Advances in Web Development Journal
vol. 1 no. 7, pp. 83–106

Submitted: 2023-12-07 | Revised: 2023-12-07 | Accepted: 2023-12-30

Keywords: social engineering, cybersecurity, phishing

Łukasz BOROWIEC [1], Krzysztof DEMIDOWSKI [2], Milena PECKA [2], Amelia JONARSKA [3]

THE ANALYSIS OF SOCIAL ENGINEERING METHODS IN ATTACKS ON AUTHENTICATION SYSTEMS

Abstract

This comprehensive exploration of social engineering attacks provides insights into various methods, including phishing, vishing, baiting, tailgating, and ransomware. The "grandchild" scam and its variations, as well as phishing examples, illustrate the evolving tactics used by attackers. Prevention strategies encompass education, training, and technological tools, emphasizing the need for a balanced approach. The conclusion underscores that public awareness, continuous training, and specialized detection tools are vital in mitigating the risks associated with social engineering attacks on authentication systems.

1. INTRODUCTION

The document will identify and discuss the sociotechnical methods that are used to break authentication systems (Foriano & Jungnickel, 2015). Social engineering used to break authentication barriers is probably one of the most dangerous forms of attack (Krombholz et al., 2015) , the aim of which is to achieve financial gain or obtain confidential data such as personal data, social security numbers, passwords, bank account numbers, medical records and many other pieces of information by deceiving an individual, a company or organizational unit (Mashtalyar et al., 2021). Knowledge of the threats and methods of defense against them can contribute significantly to countering their effects.

Despite the widespread use of common cybersecurity measures such as antivirus software and network security procedures, there is a noticeable lack of focus on certain security practices, including encryption of emails, flash drives, laptops and documents (Strzałka, 2022). A study by the cybersecurity company Cybint highlighted that in 2018, 62% of businesses fell victim to phishing or other social engineering tactics (Thakur et al., 2022).

1. University of Information Technology and Management, Poland
2. Rzeszow University of Technology, Department of Complex Systems, Poland
3. Rzeszow University of Technology, The Faculty of Mathematics and Applied Physics, Poland

2.AUTHENTICATION SYSTEMS

Authentication is the act of proving one's identity as a user in an IT system (Usmonov, 2021), so it is a verification process. Identity verification can involve checking identity documents or in IT systems using, for example, a certificate to verify the authenticity of websites. Depending on the communication channel, various authentication methods are utilized (Tab 2.1). An authentication system consists of three elements.

The first element of the system is identification context:

- identification of a person, an entity (e.g. when logging in to a service, website or application the user provides a login),
- telephone call (e.g. call to a bank, where the name or customer number is given),
- connecting a browser to a website, where the identifier is an SSL certificate issued by a Root Certificate Authority (Syed Idrus et al., 2013).

The second element of the authentication system uses a suitable method to verify a person's identity through, for example:

- a service, website or application asks for your password (Dul et al., 2023),
- in a telephone conversation, the staff of a bank or other institution (e.g. a doctor's surgery) ask a user for personal data eg. user date of birth, mother's maiden name, parents' first names, last digits of your national identification number, date of issue of your identity card or the number of a card created at a clinic,
- the browser checks with an intermediate certificate whether the SSL certificate is issued by the correct CA (Barkadehi et al., 2018).

The third element is authorization, during which it is checked whether the verified person is entitled to the information he or she wants to obtain, e.g:

- the service, website or application verifies which services or files the user has access to (Komarova et al., 2018),
- the bank confirms that the person logging on to the service has access to account, where user can perform various transactions, but no longer has access to the account of his/her spouse or children when they reach the age of majority, for example (Hiltgen et al., 2006),
- the browser verifies the KeyUsage flags (which provides read access to the properties of the certificate key) stored in the certificate by an authorized party (Wang et al., 2019).

Tab 2.1: Various authentication methods utilized depending on the communication channel

Channel	Methods
For individuals	identity documents (e.g., ID card, passport, driving license), passwords, microprocessor cards, tokens (one-time codes generated for authentication of specific transactions, such as bank transactions), biometric data (e.g., facial images, fingerprints, iris scans), and biochips (RFID implants - radio frequency identification systems placed under the skin) (Dewangan, 2015)
For paper documents	stamps, signatures, and watermarks (van Renesse, 1997)
For electronic documents and messages	digital signatures Katz, J. (2010)
For electronic communications	passwords, symmetric cryptography (where encryption and decryption are performed using a single key), asymmetric cryptography (utilizing a public key for encryption and a private key for decryption), one-time passwords, and zero-knowledge proofs (a cryptographic method where one party proves to another that they possess certain information without revealing that information)

Such a model of systems is referred to as single-factor authentication. For two-factor authentication (2FA), two of the analyzed methods are combined. For instance, when logging into a bank, in addition to entering a login and password, one must also input a code from a received SMS or verify their identity using the bank's phone application by inputting a login code to confirm the login. Another method for the second factor of authentication could be a hardware token, which might require an additional PIN or the use of an authentication application (Szczygieł et al., 2023). An example of a two-factor authentication system is an ATM card combined with a PIN. For the highest security systems, access may also necessitate biometric data such as a fingerprint, iris scan, facial recognition, or other biometric measures. 2FA methods are threatened by potential identity theft (Matejkowski & Szmyd, 2023) or risks of SMS-based authentication (Stęchły & Szpunar, 2023).

2.1.Continuous authentication system

In conventional computer systems, user authentication typically occurs only during the initial login session and not throughout the user's active session on the system. Continuous authentication of a user's identity, however, can be achieved using specific biometric attributes and behavioral characteristics (Baig & Eskeland, 2021). This can be based on factors such as typing style, keystrokes on mobile devices, touch dynamics, or even gait recognition. Authentication systems that rely on behavioral biometrics are known as continuous authentication systems (Stylios et al., 2016).

3.SOCIAL ENGINEERING DECEPTION

Many definitions of social engineering can be found on the Internet or in relevant books, with varying degrees of accuracy. One of the most common definitions comes from Kevin Mitnick in his book "The Art of Deception". Kevin Mitnick describes:

"Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he isn't, or through manipulation. Consequently, the social engineer can exploit individuals to acquire information, with or without the aid of technology" (Simon & Mitnick, 2002).

Based on this definition, it is possible to infer that sociotechnics revolves around identifying and exploiting gaps in human nature, or in other words, human weaknesses. This involves manipulating an individual to obtain coveted information that can then be used to breach security measures in information systems.

Social engineering attacks can be characterized as efforts of persuasion, manipulation, influence, and deception (C. Hadnagy, 2010). In the realm of cyber security, such attacks encompass online fraud, often manifesting in forms such as phishing. The foundation of these attacks lies in pinpointing and leveraging human vulnerabilities. This could be due to lack of knowledge, undue trust in others, or even the victim's personal circumstances, which increases the success rate of the attack. Quite often, victims remain unaware of the attack (Gupta et al., 2016).

Despite the varied methods and tools used for social engineering attacks, they typically follow a common pattern that includes manipulating individuals into divulging sensitive information or taking actions against their best interests (Tab 3.1). Understanding and recognizing this pattern is crucial for enhancing cybersecurity defenses. Social engineering attacks can be qualified into two categories:

- a human-based attack, where the perpetrator interacts directly with the victim,
- and a software-based attack, where the perpetrator uses a computer or phone to attack the victim. The perpetrator in this category has the ability to attack many people simultaneously (Yasin et al., 2019).

Tab 3.1: Common elements of social engineering attacks

1.	Gathering information about the victim
2.	Developing and fostering a relationship with the victim
3.	Utilizing the information amassed to execute an attack, establishing trust, inducing guilt, or capitalizing on the victim's sense of civic duty
4.	Ensuring no evidence is left behind

Depending on the way how the social engineering attack is carried out, we can distinguish between three types:

- social attacks - carried out on people by relating to the victim and playing on their emotions. An example of such an attack is personalized spear phishing, preceded by community intelligence,
- technology-based attacks are attacks carried out via the Internet, e.g.: social networks, websites to collect sensitive information such as login details, passwords, bank account details, credit card details, etc,
- physically based attacks, i.e. physically performing an action, e.g. going through the trash to obtain valuable documents.

All of these categories can intermingle and combine during a social engineering attack. Examples of social engineering attacks include shoulder surfing, dumpster diving, phishing, document theft, fake software, pretexting, phone social engineering, ransomware, reverse social engineering, phone help desk impersonation, theft diversion, Pop-Up windows, tailgating, Robocalls (phone call with an automated machine), baiting (e.g. dropping off an infected memory stick at a company).

When analyzing the different categories of Social engineering attacks, we can distinguish another division between direct and indirect attack. A direct attack refers to physical, visual or conversational contact between the perpetrator and the victim. The perpetrator may be present in the victim's company and launch the attack there, e.g. document theft, physical access, pretexting, shoulder surfing. An indirect attack, on the other hand, is carried out using an ICT system by means of e.g. malware, phishing, ransomware, online social engineering, Pop-Up windows, SMishing.

4.CHARACTERISTICS OF SOCIAL ENGINEERING ATTACKS

4.1.The “Elder Scam” method

The Elder Scam, as well as its more recent variations like the "policeman" or "clerk" scams, is a prevalent social engineering attack (Parti, 2022). These scams operate on a similar mechanism. The primary targets are typically the elderly, as they are perceived as being physically and mentally more vulnerable, often isolated, and are more likely to trust those who seem to hold authority. These victims may possess tangible assets that, given their perceived vulnerabilities, are seen as easily exploitable (Shao et al., 2019).

Key to the success of these scams is the imposition of time pressure on the victims. This urgency keeps them engaged and limits their opportunities to consult with others, ensuring they remain isolated and susceptible to manipulation.

In the elder scam, the scammer might introduce themselves vaguely, such as a distant family member, encouraging the victim to "recognize" them. Once the victim incorrectly identifies them as a grandchild, the scammer acts indignant, invoking guilt by

questioning how the grandparent could forget them. The scammer then proceeds to narrate a fabricated emergency necessitating immediate financial assistance. Typically, an exorbitant sum is first requested, and upon refusal, a more reasonable amount is suggested. This tactic, termed 'refusal-withdrawal', plays on the victim's sense of responsibility, making them more inclined to agree to the lesser request. To identify potential victims, perpetrators might resort to old telephone directories, targeting older-sounding names.

The "policeman" variation hinges on the victim's sense of civic duty and trust in law enforcement. Victims manipulated by these methods may be compelled to exhaust their savings or even acquire loans, only realizing the deceit once the funds have been transferred, or when they recount the event to a family member. These scams utilize social engineering tactics like inducing guilt, manipulating conversation to extract information, exploiting societal trust (e.g., in the police), and leveraging the victim's desire to assist.

A concerning aspect of this scam is the use of a "courier" or "post" – individuals who, unbeknownst to them, are participating in the fraud, thinking they are merely earning a quick buck.

Public awareness campaigns have led to modifications in the "grandchild" scam technique. For instance, in the first half of 2021, victims defrauded by this method lost a staggering PLN 63 million. The largest single transaction to a scammer in 2022 was PLN 250,000. Moreover, a criminal group apprehended in 2023 had, since January that year, swindled over PLN 1.5 million using a version of this scam (KKG, 2021).

4.2.Phishing

The most prevalent technique-based social engineering attack is phishing. Its objective is to acquire private or confidential data by misleading or deceiving the target (Chang et al., 2013). Attackers use various tools like SMS on phones or emails and redirect links on the Internet. Manifestations of phishing include counterfeit websites, ads, emails, antivirus software, PayPal pages, and deceptive offers of free rewards. Sometimes, attackers use phones or emails to inform about a significant prize, baiting victims into revealing their personal details (Mishra & Soni, 2019). There are numerous types of phishing attacks, and among them, we can highlight:

- **Spear Phishing** - This is a personalized form of phishing attack directed towards a specific individual or organization. Instead of sending generic emails to a vast audience, attackers target a single individual, having beforehand gathered detailed information about them. This ensures the crafted message appears credible. The objective is to acquire valuable and confidential details about an entity, ranging from business insights and health records to banking details. The method usually involves sending a counterfeit email to the selected victim. Upon interacting with the email (e.g., clicking a link or opening an attachment), the victim might unintentionally compromise their system. Given their personalized nature, spear phishing attacks are hard to detect and are highly effective. A countermeasure involves being cautious about the personal information shared online, especially for individuals in sensitive sectors like government or military. Additionally, it's crucial to remain skeptical of suspicious emails and links (Parmar, 2012).

- **Whaling phishing** - This is a subset of spear phishing, focusing exclusively on high-ranking individuals within an organization, such as CEOs or government officials. Given the potential gain from such individuals, these attacks can be particularly devastating (Kalaharsha & Mehtre, 2021).
- **Vishing** - is a type of phishing attack carried out using telephone calls, often utilizing Voice over the Internet Protocol (VoIP). In these attacks, perpetrators usually pretend to be employees from trusted institutions, such as banks, and might request sensitive details like logins, passwords, and national identification numbers. Another tactic involves urging victims to install specific software on their devices, which could capture confidential data or give the attacker control over the victim's system. A notable real-world example of vishing involves cryptocurrency scams. After a data breach, fraudsters might contact potential victims offering assistance or a fabricated scenario. They then help the victim install malicious software, which provides the scammer control over the victim's computer. This access allows them to make large transactions, often draining the victim's cryptocurrency holdings (Griffin & Rackley, 2008).
- **Interactive Voice Response Phishing** - involves using an interactive voice response system to convince victims to divulge sensitive information (Choi et al., 2017).
- **Business Email Compromise Phishing** - Business Email Compromise Phishing focuses on high-profile individuals in companies or organizations. The goal is to intercept crucial details, such as email communications, payment schedules, or other confidential data. In this scheme, attackers gather in-depth information about their targeted individual and the company. They may then craft a convincing business email, often sent to a subordinate, enticing them to click a link or open an attachment. This action can potentially grant attackers access to the company's network. The content of these deceptive emails often exerts time pressure on the recipient, encouraging hasty actions without thoughtful consideration (Atlam & Oluwatimilehin, 2023).
- **Social media phishing** - is a form of attack wherein the perpetrator monitors the victim's social media and other frequently visited sites to gather detailed information. Using this information, the perpetrator devises an attack strategy. The collected data can then be used in various ways to deceive the victim (Vishwanath, 2017).
- **Clone** phishing involves email-based attacks. In these instances, the perpetrator is familiar with many of the business applications used by an individual or organization. Using this knowledge, the attacker replicates a similar email message to mimic a standard, legitimate email. The primary objective of this attack is to acquire sensitive information, including the victim's credentials. Clone phishing is also based on fake websites (Chaudhuri, 2023).
- **Smishing** - is a text message format based on a vishing attack. The only difference in smishing is that it is based on a text message rather than a phone call (Mishra & Soni, 2020).

Attacks of the type in discussion, despite common features (Tab 3.1), have different forms of course. A person's susceptibility to the impact of an attack can depend on a number of factors. Among other things, it depends on the situation the potential victim is in. An example phishing attack may look like the following:

- The victim received an SMS message stating that they had underpaid their electricity bill and needed to settle the payment to avoid having their electricity cut off. A link was provided for the payment. Despite being in the industry and well aware of such scams, the victim's recent move into a new flat and the ensuing complexities of managing utility contracts momentarily made the message seem plausible.
- The victim, experiencing a prolonged renovation process for their flat, had not received any electricity bills during this period. Consequently, when an SMS asserted an outstanding payment, genuine concern about a potential missed payment led the victim to click on the provided link to settle the supposed debt. However, just before completing the transaction, a nagging doubt prompted the victim to double-check the claim in person at the customer service office.
- Upon reaching the service office, the victim was promptly informed that such messages were not sent by them, and caution was advised against following through with such links. Reflecting on the situation, the victim realized that the ongoing stress related to the new flat had made them susceptible to the scam
- The deceitful link in the SMS led to a payment portal, which, in hindsight, had all the hallmarks of a phishing site. After selecting the bank, it only required the customer number without any password. The subsequent step was an SMS code verification.

Many received similar deceitful messages, prompting an awareness campaign to combat the scam. These mass-sent messages about electricity arrears targeted unsuspecting individuals via SMS and email. Although many recognized the scam, the sheer volume of attempts meant some fell prey, leading to significant financial losses.

From my findings, between 5 and 19 May 2022, the culprits dispatched over a million such deceptive messages. The total financial damages caused by these attacks exceeded PLN 52,000. Apart from monetary loss, victims also compromised sensitive information, including login credentials, credit card details, and more. The local authorities arrested 14 individuals suspected of involvement in this widespread scam (Policja Śląska, 2022).

4.3.Examples of phishing attacks

- In 2020, several celebrity Twitter accounts fell victim to a spear-phishing attack targeting a Twitter employee. These high-profile accounts were hijacked and subsequently misused by Bitcoin scammers. This calculated breach reportedly earned the attackers around $100,000 . The hackers strategically targeted a select group of Twitter employees, deploying tactics of manipulation and deceit. Leveraging the trust of these employees during phone calls, the attackers masqueraded as genuine individuals seeking assistance. Unfortunately, in their bid to assist the supposed caller, these employees inadvertently provided access credentials to Twitter's internal systems (Frenkel et al., 2020) .

- A renowned real estate agent, who is also a business connoisseur, lost $380,000 due to a spear-phishing ploy. The attacker cunningly crafted an email address mimicking

that of her assistant; however, it had a single letter misaligned. This deceptive email carried a counterfeit invoice demanding the payment of $380,000. Without recognizing the discrepancy, the accountant proceeded to settle the invoice. The scam came to light only when the accountant, in a subsequent response, tagged the authentic email address of the assistant (Sandler, 2022).

- Toyota Boshoku Corporation, a key component supplier for Toyota, fell victim to a BEC (Business Email Compromise) scheme. In this phishing email assault, the culprits successfully swindled the company out of over 37 million. On August 14, 2019, these fraudsters duped an individual at Toyota with financial authorization into altering account details for an electronic funds transfer (Mathews, 2019). A report by the FBI reveals that BEC scams have inflicted a staggering loss of approximately $5.3 billion on the global economy in the last six years . Surveys suggest that around 75% of businesses face at least one BEC attack attempt annually (FBI, 2022).

- Between 2013 and 2015, tech giants Google and Facebook were deceived out of a staggering US$100 million. The assailant executed a sophisticated phishing scheme against them, masquerading as an Asian manufacturer. The meticulously crafted emails, designed to mimic authentic correspondence, were dispatched to employees and agents overseeing multi-million dollar transactions for both corporations. Not stopping at emails, the scammer also fabricated invoices, contracts, and letters mirroring legitimate company documents, even going so far as to fake the signatures of top executives from both Google and Facebook. The success of this ruse might be attributed to employees' presumption of security, given the stature of their employers. As a measure against such future threats, both companies have pledged to bolster their staff's awareness and training regarding cybersecurity risks (Huddleston, 2019).

- In 2018, Marriott, a renowned hotel chain, disclosed a massive security breach compromising several hundred million customer records, including sensitive details like credit card and passport numbers. This intrusion was detected by the company's security mechanisms, which flagged unauthorized access attempts to their guest reservation system between 2014 and 2016 (Perlroth et al., 2018).

  Upon investigation, Marriott uncovered encrypted data, evidencing the criminals' sophisticated actions. Notably, the unauthorized activities stemmed from an administrator account; however, the individual assigned that account wasn't the perpetrator. Instead, an external entity had compromised it. Technical evaluations revealed the presence of two malicious software: the RAT remote access Trojan and MimiKat malware. Both tools facilitated the unauthorized takeover of the privileged account, suggesting that the initial breach might have been initiated via a deceptive phishing email.

  Contributing to the vulnerability were Marriott's scaled-back investments in security technology and significant staff reductions in the IT department. There's speculation that the cyber assault bore hallmarks of an operation linked to Chinese intelligence. Indicators include the specific use of cloud-hosting environments and the conspicuous absence of the stolen data on the dark web. Instead of monetizing the data, it's believed the acquired information, especially on US government personnel, was consolidated into a data repository for subsequent in-depth analysis by Chinese agencies.

The breach's root cause is suspected to be a craftily engineered phishing email, feigning to be from a trusted source and requesting a password reset under the guise of addressing a technical hiccup, thus securing unauthorized access credentials (Volodzko, 2018).

4.4.Open redirect links - anti-phishing campaign by Microsoft

Microsoft is spearheading an initiative against phishing attacks that employ redirect links to steal user credentials . In these attacks, cybercriminals cleverly disguise these links as reputable services, enticing users to click on them. These links then lead to CAPTCHA verification screens, which, due to their authentic appearance, both deceive users and potentially bypass certain automated security systems. After the CAPTCHA, users are then funneled to fake login pages (Intelligence, 2021).

One tactic attackers employ involves setting up redirect links within a trustworthy domain. This way, when users hover over the link, they see a familiar and supposedly safe domain address. Additionally, cybercriminals are exploiting free email domains to pose as legitimate, trusted entities (Suriya et al., 2009).

Microsoft's research reveals a staggering 91% of these attacks are initiated through email, often culminating in credential theft and unauthorized network access. Phishing remains the primary method attackers employ to siphon off user data. According to Microsoft's 2020 Digital Defence report, they thwarted 13 billion malicious and suspicious emails, of which 1 billion were URL-based (Microsoft, 2020).

Here's a brief rundown of how these redirect link attacks function: A user is lured into clicking a camouflaged link, leading them to the attacker's site. These sites cleverly utilize Google's reCAPTCHA service, which, aside from giving an air of legitimacy, can stymie some security systems from identifying the genuine phishing page.

To counteract this abuse, Microsoft suggests users adhere to best practices from their software vendors, including ensuring automatic updates for the most recent software versions.

4.5.Pretexting

Pretexting is an attack method where attackers craft convincing scenarios to steal a victim's personal information. They carry out these schemes mostly through phone calls or emails. To prepare for the attack, they gather information from various places such as phone directories, websites, business conferences, social media platforms, and company profiles (Workman, 2008) (Thilakarathne & Samarasinghe, 2022).

Often, the attackers create scenarios that range from job offers, lottery wins, or even impersonating business partners (C. J. Hadnagy et al., 2010). With the information they've gathered, they ensure the scenario sounds plausible enough to gain the victim's trust (Alazri, 2015). An example would be an attacker acting as a salesperson demanding an upfront payment, using a false account number. In another case, they might pose as a bank

representative, expressing concerns about suspicious activities on the victim's account. In doing so, they aim to coax the victim into revealing sensitive details.

While the main goal of pretexting is either to swindle money or acquire authentication credentials, it is one of the prominent tactics used in social engineering attacks, particularly on digital platforms. It's different from phishing, which casts a wider net. Pretexting focuses on creating trust through fabricated stories or identities, targeting specific individuals.

To protect oneself from such deceptive tactics, it's vital always to verify information with trusted sources. Limiting personal information shared online, using VPNs to protect online identities, encrypting personal data, avoiding public unsecured networks, and adopting strong, unique passwords are also recommended defensive strategies (Ghani et al., 2019).

4.6.Baiting

Bait attacks are a type of phishing attack where the user is lured into clicking on a link under the guise of receiving a free item or winning a lottery . It can also resemble a Trojan horse . The attack can be carried out using a USB stick containing malware (Koyun & Al Janabi, 2017). The USB stick is deliberately left in a car park or restaurant so that the victim, out of curiosity, picks it up and connects it to their computer while malware such as spyware is running. The malware runs in the background, unnoticed by the victim.

The perpetrator can also use the attack to send an email with a link to a website containing malicious code. When the link is clicked, the victim's computer is infected with the malware (Sethi, 2022). The bait can take a variety of forms, including links to malicious files sent by email, enticing offers such as an email offering a discount on a particular product that the victim unknowingly downloads onto their computer after clicking on the link, or infected devices that the victim unknowingly connects to their computer. Countermeasures against this form of attack include not clicking on every link on a website or in an email received, not connecting USB devices of unknown origin to your computer equipment, using tested anti-virus and anti-malware software to detect the threat, and increasing your knowledge of the methods of social engineering attacks on IT systems (Ferguson, 2017).

4.7.Tailgating

A tailgating attack involves gaining physical access to a building or a restricted area within a company or organization. This is often achieved by following someone who is authorized to enter the location. For instance, the attacker might ask someone to hold the door open, claiming they've forgotten their badge or RFID card (Bhattad & Patil, 2023).

In another scenario, the perpetrator might ask to borrow a mobile phone, citing the need to make an urgent call. Once they have the phone, they can quickly install malware to access confidential data (Salahdine & Kaabouch, 2019).

4.8.Ransomware

A ransomware attack involves encrypting data and files, effectively blocking access to them. Victims are then coerced into paying a ransom, often with the added threat of the data being published if the ransom isn't paid (Kok et al., 2019).

Ransomware typically enters a system through various means. This can be by clicking on deceptive links promising free items, which then redirect users to malicious websites. Another common entry point is through emails containing harmful links or through ads that offer products at seemingly discounted prices (Moon & Chang, 2016).

During an attack, victims might see fraudulent messages on their screens. These messages could falsely claim to be from authorities, such as the police, alleging that the user's system has been used for illegal activities or contains illicit content like pornography or unauthorized software (Vardalaki & Vlachos, 2021).

A particularly menacing variant of this attack encrypts the victim's data. Ransomware attacks can be broken down into six stages: malware creation, deployment, installation, command and control, destruction, and extortion. According to FBI statistics, the most financially damaging year for ransomware was 2016, with victims suffering around $1 billion in losses from data compromises. Often, the damages caused by the ransomware far exceed the ransom amount itself (Brewer, 2016).

5.PREVENTION

Preventing social engineering attacks with IT systems requires a multi-pronged approach. Foremost, it involves security education and training (Beuran et al., 2016) ICT . Awareness campaigns on social media and television can be especially beneficial for older individuals who might not be as well-acquainted with ICT tools and are therefore more susceptible to attacks.

For businesses, it's crucial to invest in tools that detect malware threats. But even more important is educating employees about safeguarding sensitive data and promptly reporting any unusual activities. Implementing a robust company policy regarding information and network security can reinforce the importance of being cautious. This includes making staff aware of the risks associated with opening emails from unknown senders or clicking on uncertain links (Kemper, 2019).

In terms of telephonic threats, the first line of defense is to verify the caller's identity. If the source of the call is dubious and the caller's intentions remain unclear, it's advisable to end the call and alert relevant authorities (Subbalakshmi et al., 2022).

For email phishing attacks, one effective measure is to inspect the sender's email address and authenticate the email's source before engaging with any links or attachments. Training company employees by simulating a phishing attack on a fictional business can also be enlightening. This hands-on approach helps them understand the mechanics of Social engineering phishing attacks. Such knowledge equips them with heightened vigilance and

security awareness (Cuchta et al., 2019). To counter tailgating attacks, consistent training and awareness campaigns are essential. Employees should be conditioned to always verify an individual's identity before granting access to any company premises.

Machine learning algorithms offer another line of defense against phishing. By analyzing the typical features of phishing attacks, these algorithms become adept at identifying related anomalies early on (Martínez Torres et al., 2019).

In the context of ransomware threats, companies should enforce an IT security policy that encompasses the use of both the organization's systems and external devices like USBs. Employees should be educated about the risks associated with using unfamiliar computers or plugging in unidentified USB devices. Emphasizing the importance of antivirus software is also crucial (Richardson & North, 2017).

Countermeasures against threats can be categorized into two main types: human-centric and system-centric:

- Human-centric countermeasures focus on education and awareness. This involves regular training, informational campaigns, and hands-on demonstrations of Social engineering attack mechanisms. By understanding how these attacks operate, individuals can be better prepared to defend against them, ensuring they remain vigilant against potential threats.
- System-centric countermeasures rely on leveraging the right technological tools. Specialized software solutions are employed to safeguard users from various threats, including but not limited to phishing, ransomware, and pretexting.

Considering these countermeasures, we can enumerate:

- Filtering tools - Examples include Microsoft filter, McAfee filter, and WebSense. These tools block email and web-based phishing attacks. However, they offer low performance (Moallem, 2021).
- Alerting and scanning tools e.g: Such as antivirus, anti-spams, and anti-scams. While they effectively warn of threats and initiate immediate scans, their effectiveness is often limited by human response time (Kandan et al., 2019).
- Biometric tools - Relying on unique biological traits, these tools excel in distinguishing genuine profiles from fake ones (Рамський et al., 2021).
- Artificial Intelligence Tools - Leveraging machine learning, these tools continually adapt for early threat detection, providing highly effective performance (Sarker et al., 2021).
- SERA (Social Engineering Centered Risk Assessment) tool - Though highly effective, this tool comes with a higher cost (Salahdine & Kaabouch, 2019).
- Phone-based tools - These tools are easy to use but typically offer low effectiveness.
- Flow Whitelisting Identifying - This learning-based tool distinguishes between malicious and legitimate traffic entering a company's network. However, its effectiveness can be hampered if users ignore its alerts (Alabdulrazzaq, 2017).
- IDS (Intrusion Detection System) - This system actively monitors networks or systems for malicious activities or potential breaches in policy (Ashoor & Gore, 2011).

While these tools offer robust defense mechanisms, many are costly to implement. Moreover, their efficacy often relies heavily on human interaction. Ignoring tool alerts can undermine their capabilities. Hence, a balanced approach that combines both training and cutting-edge technological safeguards is crucial. Tools powered by machine-learning algorithms are especially notable for minimizing human error. Still, it's important to remember that while these tools are continually evolving, so too are the methods employed by attackers. It's an ongoing battle to keep systems secure (Huang, 2020).

6.CONCLUSION

In the present study, the author has elucidated the conceptual frameworks of social engineering and authentication methods. A comprehensive exploration of the methodologies and tools employed in social engineering attacks targeting authentication systems has been undertaken, with particular emphasis on notable instances of phishing attacks encountered by prominent global information technology companies.

Drawing upon real examples, the present investigation has elucidated the phenomenon of phishing SMS attacks and telephone scams, predominantly directed at mature individuals. Furthermore, a delineation of defensive strategies against such attacks, coupled with methodologies for their detection, has been expounded.

From the research and articles referenced in this project, a clear conclusion emerges: Social engineering attacks, whether direct or via intermediaries like phones or internet-connected computers, cannot be entirely neutralized by relying solely on specialized IT and physical security measures. The primary emphasis must be on education, continuous training, and enhancing the knowledge of both employees within organizations and the public.

Consistent public awareness about the dangers present in the internet and telecommunication realms, coupled with strategies to counteract them – and bolstered by specialized detection tools for various Social engineering attacks – can help prevent the loss of personal data, confidential information, or financial assets, be it personal or corporate.

REFERENCES

Alabdulrazzaq, H. K. (2017). *Securing Web Applications: Web Application Flow Whitelisting to Improve Security* [PhD Thesis, Auburn University]. https://search.proquest.com/openview/13230f3d179c91c1fe4ba63355077e02/1?pq-origsite=gscholar&cbl=18750&diss=y

Alazri, A. S. (2015). The awareness of social engineering in information revolution: Techniques and challenges. *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 198–201. https://doi.org/10.1109/ICITST.2015.7412088

Ashoor, A. S., & Gore, S. (2011). Importance of intrusion detection system (IDS). *International Journal of Scientific and Engineering Research*, *2*(1), 1–4.

Atlam, H. F., & Oluwatimilehin, O. (2023). Business Email Compromise Phishing Detection Based on Machine Learning: A Systematic Literature Review. *Electronics*, *12*(1), Article 1. https://doi.org/10.3390/electronics12010042

Baig, A. F., & Eskeland, S. (2021). Security, Privacy, and Usability in Continuous Authentication: A Survey. *Sensors*, *21*(17), Article 17. https://doi.org/10.3390/s21175967

Barkadehi, M. H., Nilashi, M., Ibrahim, O., Zakeri Fardi, A., & Samad, S. (2018). Authentication systems: A literature review and classification. *Telematics and Informatics*, *35*(5), 1491–1511. https://doi.org/10.1016/j.tele.2018.03.018

Beuran, R., Chinen, K., Tan, Y., & Shinoda, Y. (2016). *Towards effective cybersecurity education and training*. https://dspace02.jaist.ac.jp/dspace/handle/10119/13769

Bhattad, P., & Patil, M. R. (2023). *Social Engineering in Cyber Security: A Comprehensive Review of Modern Threats, Challenges, and Counter Measures*. http://mahratta.org/CurrIssue/2023_November/8.%20Social%20engineering%20in%20Cyber%20security%20A%20Comprehensive%20Review%20of%20Modern%20Threats,%20Challenges,%20and%20Countermeasures-%20Prasad%20Bhattad,%20Ra

kesh%20Patil.pdf

Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. *Network Security*, *2016*(9), 5–9.

Chang, E. H., Chiew, K. L., Sze, S. N., & Tiong, W. K. (2013). Phishing Detection via Identification of Website Identity. *2013 International Conference on IT Convergence and Security (ICITCS)*, 1–4. https://doi.org/10.1109/ICITCS.2013.6717870

Chaudhuri, A. (2023). *Clone Phishing: Attacks and Defenses*. https://www.researchgate.net/profile/Ayan-Chaudhuri-2/publication/369735641_Clone_Phishing_Attacks_and_Defenses/links/6429aa76a1b72772e44625ed/Clone-Phishing-Attacks-and-Defenses.pdf

Choi, K., Lee, J., & Chun, Y. (2017). Voice phishing fraud and its modus operandi. *Security Journal*, *30*(2), 454–466. https://doi.org/10.1057/sj.2014.49

Cuchta, T., Blackwood, B., Devine, T. R., Niichel, R. J., Daniels, K. M., Lutjens, C. H., Maibach, S., & Stephenson, R. J. (2019). Human Risk Factors in Cybersecurity. *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, 87–92. https://doi.org/10.1145/3349266.3351407

Dewangan, S. K. (2015). Human Authentication Using Biometric Recognition. *Engineering Technology*, *6*(04).

Dul, M., Gugała, Ł., & Łaba, K. (2023). Protecting web applications from authentication attacks. *Advances in Web Development Journal*, *1*(1), Article 1. https://doi.org/10.5281/zenodo.10049992

FBI. (2022). *Business Email Compromise and Real Estate Wire Fraud*.

Ferguson, I. Y. (2017). *The Effectiveness of Social Engineering as a Cyber-Attacking Vector: People Do Use Unknown USB Drive, They Find*. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1205010

Foriano, L., & Jungnickel, K. (2015). *Hacking binaries/hacking hybrids: Understanding the black/white binary as a socio-technical practice*. https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/26318/ada06-hacki-fo

r-2015.pdf?sequence=1

Frenkel, S., Popper, N., Conger, K., & Sanger, D. E. (2020, July 15). A Brazen Online Attack Targets V.I.P. Twitter Users in a Bitcoin Scam. *The New York Times*. https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html

Ghani, M. A. N. U., Farooq, E., & Asghar, K. (2019). A Contextual Approach Protecting Online Privacy, A Crucial Need. *2019 International Conference on Innovative Computing (ICIC)*, 1–10. https://doi.org/10.1109/ICIC48496.2019.8966722

Griffin, S. E., & Rackley, C. C. (2008). Vishing. *Proceedings of the 5th Annual Conference on Information Security Curriculum Development*, 33–35. https://doi.org/10.1145/1456625.1456635

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 537–540. https://doi.org/10.1109/CCAA.2016.7813778

Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. John Wiley & Sons.

Hadnagy, C. J., Aharoni, M., & O'Gorman, J. (2010). Social engineering capture the flag results defcon 18. *Retrieved October*, *30*, 2010.

Hiltgen, A., Kramp, T., & Weigold, T. (2006). Secure Internet banking authentication. *IEEE Security & Privacy*, *4*(2), 21–29. https://doi.org/10.1109/MSP.2006.50

Huang, H. (2020). A Collaborative Battle in Cybersecurity? Threats and Opportunities for Taiwan. *Asia Policy*, *27*(2), 101–106.

Huddleston, T. (2019, March 27). *How this scammer used phishing emails to steal over $100 million from Google and Facebook*. CNBC. https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html

Intelligence, M. T. (2021, August 26). *Widespread credential phishing campaign abuses open redirector links*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2021/08/26/widespread-credential-phi

shing-campaign-abuses-open-redirector-links/

Kalaharsha, P., & Mehtre, B. M. (2021). *Detecting Phishing Sites—An Overview* (arXiv:2103.12739). arXiv. https://doi.org/10.48550/arXiv.2103.12739

Katz, J. (2010). *Digital signatures* (Vol. 1). Berlin: Springer.

Kandan, A. M., Kathrine, G. J., & Melvin, A. R. (2019). Network attacks and prevention techniques-a study. *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 1–6. https://ieeexplore.ieee.org/abstract/document/8869077/

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, *2019*(8), 11–14. https://doi.org/10.1016/S1361-3723(19)30085-5

KKG. (2021, December 9). *Oszuści żerują na seniorach. Wyłudzili 85 mln zł*. finanse.wp.pl. https://finanse.wp.pl/oszusci-zeruja-na-seniorach-wyludzili-85-mln-zl-6713468908448480a

Kok, S., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). Ransomware, threat and detection techniques: A review. *Int. J. Comput. Sci. Netw. Secur*, *19*(2), 136.

Komarova, A., Menshchikov, A., Negols, A., Korobeynikov, A., Gatchin, Y., & Tishukova, N. (2018). Comparison of Authentication Methods on Web Resources. In A. Abraham, S. Kovalev, V. Tarassov, V. Snasel, M. Vasileva, & A. Sukhanov (Eds.), *Proceedings of the Second International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'17)* (Vol. 679, pp. 104–113). Springer International Publishing. https://doi.org/10.1007/978-3-319-68321-8_11

Koyun, A., & Al Janabi, E. (2017). Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, *4*(6), 7533–7538.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Review: Machine learning techniques applied to cybersecurity. *International Journal of Machine*

Learning and Cybernetics, *10*(10), 2823–2836. https://doi.org/10.1007/s13042-018-00906-1

Mashtalyar, N., Ntaganzwa, U. N., Santos, T., Hakak, S., & Ray, S. (2021). Social Engineering Attacks: Recent Advances and Challenges. In A. Moallem (Ed.), *HCI for Cybersecurity, Privacy and Trust* (pp. 417–431). Springer International Publishing. https://doi.org/10.1007/978-3-030-77392-2_27

Matejkowski, D., & Szmyd, P. (2023). Online identity theft detection and prevention methods. *Advances in Web Development Journal*, *1*(1), Article 1. https://doi.org/10.5281/zenodo.10051152

Mathews, L. (2019). *Toyota Parts Supplier Hit By $37 Million Email Scam*. Forbes. https://www.forbes.com/sites/leemathews/2019/09/06/toyota-parts-supplier-hit-by-37-million-email-scam/

Microsoft. (2020, September 29). *Microsoft Digital Defense Report 2020: Cyber Threat Sophistication on the Rise*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2020/09/29/microsoft-digital-defense-report-2020-cyber-threat-sophistication-rise/

Mishra, S., & Soni, D. (2019). SMS Phishing and Mitigation Approaches. *2019 Twelfth International Conference on Contemporary Computing (IC3)*, 1–5. https://doi.org/10.1109/IC3.2019.8844920

Mishra, S., & Soni, D. (2020). Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Generation Computer Systems*, *108*, 803–815.

Moallem, A. (2021). *Understanding Cybersecurity Technologies: A Guide to Selecting the Right Cybersecurity Tools*. CRC Press. https://books.google.com/books?hl=en&lr=&id=sO5LEAAAQBAJ&oi=fnd&pg=PP1&dq=Filtering+tools+cybersecurity+McAfee+&ots=_nqVaaABTt&sig=wAJPZ74BzH1VGd92TBhC8SAibZA

Moon, J., & Chang, Y. (2016). Ransomware Analysis and Method for Minimize the Damage.

The Journal of the Convergence on Culture Technology, *2*(1), 79–85. https://doi.org/10.17703/JCCT.2016.2.1.79

Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security*, *2012*(1), 8–11. https://doi.org/10.1016/S1361-3723(12)70007-6

Parti, K. (2022). *"Elder Scam" Risk Profiles: Individual and Situational Factors of Younger and Older Age Groups' Fraud Victimization*. https://vtechworks.lib.vt.edu/handle/10919/112369

Perlroth, N., Tsang, A., & Satariano, A. (2018, November 30). Marriott Hacking Exposes Data of Up to 500 Million Guests. *The New York Times*. https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html

Policja Śląska. (2022). *Podszywając się pod dostawcę energii, wysłali ponad milion fałszywych SMS-ów*. Policja Śląska. https://slaska.policja.gov.pl/kat/informacje/wiadomosci/338196,Podszywajac-sie-pod-dostawce-energii-wyslali-ponad-milion-falszywych-SMS-ow.html

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10.

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), Article 4. https://doi.org/10.3390/fi11040089

Sandler, R. (2022). *Shark Tank Host Barbara Corcoran Loses $380,000 In Email Scam*. Forbes. https://www.forbes.com/sites/rachelsandler/2020/02/27/shark-tank-host-barbara-corcoran-loses-380000-in-email-scam/

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*, *2*(3), 173. https://doi.org/10.1007/s42979-021-00557-0

Sethi, P. (2022). Social Engineering in Cyber Security. *Jus Corpus LJ*, *3*, 1025.

Shao, J., Zhang, Q., Ren, Y., Li, X., & Lin, T. (2019). Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud.

Journal of Elder Abuse & Neglect, *31*, 1–19. https://doi.org/10.1080/08946566.2019.1625842

Simon, W. L., & Mitnick, K. D. (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley. https://extranet.blanchisserie-toulousaine-de-sante.com/sites/extranet.blanchisserie-toulousaine-de-sante.com/files/documents/justificatifs/pdf-the-art-of-deception-controlling-the-human-element-of-security-william-l-simon-steve-wozniak-kevin-d-mitnick-pdf-download-free-book-35b2e50.pdf

Stęchły, A., & Szpunar, A. (2023). Analysis of potential risks of SMS-based authentication. *Advances in Web Development Journal*, *1*(1), Article 1. https://doi.org/10.5281/zenodo.10049987

Strzałka, D. (2022). *Risks, Challenges and Opportunities—Cybersecurity in SME's. A Case Study About Poland*.

Stylios, I. C., Thanou, O., Androulidakis, I., & Zaitseva, E. (2016). A Review of Continuous Authentication Using Behavioral Biometrics. *Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference*, 72–79. https://doi.org/10.1145/2984393.2984403

Subbalakshmi, C., Pareek, P. K., & Sayal, R. (2022). A Study on Social Engineering Attacks in Cybersecurity. In H. S. Saini, R. Sayal, A. Govardhan, & R. Buyya (Eds.), *Innovations in Computer Science and Engineering* (Vol. 385, pp. 59–71). Springer Singapore. https://doi.org/10.1007/978-981-16-8987-1_7

Suriya, R., Saravanan, K., & Thangavelu, A. (2009). *An integrated approach to detect phishing mail attacks a case study* (p. 199). https://doi.org/10.1145/1626195.1626244

Syed Idrus, S. Z., Cherrier, E., Rosenberger, C., & Schwartzmann, J.-J. (2013). A Review on Authentication Methods. *Australian Journal of Basic and Applied Sciences*, *7*(5), 95–107.

Szczygieł, I., Florczak, S., & Jasiak, A. (2023). Two-factor authentication (2FA) comparison of methods and applications. *Advances in Web Development Journal*, *1*(1), Article 1.

https://doi.org/10.5281/zenodo.10050024

Thakur, G., Nayak, S., & Mangrulkar, R. S. (2022). A Comparative Analysis of Tree-Based Algorithms in Malware Detection. In *Cyber Security Threats and Challenges Facing Human Life* (pp. 99–120). Chapman and Hall/CRC. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003218555-11/comparative-analysis-tree-based-algorithms-malware-detection-govind-thakur-shreya-nayak-ram chandra-sharad-mangrulkar

Thilakarathne, N., & Samarasinghe, R. (2022). *Social Engineering Techniques and Mitigation Approaches*.

Usmonov, M. T. O. (2021). Autentification, authorization and administration. *Science and Education*, *2*(7), 233–242.

van Renesse, R. L. (1997). Paper based document security-a review. *European Conference on Security and Detection, 1997. ECOS 97.*, 75–80. https://ieeexplore.ieee.org/abstract/document/605803/

Vardalaki, A., & Vlachos, V. (2021). Emerging Malware Threats: The Case of Ransomware. In *Cybersecurity Issues in Emerging Technologies* (pp. 153–170). CRC Press. https://books.google.com/books?hl=en&lr=&id=QiRAEAAAQBAJ&oi=fnd&pg=PA153&dq=ransomware+messages++police&ots=Kytey3ompG&sig=brUil9LHq9QGewb1uTo9xmziMPQ

Vishwanath, A. (2017). Getting phished on social media. *Decision Support Systems*, *103*, 70–81.

Volodzko, D. (2018). *Marriott Breach Exposes Far More Than Just Data*. Forbes. https://www.forbes.com/sites/davidvolodzko/2018/12/04/marriott-breach-exposes-far-more-than-just-data/

Wang, C., Lin, J., Li, B., Li, Q., Wang, Q., & Zhang, X. (2019). Analyzing the Browser Security Warnings on HTTPS Errors. *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 1–6. https://doi.org/10.1109/ICC.2019.8761629

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext

social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662–674. https://doi.org/10.1002/asi.20779

Yasin, A., Fatima, R., Liu, L., Yasin, A., & Wang, J. (2019). Contemplating social engineering studies and attack scenarios: A review study. *SECURITY AND PRIVACY*, *2*(4), e73. https://doi.org/10.1002/spy2.73

Рамський, А. Ю., Венгер, В. В., Романовська, Н. І., & Чижевська, М. (2021). Behavioral Biometry as a Cyber Security Tool. *Cybersecurity Providing in Information and Telecommunication Systems*, *II*. https://elibrary.kubg.edu.ua/id/eprint/42782/