given the option to withdraw from the study at any time. All data collected for this study were kept confidential and were only accessible to the researcher.

Overall, the methodology employed in this study allowed for the collection of quantitative data on social engineering awareness among participants. The use of a self-administered questionnaire and convenience sampling limited the generalizability of the results, but the findings of this study can provide insights into the development of cybersecurity education programs that target both male and female students equally.

3 Literature Review

3.1 Introduction to the literature review

The field of information security is a rapidly expanding discipline, wherein the efficacy of security measures in safeguarding sensitive information is on the rise. However, the human element continues to pose the weakest link in the security chain due to their susceptibility to manipulation [2]. Protecting information is crucial for organizations and governments, and therefore, the development of measures to prevent unauthorized access to information is an area that demands greater attention. It is imperative to note that technology alone cannot provide adequate protection against information theft, as employees often constitute the weakest link in an information security system [3]. Employees may inadvertently disclose confidential information, allowing unauthorized persons to gain access to protected systems [4]. Kevin Mitnick, regarded as one of the most prolific social engineers in history, argues that despite organizations spending millions of dollars on firewalls and secure access devices, these measures fail to address the weakest link in the security chain- the individuals who operate, administer and use computer systems [3].

Social engineering is a discipline within cybersecurity that involves manipulating individuals to divulge sensitive information. With the increase in internet activity and the number of active users around the world, people have easy access to vast amounts of data and connect with others virtually [4]. Every piece of information shared, whether it is a social media post or an email with confidential business information, carries risks that can be underestimated by an inexperienced user [5]. Unfortunately, inexperienced users are also the perfect targets for social engineering attacks, where an attacker studies an individual's behavior to obtain useful information and gain access to computer systems [3]. The social engineer preys on the weakest link in the system - the human - and uses various tactics to bypass hardware and software defenses [6].

Humans are susceptible to social engineering attacks due to their emotions and moods, such as fear, guilt, compassion, interest, love, and sadness [7]. These emotional states can alter their perception of reality, rendering them vulnerable to exploitation by attackers. In order

to take advantage of the victim, social engineers use psychological techniques to cross the thin red line that separates them from the victim [7]. Anyone can install a good antivirus program and a very good firewall, but if the engineer can gain the necessary trust, they will have no problem in overriding the victim's defenses.

Similarly, social engineers sell themselves to their interlocutors to acquire the information they are interested in and then disappear without a trace. This is done by exploiting human behavior, including elements of persuasion, deception, and manipulation. In doing so, social engineers exploit human trust, kindness, and a lack of knowledge to achieve their objectives [8]. Therefore, it is crucially important for individuals to be aware of various forms of techniques used in order to take measures to protect themselves from social engineering attacks. This can include being skeptical of unexpected requests for information, being cautious of unsolicited emails, and avoiding divulging personal information to unknown individuals or sources [6].

Social engineering attacks refer to a series of techniques used by social engineers to trick individuals into divulging personal information or engaging in activities that can make their computer systems vulnerable to attack [9]. Unlike other cyber-attacks, social engineering attacks do not result in immediate and obvious damage, such as system breaches or damage to critical resources [6]. These attacks are insidious, premeditated, and involve an in-depth study of the target victim, often taking hours, days, and even months [6]. The classic example is the Trojan horse, which in the IT world is software that is disguised as trustworthy software, but which runs completely different code inside [9]. Social engineering attacks can take various forms, including pretexting, phishing, baiting, and piggybacking, each exploiting human vulnerabilities in different ways [6]. It is crucial to emphasize that social engineering attacks are constantly evolving, and organizations must remain vigilant in their efforts to protect their systems and sensitive information.

The primary motivation for social engineering attacks is typically financial gain, followed by the acquisition of personal and competitor information [5]. In some cases, social engineering attacks may be motivated by a desire for revenge, such as in the case of disgruntled former employees [10]. The objective of social engineers is to establish a

relationship of trust with the victim as quickly as possible in order to facilitate the process of extracting the information they need [8].

Recent research suggests that social engineering is the leading cause of network compromise. A security state research report published by The Information Systems Audit and Control Association (ISACA) in 2022 identifies social engineering as the primary threat facing organizations today [8]. Furthermore, the 2022 Cost of a Data Breach report by the International Business Machines Corporation (IBM) reveals that social engineering attacks are one of the most financially damaging among cyber-attacks, with companies losing a staggering 4.10 million USD due to such attacks [11]. These findings underscore the critical importance for organizations to prioritize measures that prevent and mitigate social engineering attacks.

Phishing is a prevalent and well-known form of social engineering that involves extracting sensitive information from a targeted user's social network. As depicted in Figure 1, phishing accounts for 35.3% of social engineering attacks [11]. According to the FBI Internet Crime Complaint Center's Recovery Asset Team (RAT), there has been a significant increase in phishing attacks by 1,178% between 2017 and 2021, as reported by all cybercrime metrics [12]. In 2021 alone, social engineering attacks resulted in a total of $6.9 billion in losses to cybercriminals out of 466,502 reports of individual and corporate cybercrime events to the FBI in the US [12]. Figure 1 presents a breakdown of the various social engineering techniques that were used in cyber-attacks during the COVID-19 pandemic, along with the percentage of attacks that utilized each technique.

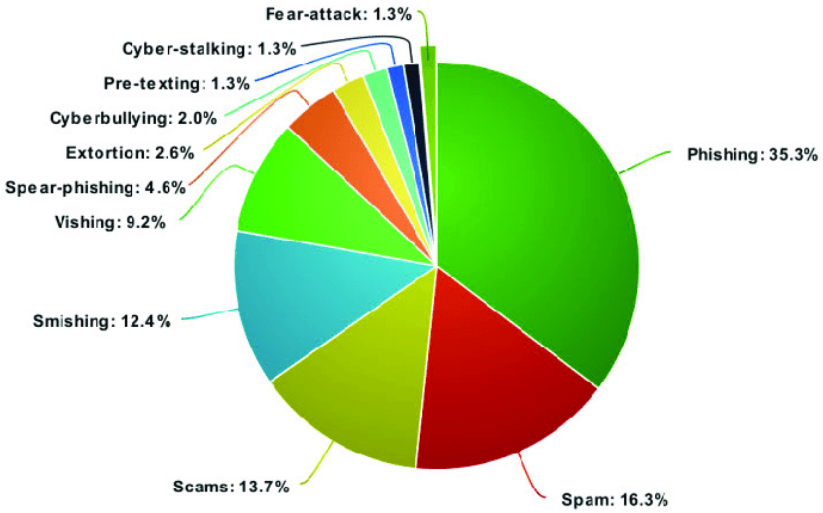


Figure 1: Different social engineering techniques used for cyber-attacks/threats during the COVID-19 pandemic shown in percentages of the attacks/threats [13].

Figure 1 presents the different social engineering techniques used for cyber-attacks and threats during the COVID-19 pandemic, with each technique's percentage of attacks/threats displayed. According to the data presented, phishing was the most commonly used technique, accounting for 35.3% of the attacks/threats [13]. Following phishing, spam was the second most common technique, accounting for 16.3% of attacks/threats, followed by scams at 13.7%, and smishing at 12.4% [13]. Vishing, spear-phishing, extortion techniques accounted for 9.2%, 4.6%, 2.6% attacks/threats, respectively [13].

The high percentage of phishing attacks is consistent with previous research on social engineering techniques [9]. It is vital to be aware of these different techniques and their prevalence during the pandemic, as cyber criminals continue to target individuals and organizations. As such, it is essential to remain vigilant and take proactive measures to protect oneself and one's organization against these social engineering techniques.

Addressing the high prevalence of social engineering attacks, effective research, understanding, development and maintenance of robust defense mechanisms are imperative. The use of the best firewalls, intrusion detection systems, and information security experts are necessary but not sufficient. In fact, educating employees and keeping them informed of security risks can have a significant impact on mitigating attacks. However, few companies provide security training to employees, and even fewer empower them to prevent or intervene in potential security incidents. Fortunately, new technologies can be leveraged to

alert and educate employees about access policies and minimize the frequency, risk and cost of social engineering attacks. The yearly IBM report for 2022 in Figure 2 illustrates the cost and frequency of data breaches.

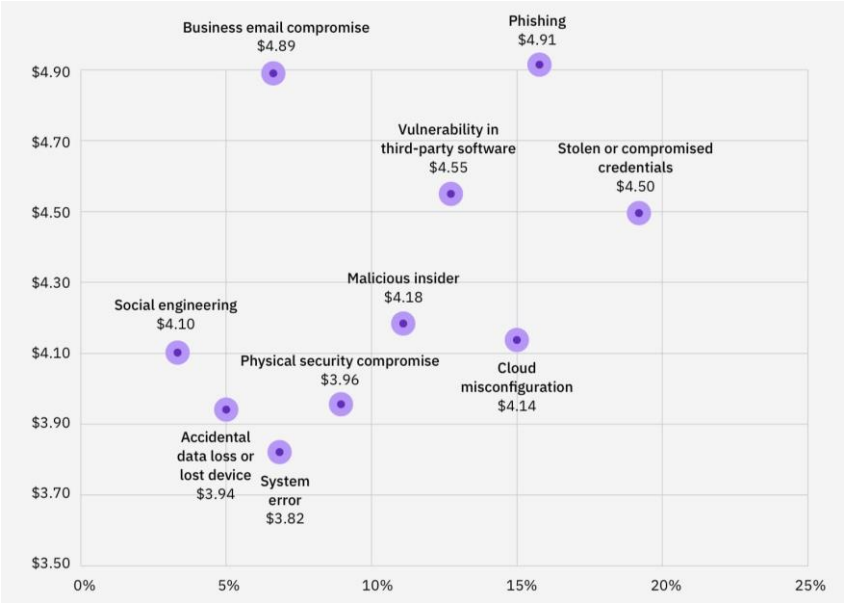


Figure 2: Average cost and frequency of data breaches by initial attack vector (Measured in USD millions) [11].

Figure 2 provides valuable insight into the financial impact of different initial attack vectors on organizations that suffer a data breach. The IBM Cost of a Data breach Report 2022 is based on an analysis of data breaches that occurred in various countries and industries, including healthcare, finance, and retail.

According to the figure, the most frequently observed initial attack vectors were compromised credentials, which accounted for 19% of the total breaches, followed by phishing at 16%, cloud misconfiguration at 15%, and vulnerabilities in third-party software at 13% [11]. It is noteworthy that the order of these four attack vectors remained the same as the previous year's report [11]. Among these attack vectors, phishing was found to be the costliest initial attack vector in 2022, with an average cost of USD 4.91 million, followed by business email compromise at USD 4.89 million and 6% of breaches, vulnerabilities in third-party software at USD 4.55 million, and compromised credentials at USD 4.50 million [11].

The data presented in the figure highlights the importance of implementing strong security measures, such as multi-factor authentication and regular access reviews, to prevent attacks that involve privileged credentials and cloud misconfigurations. It also emphasizes the need for organizations to educate their employees on how to recognize and avoid phishing attacks, which are the most common type of initial attack vector.

Cybersecurity and social engineering are closely related as both pertain to the manipulation of individuals in order to achieve a certain objective [6]. Social engineering is a form of psychological manipulation used by attackers to trick individuals into divulging confidential information or performing actions that compromise security [5]. On the other hand, cybersecurity focuses on protecting against malicious actors who seek to exploit vulnerabilities in computer systems, networks, and applications [3]. A successful social engineering attack can lead to a cybersecurity breach, as the attacker gains access to sensitive information or systems that were previously secure.

For example, an attacker may use phishing tactics to trick an individual into providing their login credentials, which can then be used to access sensitive information stored on the network [14]. Another example is when an attacker poses as a trusted authority figure, such as a bank representative, to trick the individual into providing financial information. These types of attacks highlight the interplay between social engineering and cybersecurity, as the success of a social engineering attack often hinges on the exploitation of human behaviour and vulnerabilities [15]. As such, organizations must take a multi-faceted approach to cybersecurity that not only includes technical measures, but also focuses on raising awareness and educating employees about the dangers of social engineering [16].

In the subsequent sections of the current state of the art, a comprehensive examination of cyber-security, social engineering, and social engineering attacks will be conducted.

3.2 Cyber-security

The concept of cybersecurity has undergone significant development and extensive research [13]. Cyber threats are no longer limited to external actors seeking financial or political gain, but can also arise from internal sources such as employees or unauthorized access to systems

[17]. Attackers now prefer to find security vulnerabilities in the network layers of organizations rather than attacking the existing security walls [17].

The impact and damage caused by cyber-attacks have made the detection of these attacks a critical issue, and extensive academic research in this area has been conducted. The primary goal of cyber-attacks is to cause harm to the other party in various ways, including economic, political, social, and personal harm through unauthorized acquisition of intelligence information [13]. Information technology is often used as a tool in these attacks.

Protecting increasingly diverse and growing information systems from these attacks, detecting attacks and cybersecurity incidents, and establishing response mechanisms are essential in reducing or eliminating these events, provided that the necessary measures are taken in the field of cybersecurity.

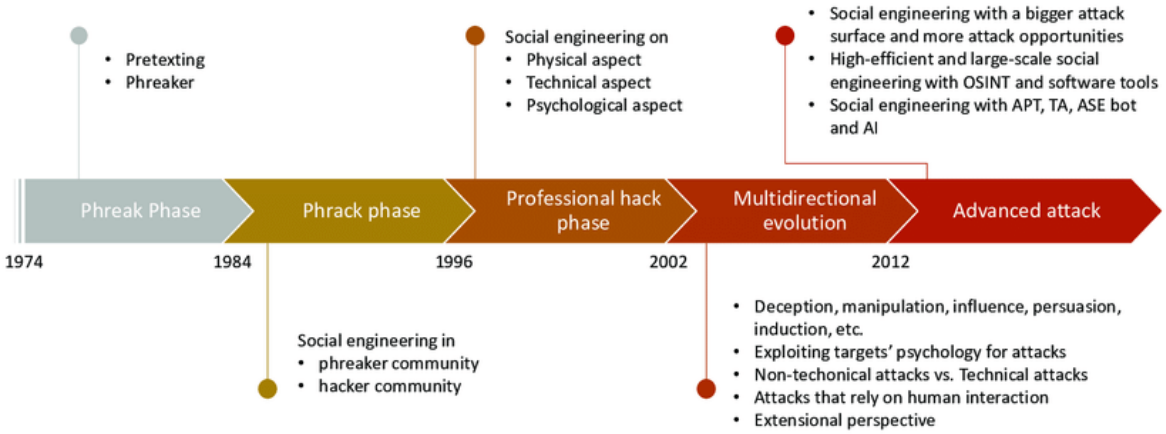


Figure 3: The Conceptual Evolution of Social Engineering in Cybersecurity [18].

As it is illustrated in Figure 3, the conceptualization of social engineering within the realm of cybersecurity has undergone significant evolution over the years. Initially, social engineering was viewed primarily as a low-tech form of attack, relying on psychological manipulation to trick individuals into divulging confidential information [18]. However, as the threat landscape has evolved and become increasingly sophisticated, the definition of social engineering has expanded to encompass a broader range of tactics and techniques [18]. This includes the use of advanced technologies, such as phishing scams and voice over IP (VoIP) impersonation, to carry out attacks.

In recent years, social engineering has gained recognition as a serious threat to cybersecurity, prompting the development of strategies to defend against these types of attacks. This has involved the implementation of technical solutions, including multi-factor authentication and threat detection systems, as well as the implementation of awareness and training programs for employees to help them recognize and respond to social engineering attacks [18, 19]. As a result, the conceptualization of social engineering in cybersecurity has evolved from a simple form of trickery to a complex and ever-evolving threat that requires a multi-layered approach to defense.

3.3 Social engineering

Social engineering is a significant threat to cybersecurity that requires a multi-layered approach to defense. It involves gaining people's trust, convincing them to perform actions they may not want to do and exploiting their weaknesses, mistakes or emotions. Social engineering is defined as the manipulation of human behavior in order to take over a system or obtain confidential and sensitive data [3]. In other words, it is the art of persuasion and information gathering based on deception, lies, and intimidation.

Social engineering attacks are often carried out by external attackers, also known as social engineers. However, it is important to note that such attacks can also originate from within an organization [3]. These attackers are experts in human psychology and use a variety of tactics to manipulate their targets and obtain the information they need. They take advantage of human vulnerabilities such as ignorance, carelessness, or personal weaknesses, making it easier to achieve their objectives [5].

To prevent social engineering attacks, organizations must take a multi-faceted approach that includes not only technical solutions, such as multi-factor authentication and threat detection systems but also employee education and awareness programs. Such programs help employees to recognize and respond to social engineering attacks by teaching them about the tactics and strategies used by social engineers [5]. By being proactive and vigilant, organizations can mitigate the risks associated with social engineering attacks and protect their valuable assets from unauthorized access.

Social engineering is a type of hacking methodology that relies on exploiting trust and communication rather than technical skills, and it offers several advantages compared to other hacking methods [16]:

- Is easier to implement than any other hacking method;
- Does not require IT specialism;
- Involves minimal cost;
- Involves low risk;
- Works with any operating system;
- Does not require networking;
- Leaves no trace;
- Is generally secure and effective;
- Does not become obsolete over time;
- Is not well known to the victims.

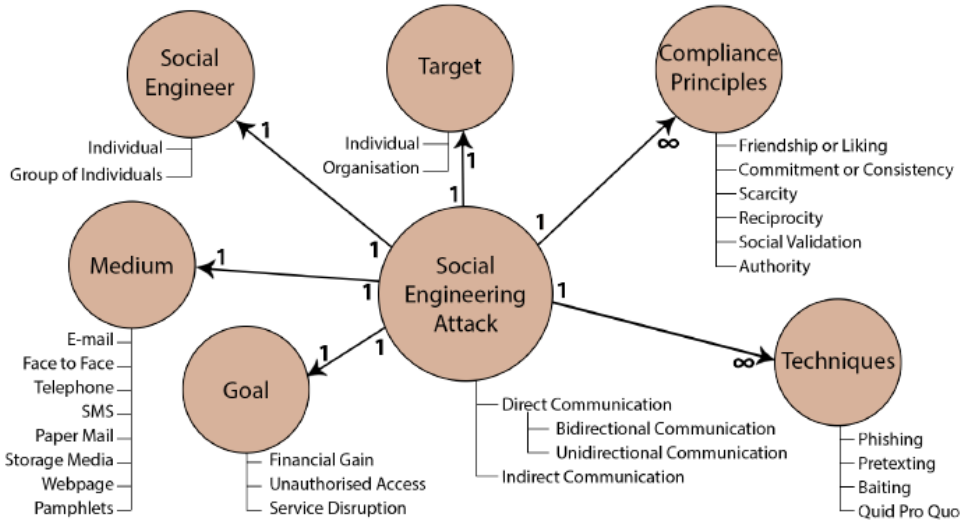


Figure 4: An Ontological Model of a Social Engineering attack [20].

Figure 4 demonstrates the ontological model of Mouton which explains how a classic social engineering attack works. As can be seen, a social engineering attack uses direct or indirect communication [20]. The attack can be divided into several attack phases, and each phase is treated as a new attack according to the model [20]. Instead of disconnecting the target system, bypassing the firewall or bypassing other security measures, the social engineer tries

to hack the system user directly in a shorter and less risky way [20]. Kevin Mitnick, who is seen as the inventor of social engineering, stated in his book on social engineering that he used this method and accessed 80% of the systems he entered through social engineering methods [3]. Mitnick infiltrated even some of the most secure computer systems in the world with social engineering methods instead of following a technical method and gained access to thousands of Telecom data [3].

The perception that security breaches are solely due to technical means is a common misconception. In reality, vulnerabilities within the system can be exploited by intruders, making technical measures insufficient in ensuring complete security. The continuous updates to the system can introduce new flaws and security vulnerabilities that are unknown, leading to an increased risk of attacks [18].

Moreover, social engineering attacks can bypass software and hardware security measures, and only require the attacker to obtain the target system's credentials, which can be done through a variety of social engineering techniques [20]. Social engineers identify the weaknesses and shortcomings of their target system's users and wait for the right moment to launch their attack, making their efforts more effective [20].

System users' lack of knowledge of security policies, inadequate security awareness, ignorance of the negative consequences of their actions, and delays in addressing security vulnerabilities all contribute to making the work of social engineers easier [20].

3.4 Attributes and motives of a social engineer

Social engineering is a tactic used by attackers to manipulate individuals into revealing sensitive information or granting unauthorized access to secure systems. Attackers typically assign roles to the victim in accordance with the attack scenario they find most applicable. They tend to act friendly, build good relationships, and use imitation and persuasion methods to get faster results than attacking the system network directly [10].

In order for social engineering attacks to be successful, the social engineer utilizes a variety of skills including high persuasion and imitation skills, snappiness, decent impression, good

observation, and the ability to keep up with changing situations while having good communication skills [5].

A social engineer is someone who understands and manipulates human psychology in a methodical way to achieve their goals. They are skilled in managing their emotions, choosing their words carefully, and finding creative solutions to problems. The social engineer can be portrayed as someone who is curious in both the IT and psychological fields [3].

Recognizing a social engineer is difficult since they can hide behind any person or professional role. They may present themselves as a customer, an expert, or a new insider, making it challenging to identify and expose them before they compromise the system and disseminate the information. This is why a real social engineer may hide behind a skilled speaker who is not necessarily an IT expert but rather a communication expert capable of impersonating any professional figure. This means that anyone can be a social engineer, as many of us have unknowingly used their techniques in everyday life [3].

For example, the following is a social engineering attack that demonstrates in practice the characteristics described above so far:

- A sudden phone call is received during a quiet afternoon. The attacker, posing as an employee of an airline agency, claims that tickets to Prague have been booked in the victim's name. Despite the victim's insistence that they did not book the trip, the attacker asks for their social security number to check the reservation. However, in reality, the attacker is using this pretext to obtain the victim's personal information.

As it can be seen on the example above, the real target of a social engineer is people, especially those who are easily manipulated. As Albert Einstein once said, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former" [5]. This quote highlights the need for individuals to be vigilant and aware of the risks associated with social engineering attacks.

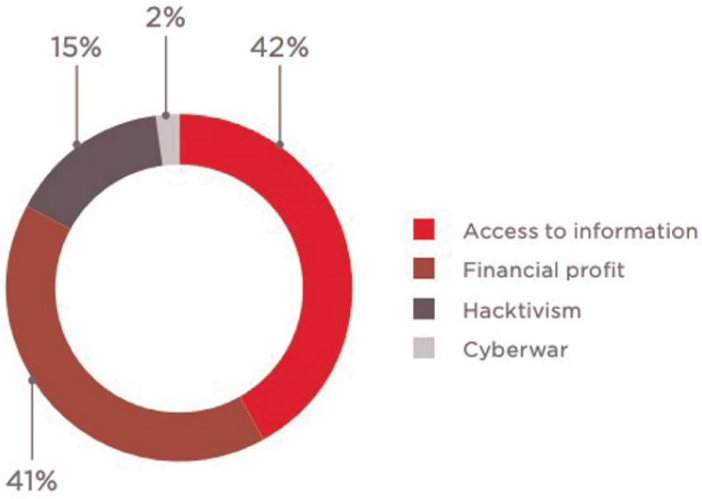


Figure 5: The most common attacker motives [21].

Figure 5 provides an overview of the different reasons why attackers engage in social engineering attacks. The figure highlights 4 common attacker motives: access to information, financial profit, hacktivism, cyberwar. It's important to note that these percentages are based on the research and data presented in the article, and may not necessarily apply to all cases of social engineering attacks [21].

According to the study, "Access to Information" is the most common attacker motive, with approximately 42% of attacks motivated by the desire to gain access to sensitive information [21]. This may include personal information, financial information, or corporate information.

"Financial Profit" is the second most common motive, with approximately 41% of attacks motivated by the desire to make money [21]. This may involve stealing money directly, such as through online banking fraud, or indirectly, such as by selling stolen information on the black market.

"Hacktivism" is the third most common motive, with approximately 15% of attacks motivated by political or ideological reasons [21]. This may involve targeting specific organizations or individuals as part of a larger campaign or movement.

Finally, "Cyberwar" is the least common motive, with approximately 2% of attacks motivated by the desire to cause harm to national security or critical infrastructure [21].

These attacks may be carried out by state-sponsored actors or other groups with political or ideological motivations.

3.5 The cycle of social engineering attacks

Social engineers target people to achieve their objectives, which can range from causing damage to a company's core business to disrupting its system. Typically, social engineers do not attack systems to take them offline, but instead, launch attacks on selected victims. Cyber social engineering attacks are generally divided into four main phases: information gathering, developing relationships, exploitation, and execution.

The first phase, information gathering, involves collecting data about the target and the organization. The social engineer uses different techniques such as pretexting, phishing, and dumpster diving to gather information [9]. Pretexting involves creating a false identity to gain access to sensitive information. Phishing involves sending emails or messages that appear to be from a legitimate source to trick the recipient into giving up sensitive information [9]. Dumpster diving involves searching through the target's trash for useful information [9].

The second phase, developing relationships, is achieved by building trust and rapport with the target. The social engineer uses techniques such as authority, familiarity, and liking to establish a relationship with the target [22]. Authority involves presenting oneself as someone with power or influence. Familiarity involves presenting oneself as a friend or someone with shared interests. Liking involves creating a bond by expressing commonality with the target.

The third phase, exploitation, is accomplished by using the information and relationship established in the previous phases to gain access to the target's system or information. Social engineers use techniques such as baiting, piggybacking and quid pro quo to exploit their targets [22]. Baiting concerns offering something of value to the target in exchange for sensitive information [9]. Piggybacking comprises following someone into a restricted area or using a stolen access card to gain entry [9]. Quid pro quo involves offering a service or benefit in exchange for sensitive information [9].

The fourth and final phase, execution, is completed by carrying out the attack to achieve the desired objective. The social engineer uses the access and information gained in the previous phases to accomplish the goal, which can include stealing data, compromising systems, or causing damage to the target organization.

As shown in Figure 6, the typical social engineering attack cycle has four phases: information gathering, developing relationship, exploitation, and finalization (execution implementation). Depending on the nature of the attack, some or all of the steps may be repeated until the attacker has been caught, has given up, or has obtained the desired result.

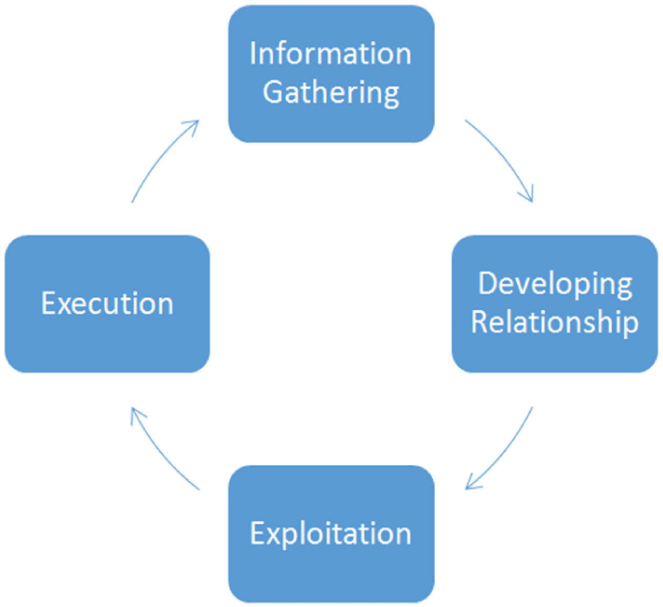


Figure 6: Social engineering attack lifecycle [22].

3.6 Social engineering approaches

Social engineering attacks are complex and can involve various physical, social, and technical tactics that are employed at different stages of the attack. Even with strong encryption and software security measures, a network is never completely immune to technical or non-technical attacks. The human factor remains the weakest link when it comes to achieving fully secure systems and should not be ignored [20].

One of the simplest ways to breach a system is by asking permission from the person in charge. Attackers may use social engineering tactics to convince an employee to grant them

access, such as posing as an IT technician or a high-ranking executive. This highlights the importance of training employees to recognize and avoid social engineering attacks.

In terms of technical measures, even the most advanced security software cannot fully protect a network if employees inadvertently or deliberately provide access to attackers. Virtual private networks (VPNs), firewalls, antivirus, anti-malware, and encryption devices are all essential tools for cybersecurity, but they should not be relied upon exclusively [23].

To mitigate social engineering attacks, it is important to understand the different approaches employed by attackers. These approaches can be categorized under 5 branches as: physical, social, technical, reverse-social, socio-technical approaches. By familiarizing themselves with these tactics, individuals and organizations can better recognize and defend against social engineering attacks. This sub-section aims to explain the different approaches used by attackers.

		Phishing	Shoulder Surfing	Dumpster Diving	Reverse Social Engineering	Waterholing	Advanced Persistent Attack	Baiting
Channel	E-Mail	✓			✓			
	Instant Messenger	✓			✓			
	Telephone, VoIP	✓			✓			
	Social Network	✓			✓			
	Cloud	✓						
	Website	✓				✓	✓	
	Physical	✓	✓	✓	✓			✓
Operator	Human	✓	✓	✓	✓			✓
	Software	✓		✓	✓	✓	✓	
Type	Physical		✓	✓				✓
	Technical					✓	✓	
	Social				✓			
	Socio-technical	✓			✓	✓		✓

Table 1: Classification of social engineering attacks [23].

Table 1 presents a taxonomy of social engineering attacks. The table lists different categories of social engineering attacks and provides examples of each. The categories of social

engineering attacks include technical attacks, which exploit vulnerabilities in technology; human-based attacks, which exploit human behavior and weaknesses; and blended attacks, which combine technical and human-based attacks [23]. Examples of technical attacks include social network attacks and malware, while examples of human-based attacks include pretexting, baiting, and piggybacking. Blended attacks include spear phishing and watering hole attacks. The taxonomy presented in Table 1 can be useful in developing strategies to mitigate the risk of social engineering attacks by understanding the different types of attacks and how they operate [23].

3.6.1 Physical approaches

In social engineering attacks, physical approaches refer to the methods where the attacker performs some physical action to gather information about a target victim [24]. Personal information, such as social security numbers and dates of birth, and valid credentials for computer systems can be obtained through these approaches. Dumpster diving is a common method used by attackers, which involves going through an organization's or individual's trash [24]. Attackers can find personal information about employees, manuals, notes, and even printouts of sensitive information, such as user credentials, in the trash. For example, if the attacker has access to a targeted organization's offices, they can find information such as passwords written on post-it notes in open work areas. Less sophisticated physical attacks require theft or extortion to obtain information [24].

3.6.2 Social approaches

Social engineering attacks often utilize social approaches that leverage social psychological techniques to manipulate victims. These techniques may include persuasion methods, such as perceived authority, which are based on principles like Cialdini's principles [14]. However, social vectors that rely on human curiosity, such as spear phishing and baiting attacks, are also used [5]. Additionally, attackers often try to establish a relationship with their victims to increase the chances of success of these attacks [3]. One common social attack vector not addressed by Cialdini is the vishing, which is one the most prevalent type of social engineering attack [4, 22].

3.6.3 Reverse social engineering approaches

Reverse social engineering is an indirect approach used by attackers to trick potential victims into thinking that they are a trustworthy entity, leading them to approach the attacker for help. This approach involves three main parts: sabotage, advertising, and assisting [14]. The first step is to sabotage the company's computer system by gaining easy access to the system and corrupting it. This technique is used to make the victim realize that something is wrong and start looking for help to repair the system. The attackers then pose as an IT support team and offer to fix the problem. The victim, thinking that they are dealing with legitimate support personnel, begins to provide the attacker with all the information they need to gain access to critical information.

3.6.4 Technical approaches

Most technical attacks are conducted over the Internet [25]. According to Granger, the Internet is particularly appealing for social engineers to collect passwords because people often use the same (simple) passwords for different accounts [25]. However, most people are unaware that they are providing attackers or potential attackers with a vast amount of personal information [25]. Attackers often use search engines to gather personal information about potential victims, and there are also tools that can collect information from various web sources. One popular tool is Maltego, which can be used to automate information gathering and analysis [14]. In addition, social networking sites are becoming valuable sources of information for attackers. Thus, personal information can be easily accessed by browsing with tools in a more convenient way.

In the field of information gathering, Maltego serves as a relational database for information which can help locate links between different pieces of information, also known as entities within the application [26]. With Maltego, users can quickly identify connections between seemingly disparate entities that may be of interest [26].

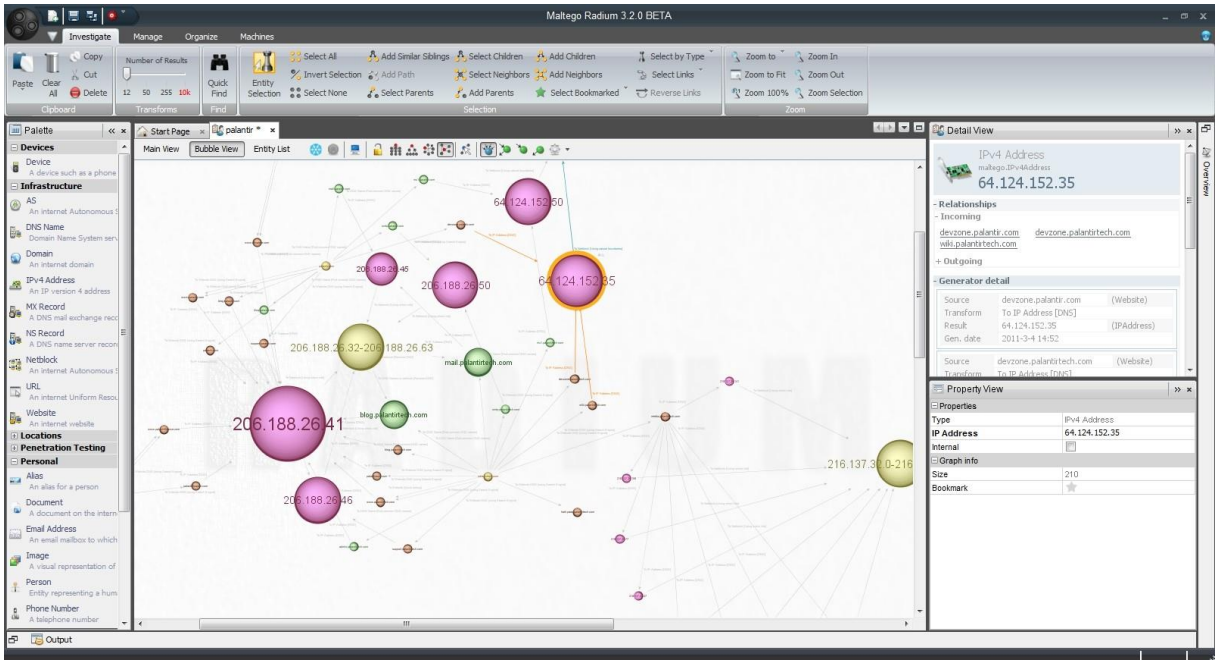


Figure 7: An in-sight to Maltego software illustrating order of links away from the original target [27].

For instance, imagine a user has a list of email addresses and websites and they are trying to determine which websites are linked to two or more of the email addresses. Such an analysis would be impractical to perform manually. However, Maltego automates this process, allowing the user to easily identify any connections between entities of interest.

Additionally, Maltego simplifies the task of mining information, including email addresses, websites, IP addresses, and domain information [26]. For example, Maltego enables users to automatically search for any email addresses within a target domain or domains with just a few clicks.

Maltego's ability to automate the process of identifying relationships between entities and simplifying the task of mining information has made it a popular tool in the field of information gathering [26]. Its effectiveness has been demonstrated in a variety of settings, including cybersecurity, law enforcement, and intelligence operations [26].

3.6.5 Socio-technical approaches

Social engineering attacks have become one of the most powerful weapons in the hands of attackers, combining several approaches to increase their effectiveness. Successful social

engineering attacks typically utilize baiting attacks, in which attackers leave infected storage devices in places where they are likely to be found. One example is the use of USB drives with a Trojan horse, which can compromise the security of the target system [9]. Attackers also take advantage of people's natural curiosity by using labels such as "confidential" or "employee layoff 2023" to lure users into clicking on the infected device.

Phishing is another commonly used socio-technical approach that targets a large group of users through email or instant messaging. Although phishing is not typically targeted at specific individuals or small groups, scammers hope to fool enough people to make the attacks profitable. However, traditional phishing attacks are becoming less profitable, leading to the evolution of more sophisticated "spear phishing" attacks [14]. These attacks are highly targeted and personalized, using data mining techniques to gather information about the target and craft convincing messages. By utilizing social data from sources like social networking sites, attackers have increased the success rate of targeted phishing attacks from 16 % to 72 % [28].

The combination of technical and social approaches in social engineering attacks highlights the importance of both technical and human factors in cybersecurity. Effective defense against social engineering attacks requires a multi-faceted approach that addresses both technical vulnerabilities and human weaknesses [3].

3.7 Methods of the social engineering attacks

Hackers have turned their attention to social engineering as a way to bypass network security and gain access to sensitive information. As security measures for networks and applications improve, social engineers target the weakest link in the system: people [14]. Users may believe that their communication networks are secure and may let their guard down, making them vulnerable to social engineering attacks. Social engineers may first need to gather information on their targets, such as their contact information, before launching their attacks.

Social engineering is a widespread form of attack that takes advantage of human psychological factors, including our willingness to trust and our desire to help others. Social engineers may use a range of tactics, from impersonation to pretexting to baiting, to manipulate individuals into divulging confidential information or performing certain actions

[5]. These attacks often rely on the target's ignorance or carelessness in protecting personal data and identities.

Understanding the psychological factors that underlie successful social engineering attacks is crucial for developing effective defenses against them. Researchers have identified various number of factors that contribute to vulnerability, including trust, authority, urgency, and curiosity [3]. By exploiting these factors, social engineers can increase their chances of success. However, by raising awareness of these tactics and educating users about best practices for protecting their personal information, organizations can reduce the likelihood of successful attacks [5].

3.7.1 Impact of human factors on attacks

The topic of analyzing and relating the human factor in the context of computer and information security is still underdeveloped. Previous studies have primarily focused on developing security methods using smart cards, passwords, or biometric devices, ignoring the importance of the human factor for organizations. However, researchers now realize that humans are the biggest obstacle to effective computer and information security. This is because 80% of the financial losses of organizations are caused by security breaches, with most of these breaches being caused by people involved in various roles such as users, developers, stakeholders, and suppliers [11].

As the amount of data continues to increase, the infrastructure put in place for information security is no longer sufficient. To improve their knowledge and workforce, organizations need to address the human factor aspect of cybersecurity. The human factor of cybersecurity refers to actions or events that result in a cyberattack or data breach due to human error, such as sharing passwords, poor patch management, or gaining corporate access through a personal device.

Studies show that the impact of the human factor in increasing cybersecurity risks cannot be ignored and should concern organizations. Many employees put the organization's data or systems at risk due to carelessness, lack of due diligence, or lack of training in protecting their work. A survey conducted by Kaspersky Lab and B2B International among more than 5,000 companies worldwide revealed that 52% of companies are at risk from their employees

[7]. In fact, 57% of companies are aware that their own employees are the weakest link in their armor against cyber-attacks [7].

The human factor and employee behavior are directly proportional to insider risk and security anxiety [29]. The 2022 Cost of Insider Threats: Global Report provides some alarming statistics on this issue, showing that 47% of employees shared sensitive workplace data using their mobile devices, 46% caused the loss of physical devices containing data, and 44% used IT resources inappropriately [29]. Moreover, the report reveals that insider threat incidents have risen by 44% over the past two years, with costs per incident increasing by over a third to $15.38 million [29].

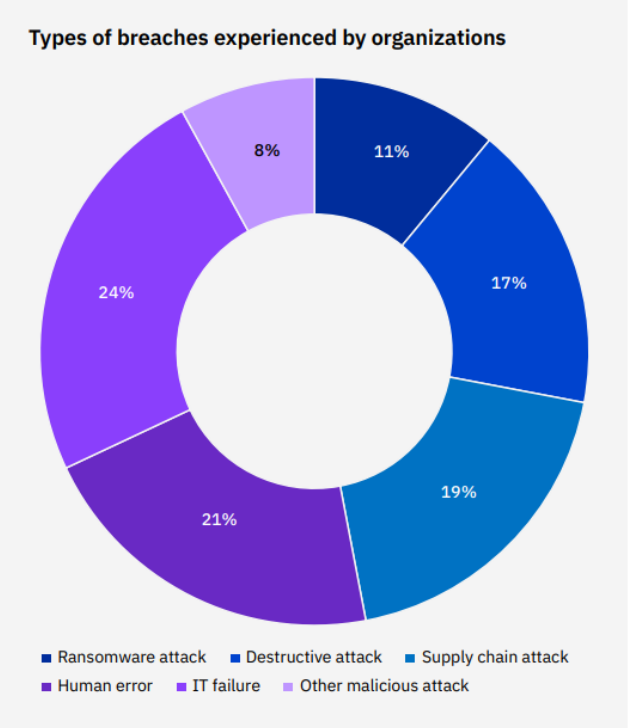


Figure 8: Types of breaches experienced by organizations [11].

The IBM Cost of Data Breach report echoes the conclusions of the 2022 Cost of Insider Threats: Global Report, providing further evidence of the importance of human factors in data breaches [11]. Specifically, as it can be seen in Figure 8, 21% of breaches were caused by human errors resulting from the negligent actions of employees or contractors [11].

It is concerning that many employees remain unaware of the risks they pose to their organizations, particularly in small businesses where supervision on issues such as

information security, IT resource use, and cybersecurity policies is often lacking [11]. This lack of awareness is a significant contributor to the high rates of employee errors observed in these environments [11].

Figure 8 from the IBM Cost of Data Breach Report 2022 also shows the various types of breaches experienced by organizations, with human error and system glitches being among the most common causes [11]. This highlights the importance of addressing the human element in cybersecurity measures and implementing comprehensive training programs that educate employees on the risks of social engineering and other forms of cyberattacks. By improving employee awareness and understanding of cybersecurity best practices, organizations can significantly reduce the risks of data breaches and other cybersecurity incidents caused by human error.

3.7.2 Psychological manipulation methods behind the attack

The term "Social Engineer" is often used to describe someone who is skilled at manipulating people to achieve their goals. These individuals are often referred to as "excellent psychologists" because of their ability to empathize with their targets, understand their behaviors, and build relationships with them. This psychological approach is a key factor in the success of social engineering attacks [5].

Bruce Snell, the director of technical marketing for McAfee Security System, explains that every person has a trigger, and a skilled social engineer will find it [30]. Social engineering techniques are based on strong psychological principles, and any social engineer will always focus on certain behavioral and psychological traits of their target in order to extract as much information as possible. Some of the tools that social engineers use include lying, telling partial truths, providing a reason, avoidance and diversion, interrelation, and the use of humor.

3.7.2.1 Lie

Social engineers are skilled in the art of deception, and lying is one of the primary techniques they use to manipulate their targets. People tend to judge others based on their own qualities, so social engineers take advantage of this by making themselves seem trustworthy and honest, while simultaneously lying to extract information from their targets [5]. By gathering

information about their target's behaviors, relationships, and habits, social engineers can identify their vulnerabilities and tailor their lies to exploit them.

3.7.2.2 Telling the partial truth

Social engineers may also tell partial truths in order to gain their target's trust. By selectively sharing certain facts and omitting others, they can manipulate their target's perception of reality and make them more susceptible to their influence. This technique is especially effective for social engineers who are not skilled at lying or keeping track of their lies [3].

3.7.2.3 Providing a reason

If a social engineer provides a reason for their request, even if the reason is absurd or nonsensical, their target is more likely to comply with their demands. This is because people tend to respond to requests that are accompanied by a reason, regardless of whether the reason itself is rational [3]. For example, in a study conducted at a library, people were more likely to let someone cut in line to use the photocopier if they provided a reason, such as "because I am in a hurry," even if the reason did not make logical sense. In the study scenario, participants were presented with the following dialogs [31]:

- "Excuse me, I have five pages. Can I use the copy machine because I am in a hurry?"

After this offer, 94% of the participants allowed him to copy their pages in front of them. In another group, the same person asks:

- "Excuse me. I have five pages. Can I use the photocopier?"

After such an offer without any reason, only 60% let him get in line. They refuse to let the new man take their copies and only complain that they are waiting for the same reason he mentioned. In the last group, the same person asks again:

- "Excuse me, I have five pages. Can I use the photocopier because I need to make copies?

After hearing such a strange reason, 93% of people let him go through the line [31]. This example was a real life case study and it clearly shows that the use of "because" is enough to make people think they have a valid reason for cutting the line, and that they cannot even process the reason themselves [31].

3.7.2.4 Avoidance and diversion

Social engineers may try to avoid or divert questions in order to conceal their true intentions or manipulate their target's perception of reality. They may change the subject or provide vague or irrelevant responses in order to distract their target or make them feel confused. Alternatively, they may feign innocence, anger, or confusion in order to make their target feel guilty or doubt their own perception of reality [3].

3.7.2.5 Interrelation

Interrelation involves establishing an emotional bond with the target by offering them a gift or favor, which creates a sense of indebtedness and makes them more likely to comply with the social engineer's demands. However, if the target perceives the gift or favor as a bribe or if they suspect that the social engineer has bad intentions, they may become resistant to their influence. Social engineers must be careful not to overuse this technique, as the feeling of reciprocity may diminish over time [5].

3.7.2.6 Use of humor

Social engineers may use humor to establish a positive relationship with their target and put them at ease. By making their target laugh and feel relaxed, social engineers can build trust and establish rapport, which makes their target more likely to comply with their demands. Additionally, humor can be used to defuse tense or problematic situations, making the social engineer's attack less visible [3].

3.8 Types of social engineering attacks

Although new social engineering attack techniques are constantly being created, based on the data obtained from the literature review, it is possible to classify the most well-known and preferred techniques under certain headings. These attacks can be gathered under 20 headings which are shown in Figure 9.

Figure 9: Social engineering attack methods [9].

Moreover, there are a few more titles that could be added to these headings, it was not found appropriate to include them here, as they are not well known and rarely used. In addition, it is necessary to remind that there may be new techniques that are not mentioned here, as new techniques are being built every day and are still used and known by a limited number of people. In the following sub sections, the most important methods will be studied in detail.

3.8.1 Pretexting

Pretexting is a tactic used by attackers to gain unauthorized access to sensitive information [3]. It involves creating a false scenario to convince the victim to divulge confidential information. The attacker may use various pretexts, such as claiming to be a representative of a legitimate company or organization, in an attempt to gain the victim's trust. This method of social engineering relies on the victim's willingness to help and provide the requested information.

Pretexting can take many forms, including phone calls, emails, or text messages. Attackers may use social media platforms to gain personal information about the victim that they can use in their pretext. Pretexting emails often create a sense of urgency or fear in the victim to prompt a quick response [23]. The attacker may threaten to take away some benefits or claim that the victim's account has been compromised, and they need to verify their personal information.

Pretexting is a serious security threat that can result in the loss of sensitive information and financial fraud [3]. Organizations and individuals can protect themselves from these attacks by being vigilant and not providing personal or financial information without verifying the legitimacy of the request. Education and awareness training for employees can also help prevent such attacks.

3.8.2 Reverse social engineering (RSE)

Another technique used by social engineers is reverse social engineering. This technique consists of convincing the target that they have a problem, or will have a problem in the near future, and that the attacker is willing to solve it. The reverse social engineering attack consists of three parts [23]:

- Sabotage: This is the phase in which the attacker compromises the system by pointing out the problem to the users, after which the victim will try to find help to solve the problem he or she has experienced [23].

- Advertising: At the very moment when the victim seeks help to solve the problem, the attacker presents himself as the only support for the problem he has created [23].

- Support: Having gained the necessary trust, the attacker is free to operate and has the ability to access the system and sensitive data [23].

The three phases described above are, of course, interdependent and consequential. The entire process of which they are a part is based on the social engineer's use of all the psychological techniques described in Chapter 3.7.2, with the goal of "earning" the user-victim's trust and thus more effectively perpetuating the attack.

3.8.3 Piggybacking

Piggybacking is a social engineering technique in which a perpetrator gains access to restricted areas by closely following authorized personnel. The social engineer pretends to be an authorized employee and follows an employee who has access to a target building. The social engineer may imply that they cannot open the door because they are carrying a heavy box and cannot reach their badge. They then try to enter the building by asking people for help and pretending to be an employee of the target building. This technique exploits the helpful nature of individuals, and the perpetrator relies on the fact that people are less likely to question someone who is following a legitimate employee [5].

The consequences of piggybacking can be devastating, as it can lead to unauthorized access to sensitive information, theft, or destruction of assets. Organizations should provide security awareness training to employees to educate them about the risks associated with piggybacking and to encourage them to report any suspicious activity. It is also essential for companies to implement access control measures such as security cameras, biometric systems, or security guards. If an authorized employee is approached by someone claiming to be an employee but without proper identification, the employee should be trained to politely refuse to assist and instead, direct the individual to the proper channels for access [3]. They should also report the incident to the security team, as it is an indication of a potential security breach [3].

3.8.4 Whaling

Social engineering attacks often target high-profile individuals, such as executives and managers, as they tend to have personal information that is easily accessible on social media sites or on the company's official website [23]. For instance, the online biography of a business administrator can reveal personal information, such as their interests or education history, which can be exploited by a social engineer to craft a convincing attack.
By leveraging the information gathered, a social engineer can design an attack that appears legitimate, such as an email invitation to a special alumni basketball tournament for graduates of a particular university's alumni department. The email might request that the executive visit a website to enter credit card information to reserve a good spot in the tournament [23].

These types of social engineering attacks are becoming increasingly popular, as verified personal information makes it easier for social engineers to persuade their targets [23]. Even with carelessly provided information, social engineers can attack specific targets who know their interests or what they like and dislike [23].

3.8.5 Dumpster diving

Dumpster diving is a social engineering method used to collect all kinds of information about a targeted person or organization. Information on discarded papers, invoices, charts, account numbers, customer information, personal information, CDs, etc., which are not completely torn up, can be used to make estimations [5]. Dozens of information such as food and drink consumed, the medical prescriptions, brand preference can be collected from personal trash. For social engineers and detectives, these areas are considered a treasure trove [3]. There is a lot of information that can be gathered from garbage alone, even detailed reports can be prepared. A lot of information can also be obtained (by recycling) from obsolete, scrapped hardware. Some of the materials used for this purpose are as in the following: CDs, hard drives, memory cards, etc. that have not been properly destroyed or recycled [3].

3.8.6 Social media network

Social networks like Facebook, Twitter, Instagram, and others provide a goldmine of information for social engineers [21]. They can quickly and easily gather a wealth of information about their targets, including their work history, hobbies, likes and dislikes, fears and beliefs. Social engineers use this information to tailor their tactics to the target's psychological profile [3]. The willingness of people to share their personal information on social networks can be exploited by social engineers to conduct successful attacks [6]. In addition, users' preference for allowing location and reporting services on social networks makes it easier for social engineers to discover their location and launch attacks [7]. By sending a friend request, a social engineer can establish an online friendship with a target and use the information gathered about the target's age, education level, profession, organization, and hobbies to tailor their tactics to be more effective [5].

This approach can be used in several ways:

- Sending an email impersonating a friend listed on the victim's page,
- Viewing a person's pictures in order to discover popular hangouts and then showing up with them nearby or in the same place,
- Discovering that a person's age, school, previous companies, place of birth, all of which can be used to target them,
- Adding the victim as a friend to establish an online relationship with someone to build trust.

The social engineer will then not hesitate to use the information about the victim to launch another attack.

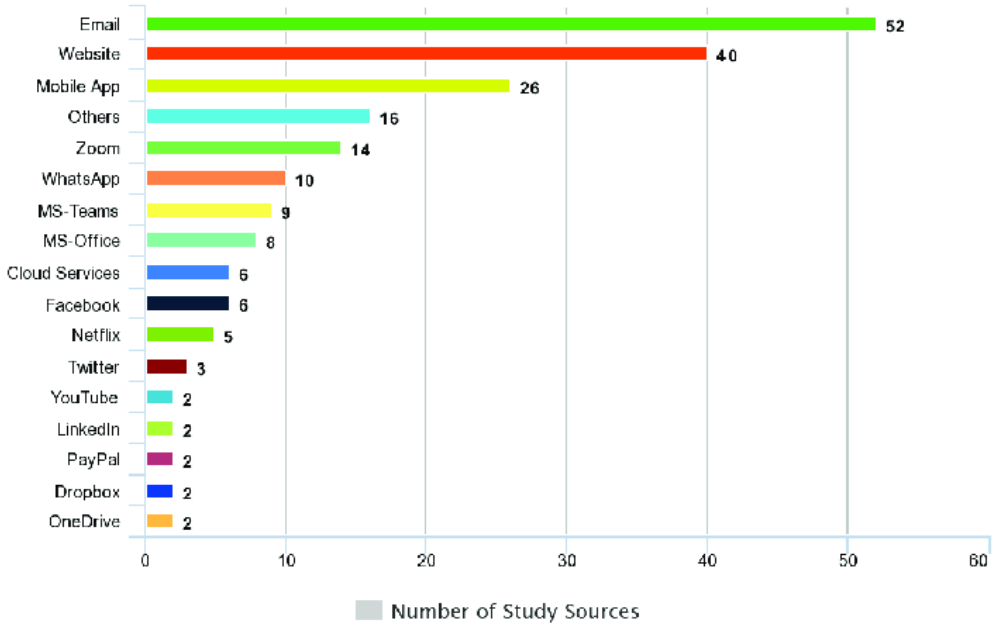


Figure 10: Mapping of study sources by the platform used as a weapon for social engineering based cyber-attacks/threats [13].

Figure 10 presents a mapping of the study sources based on the platforms used as weapons for social engineering attacks during the COVID-19 pandemic. The platforms identified include social media, email, and messaging applications. The figure shows that the majority of the studies focus on social media platforms as the most prevalent weapon for social engineering attacks. However, the figure also indicates an increase in the number of studies on email and messaging applications as these platforms have also become popular vectors for social engineering attacks during the pandemic [13].

3.8.7 Neuro-linguistic programming (NLP)

A key skill for social engineers is their ability to manipulate human behavior or information, as noted by Hadnagy in 2010 [5]. One of the powerful psychological approaches they use to achieve this is Neuro-Linguistic Programming (NLP), which deals with a person's neurological processes, language, and learned behavioral responses [32]. While NLP was originally intended for use in therapeutic contexts, it is now widely used by social engineers to manipulate the human mind and gather information from their victims.

In this technique, the social engineer employs body language and a strategic choice of words to deliver subliminal messages to the person they are attempting to manipulate. The candidate first matches their body language to that of the victim, including breathing rate, voice pitch, accent, and vocabulary, to establish a subconscious connection. Then, they may use further subliminal messages by changing body language, lightly touching the shoulders or arms, or using words that express positive thoughts and feelings [32]. These actions, known as anchoring and reframing in NLP terms, influence the person to have positive emotions and establish a sense of harmony with the social engineer. With this connection, the social engineer can effectively communicate their goals, such as gaining access to a company's sensitive information.

3.8.8 Honey trapping

Honey trapping is a social engineering tactic where an attacker impersonates an alluring individual to extract sensitive information from their target [5]. This type of attack is typically carried out by engaging with individuals who hold influential positions, such as successful business executives, to obtain confidential information.

In a honeytrap attack, social engineers pose as an attractive man or woman to create a romantic or sexual relationship with their target. The attacker builds rapport and gains the victim's trust to extract sensitive information. The attackers may also use flattery, subtle manipulation, and emotional pressure to lure their victims into revealing valuable data.

Honeytraps are used by both cybercriminals and state-sponsored actors, as it is an effective way to acquire sensitive information without the need for technical expertise [3]. This type

of attack is not only limited to online interactions but can also happen in person through physical seduction. In fact, there are cases where the attacker uses the help of a third-party accomplice to create a more convincing scenario.

3.8.9 Shoulder surfing

Shoulder surfing is a technique in which an individual stands close to another person who is entering sensitive information into a computer or mobile device, without revealing the contents or information such as password, PIN code, username, etc. This practice can occur in various settings, such as workplaces, public transportation, cafes, and ATMs [33].

Attackers may use shoulder surfing to gather confidential information for malicious purposes. They may rely on their observation skills and the victim's negligence to obtain valuable data. This type of attack can be especially effective in crowded public places, where it may be difficult for victims to notice someone standing too close [33].

To mitigate the risk of shoulder surfing, it is recommended to maintain a safe distance between oneself and others when entering sensitive information. Additionally, using privacy filters or shielding screens can help prevent attackers from observing the screen. It is also advised to be aware of one's surroundings and suspicious behavior of those around them [33].

3.8.10 Quid pro quo

Quid pro quo is a social engineering technique where an attacker offers help to a target user in exchange for obtaining access to their data. The attacker takes advantage of a supposed technical error on the target user's computer to gain their trust [5]. For example, an attacker posing as an IT support representative may offer to fix a user's computer issue in exchange for their login information [23]. Once the attacker gains access, they can install malware on the victim's computer, demand a ransom, or steal sensitive information [23].

3.8.11 Watering hole

Watering hole attacks involve exploiting security vulnerabilities in websites that are commonly visited and trusted by a target audience in order to gain access to their information

and computer systems. Attackers may use tactics such as injecting malicious code into the website to install malware on the victim's computer or to steal credentials used to access sensitive data [21].

3.8.12 Scareware

Intimidation attacks are a type of scam that preys on a victim's fear of malware infection or illegal downloading. The attacker presents a fake solution that purports to solve the non-existent problem, thereby tricking the victim into downloading and installing malware. These attacks begin by persuading the victim that their system is infected with viruses, and then provide a link to anti-virus software that the victim must download for a fee to remove the viruses. The security software also displays periodic warnings about infections, and the victim is asked to pay again to remove them. These types of attacks have become widespread in recent years and are aimed at individuals in positions of authority, such as police officers, prosecutors, and judges, informing them that their name has been linked to a terrorist group or gang and that they can take care of the problem in exchange for payment [23].

3.9 Advanced social engineering attacks

3.9.1 Phishing

Phishing is a fraudulent activity that involves the collection of sensitive information such as usernames, passwords, and credit card details by posing as a trusted entity in electronic communication [14]. This technique is often used to deceive targets into opening deceptive messages, links, or files that contain malicious data payloads, which can install a program or application on the target's device without their knowledge [34].

According to Hadnagy (2017), cybercriminals often use phishing as a way to gain unauthorized access to an individual's personal or business information. As a result of clicking on the link address sent in the email or opening the attached file, the victim's device can be infected with malware such as a Trojan horse or keylogger, allowing the attacker to take control of the victim's device and carry out various malicious activities [34].

Phishing attacks have become increasingly common and sophisticated in recent years [35]. It was reported that phishing is the most common type of social engineering attack [9]. It is

crucial for users to be aware of phishing tactics and learn how to identify and avoid suspicious emails or links to protect their personal and sensitive information from being compromised [2, 34].

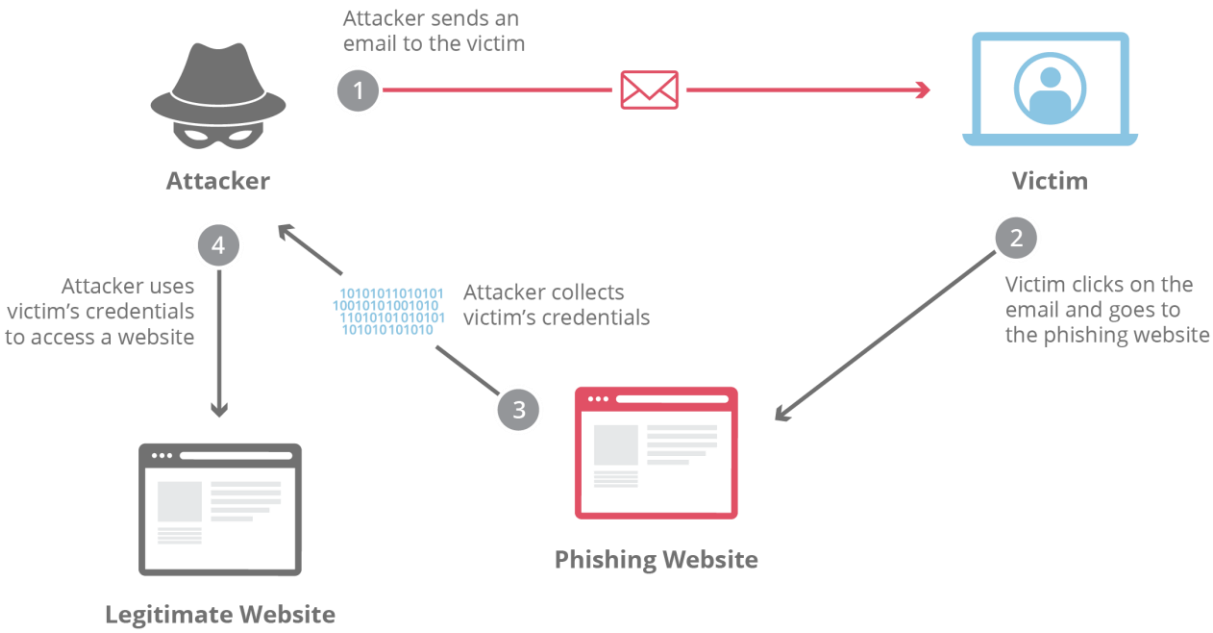


Figure 11: A demonstration of a phishing attack [36].

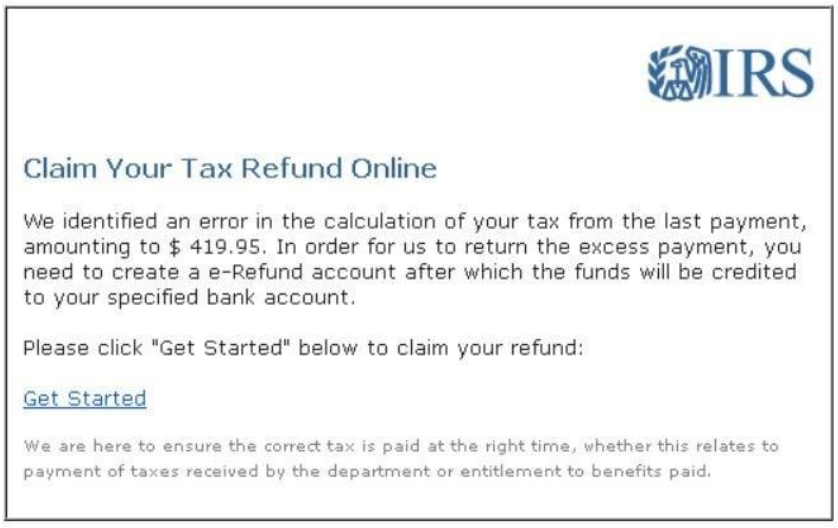


Figure 12: An example of a tax refund phishing email [37].

Figure 12 shows an example of a phishing email from the Internal Revenue Service (IRS). The email is designed to look like an official communication from the IRS, informing the recipient that their tax return has been calculated incorrectly. The e-mail contains a link that

the recipient is prompted to click in order to fix the issue. However, the link in the email leads to a fake website that is designed to look like the official IRS website. The fake website asks the recipient to enter their personal information, such as their Social Security number, date of birth, and credit card information. If the recipient enters their information, the cybercriminals behind the phishing email can use it for fraudulent purposes, such as identity theft or financial fraud [37].

This type of phishing scam is a form of social engineering that exploits the trust that people have in government institutions, such as the IRS [37]. By impersonating a trusted source, the phishing email creates a false sense of security in the recipient, who may not suspect that the email is fraudulent as the IRS would never contact taxpayers via email to request personal or financial information [37].

3.9.2 Voice phishing (Vishing)

Vishing, or voice phishing, is a social engineering technique used to trick targeted individuals into disclosing personal and financial information over the phone [5]. The attacker can adapt their strategy based on the victim's responses during the phone call, which gives them greater control over the conversation and the ability to persuade the victim [3]. In some cases, even the victim's tone of voice can be used as a clue to help the social engineer achieve their goal [3].

One common and highly effective vishing technique is the use of pre-recorded messages [12]. The message may claim to be from the victim's bank and alert them that their credit cards have been compromised. The victim is then instructed to call a number to resolve the problem, and when they do, they are prompted to enter their credit card number, PIN, and other sensitive information [12]. Alternatively, a social engineer may conduct the conversation themselves and use office sounds in the background to make the victim believe they are speaking to a legitimate representative from the company or bank [3].

Vishing can also be used in conjunction with other types of attacks to increase their success rate [14]. The victim may be given a sense of urgency or a time limit to complete a task, which can increase the likelihood that they will comply with the attacker's demands [14].

3.9.3 Spear phishing

Spear phishing is a targeted form of phishing in which the attacker selects a specific individual or organization to attack rather than sending out mass or random emails [14]. The attacker gathers information about the victim from various sources such as social media, the internet, and other publicly available data, and then sends carefully crafted and personalized emails to the victim in order to trick them into clicking on a link that will lead to a website with malware [14]. These emails are designed to appear legitimate and often include details that are specific to the victim, making them more likely to fall for the attack.

3.9.4 Baiting

Baiting is a type of social engineering attack that involves leaving a physical item, such as a USB drive, CD, or DVD, in a place where someone is likely to find and take it [3]. The item typically contains malicious software, a fake update, or some other type of malicious content that can compromise the person's computer or steal sensitive information when the person inserts the device into their computer [3].
The attacker counts on the person's natural curiosity and the trust they have in technology to lure them into inserting the device into their computer. The attack works because the person believes that they have found something of value and doesn't suspect that the device is actually a trap.

Baiting is an effective form of attack because it takes advantage of people's basic human tendencies, such as the desire to find something valuable or the tendency to trust technology [23]. It can be difficult to detect and defend against because the person doesn't realize they are being attacked until it is too late. To protect against baiting attacks, it is important to be vigilant and suspicious of unexpected or unidentified items, and to practice safe computing habits, such as avoiding unknown USB drives and verifying the authenticity of software before installing it.

4 Countermeasures for the Social Engineering Attacks

Constantly evolving and changing technology has created new areas. Of course, this has not escaped the attention of social engineers who have taken advantage of the disadvantages of diversity and novelty. By developing new methods, they are becoming more successful in cyber-attacks. These attacks continue to cause severe social, economic, and reputational damage to victims [38].

Although there is no way to prevent social engineering attacks, there are ways to mitigate the risks and damage. All the measures taken against cyber-attacks are accepted for social engineering attacks. However, in addition to system and network infrastructure measures, employee awareness and training measures for social engineering attacks are becoming increasingly important [11]. Attacks can target senior executives as well as a janitor, security guard, or even a new employee [11]. It has always been tempting for social engineers to target the weakest link in the security chain, the human being, in order to gain easy access even to organizations protected by the best security measures. Organizations should implement measures that can be taken against social engineering attacks, not ignoring that a system with a human element is not absolutely secure. Some of these measures include:

Countermeasure	Description
Employee training	Educate employees about social engineering attacks and how to prevent them. Training should include how to recognize and respond to phishing emails, how to identify and report suspicious activity, and how to protect sensitive information [2, 34].
Security policies	Establish clear security policies and procedures that outline best practices for protecting sensitive information. Policies should address topics such as password management, data classification, and access control [2, 16, 34].
Two-factor authentication	Require employees to use two-factor authentication for accessing sensitive information or systems. This adds an extra layer of security that makes it more difficult for attackers to gain access to accounts [6].

Anti-phishing software	Deploy anti-phishing software to prevent phishing emails from reaching employees' inboxes. This software can automatically detect and block phishing attempts [38].
Email filters	Implement email filters that can identify and block emails that contain suspicious links or attachments. This can prevent employees from accidentally clicking on malicious links or downloading infected files [11].
Incident response plan	Develop an incident response plan that outlines the steps to take in the event of a social engineering attack. This should include procedures for reporting incidents, assessing the impact of the attack, and containing and mitigating the damage [2, 34].

Table 2: The most commonly used countermeasures against social engineering attacks.

4.1 Defence mechanisms

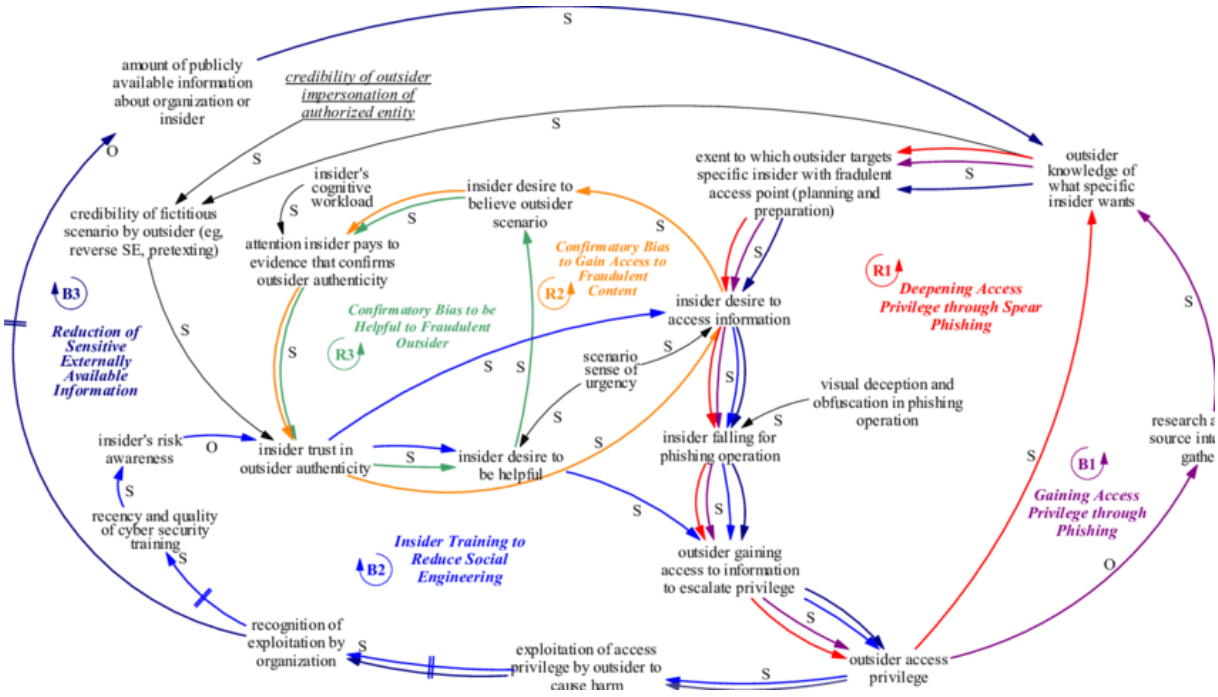


Figure 13: Causal Loop Diagram of Avenues for Social Engineering Mitigation [39].

As can be observed in Figure 13, a Causal Loop Diagram (CLD) is a visual representation of the interactions between different variables in a system and can be used to analyze and understand the causes and effects of social engineering attacks. The study of CLDs in the context of social engineering mitigation provides a valuable framework for organizations to understand the avenues for mitigating these attacks and protecting against them.

In social engineering attacks, attackers manipulate individuals into divulging confidential information or performing actions that compromise security. The CLD of social engineering mitigation encompasses a number of variables that interact with each other, including the psychological, technological, and organizational factors that contribute to the success of these attacks [34].

At the psychological level, social engineering attacks often exploit human emotions, biases, and trust to trick individuals into providing sensitive information or performing actions that compromise security. To mitigate these attacks, organizations must raise awareness and educate employees about the dangers of social engineering and how to identify and avoid these tactics. This can be accomplished through training programs, awareness campaigns, and regular reminders about the importance of maintaining secure behavior.

At the technological level, organizations can implement technical measures to protect against social engineering attacks, such as firewalls, intrusion detection systems, and anti-virus software. These tools can help prevent attackers from accessing sensitive information or systems, and can provide a first line of defense against these attacks [40]. However, these technical measures alone may not be sufficient to prevent successful attacks, and must be combined with other measures to be effective [40].

Finally, at the organizational level, organizations must take a multi-faceted approach to social engineering mitigation that includes both psychological and technological measures. This requires a culture of security that places a strong emphasis on maintaining secure behavior and establishes clear policies and procedures for responding to social engineering attacks. Additionally, organizations must regularly assess and update their mitigation strategies to ensure that they are effective in preventing attacks and protecting against them. Overall, the study of the CLD of social engineering mitigation provides organizations with a valuable framework for understanding the complex relationships between the psychological, technological, and organizational factors that contribute to the success of these attacks [41]. By adopting a multi-faceted approach to mitigation that includes both psychological and technological measures, organizations can protect themselves against these attacks and reduce the risk of a security breach [41].

In the subsequent sub-sections, the most efficacious defense mechanisms for countering attacks will be elucidated.

4.1.1 Cyber security and social engineering awareness and training

The human element in organizations is increasingly vulnerable to social engineers, as they have become easier to access and exploit [34]. Organizational policies such as strong passwords, two-factor authentication, and firewalls may not be effective if employees do not understand the importance of securing their access cards and passwords [23]. The security of a company is only as strong as its weakest link, and in many cases, it can be the employees themselves. Since the beginning of modern technology, social engineers and hackers have recognized that any technological system is most vulnerable when it involves human interaction [3]. They perceive people as entry points that can be easily manipulated to gain access to any network, system, or data. Consequently, their methods of infiltrating targets have changed. Social engineers now use deception, manipulation, coercion, and other tactics to obtain information through false claims [3]. To prevent cyber-attacks and protect organizations, employees must be trained in cyber-attack awareness and information security [23].

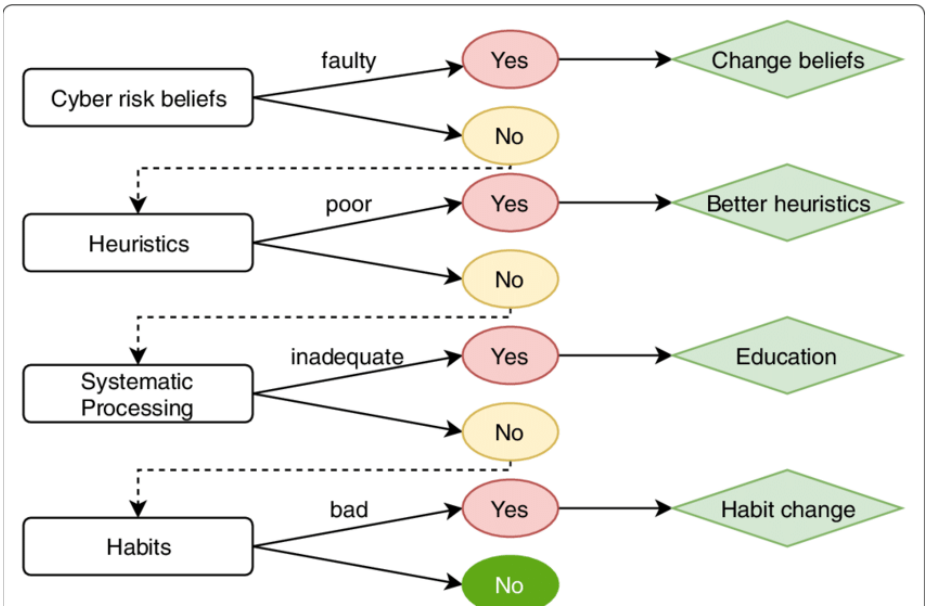


Figure 14: Algorithm that determines why users potentially fall victim to phishing and what is necessary course of action as a countermeasure [35].

Phishing attacks are a widespread threat to computer security, and users often fall victim to these attacks due to a lack of knowledge or awareness of the warning signs [14]. To counteract these attacks, an algorithm can be developed to analyze user behavior and interaction patterns and identify specific areas of weakness, such as a tendency to click on unknown links or provide personal information without verifying the legitimacy of the request [6]. Once these weaknesses are identified, countermeasures can be put in place, such as implementing user training programs, providing clear warnings about the risks of phishing attacks, and incorporating anti-phishing tools in web browsers and email systems [35]. These measures can help users become more aware of the dangers of phishing attacks and how to avoid them, ultimately reducing the success rate of these attacks and increasing the overall security of computer systems.

The most effective strategy for dealing with social engineering attacks is training, which can make employees more skeptical and aware of cyber-attacks [34]. It is critical for organizations to ensure that employees understand the importance of protecting sensitive data and how to make it difficult for social engineers if they choose to do so [35]. With further awareness through training, employees will be able to differentiate between different attack vectors, where, how, and through which channel the attack is coming from [34]. This increased awareness can turn the weakest link in an organization into the strongest, making it harder for social engineers to get information, requiring more time and effort on their part, and often leading to failure [42].

Awareness training should be continuous because people tend to forget 50% of the information they learn in an hour, 70% in a day, and 90% in a week [43]. Although intensive and costly, organizations should not avoid this training against social engineering attacks, as it is one of the only effective ways to protect against them [11]. As Guido Robling notes, "Only two things can help against social engineering: awareness and vigilance" [5].

4.1.2 Creating an effective security policy

Due to the ever-changing dynamics of today's information technology world, managers and employees must be aware of current security policies and procedures [44]. The security policy determines the methods of protecting the sensitive data and assets of the company, institution, and organization. The rules for an effective security policy should be clear,

understandable, reasonable, enforceable, accessible, and available to all users [45]. Policies should also prevent social engineers from gaining access to information about the inner workings of the organization. Unclear and ambiguous security policies can lead to incompatibilities among employees and in such cases, attacks succeed [46].

Kevin Mitnick emphasized the importance of an organized and consistent security policy by saying, " Designed at lowering exposure to semantic attacks, well-maintained policy and organizational procedures help to mitigate and significantly lower the risk of a potential exploit occurring, without relying on the technical capabilities of users" [41]. The security policy will not only protect the organization, but also the employees from possible harm. Therefore, managers have an important role to play in this context and should be aware of any changes in the security policy at an early stage. In addition, they should create flexible and up-to-date policies against unknown and unpredictable attacks and their ever-changing methods. Strong and effective computer access and authorization policies, firewalls, and corporate antivirus can sometimes stop a social engineering attack [6].

4.1.3 Physical security

Almost every security-conscious organization has strong physical security in place. If security measures are lax, attackers will find it easier to launch a digital attack. It is not enough to create clear and effective security policies; tests should also be conducted to determine whether security awareness has been established among employees. Because the attacker can be an outsider or someone inside the organization [41]. If it is an insider, it is difficult to talk about physical security. The reliability of employees authorized to access systems should also be checked, otherwise the likelihood of physical threats will increase. Physical barriers, security lighting, alarms, the installation of motion detectors, lockers, camera systems, and the use of biometrics to identify employees are among the physical measures to protect the organization from potential attacks [41]. Employees should also be informed about physical security during normal hours. For example, there should be reminders throughout the organization that they should not use USB drives or other digital devices that they find without being sure. If adequate physical controls are in place, it may be possible to fend off a serious social engineering attack. However, if strict physical security policies are not implemented, the doors of the company, institution, and organization will always be open to attack [41].

4.1.4 Digital security

Another measure against social engineering attacks is to implement a set of digital protection services and software tools in the organization. While the use of digital security services is effective against some types of social engineering attacks, it is not fully effective against other types of attacks. They are usually implemented to eliminate the risk of attack [41]. For example, a company, institution, or organization that uses antivirus or malware protection and a good firewall is less likely to be phished.

Timely updates, the use of protective software, etc., will not provide complete protection for the organization. Of course, this does not mean that the use of software is unnecessary. In fact, the more measures taken to protect digital data and assets, the better. These measures will provide partial protection. In addition, sandboxing creates an isolated area to protect virtual machines from malware. The use of sandboxing is very effective against some virtual attacks. The popular Google Chrome and Firefox browsers use built-in sandboxing technologies to prevent exploitation through their web browsers [47]. This prevents malicious software from being downloaded without the web user's permission when connecting to a compromised website. It ensures that all downloads are first redirected to a sandbox, from where the item safely lands on the user's computer.

Specialized measures such as proactive monitoring, attacker user authentication, machine learning, and algorithm analysis can provide effective mitigation strategies against social engineering attacks [47]. These structures observe normal system behavior and make distinctions between legal and illegal user actions and packet or data transmission inconsistencies. The resulting detection results are used in machine learning to create a machine learning system. The machine learning system develops a user profile by examining the user's writing style, punctuation, character recognition, word frequency, mailbox contents, email flow, and other parameters. The developed profile is used for each is updated in the email exchange. The resulting algorithm can detect and prevent many social engineering attacks [47]. Digital defences provide the desired results in detecting attacks at the first stage. The important thing is to constantly analyse attack attempts and upgrade the organizational infrastructure accordingly.

4.1.5 Password security policy

A password security policy is established throughout the company, institution, and organization, and everyone, including the management, is expected to comply with this policy. Considering that all kinds of sensitive data in the systems are protected by passwords, attackers will want to capture the target user's passwords to access the data [48]. The acquisition of passwords by unauthorized persons and their misuse and malicious use can cause serious security problems for organizations. Employees should be made aware of password security, they should be prevented from choosing easily guessed passwords, passwords that do not comply with the password security policy should be detected and necessary warnings should be issued. Most of the employees' passwords are easily guessed passwords, such as date of birth [48]. Some of them may write their user passwords on a piece of paper and leave it on the desk, thinking that they are giving complex and difficult passwords and may forget them. Remember that such situations are exploited by social engineers. Employees should prefer separate user passwords for each account or system they access. Passwords should be changed periodically, and security mechanisms should be in place to disable the user account after a certain number of consecutive incorrect passwords are entered. Employees who believe that their passwords have been compromised by unauthorized persons or that unauthorized access has been gained to their user accounts should report this to the appropriate units and security measures should be taken [48].

4.2 Fundamental corporate security measures to be taken against social engineering attacks

Test studies should be conducted by organizations to measure the competence and strength of the organization's personnel against social engineering attacks. However, because the testing studies are labor intensive and require a high level of expertise, only a limited number of such measurements can be performed. In addition, these testing studies are conducted on a small group rather than the entire organization. Studies conducted on small groups may not yield clear results. In addition, it is not possible to conduct these studies in a healthy environment where employees in the testing phase share the information gained during the test with each other [38].

In order to carry out social engineering tests on all the organizations of a company, it is necessary to use some techniques to evaluate the personality profiles of employees [42]. When evaluating the personality profiles of the people working in the organization, their tendency to respond to an attack or challenge the attack in a way that would be useful to a social engineer should be examined. At this point, different personality profile questions should be created within different personality groups (sales, management, research, finance, security, etc.) in order to understand the vulnerabilities. A simple format should be prepared to get quick answers from employees and measure their initial reactions without making them think too much, and employees should be assured that their individual answers will not be shared with their managers [38].

In the social engineering defence model, the vast majority of system enhancements provide a strong defence against social engineering. However, in many cases, these systems can be successfully exploited by a hacker to successfully trick and convince a user to allow an attack that results in a system breach. Therefore, personnel awareness activities provide a much stronger and more consistent layer of defence.

Figure 15 shows that staff awareness is the first response and the most important layer of defence. In a social engineering attack, this layer may be the first to be breached. Therefore, relying solely on systemic defences in a strategic sense is risky. Depending on the awareness of the personnel, the information and systems within the organization will be vulnerable to the degree of the nature of the attacks on the human element [42]. Therefore, to create an effective defence, it is necessary to combine the personnel awareness layer with systemic protection layers. The diagram assumes that the layers are impenetrable.

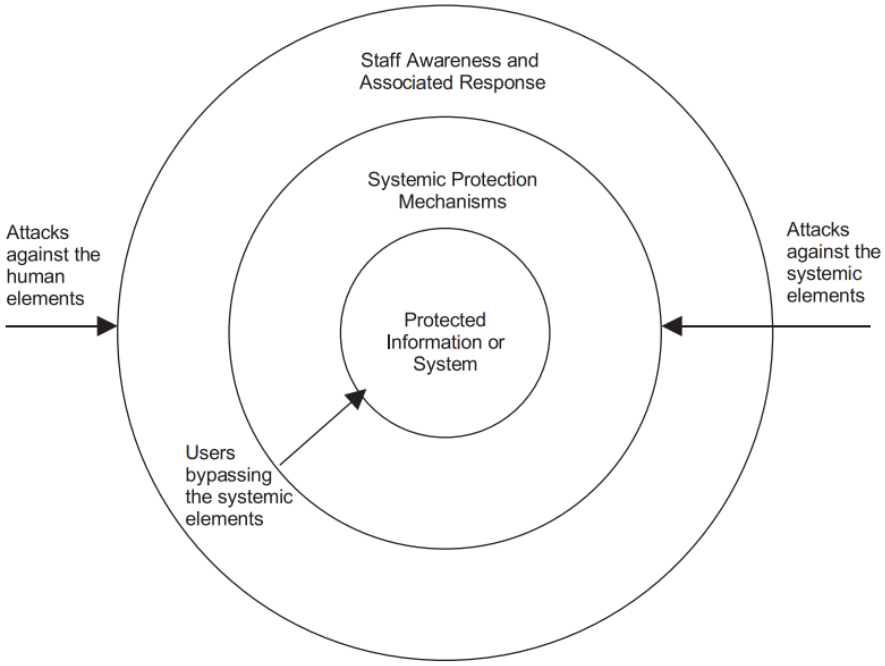


Figure 15: Social engineering protection model [42].

4.2.1 Reinforcing information security awareness in organizations

The human factor is the weakest link in information security. Users make their organizations vulnerable to threats through their conscious or unconscious use of information networks. Security programs tend to focus on technical controls rather than the human factor. While human-related security risk can never be eliminated, it can be reduced to a manageable level. It is critical for management to ensure that users understand their responsibilities in protecting information and information resources. The following steps should be followed to develop an effective information security awareness program against social engineering attacks [42].

- The organization's information security policy should be written clearly and concisely and reflect the organization's information security priorities.
- The second step in developing a successful information security program is to determine the current training needs of the organization's personnel.
- Once the security needs have been identified, the next step is to gain the support of senior management and those with authority within the organization.

- The subsequent step is to identify the target audience. Not everyone in the organization needs the same level of security awareness to do their jobs. Therefore, all users should be grouped. This grouping should be based on the user's level of awareness, level of technical knowledge, title, level of authority, and job function.
- High-level key messages should be developed for each group.
- The next step after the awareness program is to determine the communication tools available. These tools should include public or private e-mail, voice mail, system login messages, posters or brochures, face-to-face training, meetings, presentations, training and safety seminars, and reminder materials (pencils, erasers, key chains, notepads, etc.).
- The penultimate step in a successful awareness campaign is to develop a strategic framework for consistent and effective message delivery. Tactics in this framework should include information at the time of hiring, monthly company newsletters, company luncheons and training sessions, annual safety seminars, incentive awards for safety achievements, games and contests.
- Measuring awareness is the final step. At this stage, future progress and regression can be measured. Measurement should be based on qualitative criteria.

4.2.2 Fundamental corporate security measures against social engineering attacks

The main organizational security measures that can be taken against social engineering attacks are listed below [38].

- Discarded documents and all documents should be run through scissors or torn in such a way that they cannot be read.
- Personal passwords should never be shared with anyone and should not be posted in visible places.
- A clean desk/clean screen policy should be implemented.
- Procedures should be in place for personnel leaving the organization, and passwords to systems used by these individuals should be deactivated immediately.

- Individuals entering the organization as visitors should be issued with a badge and if necessary, should be accompanied by someone from the organization.
- It should be remembered that even the closest of friends can sometimes be tricked into using social engineering techniques.
- It should be known that using more than one email for information security may be more effective in some cases.
- When entering passwords via keyboard-type input devices, be aware of shoulder surfing, which allows others to spy on you unnoticed.
- Security cameras that operate 24 hours a day should be placed in sensitive areas of the organization.
- Employees should be reminded that someone can access any personal information and postings they share on the Internet and should be encouraged to act in a controlled manner. Care should be taken not to share particularly sensitive personal information (social security number, phone number, place of birth, date of birth, etc.) anywhere, especially on social media (Instagram, Facebook, Twitter, etc.).
- When phishing emails with social engineering methods are examined in detail, general and unclear expressions are used. Spelling rules are used awkwardly. Unnecessary and irrelevant promises are made, and expressions are used to panic the person that the event is very urgent. Attempts are made to create panic in the person to comply with the given instructions immediately. You should be aware of such psychological email attacks. It is also necessary to be wary of emails that try to direct the person to links that he/she did not know before.
- Information security tests, including social engineering attack tests, should be performed periodically.

In today's digital landscape, organizations face numerous risks and threats to their computer systems and data. While measures can be taken to reduce these risks, it is not possible to eliminate them entirely. Thus, no organization should assume that their systems are 100% secure. To best protect against these risks and attacks, it is essential to maintain constant vigilance and stay up to date with the latest security policies. Implementing corporate information security standards is also a crucial factor in ensuring high-level protection [23].

To aid institutions in this process, the International Organization for Standardization (ISO) has established standards for best practices at every stage of the information production and usage process. ISO 27001, in particular, serves as a documented Information Security Management System (ISMS) standard. Many companies allocate significant resources to certifying these standards due to financial reasons, such as building a positive corporate image, maintaining reputation, and gaining a competitive advantage[49].

Social engineering remains a prevalent tactic for attackers to gather internal and external sources of information. This technique includes methods such as vishing, phishing, dumpster diving, and physical access. When evaluating internal security tests, the risk ranking level of social engineering tests is considered medium. In many cases, the weakest link in an organization's information security is its people. Thus, it is crucial to employ security testing using social engineering techniques to determine any weaknesses in security awareness. With the advancement of technological measures, software and hardware vulnerabilities have been reduced in the information security of organizations. However, this has forced attackers to exploit human vulnerabilities to gain unauthorized access. Therefore, users at all levels must be knowledgeable about social engineering techniques to prevent threats to corporate information security[6].

5 Practical Part

5.1 Purpose and scope of the practical part

The objective of this practical part of the thesis is to gain a better understanding of the prevalence and impact of social engineering attacks, as well as the awareness and behaviours of individuals in protecting themselves against these attacks.

To achieve this objective, a survey was conducted to gather data on the experiences and perceptions of individuals regarding social engineering. The survey consisted of a set of yes/no questions and was distributed to a sample of individuals who were selected to represent a diverse range of ages, occupations, and levels of technology literacy. The results of this survey provide valuable insights into the current state of social engineering and can inform the development of effective strategies for defending against these types of attacks.

5.2 Design and implementation of the survey

The purpose of this study was to assess the level of knowledge and awareness of cybersecurity and social engineering among participants in the education sector. To accomplish this goal, a survey was designed and sent to 100 participants, including students, faculty, and staff from various educational institutions. In order to insure the anonymity of the participants, the survey was conducted as anonymous and did not require any personal information. The anonymity of the survey was emphasized to encourage participants to provide honest and accurate responses to the questions.

The survey was created through Google Forms and was composed of multiple-choice and yes/no questions. The questions aimed to collect information about participants' experience with cybersecurity and social engineering, their understanding of these topics, and their attitudes towards these issues.

The survey was divided into four sections. The first part gathered demographic information, including age, gender, educational background, and employment status. The second part

focused on participants' exposure to cybersecurity and social engineering, such as previous experiences with online threats and the measures taken to prevent these threats. The third section aimed to measure participants' knowledge of cybersecurity and social engineering, with questions intended to evaluate their grasp of fundamental security concepts and their ability to recognize phishing emails and other social engineering techniques. The final section examined participants' attitudes towards cybersecurity and social engineering, including their perception of the importance of these issues and their willingness to adopt best practices to protect themselves online.

The survey was distributed using email and social media platforms, and participants were given a two-week window to complete it. Data collected from the survey was analysed using IBM SPSS version 28. The data was summarized using descriptive statistics such as frequency, percentage, mean, and standard deviation. To further explore the demographic data, graphical representations such as pie charts, histogram and cross tables will be utilized. These visual aids can help to highlight any significant differences or patterns among the participants' characteristics, making it easier to interpret and communicate the data effectively.

The survey questions can be found in the Appendix section of this thesis.

5.3 Survey evaluation

In the survey evaluation section, firstly the demographic data collected from the participants will be presented and analysed. This section aims to provide a comprehensive overview of the participants' characteristics and to identify any patterns or trends that may be relevant to the study. Secondly, the primary 30 survey questions that were designed to assess participants' knowledge and awareness of cybersecurity and social engineering will be presented and analysed.

5.3.1 Demographic analysis

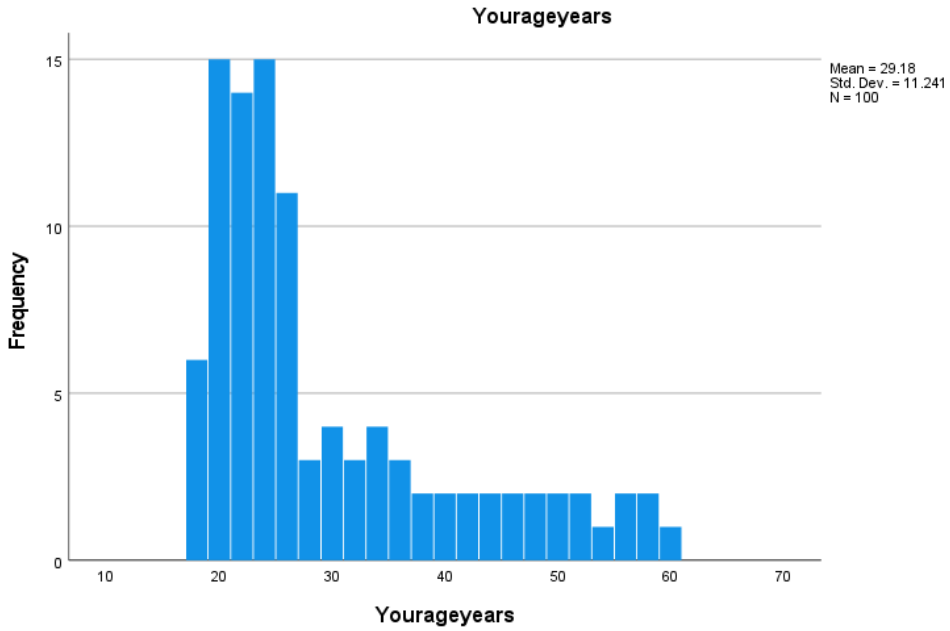
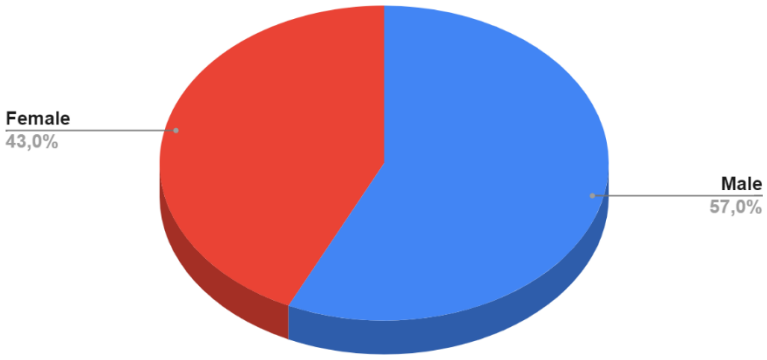


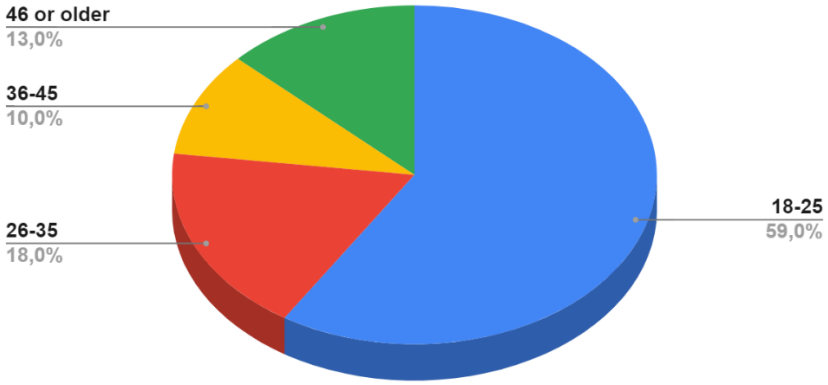
Table 3: The Age Distribution of Survey Participants analyzed by using a histogram (own source).

The table displays a histogram of the age distribution of the survey participants. The horizontal axis shows the age range, with intervals of two years, and the vertical axis shows the number of participants. The histogram is left-skewed, indicating that most of the participants are younger, with fewer participants in the older age ranges. The peak of the distribution occurs in the 20-26 age range, with a steep decline in the number of participants in the older age ranges. The average age of the participants is 29 years, with a standard deviation of 11.2 years.



Graph 1: The gender distribution of the survey participants (own source).

As it can be observed from Graph 1, the demographic data collected from the 100 participants revealed that the sample was diverse in terms of age, gender, educational background, and employment status. In total, 57 of the participants were male and 43 were female, indicating that the majority of the participants were male.



Graph 2: The age distribution of the survey participants (own source).

Graph 2 demonstrates that the gender category ranged from 18 years old to 60 years old, with a mean age of 32 years for Females and 27 for males. Also, the minimum age for females is 18 and the maximum age is 60, but for males, the minimum age is 18 and the maximum age is 55. This suggests that, on average, female participants were older than male participants.

Descriptives

	Yourgender			Statistic	Std. Error
Age	Female	Mean		32.12	1.863
		95% Confidence Interval for Mean	Lower Bound	28.36	
			Upper Bound	35.88	
		5% Trimmed Mean		31.41	
		Median		30.00	
		Variance		149.248	
		Std. Deviation		12.217	
		Minimum		18	
		Maximum		60	
		Range		42	
		Interquartile Range		16	
		Skewness		.933	.361
		Kurtosis		-.224	.709
	Male	Mean		26.96	1.324
		95% Confidence Interval for Mean	Lower Bound	24.31	
			Upper Bound	29.62	
		5% Trimmed Mean		26.03	
		Median		24.00	
		Variance		99.856	
		Std. Deviation		9.993	
		Minimum		18	
		Maximum		55	
		Range		37	
		Interquartile Range		9	
		Skewness		1.524	.316
		Kurtosis		1.233	.623

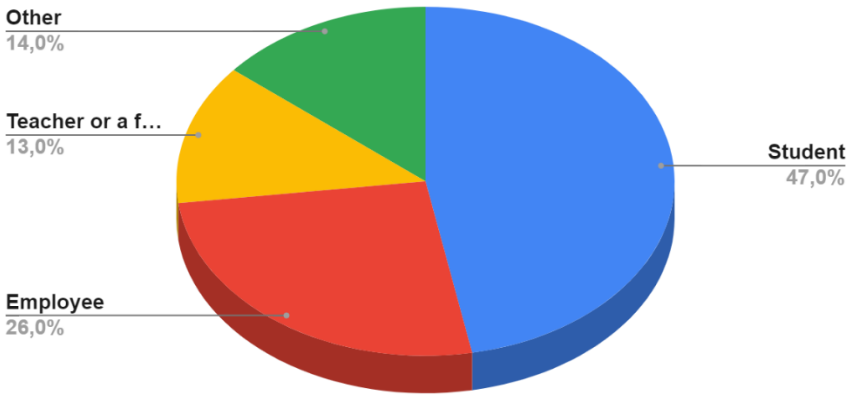
Table 4: The age-related descriptive comparison between female and male survey participants (own source).

The age-related descriptive comparison between female and male survey participants is presented in Table 4. The median age for female participants was 30, which was higher than the median age for male participants, which was 24. This implies that the age distribution for female participants was skewed to the right, with more participants in the higher age range than the lower age range, while the age distribution for male participants was skewed to the left, with more participants in the lower age range than the higher age range.

The variance of age for female participants was 149.248, which was higher than the variance of age for male participants, which was 99.856. This indicates that the age range for female

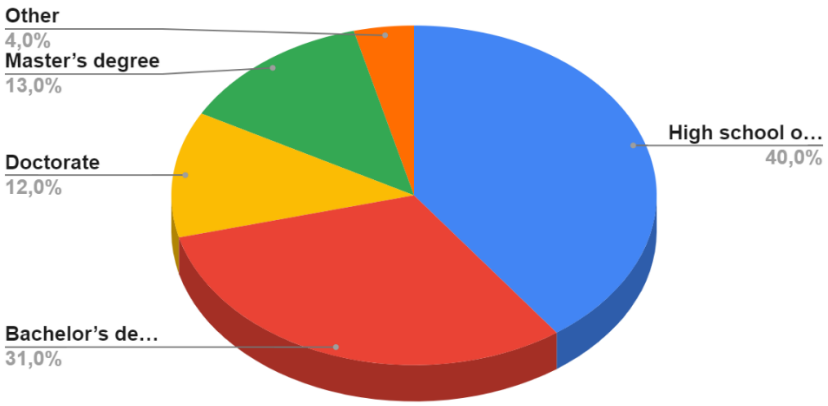
participants was wider than that of male participants. The standard deviation for female participants was 12.217, which was also higher than the standard deviation for male participants, which was 9. 993.

Overall, the age-related descriptive comparison between female and male survey participants revealed that female participants were older on average, had a wider age range and more spread-out age distribution, and a larger interquartile range than male participants. These findings provide important insights into the age demographics of the survey participants.



Graph 3: The occupations of the survey participants (own source).

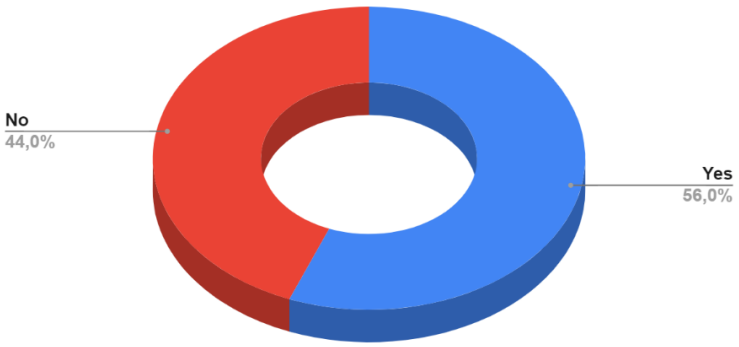
As it is illustrated Graph 3 among the participants, the results indicate that the majority of the participants were students, accounting for 47% of the total sample. This is not surprising considering that the survey was conducted among the students. Employed individuals represented the second largest group in the sample, comprising 26% of the total participants. Meanwhile, teachers or faculty members accounted for 13% of the participants, indicating that the study included a small proportion of academic professionals.



Graph 4: The highest level of education achieved by the survey participants (own source).

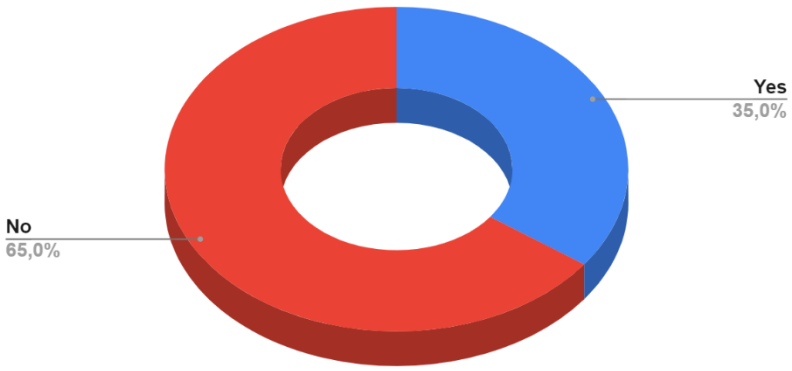
The results of the participant's highest level of education completed which can be observed in Graph 4 show that the majority of participants, 40%, had completed high school or equivalent. Meanwhile, 31% participants had obtained a Bachelor's degree, 13% had completed a Master's degree, and 12% had earned a Doctorate. The remaining 4% participants had completed other educational qualifications. These findings suggest a diverse range of educational backgrounds among the participants, which may be an important factor in understanding their level of knowledge and awareness of cybersecurity and social engineering. Further analysis will be conducted to examine the potential relationship between participants' level of education and their understanding of these issues.

5.3.2 Social engineering exposure analysis



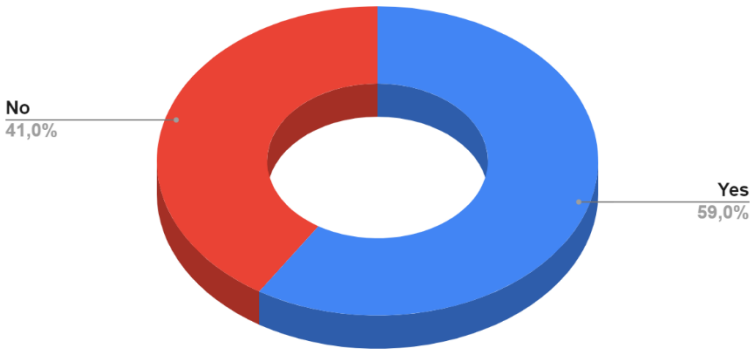
Graph 5: The answers for the question: "Have you ever clicked on a link in an e-mail or on the internet that led you to the download of potentially harmful files?" (own source).

As it is demonstrated in Graph 5, out of the 100 participants, 56% reported that they had clicked on a link in an email or on the internet that led them to download potentially harmful files, while 44% stated that they had not. This question aimed to measure participants' experience and behavior related to social engineering attacks through email or the internet. The result indicates that a significant number of individuals have been exposed to potentially harmful files through this common social engineering tactic. This finding emphasizes the need for increased awareness and education on the risks associated with clicking on unknown or suspicious links in emails or on the internet.



Graph 6: The answers for the question: “Have you ever received a phone call from someone claiming to be from technical support and asking for access to your computer?” (own source).

This survey question was used to assess the participants' exposure to a specific type of social engineering attack. The results indicated that 35% of participants reported having received such a call, while the majority (65%) had not. These findings suggest that a significant proportion of individuals may be vulnerable to this particular form of social engineering, which involves exploiting individuals' trust in technical support personnel to gain unauthorized access to their devices. This highlights the importance of awareness and education efforts aimed at helping individuals recognize and respond to social engineering attacks.



Graph 7: The answers for the question: “Have you ever received a message from a social media account claiming to be from a friend or relative and asking for personal information?” (own source).

As part of the "Social Engineering Exposure Analysis" section of this thesis, participants were asked to respond to a survey question regarding the frequency of their exposure to a specific type of social engineering attack. The results of the survey showed that 59% of the participants had received such messages, while 41% had not. This highlights the potential vulnerability of individuals to social engineering attacks through social media platforms. Social media platforms provide a wealth of personal information that can be used by attackers to craft convincing messages that appear to be from a friend or relative. The fact that most of the participants had received such messages indicates the prevalence of this type of attack and the need for increased awareness and education to protect against them.

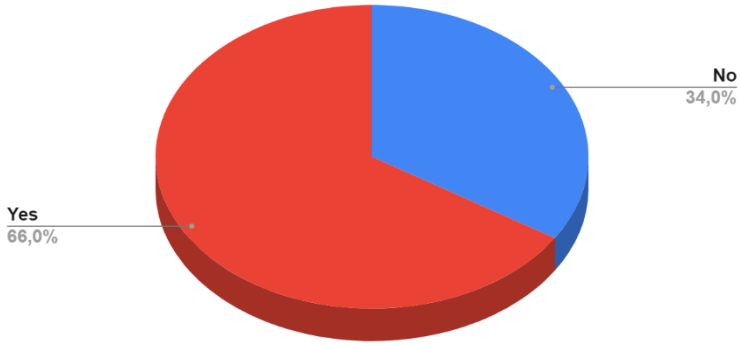
5.3.3 Social engineering knowledge analysis

do_you_believe_sc_is_threat

Occupation			Frequency	Percent	Valid Percent	Cumulative Percent
Employee	Valid	I am not sure	8	30.8	30.8	30.8
		No	5	19.2	19.2	50.0
		Yes	13	50.0	50.0	100.0
		Total	26	100.0	100.0	
Other	Valid	I am not sure	4	28.6	28.6	28.6
		No	2	14.3	14.3	42.9
		Yes	8	57.1	57.1	100.0
		Total	14	100.0	100.0	
Student	Valid	I am not sure	22	46.8	46.8	46.8
		No	5	10.6	10.6	57.4
		Yes	20	42.6	42.6	100.0
		Total	47	100.0	100.0	
Teacher or a faculty member	Valid	I am not sure	2	15.4	15.4	15.4
		Yes	11	84.6	84.6	100.0
		Total	13	100.0	100.0	

Table 5: The statistical analysis of the answers for the survey question: “Do you believe that social engineering is a serious threat to individuals and organizations?” (own source).

This survey question was aimed at determining the participants’ perception of the level of danger posed by social engineering attacks. The results showed that the majority of respondents recognized social engineering as a significant threat, with 52% of the total participants responding affirmatively, 36% being unsure, and 12% stating that it is not a serious threat. Specifically, among the subgroups, teachers or faculty members demonstrated the highest level of awareness, with 84.6% of them recognizing the danger of social engineering attacks. The “other” occupation showed a slightly lower level of concern, with 57.1% acknowledging the severity of the threat, while students had the lowest level of awareness as 42.6% , with all participants acknowledging social engineering as a serious threat. These findings indicate that there is still a need to raise awareness and educate individuals in all groups about the potential risks associated with social engineering attacks.



Graph 8: The answers for the question: “Are you aware of the potential risks associated with social engineering attacks?” (own source).

The result of the survey question shows that only 66% of the participants are aware of the potential risks associated with social engineering attacks, while 34% are not aware. This indicates a significant gap in knowledge and awareness about the risks of social engineering attacks among the participants.

It is important to remember that social engineering attacks are becoming increasingly sophisticated and prevalent in today's digital age, and individuals and organizations are at high risk of falling victim to such attacks. Therefore, it is crucial that individuals are aware of the potential risks associated with social engineering attacks and take necessary measures to protect themselves and their organizations from such attacks. The result of this survey highlights the need for educational programs and awareness campaigns to be implemented to improve people's knowledge and understanding of social engineering attacks and their associated risks.

what_is_most_common_typeof_attack

Occupation			Frequency	Percent	Valid Percent	Cumulative Percent
Employee	Valid	Baiting	5	19.2	19.2	19.2
		I do not know	8	30.8	30.8	50.0
		Phishing	10	38.5	38.5	88.5
		Scareware	2	7.7	7.7	96.2
		Social networking sites	1	3.8	3.8	100.0
		Total	26	100.0	100.0	
Other	Valid	I do not know	5	35.7	35.7	35.7
		Phishing	4	28.6	28.6	64.3
		Scareware	1	7.1	7.1	71.4
		Social networking sites	4	28.6	28.6	100.0
		Total	14	100.0	100.0	
Student	Valid	Baiting	6	12.8	12.8	12.8
		I do not know	14	29.8	29.8	42.6
		Phishing	15	31.9	31.9	74.5
		Scareware	2	4.3	4.3	78.7
		Social networking sites	10	21.3	21.3	100.0
		Total	47	100.0	100.0	
Teacher or a faculty member	Valid	Baiting	3	23.1	23.1	23.1
		I do not know	3	23.1	23.1	46.2
		Phishing	5	38.5	38.5	84.6
		Scareware	1	7.7	7.7	92.3
		Social networking sites	1	7.7	7.7	100.0
		Total	13	100.0	100.0	

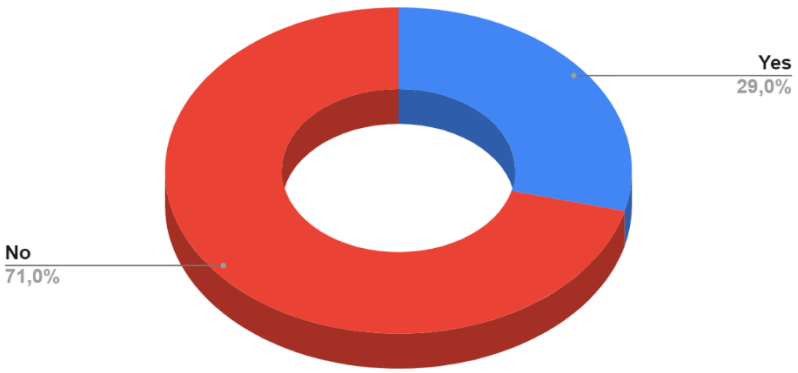
Table 6: The statistical analysis of the answers for the survey question: “What is the most common type of attack” according to various occupations (own source).

The survey question, “What is the most common type of attack?”, was administered to participants of different occupational backgrounds. The results of the survey indicate that phishing is the most commonly recognized type of social engineering attack, with a total of 34 out of 100 participants selecting this option. Social networking sites were the second most recognized type of attack, with a total of 16 participants selecting this option. Scareware, Baiting, and "I do not know" responses were selected by 6, 14, and 30 participants, respectively.

When analyzing the responses by occupation, It was found that phishing was the most commonly recognized type of attack across all groups, with the exception of the other group where "I do not know" option was slightly more recognized. In the employee group, 38.5% recognized phishing as the most common type of attack, while 19.2% recognized baiting.

Similarly, in the teacher/faculty member group, 38.5% recognized phishing as the most common type of attack, while 23.1% recognized baiting. In the student group, phishing was also the most recognized type of attack, with 31.9% of participants selecting this option.
These results indicate a significant lack of knowledge among the surveyed population regarding social engineering attacks. It is also noteworthy that 66% of the participants did not answer this question correctly, indicating a significant knowledge disparity among the surveyed population with regards to social engineering attacks. The high proportion of "I do not know" responses across all groups highlights the need for increased education and training on the topic of social engineering.

5.3.4 Attitudes towards social engineering analysis

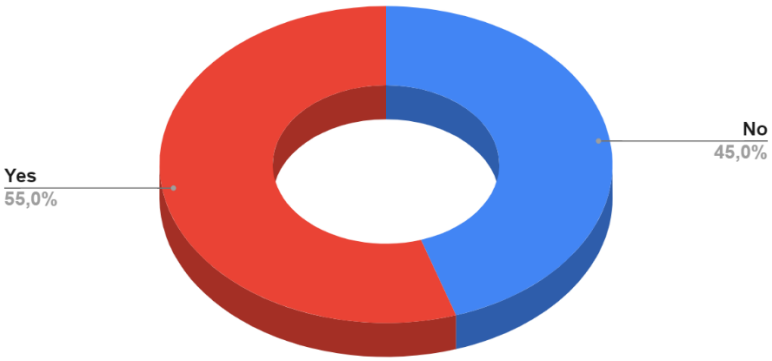


Graph 9: The answers for the question: “Have you received any training or education on how to identify and protect against social engineering attacks?” (own source).

In the context of social engineering attacks, training and education are important factors that can help individuals identify and protect against such attacks. Therefore, it is essential to investigate whether the surveyed population has received any training or education on this topic.

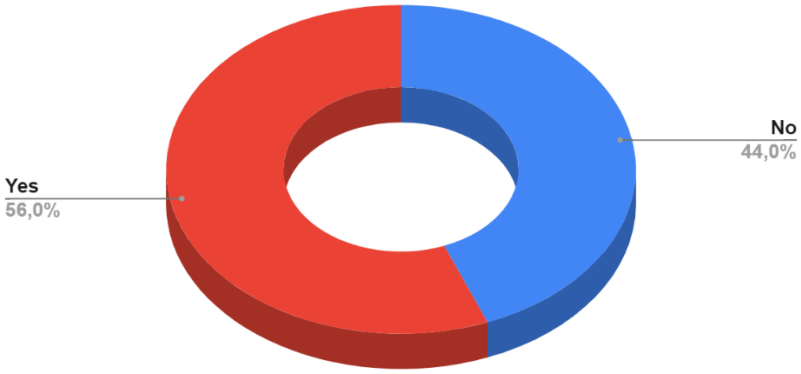
The results of the survey indicate that a large majority of the participants, 71%, have not received any training or education on how to identify and protect against social engineering attacks. The results of the survey reveal a notable lack of knowledge and awareness among participants when it comes to social engineering attacks. On the other hand, 29% of the participants reported having received some form of training or education on this topic. While

this is a positive indication, it is still a relatively small proportion of the surveyed population. Therefore, there is a need to increase the efforts towards educating individuals and raising awareness about social engineering attacks.



Graph 10: The answers for the question: “Do you take measures to protect yourself from falling victim to a social engineering attack?” (own source).

One of the key objectives of the present study was to examine the attitudes of the surveyed population towards social engineering attacks. To this end, participants were asked whether they take measures to protect themselves from falling victim to such attacks. The results of the survey reveal that 55% of the participants reported taking measures to protect themselves, while 45% did not. This indicates a positive trend in terms of self-protection measures against social engineering attacks, although nearly half of the participants reported not taking any measures. This is a concerning finding, as social engineering attacks can have severe consequences, such as financial losses or identity theft.



Graph 11: The answers for the question: “Do you want to take courses in social engineering?” (own source).

The survey question "Do you want to take courses in social engineering?" yielded a response of 56% "yes" and 44% "no" among the surveyed population. This finding suggests a moderate level of interest in social engineering courses. The results indicate that more than half of the participants are interested in gaining knowledge and skills in this area, which can be a positive step towards increasing awareness and protection against social engineering attacks. However, it is also worth noting that a significant proportion of participants, nearly half, expressed no interest in taking courses on social engineering. Further research is needed to understand the reasons behind this lack of interest and to develop effective strategies for promoting social engineering education and training.

5.4 Hypothesis

The present study aimed to investigate the awareness and education levels of males and females regarding social engineering attacks. Two questions were posed to each group to elicit their level of knowledge and experience: "Are you aware of the concept of social engineering?" and "Are you aware of the potential risks associated with social engineering attacks?" The study also sought to determine if the participants had received any training or education on how to identify and protect against social engineering attacks. The Chi-Square Test was used to test the hypotheses related to the differences in awareness and education levels between males and females.

Chi-Square Tests was used to statistically analyse the data since these are easy to use and interpret. Moreover, the use of Chi-Square Tests allows to test multiple hypotheses in a

single analysis, making the research process more efficient. Specifically, the study investigated three different hypotheses related to social engineering attacks, and the Chi-Square Test was used to test each hypothesis.

The null hypothesis (H0) for the first hypothesis was "There is no significant difference in the level of awareness of social engineering concepts between males and females," with the alternative hypothesis (HA) being "There is a significant difference in the level of awareness of social engineering concepts between males and females." The chi-square test result was 3.826 with a p-value of .148. Consequently, since the p-value (.148) is greater than the significance level (set at 0.05), the null hypothesis could not be rejected, indicating that there is no significant difference in the level of awareness of social engineering concepts between males and females.

Crosstabulation

			Awareness_Concept_SocialEngineering			
			No	Partially	Yes	Total
Gender	Female	Count	11	21	11	43
		% within Gender	25.6%	48.8%	25.6%	100.0%
	Male	Count	13	19	25	57
		% within Gender	22.8%	33.3%	43.9%	100.0%
Total		Count	24	40	36	100
		% within Gender	24.0%	40.0%	36.0%	100.0%

Table 7: Crosstabulation of the null hypothesis (H0): “There is no significant difference in the level of awareness of social engineering concepts between males and females” (own source).

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	3.826[a]	2	.148
Likelihood Ratio	3.891	2	.143
Linear-by-Linear Association	1.836	1	.175
N of Valid Cases	100		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 10.32.

Table 8: Pearson Chi-Square Test results (own source).

The second hypothesis tested whether there was a significant difference in the level of awareness of potential risks associated with social engineering attacks between males and

females. The null hypothesis (H0) was "There is no significant difference in the level of awareness of potential risks associated with social engineering attacks between males and females," while the alternative hypothesis (HA) was "There is a significant difference in the level of awareness of potential risks associated with social engineering attacks between males and females." The chi-square test result was 3.488 with a p-value of .062, since the p-value (.062) is greater than the significance level (set at 0.05) indicating that there is no significant difference in the level of awareness of potential risks associated with social engineering attacks between males and females.

Crosstabulation

			are_you_aware_potential_risk_sc		
			No	Yes	Total
Gender	Female	Count	19	24	43
		% within Gender	44.2%	55.8%	100.0%
	Male	Count	15	42	57
		% within Gender	26.3%	73.7%	100.0%
Total		Count	34	66	100
		% within Gender	34.0%	66.0%	100.0%

Table 9: Crosstabulation of the null hypothesis (H0): "There is no significant difference in the level of awareness of potential risks associated with social engineering attacks between males and females" (own source).

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	3.488[a]	1	.062		
Continuity Correction[b]	2.737	1	.098		
Likelihood Ratio	3.477	1	.062		
Fisher's Exact Test				.088	.049
Linear-by-Linear Association	3.453	1	.063		
N of Valid Cases	100				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 14.62.

b. Computed only for a 2x2 table

Table 10: Pearson Chi-Square Test results (own source).

The third hypothesis tested whether there was a significant difference in the level of education and training on how to identify and protect against social engineering attacks between males and females. The null hypothesis (H0) was "There is no significant difference

in the level of education and training on how to identify and protect against social engineering attacks between males and females," while the alternative hypothesis (HA) was "There is a significant difference in the level of education and training on how to identify and protect against social engineering attacks between males and females." The chi-square test result was 8.295 with a p-value of .004. Therefore, the null hypothesis was rejected, suggesting that there is a significant difference in the level of education and training on how to identify and protect against social engineering attacks between males and females. Females were less likely to have received training or education on how to identify and protect against social engineering attacks compared to males.

Crosstabulation

			Received_training_on_preventing_social_engineering_attacks		
			No	Yes	Total
Gender	Female	Count	37	6	43
		% within Gender	86.0%	14.0%	100.0%
	Male	Count	34	23	57
		% within Gender	59.6%	40.4%	100.0%
Total		Count	71	29	100
		% within Gender	71.0%	29.0%	100.0%

Table 11: Crosstabulation of the null hypothesis (H0): "There is a significant difference in the level of education and training on how to identify and protect against social engineering attacks between males and females" (own source).

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	8.295[a]	1	.004		
Continuity Correction[b]	7.062	1	.008		
Likelihood Ratio	8.794	1	.003		
Fisher's Exact Test				.004	.003
Linear-by-Linear Association	8.212	1	.004		
N of Valid Cases	100				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 12.47.

b. Computed only for a 2x2 table

Table 12: Pearson Chi-Square Test results (own source).

In conclusion, the study found that there is no significant difference in the level of awareness of social engineering concepts and potential risks associated with social engineering attacks between males and females. However, there is a significant difference in the level of education and training on how to identify and protect against social engineering attacks between males and females, with males being more educated and trained on this topic. These findings highlights the need for organizations to provide gender-inclusive training on preventing social engineering attacks to increase awareness and reduce the risk of successful attacks.

6 Conclusion

After an extensive review of the current state of the art of social engineering attacks, this thesis aimed to evaluate the level of social engineering awareness among individuals and the effectiveness of existing countermeasures. The practical part of the study involved a survey conducted among 100 participants, which evaluated demographic data, social engineering exposure, knowledge, and attitudes towards social engineering.

The results of the survey revealed that there was no statistically significant difference in the level of social engineering knowledge between males and females. However, there was a significant difference in the level of education and training on how to identify and protect against social engineering attacks, with males being more educated and trained on this topic. The study's findings suggest that there is a need for educators and policymakers to develop gender-inclusive cybersecurity education programs that target both males and females equally.

The survey also indicated that the majority of participants had experienced some form of social engineering attack, highlighting the importance of awareness and education. The research also showed that traditional security measures, such as strong passwords, may not be sufficient to protect against social engineering attacks.

The study also explored the effectiveness of different countermeasures against social engineering attacks, including cybersecurity awareness and training, effective security policies, physical security, digital security, and password security policies. The findings suggested that spreading information security awareness in organizations and implementing fundamental corporate security measures were essential in protecting against social engineering attacks.

The research contributes to the existing literature on social engineering attacks by evaluating the effectiveness of different countermeasures against social engineering attacks and highlighting the need for increased awareness and education. The findings suggest that a combination of traditional security measures and effective education programs can significantly reduce the likelihood of social engineering attacks.

Overall, this study emphasizes the importance of addressing social engineering attacks and implementing effective countermeasures to protect against them. By highlighting the need for increased awareness and education, policymakers and educators can develop strategies to help individuals and organizations protect themselves against social engineering attacks.

It is important to acknowledge the limitations of this study. One limitation is the sample size, which may not be representative of the entire population. The study only focused on participants from a single geographic region, which may not generalize to other populations. Additionally, the study relied on self-reported data, which may be subject to bias and may not accurately reflect the participants' actual knowledge and behaviour regarding social engineering attacks. Future research could address these limitations by utilizing larger and more diverse samples, using objective measures of knowledge and behaviour, and considering additional factors that may impact awareness and education levels regarding social engineering attacks.

In conclusion, this study provides valuable insights into the prevalence of social engineering attacks and the effectiveness of existing countermeasures. The results suggest that education and awareness are essential components in protecting against social engineering attacks, and policymakers and educators must work together to develop effective strategies to combat these types of attacks.

7 References

[1] R. Heifetz and M. Linsky, “A Survival Guide for Leaders,” *Harvard Business Review*, Jun. 01, 2002. Accessed: Jan. 29, 2023. [Online]. Available: https://hbr.org/2002/06/a-survival-guide-for-leaders

[2] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim, “Social Engineering Attacks Prevention: A Systematic Literature Review,” *IEEE Access*, vol. 10, pp. 39325–39343, 2022, doi: 10.1109/ACCESS.2022.3162594.

[3] Mitnick, K. D., & Simon, W. L., “The art of deception: Controlling the human element of security,” *John Wiley Sons*, 2002, doi: 10.1002/9780471437114.

[4] Fink, J. L., “The human factor in cybersecurity: six key takeaways,” *Harv. Kennedy Sch. Belfer Cent. Sci. Int. Aff.*, 2018, [Online]. Available: https://www.belfercenter.org/sites/default/files/legacy/files/Human-Factor-Cybersecurity.pdf

[5] C. Hadnagy, *Social Engineering: The Art of Human Hacking*. John Wiley & Sons, 2010.

[6] Mishra, P., & Singh, A. K, “An Empirical Study of Social Engineering Attacks and Countermeasures in Information Security,” *J. Inf. Syst. Technol. Manag.*, p. 18, 2021.

[7] Kaspersky, “The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within.” https://www.kaspersky.com/blog/the-human-factor-in-it-security/ (accessed Feb. 15, 2023).

[8] “State of Cybersecurity 2022,” *ISACA*. https://www.isaca.org/go/state-of-cybersecurity-2022 (accessed Feb. 18, 2023).

[9] F. Salahdine and N. Kaabouch, “Social Engineering Attacks: A Survey,” *Future Internet*, vol. 11, no. 4, Art. no. 4, Apr. 2019, doi: 10.3390/fi11040089.

[10] J.-W. H. Bullée, L. Montoya, W. Pieters, M. Junger, and P. Hartel, “On the anatomy of social engineering attacks—A literature-based dissection of successful attacks,” *J. Investig. Psychol. Offender Profiling*, vol. 15, no. 1, pp. 20–45, 2018, doi: 10.1002/jip.1482.

[11] “Cost of a data breach 2022,” Nov. 07, 2022. https://www.ibm.com/reports/data-breach (accessed Jan. 29, 2023).

[12] “Federal Bureau of Investigation. (2022). Internet Crime Complaint Center report (IC3).” Accessed: Feb. 18, 2023. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[13] M. Hijji and G. Alam, “A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/ Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions,” *IEEE Access*, vol. PP, pp. 1–1, Jan. 2021, doi: 10.1109/ACCESS.2020.3048839.

[14] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks,” *J. Inf. Secur. Appl.*, vol. 22, pp. 113–122, Jun. 2015, doi: 10.1016/j.jisa.2014.09.005.

[15] Sasse, M. A., Brostoff, S., & Weirich, D., “Transforming the weakest link: A human/computer interaction approach to usable and effective security.,” *BT Technol. J.*, vol. 19, no. 2, pp. 122–131, 2001, doi: 10.1023/A:1011219017279.

[16] National Institute of Standards and Technology (NIST), *NIST Cybersecurity Framework*. U.S. Department of Commerce, 2021.

[17] H. Kayan, M. Nunes, O. Rana, P. Burnap, and C. Perera, “Cybersecurity of Industrial Cyber-Physical Systems: A Review,” *ACM Comput. Surv.*, vol. 54, no. 11s, pp. 1–35, Jan. 2022, doi: 10.1145/3510410.

[18] Z. Wang, L. Sun, and H. Zhu, "Defining Social Engineering in Cybersecurity," *IEEE Access*, vol. 8, pp. 85094–85115, May 2020, doi: 10.1109/ACCESS.2020.2992807.
[19] N. Yathiraju, G. Jakka, S. K. Parisa, and O. Oni, "Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security: A Survey of Social Engineering Attacks and Steps for Mitigation of These Attacks," *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security*, 2022. https://www.igi-global.com/chapter/cybersecurity-capabilities-in-developing-nations-and-its-impact-on-global-security/www.igi-global.com/chapter/cybersecurity-capabilities-in-developing-nations-and-its-impact-on-global-security/296835 (accessed Feb. 18, 2023).
[20] F. Mouton, M. Malan, L. Leenen, and H. s Venter, "Social Engineering Attack Framework," presented at the Information Security for South Africa, Aug. 2014. doi: 10.1109/ISSA.2014.6950510.
[21] N. Duarte, N. Coelho, and T. Guarda, "Social Engineering: The Art of Attacks," in *Advanced Research in Technologies, Information, Innovation and Sustainability*, Cham, 2021, pp. 474–483. doi: 10.1007/978-3-030-90241-4_36.
[22] H. Chizari, A. Zulkurnain, A. Hamidy, and A. Husain, "Social Engineering Attack Mitigation," *Int. J. Math. Comput. Sci.*, vol. 1, pp. 188–198, Jan. 2015.
[23] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Social engineering attacks on the knowledge worker," in *Proceedings of the 6th International Conference on Security of Information and Networks*, New York, NY, USA, November 2013, pp. 28–35. doi: 10.1145/2523514.2523596.
[24] J. Long, *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Syngress, 2011.
[25] G. Watson, A. Mason, and R. Ackroyd, *Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense*. Syngress, 2014.
[26] L. Ball, G. Ewan, and N. Coull, "Undermining: 4th International Conference on Knowledge Discovery and Information Retrieval," *Proc. Int. Conf. Knowl. Discov. Inf. Retr.*, vol. 1: KDIR, pp. 275–280, 2012, doi: 10.5220/0004168802750280.
[27] "(25) The Art of Social Engineering Part 1 | LinkedIn." https://www.linkedin.com/pulse/art-social-engineering-part-1-marat-kovalyov/ (accessed Feb. 18, 2023).
[28] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Commun ACM*, vol. 50, pp. 94–100, Oct. 2007, doi: 10.1145/1290958.1290968.
[29] "2022 Ponemon Cost of Insider Threats Global Report | Proofpoint US," *Proofpoint*, Jan. 31, 2020. https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats (accessed Feb. 19, 2023).
[30] R. O. Jr, "In cyberattacks, hacking humans is highly effective way to access systems," *Washington Post*, Sep. 26, 2012. Accessed: Feb. 05, 2023. [Online]. Available: https://www.washingtonpost.com/investigations/in-cyberattacks-hacking-humans-is-highly-effective-way-to-access-systems/2012/09/26/2da66866-ddab-11e1-8e43-4a3c4375504a_story.html
[31] L. Bickman, "The Social Power of a Uniform1," *J. Appl. Soc. Psychol.*, vol. 4, no. 1, pp. 47–61, 1974, doi: 10.1111/j.1559-1816.1974.tb02599.x.
[32] Y. Sawa, R. Bhakta, I. G. Harris, and C. Hadnagy, "Detection of Social Engineering Attacks Through Natural Language Processing of Conversations," in *2016 IEEE Tenth International Conference on Semantic Computing (ICSC)*, Feb. 2016, pp. 262–265. doi: 10.1109/ICSC.2016.95.

[33] Mrs. A. S. Gokhale and V. S. Waghmare, “The Shoulder Surfing Resistant Graphical Password Authentication Technique,” *Procedia Comput. Sci.*, vol. 79, pp. 490–498, Jan. 2016, doi: 10.1016/j.procs.2016.03.063.
[34] C. Hadnagy, “Social Engineering: The Science of Human Hacking,” 2017, [Online]. Available: https://theswissbay.ch/pdf/Books/Computer%20science/socialengineering_thescienceofhumanhacking_2ndedition.pdf
[35] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, “Don’t click: towards an effective anti-phishing training. A comparative literature review,” *Hum.-Centric Comput. Inf. Sci.*, vol. 10, Dec. 2020, doi: 10.1186/s13673-020-00237-7.
[36] “What is a phishing attack?,” *Cloudflare*. https://www.cloudflare.com/learning/access-management/phishing-attack/ (accessed Feb. 04, 2023).
[37] “Phishing email examples to help you identify phishing scams.” https://us.norton.com/blog/online-scams/phishing-email-examples (accessed Feb. 18, 2023).
[38] Larrivée, P., “Social engineering: The risks and countermeasures,” *J. Inf. Priv. Secur.*, vol. 11, no. 2, pp. 66–77, 2015, doi: 10.1080/15536548.2015.1069295.
[39] F. Greitzer, J. Strozer, S. Cohen, A. Moore, D. Mundie, and J. Cowley, “Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits,” presented at the Proceedings - IEEE Symposium on Security and Privacy, May 2014, vol. 2014. doi: 10.1109/SPW.2014.39.
[40] A. Shostack, *Threat Modeling: Designing for Security*. John Wiley & Sons, 2014.
[41] J. Saleem and M. Hammoudeh, “Defense Methods Against Social Engineering Attacks,” in *Computer and Network Security Essentials*, 2018, pp. 603–618. doi: 10.1007/978-3-319-58424-9_35.
[42] I. Mann, *Hacking the Human: Social Engineering Techniques and Security Countermeasures*. London: Routledge, 2017. doi: 10.4324/9781351156882.
[43] H. Ebbinghaus (1885), “Memory: A Contribution to Experimental Psychology,” *Ann. Neurosci.*, vol. 20, no. 4, pp. 155–156, Oct. 2013, doi: 10.5214/ans.0972.7531.200408.
[44] National Institute of Standards and Technology (NIST), *Information Security Handbook: A Guide for Managers*. U.S. Department of Commerce, 2017.
[45] Information Systems Security Association (ISSA), “Security Policies Every Organization Must Have,” 2014.
[46] Sharma, S. K., & Gupta, B. B., “A Study on the Effectiveness of Information Security Policies in Indian Organizations,” *J. Inf. Secur.*, vol. 7, no. 3, pp. 165–178, 2016.
[47] D. Alharthi and A. Regan, “A Literature Survey and Analysis on Social Engineering Defense Mechanisms and INFOSEC Policies.” Rochester, NY, 2021. Accessed: Feb. 09, 2023. [Online]. Available: https://papers.ssrn.com/abstract=3830208
[48] S. Furnell, “An assessment of website password practices,” *Comput. Secur.*, vol. 26, no. 7, pp. 445–451, Dec. 2007, doi: 10.1016/j.cose.2007.09.001.
[49] W. Fan, L. Kevin, and R. Rong, “Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations,” *J Comput. Netw. Inf. Secur.*, vol. 9, no. 1, Art. no. 1, Jan. 2017.

8 List of Figures, Tables, Graphs

8.1 List of figures

8.2 List of tables

8.3 List of graphs

Appendix

The below survey is also accessible on the following link: https://forms.gle/2DPX8NQEkGnK7f4j8

1. Are you aware of the concept of social engineering?

a) Yes
b) No
c) Partially

2. Do you know what the definition of social engineering is?

a) Yes
b) No
c) Partially

3. Do you believe that social engineering is a serious threat to individuals and organizations?

a) Yes
b) No
c) I am not sure

4. Are you aware of the potential risks associated with social engineering attacks?

a) Yes
b) No

5. What is the most common type of social engineering attack?

a) Phishing
b) Baiting
c) Social networking sites
d) Scareware
e) I do not know

6. Attackers cannot target me; my computer has no value to them.

a) Yes

b) No

c) I am not sure

7. Have you had access to your personal information on a public computer, such as a library or computer lab?

a) Yes

b) No

8. Would you be able to tell if your personal computer was being hacked?

a) Yes

b) No

9. Have you ever found a virus or a trojan horse on your own personal computer?

a) Yes

b) No

c) I cannot tell

10. Do you know how to tell if your computer has been hacked?

a) Yes

b) No

11. Do you know that your device has been attacked or compromised in the past?

a) Yes

b) No

12. Do you know what to do if there is an attack on your computer or if you get a virus on your computer?

a) Yes

b) No

13. Do you have knowledge about the concept of cybercrime?

a) Yes
b) No
c) Partially

14. Is your computer's firewall activated?

a) Yes
b) No
c) I do not know

15. How careful are you when opening email attachments?

a) I always make sure it is from someone I know or from someone I am expecting an email from
b) I open the attachment as long as I know the sender
c) I open attachments regardless of whether I know the sender or not

16. Have you ever clicked on a link in an e-mail or on the internet that led you to the download of potentially harmful files?

a) Yes
b) No

17. Have you ever received a phone call from someone claiming to be from technical support and asking for access to your computer?

a) Yes
b) No

18. Have you ever received a message from a social media account claiming to be from a friend or relative and asking for personal information?

a) Yes
b) No

19. Do you usually share your passwords with anyone?

a) Yes, only with family members
b) No, I do not share my passwords with anyone
c) Yes, with many people including my colleagues, friends, family members, etc.

20. How do you typically create your passwords?

a) I usually create my passwords with a combination of letters, numbers, and special characters.
b) I usually create my passwords using my personal information, such as my name and date of birth.

21. Is USB considered transmitting viruses?

a) Yes
b) No
c) I do not know

22. Have you ever noticed someone you do not know or trust eavesdropping on your conversations, either over the phone or face-to-face conversations?

a) Yes
b) No
c) I cannot tell

23. Do you have any antivirus software installed on your device?

a) Yes
b) No

24. Do you regularly update your antivirus software?

a) Yes
b) No

25. How often do you scan your device?

a) Once a week
b) Once a month
c) Once every three months
d) Once every six months
e) Once a year
f) I do not scan my device

26. Is the cost of the antivirus program reasonable?

a) Yes
b) No

27. Do you regularly update your operating system?

a) Yes
b) No

28. Have you received any training or education on how to identify and protect against social engineering attacks?

a) Yes
b) No

29. Do you take measures to protect yourself from falling victim to a social engineering attack?

a) Yes
b) No

30. Do you want to take courses in social engineering?

a) Yes
b) No