Social Engineering Attacks In The Modern Age

Austin Brightly Michael Hernandez Michael Cuebas

May 28, 2024

Abstract

Social Engineering Attacks are malicious attacks that use social techniques that aim to trick their targets into giving unauthorized access to sensitive information or objects. In modern society, while these attempts are widespread and dangerous, many individuals aren't aware of how dangerous and sophisticated attacks are becoming. It is for this purpose that this paper will cover the topic of Modern Social Engineering. It covers the current landscape of security, the life cycle and mythology of attacks, specific incidents of security breaches, and mitigation strategies for general planning. This paper takes the approach that the most effective method to maintain security is in the prevention of breaches through education. Malicious actors exploit the unaware for profit, therefore it is then most reasonable to employ the strategy of educating people in order to prevent unauthorized actions.

1 Introduction

Social engineering attacks are a continuing concern in the world as it advances and becomes more digitally interconnected. These malicious strategies aim to encourage disclosing private information or allowing unwanted access, jeopardizing both individual security and the security of society. The consequences of a successful social engineering attack can have effects on the individual level, as well as corporations, political institutions, and essential infrastructure. These attacks have the potential to cause more harm than just monetary loss or theft of personal information but can corrupt the trust of social and commercial relationships. It is important to investigate the different methods used to successfully mitigate risks to information and protect individual and group security.

Social engineering attack methods are constantly evolving. As society becomes more reliant on digital communication and information sharing, malicious attackers find new ways to exploit these connections. Some of these tactics include phishing emails that target specific individuals

or impersonation tactics used to gain unauthorized access to critical systems. These methods employed by social engineers have become more comprehensive and convincing, increasing the risk to individual security and posing a significant threat to society.

2 Existing approaches

Existing approaches to countering social engineering attacks primarily focus on raising awareness and implementing security measures. Employee training and awareness programs are common tools to combat social engineering. These programs educate individuals within organizations about various social engineering techniques, such as phishing, pretexting, and tailgating. By training employees to recognize suspicious behavior and report potential threats, organizations can create a more vigilant workforce that is less susceptible to manipulation. Security policies and procedures are also essential in combating social engineering. Clear and comprehensive policies outline how sensitive information should be handled, who has access to it, and the conditions under which it can be disclosed. By implementing access controls, authentication mechanisms, and data protection measures, organizations can establish boundaries and safeguards to minimize the risk of unauthorized data exposure. These policies, combined with ongoing employee training, form a strong defense against social engineering attacks. Beyond social engineering, security breaches can occur through common, uncommon, or innovative methods. Common security breaches often involve exploiting known software vulnerabilities or employing malware like ransomware or keyloggers. To mitigate these threats, organizations typically rely on antivirus software, firewalls, and prompt software updates to patch vulnerabilities.

3 Social Engineering in Critical Infrastructure

Social engineering poses a threat to critical infrastructure by tricking employees into providing critical information that can have a drastic impact on sectors such as healthcare, finance, and power systems. This can result in massive data breaches, power outages, and financial loss, leading to distrust in essential services. These attacks encompass a broad range of methods, including phishing, pretexting, RFID card attacks, or popup windows.

Phishing attacks are one of the most abundant attacks used by social engineers aimed towards acquiring information through false emails, phone calls, fake websites, and misleading communication to exploit employees for their confidential data. There are five different categories of phishing. These include spear phishing, which targets individuals with personal information, whale phishing, which focuses on companies, vishing, which involves phone calls and text messages, interactive voice response phishing, which manipulates voice response systems, and business email

phishing, which targets essential corporate figures.

Pretext Attacks involve the creation of pre-constructed fake scenarios to cause the victim to trust the social engineer. By manipulating the victim's emotions and often using a false representation of an authoritative figure, the exploitation of social norms can result in a lack of discretion and cause an information or data leak.

Popup windows are another social engineering tactic when attempting to compromise critical infrastructure. This tactic utilizes popups that can falsely convince the victim to provide secure information, such as login credentials, into a malicious popup or website. After the victim mistakenly provides the information, social engineers can then receive and use the data to infiltrate their intended target.

4 Foundations of Data Protection and Responsibility

Data protection and ethical concerns are basic principles underpinning the security of critical information in view of social engineering. First of all, users should get enough awareness and education followed by the employees. Since then, the training should ensure that employees live in a constant alert state directed at saving the vital data pertaining to the organization for safety purposes.

When applying a social engineering approach, it is essential to also note some of its main pillars such as data minimization and control, among others. It may be reduced for the purpose of information collection so as to avert possible future leakage that may be adverse. Authoritative access controls also allow users to have the specific information they will use at work hence minimizing its exposure outside of workplaces. Hereby, it offers an extra safeguard that ensures that the credentials are not stolen hence no access is given.

Hence, an incident response plan should be robust enough to respond swiftly because of social engineering. Ethics, legalities, authenticating user, and validating the plan. New social engineering initiatives fall foul of security audits, and there is constant monitoring. As a result, every organization needs to consider good data practice integrity and data security as the overall foundation, which will prevent social engineering attacks, and deliver the truth about honest data practices.

5 Cyber-Security Policies and Best Practices

Organizations have to implement cybersecurity policies and best practices to overcome the dangers that now take place online. Cybersecurity policy is generally well-defined and sets the overall guiding tone for all things about information security in an organization. These policies are customized for the unique risks and requirements that the organization faces in relation to security, such as data protection, access controls, incident response, and compliance.

The first good practice is putting up strong access controls. The prevention of unauthorized entry and possible violations is enhanced when you limit access to delicate data and systems to authorized people alone. It entails the deployment of robust password control methods, including multi-factor authentication. The job responsibility should also be used in determining the user access permissions. Lastly, companies need to ensure that they continually provide their employees with refresher courses on the modern risks associated with computers and internet usage security. However, such a human-centric approach is critical because most security incidents occur as a result of human error and/or negligence.

An all-encompassing incident response program constitutes a crucial component of cybersecurity best practices. It is one of the factors that contribute to the success of the company. In addition, organizations must be ready to spot, deal with, and restore normalcy after security incidents in a quick time. Developing a response team to handle incidents, utilization of advanced intrusion/threat detection equipment, and continual testing of the response plan via simulated exercises. A proactive approach to cybersecurity covers continuous monitoring of network traffic and system logs for malicious activity indicators.

Furthermore, keeping abreast of the latest software updates and patches cannot be overlooked when it comes to securing one's infrastructure. Cybercriminals target vulnerabilities in software and applications in an attempt to find and exploit security loopholes. Lastly, organizations need to view encryption as a fundamental business practice for securing confidential information even during transmission and resting.

In summary, cybersecurity policies and practices have become imperative for every company engaging in the digital realm. Through the use of a sturdy framework, fostering a conscious culture of security, and practicing effective prevention strategies, organizations could enhance the security of their system and increase their resilience against possible cyber attacks.

6 Social Engineering Life Cycle

The social engineering life cycle encompasses a series of carefully orchestrated steps that cyber attackers follow to exploit human psychology and manipulate individuals or organizations. The first phase is information gathering, where attackers collect as much data as possible about their targets. This involves scouring social media, public databases, and any available online information to build a comprehensive profile. The data collected during this stage serves as the foundation for creating convincing and personalized lures in the subsequent phases.

The second phase is "Hooking the Target, where attackers craft a message or scenario designed to manipulate the emotions or vulnerabilities of the target. This could take the form of a phishing email, a phone call, or a social media message. The goal is to establish a connection with the

target, exploiting their trust, curiosity, or fear. Attackers often use social engineering techniques to create a sense of urgency or importance, compelling the target to take the desired action without questioning the legitimacy of the request.

Once the target is hooked, the attacker moves to the ”exploitation” phase. This involves extracting the desired information, gaining unauthorized access to systems, or convincing the target to perform specific actions. The exploitation phase varies based on the attacker's objectives, which could range from stealing sensitive data and credentials to planting malware on a system. Successful exploitation marks the culmination of the social engineering life cycle, highlighting the critical need for individuals and organizations to be aware of these tactics and implement robust security measures to mitigate the risks associated with social engineering attacks.

7 The Psychology of Social Engineering

Social engineering psychology is based on the ability to understand and use people's behaviors for bad purposes. Cognitive biases as well as emotional triggers are among social engineers' weapons; they make people share confidential data or take measures compromising safety. Trust plays a significant role in this psychology. Social engineers, who make use of different avenues to form relationships with their potential victims, usually pose as known entities or create scenarios that appear legitimate. Human beings have a natural trait of trusting others. This can be used to lower guards, making it more likely for an individual to comply.

Authority is also another psychological factor involved in social engineering. Social engineers take advantage of people's tendency to trust those they see as authority figures by portraying themselves as individuals in positions of power, such as IT administrators or senior executives. Social engineers become authoritative in their approach; by so doing, they can make targets agree and follow instructions that their instincts could otherwise reject.

Also, social engineers take advantage of the “fear and urgency” reaction exhibited by people to make them part with information. Making people feel threatened like indicating that there is danger is necessary for forcing the targets to quickly put things into motion without analyzing whether what has been suggested is legitimate. When it comes to phishing emails and calls, this psychological manipulation seeks to elicit impulsive and emotional responses.

In addition to that, the principle of “reciprocity” is normally employed in social engineering attacks. By granting individuals some favor, people can unconsciously develop a sense of debt that has to be repaid. Social engineering takes advantage of this through the portrayal of either false assistance or helping entities, which forces targets to reciprocate compliance requests that undermine security.

Effective countermeasures can only be developed if one understands the psychology of social

engineering. Emphasizing these psychological tactics can provide people with security awareness training on how to recognize and refuse manipulation, thereby strengthening the human element of cyber defense.

8 The Role of Technology in Social Engineering Attacks

Social engineering is one of the most common attack types in today's technology world where technology plays a key role in providing sophisticated tools and platforms for cyber criminals to manipulate people. A major instance in this regard is the employment of sophisticated phishing techniques. Instead, cyber attackers use fake e-mails, websites, or messages that pretend to be communication in order to get people to disclose confidential information or download malware. They are able to use technology to fabricate convincing imitations of trusted entities so that users cannot differentiate between legitimate and deceptive transmissions.

With regard to reconnaissance, social engineers are now armed with a plethora of options that were developed as a result of the emergence of social media platforms. Exploitation on analyzing people's online actions, relationships, and interests gives attackers a chance to enhance the likelihood of successful social engineering. In addition, these platforms become a platform that spread untruth information, manages perception, and biased opinions and eventually result in tangible effects.

Social engineers use automation and artificial intelligence (AI) to maximize efforts and improve attack plans. Phishing emails are so convincing that they're automated; the messages are made with smartness and even change the tactics according to the response. Social engineering attacks can also be conducted by deploying Chatbots powered by AI to simulate natural conversations with targets.

In addition, malicious software is spread through social engineering with the help of technology. Malware is utilized by attackers using different delivery channels like malicious emails with attachments, compromised websites, and infected software download links or installations. This malware can then give away vital data, obtain unauthorized access, or disrupt the system. With time, technology becomes more developed and so do social engineering attacks. It is crucial to adopt a comprehensive approach to cyber security which involves addressing technology and human vulnerability aspects.

9 Mitigating Human Factors

Preventing social engineering attacks involves specialized training that recognizes different methods and tactics to help employees identify and prevent information breaches. Email filters and

multi-factor authentication enhance security and prevent phishing while educating about risks associated with sharing personal information and implementing verification procedures to prevent pretexting. Regular security briefings, updating RFID systems with encrypted data transmission, offline data backups, antivirus software, and popup blockers reduce the possibility of data breaches or information leaks.

Focusing on employee education to raise awareness about social engineering, along with implementing strict security measures, is essential for critical infrastructure. Utilizing the principles of confidentiality, integrity, and availability (CIA) is crucial to prevent distrust in essential services and support data privacy policies that prevent the exploitation of human vulnerability.

By taking a proactive approach towards social engineering, prevention methods become more successful. By integrating behavioral analytical tools and using machine learning algorithms, systems can analyze behavior patterns to detect possible information breach attempts and prevent employees or victims from receiving fraudulent and malicious attempts in the first place. With consistently updated and modified algorithms, along with continued education, there will be an increase in the successful mitigation of social engineering attacks.

10 Cross-Industry Comparisons of SE Vulnerabilities

Social engineering vulnerabilities vary across different industries. Some industries face sector-specific challenges, sometimes with terrible consequences for breaches in security. Healthcare workers can accidentally leak important documents and information, while stolen employee credentials can lead to massive breaches of data for important businesses. One such incident occurred when the Italian Prime Minister fell victim to a social engineering attack. The Minister stated that ”Meloni’s office said in a statement it regretted she had been deceived by an imposter posing as the head of the African Union Commission”.[Rey23] High-value targets such as influential figures, are typically also the most vulnerable, as seen in cases similar to Italy’s Minister. It is also important to note that targets such as government officials may contain dangerous information in the wrong hands. Not all industries are equally vulnerable, and similarly, not all industries have equal consequences for social engineering attacks.

11 Recognizing Better Solutions

One approach to fixing security issues is to fire any employees who accidentally leak information in security penetration tests. According to a man named Thor, a former employee of Blizzard Entertainment, Amazon Games Studios, and the United States Department of Energy, the director of customer service wanted to fire the employees who failed a social engineering penetration test.

”You’d fire all these people who are your best employees”...” and in 4 years you will have the same exact problem with people that are newbies right now”.[Pir23] While the director assumed the obvious solution of treating the symptoms of a social engineering attack, he failed to recognize the core issue. ”The issue is not the employees, It’s your training regiment”.[Pir23] According to Thor, the company only trained employees in their first year. This correlated with his findings that senior employees were the ones who failed in these tests. They collaborated to create a 6-month plan, and ”about a year later, did the same thing. All those people passed with flying colors”. Straightforward solutions aren’t always the best answer to social engineering attacks. Recognizing the underlying problem as this employee did, not only solves the immediate crisis but fixes the overarching threat of future security breaches due to under-education.

12 Social Engineering in the Age of Social Media

Social Media is a treasure trove for attackers, and many people document numerous things throughout their lives on publicly accessible websites. Web scrapers, hackers, and malicious individuals can all access and record this information to their own ends. What someone thought was an innocent comment could actually be the final piece of information they need to initiate a social engineering attack. Someone with the right knowledge could be phishing for account recovery information on an individual’s social media page. Furthermore, when cyber criminals get unauthorized access to accounts, they can abuse the trust those accounts have with other people. The ’social’ part of social media makes it one of the more lucrative places on the internet for malicious actors. Relationships are easily abused, the number of people in a single place is massive, and the ease of messaging makes social media particularly appealing.

13 Future Trends

When it comes to social engineering attacks, these unconventional tactics are only to be expected. Attacks have only grown ever more complex in recent times. An example of some real-world advanced vulnerability testing is documented in the lecture ”Through the Eyes of a Thief” by Deviant Ollam. He describes himself as a ”professional thief” whose job ”is to mimic and simulate and emulate attackers”.[Dev21] During a previous penetration testing job he took, his objective was to enter a building and get into secure rooms with keycard locks he wasn’t authorized for. To circumvent this he used a bio-implant to exploit the data of other’s RFID cards and entered rooms he wasn’t supposed to. Security ended up discovering him, but camera footage had shown him ’somehow’ badging in with an unqualified card. What they didn’t realize is that ”they could have searched me and I wouldn’t have another badge on me because it was in my freaking hand”.[Dev21] In this

instance the building security was unaware of the type of attack that had occurred, so they couldn't properly understand what was going on, let alone address the problem. New technologies beget new vulnerabilities, and the march of progress isn't only for the virtuous.

14 Architecture and Methodologies

In order to prevent data breaches and deter social engineering attacks, a combination of multiple strategies needs to be used. One of the many important parts of prevention is enacting plans for a quick reaction when an attack occurs. In addition to the multiple layers of security, which include special software and password encryption methods, education and training are essential for handling security threats. Regular testing is another critical component to ensure readiness and identify any potential weak points in security. Using adaptive technology and applying futuristic approaches will help further mitigate potential risks to valuable information.

15 Results and or Evaluation

Cybercrime is on the rise, and social engineering attacks are no exception. According to the FBI's Annual Report of 2022, the number of reported phishing crimes has exceeded 10x from 2018 to 2022, but also that "the public can play a crucial role by taking proactive measures to prevent and prepare for a potential cyber attack".[22] Preparation is the first line of defense, and knowledge of the tactics and weapons that cyber criminals use is of great importance when dealing with social attacks.

16 Future Trends

Advancements in technology, human behavior, and security measures all factor into the formulation of new attacks. Much of the general population doesn't fully understand the dangers of emerging social engineering attacks. One new danger in social engineering attacks is impersonation with the emergence of AI face and voice technology. AI has already been used to impersonate Russian President Vladimir Putin, Biometrics have shown themselves to be problematic with RFID systems, and AI is emerging to take things even further beyond. Based on the relatively quick advancement of Social Engineering attacks, we can project that new forms of malicious action will only continue to become harder to detect. Likely defensive measures will be rapidly produced to fight against these emerging threats as they appear. In regard to general education, as more young people grow accustomed to technology and the perils of cyber crime, knowledge of social engi-

neering attacks will become more pervasive in society. With more eyes on the problem, it is more probable that better solutions to these problems will appear.

17 Conclusion

There are a variety of ways security can be compromised in the modern age, and no approach will guarantee that security will be perfect. Even without perfection, we can still reliably reduce and contain actions taken by malicious actors. Double checking the source of the information you're examining, and not letting urgency control your pattern of thinking. Asking a third party for confirmation can also help discover unreliable and malicious actors in the act. Refraining from directly using links and information from unverified sources will help prevent scams such as malicious URL links, personal information phishing, and other forms of social deception. One of the best forms of prevention is education on these topics. Knowledge of common types of attacks helps users anticipate and recognize when they are being taken advantage of. This is why the most vulnerable are typically people who are less familiar with technology. Investigation and learning of tactics and forms of deception are critical pieces in keeping up against the progress of security attacks.

18 Future Work

Further research into which kinds of education are most effective, and analysis of real human behavior could provide additional insight into the topic of social engineering. AI detection of malicious actors is another avenue where exploration is warranted, but social issues surrounding the data gathering of AI may raise ethical questions. Ethical penetration testing methods require further development, though it is difficult to predict practical or future-proofing approaches. Some preventative measures were explored in this paper, however, as technological commutation advances, more vigorous and study security will be required to protect against attacks.

19 Related Work

Austin Brightly has contributed to specific incident research. He delved into reports such as the former Blizzard Employee, security penetration tester Deviant Ollam, Putin deep fake, and the Italian Prime Minister scandal. He also covered cross-industry comparisons of social engineering vulnerabilities, recognizing better solutions in the modern world, social engineering the age of social media, and future trends that attacks are following. He also formed relevant information in

the conclusion and formatted the references. He also contributed to the abstract, future trends, and future work sections.

Michael Cuebas contributed toward Social Engineering in Critical Infrastructure which includes different social engineering attacks and how they are implemented. The Mitigation of Human Factors was also one of the contributions that explains different preventative tactics such as multi-factor authentication systems and employee awareness. This section also serves to represent the importance of having a proactive approach rather than a reactive approach and introduces the idea of using machine learning algorithms to solve this issue. Then, he worked on the Architecture and Methodologies section and reworded sentences, fixed grammatical errors, and contributed source material.

Michael Hernandez contributed toward the foundation of data protection and responsibility in social engineering. Next, he researched the Cyber-security policies and best practices to limit social engineering. Also one of the contributions was the Social Engineering Life Cycle. Then he researched and developed the psychology of social engineering section. Lastly, he created a section that goes into detail about the role of technology in social engineering attacks. While also contributing to the overall structure, grammar, and references of the paper.

References

[Gra94] Sarah Granger. *The hacker ethic*. 1994. DOI: 10.1145/199544.199550.

[Tho04] Tim Thorneburgh. *Social Engineering, The Dark Art*. Association for Computing Machinery. 2004. URL: https://dl-acm-org.libproxy.txstate.edu/doi/10.1145/1059524.1059554.

[Eli08] Plamenka Borovska Elior Vila. *Data protection utilizing trusted platform module*. Association for Computing Machinery. 2008. URL: https://dl-acm-org.libproxy.txstate.edu/doi/10.1145/1500879.1500961.

[Gre+15] Benjamin Green et al. *The Impact of Social Engineering on Industrial Control System Security*. Association for Computing Machinery. 2015. URL: https://dl-acm-org.libproxy.txstate.edu/doi/10.1145/2808705.2808717.

[Nel+16] Jennifer Nelson et al. *Social Engineering for Security Attacks*. Association for Computing Machinery. 2016. URL: https://dl-acm-org.libproxy.txstate.edu/doi/10.1145/2955129.2955158.

[Fat18] Fabiano Dalpiaz Fatma Basak Aydemir. *Ethics-aware software engineering*. Association for Computing Machinery. 2018. URL: https://dl-acm-org.libproxy.txstate.edu/doi/10.1145/2808705.280871.

[Had18] Christopher Hadnagy. *Social engineering : the science of human hacking*. Indianapolis, IN : John Wiley & Sons, Inc., [2018]. 2018.

[19] *Email Threat Isolation*. Symantec. 2019. URL: https://docs.broadcom.com/doc/isolate-advanced-email-attacks-en.

[SK19] Fatima Salahdine and Naima Kaabouch. "Social Engineering Attacks: A Survey". In: *Future Internet* 11.4 (2019). ISSN: 1999-5903. DOI: 10.3390/fi11040089. URL: https://www.mdpi.com/1999-5903/11/4/89.

[Rai20] Tim Rains. *Cybersecurity threats, malware trends, and strategies : mitigate exploits, malware, phishing, and other social engineering attacks / Tim Rains.* 2020.

[21] *Avoiding Social Engineering and Phishing Attacks*. Cyber Security & Infrastructure Security Agency. 2021. URL: https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks.

[Dev21] DeviantOllam. *"Through the Eyes of a Thief" - LMG Basement, 2019-10-10*. Youtube. 2021. URL: https://www.youtube.com/watch?v=S9BxH8N9dqc.

[Che22] Rathnakar Achary Chetan J Shalke. *Social Engineering Attack and Scam Detection using Advanced Natural Langugae Processing Algorithm*. 2022. DOI: 10.1109/ICOEI53556.2022.9776697.

[22] *Federal Bureau of Investigation Internet Crime Report 2022*. FBI. 2022. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

[Rob22] Sean T. Lawson Robert W. Gehl. *Social engineering : how crowdmasters, phreaks, hackers, and trolls created a new form of manipulative communication*. Cambridge : The MIT Press, 2022. 2022.

[Sya+22] Wenni Syafitri et al. "Social Engineering Attacks Prevention: A Systematic Literature Review". In: *IEEE Access* 10 (2022), pp. 39325–39343. DOI: 10.1109/ACCESS.2022.3162594.

[Ada23] Rathnakar Achary Adarsh S V Nair. *Social Engineering Defender (SE.Def): Human Emotion Factor Based Classification and Defense against Social Engineering Attacks*. 2023. DOI: 10.1109/ICAIA57370.2023.10169678.

[23a] *CyberCrime*. FBI. 2023. URL: https://www.fbi.gov/investigate/cyber.

[Gro23] Juliana De Groot. *What Are Social Engineering Attacks? (Types & Definition)*. DataInsider. 2023. URL: https://www.digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack.

[Li23] Chun Li. *Building Effective Defenses Against Social Engineering*. ISACA. 2023. URL: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/building-effective-defenses-against-social-engineering.

[Lim23] Mieng Lim. *Social Engineering Attacks: Common Techniques and How to Prevent Them*. Digital Defence. 2023. URL: https://www.digitaldefense.com/blog/social-engineering-attacks-common-techniques-and-how-to-prevent-them/.

[McS23] Bernard McShea. *Active Social Engineering Defense (ASED)*. DARPA. 2023. URL: https://fieldeffect.com/blog/social-engineering-attacks.

[Pir23] PirateSoftware. *Social Engineering*. Youtube. 2023. URL: https://www.youtube.com/shorts/VAWwtjtRM98.

[Rey23] James Reynolds. *Errore mio! Italian Prime Minister Giorgia Meloni hit by Russian pranksters in 13-minute stunt to say West is 'fatigued with Ukraine war'*. Daily Mail. 2023. URL: https://www.dailymail.co.uk/news/article-12700299/Italian-Prime-Minister-Giorgia-Meloni-hit-Russian-pranksters-13-minute-stunt-released-online.html.

[SA 23] I. Sogukpinar S.A. Duman R. Hayran. *Impact Analysis and Performance Model of Social Engineering Techniques*. 2023. DOI: 10.1109/ISDFS58141.2023.10131771.

[Sal+23] R. Salama et al. *Social engineering attack types and prevention techniques- A survey*. 2023. DOI: 10.1109/CICTN57981.2023.10140957.

[Son23] Paul Sonne. *Fake Putin Speech Calling for Martial Law Aired in Russia*. The New York Times. 2023. URL: https://www.nytimes.com/2023/06/05/world/europe/putin-deep-fake-speech-hackers.html.

[23b] *Symantec® Email Security.cloud*. Broadcom. 2023. URL: https://docs.broadcom.com/doc/email-security-cloud-en.

[Yah23] Katie Yahnke. *Social engineering: Attacks, techniques, and defences*. Field Effect. 2023. URL: https://fieldeffect.com/blog/social-engineering-attacks.

[Ton] Yeming Ni Tong Li Xiaowei Wang. *Aligning social concerns with information system security: A fundamental ontology for social engineering*. DOI: 10.1016/j.is.2020.101699.