GAZİANTEP UNIVERSITY
JOURNAL OF SOCIAL SCIENCES

Journal homepage: http://dergipark.org.tr/tr/pub/jss

Araştırma Makalesi ● Research Article

Non-Technical Cyber-Attacks and International Cybersecurity: The Case of Social Engineering[1]

Teknik Olmayan Siber Saldırılar ve Uluslararası Siber Güvenlik: Sosyal Mühendislik Örneği

Nezir AKYEŞİLMEN[a]* Amal ALHOSBAN[b]

[a] Prof. Dr., Selçuk Üniversitesi, Uluslararası İlişkiler Bölümü, Konya / TÜRKİYE
ORCID: 00-0001-8184-5280
[b] Assoc. Prof., Michigan University, Flint Campus, Computer Science, Ann Arbor / ABD
ORCID: 0009-0006-9267-613X

MAKALE BİLGİSİ

Makale Geçmişi:
Başvuru tarihi: 19 Ağustos 2023
Kabul tarihi: 10 Ekim 2023

Anahtar Kelimeler:
Sosyal mühendislik,
Siber Güvenlik,
İnsan hatası,
Uluslararası güvenlik,
Oltalama.

ÖZ

Bu makale, sosyal mühendislik saldırılarına ve bunların ulusal ve uluslararası güvenlik de dahil olmak üzere siber güvenlik üzerindeki etkilerine genel bir bakış sunmayı amaçlamakta, tespit tekniklerini ve karşı önlem için başlıca yöntemleri ortaya koymaktadır. Sosyal mühendislik saldırıları ulusal ve uluslararası güvenliği nasıl etkiler? Peki onlarla baş etmek neden bu kadar zor? Bu soruların yanıtlarını arayan bu makalede, özellikle literatür taraması ve vaka analizi olmak üzere nitel araştırma yöntemleri kullanılmaktadır. Araştırmada ağırlıklı olarak nitel araştırma yöntemleri kullanılmakla birlikte, gerekli görüldüğünde nicel araştırma yöntemlerinden de yararlanılacaktır. Online dolandırıcılık olarak da bilinen sosyal mühendislik saldırıları çoğu zaman az teknik bilgi ya da teknik bilgi gerektirmeyen nitelikte saldırılardır. Kullanıcı siber güvenlikte en zayıf halka olarak kabul edildiğinden, sosyal mühendislik saldırıları bireylerin zaaflarından ve hatalarından faydalanır. Birçok çalışma, dijital dünyadaki başarılı siber saldırıların büyük çoğunluğunun sosyal mühendislik (SE) saldırıları olduğunu, çünkü bunlara karşı koymanın teknik siber saldırılara karşı koymaktan daha zor olduğunu göstermiştir. 2016 ABD Başkanlık seçimlerine müdahale, 2015'te CIA direktörü John Brennan'in hacklenmesi ve 2010'da Stuxnet gibi bazı büyük siber saldırıların analizine dayanan makale, sosyal mühendislik saldırılarının bireysel, kurumsal, toplumsal, ulusal ve uluslararası düzeyde siber güvenlik üzerinde çok büyük etkiye sahip olduğunu ortaya koymaktadır. Sızma testleri ve farkındalığı artırmaya yönelik eğitimler, sosyal mühendislik saldırılarını azaltmanın etkili yöntemlerindendir.

ARTICLE INFO

Article History:
Received: August 19, 2023
Accepted: October 10, 2023

Key Words:
Social engineering,
Cybersecurity,
Human error,
International security,
Phishing.

ABSTRACT

This paper aims to provide an overview of social engineering attacks, and their impacts on cybersecurity, including national and international security, and figures out detection techniques, and major methods for countermeasure. How do social engineering attacks affect national and international security? And why is it so hard to cope with them? Seeking for answers to these questions, this paper applies qualitative research methods particularly literature review and case analysis. While qualitative research methods are predominantly employed, quantitative methods will also be utilized when deemed essential. Social engineering attacks, also referred to as online fraud, are a type of attack that typically necessitates minimal or no technical knowledge. Social engineering attacks, instead benefit from the weaknesses and mistakes of individuals, since the user is accepted as the weakest link in cybersecurity. Many studies have shown that the vast majority of successful cyber-attacks in the digital world are social engineering (SE) because countering them is more difficult than countering technical cyber-attacks. Based on the analysis of some major cyber-attacks such as the intervention in the 2016 US Presidential elections, the hacking of CIA director, John Brennan in 2015, and Stuxnet in 2010, the paper figures out that social engineering attacks have a tremendous impact on cybersecurity on the individual, institutional, societal, national, and international levels. Penetration tests and training for raising awareness are the prolific ways to mitigate social engineering attacks.

[1] This research is supported by Scientific Research Project Office of Selçuk University within the context of Project entitled "Non-Technical Cyber-attacks and Cybersecurity: The Case of Social Engineering" with number of 21409001.

* *Sorumlu yazar/Corresponding author*.
e-posta: nezmen@@yahoo.com

Introduction

Social engineering (SE) from the security perspective is a collection of dynamic activities including new forms and tactics growing constantly, particularly since it has evolved and developed dramatically in the last two decades. It is similar to a moving target. “Social engineering has existed in many forms throughout history and will continue to exist" (Wang, et.al, 2020, s. 85095). That is one of the causes why it is hard to develop a proper definition for them and likewise to cope with them.

SE is not a novel strategy. In the 1990s, Kevin Mitnick, a well-known hacker, contributed to the idea's widespread dissemination in cybersecurity, however, such tactics had existed since 1184 B.C. Greece-Troy tensions arose when the Trojan horse deception was initially employed. Today, it has become one of the most prevalent cyberattacks in the digital realm. As cybersecurity tools and countermeasures against technology-based assaults like malware have matured, cybercriminals have moved to SE techniques.

The goal of SE is to trick the system users by providing their needs based on human nature. For example, when the customer service employee is trying to help the customer by providing detailed information about his organization. Cyber security is commonly seen as a consequence of technical cyberattacks. Nevertheless, there are non-technical and/or minimally technological cyberattacks known as SE that pose a severe risk to cybersecurity. Social engineering attacks are conducted using tricks to collect the needed information from the system end users. Literature on SE is scarce, particularly literature on the national and international security impacts of SE attacks. Therefore, our study seeks to contribute to the literature in this regard as well. This study seeks to answer questions such as "How do SE attacks impact national and international security?" and "Why is it difficult to combat SE attacks?" as well as "What can be done to lessen their impact on cybersecurity in general and national and international security in particular?"

This research employs a literature review, existing statistics on SE, and a major international case analysis to answer these problems. The literature will provide us with definitions and some methods of detection and mitigation, statistics will outline the effectiveness of SE, and case studies, such as the intervention in the 2016 US Presidential elections, the hacking of CIA director John Brennan in 2015, the South Caroline spam e-mail attack in 2012, and Stuxnet in 2010, will illustrate the impact of SE on cybersecurity, which has become the most important component of both national and international security globally over the last decade.

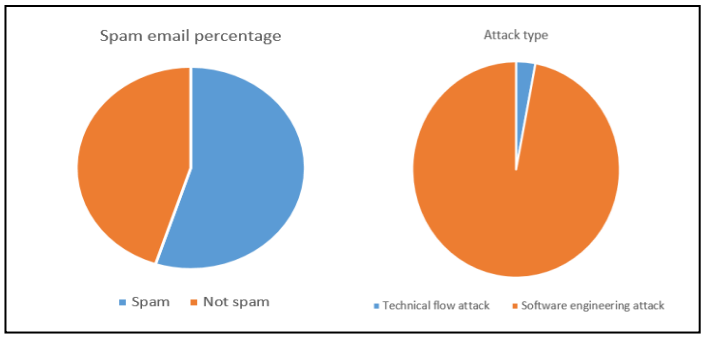
This study focuses on the theoretical and conceptual framework, assesses some of the most significant SE attacks in international relations, and evaluates the existing detection and countermeasures against SE. Before the conclusion, discussions and findings will be further upon.

Theoretical and Conceptual Outline

Whether the data of states, companies, or even individuals is on paper or in information systems, information must always be protected against threats to itself and protected by those who use it. Cyberspace, which is the most frequently used for accessing information, has been the most important source for accessing information concerning personal and national security. The infrastructure systems used to play a critical role, from ensuring the security of the information concerning public security and sharing it among the institutions that provide national security. Changes in areas such as the internet and metaverse in today’s world have led to the expansion of cyberspace (Şöhret, 2022, s. 133)

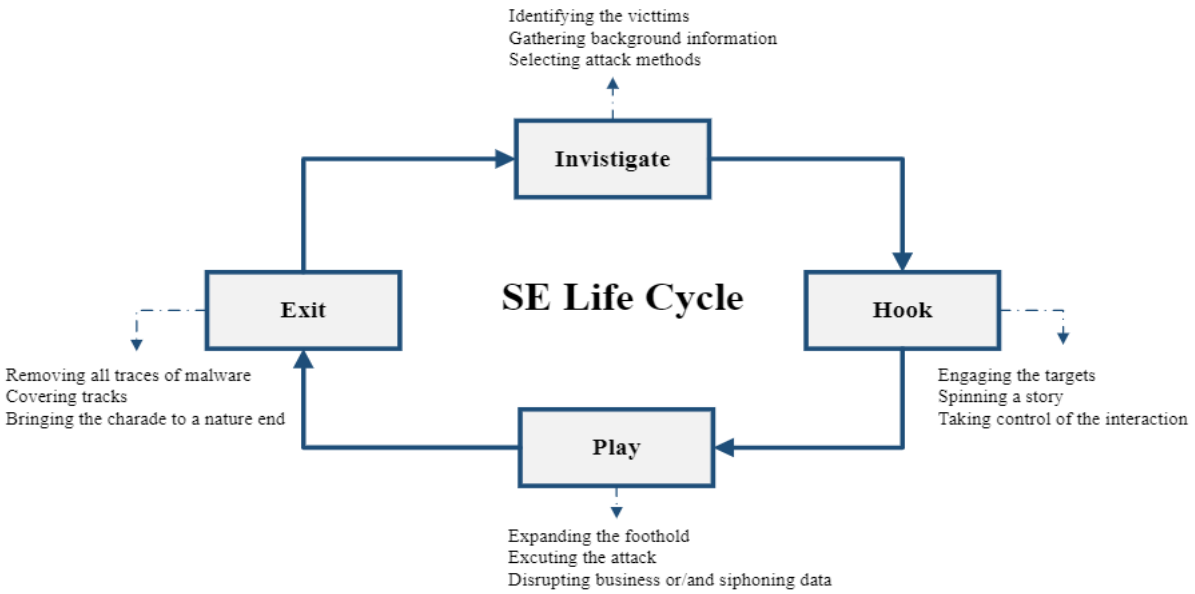
Social engineering attack is a widely known issue in cybersecurity and is one of the most difficult tests faced by all cyberspace stakeholders as it exploits one's trust-based propensity (Jimoh, 2022). SE attacks pose a serious threat to all levels of security from individual to global cybersecurity. 98% of cyber-attacks involve some form of SE and it is used in up to 90% of malicious data breaches (Reed, 2022). Figure 1 demonstrates that just 3% of malware tries to take advantage of a purely technical weakness. Instead, the remaining 97% use SE to target users. 55% of all emails are spam (Sysgroup, 2022). Consider that according to Internetlivestats on average 250 billion e-mails are sent worldwide per day (Internetlivestats, 2022).

Figure 1: Statistics on spam email and general attack types



Social engineering does not usually require a high level of technology knowledge. SE takes advantage of common human characteristics like curiosity, politeness, trust, greed, lack of thought, shyness, and apathy (CERT-UK, 2015, s. 3). Although it requires the least technical knowledge, SE is one of the most fertile, thriving, and conclusive ways of accessing closed systems and acquiring sensitive information. With features full of secrets and unknowns, it has a wide range from phishing e-mails to pretexting, from tailgating to quid pro quo, and more (CERT-UK, 2015, s. 3). Social engineers are masters of their craft because they use the standards of human brain research to build beliefs with users regularly, knowing that the individual may be their "in." It all starts with deciding on a brand and human target(s) (Mitnicksecurity, 2015, s. 3).

Figure 2: Social Engineering Life Cycle



Resource: Duarte, N., Coelho, N., Guarda, T. " SE: The Art of Attacks", In Guarda, T., Portela, F., Santos, M.F. (eds) *Advanced Research in Technologies, Information, Innovation, and Sustainability*. ARTIIS 2021. Communications in Computer and Information Science, vol 1485. Springer, Cham. https://doi.org/10.1007/978-3-030-90241-4_36 [Access date: November 04, 2022].

Figure 2 illustrates the SE life cycle, which includes several steps. According to this scheme, the attacker first conducts a thorough investigation, including identifying the target, gathering background information, and determining the methods to be used. The second step entails communicating with the target, fabricating a story, and exerting control over the interaction. The next step is to identify the target and launch the attack, either by blocking the service or obtaining the desired information. Finally, it is to clear all traces, restore the system to its original state, and exit.

Defining Social Engineering

In the literature, there are too many distinct definitions for the concept, each of which captures different parts of the process. Hadnagy, for instance, proposes a broad, vague, and non-cyberspace-specific definition of cyber environment, arguing that SE refers to any activity that influences an individual to take a course of "action that may or may not be in his or her best interests" (Hadnagy, 2018, s. 7). However, another definition offers a more precise meaning of social security. The act of misleading someone in person, over the phone, or through a computer to breach some level of personal or professional security (Chinta, Alaparthy, and Kodali, 2016, s. 225). Recent definitions in the literature tend to emphasize the concept's non-technological aspects. Krombholz et al. make a compelling case for such claims, defending the position that SE is the act of convincing end users to breach IT systems. Social engineers are a subset of hackers that don't focus on technology but rather on persuading and influencing people in positions of power to commit destructive acts, such as leaking sensitive information or launching attacks. Breda, Barbosa, and Morais on the other hand, focus on cybersecurity aspects of the concept by arguing that "it is primarily used to induce victims towards disclosing confidential data, or to perform actions that breach security protocols, unknowingly infecting systems or releasing classified information" (Breda, Barbora and Morais, 2017). In addition to that SE is a type of attack when a hacker(s) use social interaction to exploit human vulnerabilities to violate cybersecurity through technical and non-technical vulnerabilities (Wang, et.al, 2020, s. 85105). In this context, Oosterloo provides a comprehensive definition, stating that it is the successful or unsuccessful efforts to persuade an individual(s) to disclose details or behave in a way that might cause the illegal disclosure, use, or declassification of a computer system, network, or data (Oosterloo, 2008, s. 3).

Based on the definitions provided above, this paper defines SE as primarily non-technical activities, methods, and processes to get into desired confidential data or information or closed systems by deceiving and using people as pawns by exploiting his or her mistakes, weaknesses, psychological, and moral states. Any definition of SE will be incomplete because it is a constantly evolving cyberattack with new forms emerging every day. That is why, over the last 20 years, it has become such a popular, prolific, and effective method of cyber-attacks. According to Wang et al., such a variety of definitions has resulted in many "conceptual deficiencies (such as inconsistent conceptual intentions, a vague conceptual boundary, confusing instances, overgeneralization and abuse) of the term making serious negative impacts on the understanding, analysis, and defense of social engineering attacks" (Wang, et.al, 2020, s. 85094).

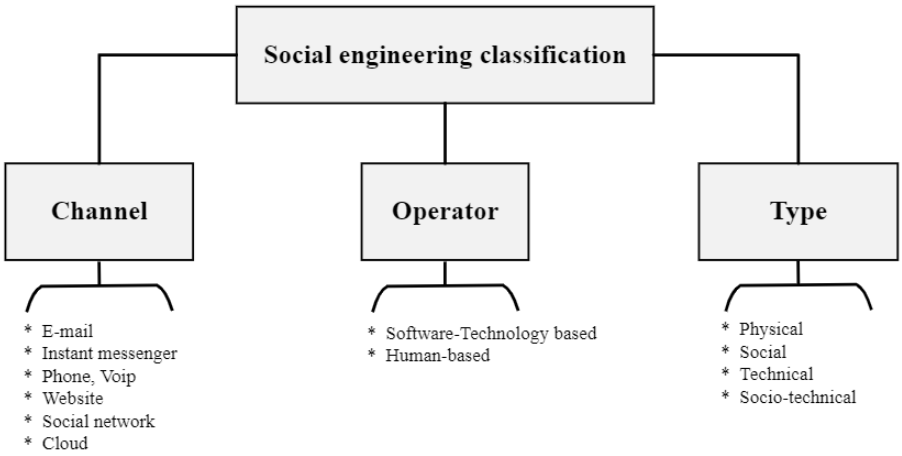
There is a wide variety of resources available to social engineers for use in gaining access to confidential information. These may serve as informational resources, or they may employ manipulative psychological techniques that play on people's vulnerabilities. OSINT and HUMINT are the two most important ones. Other personal resources include strong emotion,

overloading, reciprocation, deceitful relationships, diffusion of responsibility, moral duty, authority, integrity, and consistency.

Classification of Social Engineering Attacks

The internet evolution simplifies information sharing using the social media platforms such as Facebook, Snapchat, WhatsApp, Instagram, and much more. Social engineering assaults, which pose a grave threat to cybersecurity, can be classified on a variety of grounds (see Figure 3). It can be based on operators like software or humans, or it can be based on channels like e-mail, SMS, phone, websites, the physical cloud, or social networks, and it can be based on tactics like technical, social, physical, or socio-technical (Krombholz et al., 2014, s. 5).

Figure 3: Classification of Social Engineering



Classification based on technology and humans will be elaborated and analyzed in this paper. Phishing, baiting, virtual impersonation, watering holes, and whaling are among technology–based SE attacks, while tailgating, dumpster diving, pretexting, and reverse SE are accepted as human-based SE attacks. Human-based attacks involve the attacker physically meeting with the target and engaging in conversation to glean the information they need. As a result, they are restricted in the number of people they can harm. Software-based assaults collect information from their targets via electronic devices like computers and mobile phones (Salahdine, and Kaabouch, 2019, s. 3). Attacks employing SE may incorporate social, human, technical, computer, and physical elements. Phishing, help desk impersonation, dumpster diving, document theft, diversion theft, bogus software, quid pro quo, baiting, pretexting, pop-up windows, tailgating, ransomware, reverse SE, and phone SE are all forms of social engineering. (Salahdine, and Kaabouch, 2019, s. 3).

Table 1: Major Social Engineering Attacks Based on Types of Operator

	Technology-Based Attacks	**Human-Based Attacks**
1	Phishing	Vishing
2	Impersonation	Baiting
3	Spear Phishing	Pretexting
4	Smishing	Dumpster Diving
5	Whaling	Tailgating

6	Brand Theft / Typosquatting	Quid Quo Pro
7	Watering hole	Scareware
8		Reverse SE

Resource: The table is designed by the authors.

Social engineering is a dynamic process that grows, changes, and transforms considerably more rapidly than countermeasures. Therefore, SE techniques and methods are not restricted to those listed above. They are, however, the most significant and widespread types of SE attacks over the last two decades. All of these strategies, their functions, methodologies, and effects on cybersecurity will be described in this paper in brief.

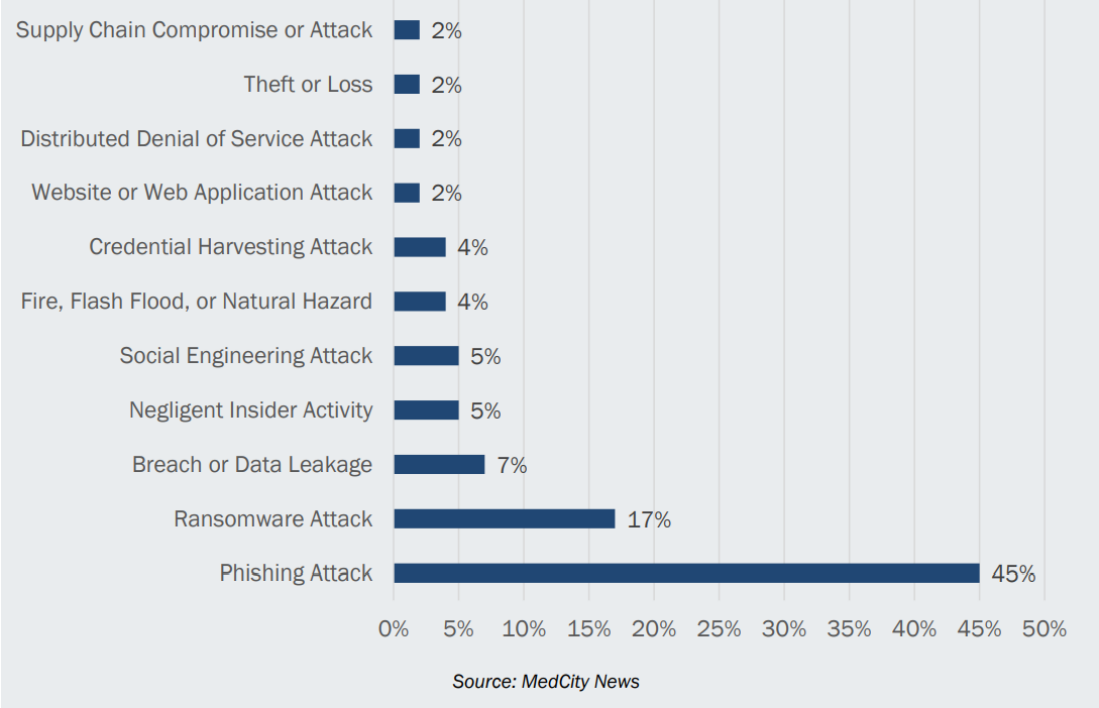
Technology-Based SE

Some of the SE attacks are performed through technology tools and channels such as emails, SMS, social media, websites, etc. Some of them are phishing, spear phishing, brand theft, watering holes, etc.

Phishing is one of the oldest techniques in the toolbox of the malicious actor (Indzhov, et.al.,2022, s. 13). Phishing (e-mail phishing, smishing, and social phishing) is a type of SE assault used to gain sensitive or personal data from a corporation or institution. By posing as a trustworthy source, an attacker attempts to deceive a victim into opening an email (email phishing or spam-phishing), instant message (smishing), or social media message (social phishing). Phishing is the practice of sending harmful emails purporting to originate from legitimate sources (Hadnagy, 2018, s. 229). Some may request a response to the email, after which they will participate in an exchange of communications to elicit sensitive information (CERT-UK, 2015, s. 4). Phishing attacks can be performed via email, text messages, phone calls, social media, fax, and other modes of communication, including social media (CERT-UK, 2015, s. 3). The victim is then tricked into clicking on a malicious attachment or link, which can result in the installation of Trojan horse into computer or the system.

Phishing, which accounts for an estimated 77% of all social-based attacks, is the most productive form of SE (CERT-UK, 2015, s. 3). A Phishing attack can have disastrous consequences for the target person, institution, organization, or state. The purpose of phishing is to steal personal data such as passwords, usernames, credentials, or credit or social security card information, download information from the system or can be placed to make a larger attack such as an advanced persistent threat (APT) event on an organization or a national critical infrastructure. According to Carahsoft's 2021 HIMSS Healthcare Cybersecurity Study, over 12 months, Figure 4 reveals that phishing attempts were the most common threat, accounting for 45% of security events.

Figure 4: Phishing Attacks Top Threat to Healthcare



Resource: https://www.hhs.gov/sites/default/files/the-impact-of-social-engineering-on-healthcare.pdf

Spear phishing is utilized by more advanced attackers who restrict their target group and increase the precision of their messages, thereby enhancing their credibility. Those targeted by a spear phishing assault may be in the same field of work, belong to the same organization, or share some other commonality (CERT-UK, 2015, s. 5). Spear phishing, in all its different forms, is a type of phishing that is very personalized (Hadnagy, 2018, s. 231). A good attacker will learn as much as they can about their target(s) to increase their potential for success. Attempts will be made to learn more about the organization, such as its structure and how to get in touch with it. They will combine this information with what they know about their target using information available online, such as social media accounts. The message will probably include specifics about the recipient, such as using their name instead of a generic greeting that makes it more personal (CERT-UK, 2015, ss. 5-6). Spear-phishing is the first stage of an Advanced Persistent Threat (APT) attack, that is utilized to gain access to a computer system. It's a form of assault that aims at a particular segment of a company's workforce. By combing through websites, blogs of employees, and social profiles tailored phishing is developed. Malware is sometimes hidden within phishing emails, such as Trojan, whose primary purpose is mass surveillance (Aldawood and Skinner, 2019, s. 10).

Whaling is a phishing attack, similar to spear phishing, and usually targets company owners and senior personnel.

Smishing or SMS Phishing SMS phishing is based on the same fundamentals as phishing but uses a different channel, SMS. As suggested by its name, smishing is simply mobile phishing. The origin of the term "smishing" is a combination of "phishing" and "SMS". (Indzhov, O.et.al., 2022, s. 18) This threat should not be ignored because it uses the same psychological factors that make phishing and other SE techniques so effective.

Brand Theft and Typosquatting to automate exploits to incentivize employees. In brand theft, employees are led to believe They are using legitimate platforms and services. These attacks employ typosquatting URL hijacking or the registration of domain names containing minor typographical errors. The misspelled domains are intended to deceive users who do not

closely examine email headers. It leads to copyright violations and a loss of public confidence in institutions (Aldawood and Skinner, 2019, s. 10).

A watering hole is an SE attack in which attackers in the digital realm target website users by taking over websites that their targets frequently visit and installing malware on them. Similar to baiting, attackers use trustworthy web pages to cause in infection in victims' electronic devices. In addition to requiring technical knowledge in most cases, they are more advanced than other SE methods. A watering hole attack involves compromising a trusted third-party web page to cause harm by transmitting harmful software to the computer of the target person, company, or organization (CERT-UK, 2015, s. 6).

Human-Based Social Engineering Attacks

Among too many ways of conducting SE based on human channels scareware, baiting, tailgating, pretexting, quid quo pro, dumpster diving and reverse SE are the most common ones.

Impersonation is the practice of adopting the identity of another person to obtain or alter information (Ghauri, 2021). It is accepted as one of the most hazardous channels, yet also one of the most lethal for SE attackers to deploy. Consequently, it is the least utilized of the four vectors. Impersonation is the process of dressing up as an employee of a competing company employee or a trusted authority figure, such as law enforcement, a utility worker, etc (Hadnagy, 2018, s. 241). To carry out subsequent hostile acts, such as piggybacking, pretexting, and quid pro quo, the malicious actor takes on a fictitious identity to obtain credibility (Breda, Barbosa, and Morais, 2017).

Pretexting assaults involve the creation of fictitious and persuasive situations to steal identifying information from a victim. Attacks are predicated on making the victim believe and trust the attacker. The attack is carried out by e-mails, physical media, or phone calls (Salahdine and Kaabouch, 2019, s. 5). The heart of this attack is the creation of a realistic situation suitable for engaging the targeted person(s). The attacker tries to breach security procedures by mimicking a legitimate source to steal sensitive data such as passwords and bank account numbers. To avoid suspicion, this strategy necessitates a convincing story, which necessitates extensive research on the target (Breda, Barbosa, and Morais, 2017). The malicious user adopts a fake personality and uses the name of a trusted organization. This persona is used to facilitate interaction with the intended target. Data, finances, passwords, and other information about the target are used to try to take control after a certain amount of time has passed.

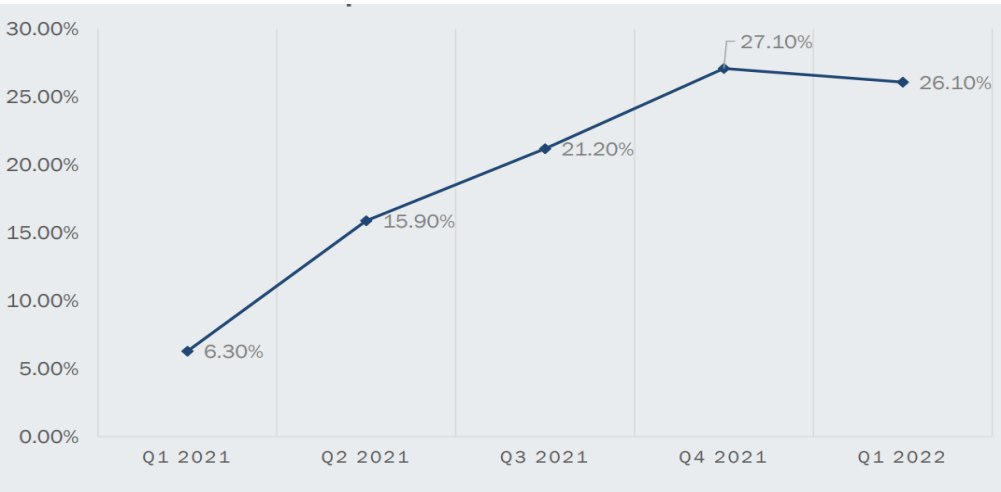
Baiting is a type of SE used to gain access to air-gapped systems or intranet that is inaccessible online. Through baiting cybercriminals exploit the curiosity of target user groups to launch cyberattacks. An opponent can use hardware in an attempt to attract a target or target. Due to its specific nature, this form of SE is typically used by more advanced attackers against a targeted industry, organization, or person. Baiting typically entails leaving discarded digital media (such as a USB flash drive, CD, or DVD) in a place visited often by the target, sometimes with a tempting label (like a car park). Hoping that they will take it and then put it to work on a computer at home or the office, spreading malware. The attacker may be in a position to give away infected USB drives at conferences or other events or to provide extra details on digital media that has been compromised (CERT-UK, 2015, s. 7).

Often referred to as "road apples," baiting attacks are a form of phishing that promises users something of value if they click on a link. They function as trojan horses, attacking targets using easily accessible, unprotected computer materials like storage media or USB drives infected with malware. This USB drive is a real-life Trojan horse that will attack any computer it is plugged into. This form of attack is stealthy, taking place in the background and performing

malicious tasks without the targets' knowledge (Salahdine and Kaabouch,2019:6; Mitnicksecurity, 2022, s. 9).

Vishing (Voice Phishing) "is a mash-up of voice phishing, which is phishing over the phone." (Hadnagy, 2018, s. 233). In such attacks, the user is contacted over the phone and attempts are made to gather information from the user that will complete or facilitate the attack. Sometimes, terrible actors take advantage of the influence of a gentle voice. These are voicemails that tell you to call back right away to do something, and they often use fear to get you to call back (Mitnicksecurity, 2022, s. 8). Based on the data presented in Figure 5, the volume of phishing attacks rose by 6% between Q1 and Q2 of 2022.

Figure 5: Share of Reported Vishing Cases



Resource: https://www.hhs.gov/sites/default/files/the-impact-of-social-engineering-on-healthcare.pdf

Scareware is a type of malicious code that an attacker uses to frighten users with worrisome messages, pop-ups, and warnings that their account has been hijacked. The objective of scareware is to coerce the user into performing a repository function. It attempts to convince victims to purchase and download potentially harmful code. People's attention may be grabbed and held with this method and be terrified. All of these characteristics are typical of scareware: difficult-to-close pop-up advertisements, software companies with unfamiliar names, and unauthorized virus scanning (ESET, 2021, s. 19). Thus, Because of this, paid and free cyber security programs that compromise user privacy become widely available (Ghauri, 2021).

Tailgating implies following a human target who has permission to enter a secure area past a closed door without the victim's knowledge. The offender could either have the victim hold the door for him or sneak in right before it closes down (Breda, Barbosa, and Morais, 2017). Assaults committed by "tailing," "piggybacking," or "physical access" involve following someone who has been granted access to a restricted area or building. They provide trespassers with a means of entering structures illegally. If the assailants forget their ID card or RFID card, they may ask a bystander to hold the door open for them. They can even use someone else's computer or mobile device to harm, like installing malware (Salahdine and Kaabouch,2019, s. 6). In the same way that a driver may hug the back of your car to get a better view of what you're doing, to get entry to a secure area that requires a fob or code, social engineers may follow a worker as they enter the facility. The attackers usually enter a building while following their target, and they do so by using a cunning pretext, like dressing up carrying packages as a deliveryman or as a friendly face bringing some food for the staff (Mitnicksecurity, 2022, s. 9).

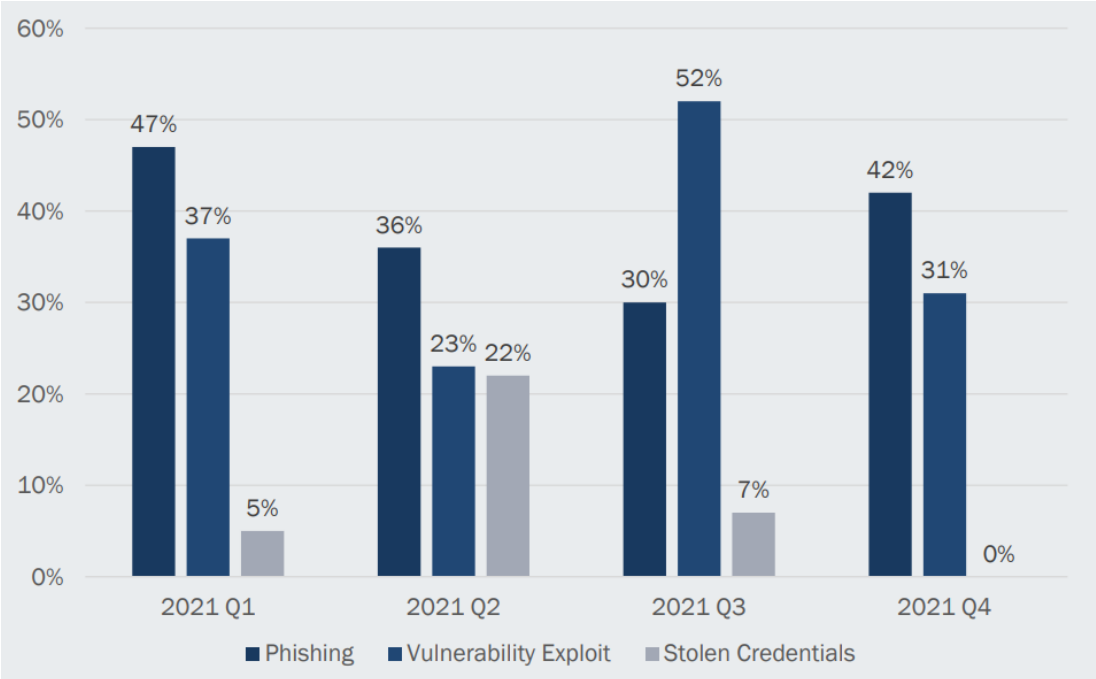
Quid Pro Quo, derived from the Latin phrase "exchange for values or something for something," is a social manipulation approach in which the malicious user promises a benefit in return for information or access (Mitnicksecurity, 2022, s. 9). As a sort of SE and cyber

security "extortion," this assault typically takes the shape of a purported technical service offered to the victim in exchange for the latter's private information. By pretending to be a helpful IT professional, the attacker can infect a victim's system while appearing to help them out with their problems (Breda, Barbosa, and Morais, 2017).

Dumpster diving is a common method among attackers for obtaining sensitive information by simply searching within the garbage. Documents, papers, and even hardware are often improperly discarded by individuals and corporations from which confidential data/information can be recovered (Breda, Barbosa, and Morais, 2017). It is gathering confidential information from company waste or outdated technology (e.g., hard drives, CDs, and DVDs) (Salahdine, F., and Kaabouch, 2019, s. 8).

Reverse Social Engineering, uses techniques to persuade their victim to approach them first, lowering the likelihood that they will raise suspicion. The attacker assumes the role of a trustworthy third party, develops a fictitious problem for the victim, and then indirectly offers a remedy (Breda, Barbosa, and Morais, 2017). In this type of SE assault, the bad guys pose as the ones who can help you with your network's issue. There are essentially three stages involved: (1) producing some sort of difficulty, like a network crash; (2) advertising that only the attacker can cure the problem; and (3) fixing the problem while also obtaining the needed information and then disappearing undetected (Duarte, Coelho and Guarda, 2021; Salahdine and Kaabouch, 2019, s. 6).

Figure 6: Attacks Linked to Social Engineering



Resource: https://www.hhs.gov/sites/default/files/the-impact-of-social-engineering-on-healthcare.pdf

SE attacks are not limited to these techniques, but they are the most frequently used and applied. As previously stated, because these attacks are dynamic, new types are constantly emerging. Attacks including social engineering are depicted in Figure 6 below. Quarterly in 2021, the proportion of assaults attributable to phishing, exploiting vulnerabilities, and using stolen credentials.

Major Social Engineering Attacks at the Global Level

An individual, a business, or even a country may be the target of a SE attack. As the case studies below demonstrate, these types of attacks have significant effects on security at the

individual, societal, and international levels. Some of these attacks target vital national infrastructures, while others target national security facilities and political institutions and processes. Below is a list of notable international SE attacks and how they threaten international security.

Russian Spear Phishing Attack on US Presidential Elections of 2016: Digital Cold War?

One of the most prominent examples of SE is the U.S. presidential election of 2016. The triumph of Donald Trump over Hillary Clinton may have been influenced by the leak of thousands of messages and information from the Democratic Party as a result of spear phishing attacks (Gatefy, 2021). Russian hackers allegedly sent spearphishing emails posing as Google warning Democratic National Convention staff of suspicious activity on their Google accounts. After simply clicking the shortened link, the website prompts for new passwords. After victims clicked on the phishing link and entered their login information, cybercriminals got full access to their Google accounts, including Gmail, and deleted thousands of emails with sensitive Hillary Clinton campaign information (Mitnicksecurity, 2020).

Impersonation Attacks on CIA Director

British teen Kane Gamble hacked the e-mail account of CIA director John Brennan, then made phone calls to his home, and even gained control of the iPad of Brennan's wife. The hacks were part of a politically motivated campaign to harass senior U.S. officials. Gamble was only 15 years old when he impersonated a telecoms employee and Brennan to obtain passwords, contact lists, and confidential documents about operations in occupied Iraq and Afghanistan. After Brennan, Gamble launched a series of attacks from his bedroom in Leicestershire against other top security officials. Jeh Johnson, the Secretary of Homeland Security, was one of his victims. He also targeted James Clapper, the director of national intelligence, and the families of Mark Giuliano, the former deputy director of the FBI during the Obama administration. The identities of 1,000 employees and information on the officer who shot Michael Brown in Ferguson were leaked to the public when hacked into an FBI database (Michael, and Cambridge, 2018).

Phishing in the Department of Revenue in South Carolina

The South Carolina Department of Revenue has millions of stolen Social Security numbers and debit and credit card data in 2012. Workers fell for the phishing scam and revealed their passwords to the attackers. Criminals breached the governmental agency's network by stealing user credentials (Gatefy, 2021). According to studies, the intrusions were the greatest cyberattack ever perpetrated against a state government body, leading to the loss of 3.8 million Social Security numbers and 387,000 credit and debit card data. After the incident, computer security firm Mandiant released a report with fresh information. Scammers infiltrated the state agency's network by delivering malicious links in spam emails to state personnel. Mandiant found that when workers visited the link, malicious malware was installed on their computers and stole their login information. Using this, the hackers may pose as tax authorities and gain access to confidential data (Brown, 2012).

Baiting in Stuxnet

Stuxnet is the most well-known, discussed, and studied cyber attack in the world. Stuxnet is the most complex malware ever created by humans, and it is the first known code to physically damage machines in addition to damaging computer programs. It was aimed specifically at a particular centrifuge.[1] In addition to delivering the virus to its intended target, the Iranian engineer reportedly provided intelligence agencies with information about the centrifuges and their installation, allowing allegedly to US developers to write code targeting

the Natanz using Windows operating systems manufactured by Siemens, a German company that produces enriched uranium for nuclear weapons and reactors (Fruhlinger, 2017). The Stuxnet worm demonstrated that infecting computers via USB drives is an effective method for targeting air-gapped (intranets or networks that are not connected to the internet) networks (Baezner, and Robin,2017, s. 11). Experts believe that an infected USB stick was either given to an Iranian facility operator by SE (the most likely scenario being a baiting attack) or used by a double agent working inside the facility to breach the "air gap" network defense at a facility that used Siemens software but was not connected to the Internet, such as Iran's nuclear program (Tabba, 2020).

Spear Phishing in Snowden Leaking

Edward Snowden, a former CIA and National Security Agency (NSA) employee has provided news sources with findings that the United States digitally monitors its citizens. The NSA is reportedly gathering the phone information of millions of Verizon customers, one of the biggest telecom firms in the United States, by a secret court order. The order, a copy of which was acquired by The Guardian, mandates that Verizon "ongoing, daily" furnish the NSA with data on all calls placed within the United States and between the United States and foreign nations. It reveals for the first time that the Obama administration gathers communication information of millions of American individuals regardless of whether or not they have done anything illegal (Greenwald, 2013).

Some of the sensitive material Snowden disclosed came from a spy base in Hawaii, and He accessed it using credentials supplied to him by his coworkers there. According to research, 20 to 25 intelligence service workers who provided Snowden with access information were tracked down, questioned, and dismissed. Snowden socially engineered these people by claiming he needed their login information to do his job as a systems administrator (Sjouwerman, 2022).

Electricity Hack in Ukraine

SE techniques are never to be underestimated. This became especially apparent on December 23, 2015, when the lights went out in Ivano-Frankivsk, a city in western Ukraine. Several power plants were damaged and rendered inoperable in this area, leaving tens of thousands without power (Kontio, 2016, s. 39). As is typical in cyberattacks, Ukraine's electricity system was first compromised by human error: The attacks known as spear-phishing were used to access to the power-plant (McLellan, 2016) and cyber attacked was realized.

Whaling Attack on Belgian Bank

The Belgian bank Crelan was the target of likely the most successful SE attack in history. Crelan figured out its CEO had been "whaled" after applying internal monitoring (Sjouwerman, 2022) but the perpetrators got away with $75 million and have never been brought to justice (Zorz, 2016).

The number and scope of SE attacks against critical infrastructures and other sensitive plants that have an impact on national and international security are expanding daily. These attacks typically target individuals as information sources. Since cybercriminals are aware that the user is the most vulnerable component of cyberspace.

Discussions and Findings

Each case examined so far has implications for cybersecurity, national security, and international security. Long before international cybersecurity discussions in international relations, the globalization literature widely acknowledged the interaction and interconnectedness of security at all levels, such as individual, societal, national, and

international. Cyberspace bolstered this case. Not only do the examples above illustrate how SE attacks threaten national and international security, but they also demonstrate the interconnectedness of security at all levels. For instance, an individual's error can jeopardize national security, as in the South Carolina Department of Revenue, impersonation attacks on the CIA director, Stuxnet attack on Iran's nuclear facilities, or the errors of a few can endanger global democracy, as in the 2016 attacks on the US presidential election.

It is known that numerous SE techniques exist. Since people can develop new techniques, it would not be incorrect to assert that their number is theoretically infinite. However, there are a few widely employed and effective strategies. The first of these is phishing, followed by spear phishing and impersonation. It is well known that baiting is a very effective way to get into systems or intranets that are not connected to the outside world.

Russian interference with the US presidential election of 2016 has raised concerns about global democratization and democratic processes. On July 29, 2018, Republican Senator James Lankford told ABC television that Russia will "continue its war with our democracy", claiming that the attacks so far have not been successful, but that Russia has tried every means to interfere in the elections and continues to do so, even today (Scanlan, 2018).

Although all these discussions are focused on the US election, there is a serious fear of interference and discussions about it, especially in the upcoming elections globally, particularly in EU countries (Dorell, 2017). One factor that strengthens this fear is the claim that the intelligence reports published in January 2017 suggest that Russia will try to influence the elections to be held across Europe (Ignatius,2017). Ignatius argues that Russian interference in the elections is a global threat. If the necessary measures are not taken, this process may be the beginning of the "Post-Western era" as Lavrov claims (Ignatius, 2017). Not only international interventions but also the issue of election security and cyber interventions by internal power centers in the world, especially in countries where authoritarian tendencies are stronger, arouses concern among the public (Akyeşilmen, 2018, s. 242).

Some argue that cyber attacks against the USA and its allies are different from conventional warfare (Singer, 2017) and that it is a kind of cyber cold war (Dolly, 2017). Intelligence reports suggest that Russia undermines American politics with hacks, e-mail leaks, and campaigns such as fake news, and makes the Presidential election the subject of discussion. Considering the series of cyber conflicts in which Russia is involved, the conflicts are drawn into cyberspace and experts agree that this is a digital cold war (Pagliery, 2017).

Stuxnet is the most complicated malware ever produced by human beings, and it is known not only to damage computer programs but also to be the first code that physically damages industrial machines. It specifically targeted a special centrifuge that used the Windows operating system and was manufactured by Siemens, a German company that produces enriched uranium for nuclear weapons and reactors (Fruhlinger, 2017).

Stuxnet was the first cyber weapon because, as the first of its kind, it caused physical destruction. It is also claimed that Stuxnet is the first aggressive cyber tool used by countries to achieve their foreign policy goals (HIIK, 2017, s. 37). Stuxnet, which accomplished what conventional weapons could not and rendered the victim helpless because it self-destructed and its source is unknown, is a watershed moment that profoundly affects the concept of cyberspace, including cyber weapons and cyberwar (Fleming, 2010).

States may wish to improve their cybersecurity to avoid a repeat of the Stuxnet-like incidents. The Stuxnet worm demonstrated that infecting computers via USB drives is an effective method for targeting air-gapped networks. That's why governments must focus on the problem of people utilizing unrecognized USB devices on their computers. To ensure that users

are aware of the risks and the harm that this behavior might create, states can launch targeted efforts to educate those who work in key infrastructures on the issue. This would hopefully encourage a more circumspect approach to this matter (Baezner and Robin, 2017, s. 11).

Snowden case is about individual freedoms, human rights, and the right to protect private life, as well as re-questioning and restructuring citizen-state relations; He brought up the issue of the reliability of companies that store sensitive information (Israel, 2018). NSA Director Keith Alexander claimed that Snowden obtained unauthorized confidential information and documents and obtained the generated digital keys. This event clearly shows that companies and institutions that store personal data, confidential, and sensitive information should develop policies on how to protect their internal mechanisms, how to secure encryption, and how best to provide authorization (Hill, 2018) and be careful against SE attacks.

The energy shutdown in Ukraine in 2015, SE attacks on an Austrian aircraft manufacturer, and whaling on the Belgian Crelan Bank illustrate the vulnerability of cyber technology to SE attacks. The phishing attack on the South Carolina Revenue Department in 2012, the breach of the Ukraine power grid in 2015, and the whaling on Belgian Cleran Bakn in 2016 have illustrated those national critical infrastructures such as finance, energy, transportation, telecommunication, etc. are vulnerable against SE attacks. These sectors are vital for national security and political stability. Therefore, governments, institutions, corporations, and world leaders should develop better techniques and methods against SE attacks to better protect their data and information and prevent leaks. States will have a more difficult time providing genuine network security.

Detecting and Mitigating Social Engineering Attacks

Human-based attacks are far more sophisticated and difficult to detect, necessitating their prevention. To protect against SE assaults and lessen the damage they do by taking advantage of employees' vulnerabilities, organizations should use both technical and human forms of protection. Mitigation techniques for SE attacks aim to lessen the impact of the attacks on individuals, institutions, and national security. There are many different ways to protect against SE, but education, training, and awareness activities; implementing SE penetration tests, and technological measures are among the most common and effective.

The first step should be to train users and raise their awareness. To raise awareness, designers focus on providing instruction on SE attacks, employee training courses, television programs, and/or publications on actual case scenarios. Perhaps the most effective way is to provide all citizens with a comprehensive digital citizenship education, particularly employees in both private and public institutions.

While conducting a penetration test, social engineers zero in on the weak spots in people and procedures. Common social engineering (SE) attacks carried out by an ethical hacker during a pen test include phishing, vishing, smishing, USB drops or baiting, and impersonation. The purpose of this evaluation is to find areas of improvement in an individual, team, or procedure, as well as to pinpoint vulnerabilities that may be easily fixed (Allen, 2022).

Technology-based measures also help detect and mitigate technology-based SE attacks, specifically, the use of technological measures, including spam filters, anti-virus software, and the banning of known phishing/baiting websites, which can aid in the prevention of some phishing assaults. Create measures that lessen the likelihood of a successful phishing attempt (CERT-UK, 2015, s. 8). There have been suggestions for anti-phishing technologies that can blacklist and ban known phishing domains. McAfee anti-phishing filter, Microsoft phishing filter, and Web sensing are examples of these tools (Salahdine and Kaabouch, 2019, s. 9) and "For tailgating attacks, they may be prevented by training employees to never give access to

someone without badge with no exceptions and requiring locks and IDs for all employees" (Salahdine and Kaabouch, 2019, s. 9).

Social engineering attacks pose major security risks, and companies and organizations should address them. Companies should promote employee security awareness. Several techniques exist to detect and prevent these attacks (Salahdine and Kaabouch, 2019, s. 8). Some of the most important techniques are: One, all employees, including management and IT staff, should get consistent cybersecurity training. Two, check for passwords that are too simple and might let an intruder into your company's system. Increase password security by using multi-factor authentication; Third, use technological means to prevent fraud in the form of electronic messages by detecting, quarantining, neutralizing, and erasing spam and phishing messages. Provide security guidelines that staff can follow in the case of a SE and that they can easily comprehend (ESET, 2021, s. 20). 5- Disseminate information about security attacks.;6- Web pages with the authenticated credential should be utilized.; 7-Users must pause before spreading credentials; 8-Must verify the legitimacy of websites before making a payment." (Ghauri,2021). 9- Make sure users are conscious of the warning signs of phishing emails.; 10 - Think about doing user awareness sessions, perhaps as a part of training or induction days, and incorporating a penetration test depicting a successful SE attack against an (anonymous) member of the business.;11- The eleventh piece of advice is to tell your users to double-check any odd requests or communications by phoning the sender at a known number.; 12-Do not disclose your ID or password over the phone; 13- Never leave vital information on your desk unattended.; 14- Shred documents before discarding them to prevent their contents from being read.

To achieve its objectives, SE attacks exploit human errors and psychological vulnerabilities. There is no doubt that SE attacks against individuals and employees will increase in the future. Some phishing attacks can be prevented by employing technological measures, such as spam filters, anti-virus software, and the banning of known phishing/baiting web pages. Disabling CD/DVD drives and restricting access to USB ports can help protect against baiting attacks. A successful social engineer, on the other hand, will try to circumvent these safeguards. As a result, increasing user education and awareness is the best way to prevent SE (CERT-UK, 2015, s. 8).

Conclusion

The proliferation and increasing integration of digitalization in all aspects of everyday life have led to the emergence of novel cyberattack techniques that target consumers in cyberspace. In the face of persistent attacks targeting individuals, companies, and even states, it is noteworthy that social attacks, which exploit human vulnerabilities, represent the prevailing kind of attack. With the advancement of cybersecurity products and measures, there has been a notable shift in the strategies employed by attackers, who have transitioned from technical cyber-attacks to a more targeted approach that capitalizes on individuals' vulnerabilities and shortcomings.

The utilization of social engineering techniques can serve as a means to independently gather sensitive information or as a component inside a broader and intricate attack strategy. In essence, a cyber-attack can be executed exclusively through social engineering tactics, or it can be employed as a constituent or instrument during specific stages of a technological cyber-attack.

Social engineering and other non-technical cyberattacks constitute a substantial danger to international cybersecurity. These attacks are frequently difficult to detect and avoid, and the implications for individuals, businesses, governments, and the international community can be disastrous.

In the instance of social engineering, attackers use human psychology to dupe others into disclosing sensitive information or acting in ways that jeopardize their security. This can be accomplished using a variety of techniques, including phishing emails, vishing phone calls, and luring assaults.

Social engineering assaults are frequently successful because they exploit people's vulnerabilities, such as their confidence in others, desire to help others, or fear of missing out. Furthermore, social engineers are continually developing new strategies to capitalize on the most recent technologies and trends.

To defend against social engineering assaults, it is critical to understand the various types of attacks and the strategies used by attackers. Security methods like secure passwords, multi-factor authentication, and security awareness training are also essential. At the international level, governments and organizations must collaborate to increase awareness of social engineering attacks and establish risk-mitigation techniques. This involves exchanging information about new threats, creating shared training programs, and working with law enforcement on investigations.

The final inferences from the analysis above are: a) User or human being is the weakest link in cybersecurity. b) SE attacks rely on human weaknesses and vulnerabilities. c) SE attacks need less technical or software knowledge. d) Phishing, spear phishing, impersonation, and baiting are widely used attacks. e) SE techniques are the only way to access to air-gapped networks or intranets. f) SE attacks have deep impacts on national and international security along with individual and company security. g) Some very powerful SE attacks have been launched on national and international security in the last decade including attacks on the Iran nuclear facility, intervention in the US Presidential Election of 2016, hacking of the CIA director, and some major attacks on critical infrastructures. h) Awareness training particularly digital citizenship education is the most effective way of preventing and mitigating SE attacks. i) Finally, SE is a dynamic process evolving constantly and thus needs constant measures and development policies.

References

Akyeşilmen, N. (2018). *Siber politika ve siber güvenlik,* Ankara: Orion Kitapevi.

Aldawood, H. And Skinner, D. (2019). Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal, *International Journal of Security (IJS)*, 10(1), 1-15. https://f.hubspotusercontent30.net/hubfs/8156085/WhitePaper%20-%20IJS%20-%20Contemporary%20Cyber%20Security%20Social%20Engineering%20Solutions%5B1%5D.pdf Access date: October 30, 2022.

Allen, J. (2022). Social engineering penetration testing: Attacks, methods, & steps. https://purplesec.us/social-engineering-penetration-testing/ Access date: November 13, 2022.

Baezner, M and Robin, P. (2017). *Hotspot analysis: Stuxnet,* Zürich:Center for Security Studies (CSS). https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf Access date: November 10, 2022.

Breda, F., Barbosa, H. and Morais, T. (2017). Social engineering and cybersecurity, conference: International technology, education and development conference. https://www.researchgate.net/publication/315351300_SOCIAL_ENGINEERING_AND_CYBER_SECURITY Access date: October 30, 2022.

Brown, R. (2012). South Carolina offers details of data theft and warns it could happen elsewhere. https://www.nytimes.com/2012/11/21/us/more-details-of-south-carolina-hacking-episode.html Access date: November 10, 2022.

CERT-UK. (2015). *An introduction to social engineering, Cert-UK publicaiton*, https://info.publicintelligence.net/UK-CERT-SocialEngineering.pdf Access date: October 29, 2022.

Chinta, M., Alaparthi, J. And Kodali, E. (2016). A study on social engineering attacks and defense mechanisms. *International Journal of Computer Science and Information Security (IJCSIS)*, 14 Special issues,225-231. https://archive.org/stream/IJCSISVol14SpecialIssueICETCSE2016Final/IJCSIS%20Vol%2014%20Special%20Issue%20ICETCSE%202016%20Final_djvu.txt Access date: October 30, 2022.

Dolly, J. (2017). The cyber cold war: The silent, but persistent threat to nation-states. https://www.itproportal.com/features/the-cyber-cold-war-the-silent-but-persistent-threat-to-nation-states/ Access date: November 08, 2022.

Duarte, N., Coelho, N., Guarda, T. (2021). Social engineering: The art of attacks, In Guarda, T., Portela, F., Santos, M.F. (eds) *Advanced Research in Technologies, Information, Innovation, and Sustainability*. ARTIIS 2021. *Communications in Computer and Information Science*, vol.1485. Springer, Cham. https://doi.org/10.1007/978-3-030-90241-4_36 Access date: November 04, 2022.

ESET. (2021). *Social engineering handbook: How to take the right action*. https://www.eset.com/fileadmin/ESET/INT/Landing/2021/Project_progress/ESET-Social_engineering_handbook.pdf Access date: November 04, 2022.

Fleming, R. (2010). Bits before bombs: How Stuxnet crippled Iran's nuclear dreams. https://www.digitaltrends.com/computing/bits-before-bombs-how-stuxnet-crippled-irans-nuclear-dreams/ Access date: November 10, 2022.

Fruhlinger, J. (2017). What is Stuxnet, who created it and how does it work? https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html Access date: November 12, 2022.

Gatefy. (2021). 10 real and famous cases of social engineering attacks. https://gatefy.com/blog/real-and-famous-cases-social-engineering-attacks/ Access date: November 08, 2022.

Ghauri, F. A. (2021). Social engineering and its importance. https://www.researchgate.net/publication/354849736 Access date: November 04, 2022.

Greenwald, G. (2013). NSA collects phone records of millions of Verizon customers Daily. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order Access date: November 10, 2022.

Hadnagy, C. (2018). *Social engineering: The science of human hacking*, Indianapolis: John Wiley & Sons, Inc.

Hiik.(2017). *Conflict Barometer-2017*. https://hiik.de/conflict-barometer/current-version/?lang=en Access date: November 08, 2022.

Hill, G. (2018). Lessons learned from Snowden. https://www.scmagazine.com/lessons-learned-from-snowden/article/541919/ Access date: November 08, 2022.

Ignatius, D. (2017). Russia's assault on America's elections is just one example of a global threat https://www.washingtonpost.com/opinions/global-opinions/russias-assault-on-americas-elections-is-just-one-example-of-a-global-threat/2017/02/23/3a3dca7e-fa16-11e6-9845-576c69081518_story.html? noredirect=on&utm_term=.179c499b359b Access date: November 12, 2022.

Indzhov, O. et. al. (2022). Social Engineering Threats Towards Non-IT Students: A Case Study on Mitigation Strategies. https://www.diva-portal.org/smash/get/diva2:1671049/FULLTEXT01.pdf Access date: November 04, 2022.

Israel, R. (2018). Lessons Being Learned From Edward Snowden. http://www.theglobalcitizensinitiative.org/lessons-being-learned-from-edward-snowden/ Accessed date: July 28, 2018.

Internetlivestats. (2022). Internet live stats. https://www.internetlivestats.com/ Access date: November 12, 2022.

Jimoh, A. (2022). Social Engineering Attacks. https://www.researchgate.net/publication/358647625_Social_Engineering_Attacks Access date: October 30, 2022.

Kontio, M. (2016). *Social Engineering 101*, Bachelor's Thesis, Turku University of Applied Sciences, Business Information Technology | Business Data Communications and Information Security. https://core.ac.uk/download/pdf/38134896.pdf Access date: November 08, 2022.

Krombholz, K, et. al. (2014). Advanced Social Engineering Attacks, Journal of Information Security and Applications. https://www.researchgate.net/publication/267340031_Advanced_social_engineering_attacks Access date: October 30, 2022.

McLellan, C. (2016). How hackers attacked Ukraine's power grid: Implications for Industrial IoT security. https://www.zdnet.com/article/how-hackers-attacked-ukraines-power-grid-implications-for-industrial-iot-security/ Access date: November 10, 2022.

Michael, T. And Cambridge, E. (2018). 'Cyber Terrorist' Caged Brit teen hacker Kane Gamble posed as CIA boss to access secret military files locked up for two years. https://www.thesun.co.uk/news/6105694/british-teen-hacker-kane-gamble-cia-boss-jailed-two-years/ Access date: November 08, 2022.

Mitnicksecurity. (2020). The Top 5 Most Famous Social Engineering Attacks of the Last Decade. https://www.mitnicksecurity.com/blog/the-top-5-most-famous-social-engineering-attacks-of-the-last-decade Access date: November 08, 2022.

Mitnicksecurity. (2022). *The History of Social Engineering* (And How To Stay Safe Today). https://f.hubspotusercontent20.net/hubfs/3875471/Ebooks/Social-Engineering-History-MitnickSecurity.pdf?hsCtaTracking=b5736792-f5c6-4635-9ab4-072f9edae08f%7C803e6a65-4e3a-46b4-a63c-e799856aa820 Access date: November4, 2022.

Oosterloo, B. (2008). Managing Social Engineering Risk: Making Social Engineering Transparent, Master Thesis submitted to University of Twente. https://essay.utwente.nl/59233/1/scriptie_B_Oosterloo.pdf Access date: November 1, 2022.

Pagliery, J. (2017). The emergence of the 'cyber cold war'. https://money.cnn.com/2017/01/19/technology/cyber-cold-war/index.html Access date: November 09, 2022.

Reed, C. (2022).21 Social Engineering Statistics – 2022, Firewall Times, May 16, 2022. https://firewalltimes.com/social-engineering-statistics/#:~:text=The%20Average%20Organization%20Is%20Targeted,against%20about%202.7%20per%20day Access date: November 12, 2022.

Salahdine, F., and Kaabouch, N. (2019). Social Engineering Attacks: A Survey, Futur Internet, 11(89). https://www.researchgate.net/publication/332151597_Social_Engineering_Attacks _A_Survey Access date: November 04, 2022.

Scanlan, Q. (2018). Russians still trying to interfere in US elections every 'way they can': Republican senatör. https://abcnews.go.com/Politics/russians-interfere-us-elections-republican-senator/story?id=56889554 Access date: November 12, 2022.

Singer, P.W. (2017). How America Can Beat Russia in Cyberwar Despite Trump. https://www.wired.com/2017/01/america-can-beat-russia-cyber-war-despite-trump/ Access date: November 09, 2022.

Sjouwerman, S. (2022). Crelan Bank Loses 75.8 Million Dollars In CEO Fraud. https://blog.knowbe4.com/crelan-bank-loses-75.8-million-dollars-in-ceo-fraud Access date: November 10, 2022.

Sjouwerman, S. (2022). Edward Snowden Used Social Engineering To Hack NSA. https://blog.knowbe4.com/bid/351948/edward-snowden-used-social-engineering-to-hack-nsa Access date: November 10, 2022.

Sysgroup. (2022). Statistics You Need to Know About Social Engineering. https://www.sysgroup.com/resources/blog/statistics-need-to-know-social-engineering Access date: November 12, 2022.

Şöhret, M. (2022). *Methods of cyber intelligence gathering*, Yılmaz, C. İ. (Ed.). *İstihbarat araştırmaları*, Konya: Necmettin Erbakan Üniversitesi Yayınları.

Tabbaa, B. (2020). Zer0 Days: How Stuxnet Disrupted the Iran Nuclear Program and Transformed Computer Security. https://medium.com/dataseries/zer0-days-how-stuxnet-disrupted-the-iran-nuclear-program-and-transformed-computer-security-9b9587199f06 Access date: November 10, 2022.

Trendmicro. (2016). Austrian Aeronautics Company Loses Over €42 Million to BEC Scam. https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/austrian-aeronautics-company-loses-42m-to-bec-scam Access date: November 10, 2022.

Wang, Z. (2018). Sun, L. And Zhu, H., Defining Social Engineering in Cybersecurity, Vol.8. https://www.semanticscholar.org/paper/Defining-Social-Engineering-in-Cybersecurity-Wang-Sun/4f460417fc13a59326c525a9eefc77798947885a Access date: October 30, 2022.

Zorz, Z. (2016). Belgian bank Crelan loses €70 million to BEC scammers. https://www.helpnetsecurity.com/2016/01/26/belgian-bank-crelan-loses-e70-million-to-bec-scammers/ Access date: November 10, 2022.