Navigating the Social Engineering Landscape: Safeguarding Industry Networks through Diverse IT-Security Measures

Master Thesis by Tristan Gahler
Examiner: Dr.Ing. Guido Rößling
Day of submission: 24.11.2023

Thesis Statement pursuant to § 22 paragraph 7 of APB TU Darmstadt

I herewith formally declare that I, Tristan Gahler, have written the submitted thesis independently pursuant to § 22 paragraph 7 of APB TU Darmstadt without any outside support and using only the quoted literature and other sources. I did not use any outside support except for the quoted literature and other sources mentioned in the paper. I have clearly marked and separately listed in the text the literature used literally or in terms of content and all other sources I used for the preparation of this academic work. This also applies to sources or aids from the Internet.
This thesis has not been handed in or published before in the same or similar form.
I am aware, that in case of an attempt at deception based on plagiarism (§38 Abs. 2 APB), the thesis would be graded with 5,0 and counted as one failed examination attempt. The thesis may only be repeated once.
For a thesis of the Department of Architecture, the submitted electronic version corresponds to the presented model and the submitted architectural plans.

Darmstadt, 24. November 2023

Tristan Gahler

Tristan Gahler

Acknowledgements

At this point, I would like to thank everyone that helped me during my academic journey and the creation of this thesis.

First and foremost, I would like to thank Dr.-Ing. Rößling. His support and the degree of independence he allowed me were instrumental to my work.

Furthermore, my parents, as without their continuous support and understanding neither this thesis, nor my academic program as a whole would have been possible. I would also like to thank my dear friend Philipp, who helped me with gaining access to important study material.

Lastly, I would like to thank my fiancée, Annette, as she has always believed in my success, stood by me during challenging times, and offered her assistance whenever possible.

Zusammenfassung

German translation for information purposes only:

Social Engineering, verwurzelt in der Manipulation der menschlichen Psychologie, ist eine weit verbreitete und sich ständig weiterentwickelnde Bedrohung der Informationssicherheit. Diese umfassende Untersuchung zielt darauf ab, Unternehmen jeder Größe mit dem Wissen und den Strategien auszustatten, die erforderlich sind, um sich gegen diese vielschichtige Bedrohung zu verteidigen. Unsere Reise beginnt mit einer grundlegenden Definition von Social Engineering und schreitet zur Erforschung des Angriffszyklus und der Taxonomie sowohl für Angreifer als auch für Angriffsvektoren voran, bevor wir uns im Anschluss der Analyse der Angriffsmuster widmen.

Während unserer Forschung decken wir die psychologischen Schwachstellen und Verhaltensfaktoren auf, die Individuen anfällig für diese Angriffe machen. Wir tauchen auch in die komplexe Welt der Demografie ein und bieten Einblicke in die Widersprüche, die in der bestehenden Forschung auf diesem Gebiet zu finden sind.

Die Verteidigung gegen Social Engineering erfordert einen vielschichtigen Ansatz. Unsere Arbeit betont die Schlüsselrolle robuster Sicherheitsrichtlinien, den Nutzen von Serious Games in der Sicherheitserziehung und der Findung von Schutzzielen, sowie die Entwicklung effektiver Schulungsmethoden, die sicherheitsbewusstes Verhalten fördern. Ethische Aspekte werden während unserer Untersuchung berücksichtigt, einschließlich der Notwendigkeit ethischer demografischer Forschung zur Verhinderung von Diskriminierung und des ethischen Verhaltens von Penetrationstests zum Schutz der Rechte und der Würde der Mitarbeiter.

Darüber hinaus unterstreichen wir die Bedeutung von Strategien zur Notfallvorsorge als entscheidenden Bestandteil der Verteidigung, um die potenziellen Auswirkungen von Social Engineering-Angriffen zu minimieren. Unsere Forschung schließt mit der Präsentation der Best Practices für Organisationen, die sich dazu verpflichten, ihre Umgebungen vor den Hintergründen von Social Engineering-Bedrohungen zu sichern.

Zusammenfassend erkennen wir, dass Social Engineering eine dynamische Herausforderung bleibt. Diese Untersuchung unterstreicht die Bedeutung interdisziplinärer, ganzheitlicher Taktiken, welche die Bildung, die Umsetzung von Richtlinien, fortschrittliche Technologie und ethische Aspekte umfassen. Diese Elemente stärken gemeinsam die Verteidigung von Organisationen und schützen die wertvollsten Vermögenswerte - Menschen und Daten. Unsere Forschung betont die Notwendigkeit kontinuierlicher Anpassung und hebt die Bedeutung effektiver Sicherheitsschulungen und -aufklärungsprogramme für Mitarbeiter hervor, um der sich ständig verändernden Landschaft von Social Engineering-Bedrohungen zu begegnen.

Abstract

Social engineering, rooted in the manipulation of human psychology, is a pervasive and ever-evolving threat to information security. This comprehensive examination seeks to educate and equip companies of all sizes with the knowledge and strategies necessary to defend against this multifaceted threat. Our journey commences with a foundational definition of social engineering and progresses into an exploration of the attack cycle and taxonomy for both attackers and attack vectors, before we analyze the different attack patterns themselves.

As we progress, our research uncovers the psychological vulnerabilities and behavioral factors that render individuals susceptible to these attacks. It also delves into the complex realm of demographics, offering insights into the contradictions found in existing research within this field.

Defending against social engineering requires a multifaceted approach. Our work emphasizes the pivotal role of robust security policies, the utility of serious games in security education and goal elicitation, and the development of effective training methods that foster security-conscious behaviors. Ethical implications are considered throughout our examination, encompassing the need for ethical demographics research aimed at preventing discrimination and the ethical conduct of penetration tests to safeguard employee rights and dignity.

Furthermore, we highlight the significance of disaster recovery strategies as a critical component of defense, mitigating the potential fallout of social engineering attacks. Our research concludes with the presentation of tailored best practices for organizations committed to securing their environments against the backdrop of social engineering threats.

In summary, we acknowledge that social engineering remains a dynamic challenge. This exploration underscores the significance of interdisciplinary, holistic tactics that encompass education, policy implementation, advanced technology, and ethical considerations. Collectively, these elements bolster organizational defenses, safeguarding the most valuable assets—both people and data. Our research emphasizes the need for continuous adaptation and underscores the importance of effective security training and awareness programs for employees in confronting the ever-shifting landscape of social engineering threats.

Table of Contents

1 Introduction

"The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be you [...] What I found personally to be true was that it's easier to manipulate people rather than technology [...] Most of the time organizations overlook that human element." [92]

The words spoken by the once 'most wanted hacker' Kevin Mitnick in 2002 remain as true today as they were over 20 years ago. According to Purplesec, 98% of all cyber-attacks involve some form of social engineering [93]. Social engineering is the art of tricking a person into doing something they would not normally do or revealing sensitive information, such as passwords. These attacks are not only highly effective but also relatively easy to execute, requiring minimal technical knowledge [12]. Yet, in a survey of 582 information security professionals, 50% of them admitted that they do not believe their organizations are adequately prepared to defend against a ransomware attack [27]. Ransomware attacks are often directly tied to previous social engineering tactics.

In the following thesis, we will delve into the precise nature of social engineering, its remarkable effectiveness, the factors contributing to successful social engineering attacks, the distinctions between various attack patterns, and strategies for businesses to safeguard their data against each type of attack. Additionally, we will explore the psychological factors influencing victims' behavior and innovative methods for raising awareness about social engineering, while considering the ethical implications.

1.1 Motivation

To understand the motivation behind this thesis and the need for increased awareness of social engineering, we must examine the current impact of cybercrime on the industry. According to the 2022 Official Cybercrime Report by Cybersecurity Ventures [18], cybercrime is projected to cost the world $8 trillion USD in 2023. To put this into perspective, if cybercrime were a country, it would be the third-largest economy globally, following the United States and China. This figure is expected to grow by 15% annually over the next three years, reaching $10.5 trillion USD by 2025. For comparison, the cost of cybercrime in 2015 was $3 trillion USD.

These costs encompass data destruction, financial theft, loss of productivity, intellectual property theft, personal and financial data breaches, embezzlement, fraud, post-attack business disruption, forensic investigations, data and system restoration, and reputational damage [18]. Alarmingly, over 50% of small-to-mid-sized businesses fall victim to these attacks, and 60% of them go out of business within six months after a data breach or hack.

Yet, it is not just small-to-mid-sized businesses at risk. Moody's has identified industries with very high cyber exposure risks. Critical infrastructure, including utilities and hospitals, faces elevated risks, while banks, telecommunications, technology, chemicals, energy, and transportation services are rated as high risk [94].

The severe consequences of a successful attack become evident when examining data breach statistics. According to Varonis' 2021 Data Risk Report for Financial Services [95], employees typically have access to nearly 11 million files, with two-thirds of companies having over a thousand sensitive files open to every employee. About 60% of these companies have over 500 passwords that never expire, with the average data breach costing as much as $5.85 million USD.

One way to exploit these statistics is by deceiving an employee into revealing their user credentials. While one might assume that tricking someone into revealing their password demands a sophisticated approach, this might not necessarily be the case. While there are several sophisticated attack patterns, human psychology exposes several vulnerabilities that social engineers can leverage to commit attacks which can be trivial and still successful. For example, among these vulnerabilities is the inclination to reciprocate favors, even when said favors were unasked for [36]. To illustrate this point, Happ et al. [36] conducted an experiment involving pedestrians participating in a computer security study. These individuals were offered a piece of chocolate and were subsequently asked about their passwords. The astonishing result was that 38.6% of participants revealed their passwords, and an additional 47.4% shared hints about their passwords, such as using their birthdates.

The objective of this thesis is to provide a comprehensive understanding of social engineering. This includes defining the concept, analyzing its attack patterns, explaining their effectiveness, and outlining the necessary steps to protect industries of all sizes against various attack patterns.

1.2 Thesis Outline

In this thesis, we delve deep into the intricate landscape of social engineering, exploring its various dimensions and implications. The following outline provides a roadmap for our exploration, highlighting the key sections and topics covered in this thesis.

The journey begins with Chapter 1: *Introduction*, where we set the stage for our study by discussing the motivation behind addressing social engineering in the contemporary cybersecurity landscape. This section also outlines the thesis's structure, offering readers a clear overview of the chapters and their respective themes.

Chapter 2: *Related Work and Fundamentals of Social Engineering* offers an in-depth exploration of current research and literature regarding social engineering. In this chapter, we examine previous studies and their discoveries, establishing our research within the broader landscape of existing knowledge. Additionally, we will explore the fundamentals of social engineering by examining various attack frameworks, categorizing social engineering attacks, and dissecting both their characteristics and those of the attackers. We will also analyze the mediums through which these attacks are executed.

As we proceed to Chapter 3: *Attacks*, we explore a range of attack vectors, encompassing both direct and indirect-based approaches. To illustrate the practical application of these concepts and highlight the simplicity of executing a social engineering attack, we include a real-world example. This example serves to demonstrate the ease with which a social engineering attack can be carried out.

Chapter 4: *Psychological Aspects* dives into the vulnerabilities inherent in the human psyche. We explore the psychological factors that render individuals susceptible to social engineering, along with methods to address and balance these vulnerabilities. This chapter also delves into the psychological mechanisms at play during successful social engineering attacks and identifies crucial factors influencing people's compliance. Moreover, a thorough examination of demographics in social engineering attacks offers insights into the differing susceptibility of various groups, as indicated by studies. It also reveals contradictions among these findings and the resulting ethical implications.

Moving on to Chapter 5: *Defenses*, we investigate the security challenges faced across various job roles and the importance of setting clear security goals. This section introduces interdisciplinary approaches to defense strategies. We examine the role of serious games, various training methods, policies, and technical defense mechanisms in fortifying an organization's security. Ethical considerations surrounding penetration tests and disaster recovery preparations are also explored.

Chapter 6: *Best Practices* compiles a set of recommended best practices for combating social engineering attacks, drawing upon the insights gained from our extensive exploration.

Finally, in Chapter 7: *Conclusion*, we bring our comprehensive analysis of the intricate landscape of social engineering to an end. This chapter summarizes the key findings and underscores the evolving nature of the social engineering threat. It emphasizes the importance of an ongoing commitment to security, ethics, and vigilance in the battle against social engineering threats.

This thesis provides a holistic view of social engineering, from its fundamental concepts and various attack vectors to psychological aspects, defense strategies, and best practices. It serves as a valuable resource for understanding and addressing this evolving threat in the cybersecurity realm.

2 Related Work and Fundamentals of Social Engineering

In the realm of cybersecurity, a diverse body of research has been dedicated to understanding and countering social engineering attacks from different points of view. These studies focus their research on specific topics within the landscape of social engineering, offering vital insights into particular aspects of this phenomenon. What makes them particularly valuable is their analysis of the topic from diverse angles and backgrounds, encompassing not only classic IT-security perspectives but also delving into social and psychological dimensions. The forthcoming excerpt provides a glimpse of some significant work preceding this thesis, where the focus closely aligns with the thematic scope of the current research:

A Taxonomy for Social Engineering attacks
The work by Ivaturi and Janczewski [42] addresses the increasing use of social engineering attacks, and it identifies the lack of a unified approach to categorize these attack methods as a gap in fully understanding the threat. The paper aims to fill this gap by proposing a taxonomy of social engineering attacks, offering organizations a better understanding of these methods to enhance their vigilance against such attacks. The paper commences by discussing the nature and impact of social engineering attacks, laying the foundation for the proposed taxonomy. It then presents the taxonomy by describing different attack vectors and their categorizations, along with a brief discussion of possible countermeasures.

A Literature Survey and Analysis on Social Engineering Defense Mechanisms and InfoSec Policies
D. Alharthi and A. Regan [3] developed a taxonomy for social engineering defense mechanisms and subsequently conducted a study to assess employee awareness of these mechanisms. Additionally, they proposed a model of Social Engineering Information Security Policies (SE-IPs) and designed a survey to measure the level of incorporation of these policies. Their findings revealed that less than half of the employees were aware of social engineering attacks, and that corporations had implemented just over fifty percent of the identified policies. Therefore, Alharthi and Regan's paper not only raises awareness but also provides concrete measures that can be taken to enhance industry security by implementing the SE-IPs.

A Serious Game for Eliciting Social Engineering Security Requirements
Existing approaches often overlook the human factor in social engineering attacks and fail to capture the individual behaviors of employees. Despite the increasing frequency and severity of social engineering attacks, there is a notable lack of security awareness and consideration of these threats in the requirements elicitation process. To address this gap, K. Beckers and S. Pape [9] introduced a card game designed to engage all employees within a company. This game serves as a tool for comprehending the threat posed by social engineering and for documenting relevant security requirements. It takes into account the unique context of each organization and educates participants on the fundamental principles of human behavior that social engineers exploit, along with specific attack patterns.

Social Engineering in Cybersecurity: A Domain Ontology and Knowledge Graph Application Examples
Investigating the components of social engineering, Z. Wang et al. [84] developed a domain ontology for social engineering in cybersecurity. They proceeded to evaluate this ontology by applying it as a knowledge graph. The domain ontology encompasses 11 core concepts that represent significant entities and factors within the social engineering domain. Additionally, it includes 22 types of relationships that clarify the interconnections between these entities. This formal and explicit knowledge schema serves as a valuable resource for comprehending, analyzing, reusing, and disseminating domain knowledge related to social engineering.

Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal
In their work, H. Aldawood and G. Skinner [2] conducted a critical analysis of existing protection measures, tools, and policies within the industry to safeguard against social engineering attacks. Following a systematic review of recent studies on the subject, they identified the necessity of providing dedicated training for employees to enhance their understanding of the risks associated with social engineering and how to avoid

falling victim to such attacks. These measures encompass awareness programs, training for non-technical staff, the implementation of new security networks, as well as the utilization of software and security protocols to mitigate social engineering threats.

An interdisciplinary view of social engineering: A call to action for research
This paper, by A. H. Washo [86], delves into the subject of social engineering from an interdisciplinary perspective. It encompasses a comprehensive literature review spanning the information technology, psychology, and business disciplines. This review underscores the interconnected nature of the topic and emphasizes the importance of approaching it from multiple viewpoints.
Following the literature review, the paper explores the ethical dimension of social engineering research, examining it from both philosophical and professional standpoints. To aid researchers in their studies, the paper introduces a proposed framework. This framework offers a flexible model, with a particular focus on either a philosophical or practical ethics perspective.

As we delve deeper into the realm of social engineering, we will revisit certain studies to analyze their results and implications. However, before delving into the intricacies of this subject, it is essential to establish a common understanding of the term and familiarize ourselves with the various forms of social engineering.

Included in these studies are several taxonomies and models which describe the social engineering attack cycle. The most commonly used is the social engineering attack cycle model (see Fig. 1) first described by Kevin Mitnick in his book *The art of deception: controlling the human element of security* [58]. First, we will take a look at this model to get a rough understanding of what social engineering is. Afterwards, we will take a look at an ontological model that is able to represent the attack in great detail, such as flow and time.

2.1 Kevin Mitnick's Social Engineering Attack Cycle

Mitnick's attack cycle is separated into four distinct parts. Each of these phases will now be briefly discussed as explained in Mitnick's book. Nowadays, this cycle is commonly being referred to as *investigation*, *hook*, *play* and *exit*, respectively.

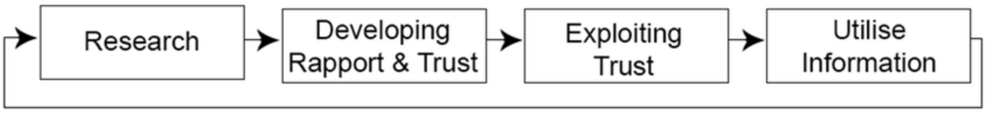


Figure 1: Kevin Mitnick's Social Engineering Attack Cycle [58]

- **Research**: this phase describes the gathering process of information regarding the chosen target. It is important for the attacker to learn as much as possible about his soon-to-be victim in order to create a convincing lie.

- **Developing Rapport & Trust**: in the second phase, the social engineer tries to gain the trust of his victim, as the target will be more likely to divulge information to an attacker, they trust [86]. This can be done in a number of ways. According to Mitnick [58], rapport and trust can be gained by abusing insider information, misrepresenting an identity, citing people known to the victim, by showing the need for assistance or by occupying an authorative role.

- **Exploiting Trust**: During this phase, the previously established trust will be exploited to elicit information from the target. This could be seemingly harmless information that could, however, be used by the social engineer when communicating with a different victim to build trust with them. For example, it could involve getting the victim to share information that a certain person will not be available at a given time, disclosing concrete information such as the password to a user's account, or engaging in *reverse social engineering* with the goal of manipulating the victim into seeking the attacker's help [58]. More details on this will be provided later.

- **Utilize Information**: finally, the previous phases' outcome gets utilized to achieve the initial goal, or the attacker moves on to his next step which might be required.

Let us look at a simple example: an attacker, who could be a disgruntled employee that wants to harm those who wronged him, needs access to a file he wants to offer to the competition. He knows through his research and insider information that a certain department is working on it collectively. He also knows that this department hired a new employee, as well as their name and telephone number. He then calls the new employee, posing as one of his higher-ups, congratulating him on his new job and wishing him well. After he has the feeling that the victim trusts him, he reveals that he called him not only to congratulate him, but because he forgot his USB stick which contained the file he was supposed to present on his current business trip. The employee who wants to impress and help out in a critical situation sends the file immediately as he has no reason to doubt the story and certainly does not want to leave his boss hanging. Thanking him for his help, the attacker hangs up, leaving behind an unsuspecting victim.

In literature, this cycle is usually being referred to as *investigation*, *hook*, *play* and *exit*. The description of the phases is a little more distinct. For example, the *exit* phase focuses solely on covering one's tracks and disappearing before the victim notices that something is off. The utilization of information therefore takes place during the *play* phase. Overall, the two naming schemas express the same procedure.

This model does have some problems though. Mitnick described this model only very briefly and without going into great detail. It is therefore very broad and can be interpretated in different ways. Hence, we will take a look at a different attack framework that was built on Mitnick's model but which covers all of the finer details, without room for interpretation. This deep understanding is necessary for the development of awareness trainings, the development of countermeasures against attacks as well as for training purposes.

2.2 Mouton et al.'s Attack Framework

In the following subchapter, we are going to explore the attack framework proposed by Mouton et al. [63], which allows us to inspect an attack pattern in much greater detail.

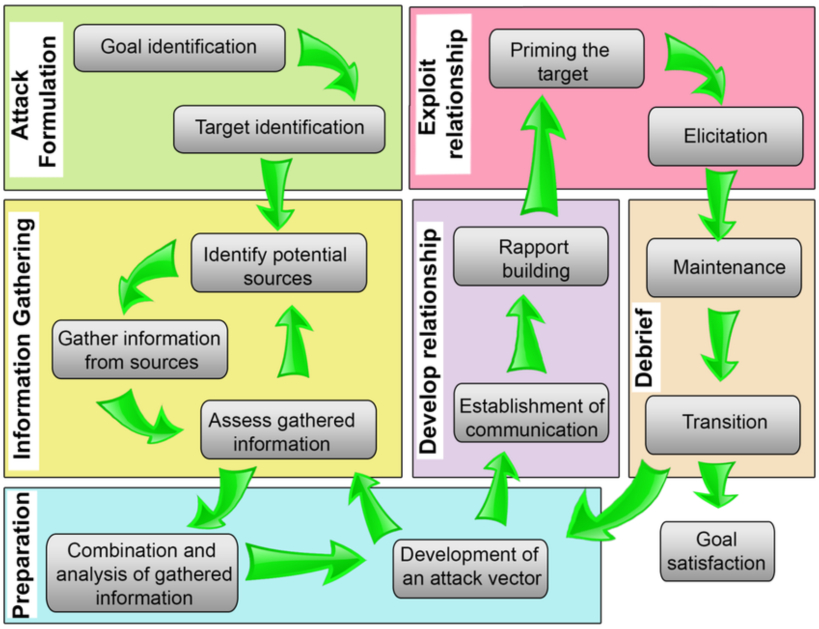


Figure 2: Social Engineering Attack Framework by Mouton et al. [63]

We will now take a close look at each of the different phases as well as their substeps.

1. **Attack Formulation**: Initially, the social engineer has to ask themselves the question of what the goal of their attack will be. Once the purpose of the attack is clear, they need to select a target or a group of individuals. It is important to note here that the goal could be to steal a file from an organization, and to achieve this, they would need to manipulate a certain employee. In this case, both the company and the employee would be targets and, therefore, important in the information-gathering phase.

   A common list of possible motives for the attacker, as suggested by Wang et al. [84], includes but is not limited to the following: 1) financial gain, 2) competitive advantage, 3) revenge, 4) external pressure, 5) personal interest, 6) intellectual challenge, 7) increasing followers or friends in social networks, 8) image spoiling (e.g., reputation destruction), 9) prank, 10) fun or pleasure, 11) politics, 12) war, 13) religious belief, 14) fanaticism, 15) social disorder, 16) cultural disruption, 17) terrorism, 18) espionage, 19) security test.

2. **Information Gathering**: The second step is crucial for the success of the attack. The social engineer needs to build trust with their victim, as the victim is more likely to share information if a relationship exists between the two [86]. The probability that the victim will trust the social engineer will be increased by the quality of the information the social engineer possesses.
   To initiate the process of gathering information, the social engineer must identify potential sources. These sources can vary widely and include publicly available information such as company websites, social media, colleagues, or even the technique known as “dumpster diving”, where the social engineer searches through discarded items of the victim in hopes of finding valuable information, such as an address or other private details [12].
   After gathering this information, it needs to be assessed for its relevance to the attack. If the attacker has collected enough data, they can proceed to the next step of preparing the attack. Otherwise, they can return to the task of identifying additional sources from which to gather more material until they are satisfied.

   The success of an attack heavily depends on the information gathered by the social engineer, which can be exploited by the attacker to identify targets, vulnerabilities, and formulate attack strategies. The following list includes the information identified by Wang et al. [84] to hold value and aid the social engineer in their attacks: 1) person name, 2) identity, 3) photograph, 4) habits and characteristics, 5) hobbies or interests, 6) job title, 7) job responsibility, 8) schedule, 9) routines, 10) new employee, 11) organizational structure, 12) organizational policy, 13) organizational logo, 14) company partner, 15) lingo, 16) manuals, 17) interpersonal relations, 18) family information, 19) profile in social networks, 20) posts in social media, 21) connections in social networks, 22) social networks group information, 23) (internal) phone numbers, 24) email information (address, format, footer, etc.), 25) username, 26) password, 27) network information, 28) computer name, 29) IP addresses, 30) server name, 31) application information, 32) version information, 33) hardware information, 34) IT infrastructure information, 35) building structure, 36) location information.

3. **Preparation**: During the third step, the social engineer combines and analyzes the previously gathered information to gain a broader perspective on the attack they have in mind. The gathered data can be used for a technique called “pretexting” [12]. Pretexting is a form of social engineering where attackers aim to persuade their victims to voluntarily disclose valuable information, such as access credentials. The distinguishing feature of pretexting lies in its creative element: the attacker attempts to utilize a fabricated scenario or false pretext to deceive the target. Success relies on the quality of the gathered information.

Afterward, the social engineer can begin to develop an attack vector. This attack vector needs to contain all the elements [61] of a social engineering attack that will ultimately lead to achieving their goal. This includes a goal, a target, a social engineer, as well as a medium over which they communicate (text, voice, video, etc.), compliance principles (principles used by the attacker to persuade the victim, e.g., authority), and techniques like impersonation.

4. **Develop Relationship**: As mentioned earlier, establishing trust is crucial for the attacker, as the victim is unlikely to share useful information if they suspect deception. Using the previously chosen communication medium, the social engineer proceeds to the “establishment of communication” step. If a pretext was chosen, it is now employed during the initial contact. The subsequent step, “rapport building”, can be quite time-consuming for the social engineer, involving the actual development of a trusting relationship through various techniques. A well-crafted pretext can simplify this step.

5. **Exploit Relationship**: The first step in exploiting the relationship is to “prime” the target. Priming involves getting the target into a desired emotional state, such as sadness or compassion. This can be accomplished by sharing a sad story to evoke specific memories or by narrating a tale of misfortune. Once this is achieved, the desired emotional state in the victim is established, and the social engineer can begin to extract the desired information, such as a password.

6. **Debrief**: The sixth and final step of an attack is the debriefing of the target. Maintenance involves resetting the emotional state of the target. This is important because the target is unlikely to dwell too much on the activities that have transpired if these activities did not appear out of the ordinary to them. If things did seem strange to them, they might become suspicious or discuss the situation with someone, potentially exposing the ruse.

   Afterwards, the attacker must decide whether they have achieved their goal and are satisfied with the outcome or if they still need more information. In the latter case, they must return to the information-gathering phase.

Now that we have an understanding of how a social engineer operates in theory, we can begin to examine the various attacks themselves. Therefore, we will now delve deeply into all aspects related to the actual attacks.

2.3 Taxonomy of the Attacker

To begin with, we will examine the attackers themselves, as understanding their characteristics provides an initial insight into their capabilities. Wang et al. [84] identified three main groups of attackers:

1. **Quantity of Attackers**: The first group categorizes the number of attackers involved, which can fall into one of the following categories:
   - An individual attacker.
   - A group of individuals working collectively.
   - An entire organization engaged in the attack, as seen in instances of state-sponsored cyberwarfare, where one nation attacks another for political, military, or espionage purposes.

2. **Internal vs. External**: The second categorization distinguishes whether the attackers are:
   - Internal to the company, such as a disgruntled employee with insider knowledge.
   - External to the company, meaning they have no prior affiliation with the organization.

3. **Nature of the Attacker**: The third classification delves into the identity of the attacker, which can be categorized as:
   - A real person, an actual human being.
   - A virtual entity, such as a bot or automated system functioning as the attacker.

Understanding these attacker categories is essential for assessing the potential risks and motivations behind cyberattacks, helping organizations tailor their security measures accordingly.

2.3.1 Internal Attackers

We would now like to place special emphasis on the group of internal attackers. This focus is crucial because a significant portion of attacks originates from within the company. According to Verizon's Data Breach Investigations Report of 2022 [95], this accounts for approximately 18% of all security incidents. While this percentage may appear relatively small, it is important to note that the company's possible interactions with attackers from the inside, particularly potential future attackers, differ significantly from those with external attackers. One distinctive aspect is that it is possible to proactively prevent these attacks through certain cybersecurity policies and by implementing measures that address employee concerns, thereby reducing the likelihood of disgruntlement and the desire for revenge.

Furthermore, attacks originating from insiders can have particularly devastating consequences, primarily due to the unique knowledge these attackers possess. They typically have a deep understanding of the specific data's value, especially when sold to the right buyer. Moreover, they know how to access this data, and in some cases, they may possess the necessary permissions to do so without raising suspicions.

Lastly, the inhibition threshold to abuse one’s access rights can be quite low. While it might sound extreme, a 2019 survey conducted by Deep Secure [20] revealed that nearly half of office employees (45%) expressed a willingness to sell information to external parties. Even more concerning, a relatively modest sum, such as £1,000, was sufficient to tempt 25% of the surveyed employees.

Now, when considering insiders, it is important to acknowledge a special type of threat, namely the disgruntled ex-employee [96]. According to OneLogin [41], 50% of former employees retained access to the company's applications after their employment ended. To better understand the gravity of this threat, we can refer to the Varonis Financial Data Risk Report [95]. This report focused on companies that are similarly trusted by their customers for their security and are prime targets for criminals due to financial motivations, specifically in the banking, insurance, and investment sectors.

The report revealed that, on average, a financial services employee has access to approximately 13% of a company's total files, including the ability to view, copy, move, modify, and delete data, including sensitive information pertaining to employees and customers. This translates to an average of around 11 million files per employee. This concerning access is compounded by poor active directory hygiene, with approximately 41% of companies having fewer than 500 passwords that never expire, 37.5% having between 500 and 1500 such passwords, and roughly 21% of companies having more than 1500 passwords that never expire. Together, these factors create a potent combination. These "ghost users" [95], referring to inactive but enabled accounts, coupled with passwords that never expire and the potential threat posed by disgruntled ex-employees, present a serious and destructive potential.

According to OneLogin [41], 20% of surveyed companies experienced a data breach due to the failure to de-provision an employee. It is worth noting that the ex-employee may not necessarily execute the attack themselves but could either sell this information or fall victim to deception tactics that lead to the exposure of sensitive data. So even parting with an employee on good terms holds risks.

All of these factors underscore the critical importance of addressing internal security risks and implementing robust measures to protect sensitive data within an organization. Furthermore, proper policies regarding employee de-provisioning are essential in mitigating these threats effectively.

However, the objective should not be to scrutinize one's employees and treat them as potential criminals. Such an approach could lead to reduced morale, erode trust, harm productivity, and affect overall work quality, potentially worsening dissatisfaction.

Instead, it is important to focus on several key strategies. First and foremost, there should be an emphasis on educating staff about security risks and the importance of safeguarding sensitive information. Building a security-conscious culture can go a long way in preventing insider threats.

Additionally, technical measures should be implemented to mitigate or prevent insider threats. These measures might include robust access controls, monitoring systems, and encryption protocols.

Furthermore, fostering a positive working environment where employees feel valued, respected, and motivated is crucial. Addressing their needs and concerns promptly can help prevent disgruntlement and potential malicious actions.

Lastly, when employees make mistakes, it is essential to handle these situations appropriately. Rather than resorting to punitive measures that may provoke revengeful behavior, offering constructive feedback and opportunities for improvement is a more effective approach. We will revisit this matter later on for a more in-depth discussion.

2.4 Taxonomy of the Attacks

Social engineering attacks can be categorized in numerous ways, but for the purpose of designing effective countermeasures, we will concentrate on the three following distinct classifications. It is worth noting that there are other classifications, such as attacks that occur in real-time, like a phone call, and non-real-time attacks, such as those conducted through SMS. While these are valid classifications, we will primarily focus on the three that are most pertinent to our discussion.

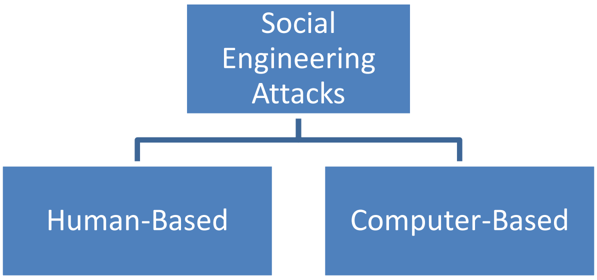


Figure 3: Social Engineering Attacks Classification [72]

The first classification (see Fig. 3) depends on the entity executing the attack. In the case of a human, attacks are carried out either in person or through digital means, such as a phone call, targeting a limited number of victims. The second classification relies solely on software, allowing for attacks on a large number of victims within seconds.

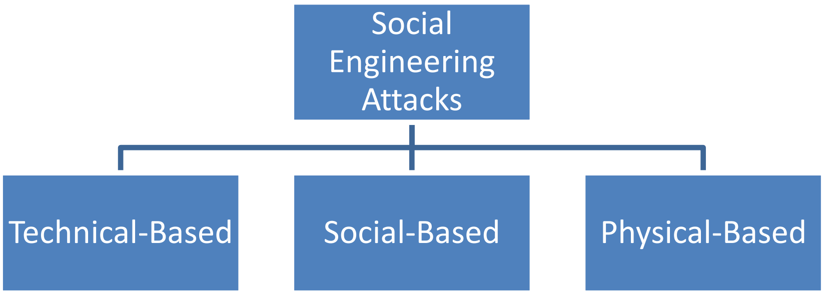


Figure 4: Social Engineering Attacks Classification [72]

The second classification (see Fig. 4) categorizes attacks based on their method of execution: technical-based, physical-based, or social-based.
Technical-based attacks are primarily conducted through the internet, often targeting service websites or social networks. These attacks aim to gather sensitive data such as passwords, credit card details, or other user credentials. They often abuse security weak points in these systems.
Social-based attacks, although time and effort-intensive, are among the most successful and consequently, the most dangerous. Their goal is to establish an exploitable relationship with the victim and playing with their psychology and emotions. An example of such an attack is the “quid pro quo” tactic, where the victim receives an unasked-for favor and, in return, is asked for a favor in a manner that makes them feel indebted to the attacker. We will delve deeper into these attacks later in this discussion.
The third classification encompasses physical-based attacks, which involve direct physical actions by the attacker to collect information. An example of this is the “tailgating” attack, in which the attacker simply follows a victim through a secured door, exploiting their access.

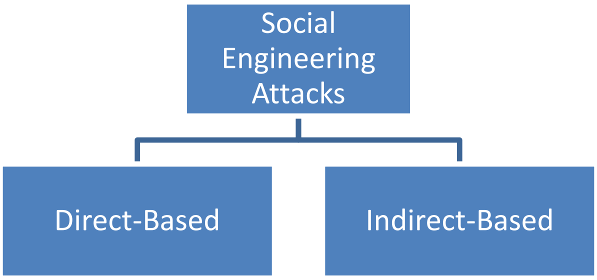


Figure 5: Social Engineering Attacks Classification [11]

The third distinction we introduce in social engineering attacks (see Fig. 5) focuses on the required form of communication or contact. Directly-based approaches involve attacks conducted through, for example, physical contact, texting, or phoning between the social engineer and the victim, often necessitating the presence of the attacker. In these cases, the victim and the social engineer stand in direct contact with one another. On the other hand, indirectly-based attacks can be launched asynchronously and do not require the victim's direct engagement with the attacker. In these cases, communication occurs through an intermediary medium. For instance, a fake pop-up window may deceive the victim into entering credentials on a compromised website where the pop-up is displayed.

2.5 Attack Mediums

The ways in which social interaction or human-computer interaction can be initiated are indeed diverse. Consequently, the nature of an attack can take on a multitude of forms, resulting in a wide array of mediums from which the social engineer can choose the one best suited for their attack. Therefore, during the design process of defense mechanisms, understanding the scope of potential attack mediums is crucial.

Wang et al. [85] have identified the following mediums to be vigilant about: 1) the real world, 2) attached files, 3) letter, 4) manual, 5) card, 6) picture, 7) video, 8) RFID tag, 9) QR code, 10) phone, 11) email, 12) website, 13) software, 14) Bluetooth, 15) pop-up window, 16) instant messenger, 17) cloud service, 18) Voice over IP (VoIP), 19) portable storage drives, 20) short message service (SMS), 21) mobile communication devices, 22) social networks.
This list is by no means exhaustive. In essence, any type of information, whether it is in written or spoken form or any other format, can be vulnerable to exploitation by an attacker if it contains data that fits into their attack strategy. This includes various items such as calendar entries, printed code, or even old and neglected external hard drives.

3 Attacks

With a clear understanding of the fundamental elements involved in a social engineering attack, we can now delve deeper into the various attack vectors. We will explore each of these attack vectors individually to gain a comprehensive insight into the tactics, techniques, and strategies employed by malicious actors in the realm of social engineering.

3.1 Attack Vectors

As exemplified in the previous subchapters, a significant challenge that makes defending against social engineering attacks so difficult is the lack of a single standardized approach. Instead, there exists a multitude of attack patterns, ranging from easily detected phishing emails laden with typos to meticulously planned, sophisticated and multilayered attacks [50]. These attacks can originate from various sources, both physical and digital, and are only limited by the creativity, skill and patience of the attacker.

The diverse forms of attacks and the mediums through which they are carried out are known as “attack vectors” or sometimes “threat vectors”. To design an effective defense strategy, it is crucial to understand the potential manifestations of these attacks. Despite targeting different companies and operating within varying contexts, these attacks can be categorized.

In the following subsection, we will explore the various existing and well-known attack patterns, dissecting how these attacks unfold, the prerequisites they require for success, and how they can be classified. For better distinction, we use the categorization of directly and indirectly-based attacks.

The descriptions of the attack patterns in the following sections (3.1.1 and 3.1.2) are derived from the insights and information obtained from the sources referenced after each attack's name.

3.1.1 Direct-based Attacks

We will begin by examining the category of direct-based attacks, which involve direct contact and interaction between the victim and the social engineer, either through physical or digital contact, such as texting.

- **Shoulder surfing** [85]: In this scenario, the attacker employs various disguises or pretenses to gain access to the victim's workspace. They may pose as a maintenance worker needing entry to the victim's office or simply pretend to have a work-related question like the demonstration of specific processes. While the victim is preoccupied and not fully attentive, the attacker discreetly observes the victim's keyboard inputs or scans prominent places, such as sticky notes or papers containing sensitive information left lying around. This covert surveillance allows the attacker to collect critical data, including usernames and passwords, without the victim's awareness.

- **Manipulating conversation** [85]: in this social engineering tactic, the attackers skillfully steer a group conversation in a specific direction, subtly directing it towards topics related to security measures for example, when trying to elicit the victim’s password. One of the attackers may initiate the process by voluntarily disclosing information about themselves, such as sharing their password, and then soliciting feedback from the group, asking if they believe it is strong enough. Other attackers within the group would join in, following suit by revealing their own passwords for scrutiny.
  The crucial element of this attack lies in the psychology of conformity. When the target of the attack observes multiple individuals in the group willingly sharing their sensitive information, they may feel pressured to conform to the group's behavior. Fearing social exclusion or wanting to appear cooperative, the target becomes more likely to disclose their own password or similar confidential information, falling victim to the attackers' manipulative tactics.

- **Tailgating** [12]: during a tailgating attack, the social engineer seeks unauthorized access to a restricted area by assuming the identity of an individual with legitimate access who appears to be occupied. This may involve waiting near the entry point, pretending to be engaged in an activity like smoking, until a person with authorized access approaches and opens the door. At this point, the attacker ceases their activity and discreetly follows the victim through the open door. The victim is unlikely to raise suspicions in such situations. In indoor environments where smoking is prohibited, the attacker might masquerade as someone having a phone conversation who momentarily exits the room to avoid disturbing colleagues, coincidentally completing the call just as the victim passes by.

    - **Piggybacking** [85]: this is a variation of the tailgating attack in which the victim is tricked into willingly assisting the social engineer in gaining access. Importantly, the victim is unaware that the attacker lacks permission to enter the premises. To lower the victim's guard, the attacker may employ tactics such as carrying a large, cumbersome object and simply asking the victim to hold the door open as they pass through. Alternatively, they might request the victim to open the door, citing that they have left their access card on the other side of the door.
      The likelihood of a successful piggybacking attack increases when the attacker presents themselves well, adopts a friendly demeanor, and exhibits politeness. The victim, in such circumstances, is unlikely to suspect any malicious intent, as they are focused on the satisfaction of having offered assistance. This scenario underscores the significance of the debriefing phase discussed in the previous chapter.

- **Impersonating** [85]: As the name suggests, this tactic involves the attacker assuming a false identity to execute various social engineering attack strategies, such as piggybacking, pretexting, or simply adopting a different persona during a phone call. This can be either used as the attack itself or as a setup for a different attack, like piggybacking.

    - **Helpdesk Impersonation** [97]: This is a notable subcategory of impersonation due to its high effectiveness. In a helpdesk impersonation attack, the attacker claims to be from the company's helpdesk and contacts the victim, citing issues with their user account, for instance. To expedite the "resolution" of the problem, they request the victim's username and password, warning that failure to provide this information would result in the account being locked for an extended period. This attack enjoys a high success rate because users typically wish to avoid having their accounts locked and often harbor no reason to distrust the user helpdesk. We will revisit this attack pattern later in the discussion, emphasizing the importance of educating employees, as the user helpdesk never legitimately requires a user's password.

- **Quid pro quo** [72]: In the realm of social engineering, a quid pro quo attack involves the attacker offering the victim a complimentary good or service with the expectation of receiving something in return. For example, the attacker may impersonate an employee of a fake security company that is running a giveaway offering enticing prizes. However, to participate, victims are required to complete a survey, during which they must disclose their login credentials.

- **Face to face interaction** [85]: Normal face-to-face interactions can be abused in a number of different ways. The main way to success is by abusing the victim’s emotions and psychological traits. Examples would be to intimidate the target, flirting, begging, flattery, using an authorative voice or by acting confidently.

- **Grooming** [91]: This is one of the more recent social engineering attacks, primarily employed by individuals with malicious intent, such as pedophiles. While it is not directly related to industrial security measures, we include it here for comprehensive coverage. The objective of this attack is to build a trusting relationship and emotional bond with the victim through SMS, email, and telephone, leveraging previously acquired information about the victim.

- **Reverse social engineering** [98]: In a reverse social engineering attack, the attacker seeks to create a problem for the victim and then offers an apparent solution, for which they require specific information from the victim. For instance, in one scenario, the attacker may send a phishing link via email, which the user unwittingly clicks on, leading to the installation of malware. Subsequently, the attacker sends a follow-up email posing as a tech support company that offers to assist the user in removing the virus. However, this "assistance" necessitates the user's login credentials. Similar attacks may be executed in person, rather than over the internet.

- **Diversion theft** [48], [79]: During a diversion theft attack, the social engineer aims to either steal physical objects or obtain sensitive information from the victim. In some cases, the attacker may also seek to introduce infected hardware into the victim's possessions. To execute this attack successfully, the attacker must first determine that the victim has ordered something or is about to receive a package. This information can be obtained through various means, such as conducting a survey under false pretenses, inquiring about recent orders, or leveraging insider knowledge.

  On the day of the scheduled delivery, the attacker assumes the role of the recipient or someone authorized to collect the item. By possessing detailed knowledge about the shipment, they are likely to be trusted and therefore able to receive the package from the delivery person. At this point, the attacker can either steal the delivered goods or replace them with identical-looking items that are infected with malware. It is worth noting that this type of attack can be particularly dangerous if the stolen or substituted items involve hazardous goods.

3.1.2 Indirect-based Attacks

The second category under consideration is indirect-based attacks, which can be initiated remotely and asynchronously and therefore do not require the attacker to be physically present. In this category of attacks, there is no direct contact between victim and social engineer.

- **Dumpster Diving** [72]: The objective of a dumpster diving attack is to retrieve valuable information from discarded items. These items can include CDs, old computers, external hard drives, paper documents, and essentially anything else that may contain stored information.

- **Eavesdropping** [12]: Within a company, it is not uncommon for confidential information to be casually discussed in open areas. This can occur because employees may be unaware that others not involved in the conversation are within earshot, or because there is a lack of awareness regarding the need for confidentiality. As a result, attackers who strategically position themselves can exploit this security lapse. Such positioning is not solely a matter of chance, as attackers may intentionally place themselves to overhear information or monitor email and phone communications.

- **Open-source reconnaissance** [71]: In many cases, a significant amount of information can be readily obtained by conducting online searches or exploring public domains related to the target of the attack. These sources may include company websites, where valuable insights into organizational structures, employee directories, and project details can be found. Additionally, email headers can reveal information about the target’s position and such.

  Phone directories available online may provide contact details and affiliations that can be exploited, while advertisements can disclose information about a target's interests, affiliations, or activities. Publicly available newspaper articles can offer insights into a target's personal or professional life, and personal or professional blogs may contain information that can be leveraged as well.

Public records and regulatory filings, such as business registrations and property records, may offer details about a target's business activities and financial history. Furthermore, professional social network platforms like LinkedIn often reveal a target's job role, professional connections, and potentially sensitive information shared within their network.

These various sources of information serve as a treasure trove for social engineers seeking to craft convincing attacks based on the specific vulnerabilities and traits of their targets.

- **Phishing** [19], [24]–[28]: Phishing attacks are by far the most commonly employed tactics. According to Deloitte [21], a staggering 91% of all cyber-attacks originate from a phishing attack. The primary objective of the attack is to persuade the victim to either click on a malicious link within an email, leading to the download of malware, or to follow the link to a spoofed website. Spoofing entails the creation of a fake website designed to mimic a legitimate one. For instance, a victim might receive an email supposedly from DHL, claiming that delivery of their package was unsuccessful due to a partially damaged address label. The email instructs them to follow a link to solve the issue. Upon clicking the link, the victim lands on a website that closely resembles, or is identical to, the legitimate DHL site, but its purpose is to steal the victim's login credentials.

  These tactics are remarkably effective, considering the minimal effort required, as we will explore later. According to IBM Security [100], the average click rate for phishing links sent via email is 17.8%. For more targeted phishing campaigns that include phone calls, the click rate jumps to 53.2%.

  Traditionally, these deceptive links were sent via email, but nowadays they are also frequently distributed through instant messaging apps. Phishing takes on various subforms, each with distinct applications, effectiveness, and required effort, which we will examine now.

  - **Smishing** [71]: Fundamentally, smishing and phishing share the same core objective and differ primarily in how links are distributed. While phishing predominantly relies on email communication, smishing operates through SMS messages. What distinguishes smishing is the inherent constraints of SMS messages, including character limits and the inability to incorporate images like company logos. Consequently, attackers must rely on psychological manipulation, such as offering financial incentives, creating a sense of urgency, or promising sexual encounters or media content, to entice victims.
    From the attacker's standpoint, smishing offers a significant advantage due to the relatively limited security measures in place for SMS messages compared to email-based phishing attacks.

  - **Vishing** [85]: Voice-over-IP (VoIP) enables attackers to leverage phone calls as a medium for their schemes. They can manipulate caller IDs to make it appear as though the calls originate from anywhere in the world, depending on the context of their ruse. For instance, if the attacker is aware that certain employees from the target company are currently on a business trip to Japan, they can spoof a call originating from Japan to make it seem credible and demand a file to be sent that has been forgotten. Typically, this technique is combined with urgency cues. Another scenario involves calling family members of a victim known to be on vacation abroad, spoofing a phone number from that location. The attacker could claim to be an authority and that the victim is in legal trouble, having caused an accident, and requires bail money for release.

  - **Spear Phishing** [71]: While phishing and smishing aim to deceive a broad audience, spear phishing, as the name implies, is tailored to a single, specific target. Executing a successful spear phishing attack demands a lot of effort and patience from the attacker, as they must gather and assess a substantial amount of information about the intended victim. However, a disgruntled ex-employee may already possess all the necessary information to carry out an effective spear phishing attack.

  - **Whaling** [71]: While spear phishing and whaling essentially follow the same attack pattern, the distinction lies in their target selection. Spear phishing can target individuals across an organization, whereas whaling specifically aims to deceive highly influential figures within a company, such as the CEO. This underscores the importance of providing comprehensive security training to all members of an organization, with a special focus on senior leadership. The reason behind this emphasis on security training is driven by the understanding that the potential damage caused by a successful whaling attack increases in proportion to the user's access rights to the company's network and sensitive files.

  - **Business email Compromise Phishing (BEC)** [72]: In a BEC attack, the social engineer meticulously studies the superiors within a company, including their writing style, email headers, and other relevant details, with the aim of closely mimicking their communication style. Subsequently, the attacker will reach out to specific employees with a request, impersonating these senior figures and creating a compelling sense of urgency. This deception is designed to manipulate employees into clicking on links, downloading specific software, or taking other actions as directed by the attacker.

  - **Interactive voice response phishing / Robocalls** [72]: This form of attack targets the masses rather than specific individuals. It involves playing a pre-recorded message when dialing numbers from a list of known phone numbers that answer the call. This method heavily relies on VoIP technology to facilitate interactive voice responses and text-to-speech capabilities. Once the call is answered, the victim's phone number is stored in the attacker's database, enabling them to call again from a different number if the victim blocks the current caller. An example of such an attack includes offering assistance with tax problems. To protect against this type of attack, it is crucial to block and avoid accepting calls from unknown numbers.

- **Trojan attack / Honey pot** [85]: The objective of this attack is to conceal malicious software on a website and entice the user into downloading it. This is often achieved by promising financial gains or tempting the victim with the prospect of explicit photos of individuals they may know, exploiting their curiosity, greed, or desires. Another commonly employed method for spreading viruses in this manner is through pirated films or video games.
  Once the file is downloaded and executed or the link is clicked, the victim's computer becomes compromised. Additionally, this attack can be combined with a phishing email sent to victims, containing a link to the infected website.

- **Baiting** [85]: In a baiting attack, the social engineer exploits the curiosity or greed of their victim by offering something desirable for free, which appears harmless. For example, the attacker might load malware onto a USB stick and then strategically place it in a visible location. The victim, motivated by either the desire to keep the USB stick or out of curiosity about its contents, picks it up. In some cases, if the attacker anticipates the victim's honesty, they might employ multiple USB sticks, adorned with a partner company's logo or a similar ruse to create the illusion of a gift for employees. When the victim inserts the USB stick into their computer, the embedded malware infects the system.

- **Pharming** [79], [101]: This is a technically sophisticated attack that often starts with a phishing attack. Its primary objective is to reroute a user's internet traffic to a fraudulent website designed to closely mimic the appearance of the legitimate site. The goal here is to trick users into providing sensitive information such as login credentials or credit card details. To accomplish this, there are two main types of pharming attacks:

  - **DNS-based Pharming** [101]: DNS-based pharming attacks aim to exploit vulnerabilities within the DNS (Domain Name System) infrastructure to redirect users to malicious websites. There are three primary methods used in these attacks. First, attackers may manipulate the DNS cache of the relevant DNS servers or routers to alter the mapping of domain names and IP addresses by injecting false DNS records into the cache. Second, by gaining unauthorized access to DNS servers, attackers can modify DNS settings to change the IP address associated with a domain name. The third method involves compromising the DNS settings directly on a user's computer or router, rerouting their DNS requests to corrupted DNS servers. All three variations result in users being redirected to fraudulent websites.

  - **Host-based Pharming** [101]: In host-based pharming attacks, the attacker seeks to manipulate the hosts file on a user's computer or the DNS configuration within a local network. This can be achieved in one of three ways. First, by altering the host file, the user's request for a legitimate website is redirected to a malicious one. Second, by targeting the DNS settings on a local network router, DNS requests from users connecting to that network are rerouted to malicious websites. Third, a malware pharming attack deploys malware that either modifies the DNS settings or the host file to achieve the same redirection of users to malicious sites.

- **Water holing** [81], [85]: While this technique can be highly effective and usually goes undetected by website blacklists or antivirus software initially, it is not easy to execute and requires a significant level of technological knowledge, often relying on an exploitable weak point. Consequently, it is rarely used. The primary goal is to infect a website with malicious code, targeting sites that the attacker knows their victim either frequents regularly, will visit soon, or is likely to visit. In addition to websites, other potential attack vectors include unsecured wireless LANs or mobile phone apps. Victims of these attacks typically do not suspect foul play because they trust the websites or apps they use. As a result, they are more likely to click on links provided by the attacker or download and execute malware planted on these platforms. Such attacks are often directed at high-security organizations that are difficult to infiltrate through conventional means. Notable instances include the compromise of the U.S. Council on Foreign Relations (CFR) website in 2012 through the Gh0st Rat exploit and the targeting of Ukrainian Government websites in 2017 to spread the ExPetr malware.

- **Ransomware** [51], [102], [103]: True to its name, a ransomware attack seeks to extort a ransom from the victim. The attacker typically gains access to the victim's PC or server through phishing techniques. Once access is achieved, the attacker encrypts the victim's files, either on the infected machine or across the network. Subsequently, the victim receives a message or encounters a pop-up window, alerting them to the security breach. The message informs them that they must pay a specified amount of money within a given timeframe to receive the decryption key. Failure to comply means their encrypted files will remain inaccessible forever. In some cases, particularly with variants like "Maze" [102], attackers may also exfiltrate the victim's data and threaten to expose it or sell it to the highest bidder. Payment is usually demanded in cryptocurrencies like Bitcoin, which offer a degree of anonymity, making it challenging to trace the attacker's identity.

  It might be surprising to learn that these types of attacks are not as rare or difficult to commit as one might think. Just as companies like Microsoft, Adobe, or Zoom offer their products through "Software-as-a-Service" models, continuously updating and patching them, hackers do the same with their tools. This is known as "Ransomware-as-a-Service" (RaaS). RaaS allows customers to use ransomware without requiring an in-depth understanding of how it operates. Depending on the subscription level, customers receive access to 24/7 support, online communities, documentation, and ongoing development. Payment structures vary, offering options like one-time fees, monthly plans, or even affiliate programs where developers earn a percentage of the ransom payments. Even if the ransom is paid, the consequences can be severe. In a study, over 40% of companies victimized by ransomware reported that some or all of their data was compromised or damaged in the aftermath.

- **Pop-up windows** [104]: These windows can suddenly appear on websites or on an infected PC. They can look like advertisements, claim that the victim has won a prize, or simply state that the session has expired, prompting the user to re-enter their credentials to log in again. In all cases, the user's machine may become infected, credentials can be stolen, or the user may pay for goods or services they will never receive.

    - **Scareware** [30], [105]: This is a distinct sub-category of pop-up windows designed to frighten the user. They often feature red, flashy warning signs, loud alert sounds, and symbols resembling police or official emblems. These scareware pop-ups inform the user that they have been caught downloading music, films, or games illegally, have been recorded watching explicit content via their webcam, or that their computer is infected. To resolve these supposed issues, users are instructed to pay a fine to avoid legal consequences, prevent the release of the supposed webcam recording, or, in the case of a virus warning, submit their credentials to supposedly receive assistance.

- **File Masquerade** [79]: This technique abuses the user's inherent trust in files present on their network, PC, external hard drives, and other hardware. The attacker strategically places deceptive files in these locations, waiting for victims to execute them. This technique can be combined with a spoofed email, possibly from the user helpdesk, instructing victims to run these files under the guise of necessary patches. Alternatively, it can be employed in conjunction with the baiting technique, where a corrupted file is placed on a USB stick disguised as a promotional gift.

It should be evident at this point that social engineering attacks present a significant threat to companies across various sizes and industries. Even the most robust security measures can potentially be circumvented if the attacker selects the appropriate attack pattern, taking into account the overall context and their objectives as a social engineer. Therefore, it is crucial to confront these challenges, educate staff about the lurking threats, implement supporting security procedures, and prepare for the worst-case scenario in which all security measures are breached by the attacker.

To provide a more comprehensive overview, Table 1 serves as a concise summary of the attack patterns available to social engineers, categorizing them for better understanding. Sub-variants of attacks have been omitted, as they typically share common characteristics with their parent patterns.

The following table is divided into the three attack classifications discussed in Chapter 2.4. The column labeled "Socio-Technical Based" has been introduced to emphasize attacks that involve a combination of social and technical elements, highlighting the interplay between human actions and technical aspects in their execution. In cases where an attack can be executed through multiple methods, such as reverse social engineering, it can be categorized as either purely social-based if it occurs in real life or socio-technical-based if it is carried out through online channels like a chatroom. This distinction captures the multifaceted nature of these attacks.

	Human-Based	Computer-Based	Human- or Computer-Based	Technical-Based	Social-Based	Socio-Technical-Based	Physical-Based	Direct-Based	Indirect-Based	Direct- or Indirect-Based
Shoulder Surfing	X				X		X	X		
Manipulating Conversation	X				X			X		
Tailgating	X						X	X		
Piggybacking	X				X		X	X		
Impersonating	X				X			X		
Quid pro Quo	X				X			X		
Face to Face Interaction	X				X			X		
Grooming	X				X	X		X		
Reverse Social Engineering	X				X	X		X		
Diversion Theft			X	X	X	X	X			X
Dumpster Diving	X						X		X	
Eavesdropping			X	X			X		X	
Open-Source Reconnaissance	X			X			X		X	
Phishing		X				X			X	
Trojan Attack		X				X			X	
Baiting	X						X		X	
Pharming		X		X					X	
Water holing		X		X					X	
Ransomware		X				X			X	
Pop-Up Windows		X				X			X	
File Masquerade		X				X			X	

Table 1: Overview of the Attack Categorizations

Notes on Diversion Theft: This attack exhibits a high level of complexity, involving various channels, which makes it challenging to classify strictly as a physical, technical, or social-based attack. Its primary objective is physical in nature, as it aims to steal or replace an item. However, the attack incorporates a social-based component, where the attacker must convincingly interact with both the delivery driver or warehouse personnel and the victim. Moreover, it can be regarded as socio-technical if information gathering involves the use of a fake online survey. In some cases, it may even be classified as technical-based, particularly when the attacker manipulates delivery information to redirect the parcel elsewhere. If this is the case, the attack may no longer necessarily be categorized as human- and direct-based, as neither the victim nor the delivery person has possibly had direct contact with the social engineer.

3.2 Example of an Attack

To demonstrate how easy and straightforward it can be to carry out an attack, we will walk through an example attack. In this scenario, our objective is to execute a phishing attack, which is one of the most commonly encountered attack vectors and often serves as a gateway to more advanced attacks. Specifically, we aim to steal user credentials for PayPal. Depending on the target and the website for which these credentials are intended, they could be used in subsequent stages of a multi-layered attack, such as in a pharming attack. Alternatively, they could be exploited directly to steal money or access sensitive information. For this attack demonstration, we will utilize the Social Engineering Toolkit (SET), a tool that comes pre-installed in Kali Linux. Kali Linux is an operating system based on Debian Linux and is specifically designed for penetration testing purposes. It offers a wide range of tools for analyzing, testing, and exploiting system vulnerabilities. Kali Linux is an open-source project funded and maintained by OffSec and is widely used by both cybersecurity professionals and enthusiasts alike [12], [46].

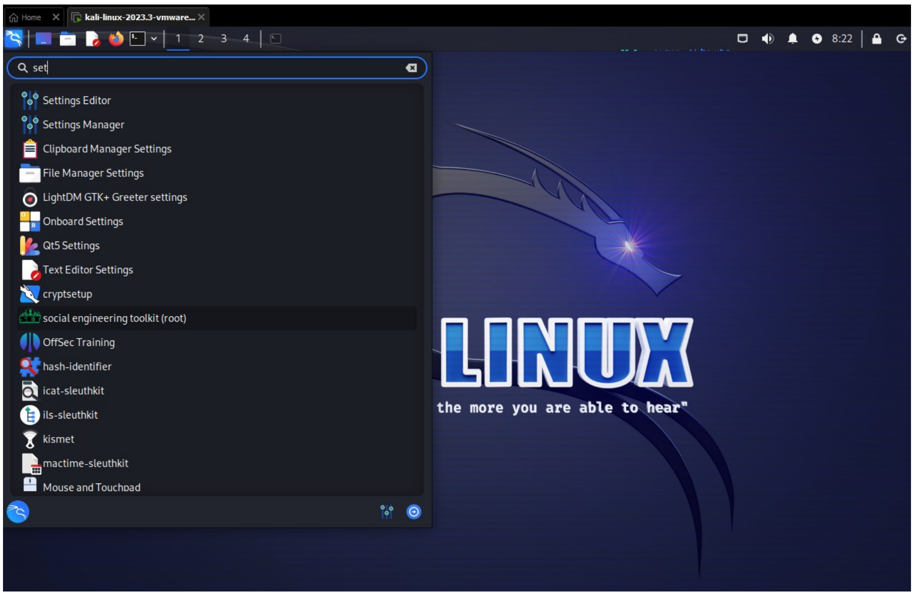
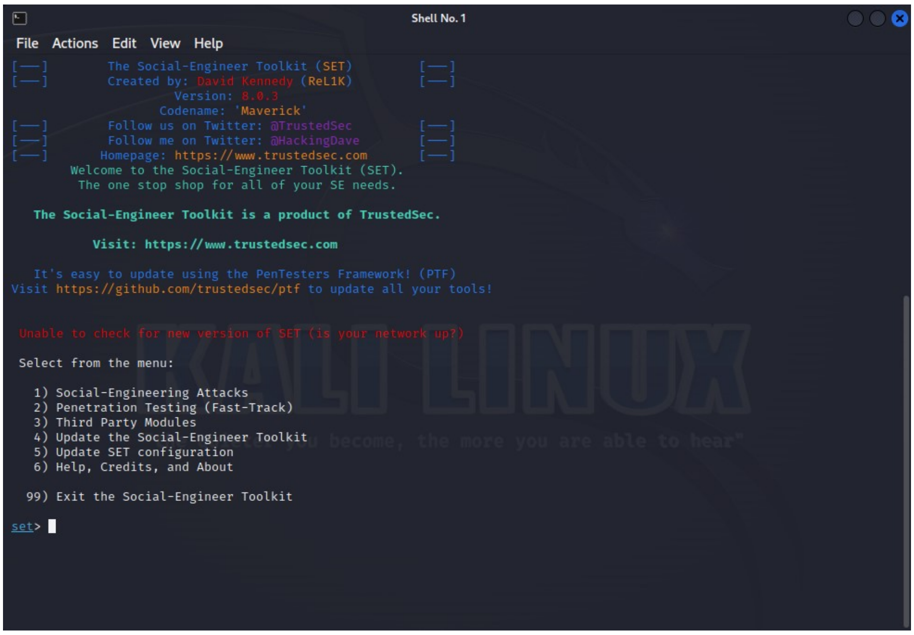


Figure 6: User Interface of Kali with the Preinstalled Social Engineering Toolkit

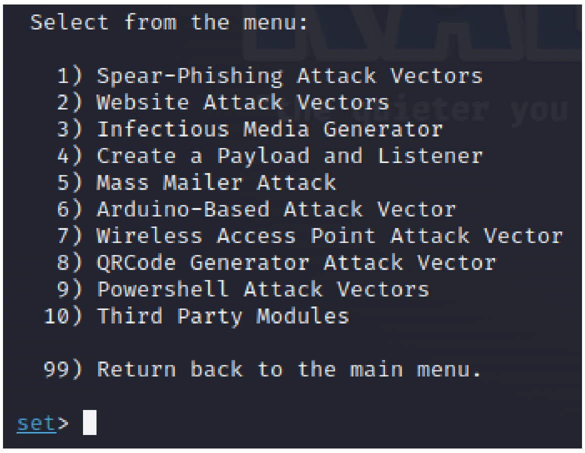
Using Kali Linux is straightforward and can be accomplished without significant expertise in the field. An easy-to-follow guide leads the user through the installation process. In our case, we installed Kali Linux on a virtual environment running Windows 11 using VMware. Once Kali Linux is launched and the user logs in with the provided credentials, they are presented with a graphical user interface displaying the Kali desktop. To initiate the Social Engineering Toolkit (SET), all that remains is to search for "set" in the home menu and click on "social engineering toolkit (root)" (see Fig. 6).



```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Unable to check for new version of SET (is your network up?)

 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 
```

Figure 7: The Social Engineering Toolkit - For our purposes, we need to select "1"

Upon launching SET, a shell opens, presenting a menu with six different options, along with the option to exit SET (see Fig. 7). For our purposes, we will select option one.



```
 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 
```

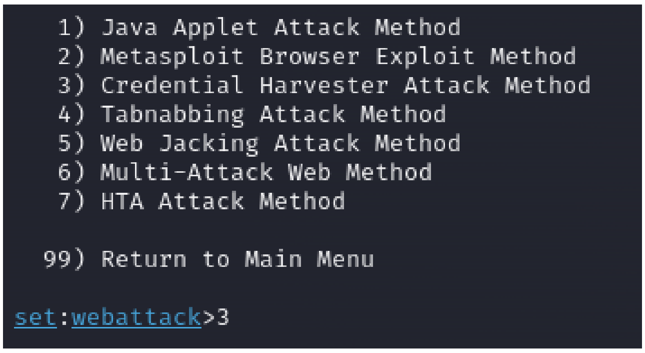
Figure 8: The Different Available Attacks

Figure eight displays the available attack vectors after launching SET. Before we proceed with creating our phishing attack, we will explore some other notable attacks that we have talked about previously and are made remarkably easy through SET.

In module one, we have the ability to create a spear-phishing email, which can be sent to a single person or to a list of targeted email addresses. Unlike sending a link to a cloned malicious website, this module allows us to create and attach a payload to the sent email.
For example, we can use a pre-made attack that includes a PDF file, which can be either an empty one or one that we provide, and inject it with an embedded EXE file. Alternatively, we can provide a custom-written DLL Hijacking attack vector, among other options.

Module three, for instance, can be employed in a baiting attack. It enables us to generate an autorun.ini file and a Metasploit file to place on an infectious CD/DVD/USB stick. When inserted into a PC with autorun enabled, it will automatically execute and compromise the targeted system.

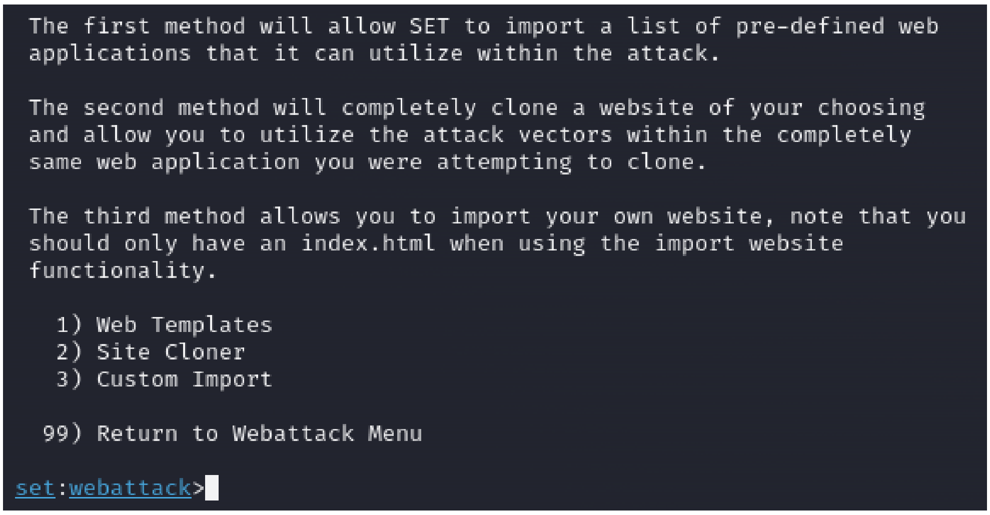
Another noteworthy attack is found in module number nine. This module empowers us to create PowerShell-specific attacks. PowerShell comes pre-installed on all Windows operating systems from Vista onwards and offers the social engineer the capability to deploy payloads and execute functions that often bypass preventative security technologies.



```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

Figure 9: Website Attack Vectors

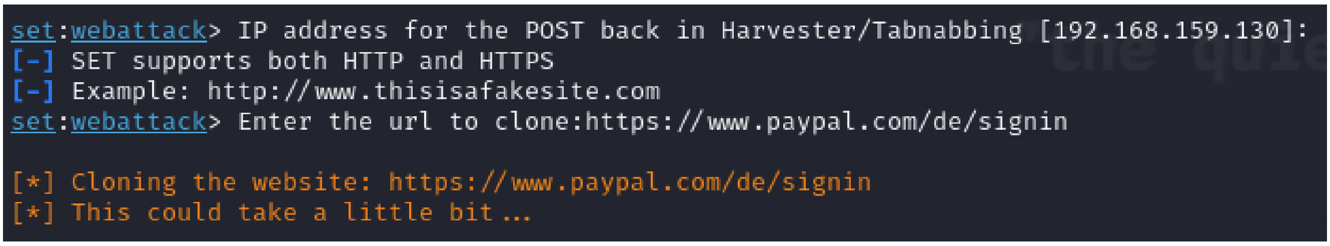
However, for our specific purpose, we will utilize option two (see Fig. 9), the "Website Attack Vectors" module. This module enables us to clone a legitimate website, redirecting any information entered in the username and password fields to an IP address of our choosing.



```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>
```

Figure 10: Credential Harvester Attack Options with Explanations

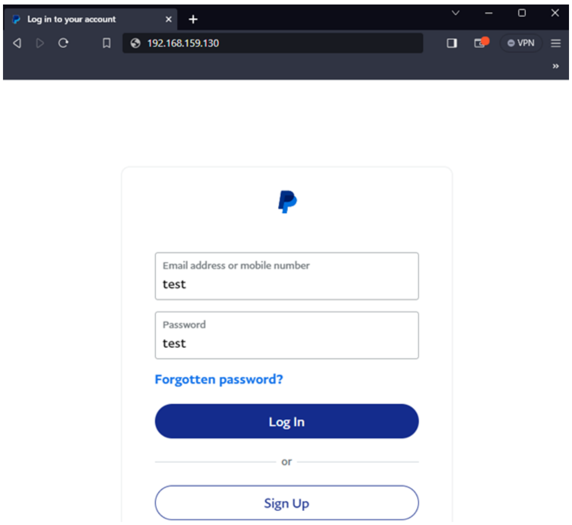
The last thing we have to choose is what website we want to target. Figure 10 shows the three possibilities, either web templates which are a selection of some popular sites like google or twitter, the site cloner option where we provide an URL ourselves, or even our own website. Additionally, Figure 10 showcases how SET gives an explanation to each selection so that it is not necessary to have prior knowledge in order to make a decision. All previous selections have these explanations as well but were omitted here.



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.159.130]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.paypal.com/de/signin

[*] Cloning the website: https://www.paypal.com/de/signin
[*] This could take a little bit...
```

Figure 11: The Last Step, Providing IP and URL

Finally, the last step involves specifying the IP address to which the entries from our fake website will be sent. SET does detect the currently used IP address automatically, but alerts the user to provide an external IP. This is essential to ensure that the malicious link can be accessed by the outside world, rather than just the local network. One can achieve this easily by using a tool like "ngrok" [106], although we will not delve into that here.



192.168.159.130

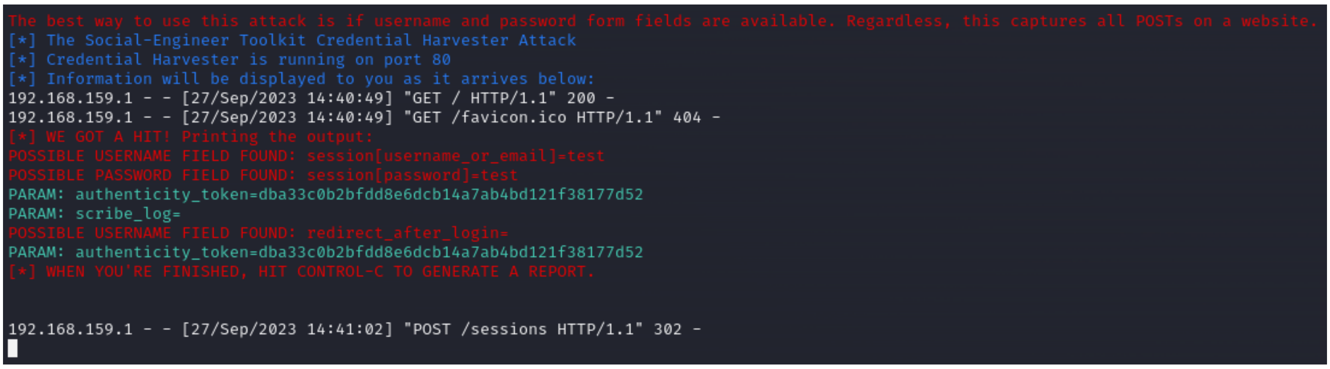
Email address or mobile number
test

Password
test

Figure 12: The Copied Website Looks Exactly Like the Original

With that in place, all that is left is to provide the link to the website you want to clone – in this case, PayPal. The attack is now ready to be executed. To do this, one would first take the previously provided IP address or ngrok link. Next, craft a convincing email, perhaps posing as PayPal customer support and mentioning a recent transaction error that requires the user to log in and resolve the issue. Insert the IP address into the email, but instead of merely displaying the IP address, change the wording to something like "click here to resolve the issue," and then send the email.

To enhance the chances of success, a social engineer may select a target they know has recently used PayPal. They can acquire this information through various means, such as conducting a deceptive survey regarding buying behavior and enticing victims with the chance to win a prize if they provide their email for winner notifications. Alternatively, another approach could be making a purchase on an online marketplace while using PayPal as the payment method. In both cases, the attacker not only acquires the victim's email address but also gains insights into their recent PayPal activities, including specific details such as the name of the marketplace involved. These precise details, typically known only to the buyer, seller, and PayPal customer support, add an extra layer of authenticity to the phishing attempt, making it highly convincing.



```
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.159.1 - - [27/Sep/2023 14:40:49] "GET / HTTP/1.1" 200 -
192.168.159.1 - - [27/Sep/2023 14:40:49] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=test
POSSIBLE PASSWORD FIELD FOUND: session[password]=test
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.159.1 - - [27/Sep/2023 14:41:02] "POST /sessions HTTP/1.1" 302 -
█
```

Figure 13: Entries by a Victim Will Be Displayed in Real-Time

Once a victim clicks on the link, SET promptly notifies the attacker and displays the entries for both the username and password fields. This notification continues until the attacker decides to terminate the process. To conclude the attack and compile all gathered data, the social engineer can simply press Ctrl + C. This action not only closes the running attack but also generates a report containing all the collected information.

After collecting the data, the social engineer would likely wait for a few weeks or even months before executing the attack. This delay serves to reduce the likelihood of the victim discovering the connection between the survey or PayPal transaction and the theft, thereby preventing them from explicitly reporting it to the authorities. During this waiting period, the victim is likely to engage in several other transactions, making it even less likely for them to single out the transaction with the attacker as suspicious, as it becomes just one among many.

Furthermore, the attacker may also employ a PayPal account created using a false identity. In the event that the transaction with the attacker is investigated, this additional layer of deception adds a level of security for the attacker, further reducing the risk of being identified or caught.

This marks the conclusion of our example illustrating an attack. It is crucial to recognize that all the information presented here is readily available to anyone through a simple search engine query and demands only minimal technical expertise to execute. It is paramount to grasp that these attacks are relatively straightforward to carry out, yet they wield immense destructive potential. Moreover, in the case of phishing attacks, they can serve as a gateway to more advanced forms of exploitation that can also be executed using tools like SET. This underscores the importance of awareness and robust cybersecurity measures to safeguard against such threats.

4 Psychological Aspects

Before delving into the concrete defense mechanisms and strategies in the next chapter, it is essential to examine the psychological traits and pitfalls that social engineers exploit through the previously shown attack vectors. Understanding the drivers behind people's decisions makes it easier to comprehend what social engineers attempt to manipulate, thus facilitating the design of more effective countermeasures. This understanding also plays a crucial role in creating awareness training programs, where it can be highlighted that attackers will seek to exploit these traits.

Similarly, these psychological factors must be taken into consideration during penetration tests and after a successful attack. For instance, feelings such as shame might deter victims from notifying the company's IT-security team after realizing they clicked on a phishing link. They might fear repercussions or being ridiculed by their colleagues. Addressing these emotional aspects is an integral part of comprehensive cybersecurity strategies.

4.1 Human Vulnerabilities

Human vulnerabilities are a crucial aspect that distinguishes social engineering from other cyber-attacks and hacks. These vulnerabilities represent the human factor exploited by social engineers to conduct their attacks. While it is possible to pair these human vulnerabilities with other factors, such as software vulnerabilities, it is not always necessary, as demonstrated in the previous chapter.

For instance, consider the "manipulating conversation" attack, where a group of attackers guides a conversation in a particular direction by revealing information about their passwords, hoping to exploit the victim's tendency to conform to the group's behavior. In contrast, there is the "water holing" attack, where a website frequented by the victim is injected with malware, exploiting their trust, carelessness, and reliance on mental shortcuts.

These vulnerabilities can be generalized and represented by four categories [84]:

1. **Cognition and Knowledge**
   Examples: ignorance, inexperience, thinking set, stereotypes, prejudices / bias, conformity, intuitive judgement, mental shortcuts, low level of need for insight

2. **Behavior and Habit**
   Examples: laziness / sloth, carelessness, thoughtlessness, fixed-action patterns, behavioral habits / habitual behaviors

3. **Emotion and Feeling**
   Examples: fear / dread, curiosity, anger / wrath, excitement, tension, happiness, sadness, disgust, surprise, guilt, impulsion

4. **Psychological Vulnerabilities**

The last category, psychological vulnerabilities, can be further divided into three sub-categories [84], [85]:

i. **Human Nature**
   Examples: self-love, sympathy, helpfulness, greed, lust

ii. **Personality Trait**
   Examples: conscientiousness, extraversion, agreeableness, openness, neuroticism

iii. **Individual Character**

Examples: gullibility, friendliness, kindness, charity, courtesy, humility, diffidence, apathy, hubris, envy

4.2 Addressing Common Vulnerability Exploits and Balancing Acts

This knowledge can be effectively applied by identifying the vulnerabilities that attackers most commonly seek to exploit because they are the most accessible to them. Additionally, it helps pinpoint the vulnerabilities that awareness trainings should prioritize in mitigating. To achieve this, Wang et al. [84] utilized the data they collected by constructing a domain ontology and subsequently creating a knowledge graph. This graph highlighted that the three vulnerabilities most frequently targeted across various attack methods are credulity, helpfulness, and conformity.

It is important to note that this does not imply that other vulnerabilities should be disregarded. Instead, it underscores the importance of giving special attention to them when designing and implementing defense mechanisms. Additionally, these findings might pose challenges for organizations, as they may lead to conflicting actions. While addressing credulity and conformity can be relatively straightforward through workshops and awareness campaigns focused on promoting mindfulness about data security, addressing helpfulness presents unique difficulties.

Discouraging employees from assisting each other is not a viable solution, as it would harm productivity and create an unpleasant work environment. Balancing the need for collaboration and helpfulness with the imperative of security awareness is a delicate challenge that organizations must effectively manage.

For instance, we consider a piggyback attack scenario. In this situation, an attacker may pose as someone who has forgotten their identity card and is unable to pass through a security door. They would then approach an employee with access rights who is passing through and request assistance.

One highly effective solution involves the implementation of specific technical measures in these areas characterized by high foot traffic or requiring enhanced security. These measures serve as supplementary protection, preserving positive employee attributes while safeguarding against potential exploitation. For instance, when addressing piggybacking, organizations can deploy singularization doors, permitting passage for only one person at a time, or opt for the implementation of biometric identification procedures.

In these security-enhanced areas, it is imperative to ensure that attackers cannot readily bypass these security measures by using an employee's access card that has been passed through the door. This situation can occur when a well-intentioned employee attempts to assist someone impersonating a fellow employee who claims to have forgotten their access card. Achieving this level of security is not only essential for effectively thwarting piggyback attacks, but also for preserving the integrity of access control, as well as the willingness to help one another.

4.3 Effect Mechanisms

The next point we need to examine is the concept of "effect mechanisms" [85]. These mechanisms provide insights into how specific consequences of attacks align with certain human vulnerabilities [84], explaining what, why, and how these vulnerabilities lead to particular outcomes. Depending on the attack scenario and the exploited human vulnerabilities, these mechanisms allow us to anticipate and, to some extent, predict the results of an attack.

We will consider an example to illustrate this concept. Imagine a new employee in a company who receives a call from an attacker posing as a member of the user helpdesk team. The attacker informs the employee that there was an issue with their user account setup and requests their credentials to log in and ensure everything is functioning correctly.

Here, the "impression management theory," which suggests that people aim to influence and control the impression they make on others, and the "reciprocity norm," which dictates that we feel obliged to reciprocate when others do something for us, come into play. The attacker anticipates that the employee will respond in a friendly and compliant manner, without many questions, in an effort to appear professional and helpful. This behavior stems from the desire to return the favor when the supposed user helpdesk employee offers assistance and checks their account.

As the example illustrated, effect mechanisms play a vital role in helping us comprehend why individuals respond as they do in specific scenarios and how attackers leverage psychological principles to attain their goals. These effect mechanisms draw upon principles and theories from various disciplines not commonly found in traditional cybersecurity, including sociology, psychology, social psychology, cognitive science, neuroscience, and psycholinguistics [84].

In their study, Wang et al. [85] identified and summarized six distinct aspects of these social engineering effect mechanisms. Below are these six aspects along with some provided examples:

1. **Persuasion**

   Examples: similarity in persuasion, liking in persuasion, helping in persuasion, distraction in persuasion, distraction in manipulation, source credibility, obeying to authorities, the peripheral route to persuasion, the central route to persuasion

2. **Influence**

   Examples: group influence, group conformity, normative influence (social validation), informational influence (social proof), social exchange theory, reciprocity norm, social responsibility norm, moral duty, self-disclosure, rapport and relation building

3. **Cognition, Attitude and Behavior**

   Examples: impression management theory, cognitive dissonance, commitment and consistency, foot in the door effect, bystander effect, diffusion of responsibility, deindividuation in group, time pressure, thought overloading, scarcity leading to a perceived value and arousing fear

4. **Trust and Deception**

   Examples: trust, risk taking, factor affecting trust, factor affecting deception, interpersonal deception theory (IDT)

5. **Language, Thought and Decision**

   Examples: relation between language and thinking, framing effect, cognitive bias, language invoking confusion: induce and manipulation

6. **Emotion and Decision-making**

   Examples: neurophysiological mechanism of emotion and decision, emotions and feelings influencing decisions, facial expression

4.4 The Crucial Factors to Influence People

While all the strategies belonging to the aforementioned mechanisms are crucial in social engineering attacks, some are more frequently utilized than others due to their notable influence on individuals. Although there is some disagreement among researchers and in the literature [15] regarding how to categorize these mechanisms, there is a general consensus on the strategies that have the most substantial impact on shaping someone's decisions and opinions. These strategies are primarily based on the work of Cialdini [17].

They are vital for the social engineer as influencing their victim is the main goal of most, if not all, social engineering attacks. Whether it is convincing someone to click a certain link or to hold open a door, understanding these strategies is a crucial step toward comprehending the factors that drive people to act in specific ways. This understanding, in turn, helps in designing and selecting the appropriate security measures based on potential victims and the specific situations in which these strategies are employed.

The six principles of influence, as described by Cialdini, are reciprocation, commitment, social proof, liking, authority, and scarcity. Following is an explanation of these terms and how they can be utilized by a social engineer:

1. **Reciprocity**

   As previously mentioned when discussing the reciprocity norm, the concept of reciprocity suggests that humans, whether by nature, upbringing, or societal norms, feel compelled to return a favor when they receive one from the same person. From a young age, children are taught that repaying kindness is the right thing to do, and on a broader scale, this contributes to the well-being of society. People often experience a sense of indebtedness when they receive a favor, even if it was unsolicited or unwanted, and they seek ways to alleviate this debt [17].

   This inclination to reciprocate favors can limit people's freedom to choose to whom they want to owe a favor. In order to relieve the discomfort of indebtedness, individuals may even agree to unequal exchanges [8]. Furthermore, this principle extends beyond material favors or actions and can encompass the exchange of information and knowledge. Additionally, there are other factors that can influence the effectiveness of the reciprocity norm. For example, the time delay between receiving a favor and having the opportunity to return the favor plays a role. As the time span between the two actions increases, the likelihood of taking the opportunity to reciprocate decreases [8].

   This behavior can be exploited by attackers using the foot-in-the-door (FITD) [87] and door-in-the-face (DITF) attack vectors [88]. Both techniques leverage the reciprocity norm but from different perspectives.

   In a FITD attack, the social engineer makes a small request after doing the victim a small, possibly unsolicited favor. The favor is designed to be small and easily fulfillable, and it is likely that the victim complies with the request to alleviate their feeling of indebtedness. The attacker's goal in this case is not to have the favor itself fulfilled, as it may be unrelated to the main attack, but rather to establish a social bond with the victim. This phenomenon of building connections through incremental agreements is referred to as "successive approximations" [8] and is exploited by the attacker. The actual attack follows when the attacker asks for a second favor, potentially a larger one. In this request, the victim feels obligated to fulfill it as well, justifying it to themselves by their favorable view of the requester.

   In a DITF attack, on the other hand, the attacker initiates with a large and unrealistic demand or request that the victim is highly likely to reject. Similar to the FITD attack, this initial request is not the actual objective of the attacker. After the victim's refusal of the first request, the attacker presents a second, much more reasonable request, which is the actual goal, such as obtaining specific information or assistance. The act of declining the initial request triggers feelings of obligation [8], as the attacker appears to compromise from their initial demand. This strategy is also commonly employed in marketing, where products are initially priced at a significantly higher rate, only to be seemingly discounted later [107].

Both the FITD and DITF strategies are effective in social engineering, as demonstrated in a previous example. In that particular study, Happ et al. [36] conducted an experiment in which they asked passersby for their passwords as part of their research. Some participants were offered a piece of chocolate either at the beginning of the interaction or shortly before being asked for their password. Alarmingly, 29.8% of participants revealed their password even without receiving chocolate. The reasons for this behavior may be related to Cialdini's other five principles of influence [17], although Happ et al.'s study did not delve further into this aspect. Meanwhile, 39.9% of participants disclosed their password when offered a piece of chocolate at the beginning, and an astonishing 47.9% did so when they received the chocolate right before being asked for their password. This study highlighted the effectiveness of reciprocity and the significant impact that timing can have [36].

2. **Commitment**

The principle of commitment, as described by Cialdini [17], highlights the human tendency to desire consistency in how they are perceived by others. Consequently, individuals are more inclined to continue and reinforce their actions after they have publicly committed to them. This inclination can be exploited by social engineers through a concept known as the "escalation of commitment." First introduced by Barry M. Staw in 1976 in his study "Knee-deep in the big muddy: a study of escalating commitment to a chosen course of action" [78], it characterizes a behavior where a group or individual faces increasingly negative outcomes resulting from a decision, action, or investment they have made, yet persist in that course of action. This persistence can be explained by people aligning their self-image with their commitment to a particular choice.

One illustrative example can be found in the world of business auctions. Some individuals are willing to continually increase their bid, even surpassing the initial value they were comfortable with, simply to secure the item and maintain consistency in their decision in front of others in the room. At this stage, it becomes a matter of personal principle rather than a rational investment [66].

To exploit this behavioral pattern, a social engineer may induce the victim to take an initial position, which they can later capitalize on by indirectly requesting it again [45]. For instance, the attacker might pose a small, easily answerable question to the victim, one they are likely to respond to. Subsequently, as the social engineer continues to pose questions, the victim, to maintain consistency with their helpful behavior and decision to assist the requester, will commit to answering those questions as well. The questions then will gradually shift toward what the attacker actually wants to know. By holding the victim accountable for their commitment, the attacker is more likely to obtain the desired answer.

Another scenario involves exploiting commitment to gain access to otherwise restricted premises. The attacker might pose as an individual struggling to carry multiple items and request the victim's assistance. In doing so, the victim is successfully induced to adopt the initial position of helping. Consequently, when the attacker later asks the victim to open a specific door and hold it open, claiming they have their hands full, the victim is more likely to comply due to their prior commitment. This can also be combined with the FITD technique where the victim receives a favor from the attacker and is then asked for a favor in return. If they comply, the victim likely continues to agree to the attacker's following requests, remaining consistent in their behavior.

3. **Social Proof**

People often exhibit a tendency to imitate the behavior of others, particularly when they are uncertain about how to act or when they perceive the individuals they are observing as similar to themselves. This inclination to conform to the actions of others is a well-documented aspect of human behavior.

A famous example illustrating this phenomenon comes from a 1960 TV episode of Candid Camera titled "Face the Rear". In this episode, there was a person already inside an elevator, whom we will refer to as the "occupant". As subsequent actors entered the elevator, they selected their desired floor and then turned to face the back of the elevator, contrary to the usual practice of facing the doors. Over time, the occupant, who initially faced the elevator doors, became aware of the divergent behavior of the others. They began to shift uncomfortably, checked their watch multiple times to avoid appearing conspicuous, and eventually turned around to face the rear, aligning their behavior with that of the actors. This experiment was repeated multiple times with consistent results, highlighting the powerful impact of this tendency to conform to others' actions on human behavior [108].

This scenario was initially portrayed in a TV sketch, but it draws inspiration from Solomon Asch's groundbreaking conformity experiments [5]. Asch's experiments delved into the psychology of group conformity, revealing a crucial aspect of human behavior. While it is evident that individuals can easily conform to a group's behavior, they can just as readily break away from it when sufficiently motivated. The presence of a single dissenting individual can stimulate others within the group to express their independent thoughts.

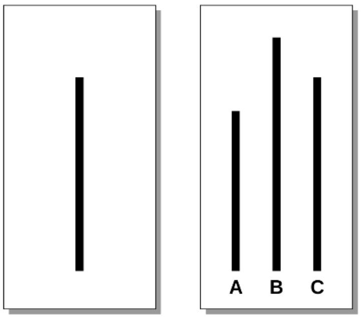


Figure 14: One of the Card Pairs Used in Asch's Experiments [5]

In Asch's original experiments, a group of participants was presented with two pictures (see Fig. 14). One picture displayed three lines of varying lengths, while the other featured a single line. The task was straightforward: determine which of the three lines in the second picture matched the length of the single line in the first picture. The correct answers were apparent, but there was a twist. The actors, who were part of the experiment, purposefully provided incorrect answers. Also, the actors were always first to answer and the unknowing participant last.

Despite the obvious correctness of the answers, participants who were unaware of the actors' true intentions often followed the lead of the actors and gave incorrect answers themselves in approximately 35.7% of the cases, compared to just 0.7% if asked in privacy [5]. In 1965, Solomon conducted another experiment that resulted in an astonishing 75% of the participants conforming to the majority [13]. However, in some variations of his line-comparison experiment, one of the actors provided the correct answer. Remarkably, this single act of dissent led to a significant reduction in group conformity among the unaware participants. They were more inclined to provide correct answers themselves, highlighting that even a lone individual can exert influence within a group by offering a different perspective or challenging the prevailing consensus [6].

This has serious implications for social engineering attacks. Attackers can exploit the need for conformity through fear-based attacks that rely on putting the user in a state of anxiety, pressure, stress or fear [55]. In these scenarios, the victim is placed in an uncomfortable position where they are told that they are the only person not helping as others have done. For instance, this could be employed to extract the user's login credentials. The attacker may pose as a new employee in the user helpdesk who claims to have made an error and needs the credentials to rectify the situation which could have dire consequences otherwise.

Another approach is to combine this technique with a phishing email, where the victim is informed that they are one of several lucky winners. The other winners have already claimed their prize by clicking on a provided link, and all the victim needs to do to receive their prize is to click the link as well. Additionally, there is a human-centered and direct attack method that we previously explored in our chapter about the different attacks themselves, known as the "manipulating conversation" attack. In this scenario, a group of attackers initiates a discussion about their login credentials, expressing doubts about the security standards. Their objective is to coax the victim in the group into revealing their credentials. All of these attacks are made possible through Cialdini's third principle of influence, social proof.

4. **Liking**

The fourth principle is summarized by Cialdini under the term "liking". This encompasses not only that we tend to like people that share the same interests or lifestyle as us, use flattery and compliment us or appear familiar. This is also the case for people that appear to work toward a common goal.
By simply being liked, it is more easily possible to convince others of our ideas [17].

However, the most critical factor in obtaining initial favor may not be our words or actions, but our appearance, which has a significant influence. Studies indicate that physical attractiveness automatically triggers positive associations with other desirable qualities, such as talent, kindness, integrity, and intelligence [17]. This effect is commonly described as "halo effect" where one positive characteristic of a person dominates how that person is perceived by others.
In the case of looks, this is especially potent as the person does not have to say a single word or do anything to be perceived in a way that is favorable for them.

This phenomenon has been supported by several conducted studies, as presented in Cialdini's work [17]. For instance, one study conducted during the Canadian federal elections found that attractive candidates received more than two and a half times as many votes as their less attractive counterparts. Similar results were observed in studies related to hiring situations, where attractive and well-groomed applicants had a higher rate of success compared to their less attractive peers. Most notably, these findings extended to the legal system, where good-looking individuals were more likely to receive highly favorable treatment. In one study, seventy-four male defendants were rated by researchers based on their attractiveness. Those perceived as good-looking were twice as likely to avoid a prison sentence compared to their less attractive counterparts. This effect even applies to children, as misbehavior by good-looking children tends to be viewed as less severe, and their teachers often perceive them as more intelligent than their less attractive peers.

What is particularly concerning is that this seems to be a completely subconscious decision, as indicated by a follow-up study to the Canadian election [17]. In this study, 73% of voters vehemently denied that physical appearance had any influence on their decision regarding whom to vote for, while only 14% of voters acknowledged the possibility that looks might have influenced their decision.

These findings can be leveraged by social engineers across various attack vectors, but physical attacks tend to benefit the most from them. When social engineers contact their victims through digital means where they cannot be seen, they rely on creating a connection or emotional bond with the victim. To maximize the chance of success, prior research about the victim is necessary. By learning about their interests, hobbies, or lifestyle, the attacker can tailor a phishing attempt, introducing themselves as someone with similar interests or hobbies.

However, when social engineers have physical contact with their victims, they can exploit the "liking" effect more effectively. Similar to digital attacks, it is beneficial to know the victim's likes or what they take pride in. Pretending to share the same interests and engaging in conversations about these topics can foster a sense of liking and connection. Claiming to work toward common goals can also enhance the likability factor.

According to Asch, the most significant influence can be achieved through one's appearance, capitalizing on the previously mentioned halo effect [5]. By presenting themselves as well-groomed and well-dressed, social engineers can enhance their chances of influencing the victim. This effect becomes even more pronounced when the attacker attempts to influence a victim of the opposite sex.

This phenomenon is particularly evident when a female member of a group of attackers is chosen to conduct the attack on a male victim, or when a female attacker operates independently in an attack on a male victim. According to Alastair Davi et al.'s study, "Exploiting the Beauty in the Eye of the Beholder: The Use of Physical Attractiveness as a Persuasive Tactic" [19], young women are especially successful in persuading members of the opposite sex. While men can also leverage their looks with female targets, women tend to receive significantly higher success ratings compared to male attackers.

In general, human-based attacks are most effective in leveraging the "liking" factor as an influential factor. Combining physical appearance with flattery and the ability to initiate casual conversations in a friendly manner makes this strategy a powerful tool in social engineering.

5. **Authority**

The next principle of influence by Cialdini that we will examine is authority. This principle describes how people tend to obey authoritative figures, even when tasked with questionable or immoral actions. As an example, Cialdini cites the atrocities committed by soldiers who claimed to have "just followed their orders" [17].

Another example is the experiment conducted by Milgram in 1961 [57] in response to the Nuremberg Trials, which we will examine next. This experiment aimed to observe destructive obedience in a laboratory setting. The study's structure was as follows: an Experimenter (E), portrayed by an actor serving as the authority figure, issued commands to a Teacher (T), a role taken on by the test subject. The Teacher's task was to read word pairs from a list to a Learner (L), who was situated in a different room and also portrayed by an actor. The Teacher was then instructed to ask the Learner to identify the matching word for a given word. If the Learner provided the wrong answer, the Experimenter instructed the Teacher to administer increasingly severe electric shocks through a machine, with the voltage increasing with each incorrect response.

However, in reality, there were no electric shocks. The Teachers were led to believe that the Learners were experiencing severe pain, as they cried out in agony as the voltage levels in the experiment increased. Even when the Learners begged for the experiment to stop and refused to answer any more questions, the Experimenter insisted that the Teachers continue. Starting with 15 volts and increasing in increments of 15 volts, 65% of the 40 participants went on to deliver the maximum shock strength of 450 volts. The first Teachers who refused to continue with the experiment did so at the 300-volt level, which was already 60 volts higher than what Milgram had initially expected as the highest level of obedience. At 300 volts, the Learner would start kicking the wall and no longer provide answers. At 420 volts, the machine displayed a label that read "Danger: Severe Shock."

While this experiment faced significant criticism and raised numerous moral and ethical questions about its conduct, it yielded two surprising findings according to Milgram. The first was the sheer strength of obedience displayed by the test participants, even though they had learned that hurting another human being was a fundamental breach of morality and contrary to what they had been taught since childhood. This is especially concerning considering that the subjects had nothing to fear themselves if they disobeyed, nor would they gain any material benefits by continuing. The second finding was the extreme responses of the participants noted by the observers who did not expect the observations they made during the experiment. Many of them expressed disbelief when a test participant administered the next shock, even though they were fully familiar with the experiment and had a deep understanding of the situation, yet they underestimated it completely. One observer noted the following:

> *"I observed a mature and initially poised businessman enter the laboratory smiling and confident. Within 20 minutes he was reduced to a twitching, stuttering wreck, who was rapidly approaching a point of nervous collapse. He constantly pulled on his earlobe, and twisted his hands. At one point he pushed his fist into his forehead and muttered: "Oh God, let's stop it." And yet he continued to respond to every word of the experimenter, and obeyed to the end."* [57]

These findings have significant implications in regards to social engineering. An attacker who convincingly poses as an authoritative figure, adopting a similar demeanor, corresponding tone, and appropriate attire, can effectively demand obedience from their victim with a high rate of success. Authoritative figures in a corporate context can take on various forms and may not be easily identified as impostors. Such attackers could impersonate higher-ranking employees, influential clients, security personnel, or even public authorities such as the police. This principle applies to both human-based and computer-based attacks. For instance, an attacker might impersonate the CEO who claims to have forgotten a crucial document during a business trip and instructs an employee to send a copy via email. Similarly, certain malware programs exploit victims' fear by displaying police logos, falsely accusing them of downloading pirated files and demanding money as a fine. This authority principle can also grant access to otherwise restricted areas by simply commanding an employee with access rights to comply without question.

Milgram's findings highlight a second aspect that we explored when examining Mouton et al.'s attack framework in Chapter 2.2, specifically the importance of the debriefing step.

Pressuring victims to obey commands, especially when these actions breach moral, ethical, or company regulations, can have psychological consequences on the victims [63]. Individuals are well aware when they are acting against their moral and ethical principles or company policies, and they may respond to this stress in various ways [57]. Therefore, it is crucial for the social engineer to ensure that the victim feels they have acted in accordance with the right course of action, even when handling a situation in breach of specifications. This approach helps prevent the victim from questioning the legitimacy of the incident and discussing it with others, potentially exposing the ruse.

For example, in the case of the CEO calling the employee, a follow-up call could express gratitude, stating that their actions helped secure a significant deal. Similarly, in the case of a pop-up logo demanding a fine under the guise of the police, a notification could be sent claiming that the fine has been paid and that no further actions will be taken against the victim.

Attackers can also exploit the effect of shame on people, inducing a fear of being devalued by others due to their actions against ethical, moral, or company policies. This fear often deters victims from seeking help or discussing the situation with others [30].

6. **Scarcity**

Cialdini's final principle of influence, scarcity, explores how limited quantity and availability affect people [17]. The concept is rooted in the psychological phenomenon known as the "fear of missing out" (FOMO), which leads us to believe that items in short supply are more valuable and desirable. Consequently, we are more likely to make a purchase if we are told it is the last one available, or to reserve a hotel room if it is the last one left for example, driven by the fear that we might miss a great opportunity.

Cialdini provides a deeper understanding of how scarcity influences us [17]. Firstly, the perception of limited quantity appeals to our sense of exclusivity, making the item appear rare and thus more attractive. Secondly, time limitations create a sense of urgency, prompting quick action. The next critical aspect is competition. When people know that others are interested in the same item, it motivates individuals to secure it for themselves. This phenomenon is commonly observed in auctions or on websites that display both the number of items left and the number of users currently viewing the product.

The fourth key aspect is what Cialdini terms "psychological reactance". When people feel that their freedom to choose is being restricted, they tend to desire the item or service more. It is essentially the idea of "you cannot have it", which amplifies its desirability.

Another essential aspect is how scarcity interacts with other principles, particularly social proof. When others appear to want an item, it reinforces the idea that the item must be valuable because so many others have purchased it, and only a few are left. This creates a sense of competition and urgency, pushing people to act quickly.

The final aspect is loss aversion, which is a powerful motivator. The fear of missing out on something scarce often outweighs the desire to gain something of value. This principle plays on our innate aversion to losing out on opportunities, even if they might not have significant material value.

In essence, scarcity leverages our innate desire to acquire something rare, which we often associate with greater value. This strategy is versatile and multifaceted, manifesting in various forms. It is usually employed by shops, salespersons, and social engineers alike.

Social engineers frequently utilize scarcity in phishing emails. Their goal is to make their offer appear legitimate, disguising themselves as a typical salesperson or service provider. These deceptive advertisements aim to exploit several key aspects outlined by Cialdini, including creating time pressure for decision-making, offering exclusive items, generating competition among potential customers for these items, or providing limited information about the products. These tactics encourage victims to investigate further by clicking on provided links.

For example, a victim might receive an advertisement promising a miraculous new weight-loss pill, but claiming that only a few remain in stock, or they may receive an offer of a free trip limited to the first ten respondents. To claim the promised reward, the victim is urged to click a link, which ultimately leads to a malicious website. This approach preys on the "fear of missing out", manipulating the victim's desire to secure these seemingly valuable opportunities quickly, despite their questionable authenticity.

Scarcity tactics are not restricted to digital means; they can also be integrated into direct-based approaches. In phone calls, victims might face intense pressure to make immediate purchases or risk forfeiting the opportunity. In some particularly devious calls that are being combined with Cialdini's authority principle, typically targeting more vulnerable individuals, such as the elderly, scammers posing as the police fabricate scenarios involving a family member causing an accident. They insist that the victim must act swiftly, such as posting bail, to avoid dire consequences for the family member. In such cases, the scammers adeptly leverage the fabricated authority figure's time-sensitive demand, preying on the victim's anxiety as well as their fear and obedience [22].

This concludes our exploration of the influence of the human psyche on the victims of social engineering attacks and how these psychological factors can be manipulated. To summarize, we initially delved into the array of vulnerabilities inherent in human nature. These vulnerabilities encompass fundamental traits that every individual possesses to varying degrees, which can be manipulated and exploited. Some of these vulnerabilities include ignorance, inexperience, fear, curiosity, guilt, helpfulness, greed, and lust.

Furthermore, we have delved into Wang et al.'s effect mechanisms [84], providing us with a framework that aids in categorizing and understanding how these vulnerabilities can lead to specific outcomes in social engineering attacks. By seamlessly combining distinct human vulnerabilities with various attack scenarios, this framework allows us to anticipate and to a certain degree predict the consequences of different social engineering attacks.

Additionally, our exploration encompassed an examination of Cialdini's work, "Influence: The Psychology of Persuasion" [17], which illustrated the six fundamental principles of persuasion that underpin most social engineering attack vectors:

- **Reciprocity**: The strategic act of giving to receive in return.
- **Commitment**: Exploitation of the human desire for consistency in decision-making, even when decisions yield unfavorable outcomes.
- **Social Proof**: Harnessing the inclination of individuals to find validation by imitating the actions of others.
- **Liking**: Capitalizing on the power of physical attractiveness and shared experiences to nurture sympathy and enhance the likelihood of receiving assistance.
- **Authority**: Manipulating individuals' tendencies to obey authoritative figures, even when tasked with unethical or immoral actions.
- **Scarcity**: Amplifying the perceived value of an item or service by framing it as rare, time-limited, or by evoking the fear of missing out.

These principles are the driving force of persuasive techniques in social engineering, forming the basis for persuading victims that the scenarios they confront are legitimate, often by exploiting their vulnerabilities, such as curiosity, greed, lust, or their desire to be helpful.

4.5 Demographics

In the subsequent sub-chapter, we will take a deeper look at the aspects regarding demographics that come into play in social engineering attacks. We already noted some specifics regarding demographics, namely during our investigation of Cialdini's influencing principles. We briefly talked about age, as elderly people are especially vulnerable to so-called shock-calls when abusing scarcity to persuade victims by claiming they need to act fast to prevent disastrous consequences [22].

In the subsequent phase of our exploration, we will delve into the various demographics frequently targeted by social engineering attacks, with a focus on the victim's side rather than the characteristics of the attackers. By examining studies conducted in this field, we aim to deepen our understanding of the intricate web of human behavior and manipulation in the context of social engineering. This exploration will help us identify particularly vulnerable groups and can subsequently assist in selecting and designing appropriate countermeasures and effective awareness training programs.

4.5.1 Study Overview

To understand the effects of gender, age, and profession on susceptibility to social engineering, several studies were consulted and their findings compared. The results, however, were largely contradictory. We will now examine some of these studies to better understand why such discrepancies may exist and to be able to compare their findings.

Goel et al. – "Got Phished? Internet Security and Human Vulnerability"

In this study by Goel et al. [31], a combination of experimental and survey methods was used to investigate vulnerabilities and factors contributing to successful phishing attacks. The researchers gathered data by creating fake phishing emails and websites to simulate real phishing attempts. They also administered surveys and questionnaires to participants who opened the phishing emails to collect information about internet usage behavior, awareness of phishing threats, and demographic details.

The findings revealed that while women were more likely to open and read the contents of phishing emails, there was little variation in the percentage of women who actually clicked the links compared to men who opened the emails. This suggests that women may be more curious about phishing emails but are equally adept as men at recognizing phishing attempts.

The study also explored the frequency of opening and clicking on links within phishing emails based on the participants' majors. The results showed that across various majors, including social, business, STEM, and humanities sciences, the rate at which phishing emails were opened and links were clicked was largely statistically insignificant. The only statistically significant deviation was that business (30.6%) and social (27.8%) sciences majors were more likely to open the emails than humanitarian sciences majors (23.8%). Interestingly, STEM sciences did not perform significantly better in spotting phishing emails, despite their involvement in the field with the most interaction with social engineering.

Li et al. – "Experimental Investigation of Demographic Factors Related to Phishing Susceptibility"

In the study by Li et al. [52], a similar approach was followed, involving fake phishing emails and landing pages. However, this study added a twist by sending a series of three waves of phishing emails with different content. The participants included university members, both students and staff.

In contrast to the findings of Goel et al., the results regarding gender in Li et al.'s study contradicted those of the former. While gender remained a small significant factor, men were more susceptible to clicking on phishing links compared to both genders clicking them equally.

Concerning age, Li et al. found that younger individuals (under 27 years) were more susceptible to financial phishing emails, while the oldest age group (over 59 years) was the most vulnerable across all three tested phishing email types. These email types included messages from the IT-Helpdesk notifying the user of suspicious activity, package delivery service failure, and a suspicious credit card charge.

However, the most significant predictor of susceptibility to phishing was whether a participant had been phished before. Those who clicked on a link the week before were significantly more likely than non-clickers to click on this week's and next week's phishing emails. Importantly, it is noted that those who clicked on all three links were also those who did not read and review feedback, which needs further examination. One possible explanation for this phenomenon is that individuals who are most susceptible to falling for phishing attacks might also be less inclined or unwilling to carefully read and evaluate feedback.

Halevi et al. – "Spear Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks"

In their study, Halevi et al. [34] focused on spear-phishing attacks. Participants were lured to a fake website, where they were instructed by their company's IT manager to download a plugin. Notably, while 62.5% of the participants followed the link, only 30% went on to download the plugin. Gender-based analysis revealed that approximately 27% of male participants downloaded the plugin, while a significantly higher percentage of female participants, around 40%, fell victim to the attack. This suggests that women may be more susceptible to spear-phishing attacks.

The study also unveiled other important insights. Conscientious individuals with low risk awareness were more likely to download the plugin, implying that authority and the appeal to efficiency could overcome participants' self-control. Additionally, participants with a high perception of risk in general and greater awareness of cyber-risks in particular were less vulnerable to phishing attacks, while those who underestimated the likelihood of cyberattacks or were unfamiliar with them proved to be more susceptible. Furthermore, the study found that participants struggled to accurately estimate their risk of falling for phishing attempts. Intriguingly, even individuals with a high computer-mediated competence (CMC) score did not necessarily exhibit a better ability to avoid falling for phishing attacks, a discovery we will revisit in our discussion of the findings.

Happ et al. – "Trick with treat – Reciprocity increases the willingness to communicate personal data"

We have previously explored Happ et al.'s study [8] when discussing the impact of reciprocity. In their study, passers-by were offered a piece of chocolate during a survey to assess whether this would increase the likelihood of them revealing their password information in return.

While both genders generally reacted similarly when approached, men appeared more susceptible to this technique under specific circumstances. When the chocolate incentive was presented at the beginning of the experiment or not at all, there was no significant difference in the percentage of men and women who disclosed their passwords. However, when the incentive was provided immediately before asking for the password, men were 1.23 times more likely to reveal their passwords compared to women. According to Happ et al., this might suggest that men might be more susceptible to social engineering.

Regarding age, Happ et al. discovered that younger individuals were more willing to share their password information compared to older individuals. One potential explanation is that younger people could more easily relate to the student interviewer, making them more susceptible to this social engineering tactic in this context.

4.5.2 Summarization and Discussion of the Findings

After a closer examination of the analyzed studies, it becomes apparent that there is no definitive answer regarding which gender, age group, or profession is particularly vulnerable to social engineering attacks. We will now rank and compare these findings, considering both the studies we have examined closely and those mentioned in section 4.5.1. In summary:

- According to Goel et al. [31], men and women were equally likely to fall victim to social engineering attacks.
- Li et al. [52] found that men were slightly more likely to be victims, although the difference was small but significant.

- In contrast, Mohebzada et al. [59], Mataracioglu and Ozkan [56], and Diaz et al. [23] reported that men were significantly more likely to be victims of social engineering attacks.
- On the other hand, Jagatic et al. [43], Sheng et al. [73], and Halevi et al. [34] found that women were more susceptible and reported statistically significant differences in victimization rates.
- Happ et al. [36] noted that young people were more susceptible to falling victim to social engineering attacks than older individuals.
- Conversely, [52] suggested that older people were more vulnerable to social engineering attacks than their younger counterparts.

	Men	Women	Both similar	Small significant differences	Significant differences	Young people	Old people	Both similar	Papers
Most vulnerable by gender			X						[31]
	X			X					[52]
	X				X				[23], [56], [59]
		X			X				[34], [43], [53], [73]
Most vulnerable by age					X	X			[36]
					X		X		[52], [53]
Most vulnerable by gender and age			X					X	[28]

Table 2: Overview of the Demographic Vulnerabilities Found by the Different Papers

These findings, summarized in Table 2, emphasize the complexity of understanding susceptibility to social engineering attacks and suggest that there is no one-size-fits-all answer regarding gender, age, or profession vulnerability. Several factors contribute to this variability in research outcomes.

First and foremost, it is important to recognize that not all social engineering attacks are alike. For instance, while phishing and spear-phishing attacks share the common objective of deceiving individuals for malicious purposes, they differ significantly in their execution and complexity. These varying tactics can result in different outcomes for distinct groups. The same principle applies to different variations of the same attack vector. For example, a shock-call targeting the elderly can have a more significant impact than on younger victims [22]. However, this cannot be generalized into assuming that vishing, as a specific type of voice-based social engineering attack, is universally more effective on the elderly than on the younger population. The effectiveness of vishing may vary depending on the specific topic or context of the attack. The variation in social engineering attacks tested could therefore be one explanation for the differing research outcomes.

Moreover, the participants in these studies were unique for each research endeavor. This diversity in participant groups makes direct comparisons between studies challenging. Differences in culture, ethical values, geographical locations, social status, and various other variables among participants from various backgrounds may significantly impact susceptibility. This assertion is reinforced by a study conducted by Hanus et al. [35], which revealed that various demographic characteristics, including age, salary, area of residence, nature of job position, and access to computers, played a role in affecting the probability of falling victim to phishing attacks.

Additionally, it is important to highlight a recurring implication that remains consistent across several studies: computer usage alone is an insufficient indicator of heightened cyber-risk awareness. For instance, in Goel et al.'s study [31], participants from diverse academic backgrounds, including those in STEM fields, exhibited similar susceptibility to social engineering attacks. This was unexpected, as STEM participants were anticipated to perform better in recognizing and resisting such attacks due to their familiarity with computers and cyber-related issues.

This aligns with findings from Halevi et al. [34], indicating that individuals who reported diverse internet use purposes were not necessarily less susceptible to phishing attacks. High computer-mediated competence did not serve as a protective factor against phishing. The inability of participants to accurately estimate their risk of falling victim to phishing attacks may explain this phenomenon, especially among those with low internet usage risk perception.

However, a person's overall awareness of cyber-risks had a positive impact on their susceptibility to phishing attacks [34], thereby decreasing the likelihood of falling victim to such attacks. This finding was supported by Flores et al. [28], who identified significant correlations between phishing behavior, participants' security awareness, their intention to resist social engineering, and their training. However, the strength of these correlations varied across different cultures. While there was only a limited correlation between the intention to resist social engineering and actual phishing behavior, as well as between security awareness and phishing behavior for American and Indian individuals, stronger correlations were observed among Swedish individuals. The connection between training and phishing behavior was more significant for Americans than Swedes, and non-significant for Indians. This indicates that the effectiveness of these factors in predicting phishing behavior may be influenced by cultural distinctions as well, further underscoring the complex nature of demographics in social engineering susceptibility.

In essence, the multifaceted nature of social engineering attacks, the diversity among participants, and the need for diversified security and awareness trainings, to educate as many employees as possible, highlight the need for a nuanced understanding of the factors contributing to susceptibility. To conduct a thorough assessment, the cybersecurity departments of companies should take into account the unique context and strategies used in each type of attack, as well as the diverse backgrounds, positions and traits of the employees involved.

Furthermore, these findings raise concerns about potential negative consequences when viewed from a certain perspective. Identifying a particular group as especially vulnerable to social engineering attacks, even if such a characterization is inaccurate, can have unintended and detrimental repercussions for these individuals.

For instance, if a group is unfairly labeled as more susceptible to social engineering attacks, it may encounter challenges in various aspects of life, such as employment opportunities. Employers might hold biases or stereotypes against individuals from this group, believing them to be less reliable or security-conscious. This could result in hiring discrimination, career limitations, or difficulties in accessing certain job positions [32], [86].

Given these implications, it becomes imperative for future research to adopt a comprehensive ethical framework. Researchers must not only examine the susceptibility of different groups but also consider the broader social and ethical consequences of their findings. This includes addressing potential stigmatization, discrimination, and biases that may arise from characterizing certain groups as more vulnerable. Ethical considerations should be an integral part of research in this domain to ensure that findings are responsibly interpreted and applied, and to prevent any unjust consequences for specific groups of people.

5 Defenses

In conclusion, our exploration has encompassed fundamental factors influencing susceptibility to social engineering. We initiated our examination by defining social engineering, analyzing attack patterns, and categorizing diverse attack vectors. Subsequently, we delved into the inherent psychological vulnerabilities of individuals and how these can be exploited through various effect mechanisms. Moreover, we identified the most influential factors that shape people's decisions.

Finally, we analyzed the demographics of those susceptible to social engineering and discovered that no single demographic characteristic can be solely attributed to susceptibility. Instead, we found indications that awareness of risks, security measures, and training play vital roles in reducing the likelihood of falling victim to a social engineering attack. However, the effects of these measures vary depending on demographics and nationalities among the study participants. Given the multicultural nature of today’s companies and their employees, it is imperative to employ a combination of security measures aimed at preventing attacks, comprehensive training on countering social engineering, and long-term awareness programs to reach as many employees as possible. Additionally, we have revealed the importance of developing, implementing and adhering to security policies to combat poor security practices, such as the use of passwords that never expire.

The insights we have gained will be of great value in the following chapter as we explore the nuances of user protection, customize different approaches for specific user roles, introduce an innovative method for identifying protection needs, conduct a comprehensive analysis of defense strategies from various disciplines, and delve into the ethical aspects of security testing. Additionally, we will address the critical element of preparedness in case protective measures fail.

5.1 Security Challenges Across Job Roles

As we have explored in the sub-chapter about demographics, individuals with diverse backgrounds and characteristics require different approaches to effectively educate them on security matters. Social engineers are well aware of this diversity and can customize their attacks based on the demographics of their potential victims, as seen in cases like vishing shock-calls that specifically target elderly individuals.

In addition to demographic factors, an individual's job position plays a significant role in determining the types of attacks they may encounter. For instance, a software developer may face different attack vectors compared to an employee working in user helpdesk, customer support, an executive role, or at the reception. Understanding an employee's work environment, user profile permissions (admin vs. standard user), file access rights, and job responsibilities is critical when designing effective security awareness training programs.

This tailored approach to security education helps address the unique security challenges faced by employees in various roles within an organization, making them better prepared to defend against social engineering attacks.

Certain job roles are particularly susceptible to being chosen as targets for social engineering attacks due to the unique rights and traits associated with their positions. For instance, employees in specific roles possess special privileges that can be exploited by social engineers. As an example, receptionists often have the ability to grant access rights, while new employees, eager to be helpful and liked, may inadvertently compromise security standards. Additionally, executive assistants may have access to valuable information, like their manager's calendar.

Wang et al. [84] have identified a range of potential targets, including but not limited to:
1) new employees, 2) secretaries, 3) help desk, 4) technical support, 5) system administrators, 6) telephone operators, 7) security guards, 8) receptionists, 9) contractors, 10) clients, 11) partners, 12) managers, 13) executive assistants, 14) manufacturers, 15) vendors.

As we see, not only demographic factors can influence the kind of attack an employee might face, but also their position. Therefore, tailored security awareness training programs and measures are essential to empower employees to recognize and defend against social engineering attacks.

5.2 Formulating Security Goals

Once we have determined who needs protection from social engineering threats, it is essential to identify what attackers are aiming to exploit. Human victims often serve as a means to an end, so comprehending the ultimate objectives is vital. For instance, in a piggyback attack, the goal is not just to overcome a physical obstacle but to potentially gain unauthorized access to locked information. Therefore, recognizing these potential end goals is critical.

In cybersecurity, the CIA triad (or AIC triad to avoid confusion with the American Central Intelligence Agency) outlines the primary security goals: Confidentiality, Integrity, and Availability. The CIA triad serves as a foundational framework for designing and assessing measures and policies to safeguard critical information and system assets. Its significance is attributed to its balanced approach, preventing security efforts from becoming one-sided. This framework effectively addresses a wide array of security concerns and aids in comprehensive threat impact assessment. It also aligns with legal and regulatory requirements, bolstering public trust by safeguarding confidentiality, data integrity, and data availability. Moreover, the CIA triad enhances resilience during security incidents and is adaptable to various contexts. These principles are fundamental to comprehending and implementing effective information security. Additional contemporary security objectives may include privacy, authenticity, non-repudiation, accountability, and auditability [40].

Although these objectives are undoubtedly crucial in the context of social engineering, they may not offer a full view. They assume that all security requirements are already known to stakeholders and only need to be implemented. However, as Pape et al. [9] point out, this can lead to security analysis gaps when certain social engineering threats are unknown to stakeholders.

For instance, specific behaviors among personnel, such as an employee repeatedly propping open a security door or attaching passwords to servers with post-it notes due to difficulty in remembering them, must be acknowledged to create an accurate model. Traditional methods for eliciting security requirements in socio-technical systems include investigating software security requirements [82], analyzing organizational security issues [54], [60], brainstorming [9], or focusing on business processes [39] or risks [38]. However, these approaches often fail to address unknown security requirements related to human-exploitable behaviors [9].

Therefore, to gain a comprehensive understanding of the spectrum of exploitable human behaviors, it is essential to involve employees in the elicitation process. This approach offers significant advantages over relying solely on security engineers, as employees possess an intimate knowledge of their own work responsibilities and daily routines. Furthermore, they often have insights into the cybersecurity awareness of their immediate colleagues, their compliance with policies and rules, and their past and present behaviors related to cybersecurity. Additionally, employees are well-versed in the intricacies of business processes and their contextual frameworks, enabling them to identify deviations from standard procedures. In essence, they unwittingly possess an awareness of potential security vulnerabilities stemming from human factors. Identifying these vulnerabilities would be a time-consuming task for a team of security engineers, and they might still overlook crucial details, all while incurring substantial costs [9].

One promising strategy we will delve into is the use of serious games. These games have gained recognition across various domains, with cybersecurity awareness being one of the key beneficiaries. Serious games have the primary goal of conveying specific knowledge or ideas in an engaging and enjoyable manner, allowing for the subconscious absorption of knowledge.

Serious games offer a unique advantage when compared to other training methods: they effectively convey ideas, facilitate learning, and provide opportunities for practice, all within an engaging and enjoyable framework. The element of entertainment is of paramount importance [49]. It ensures that the game captures the participant's attention and maintains their interest throughout. Conversely, boredom could divert participants' focus towards unrelated matters, hindering the absorption of essential knowledge. This aligns with a fundamental attribute of serious games: the immediate application of newly acquired knowledge and skills. This approach not only keeps participants engaged by sustaining their attention but also reinforces the learning process through practical implementation. This, in turn, contributes to the longevity of the acquired knowledge and skills [33].

Next, we will explore a serious game developed by Pape et al. [10], which aims to elicit and prioritize social engineering security requirements by directly involving the affected employees.

Pape et al. [9] argue for the use of a serious game based on several compelling reasons. First, games have the inherent advantage of being enjoyable, which naturally piques the interest of employees and ensures their active participation and attention. Additionally, games create a unique environment that encourages employees to think creatively and view problems from different perspectives. If a game successfully accomplishes these objectives, it can be replayed multiple times, potentially revealing new ideas with each playthrough.

Moreover, Pape et al.'s game provides a realistic scenario, while eliminating the fear of consequences for making mistakes. The introduction of consequences for errors, according to Klimmt [49], would undermine the effectiveness of the serious game, as players would not be inclined to consider possible consequences when they are immediately imposed.

Another noteworthy aspect is that games enhance the accessibility of imagined contexts and activities by allowing for fantasy and role-play in scenarios that may not be feasible, appropriate, or desirable in reality.

Furthermore, the choice of creating a physical card-based game was deliberate. This approach may be more appealing to individuals who are not fond of computer-based games. Additionally, it requires no special hardware or digital tools, only a table, and the game components can be reviewed without actively playing the game. This enhances accessibility and convenience for participants.

5.2.1 Pape et al.'s Serious Game

Now that we have explored the concept of serious games and the advantages they offer in various educational and problem-solving contexts, we will delve into the specifics of how Pape et al.'s serious game is played [9]:

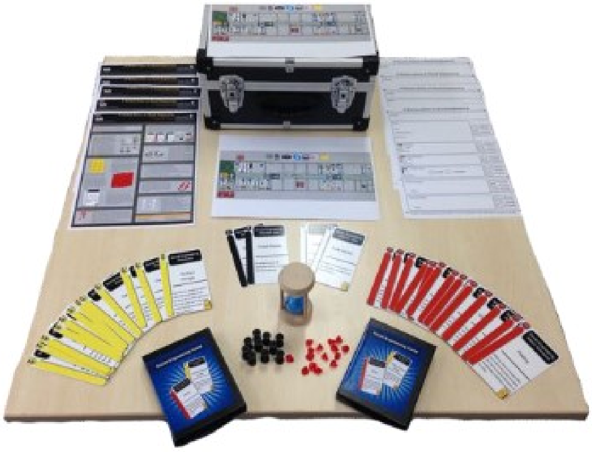


Figure 15: Pape et al.'s Serious Game [9]

1. **Game Setup**: The game is typically played in a workshop or group setting. Participants are usually stakeholders involved in the system's design and security, including end-users, system administrators, and other relevant parties.

2. **Scenario Creation**: The game begins by creating a scenario relevant to the socio-technical system under consideration. This scenario typically involves a social engineering threat or attack. For example, it might revolve around a scenario where an attacker tries to gain unauthorized access to a computer system by exploiting human vulnerabilities, such as persuading an employee to reveal their login credentials.

3. **Game Mechanics**: The participants are presented with the scenario and are asked to role-play various roles within the scenario. This may include playing the part of the attacker, system users, or other relevant characters. The game typically involves both the perspective of potential victims (system users) and the social engineer (attacker).

4. **Discussion and Analysis**: As the game unfolds, participants engage in discussions, make decisions, and analyze the scenario. They consider the various tactics employed by the social engineer, the responses of system users, and the vulnerabilities in the system that are exploited during the attack.

5. **Requirement Elicitation**: Throughout the game, participants are encouraged to identify and document system requirements that are relevant to mitigating the social engineering threat. These requirements may include technical controls, policy changes, awareness training, or other measures to enhance the system's security.

6. **Debriefing**: After playing the game and discussing the scenario, there is typically a debriefing session where the identified requirements are compiled and discussed. The goal is to ensure that relevant security requirements are documented and understood.

Pape et al.'s serious game offers an engaging and interactive learning experience, effectively uncovering social engineering-related system requirements. Participants actively immerse themselves in realistic scenarios and engage in role-playing, gaining valuable insights into vulnerabilities and security measures. This approach complements conventional methods, as it brings to light aspects that might not be as evident through traditional means. The game encourages all stakeholders to think critically about security concerns, thus contributing to improved security in socio-technical systems.

This immersive approach not only enhances employee awareness but may also unveil new security requirements that might otherwise remain unnoticed. It emphasizes the potential of interdisciplinary approaches. As we explored in the previous chapter on demographics, people do not uniformly respond to cybersecurity measures. Some individuals may for example benefit most from security training, while others may find awareness campaigns more effective [28]. A combination of defense mechanisms can cater to these diverse needs.

5.3 Interdisciplinary Approaches to Comprehensive Defense Strategies

As we have highlighted, the need for diverse defense strategies arises, among other things, from the varying demographics that require protection. However, it is crucial to recognize that diversity extends beyond the individuals themselves. The industries employing these individuals also exhibit their own unique characteristics, which, in turn, influence the types of attacks they face. Furthermore, the landscape of attack vectors is remarkably diverse. This multifaceted nature of the challenges posed by social engineering underscores the necessity for a comprehensive and adaptable defense approach that takes these various elements into account.

In the upcoming subchapter, we will thoroughly explore a range of diverse and interdisciplinary defense approaches. This examination will include an assessment of the advantages and disadvantages associated with each approach, along with a clarification of the specific issues they aim to address. It is crucial to emphasize that there is no universal, one-size-fits-all solution for countering social engineering attacks, nor can there be one. These attacks are continually evolving, presenting new variants that demand different defensive strategies. Furthermore, individual responses to these attacks can vary widely, as can the effectiveness of various defense mechanisms.

Moreover, the security requirements of organizations differ significantly, depending on their industry and operational context. While some sectors may prioritize robust physical defenses to protect against intruders, others may face more substantial threats in the digital realm. It is essential to tailor defense mechanisms to address these specific industry-related challenges.

For instance, we consider the use of serious games as an awareness and education tool. While younger individuals may be more receptive to these games due to their familiarity with digital entertainment, older individuals who are less acquainted with gaming or have a general aversion to it might perceive such games as childish [83]. This perception can hinder their engagement, making it less likely for them to take the games seriously, pay attention, and consequently, gain the intended educational benefits.

Moreover, the organizational context plays a vital role. In a small company, it may be feasible to educate most, if not all, employees relatively quickly through mechanisms like serious games, assuming that all participating employees are open to the idea of utilizing such games. However, applying this approach across a larger organization with hundreds or thousands of employees can become incredibly time-consuming and resource-intensive.

Consequently, the defense mechanisms we explore aim to provide a holistic understanding of currently employed strategies. Organizations can select and tailor these strategies to their specific requirements by thoroughly analyzing the context in which they operate. This process should also consider individual job roles. While educating every employee through mechanisms like serious games may be impractical for larger organizations, specific roles, such as receptionists or admin users, may benefit from a combination of various approaches. These considerations, along with demographic factors and industry specifics, are integral to making informed decisions about selecting the most suitable defense mechanisms.

5.3.1 Serious Games

Serious games, as exemplified by Pape et al.'s work [9], have proven to be versatile tools with applications spanning across a multitude of fields and industries. These interactive and engaging games have significantly impacted education and training paradigms. In addition to their role in eliciting security requirements, serious games find purpose in various contexts.

One primary domain where serious games have flourished is education and training. They have revolutionized traditional learning methods by providing engaging and interactive platforms to teach a wide array of subjects and skills [109].

Within the healthcare sector, serious games serve multifaceted purposes. They are employed for medical training, allowing healthcare professionals to practice critical procedures and diagnostic techniques. In one example, serious games are used to motivate trainee surgeons to practice their skills in the game called “Underground” [110]. Moreover, they play a role in patient education and promoting healthy behaviors [25].

In the corporate world, serious games facilitate employee training, particularly in areas like leadership, compliance, and customer service. New hires find these games instrumental in adapting to their roles effectively [67].

Cybersecurity, a field characterized by evolving threats and challenges, has harnessed the power of serious games. These games are used to identify and respond to cyber threats while concurrently raising awareness about security issues. Employees can practice handling various cyber threats within a secure and controlled environment [16].

In the aerospace industry, serious games have become invaluable tools for pilot and air traffic controller training. They offer realistic simulations of various scenarios, allowing professionals to develop their skills [70].

Emergency responders rely on serious games to simulate disaster response and coordination. These games help personnel prepare for a range of emergency scenarios and improve their coordination and decision-making abilities [68].

In the realm of science and research, serious games are used to crowdsource data and simulate complex phenomena. They contribute to tasks such as protein folding simulations and climate modeling, making them valuable research instruments [111].

Lastly, language learning has also benefited from the incorporation of serious games. These games provide an entertaining and interactive platform for acquiring new language skills, making the learning process more engaging [44].

These are just some of many examples where serious games are successfully being applied. The versatility and adaptability of serious games in addressing diverse educational and training needs across different sectors underscore their importance in contemporary learning environments. These games not only make learning more engaging, but may also enhance knowledge and skill retention while facilitating their practical application.

Measuring the impact of serious games on learning scientifically, however, is challenging due to several factors and high quality empirical studies to prove effectiveness are therefore scarce [7]. These include the diversity of learning outcomes, the complex learning environments created by games, variations in individual learners, difficulties in assessing long-term effects, and the absence of standardized assessments. Proving a direct causal link between game interactivity and learning is also complicated. Motivation and engagement, small sample sizes, ethical considerations, and potential publication bias further contribute to this challenge. Nonetheless, researchers are actively working on improved methods to evaluate the effectiveness of serious games in education.

Roozeboom et al.'s research [7] represents an initial step in the development of a comprehensive assessment framework for serious games. Their studies indicate that students engaged in these games achieved better results in areas associated with high-quality learning. Notably, their research underscores that serious gaming has a more pronounced impact on self-reported learning outcomes, with students perceiving these games as highly effective in imparting new knowledge compared to traditional classroom instruction. It is important to mention that these studies did not reveal significant effects of serious gaming on knowledge tests, possibly due to the limitations discussed earlier. The authors encourage further exploration to gain a deeper understanding of this aspect.

In contrast to Roozeboom et al.'s findings, Kanthan and Senger's study [47] focused on specially designed games to enhance learning in undergraduate pathology and medical education. This study demonstrated that examination scores supported by serious games were significantly higher than those relying solely on traditional learning methods. Therefore, their research revealed improved academic performance, measured through examination test scores, along with increased student satisfaction and engagement.

In conclusion, serious games have substantial potential for effectively educating employees when they offer an enjoyable experience, maintain high subjective narrative quality, and adhere to realism, as identified by

Fokides et al. [29] as the factors with the most significant impact on subjective learning effectiveness. However, because the effectiveness of serious games remains a topic of debate and highly dependent on the specific game, deploying a serious game to educate employees on social engineering attacks and awareness requires vigilant monitoring to ensure its effectiveness.

5.3.2 Training Methods

Staying within the realm of social defense strategies, our next strategy focuses on training to educate personnel in defense strategies, fundamental knowledge, skills, and raising overall awareness. These training sessions aim to convey the company's specific security policy [4], [45], [69], [80], which we will explore in our upcoming introduction to the next defense strategy.

These training programs form an integral part of the "Protect" pillar within the "Framework for Improving Critical Infrastructure Cybersecurity" by the National Institute for Standards and Technology (NIST) [64]. This framework serves as a comprehensive guide, offering best practices, guidelines, and standards to assist organizations, both in the public and private sectors, in enhancing their cybersecurity posture. It helps them efficiently manage cybersecurity risks across all aspects, encompassing identification, protection, detection, response, and recovery from cyber-attacks.

To gain insight into practical implementation, we turn to the study conducted by Rege et al. [69]. Their study provides a case study focusing on the efforts to design and develop a social engineering awareness and training program. This program was executed during the 2019 National Science Foundation Cybersecurity Summit, and it adheres to the NIST framework for program development [69], [89].
The steps required for creating an effective training program, as outlined in the framework "Building an Information Technology Security Awareness and Training Program" by Mark Wilson and Joan Hash [89], which Rege et al. followed, include:

1. Designing the training program.
2. Developing the awareness and training materials.
3. Implementing the program.

In the design phase, the primary objective is to create awareness and training programs that mirror the company's mission and culture, while equipping participants with relevant skills and knowledge [89]. For determining the education needs of the staff, the security policy established by the company's cybersecurity department is instrumental. This policy outlines the necessary measures and employee compliance rules to achieve the highest level of security [4].

Subsequently, awareness and training materials corresponding to the defined goals need to be developed. These materials should encompass both awareness and training topics. For example, training materials may include seminars and brief courses designed not to overwhelm participants with excessive information. In contrast, the training materials can be more in-depth, building upon the foundational awareness training and materials. These materials can be created in-house or sourced from external agencies [69], [89].

The final phase of shaping the awareness and training program centers on practical implementation. Various strategies are available, including posters, videos, newsletters, and in-person instructor-led sessions, among others. Instructor-led sessions are particularly noteworthy for their interactivity and the potential to incorporate video elements, making content delivery engaging and effective.

After the program is put into action, organizations should actively seek feedback and conduct evaluations to assess its effectiveness and identify areas for improvement. This feedback process should encompass an evaluation of program quality, coverage, complexity, session duration, relevance, and suggestions for potential

modifications. Valuable insights for program enhancement can be gathered through various channels, including questionnaires, focus groups, direct observations, and formal reports [69], [89].
Now that we have established the fundamentals of constructing a successful training program, we will delve into a concrete example, examining its structure and the materials employed. Our focus lies on the workshop conducted by Rege et al. [69]:

1. **Lectures and Presentations**: The workshop begins with traditional lectures and presentations. In these sessions, participants are introduced to the concept of social engineering, its various forms, and real-world examples of social engineering attacks. These lectures provide a foundational understanding of the topic.

2. **Discussion and Interaction**: The method encourages active participation and engagement from the participants. Group discussions and interactive sessions are integrated to allow participants to share their thoughts, experiences, and insights. This collaborative environment enables a more profound comprehension of the subject matter.

3. **Practical Exercises**: To reinforce learning, the workshop includes practical exercises and simulations. Participants are exposed to real-life scenarios where they can practice recognizing social engineering attempts and responding appropriately. These exercises provide hands-on experience and help participants develop practical skills.

4. **Case Studies**: The authors use case studies to delve into specific instances of social engineering attacks. By examining real cases, participants gain insights into the tactics employed by attackers, their motivations, and the consequences of successful attacks.

5. **Role-Playing**: Role-playing exercises are employed to simulate social engineering scenarios. Participants take on different roles, acting as both attackers and victims. This experiential learning method allows individuals to understand the psychology of both sides and enhances their ability to identify and counteract social engineering techniques.

6. **Question and Answer Sessions**: Throughout the workshop, attendees have the opportunity to ask questions and seek clarification on any aspects of social engineering. This interaction ensures that participants can address their specific concerns and challenges.

7. **Feedback and Evaluation**: The training method includes mechanisms for feedback and evaluation. Participants' understanding and progress are continuously assessed to identify areas that may require additional focus or clarification.

Overall, the method used in this workshop is learner-centric, promoting active engagement and practical skill development according to the framework provided by Wilson and Hash [89]. It combines theoretical knowledge with hands-on experience to create a well-rounded educational experience.

In our exploration of security awareness training programs, we have observed the significant role they play in enhancing employees' comprehension of information security. Effective training not only boosts awareness of potential risks but also imparts the knowledge required to mitigate these threats. As we transition to the next chapter, we delve into the fundamental aspects of security policies, which serve as the key principles for training programs, specifying what security measures are most important for each company and setting the standards that employees must adhere to.

5.3.3 Policies

As we advance in our exploration of information security, we reach a crucial point in our journey: security policies. Just as the laws of a society define its norms and protect its citizens, security policies create the framework and standards that ensure the safety of an organization's digital domain. These policies not only form the foundation of a secure environment but also establish explicit guidelines for employee conduct and the protection of data. We will therefore thoroughly examine the crucial role of security policies, grasp their importance, and explore the fundamental components that compose a comprehensive information security framework.

To craft a security policy tailored to a specific company, it is essential to fully grasp the extensive range of topics that such a policy should encompass. In this endeavor, the study conducted by Alharthi and Regan [3] becomes essential. Their work not only led to the creation of a taxonomy of social engineering defense mechanisms, but also developed a customizable model for Social Engineering Information Security Policies (SE-ISPs) to be used by organizations as needed.

In their taxonomy, Alharthi and Regan [3] discerned five focal points that social engineers aim to exploit. These targets are broadly categorized as:

- **People**: Social engineers manipulate and target the company's employees, persuading them to engage in unauthorized activities or divulge sensitive information. This category often involves various psychological tactics and social manipulation to deceive individuals.

- **Data**: The data component represents a critical focus of social engineering attacks. Both personal and organizational data can be at risk. This encompasses any information that could be leveraged for malicious purposes, including personal data, financial records, or proprietary business data.

- **Software and Hardware**: Social engineers may also target the software and hardware components of an organization's infrastructure. This involves exploiting vulnerabilities in computer systems, applications, or hardware devices. By doing so, they can gain unauthorized access, compromise systems, or disrupt operations.

- **Network**: The network is a prime target for social engineering attacks. Intruders may exploit weaknesses in an organization's network infrastructure, attempting to breach its security defenses. This can involve tactics such as phishing, hacking, or other network-based methods to gain access to confidential information or compromise the network's integrity.

To safeguard these assets, Alharthi and Regan grounded their approach in the cybersecurity objectives encapsulated by the CIA triad: confidentiality, integrity, and availability. For optimal protection, companies are advised to include the following 18 well-defined SE-ISPs [3]:

1. **Security Awareness Policy**: This policy serves as the cornerstone for fostering awareness and knowledge of information security within the organization. Its primary objective is to protect the organization's assets by ensuring that all employees are well-versed in safeguarding the integrity and confidentiality of valuable resources. According to Alharthi and Regan, this policy is considered one of the most effective approaches for achieving substantial and enduring enhancements in information security.

2. **Exception Management Policy**: This policy outlines the necessary procedures and approvals for managing exceptions to the organization's policies and procedures.

3. **Data Classification Policy**: This policy categorizes data into different types based on their confidentiality levels and provides guidance on how each type should be handled.

4. **Data Ownership Policy**: The Data Ownership Policy delineates the specifics regarding data ownership, including the creation, responsibilities, and control over data.

5. **Data Breach Policy**: This policy addresses the critical need to respond to data breaches effectively. Data breaches can result in severe operational, financial, reputational, and legal consequences. This policy establishes the procedures for reporting data security breaches, safeguarding employees, partners, and stakeholders from illegal or damaging actions.

6. **Encryption Policy**: The Encryption Policy defines the requirements for utilizing encryption technologies to secure the organization's data.

7. **Business Continuity and Disaster Recovery Policy**: This policy serves as a critical safeguard to ensure the organization has comprehensive plans and procedures in place that offer protection against the potential consequences of disasters or unexpected disruptions. The goal is therefore to effectively manage business continuity risks and address crisis situations. It is important to note that there are ISO standards for both Business Continuity (BC) and Disaster Recovery (DR), which we will explore in more detail later.

8. **Access Control Policy**: The Access Control Policy outlines the requirements for securely controlling access to the organization's IT services and infrastructure.

9. **Vendor Risk Management Policy**: This policy focuses on assessing security risks associated with third-party vendors.

10. **Mobile Device Policy**: The Mobile Device Policy governs the use of mobile devices, including those issued by the organization or used for business purposes, and specifies the standards and encryption requirements for data protection.

11. **Application Security Policy**: This policy guides secure coding practices, assessments, and remediation for all applications developed or integrated within the organization's environment. It addresses vulnerabilities in web applications and security threats, such as SQL injection and Denial-of-Service attacks.

12. **Security Risks and Controls**: The Consolidated IT Controls Catalog (CITCC) sets a baseline for IT security controls. It aims to minimize and manage IT risks within the organization.

13. **General IT Usage Policy**: This policy outlines the acceptable use of computer equipment, covering various aspects such as internet usage, email, remote access, and social media.

14. **Physical Security Policy**: Physical security is a non-negotiable aspect for security-conscious organizations. This policy enforces the physical security requirements for safeguarding assets, including computer hardware, workstations, servers, and building/room access.

15. **Password Policy**: The Password Policy defines the requirements for passwords used to secure systems and accounts, covering aspects like password creation, change, and protection.

16. **Network Security Policy**: This policy establishes standards for maintaining a secure network infrastructure to protect data integrity and reduce the risk of security incidents.

17. **Server Security Policy**: The Server Security Policy defines the standards for configuring internal server equipment owned or operated by the organization to prevent unauthorized access.

18. **Proxy/URL Configuration Policy**: This policy delineates the websites that are either allowed or blocked at the web proxy, thus ensuring that end users can exclusively access websites essential for their job responsibilities. In cases where access to a website is denied, a screen should be displayed, explaining the reason for the block and providing contact information for users who believe access should be granted.

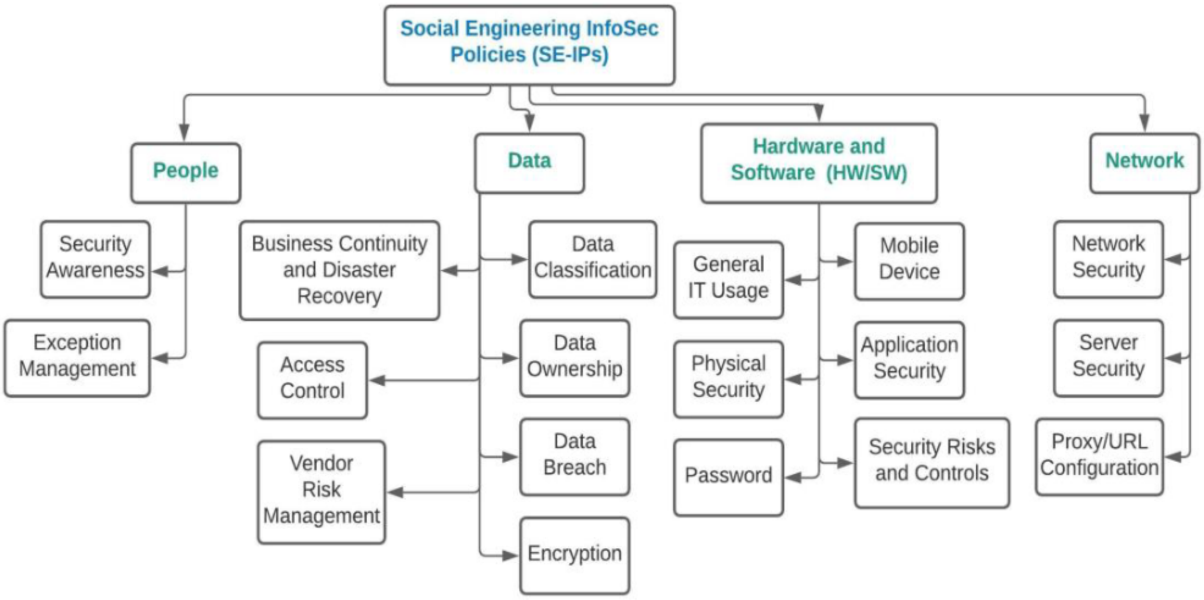


Figure 16: Proposed Formal SE-IPs by Alharthi and Regan [9]

However, the foundation for these 18 policies extended beyond the CIA-triad. Alharthi and Regan conducted two surveys and considered prior research. In one survey, they analyzed the adoption of SE-IPs within organizations, while the second assessed employees' awareness of specific social engineering defense mechanisms.

These studies revealed that, on average, only 47.5% of employees were familiar with social engineering attacks and the corresponding defense mechanisms [3]. Furthermore, they demonstrated that, on average, only 51.18% of the proposed policies were used in practice, with private companies exhibiting a higher rate of policy implementation [3]. For a comparative view, please refer to Figure 17 below.

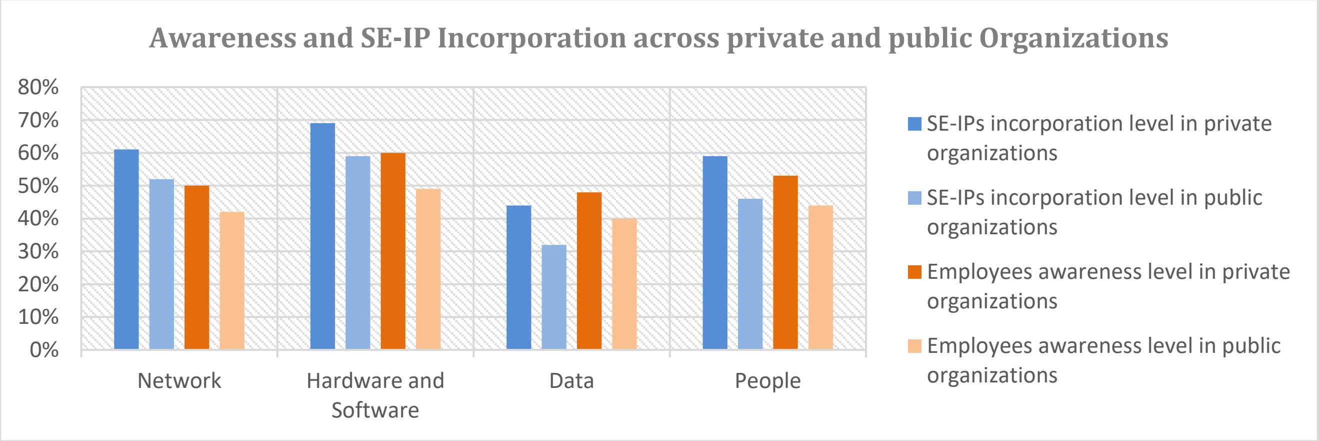


Figure 17: Comparison of Employee Awareness and SE-IPs Incorporation Levels Across Private and Public Organizations [3]

Alharthi and Regan's study exposed critical insights, illuminating several challenges faced by many companies. Their findings not only revealed a concerning lack of preparedness among organizations for potential cyber-attacks in the form of necessary policies, but also highlighted the absence of essential defense mechanisms, leaving companies vulnerable to a wide array of threats. Moreover, the study unveiled a significant lack of employee awareness concerning security policies and mechanisms. Some of the especially concerning discoveries from this study are as follows [3]:

- Just 22% of employees are familiar with their organizations' security policies, if they are accessible at all.
- A mere 66% of participants know whom to contact if their work computers are compromised.
- Only 33.42% of organizations provide cybersecurity awareness training for their employees.
- When they suspect a data breach, only 70.31% of employees feel comfortable reporting it.
- Approximately 45% of employees erroneously believe they are not being targets of cyberattacks.
- A striking 84% express overconfidence in the security of their work computers, stating that they are very secure.
- About 45% of participants claim they can detect hacking or infections on their work computers.
- 48.03% lack a dedicated email address for reporting phishing.
- Only 42.23% of organizations have policies for handling sensitive information.
- A significant 84.66% of employees don't encrypt their work files.
- Only 47.70% of employees have their data backed up by their companies.
- 60.11% of employees manually back up their data using USB devices or cloud storage.
- 42.49% use external storage devices for company data.
- Just 64.38% of organizations have policies which require employees to ask for approval before installing software on their work computers, leaving 35.62% vulnerable to downloading copyrighted software, offensive material, or infected files.

These findings underscore the threefold negligence previously mentioned - employees neglecting their company's SE-IPs, companies neglecting the implementation and education of their employees about these policies.

To tackle these challenges, companies need to do more than just implement security policies; they must also effectively educate their employees. However, this task is not without its complexities. For instance, forcing employees into compliance might lead to undesired behaviors, whereas fostering a positive attitude towards security changes can boost the likelihood of compliance [10]. Additionally, awareness training, while essential, does not automatically ensure the desired long-term educational impact and can be forgotten. Educating employees in this context is a delicate process that necessitates the avoidance of these potential pitfalls, requiring the pursuit of specific strategies. To delve into these issues and explore effective methods for educating employees about lurking dangers and the company's policies, we can refer to the following studies.

Yazdanmehr and Wang – "Employees' Information Security Policy Compliance: A Norm Activation Perspective"

This study by Yazdanmehr and Wang [90] investigates the role of norms in employees' adherence to organizational information security policies (ISPs) by integrating norm activation theory, social norms theory, and ethical climate literature. The authors, Yazdanmehr and Wang, propose a model to examine the development and activation of ISP-related personal norms and their impact on employees' compliance with ISPs. Data were collected through Amazon Mechanical Turk, revealing the significance of ISP-related personal norms in driving ISP compliance, particularly when bolstered by a sense of moral obligation.

Yazdanmehr and Wang describe how the influence of personal norms on an individual's behavior emanates from their desire to protect their core values. This intrinsic motivation prompts individuals to establish self-imposed rewards and sanctions to safeguard these values [98].

However, directly manipulating personal norms presents a challenge due to them being intrinsic and therefore not easily changed. In order to still achieve this, the study suggests that organizations should focus on reshaping ISP-related social norms. Social norms, shaped by collective beliefs about appropriate behavior in specific situations and influenced by social interactions, significantly impact behavior. This aligns with Cialdini's concept of the power of social proof [17].

To initially cultivate and subsequently activate ISP-related personal norms for compliance, the study proposes two strategies. First, organizations can establish a general atmosphere of rule adherence, with a specific focus on ISP compliance. This can be achieved through promoting ethical consistency, implementing training and socialization programs, and emphasizing organizational values related to rule and standard adherence. By fostering a shared perception of the importance of following rules, social norms concerning ISP compliance can be shaped. Organizations may also develop campaigns to reinforce these social norms.

Second, organizations should enhance awareness of the consequences and personal responsibilities associated with the ISP. This enhancement can strengthen feelings of moral obligation towards compliance and address common defense mechanisms used by employees to diminish their obligations. Programs, such as training sessions and informational brochures, can clarify the consequences of ISP violations and the role of each employee in safeguarding organizational information assets. According to Yazdanmehr and Wang, organizations should underscore that employees possess the authority and responsibility to comply with the ISP, emphasizing their role in securing information assets. Further reinforcement can be achieved by designing roles with built-in responsibilities, ensuring that employees understand their role in the consequences of ISP-related actions. As an example, a hospital can highlight that a nurse's responsibilities encompass not only patient care, but also the security of the information system resources integrated into their daily routines [98].

Al-Shanfari et al. – "Determinants of Information Security Awareness and Behavior Strategies in Public Sector Organizations among Employees"

Al-Shanfari et al.'s paper [4] presents a theoretical model integrating Protection Motivation Theory, Theory of Planned Behavior, General Deterrence Theory, and facilitating conditions (describing influential determinants used to promote specific behavior and intentions) to assess public sector employees' information security behavior intentions. Their study tested 11 hypotheses using a survey and structural equation modeling, indicating that these theories and facilitating conditions form a highly influential framework for explaining information security adoption behavior.

Unlike previous research that primarily focused on information security awareness models emphasizing either behavioral intentions or actual behavior, this study by Al-Shanfari et al. [4] uniquely addressed both aspects concurrently, recognizing their equal importance. Additionally, the study introduced organizational support (referring to employees' perceptions of institutional recognition, appreciation, and care) and communication channels as critical factors bridging the gap between intention and actual behavior. These three theories, together with these factors, encompass a combination of control, motivation, prediction, deterrence, and technical elements, all contributing to improving information security awareness levels. A visual representation of these factors, along with illustrative examples, is presented in Figure 18 below.

The study examined eleven hypotheses, and the findings demonstrated that ten of these hypotheses significantly influenced employees' intentions related to Information Security Awareness (ISA).

First and foremost, employees' attitudes towards ISA were revealed as a major driving force, positively impacting their willingness to engage in ISA activities. Similarly, subjective norms concerning ISA engagement also had a positive influence on employees' behavioral intentions, consistent with the research by Yazdanmehr and Wang. Furthermore, individuals who perceive the adoption of information security awareness as straightforward and beneficial are more likely to actively participate in information security activities.

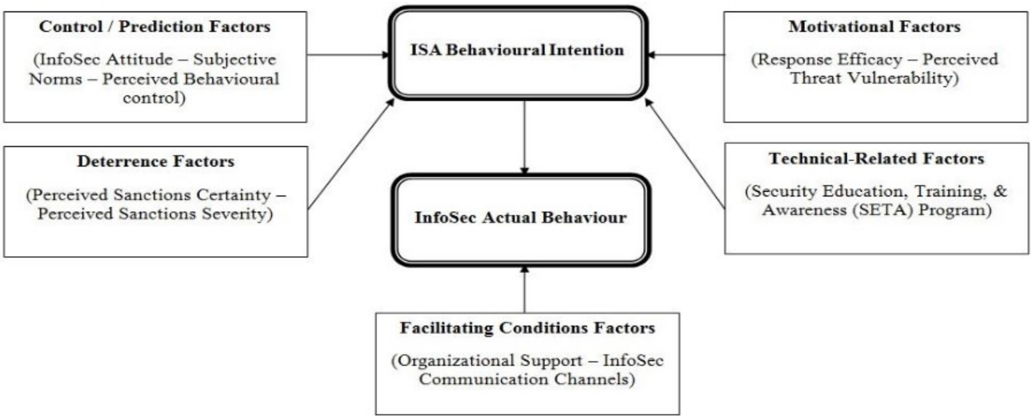

Control / Prediction Factors
(InfoSec Attitude – Subjective Norms – Perceived Behavioural control)
ISA Behavioural Intention
Motivational Factors
(Response Efficacy – Perceived Threat Vulnerability)
Deterrence Factors
(Perceived Sanctions Certainty – Perceived Sanctions Severity)
InfoSec Actual Behaviour
Technical-Related Factors
(Security Education, Training, & Awareness (SETA) Program)
Facilitating Conditions Factors
(Organizational Support – InfoSec Communication Channels)

Figure 18: The Research Model Used by Al-Shanfari et al. [4]

The study also highlighted additional factors that significantly shaped employees' actual information security (InfoSec) behavior. These factors encompass the perceived vulnerability of the company to cyber-attacks, the belief in the efficacy of preventive measures, the anticipation of severe consequences for ISA non-compliance, participation in Security Education, Training, and Awareness (SETA) programs, and the employees' own intentions to comply with teachings from ISA. All these factors were found to have a positive impact on employees' actual InfoSec behavior.

Notably, the study observed that the perceived certainty of punishment for ISA non-compliance had no favorable impact on employees' intentions. This perception relates to an individual's confidence in the authorities' ability to detect wrongful conduct and enforce penalties.

In conclusion, aligning information security awareness efforts with an organization's recognized risks and behaviors, along with consistent program provision, evaluation, organizational support, and effective communication channels, forms a vital part of ensuring that InfoSec behavior aligns with security regulations and policies.

Siponen et al. – "Employees' Adherence to Information Security Policies: An Empirical Study"

The study conducted by Siponen et al. [76] shares similarities with the one carried out by Al-Shanfari et al. [4], as they both introduced a model combining the Protection Motivation Theory and the General Deterrence Theory. However, there is a difference in the theoretical framework, as Siponen et al. additionally used the Theory of Reasoned Action to explain employee adherence to Information Security Policies (ISPs), in contrast to the Theory of Planned Behavior and facilitating actions used by Al-Shanfari et al.

Siponen et al. collected data through a questionnaire from four different companies, with responses from 917 participants across Finland. In contrast, Al-Shanfari et al.'s study [4] focused on the results of 415 public sector employees from the Sultanate of Oman. Notably, Siponen et al. did not specify the sectors of the four companies selected for the survey.

It is intriguing to observe that despite the significant demographic differences in geographical locations, the results remained consistent. This is particularly interesting when considering the findings discussed in our chapter regarding demographics, where Flores et al. [28] identified notable differences in the correlations between phishing behavior, security awareness, intention to resist social engineering, and training, depending on the cultural backgrounds of the test participants. This suggests that while cultural influences may impact susceptibility to social engineering, it does not influence the methods used to enhance policy adherence. However, this requires further investigation in future research to validate this conclusion.

The results of the survey revealed the following significant findings:

1. **Threat Appraisal**: Threat appraisal significantly influences employees' intention to comply with information security policies. This means that employees should be made aware of the severity and immediacy of information security threats to their organization.

2. **Self-Efficacy**: Belief in one's ability to apply and adhere to information security policies has a significant impact on the intention to comply with these policies. Employees must see these policies as relevant to their work and feel capable of implementing them.

3. **Response-Efficacy**: The perception of the effectiveness of adhering to information security policies influences the intention to comply. It is crucial for organizations to ensure that their information security personnel are well-prepared to handle threats and that policies are clear and up-to-date.

4. **Sanctions**: The presence of sanctions significantly influences employees' actual compliance with information security policies. It is crucial for employees to have the perception that non-compliance will be swiftly detected and result in severe legal consequences, which will be enforced quickly.
   It is worth noting that while Al-Shanfari et al. [4] discovered that the perceived certainty of punishment had no influence on compliance, Siponen et al.'s findings indicate that it does play a role. However, for this impact to be effective, perceived swift detection is crucial.

5. **Social Pressure**: Approval from top management, supervisors and information security staff plays a vital role in fostering information security policy compliance. Organizations should educate and engage these groups to create social pressure encouraging compliance. These groups should also provide clear and explicit explanations regarding the significance of adhering to ISPs to the rest of the organization.

6. **Intention**: The intention to comply with information security policies has a significant impact on actual compliance. Stronger intentions lead to a higher likelihood of compliance.

As previously mentioned, it is noteworthy that Siponen et al.’s findings align with those of Al-Shanfari et al., indicating the possible consistency of these principles across diverse geographical and cultural contexts. This highlights the potential for organizations to rely on well-established models to bolster policy adherence and to therefore protect their assets.

Herath and Rao – “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness”

The final study we will examine was conducted by Herath and Rao [37]. In their research, they collected responses from a web survey involving 312 employees from 77 organizations in Western New York, similar to the studies conducted by Al-Shanfari et al. [4] and Siponen et al. [76]. Herath and Rao validated their theoretical framework, which focused on incentive mechanisms, including penalties, social pressure, and perceived effectiveness.

This study reaffirmed some previous findings while introducing new insights and challenging others. Consistent with prior research, it confirmed that both intrinsic and extrinsic motivators influence employees' compliance intentions. Notably, intrinsic motivation, driven by the belief that compliance benefits the organization, played a significant role. Social influence, particularly normative beliefs and peer behavior, also affected security compliance.

However, in contrast to Al-Shanfari et al. and Siponen et al., Herath and Rao found that the perceived certainty of detection positively influenced compliance, with the visibility of detection mechanisms being more critical than the severity of penalties.

This study challenges the notion presented by Al-Shanfari et al. and Siponen et al. that severe punishment is the most effective, suggesting that the certainty of detection is more crucial. In contrast, Al-Shanfari et al. reported that the certainty of detection had no significant impact on ISP compliance, and Siponen et al. indicated its significance only when detection of misconduct is swift.

Furthermore, Herath and Rao's research offers practical implications for designing secure systems and security policies, emphasizing the importance of conveying the significance of information security to employees and cultivating a security-oriented climate. Notably, it introduces key suggestions not previously discussed:

1. **Well-Defined Policies**: Maintain easily accessible, unambiguous security policies covering data handling, passwords, and incident reporting.

2. **Incentive Programs**: Implement reward systems for policy adherence, motivating employees personally and benefiting the organization.

3. **Visible Safeguards**: Employ visible security measures like cameras and access controls to remind employees of scrutiny.

4. **Regular Audits**: Conduct periodic security audits to evaluate compliance and improve training programs, while at the same time working as a deterrent to misconduct.

5. **Performance Integration**: Incorporate security compliance into annual performance evaluations, offering rewards for adherence and consequences for violations.

We now conclude our discussion of the works by Yazdanmehr and Wang [90], Al-Shanfari et al. [4], Siponen et al. [76], and Herath and Rao [37]. The findings we have presented can provide practical implications for companies seeking to emphasize the importance of policies. Notably, these findings indicate that demographic differences, particularly location, had no significant impact on the results. These findings offer recommendations that can be integrated into security awareness training and the overall corporate culture. Below is a summary of the key findings from these four studies, organized into thematic blocks.

Cultivating a Culture of Compliance

- Promoting an atmosphere of rule adherence and policy compliance fosters the development of social norms [4], [37], [76], [90]
- Social norms related to policy compliance significantly influence individual beliefs [4], [37], [76], [90]
- Emphasizing individual responsibility for complying with security policies is essential [90].
- Perception of educated, and for security caring leadership is especially important due to creating social norms that can reach all employees [4], [37], [76], [90]

Attitudes and Beliefs

- Maintaining a positive attitude toward Information Security Awareness (ISA) increases the willingness to engage in ISA activities [4].
- Perceiving ISA adoption as straightforward and beneficial is crucial [4], [90].
- Recognizing the company's vulnerability to attacks is a key factor [4], [90].
- Belief in the efficacy of security-aware behavior as the primary means to mitigate risks is vital [4], [76], [90]
- Particularly strong intentions to comply are beneficial [4], [90].

Support and Communication

- Providing organizational support to employees is important for compliance [4], [76].
- Effective communication from educated leadership through various channels is essential for informing about Information Security [4], [37], [76], [90].

Punishment and Sanctions

- Clearly communicating the consequences of ISP violations for the company is necessary [4], [76], [90].
- Making information about sanctions for ISP non-compliance visible is crucial [37], [76].

Programs and Performance Integration

- Employee participation in Security Education, Training, and Awareness (SETA) programs plays an important role [4], [76], [90].
- Integrating performance evaluations with rewards for security compliance and consequences for violations is effective [37].

Well-Defined Policies

- Ensuring easily accessible, unambiguous policies that cover data handling, passwords, and incident reporting is essential [37].

Incentive Programs

- Implementing incentive programs that reward employees for compliance is effective [37].

Visible Safeguards

- Employing visible security measures like cameras and access controls, control walks from security personnel or the checking of logs to remind employees of scrutiny is advisable [37].
- Conducting regular security audits is recommended [37].

Furthermore, the various studies unearthed additional insights regarding the efficacy of sanctions and punishments. These findings, however, exhibited some contradictions. While Yazdanmehr and Wang [90], Al-Shanfari et al. [4], and Siponen et al. [76] argued that the perceived severity of punishment positively influenced policy compliance, Herath and Rao [37] presented a contrasting view. Herath and Rao contended that perceived severity not only failed to enhance compliance but that a perceived excessive punishment could also yield negative effects. In terms of the perceived certainty of punishment in the event of misconduct, essentially an employee's belief in the likelihood of being caught if they breach policies, Al-Shanfari et al. found no indication that increased certainty correlated with higher compliance rates. Conversely, Yazdanmehr and Wang, as well as Herath and Rao, reported a significant impact of perceived certainty. Siponen et al. suggested that certainty had an impact, but only when coupled with celerity, meaning only if misconduct was anticipated to be swiftly detected. These divergent findings on punishment and sanctions underscore the need for future research, particularly in the context of ethical implications as these have not been considered in any of these papers.

In summary, our exploration of security policies has revealed the comprehensive taxonomy introduced by Alharthi and Regan, which categorizes policies into five essential domains: people, data, software, hardware, and network. We have delved into the realm of 18 recommended policies, discovering that nearly half of them remain unimplemented on average, underscoring the persistent gaps in policy implementation. Furthermore, our examination has illuminated the concerning low levels of employee awareness regarding these policies. To bridge this awareness gap and bolster policy adherence, we have harnessed insights from four distinct studies, gathering valuable recommendations. These insights collectively shed light on the evolving landscape of policy compliance and equip organizations with actionable strategies to fortify their security posture.

5.3.4 Technical Defense Mechanisms

The final category of defenses we will explore comprises technical measures, both physical and digital, aimed at thwarting social engineering attacks before they can target potential victims. The selection of appropriate defense mechanisms depends on the potential attack vectors a company might face. As previously discussed in earlier chapters, it is essential to assess the extent of implementation required, as not all departments within a company necessarily need the same level of security measures.

In general, an effective technical defense against social engineering threats necessitates a layered approach that combines both physical and digital preventive measures. The following list outlines various defense mechanisms, categorized as physical and digital measures. It is crucial to emphasize that employees involved in certain mechanisms, such as receptionists or security guards, should undergo specialized training on social engineering. This training should equip them with the knowledge to recognize potential signs of a social engineering attack and respond effectively.

Physical defense mechanisms

1. **Security Doors**: Installing secure access control systems, like key card readers or PIN-based locks, can restrict unauthorized physical access to sensitive areas. Passing access key cards or something similar through turnstile doors or turning gates should not be possible, neither should it be possible that several people can pass through simultaneously.
2. **Video Surveillance**: Implementing surveillance cameras in and around a company’s premises can deter unauthorized individuals from attempting social engineering attacks.
3. **Visitor Management Systems**: Using a visitor management system can help track and monitor visitors, ensuring that only authorized individuals gain access. Furthermore, all visitors need to be registered in advance by a contact person. This contact person needs to pick the visitor up at the reception, as well as return them there when they plan to leave. Visitors need to identify themselves through an official ID card and carry a visitors pass during their stay.
4. **Security Fences**: Implementing secure perimeter fences and gates to control physical access.
5. **Secure Document Disposal**: Properly disposing of sensitive documents through shredding or incineration prevents attackers from gaining information through physical means. Besides written data, this can also encompass digital storage devices like hard drives. These can be securely stored until they are safely destroyed by external service providers specializing on document disposal.
6. **Security Guards**: Employing trained security personnel can act as a visible deterrent to unauthorized access and potential social engineers. These can be employed at the company’s main gate, other crucial spots or control the premise in general.
7. **Biometric Access Control**: Implementing biometric authentication methods such as fingerprint or retinal scans for critical access points.
8. **Secure Facilities**: Storing sensitive data in physically secure facilities, like data centers with controlled access.
9. **Privacy Screens**: Using privacy screens on computer monitors to prevent shoulder surfing attacks. These kind of screen applicators prevent the ability to look at the screen from an angle and can be attached and removed magnetically.
10. **Lockable Storage**: Providing employees with lockable storage for devices and sensitive documents. Policies should require employees to use these.
11. **Alarm Systems**: Installing intrusion detection and alarm systems to alert security personnel in the event of unauthorized access. Can be used to detect attempts to overcome turnstile doors.
12. **Security Awareness Signage**: Placing signs and posters around the workplace to remind employees of security policies and the importance of vigilance.
13. **Clean Desk Policy**: Implementing a clean desk policy, requiring employees to secure and lock away sensitive documents and materials when not in use. Effectively expanding suggestion number 10 “lockable storage”.

Digital Defense Mechanisms

1. **Phishing Filters**: Installing email filtering systems capable of detecting and blocking phishing emails is a valuable strategy to mitigate the risk of employees becoming targets of such attacks. These systems can be outsourced to external service providers, and the latest versions incorporating artificial intelligence have the potential to be particularly effective. An extensive study that assessed the efficacy of various approaches, including data mining, heuristics, machine learning, and deep learning, concluded that machine learning demonstrated the highest effectiveness with a 99% true positive rate. In contrast, heuristics and data mining methods were computationally resource-intensive and yielded a significant number of false positives [8].
2. **Anti-Malware and Antivirus Software**: Keeping security software up to date can help detect and prevent malicious software often distributed through social engineering attacks.
3. **Email Address for reporting Suspicious Activities**: Employees should be informed about an email address designated for reporting suspicious activities or potential phishing emails. This email address should be widely promoted, for example, through security awareness signage, to ensure that all employees are aware of its existence.
4. **User Training**: Regularly training employees to identify social engineering tactics and motivating them to report suspicious activities can help reduce the risk. These training sessions may be mandatory for employees at specified intervals, such as through informational presentations followed by quizzes that must be completed successfully.
5. **Security Awareness Programs**: Implementing ongoing security awareness programs can reinforce best practices and keep employees vigilant.
6. **Multi-Factor Authentication (MFA)**: Enabling Multi-Factor Authentication for user accounts enhances security by adding an additional layer of protection, making it more challenging for attackers to gain unauthorized access. However, it is crucial to note that MFA is an example illustrating that technical deterrents alone may not be entirely effective. A study by Siadati et al. [74] revealed that 50% of the participants forwarded their MFA codes using social engineering techniques.
7. **Firewalls and Intrusion Detection Systems (IDS)**: These tools can filter incoming and outgoing network traffic to identify and block suspicious activity.
8. **Access Control Lists (ACLs)**: Configuring ACLs on network devices to restrict access to specific resources and networks.
9. **Encryption**: Encrypting sensitive data both at rest and in transit can protect it from being exposed even if an attacker gains access. Employees need to be taught how to use these tools.
10. **Password Policies**: Implementing strong password policies and frequent password changes can help prevent unauthorized access to user accounts.
11. **Vulnerability Scanning**: Regularly scanning systems for vulnerabilities and promptly patching or remediating them can reduce the risk of exploitation by attackers.
12. **Behavioral Analytics**: Leveraging machine learning and behavioral analysis to identify abnormal user behavior and potential security risks. Possible applications are anomaly detection, user profiling, insider threat detection, phishing detection, pattern analysis as well as continuous monitoring. These systems work, for instance, by flagging an action as suspicious if a user suddenly accesses sensitive data they do not access usually or change communication patterns [75].
13. **Incident Response Plans**: Developing and regularly testing incident response plans is essential to guarantee a rapid and coordinated response in the event of a security breach.
14. **Phishing Simulation and Training**: Conducting regular phishing simulation exercises to train employees to recognize and respond to phishing attempts.
15. **Web Filters**: Employing web filters to block access to malicious websites and content.
16. **Patch Management**: Ensuring that systems and software are consistently updated with the latest security patches to address vulnerabilities.
17. **Secure Development Practices**: Implementing secure coding practices to minimize the risk of attackers exploiting vulnerabilities.

18. **Red Teaming**: Conducting periodic “red team exercises” with the goal to simulate real-world social engineering attacks and identify vulnerabilities.
19. **Network Segmentation**: Segregating networks and resources to limit the potential scope of an attack.
20. **Security Information and Event Management (SIEM)**: Using SIEM solutions to centralize log data and facilitate the detection of unusual activity. These solutions help organizations to detect, analyze and respond to attacks before they cause harm.
21. **Regular Risk Assessments**: Conducting risk assessments to identify and prioritize security risks and mitigation measures.
22. **Honeypots**: Setting up honeypots to detect and monitor unauthorized access attempts and malicious activity. Honeypots describe traps designed to divert and study malicious actors' activities. They mimic attractive targets to lure attackers away from critical systems, collecting data on attack tactics and tools.
23. **Web Application Firewalls (WAFs)**: Deploying WAFs to protect web applications from attacks like SQL injection and cross-site scripting.
24. **Digital Rights Management (DRM)**: Implementing DRM solutions to control and protect access to sensitive digital assets. DRM systems typically involve encryption, access controls, and licensing agreements, ensuring that only authorized users can access the protected content.
25. **Incident Response Automation**: Integrating automated incident response workflows to expedite the reaction to security incidents.
26. **User Access Rights**: Limit user privileges to reduce the risk of unauthorized installations and enhance security. Educate employees on the importance of these restrictions.
27. **Device Encryption**: Enforcing device encryption for all company-issued devices and storage media.
28. **Biometric Authentication for Workstations**: Enabling biometric authentication for user workstations for added security.
29. **Shadow IT Monitoring**: Shadow IT monitoring is the practice of tracking and managing technology and software usage within an organization that is not officially approved or supported by the IT department. It involves identifying and monitoring unauthorized or unmanaged technology solutions and applications used by employees.
30. **Secure Printing Solutions**: Implementing secure printing processes to prevent unauthorized access to printed materials.
31. **Network Access Control (NAC)**: Using NAC solutions to restrict network access to authorized and compliant devices.
32. **Third-Party Risk Assessment**: Conducting regular assessments of third-party vendors to ensure their security measures align with by the company set standards.
33. **Supply Chain Security:** Enhancing supply chain security by verifying the integrity of hardware and software components.
34. **Remote Device Management**: Employing remote device management solutions to secure, monitor, and control remote endpoints.
35. **Saliency Nudges**: Nudges are subtle interventions or cues designed to influence people's behavior or decision-making without constraining their choices. The goal of these nudges is to gently steer individuals toward making preferred decisions or actions, often by drawing from insights in behavioral economics and psychology. A common example can be seen on websites that request user consent for cookies. The "Accept" button is prominently highlighted, while the "Decline" option is typically smaller and less conspicuous. In a study conducted by Nicholson et al. [65], nudges were used to emphasize crucial information about either the sender or recipient when assessing emails. The study found that highlighting sender saliency, including the sender's name, email address, and time the email was sent, improved users' ability to detect phishing attempts. It's important to note that further research is necessary to fully validate the effectiveness of this approach.

It is vital to remember that while technical defense mechanisms play a crucial role in enhancing an organization's security, they are designed as complementary tools to mitigate vulnerabilities exposed to social engineering attacks. These mechanisms are valuable safeguards for digital assets, strengthening overall information security.

However, it is important to note that these technical safeguards should not replace the essential elements of employee awareness training and well-defined security policies. Instead, they should be considered as crucial parts working together to form the core of security. Awareness training equips employees with the knowledge and skills to recognize and respond to emerging threats, building a human firewall that enhances the organization's defenses.

Similarly, well-crafted policies serve as guiding principles that outline expectations, standards, and best practices for safeguarding information assets. They provide the framework for employees to follow, ensuring consistent security practices throughout the organization.

In summary, the combination of technical defense mechanisms, employee awareness training, and solid security policies collectively fortify an organization's security, creating a comprehensive and resilient defense against the various challenges posed by modern cybersecurity threats. These components are most effective when they work together, forming a comprehensive and robust security ecosystem.

5.4 Penetration Tests

A penetration test, commonly known as a pen test, is a cybersecurity assessment that plays a pivotal role in evaluating and enhancing the security of an organization's digital and physical assets. Its primary purpose is to simulate real-world attacks, allowing organizations to identify vulnerabilities, assess the effectiveness of security controls, and measure potential risks.

By emulating the tactics, techniques, and procedures used by malicious actors, penetration tests usually aim to uncover vulnerabilities within an organization's information systems, networks, applications, and other technology resources. These vulnerabilities could include software flaws, misconfigurations, or other security weaknesses that might be exploited by cybercriminals.

Furthermore, penetration tests assess the robustness of security controls, such as firewalls, intrusion detection systems, access controls, and encryption methods. Testers attempt to bypass or circumvent these controls to gauge their resilience under attack scenarios.

A key objective is to provide a realistic evaluation of an organization's cybersecurity posture, demonstrating how well it can defend against genuine threats. The tests also assist in assigning risk levels to identified vulnerabilities, helping organizations prioritize security enhancements based on the severity of each risk.

In addition to evaluating security controls, penetration tests can assess an organization's incident response capabilities. By simulating security incidents, they reveal how effectively an organization can detect, respond to, and recover from such events.

The way in which penetration tests work, however, introduce specific challenges when conducting tests on social engineering defense mechanisms. This is particularly evident when physical defenses, such as access restrictions, are being evaluated. In a typical penetration test focused on technological cyberattack defenses, only technological means are evaluated. However, when assessing an employee's ability to detect an attack, it necessitates subjecting them to an actual attack, involving deception and trickery. While digital attacks can be, to a certain extent, conducted in an ethical [26] and legal [77] way, that is not the case with physical attacks that require face-to-face contact and deception.

That way, if the attack is successful, it is likely to leave the victim with feelings of privacy invasion, and they may unintentionally reveal valuable information. Furthermore, they could lose the trust of their colleagues and possibly makes them victim of mockery, if they revealed important information or opened restricted areas. This, in turn, could erode trust in the organization and result in legal action and productivity loss [24].

These implications, both ethical and legal, may incline companies not to conduct physical or social engineering focused penetration tests, leaving them unaware of potential risks.

To address these concerns, we will delve into a study by Dimkov et al. [24], which explores two useable methodologies, designed to alleviate these problems: the Custodian-Focused (CF) method and the Environment-Focused (EF) method.

These methods adhere to the so called “R* requirements” by Dimkov et al. [24]. Both testing methods strike a different balance between the R* requirements. These are as follows:

- **Realistic**: Employees behave as they do in their regular work routine.
- **Respectful**: Tests are conducted with respect for employees and mutual trust.
- **Reliable**: Testing does not disrupt employee productivity.
- **Repeatable**: Results remain the same when the test is repeated in an unchanged environment.

The goals of the tests are to reveal two different kinds of security vulnerabilities. These are either lapses in the proper execution of procedural and physical policies by employees, and deficiencies in the establishment of security policies by management.

In the first scenario, the tests should evaluate the extent to which employees adhere to the organization's security policies and the effectiveness of physical security measures. In the second scenario, the primary objective is to identify and exploit weaknesses in the policies themselves rather than their execution. For instance, a test may assess the enforcement of a credential sharing policy by employees, or it may aim to exploit the absence of such a policy to gain access to a target asset.

The Environment-Focused (EF) approach assesses the security of the asset's environment and is suitable when the asset's custodian is aware of the test but not subjected to the attack themselves. An example is assessing the CEO’s office security without involving the CEO.

The Custodian-Focused (CF) methodology is broader and encompasses the asset owner, who remains unaware of the test. While more realistic, CF is therefore less respectful to the custodian and less reliable. We will now examine both methods as to learn when, and how to properly utilize them.

5.4.1 Environment-Focused Method

The Environment-Focused (EF) methodology's primary aim is to assess an environment's security while ensuring that the custodian is not deceived. This approach enhances realism but necessitates the custodian's full awareness and consent. The custodian's active involvement and agreement play crucial roles in this method, and the monitoring of the penetration test is conducted without violating the custodian's privacy. The Environment-Focused method as proposed by Dimkov et al. [24] involves the following key elements:

- **Security Officer**: This is an employee responsible for the organization's security. The security officer plays a central role in orchestrating the penetration test.

- **Custodian**: The custodian is an employee who possesses the asset being tested. They set up and monitor the penetration test and are fully aware of the test's execution.

- **Penetration Tester**: This is an employee or contractor responsible for attempting to gain possession of the asset without getting caught.

- **Employee**: Individuals in the organization who do not have specific roles related to the test.

The EF procedure consists of three stages that include setup, execution, and closure:

- **Setup**: The security officer defines the test's scope, rules of engagement, and goals. The scope includes the locations the penetration tester is allowed to enter and the business processes that can be abused. Rules of engagement specify the tools and means the tester can use. The custodian marks a non-critical asset in their possession, sets up monitoring equipment, and ensures that the asset's loss will not disrupt the organization's productivity. For example, Dimkov et al. used a marked new notebook that was not needed for anything at that moment besides the test.

- **Execution**: The penetration tester scouts the area in an unassuming way so as not to draw attention and alert the possibly present employees, proposes attack scenarios, and seeks approval from the custodian and the security officer. Attack scenarios must align with the defined scope, and approval ensures that the scenarios will not negatively affect daily operations. The execution is monitored remotely through CCTV and other monitoring equipment. An attack scenario could look like the following [24]:

    1. Through social engineering, gain a night pass from an employee.
    2. Enter the target building early in the morning.
    3. Through social engineering, get the cleaning personnel to open the target office.
    4. Cut any protection on the laptop using a bolt cutter.
    5. Leave the building during office hours.

- **Closure**: After the test, the penetration tester compiles a report listing the attack traces, which are records of both successful and unsuccessful attacks. The security officer debriefs the custodian and any employees who were deceived during the test. An example for a completed attack manuscript can be found below in Table 3.

In summary, the Environment-Focused method in physical penetration testing places a strong emphasis on the security of the environment, involving specific actors, well-defined rules, and transparent communication between the custodian, security officer, and penetration tester. The methodology strives to ensure the security of the tested environment without causing disruption to daily operations or compromising privacy.

However, it is important to acknowledge that this method is not without flaws. In their tests, Dimkov et al. [24] identified several issues. First and foremost, they noted that attack scenarios should be adaptable. This arises from the fact that, in Dimkov et al.'s experiments, penetration testers always had to deviate from planned scenarios to some extent due to unexpected behaviors or absences of the target employees. Additionally, while the EF methodology respects the custodian's privacy, it can strain the trust relationship between the custodian and other employees. For instance, if a secretary opens the custodian's office door during the test, it might lead to the custodian no longer trusting the secretary. The third challenge observed was that employees attempted to contact the custodian for guidance, putting pressure on the custodian who had to ignore these requests, resulting in uncomfortable situations. Finally, the debriefing of employees after the test proved to be a challenging process. This was particularly the case with one employee, a security guard who had opened a door three times for the penetration testers. Dimkov et al. concluded that the debriefing process caused more stress to this employee than the penetration test itself.

Generic Script	Attack trace	Circumvented mechanisms	Recommendations
Prepare for the attack	Buy a bolt cutter and hide it in a bag. Scout the building and the office during working hours. Obtain an after working hours access card.	Access control of the building entrances during working hours. Credential sharing policy.	Keep entrance doors to the building locked at all time. Provide an awareness training concerning credential sharing.
Enter the building	Enter the building at 7:30 AM, before working hours. Hide the face from CCTV at the entrance using a hat.	CCTV pre-theft surveillance.	Increase the awareness of the security guards during non-working hours.
Enter the office	Wait for the cleaning lady. Pretend you are an employee who forgot the office key and ask the cleaning lady to open the office for you.	Challenge unknown people to provide ID. Credential sharing policy.	Reward employees for discovering intruders.
Identify and get the asset	Search for the specific laptop. Get the bolt cutter from the bag and cut the Kensington lock. Put the laptop and the bolt cutter in the bag.	Kensington lock.	Get stronger Kensington locks. Use alternative mechanism for protecting the laptop.
Leave the building with the laptop	Leave the building at 8:00, when external doors automatically unlock for employees.	CCTV surveillance. Access control of the building entrances during working hours.	The motion detection of the CCTV cameras needs to be more sensitive.

Table 3: An Example for an Attack Trace Manuscript After a Successful Attack, Used by Dimkov et al. During Their Tests [24]

5.4.2 Custodian-Focused Method

The next method we will take a look at is the Custodian-Focused (CF) Method [24], an advancement of the EF method. In the CF methodology, the custodian, who has possession of the asset, is deliberately kept unaware of the penetration test, making it suitable for assessing the overall security of an area while considering the custodian's level of security awareness. Here are the key elements of the CF methodology:

- **Security officer**: An employee with the responsibility of ensuring the organization's security.
- **Coordinator**: An employee or contractor in charge of overseeing the experiment and the actions of the penetration tester. The coordinator manages the entire penetration test.
- **Penetration tester**: An employee or contractor tasked with attempting to acquire the asset without detection.
- **Contact person**: An employee who offers logistical support within the organization and serves as an emergency point of contact.
- **Custodian**: An employee at whose office the asset is situated. The custodian should remain unaware of the penetration test.
- **Employee**: Individuals within the organization who do not hold any of the aforementioned roles. Employees should also be kept unaware of the penetration test.

Following are the three stages of the CF Method:

- **Setup**: The security officer initiates the test by defining the target, scope, and rules of engagement (see Fig. 19). A coordinator is assigned, who is responsible for the experiment and the behavior of the penetration tester. Marked assets and monitoring equipment are provided to the coordinator for the test. The penetration tester signs the rules of engagement, affirming their commitment to ethical conduct. Next, the coordinator selects a group of contact persons who will manage the marked assets and monitoring equipment and also provides a cover story as to why the custodians need to store the assets.

  The contact person, as per the security officer's requirements, selects custodians, provides them with assets and monitoring tools, and secures informed consent (see Fig. 19). If data can be stored, the consent document specifies not storing sensitive information. The coordinator shares the list of penetration testers with the security officer and provides asset locations to the penetration tester before the test begins.

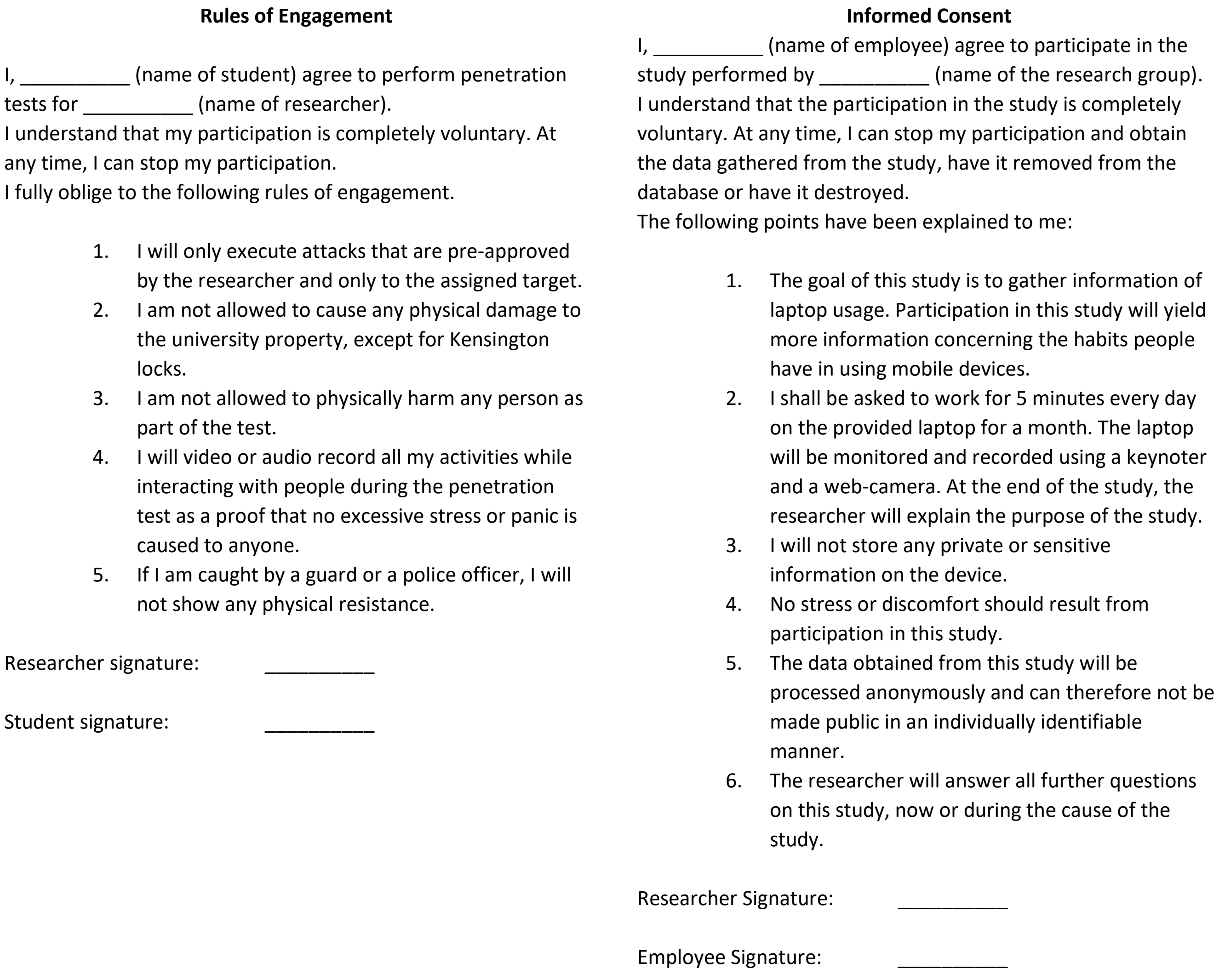
- **Execution**: The test begins with the penetration tester proposing attack scenarios, which are approved by both the coordinator and the security officer. The tester then executes the scenarios. If the tester is caught or reaches a termination condition, the contact person is immediately informed to prevent data exposure. When the tester successfully obtains the target asset, the contact person returns it to the custodian. If the asset is acquired without the custodian’s knowledge, the contact person needs to return it and remove the monitoring devices before the custodian reaches their office. Monitoring equipment records these activities, providing objective evidence.

- **Closure**: After the execution stage, the penetration tester compiles a report with all attempted attacks and provides it to the coordinator. The marked assets and monitoring equipment are returned to the security officer through the contact person. Not all socially engineered employees require debriefing, as it may cause more stress. The security officer decides who needs debriefing based on logs and monitoring data. Custodians, who initially gave consent, all need debriefing. However, this must be conducted thoughtfully to preserve trust. Three factors should be considered: custodians were deceived, privacy concerns due to monitoring equipment, and potential stress due to the interaction with the penetration tester. The focus of the debriefing should be on their contributions to identifying security vulnerabilities, with rewards for their participation.

The CF methodology was validated through eleven penetration tests by Dimkov et al. [24], each involving a marked laptop and various custodians. Different teams of students played the role of penetration testers, attempting to gain possession of the laptops. The tests revealed varying levels of resistance from employees, ranging from successfully acquiring the asset in most cases to one employee notifying security, which led to security guards searching the premises for suspicious activities.

Dimkov et al.’s experience with the CF methodology highlighted the importance of specifying what information the penetration tester can use, for example, knowledge about the cover story should be excluded. Additionally, panic situations need to be considered, as only the security officer knows about the test, as to not alert the security guards. The last noteworthy item to mention is that this test cannot be repeated many times, as the knowledge about it can spread quickly.

The CF methodology therefore aims to assess security while preserving the realism of the test without compromising the custodian's awareness and trust within the organization. It offers insights into social engineering vulnerabilities without violating privacy or causing undue stress.



Rules of Engagement

I, __________ (name of student) agree to perform penetration tests for __________ (name of researcher).
I understand that my participation is completely voluntary. At any time, I can stop my participation.
I fully oblige to the following rules of engagement.

1. I will only execute attacks that are pre-approved by the researcher and only to the assigned target.
2. I am not allowed to cause any physical damage to the university property, except for Kensington locks.
3. I am not allowed to physically harm any person as part of the test.
4. I will video or audio record all my activities while interacting with people during the penetration test as a proof that no excessive stress or panic is caused to anyone.
5. If I am caught by a guard or a police officer, I will not show any physical resistance.

Researcher signature: __________

Student signature: __________

Informed Consent

I, __________ (name of employee) agree to participate in the study performed by __________ (name of the research group).
I understand that the participation in the study is completely voluntary. At any time, I can stop my participation and obtain the data gathered from the study, have it removed from the database or have it destroyed.
The following points have been explained to me:

1. The goal of this study is to gather information of laptop usage. Participation in this study will yield more information concerning the habits people have in using mobile devices.
2. I shall be asked to work for 5 minutes every day on the provided laptop for a month. The laptop will be monitored and recorded using a keynoter and a web-camera. At the end of the study, the researcher will explain the purpose of the study.
3. I will not store any private or sensitive information on the device.
4. No stress or discomfort should result from participation in this study.
5. The data obtained from this study will be processed anonymously and can therefore not be made public in an individually identifiable manner.
6. The researcher will answer all further questions on this study, now or during the cause of the study.

Researcher Signature: __________

Employee Signature: __________

Figure 19: Exemplary "Rules of Engagement" and "Informed Consent" [24]

5.4.3 Conclusion on Penetration Test Methodologies

In this section, we evaluate methodologies based on specific criteria. The extent to which these criteria are met is determined by the rules of engagement, approved attack scenarios, and the overall structure of the methodologies. The evaluation primarily focuses on the structural aspects [24] of these methodologies:

Reliability:

- In the EF methodology, the penetration tester targets a non-critical asset, minimizing the impact on the custodian's productivity.
- In the CF methodology, the custodian's productivity may be affected, but the use of informed consent helps mitigate this impact.
- Neither methodology disrupts the productivity of other employees, since the penetration tester does not target their belongings without their consent.

Repeatability:

- The repeatability of such tests is challenging due to the unpredictable nature of human behavior. Evaluating repeatability would require a larger number of tests on multiple participants.

Reportability:

- Both methodologies provide detailed information in their reports, offering insights into how security measures were circumvented.

Respectfulness:

- Both methodologies involve a level of deception, which raises ethical concerns.
- The CF methodology manages to maintain trust between custodians and employees, as well as between employees and the organization. However, it may affect the trust between custodians and contact persons. In contrast, the EF methodology fails to preserve trust in these relationships.
- Deception in these methodologies may be considered justifiable based on specific criteria, including the principle of minimal risk and the importance of knowledge gained.
- Debriefing of participants is recommended, but it is advised to selectively debrief employees to prevent undue stress.

Realism:

- The EF methodology is less realistic in certain situations, as the custodian is aware of the test and not directly involved.
- The CF methodology is highly realistic since neither the custodian nor other employees are informed, making the test more authentic.

In summary, the Custodian-Focused methodology offers a more realistic and respectful approach to conducting penetration tests compared to the Environment-Focused methodology. CF enhances test authenticity by keeping the custodian unaware of the test, but it should be noted that this approach can potentially introduce stress to the custodian due to the element of deception.

On the other hand, the EF methodology, though less realistic, maintains minimal impact on trust relationships because the custodian is informed in advance. However, it still involves deceiving an employee.

Both methodologies raise ethical considerations due to the use of deception. Additionally, these penetration tests require a significant investment of time and resources. There is also the risk of a learning effect, where employees become more cautious once they become aware of such tests, which could potentially skew results. Moreover, if rumors about these tests spread through a company, it can further distort the outcomes.

But still, these testing methods are powerful tools for revealing social engineering vulnerabilities, but they must be employed judiciously. Careful planning, clear communication, and deliberate thorough debriefing of participants are essential to ensure that the tests yield valuable insights while respecting the well-being and trust of all involved parties.

5.5 Ethics

Throughout the preceding chapters, especially in our exploration of social engineering penetration tests, we have consistently emphasized the ethical aspects of this subject. Ethical concerns have arisen at various points during our discussions. We have encountered these concerns when examining the attacks themselves, which inherently transgress ethical codes, delving into the complexities of human psychology and the diverse reactions of different demographic groups to these attacks, examining various defense mechanisms, and dissecting the Environment-Focused and Custodian-Focused penetration testing methodologies.

As we have discovered, ethical considerations are a fundamental aspect of social engineering because it invariably involves deceiving fellow human beings. However, it is not only the initial attacks that mistreat the victims. In the aftermath, victims often endure blame and potentially even ridicule from colleagues. Furthermore, they may indirectly face consequences for displaying valuable employee qualities, such as trust, a willingness to assist colleagues, managers, and customers, and overall cooperative behavior [86]. It is important to note that these are precisely the qualities that social engineers seek to exploit.

Companies may employ penetration tests as a means to prevent such attacks. And although necessary to verify the integrity of social engineering defenses, just like actual attacks, planned attacks within the controlled framework of a penetration test can lead to similar issues. These tests can furthermore erode trust relationships, induce stress among employees, and create uncertainty about their future work. These adverse effects can result in reduced productivity and may even affect overall employee morale, potentially giving rise to other organizational challenges [24], [86]. This raises the crucial question: how should we act when confronted with ethical dilemmas?

Nonetheless, the matter of what is ethical and what is unethical is neither straightforward nor easily resolved. To gain a better understanding of how to address this question, we will delve into the study conducted by Mouton et al. [62]. Their paper sheds light on ethical concerns in the domains of public communication, penetration testing, and social engineering research. It further explores these concerns through the lenses of three normative ethics approaches: virtue ethics, utilitarianism, and deontology, which we will now examine. The objective of these approaches is to evaluate the ethics of specific actions, taking into account particular perspectives. Our analysis of these ethical frameworks will provide insights into how to approach questions of ethical soundness in general.

Virtue Ethics

Virtue ethics is a distinctive moral philosophy that places a strong emphasis on an individual's character and intrinsic virtues. Unlike other ethical frameworks that rely on external rules or consequences, virtue ethics prioritizes the inner moral qualities that guide behavior [62].

The term "virtue" refers to moral standards and desirable qualities such as honesty, fairness, kindness, and compassion. Virtue ethics raises profound questions, including "How should I live?" and "What kind of person should I aim to become?" It promotes personal growth and character development over rigid adherence to rules. According to Mouton et al. [62], a common test for ethical behavior is whether an action makes someone a better person. If the answer is affirmative, it can be considered ethical.

When applying virtue ethics to ethical considerations, the key assessment is whether the action aligns with virtuous traits. Virtuous individuals express these qualities genuinely, not out of mere obligation. For example, true virtue involves consistently displaying kindness and compassion, which is a reflection of one's character.

Virtue ethics fosters the development of one's personal character, the quest for moral excellence, and the genuine embodiment of virtuous attributes. It guides individuals toward moral integrity by instilling these principles within them.

However, applying this ethical framework within a company composed of individuals with potentially diverse values can be challenging. In such cases, it is advisable to establish a specific code of ethics that the company wishes to adhere to and what fits company culture. Mouton et al. [62] provide the ACM Code of Ethics and Professional Conduct [1] as an example, which is a well-known ethical code in the field of computer science research. The first chapter of this code, the “General Ethical Principles” [1], encompass the following seven key points.

A computing professional should...

1. *Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.*
2. *Avoid harm.*
3. *Be honest and trustworthy*

4. *Be fair and take action not to discriminate.*
5. *Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.*
6. *Respect privacy.*
7. *Honor confidentiality.*

Developing a code of ethics in a similar manner can assist organizations in determining the ethicality of actions. It can also guide the treatment of employees who fall victim to social engineering attacks. For instance, if an employee was deceived by a social engineer without any negligence on their part, should they face punishment? Would such punishment align with the organization's aspiration to be more virtuous? According to Mouton et al. [62], punishment in this scenario would be deemed unethical, as the employee should not bear the consequences for following the instructions provided by the employer.

Utilitarianism

Utilitarianism is a prominent branch of consequentialism, which assesses the ethical rightness of actions based on their outcomes. In utilitarianism, ethical judgments rely on the consequences an action generates, taking into account its impact on both individual interests and society at large [62].

To understand and evaluate utilitarianism, it is essential to consider how an action affects the well-being of the majority within society. An action is considered ethical if it benefits the majority and unethical if it does not. In the context of this paper, applying utilitarian ethics involves examining how a social engineering attack impacts not only the victim of said attack, but also anyone affected by its repercussions.

When looking at a company's perspective for example, this approach requires asking whether adopting a particular measure, such as a penetration test, benefits the entire organization more than it may harm the individual employee subjected to the test's pressure.

As utilitarianism underscores the importance of consequences regarding people's well-being, if a penetration test results in the overall well-being of the community, with the collective benefits outweighing any harm to the employee who might be deceived, utilitarians consider it ethically acceptable [62].

Deontology

Deontology is a moral framework that centers on unwavering adherence to established rules as the primary criterion for determining the morality of an action. Often termed "duty" or "obligation" based ethics, deontology asserts the existence of universal rules that govern what constitutes right and wrong behavior [62].

In deontological ethics, the fundamental principle of treating others only in ways to which they have consented serves as guidance. An action is considered ethical if it complies with these moral rules, irrespective of the potential consequences it may produce [62].

When deontological ethics is applied to an ethical dilemma, like a penetration test, it entails a rigorous evaluation of whether the test aligns with the moral rules established by the company, regardless of any foreseeable outcomes. If any aspect of the penetration test transgresses these deontological principles, the entire action may be deemed unethical. Conversely, if the penetration test fully adheres to these rules, it is regarded as ethically sound.
Choosing a specific ethical framework provides a company with a reference point for addressing moral questions as they arise. However, these questions can often be challenging to answer. For instance, we can consider whether conducting a penetration test is ethical from the perspective of virtue ethics. The company may conclude that it is unethical because it involves deceiving an employee. Yet, if an actual attack were to occur and compromise the defense mechanisms, customer data could be stolen. These customers entrusted

their data to the company, and the company has an obligation to protect them. Therefore, not conducting penetration tests might be considered unethical, as it could overlook potential vulnerabilities and therefore endanger customer data.

To demonstrate how different ethical frameworks address specific questions, Mouton et al. attempted to answer ethical questions from the viewpoints of various ethical schools. A company may employ a similar approach to determine the ethicality of certain actions, especially when choosing to follow a single ethical framework seems impractical. As an illustration, we will examine how Mouton et al. [62] practically implemented this. They offered these varying responses to the following question based on the stated school of ethics:

> *Is conducting social engineering awareness research ethical, and what is the proper debriefing process?*
>
> **Virtue Ethics**: *From an external standpoint, it may appear ethical since social engineering awareness testing is necessary research. However, it necessitates proper debriefing to align with ethical standards. The ACM codes of ethics as an example, emphasizes responsibility, avoiding harm, and contributing to human well-being, which includes thorough debriefing* [62].
>
> **Utilitarianism**: *Utilitarianism deems research ethical if it ultimately benefits society, even if some participants experience harm. As long as the research aims to improve society as a whole, it aligns with utilitarian ethics. Any research contributing to the greater good is considered ethical from this perspective* [62].
>
> **Deontology**: *Deontology requires adhering to moral rules, including not deceiving or tricking research participants. Since social engineering awareness testing involves deception, it conflicts with deontological ethics, which deems such behavior unethical* [62].

This comparison can be performed for various ethical frameworks to determine whether an action can be considered ethical. Alternatively, a series of questions may assist in identifying an ethical framework that aligns with the company's culture and values.

These are just a few examples of various ethical frameworks. The objective of this thesis is not to determine which one is best suited for use within a company or to conclusively establish what is considered ethical or not. Instead, the goal is to encourage the consideration of ethical implications related to victimized parties, as well as the consequences stemming from penetration tests and studies involving the susceptibility of specific demographic groups, along with various other aspects of the social engineering landscape. The mentioned ethical frameworks serve as potential models for constructing a company-wide code of ethics. Nevertheless, delving into a comprehensive discussion of the merits of each ethical framework is beyond the scope of this thesis. Further analysis is required to gain a comprehensive understanding of this subject and to make well-informed decisions

5.6 Disaster Recovery

To conclude our chapter on social engineering defenses, we need to consider scenarios where implemented defense mechanisms fail. This can occur due to a variety of reasons, including employee negligence, the exploitation of new social engineering attack vectors, or technical vulnerabilities that expose an organization's systems to potential infiltration. The importance of preparation cannot be overstated. To remind ourselves, statistics from Cybercrime Magazine [18] reveal that 60% of businesses victimized by social engineering attacks closed their doors within six months of the incident. Furthermore, the financial repercussions can be substantial, with the average cost of a successful attack, as reported in Varonis' 2021 Data Risk Report for Financial Services [95], amounting to nearly six million dollars.

A significant part of this problem can be attributed to insufficient attention to an organization's disaster recovery capabilities. Consider a scenario where an attacker encrypts critical data and demands a ransom for decryption. If the ransom cannot be paid, the files are damaged, or no decryption key is provided, the consequences can be devastating.

Hence, having a well-defined recovery plan in place is crucial not only to mitigate the risks associated with social engineering but also to address broader threats like cybercrime in general, natural disasters, accidents, and technical malfunctions. This importance was underscored by Alharthi and Regan [3], who emphasized the need for a well-structured disaster management strategy to effectively manage unforeseen events and facilitate recovery. In this chapter, we will explore the critical components of disaster recovery planning and its relevance within the broader context of security and business continuity.

To help organizations secure their critical assets, there are various guidelines and standards they can follow. For instance, the International Organization for Standardization (ISO) has developed standards such as ISO 22301 [112] for business continuity and ISO 27031 [113] for disaster recovery. Another example is the BSI-Standard 200-4 [14] from the German Federal Office for Information Security, which focuses on Business Continuity Management and assists organizations in establishing their own Business Continuity Management System (BCMS).

A Business Continuity Management System (BCMS) is a comprehensive framework designed to proactively prepare organizations for potential disruptions or disasters that could threaten their operations. The primary objective of a BCMS is to ensure the continuity of critical business functions and minimize the impact of incidents that may disrupt regular operations.

Although these standards vary, they all share a common goal of enhancing an organization's resilience in the face of unpredictable threats to day-to-day operations. In the case of ISO standards, companies have the option to pursue ISO certifications. It is worth noting that planning for emergencies is legally mandated for some companies in certain industries such as utilities, transportation, healthcare, and public services [112].

In addition to these standards, involving the public in disaster recovery planning can raise stakeholder awareness of risks and garner support for resilience-building policies [3]. In the case of companies, it may also be advantageous to engage employees in the planning process to foster awareness and cultivate a security-conscious environment.

The specific contents of these BCMSs may vary, but they typically encompass the following key elements [14], [112], [113]:

1. **Risk Assessment and Analysis**: The first step in building a BCMS involves identifying and assessing potential risks and threats to the organization. This includes natural disasters, technological failures, social engineering attacks, cyberattacks, supply chain disruptions, and other incidents that could affect business operations.

2. **Business Impact Analysis (BIA)**: BIA helps organizations evaluate the consequences of a disruption, such as financial losses, damage to reputation, and legal issues. This analysis helps in prioritizing critical business functions and setting recovery time objectives (RTOs) and recovery point objectives (RPOs).

3. **Business Continuity Strategy**: Organizations need to develop strategies to maintain essential functions and services during a crisis. This may involve creating backup sites, implementing redundant systems, and outlining procedures for resuming operations.

4. **Response and Recovery Plans**: Detailed plans are created to guide actions during and after an incident. These plans include communication strategies, resource allocation, and recovery procedures. They ensure that all employees know their roles and responsibilities during a crisis.

5. **Testing and Exercises**: Regular testing and simulation exercises are conducted to evaluate the effectiveness of the BCMS. This helps identify weaknesses and areas for improvement. Exercises range from discussions to full-scale drills.

6. **Monitoring and Review**: Continuous improvement is a fundamental principle of a BCMS. Organizations must regularly monitor their BCMS and review its performance to ensure it remains effective and relevant. Feedback and lessons learned from real incidents and tests are incorporated into the system.

7. **Documentation**: A comprehensive and well-documented BCMS ensures that processes are consistent, transparent, and accessible to all relevant personnel. Documentation includes plans, procedures, contact lists, and recovery strategies.

8. **Crisis Communication**: Effective communication is crucial during a crisis. A BCMS includes plans for internal and external communication to keep employees, stakeholders, customers, and the public informed and reassured.

9. **Compliance and Legal Aspects**: BCMS often includes a focus on compliance with relevant laws, regulations, and industry standards, as well as legal aspects like data protection and privacy.

10. **Certification and Auditing**: Organizations may seek certification under standards like ISO 22301, which demonstrates their commitment to business continuity. Auditing is conducted to ensure compliance and evaluate the effectiveness of the BCMS.

A Business Continuity Management System (BCMS) provides a structured approach to enhance an organization's resilience, particularly in industries where downtime can lead to substantial financial losses, reputational damage, or public safety threats. It is well-suited to safeguard a company against the consequences of a successful social engineering attack. A well-implemented BCMS accelerates recovery, maintains stakeholder trust, and ensures the continuity of vital services. To achieve ISO certification or implement a BCMS, it is advisable to seek guidance from the mentioned reference materials or specialized third-party providers.

However, it is crucial to understand that a BCMS is not a substitute for comprehensive defense mechanisms like robust policies, awareness training, and a blend of digital and physical security measures. Instead, it serves as an effective last resort when other measures fail, with the added advantage of preparing for a wider range of potential threats.

6 Best Practices

After our comprehensive exploration of various aspects of social engineering, we can now summarize the essential measures needed to prepare any company for defending against social engineering attacks. Combatting social engineering requires a multifaceted approach, encompassing policies, employee training, technology, and a security-conscious culture within the organization. Drawing from our previous discussions, we present the recommended best practices for companies to effectively counter social engineering:

1. **Security Awareness Training:**
   - Provide regular and comprehensive security awareness training to all employees, ensuring they grasp various social engineering tactics like phishing, pretexting, baiting, and tailgating, as well as the significance of security policies.
   - New employees especially must undergo mandatory training courses before obtaining access to critical systems. Ideally, participation in these courses should take place before the first day of work. It is important to account for employees who miss their initial training when planning their tasks. This consideration ensures that they do not have access to important files they would typically handle.
   - Training should encompass various formats, such as serious games, which serve a dual purpose by educating employees and eliciting security goals. This approach, along with courses, online seminars, and tests to assess knowledge, helps employees understand and meet security objectives effectively.
   - Tailor training frequency and depth based on job roles (e.g., security guards and secretaries may require more frequent and in-depth training).
   - Pay attention to the design of these training programs and the necessary requirements to ensure they have a lasting impact and are memorable for employees.

2. **Establish a Security Culture**:
   - Foster a pervasive culture of security, where employees actively participate in safeguarding the organization.

3. **Recognizing Red Flags**:
   - Instruct employees to identify common red flags in social engineering attempts, such as unsolicited requests for sensitive information, unusual email addresses, or inconsistencies in communication.

4. **Verify Requests**:
   - Encourage employees to independently verify requests for sensitive information or actions, especially when they receive unusual or unexpected requests. Utilize established contact information for verification.

5. **Establishing Policies and Regulatory Compliance**:
   - Develop and communicate clear security policies that address various attack vectors while ensuring compliance with relevant data protection and privacy regulations.
   - Follow the research findings to understand what is necessary for achieving compliance with information security among employees.

6. **Data Classification and Handling**:
   - Implement well-defined data classification policies to identify sensitive information, coupled with educating employees on secure data handling and sharing.
   - Develop secure procedures for disposing of sensitive information, whether in printed or digital form.

7. **Access Control**:
   - Enforce strict access control and least privilege principles to limit employee access to information, thus reducing vulnerability to social engineering attacks.
   - Implement practices such as visitor escorting and identity verification for enhanced physical security.

8. **Digital Hygiene**:
   - Promote strong password practices, including regular updates and discouraging password sharing. Employ multi-factor authentication where feasible.
   - Automatically expire passwords as needed.
   - Grant administrative privileges only in response to necessary user requests.
   - Regularly review and revoke unnecessary admin privileges.

9. **Email Security and Vendor Verification**:
   - Implement robust email security measures, including anti-phishing filters, email authentication protocols, and user-friendly email warnings about potentially suspicious messages.
   - Teach employees the importance of email encryption and when to employ it.
   - Ensure third-party vendors also adhere to stringent security practices, including credible email communication verification.
   - Teach employees the importance of email encryption and when and how to employ it.

10. **Physical Security**:
    - Ensure physical security through measures like badge access control, visitor logs, and raising employee awareness of tailgating risks.
    - Educate staff in roles vulnerable to specific social engineering attacks like piggybacking and diversion theft.
    - Deploy physical security enhancements such as fences, cameras, security doors, and turnstiles as required to prevent breaches.
    - When terminating an employee, promptly deactivate their user accounts and provide escort services to the exit.

11. **Incident Response and Employee Vigilance**:
    - Develop and regularly update an incident response plan that addresses social engineering incidents.
    - Foster a "see something, say something" culture, encouraging employees to trust their instincts and report suspicious or unusual situations.

12. **Phishing Simulations**:
    - Conduct routine phishing simulations to assess and enhance employees' ability to recognize and respond to phishing attempts. Ensure ethical treatment of participants and prevent data exposure.

13. **Employee Support**:
    - Offer psychological and emotional support to employees who may become victims of social engineering attacks. Create an environment where reporting incidents is encouraged without fear of blame.

14. **Cybersecurity Technology**:
    - Invest in robust cybersecurity tools and technologies, such as endpoint protection, intrusion detection systems, and security information and event management (SIEM) systems to detect and prevent social engineering attacks.

15. **Regular Audits and Continuous Updates**:
    - Perform regular security audits and assessments to identify vulnerabilities and areas for improvement, while keeping security policies and training materials updated to address emerging social engineering techniques and threats.

16. **Senior Leadership Involvement**:
    - Encourage senior leadership to lead by example, adhering to security protocols and communicating the organization's commitment to security.

In conclusion, safeguarding an organization against social engineering attacks is a multifaceted endeavor that hinges on a combination of robust security policies, vigilant employees, cutting-edge technology, and a culture of security consciousness. Throughout this chapter, we have delved into various facets of social engineering prevention, including employee training, access controls, digital hygiene, email security, and physical security. The importance of continuous updates, senior leadership involvement, and compliance with regulatory standards has also been emphasized.

It is crucial to understand that the battle against social engineering is an ongoing one, with adversaries constantly evolving their tactics. By implementing the recommended best practices outlined in this chapter, organizations can significantly reduce their vulnerability to social engineering attacks, protect sensitive data, and maintain the trust of both employees and customers. As organizations adapt to emerging threats, they must remain proactive, adaptable, and committed to a culture of security.

7 Conclusion

As we conclude our exploration of the recommended best practices, we bring our analysis of the intricate landscape of social engineering to an end. This investigation has equipped us with a comprehensive understanding of the various facets that define this evolving threat. From the classification and analysis of social engineering attacks to an exploration of the human factors that contribute to susceptibility, we have dissected the mechanisms and vulnerabilities at play.

Throughout our journey, we have highlighted the vital role of robust policies in fortifying an organization's defenses against social engineering attacks. These policies are more than static documents; they are living guidelines that require careful design to ensure they are not only effective but also memorable, leaving a lasting impression on the workforce.

In addition to our exploration, we have emphasized the significance of ethical considerations on various fronts. Ethical demographic research is pivotal to prevent discrimination and ensure that the human element in security remains equitable. Ethical penetration testing practices are equally critical, guiding the responsible use of powerful tools while respecting the rights and dignity of employees.

Looking to the future, the landscape of social engineering continues to evolve, presenting new challenges and threats. Emerging technologies, such as AI-driven content generation tools, pose novel risks that demand further research and innovation in detection and prevention strategies. The adaptation and enhancement of our security measures are essential to stay ahead of these threats.

Furthermore, these evolving challenges emphasize the necessity of cross-industry collaboration. Social engineering threats affect not only individual organizations but entire sectors and industries. By establishing networks for information exchange and joint strategies, we can collectively respond to these emerging risks. In this interconnected digital age, a collaborative approach, extending beyond organizational boundaries, will be crucial in fortifying our defenses and ensuring the resilience of our digital infrastructure against evolving social engineering attacks.

In this ever-shifting landscape, a holistic approach that combines employee education, robust policies, advanced technology, and ethical considerations remains the foundation for effectively combating social engineering. As we continue to adapt to new challenges, our unwavering commitment to security, ethics, and vigilance will be our strongest assets in the ongoing battle against social engineering threats.

Appendix

List of Abbreviations

ACM	Association for Computing Machinery
ACL	Access Control Lists
BC	Business Continuity
BCIA	Business Impact Analysis
BCMS	Business Continuity Management System
BEC	Business Email Compromise Phishing
BYOD	Bring Your Own Device
CF	Custodian-Focused
CFO	Chief Financial Officer
CIAT	Confidentiality, Integrity, Availability triad
CFR	U.S. Council on Foreign Relations
CMC	Computer-mediated Competence
CEO	Chief Executive Officer
DITF	Door in the Face Technique
DNS	Domain Name System
DR	Disaster Recovery
DRM	Digital Rights Management
EF	Environment-Focused
FOMO	Fear of Missing Out
IDT	Interpersonal Deception Theory
InfoSec	Information Security
ISA	Information Security Awareness
ISP	Information Security Policy
ISO	International Organization for Standardization
MFA	Multi-Factor Authentication
NAC	Network Access Control
NIST	National Institute for Standards and Technology
R*	Realistic, Reliable, Respectful, Repeatable
RaaS	Ransomware-as-a-Service
RPO	Recovery Point Objectives
RTO	Recovery Time Objectives
SE-ISP	Social Engineering Information Security Policy
SET	Social Engineering Toolkit
SETA	Security Education, Training, and Awareness
SIEM	Security Information and Event Management
SMS	Short Message Service
UBA	User Behavior Analytics
VoIP	Voice over IP
WAF	Web Application Firewalls

Bibliography

[1] ACM Code 2018 Task Force, “ACM Code of Ethics and Professional Conduct.” Accessed: Oct. 31, 2023. [Online]. Available: https://www.acm.org/code-of-ethics

[2] H. Aldawood and G. Skinner, “Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal,” 2019.

[3] D. Alharthi and A. Regan, “A Literature Survey and Analysis on Social Engineering Defense Mechanisms and Infosec Policies,” *IJNSA*, vol. 13, no. 2, pp. 41–61, Mar. 2021, doi: 10.5121/ijnsa.2021.13204.

[4] I. Al-Shanfari, Y. Warusia, T. Nasser, I. Roesnita, and I. Anuar, “Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees,” *IJACSA*, vol. 13, no. 8, 2022, doi: 10.14569/IJACSA.2022.0130855.

[5] S. E. Asch, *Groups, Leadership and Men: Research in Human Relations*. Carnegie Press, 1951. ISBN: 978-0-608-11271-8

[6] S. E. Asch, “Studies of independence and conformity: I. A minority of one against a unanimous majority.,” *Psychological Monographs: General and Applied*, vol. 70, no. 9, pp. 1–70, 1956, doi: 10.1037/h0093718.

[7] M. Bakhuys Roozeboom, G. Visschedijk, and E. Oprins, “The effectiveness of three serious games measuring generic learning features,” *Brit J Educational Tech*, vol. 48, no. 1, pp. 83–100, Jan. 2017, doi: 10.1111/bjet.12342.

[8] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, “A comprehensive survey of AI-enabled phishing attacks detection techniques,” *Telecommun Syst*, vol. 76, no. 1, pp. 139–154, Jan. 2021, doi: 10.1007/s11235-020-00733-2.

[9] K. Beckers and S. Pape, “A Serious Game for Eliciting Social Engineering Security Requirements,” in *2016 IEEE 24th International Requirements Engineering Conference (RE)*, Beijing, China: IEEE, Sep. 2016, pp. 16–25. doi: 10.1109/RE.2016.39.

[10] F. Bélanger, S. Collignon, K. Enget, and E. Negangard, *Determinants of early conformance with information security policies*, 54th ed. in Information & Management, no. 7. 2017.

[11] D. Bersei, K. Dolgopolov, O. Amvrosova, T. Zhukova, and L. Sherbakova, “CLASSIFICATION OF SOCIAL ENGINEERING METHODS AND TYPES OF SOCIAL ENGINEERING ATTACKS”.

[12] F. Breda, H. Barbosa, and T. Morais, “SOCIAL ENGINEERING AND CYBER SECURITY,” presented at the International Technology, Education and Development Conference, Valencia, Spain, Mar. 2017, pp. 4204–4211. doi: 10.21125/inted.2017.1008.

[13] 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,” *Journal of Investigative Psychology and Offender Profiling*, vol. 15, no. 1, pp. 20–45, 2018, doi: 10.1002/jip.1482.

[14] Bundesamt für Sicherheit in der Informationstechnik, “BSI-Standard 200-4,” Bundesamt für Sicherheit in der Informationstechnik. Accessed: Oct. 24, 2023. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management.html?nn=531576

[15] M. Butavicius, K. Parsons, M. Pattinson, and A. McCormac, “Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails,” 2015.

[16] Centigrade GmbH, “Cyber Security Training durch Serious Games · Centigrade GmbH.” Accessed: Oct. 19, 2023. [Online]. Available: https://www.centigrade.de/de/referenzen/cyber-security-training-serious-games

[17] R. B. Cialdini, *Influence: The Psychology of Persuasion*. Harper Collins. ISBN: 0-688-12816-5

[18] Cybercrimemag, “Cybercrime To Cost The World $10.5 Trillion Annually By 2025,” Cybercrime Magazine. Accessed: Jul. 10, 2023. [Online]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[19] A. P. C. Davies, A. T. Goetz, and T. K. Shackelford, “Exploiting the beauty in the eye of the beholder: The use of physical attractiveness as a persuasive tactic,” *Personality and Individual Differences*, vol. 45, no. 4, pp. 302–306, Sep. 2008, doi: 10.1016/j.paid.2008.04.016.

[20] Deep Secure, “What is the Price of Loyalty?” Deep Secure. Accessed: Oct. 02, 2023. [Online]. Available: https://www.deep-secure.com/reports/49-what-is-the-price-of-loyalty.php

[21] Deloitte, “91% of all cyber attacks begin with a phishing email to an unexpected victim | Deloitte Malaysia | Risk Advisory | Press releases,” Deloitte Malaysia. Accessed: Sep. 22, 2023. [Online]. Available: https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

[22] Deutschlandfunk, “Betrug mit Schockanrufen - Wie Kriminelle ihren Opfern Angst einjagen und abkassieren,” Deutschlandfunk. Accessed: Oct. 11, 2023. [Online]. Available: https://www.deutschlandfunk.de/kriminelles-geschaeft-mit-schockanrufen-100.html

[23] A. Diaz, A. T. Sherman, and A. Joshi, “Phishing in an Academic Community: A Study of User Susceptibility and Behavior.” arXiv, Nov. 14, 2018. Accessed: Oct. 13, 2023. [Online]. Available: http://arxiv.org/abs/1811.06078

[24] T. Dimkov, A. Van Cleeff, W. Pieters, and P. Hartel, “Two methodologies for physical penetration testing using social engineering,” in *Proceedings of the 26th Annual Computer Security Applications Conference*, Austin Texas USA: ACM, Dec. 2010, pp. 399–408. doi: 10.1145/1920261.1920319.

[25] I. E. Espinosa-Curiel *et al.*, “HelperFriend, a Serious Game for Promoting Healthy Lifestyle Behaviors in Children: Design and Pilot Study,” *JMIR Serious Games*, vol. 10, no. 2, p. e33412, May 2022, doi: 10.2196/33412.

[26] P. Finn and M. Jakobsson, “Designing and Conducting Phishing Experiments”, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4135777

[27] J. Firch, “10 Cyber Security Trends You Can’t Ignore In 2021,” PurpleSec. Accessed: Sep. 13, 2023. [Online]. Available: https://purplesec.us/cyber-security-trends-2021/

[28] W. R. Flores, H. Holm, M. Nohlberg, and M. Ekstedt, *Investigating personal determinants of phishing and the effect of national culture*. 2015.

[29] E. Fokides, P. Atsikpasi, P. Kaimara, and I. Deliyannis, “Factors Influencing the Subjective Learning Effectiveness of Serious Games,” *JITE:Research*, vol. 18, pp. 437–466, 2019, doi: 10.28945/4441.

[30] P. Gilbert, “The relationship of shame, social anxiety and depression: the role of the evaluation of social rank,” *Clinical Psychology & Psychotherapy*, vol. 7, no. 3, pp. 174–189, Jul. 2000, doi: 10.1002/1099-0879(200007)7:3<174::AID-CPP236>3.0.CO;2-U.

[31] S. Goel, K. Williams, and E. Dincelli, “Got Phished? Internet Security and Human Vulnerability,” *JAIS*, vol. 18, no. 1, pp. 22–44, Jan. 2017, doi: 10.17705/1jais.00447.

[32] R. Goyette, Y. Robichaud, and F. Marinier, “A Research Agenda for Security Engineering,” *Technology Innovation Management Review*, 2013.

[33] F. L. Greitzer, O. A. Kuchar, and K. Huston, “Cognitive science implications for enhancing training effectiveness in a serious gaming context,” *J. Educ. Resour. Comput.*, vol. 7, no. 3, p. 2, Nov. 2007, doi: 10.1145/1281320.1281322.

[34] T. Halevi, N. Memon, and O. Nov, “Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks,” *SSRN Journal*, 2015, doi: 10.2139/ssrn.2544742.

[35] B. Hanus, Y. A. Wu, and J. Parrish, “Phish Me, Phish Me Not.” Journal of Computer Information Systems, 2021. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/08874417.2020.1858730

[36] C. Happ, A. Melzer, and G. Steffgen, “Trick with treat – Reciprocity increases the willingness to communicate personal data,” *Computers in Human Behavior*, vol. 61, pp. 372–377, Aug. 2016, doi: 10.1016/j.chb.2016.03.026.

[37] T. Herath and H. R. Rao, “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness,” *Decision Support Systems*, vol. 47, no. 2, pp. 154–165, May 2009, doi: 10.1016/j.dss.2009.02.005.

[38] A. Herrmann, A. Morali, S. Etalle, and R. Wieringa, “RiskREP: Risk-Based Security Requirements Elicitation and Prioritization”.

[39] P. Herrmann and G. Herrmann, “Security requirement analysis of business processes,” *Electron Commerce Res*, vol. 6, no. 3–4, pp. 305–335, Oct. 2006, doi: 10.1007/s10660-006-8677-7.

[40] Y. Hilton and J. Cherdantseva, *Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals*. in Organizational, Legal, and Technological Dimensions of Information System Administrator. IGI Global Publishing, 2013.

[41] N. Ismail, "The curse of the ex-employee," Information Age. Accessed: Oct. 02, 2023. [Online]. Available: https://www.information-age.com/curse-ex-employee-6828/

[42] K. Ivaturi and L. Janczewski, "A Taxonomy for Social Engineering attacks", [Online]. Available: https://aisel.aisnet.org/confirm2011/15/

[43] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing," 2007. Accessed: Oct. 13, 2023. [Online]. Available: https://webpages.charlotte.edu/richter/classes/2007/6010/readings/phishing-preprint.pdf

[44] W. L. Johnson, "Serious Use of a Serious Game for Language Learning", doi: 10.3233/JAI-2010-0006.

[45] M. Junger, L. Montoya, and F.-J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," *Computers in Human Behavior*, vol. 66, pp. 75–87, Jan. 2017, doi: 10.1016/j.chb.2016.09.012.

[46] Kali Linux, "Penetration Testing and Ethical Hacking Linux Distribution," Kali Linux. Accessed: Sep. 27, 2023. [Online]. Available: https://www.kali.org/

[47] R. Kanthan and J.-L. Senger, "The Impact of Specially Designed Digital Games-Based Learning in Undergraduate Pathology and Medical Education," *Arch Pathol Lab Med*, vol. 135, 2011.

[48] H. Khachunts, "What is Diversion Theft? Attack and Defense Strategies," Security Boulevard. Accessed: Sep. 25, 2023. [Online]. Available: https://securityboulevard.com/2022/02/what-is-diversion-theft-attack-and-defense-strategies/

[49] C. Klimmt, *Serious games and social change: Why they (should) work*, vol. Serious games: Mechanisms and effects. Routledge, 2009.

[50] N. Kostic, "The 15 Most Famous Social Engineering Attacks," phoenixNAP Blog. Accessed: Sep. 19, 2023. [Online]. Available: https://phoenixnap.com/blog/social-engineering-examples

[51] J. Kröger, "Ransomware-as-a-Service nimmt zu - Im Darknet lässt sich Ransomware einfach mieten," IT-SERVICE.NETWORK Blog. Accessed: Sep. 25, 2023. [Online]. Available: https://it-service.network/blog/2021/07/05/ransomware-as-a-service-raas/

[52] W. Li *et al.*, "Experimental Investigation of Demographic Factors Related to Phishing Susceptibility," *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020, [Online]. Available: https://pdfs.semanticscholar.org/dbd1/d236dbf9548c0a4a44d001b2e5d1300fa76d.pdf

[53] T. Lin *et al.*, "Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content," *ACM Trans. Comput.-Hum. Interact.*, vol. 26, no. 5, pp. 1–28, Oct. 2019, doi: 10.1145/3336141.

[54] L. Liu, E. Yu, and J. Mylopoulos, "Security and privacy requirements analysis within a social setting," in *Journal of Lightwave Technology*, Monterey Bay, CA, USA: IEEE Comput. Soc, 2003, pp. 151–161. doi: 10.1109/ICRE.2003.1232746.

[55] C. E. Lively, "Psychological Based Social Engineering," *GIAC practical repository*, 2004, [Online]. Available: https://www.giac.org/paper/gsec/3547/psychological-based-social-engineering/105780

[56] T. Mataracioglu and S. Ozkan, "Towards a Security Lifecycle Model against Social Engineering Attacks: SLM-SEA".

[57] S. Milgram, "Behavioral Study of obedience.," *The Journal of Abnormal and Social Psychology*, vol. 67, no. 4, pp. 371–378, Oct. 1963, doi: 10.1037/h0040525.

[58] K. D. Mitnick and L. S. William, *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley, 2002.

[59] J. G. Mohebzada, A. E. Zarka, A. H. Bhojani, and A. Darwish, "Phishing in a university community: Two large scale phishing experiments," Abu Dhabi, United Arab Emirates, 2012 International Conference on Innovations in Information Technology (IIT), 2012. doi: 10.1109/INNOVATIONS.2012.6207742.

[60] H. Mouratidis and P. Giorgini, "Secure Tropos: A Security-Oriented Extension of the Tropos Methodology," *Int. J. Soft. Eng. Knowl. Eng.*, vol. 17, no. 02, pp. 285–309, Apr. 2007, doi: 10.1142/S0218194007003240.

[61] F. Mouton, L. Leenen, M. M. Malan, and H. S. Venter, “Towards an Ontological Model Defining the Social Engineering Domain,” in *ICT and Society*, vol. 431, K. Kimppa, D. Whitehouse, T. Kuusela, and J. Phahlamohlaka, Eds., in IFIP Advances in Information and Communication Technology, vol. 431. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 266–279. doi: 10.1007/978-3-662-44208-1_22.

[62] F. Mouton, M. M. Malan, K. K. Kimppa, and H. S. Venter, “Necessity for ethics in social engineering research,” *Computers & Security*, vol. 55, pp. 114–127, Nov. 2015, doi: 10.1016/j.cose.2015.09.001.

[63] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, “Social engineering attack framework,” in *2014 Information Security for South Africa*, Johannesburg, South Africa: IEEE, Aug. 2014, pp. 1–9. doi: 10.1109/ISSA.2014.6950510.

[64] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[65] J. Nicholson, L. Coventry, and P. Briggs, “Can We Fight Social Engineering Attacks By Social Means? Assessing Social Salience as a Means to Improve Phish Detection”, [Online]. Available: https://www.usenix.org/system/files/conference/soups2017/soups2017-nicholson.pdf

[66] D. Noll, “The Dollar Auction Game: A Lesson in Conflict Escalation,” Mediate.com. Accessed: Oct. 06, 2023. [Online]. Available: https://mediate.com/the-dollar-auction-game-a-lesson-in-conflict-escalation/

[67] P. Petridis *et al.*, “State-of-the-art in Business Games,” *IJSG*, vol. 2, no. 1, Feb. 2015, doi: 10.17083/ijsg.v2i1.54.

[68] A. Redhead and S. Davey, “Serious Games for First Responders,” in *Serious Games for Enhancing Law Enforcement Agencies*, B. Akhgar, Ed., in Security Informatics and Law Enforcement. , Cham: Springer International Publishing, 2019, pp. 173–188. doi: 10.1007/978-3-030-29926-2_10.

[69] A. Rege, T. Nguyen, and R. Bleiman, “A social engineering awareness and training workshop for STEM students and practitioners,” in *2020 IEEE Integrated STEM Education Conference (ISEC)*, Princeton, NJ, USA: IEEE, Aug. 2020, pp. 1–6. doi: 10.1109/ISEC49744.2020.9280596.

[70] H. J. Reynolds, B. C. Soulliard, and R. A. DeLaura, “NASPlay: A Serious Game for Air Traffic Control,” vol. 23, no. 1, 2019.

[71] R. M. Rodriguez, A. Atyabi, and Shouhuai, “Social Engineering Attacks and Defenses in the Physical World vs. Cyberspace: A Contrast Study.” arXiv, Mar. 09, 2022. Accessed: Aug. 02, 2023. [Online]. Available: http://arxiv.org/abs/2203.04813

[72] F. Salahdine and N. Kaabouch, “Social Engineering Attacks: A Survey.” 2019. [Online]. Available: https://www.mdpi.com/1999-5903/11/4/89

[73] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, “Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Atlanta Georgia USA: ACM, Apr. 2010, pp. 373–382. doi: 10.1145/1753326.1753383.

[74] H. Siadati, T. Nguyen, and P. Gupta, “Mind your SMSes: Mitigating social engineering in second factor authentication”, [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S016740481630116X?via%3Dihub

[75] J. Sibley, “Social Engineering - The Intersection of Artificial Intelligence,” VerSprite. Accessed: Oct. 27, 2023. [Online]. Available: https://versprite.com/blog/the-intersection-of-artificial-intelligence-and-social-engineering-next-generation-threats/

[76] M. Siponen, S. Pahnila, and A. Mahmood, “Employees’ Adherence to Information Security Policies: An Empirical Study,” in *New Approaches for Security, Privacy and Trust in Complex Environments*, vol. 232, H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. Von Solms, Eds., in IFIP International Federation for Information Processing, vol. 232. , Boston, MA: Springer US, 2007, pp. 133–144. doi: 10.1007/978-0-387-72367-9_12.

[77] C. Soghoian, “Legal risks for phishing researchers,” presented at the 2008 eCrime Researchers Summit, Atlanta, GA, USA: IEEE, Oct. 2008. doi: 10.1109/ECRIME.2008.4696971.

[78] B. M. Staw, *Knee-deep in the big muddy: a study of escalating commitment to a chosen course of action*. in Organizational behavior and human performance. 1976.

[79] 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.

[80] G. Tally, R. Thomas, and T. Van Vleck, “Best Practices for Institutions and Consumers,” 2004, [Online]. Available: https://www.researchgate.net/publication/245425937_Anti-Phishing_Best_Practices_for_Institutions_and_Consumers

[81] TheFourSec, “Social Engineering Technique: The Watering Hole Attack,” Medium. Accessed: Sep. 25, 2023. [Online]. Available: https://medium.com/@thefoursec/social-engineering-technique-the-watering-hole-attack-9ee3d2ca17b4

[82] A. V. Lamsweerde and E. Letier, “Handling obstacles in goal-oriented requirements engineering,” *IEEE Trans. Software Eng.*, vol. 26, no. 10, pp. 978–1005, Oct. 2000, doi: 10.1109/32.879820.

[83] M. A. Vugts, A. M. Zedlitz, M. C. Joosen, and H. J. Vrijhoef, “Serious Gaming During Multidisciplinary Rehabilitation for Patients With Chronic Pain or Fatigue Symptoms: Mixed Methods Design of a Realist Process Evaluation,” *J Med Internet Res*, vol. 22, no. 3, p. e14766, Mar. 2020, doi: 10.2196/14766.

[84] Z. Wang, H. Zhu, P. Liu, and L. Sun, “Social engineering in cybersecurity: a domain ontology and knowledge graph application examples,” *Cybersecur*, vol. 4, no. 1, p. 31, Dec. 2021, doi: 10.1186/s42400-021-00094-6.

[85] Z. Wang, H. Zhu, and L. Sun, “Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods,” *IEEE Access*, vol. 9, pp. 11895–11910, 2021, doi: 10.1109/ACCESS.2021.3051633.

[86] A. H. Washo, “An interdisciplinary view of social engineering: A call to action for research,” *Computers in Human Behavior Reports*, vol. 4, p. 100126, Aug. 2021, doi: 10.1016/j.chbr.2021.100126.

[87] A. Waude, “Foot-in-the-Door As A Persuasive Technique.” Accessed: Oct. 05, 2023. [Online]. Available: https://www.psychologistworld.com/behavior/compliance/strategies/foot-in-door-technique

[88] A. Waude, “The Door-in-the-Face Technique: Persuading People To Agree To Requests.” Accessed: Oct. 06, 2023. [Online]. Available: https://www.psychologistworld.com/behavior/compliance/strategies/door-in-the-face-technique

[89] M. Wilson and J. Hash, “Building an Information Technology Security Awareness and Training Program,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-50, 2003. doi: 10.6028/NIST.SP.800-50.

[90] A. Yazdanmehr and J. Wang, “Employees’ information security policy compliance: A norm activation perspective,” *Decision Support Systems*, vol. 92, pp. 36–46, Dec. 2016, doi: 10.1016/j.dss.2016.09.009.

[91] P. Zambrano, J. Torres, and P. Flores, *How Does Grooming Fit into Social Engineering?* in Advances in Intelligent Systems and Computing. 2019.

[92] “How to hack people,” Oct. 14, 2002. Accessed: Sep. 13, 2023. [Online]. Available: http://news.bbc.co.uk/2/hi/technology/2320121.stm

[93] “The Latest Cyber Security Resources,” PurpleSec. Accessed: Sep. 13, 2023. [Online]. Available: https://purplesec.us/cyber-security/

[94] “Moody’s - credit ratings, research, and data for global capital markets.” Accessed: Sep. 13, 2023. [Online]. Available: https://www.moodys.com/research/Moodys-Cyber-Heatmap-Cyber-Risk-Is-Rising-Across-70-Global--PBC_1343021

[95] “The 2021 Financial Data Risk Report Reveals Every Employee Can Access Nearly 11 Million Files.” Accessed: Jun. 26, 2023. [Online]. Available: https://www.varonis.com/blog/2021-financial-data-risk-report

[96] “Disgruntled Employees,” Security Through Education. Accessed: Oct. 02, 2023. [Online]. Available: https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/disgruntled-employees/

[97] “Does Your Help Desk Know Who’s Calling?,” The Hacker News. Accessed: Sep. 21, 2023. [Online]. Available: https://thehackernews.com/2023/03/does-your-help-desk-know-whos-calling.html

[98] “What is Reverse Social Engineering? And How Does It Work? | Aware | EC-Council.” Accessed: Sep. 21, 2023. [Online]. Available: https://aware.eccouncil.org/what-is-reverse-social-engineering.html

[99] "The Latest Phishing Statistics (updated September 2023) | AAG IT Support." Accessed: Sep. 22, 2023. [Online]. Available: https://aag-it.com/the-latest-phishing-statistics/

[100] "X-Force Threat Intelligence Index 2022." Accessed: Sep. 22, 2023. [Online]. Available: https://www.ibm.com/downloads/cas/ADLMYLAZ

[101] "What Is Pharming? - Definition, Examples & More | Proofpoint US," Proofpoint. Accessed: Sep. 25, 2023. [Online]. Available: https://www.proofpoint.com/us/threat-reference/pharming

[102] "What is Maze ransomware?," Cloudflare. Accessed: Sep. 25, 2023. [Online]. Available: https://www.cloudflare.com/learning/security/ransomware/maze-ransomware/

[103] "Ransomware Attack - What is it and How Does it Work?," Check Point Software. Accessed: Sep. 25, 2023. [Online]. Available: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/

[104] "An Overview of Social Engineering: Pop-Up Windows," Saylor Academy. Accessed: Sep. 25, 2023. [Online]. Available: https://learn.saylor.org/mod/book/view.php?id=29612&amp;chapterid=5165

[105] "Was ist Scareware? - Definition von WhatIs.com," ComputerWeekly.de. Accessed: Sep. 25, 2023. [Online]. Available: https://www.computerweekly.com/de/definition/Scareware

[106] "ngrok | Unified Ingress Platform for Developers." Accessed: Sep. 29, 2023. [Online]. Available: https://ngrok.com/

[107] "Door-in-the-face-Technik," Münchner Marketing Akademie. Accessed: Oct. 06, 2023. [Online]. Available: https://www.akademie-marketing.com/marketing-lexikon/door-in-the-face-technik

[108] *Face the Rear*, (Jan. 21, 2021). Accessed: Oct. 09, 2023. [Online Video]. Available: https://www.youtube.com/watch?v=OcyqWkHURxU

[109] "Serious gaming for education | seriously entertaining | Grendel Games." Accessed: Oct. 19, 2023. [Online]. Available: https://grendelgames.com/serious-games/education/

[110] "Underground - Grendel Games." Accessed: Oct. 19, 2023. [Online]. Available: https://grendelgames.com/spotlight/underground/

[111] "Foldit." Accessed: Oct. 19, 2023. [Online]. Available: https://fold.it/

[112] "ISO 22301 - Framework for Business Continuity Management - DataGuard." Accessed: Nov. 01, 2023. [Online]. Available: https://www.dataguard.co.uk/blog/iso-22301/

[113] "ISO 27031: How to use ISO 27031 for IT disaster recovery | DataGuard." Accessed: Oct. 24, 2023. [Online]. Available: https://www.dataguard.co.uk/blog/iso-27031-it-disaster-recovery-plan