Social Engineering and Human Hacking

Y.M.L.K. BANDARA
IT23620834
IE2022- INTRODUCTION TO CYBER SECURITY
SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY,
KANDY UNI.

Abstract— Social engineering is a form of cyber-attack that goes beyond traditional hacking methods. It exploits human psychology to gain unauthorized access to sensitive information. These types of attacks are becoming more frequent and widespread across industries. Instead of targeting technical vulnerabilities, attackers manipulate individuals into revealing confidential data or performing actions that compromise security. Both individuals and organizations are vulnerable to such manipulation. This report investigates the concept of social engineering by examining its historical evolution, its modern-day applications, and its potential future developments.

The report describes how attackers have developed their tactics to include highly targeted and personalized attacks, frequently utilizing social media and real-time information, starting with early tactics like phishing, pretexting, impersonation, emails, and phone scams. To get around the new security features, these tactics are updated frequently. The study's objectives are to identify popular social engineering techniques, assess the risks they pose to people and organizations, and evaluate their efficacy using real-world examples. It also looks at how future developments (specifically the incorporation of artificial intelligence) should make these attacks harder to spot and more convincing. The report also discusses preventive measures and awareness strategies that can be implemented to reduce vulnerability and strengthen human defenses in the **cybersecurity field.**

I. INTRODUCTION

In July 2020, Twitter suffered the largest social engineering attack in recent history. [1] Hackers targeted Twitter employees with access to internal systems and tricked them into giving up their login credentials through phone-based social engineering. Once inside, the attackers took over 130 twitter accounts including high-profile Twitter accounts like Elon Musk, Bill Gates, Barak Obama, and even the accounts of world-class companies like Apple. These accounts were used to tweet a Bitcoin scam message promising to double any amount of Bitcoin sent to a given address. This incident allowed the attackers to gain possession of over $100,000 worth of Bitcoin within a few hours. It also caused great damage to Twitter's reputation and reduced public trust in Twitter. This incident clearly illustrates that Social Engineering is a type of cyber-attack that targets human behavior rather than technical vulnerabilities, and it also shows the severity and impact of these attacks, and how even tech giants can fall victim to social engineering when employees are manipulated.

In this complex digital era, when we talk about cybersecurity, it mainly focuses on strengthening firewalls, encrypting data, and repairing software vulnerabilities. But above all, human behaviors still remain as the weakest link. Attackers exploit this vulnerability to manipulate people instead of targeting a vulnerability in a system. Unlike typical cyberattacks, Social Engineering attacks do not require special skills. They are based almost entirely on psychological tactics. They do not require special software, etc., and these attacks can be launched with a simple email message or phone call.

There has been a significant increase in social engineering attacks in recent history, with high profile incidents like the Twitter bitcoin scam and deepfake voice fraud against a UK-based company among them. Social engineering attacks increased by 500% between 2020 and 2023 [2]**,** and 98% of cyberattacks in 2024 involved some form of social engineering. [3] This data clearly demonstrates the growth and risk of social engineering attacks, and why this topic is worth discussing.

Because these attacks can be launched without any special technical equipment or knowledge, todays widely used remote work, social media or information sharing applications have become a major source of social engineering attacks. As consumers knowingly or unknowingly submit their personal information and data to these applications, attackers use this information to create convincing phishing emails or impersonate trusted sources.

The main objective of this report is to explore the concept of social engineering within the field of cybersecurity. Given the growing number of social engineering attacks across various industries, understanding its mechanics is more important than ever. It focuses on how social engineering has evolved over time, how it is applied in the modern digital world, and how it may continue to develop in the future-particularly with the involvement of artificial intelligence (AI). This report aims to identify the key techniques used in these attacks, demonstrate their effectiveness through real-world examples, and assess the risks they pose to both individuals and organizations. In addition, it examines the preventive actions that can be implemented to reduce the success of such attacks, as well as strategies to enhance public awareness and education regarding this growing threat.

This report is structured into several key sections to provide a detailed and organized understanding of social engineering within the context of cybersecurity. After this introduction, the next section examines the **evolution of social engineering**, beginning with its earliest forms such as phishing, baiting, vishing, and pretexting. It describes how these techniques have developed from basic email scams to more sophisticated and targeted attacks, using data gathered from social media and other online sources. It also highlights how these methods have adapted over time to overcome improvements in digital security systems and user awareness.

The following section explores **future developments** in social engineering, with a focus on how artificial intelligence (AI), deepfake technology, and multi-platform integration are expected to increase the complexity and realism of attacks. This section also discusses the potential consequences of such advancements, including the difficulty in identifying fake content and the risks it poses to individuals, businesses, and society as a whole.

The report then concludes by summarizing the key findings and suggesting practical measures for prevention, awareness, and training. A list of **IEEE-formatted references** is included at the end to support the information presented and acknowledge all sources used.

II. EVOLUTION

Over the past decades, Social Engineering has undergone significant transformation, evolving from basic manipulation techniques into highly targeted and personalized attacks. In the beginning, attackers used simple tricks like phishing emails or phone scams to manipulate people to get their sensitive information. But nowadays, with the advancement of the technology and availability of personal data online, these attacks are becoming more convincing and personalized. Today, social engineering attacks often use real-time data, artificial intelligence, and even deep-fake technology. As technology has improved over the years, so do the techniques used by cybercriminals. Understanding how social engineering has evolved shows us how series the threat has become and why better protection is required. In the next part of the report, the major stages of this evolution will be discussed in detail. [4]

A. Early Social Engineering Techniques

In the early days of cybercrime, social engineering attacks were relevantly simple but still highly effective. One of the most common methods used was phishing. In this method, attackers send fake emails or messages pretending to be from trusted sources. (Like bank, company or website) When people click the link or open the message, they trick these people into giving their sensitive information such as credit card numbers or passwords. People really fell on these scams because back then, people weren't aware of these kinds of scams. So, they trusted their emails and didn't know how to detect fake ones.

The first recorded **phishing attack** took place in the mid-1990s by a group of hackers who targeted America Online (AOL) users**.** [5] They started sending these fake emails to AOL users by pretending to be AOL staff asking for users' login credentials to verify their accounts. Users were tricked into giving away their usernames and passwords.

Another method that was used is **Vishing** (also known as Voice Phishing). In this method, attackers use phone calls to trick people. They pretend to be trustworthy like tech support, or a bank employee, and ask for sensitive information like bank details or passwords. This method is completely based on human brain manipulation. The caller spoke confidentially and used technical terms and made people panic, so they acted quickly.

One of the major vishing attacks was the "Microsoft Tech Support" scan in the early 2000s. [6] Attackers would call people by pretending they are from Microsoft tech support. They falsely claimed that victims' computers had a virus, and they needed remote access to the computer or needed to deposit a payment to repair it. These kinds of scams ran for years, targeting thousands of people around the world.

Pretexting was also common. Here, the attacker uses a false identity or scenario to gain the trust of the victim and trick them into giving away private information. The attacker usually pretends to be like tech support, a bank employee, or even a government official.

HP scandal in 2006 can be shown as an example of the pretexting. [7] A private investigator who works for Hewlett-Packard (HP) pretended as HP board members and contacted phone companies to get their phone records.

Lastly, **Baiting** is another method that tricks people by using physical media like USB drivers or CDs. Attackers leave infected devices like CDs or USBs where people might find them. Once someone picks up and plugs it into their computer, the malware is installed itself without the person knowing it.

In the early 2000s, these kinds of baiting happened a lot. Attackers mailed CDs labeled "Free Drivers" or "Photos" to people or left them in public places. When people use the CD, their computers get infected with a virus or spyware. [8]

These early social engineering techniques laid the foundation for modern attacks. While they seem simple compared to today's AI-driven scams, they were effective at that time due to the lack of awareness and digital literacy at that time.

B. Rise of Targeted Attacks

Instead of sending messages to thousands of people, attackers started to focus on specific individuals or roles within an organization. So, they began to develop more personalized and targeted forms of social engineering. These techniques focus on gathering background information to trick victims more effectively. This new phase of social engineering introduced techniques such as Spear Phishing, Whaling, and Business Email Compromise (BEC). [9]

In **Spear Phishing**, Attacker research the target in advance usually by gathering personal or professional information from social media, company websites or leaked databases. They use this data to send realistic-looking emails designed just for them.

A well-known example happened in 2014 when Sony Pictures employees were tricked by emails that were carefully created to look like internal communication from executives, using project names, employee titles, and insider terms**.** [10] Once they opened attachment or clicked on link, the malware was installed that gave attackers access to confidential emails, unreleased movies and personal data.

Whaling is a spear phishing attack type that targets high level individuals like CEOs, CFOs or directors. The risk is high when compared to the typical phishing attacks, so attackers create emails that look convincing and urgent. These emails often related to security, financial or legal issues. [11]

In 2016, CEO of FACC, an Australian aerospace company, was fired after the company suffered a record €50 million lost due to email scam**.** [12] He received an email that looked like it came from company's chairman. The email requested an urgent fund transfer for a business deal. By the time he discovered it was a scam, most of the money was unrecoverable.

Business Email Compromise (BEC) is one of the most financially damaging forms of targeted social engineering. In BEC attacks, attackers compromise high-level company individuals like executives' email accounts and use them to send instructions to employees who are mostly in the financial department. These emails often request to transfer money to an external account. Because these emails look so real, employees trust the email and fall into the attacker's trap. [13]

One of the most famous BEC attack happened in 2013 and 2015, when a Lithuanian hacker tricked Facebook and Google into transferring over $100 million by pretending as a real Asian hardware supplier. He sent fake contracts and invoices. The emails look so real, and the two companies didn't realize they were being scammed until it was years late.

These targeted attacks marked a significant difference in social engineering. Going after high-level individuals using research and planning, rather than targeting a wide area, increased the success rate of these attacks significantly. Even though this approach requires more effort, the result is far greater reward.

C. Use of Social Media & Information Gathering

In the recent past, with the increase in use, social media has become one of the most valuable tools for social engineering. Platforms like Facebook, Instagram, Twitter, and LinkedIn are like gold mines for social engineering attackers because people share their personal and professional information without thinking twice. Details like personal information, Job titles, and locations can be easily collected and help attackers to build more convincing and personalized scams.

Attackers often begin by studying their target's online profile to understand their living situations like their habits, relationships, or communication style. This information is used to create highly convincing phishing emails, messages, or fake support calls. [14]

One of the most common platforms they use for these kinds of attacks is LinkedIn because it focuses on work and career. [15]They create fake recruiter profiles or company pages and contact employees with fake job offers. When they contact these employees, they use real job titles, employee names, and professional language, which makes them more convincing.

In 2019, attackers created fake LinkedIn profiles and sent people fake personalized job offers by pretending they were from Google or Amazon. These job offers are personalized based on their profile. The goal was to either collect personal information (such as banking details or Social Security Numbers) or trick people into downloading malicious attachments or visiting phishing websites. [16]

These tactics show how dangerous oversharing on social media can be. What seems like harmless personal content can help an attacker build a complete profile of the target and build a well-planned attack. As a result, social media has become a central part of modern social engineering, not just for delivering attacks, but for preparing.

D. Recent Trends – AI & Deepfakes

The rapid advancement in artificial intelligence (AI) and deepfake technology have significantly impacted social engineering. These technologies allow attackers to create more personalized, realistic scams that are difficult to detect. In the past, attackers manually wrote phishing emails or scam messages. Now, AI can automatically create personalized phishing emails that look very realistic.

These AI tools can scan a person's social media profiles or any available database to create messages that seem genuine. For example, AI written email might mention your recent LinkedIn post or your company's latest news, making it harder for you to doubt the email. [17]

In 2021, security researchers found that during COVID-19 using AI-generated phishing emails, attackers trick employees working from home. [18] These emails used real company details and other information (recent events) to make the message look urgent and real.

One of the most concerning developments in recent years has been the rise of deepfake technology. [19] Deepfake creates video or audio recordings using AI, that sound like or look like real people. Deepfake technology can impersonate someone's voice, face, or even body movements to create fake, yet highly convincing media. Deepfake has made social engineering even more dangerous. Attackers can create fake voicemails, video calls, or even fake messages from colleagues, CEOs, celebrities, or government officials.

Deepfake doesn't just affect businesses. It's used to spread misinformation on a large scale. Using the fake video or voice of politicians and public figures, deepfake technology can be used to spread false or misleading information, damage reputations, or influence public opinion. As deepfake continues to improve, it will become more difficult to detect, making it a powerful tool for social engineering.

UK-based CEO fraud scam in 2019 can be shown as a significant example of deepfake technology. [20] An employee received a call, what sounded exactly like his CEO's voice, urgently asking for a transfer of €220,000 to a supposed business partner. Trusting the voice, the employee transferred the money immediately to the account. Only later was it discovered that the CEO's voice had been faked using AI. This was one of the first known cases where deepfake audio was used successfully for financial fraud.

These recent trends and examples show how artificial intelligence is evolving social engineering methods to make attacks more realistic, convincing, and harder to trace. As these kinds of technologies advance, these methods will likely become more common, requiring new defense strategies to detect and counteract them effectively.

E. Summary of Evolution

Over the past few decades, social engineering has advanced from basic and simple widespread attacks to complex and targeted attacks. Early techniques like phishing attacks, vishing phone calls, or basic pretexting were successful at that time because people were less aware of social engineering or any kind of cyber risks. But with the advancement of technology, attackers adapted by shifting towards more targeted and personalized methods like spear phishing, whaling, and Business Email Corporatization (BEC). These targeted attacks often use public resources to collect detailed personal information.

The rise of social media provided even more materials for attackers to create personalized attacks. Oversharing online creates opportunities for cybercriminals to create convincing pretexts or emails while the growth of professional platforms like LinkedIn opened new pathways to recruitment scams and cooptative targeting. In recent years with the advances in artificial intelligence (AI) and deepfake technology, social engineering strategies have improved, allowing attackers to impersonate real individuals and organizations with alarming concerns.

III. FUTURE DEVELOPMENT IN SOCIAL ENGINEERING

As technology continues to advance at a rapid pace, social engineering techniques are also expected to evolve, targeted, and difficult to detect. In the future, attackers will take advantage of emerging technologies such as artificial intelligence (AI), deepfakes, and the Internet of Things (IoT) to carry out more convincing and personalized attacks. Using these technologies, attackers will automate their attacks, create personalized fake messages and even impersonate individuals through realistic fake audio or video content. [21]

In the future, the use of AI will increase significantly, and it will enable attackers to quickly gather personal information, analyze behavior patterns, and create phishing emails and scam messages with higher accuracy. Deepfake technology will allow cybercriminals to create fake video calls or voice messages that are nearly impossible to spot from genuine communication. At the same time, the increasing number of Internet of Things (IoT) devices will open new opportunities for attackers to spy on victims or trick them into giving away sensitive information.

This section explores how social engineering is expected to change in the future and what new threats may arise as technology continues to develop.

A. AI's Role in Future Social Engineering

Artificial Intelligence (AI) is expected to play a major role in the future of social engineering attacks making them faster, more personalized and harder to detect. Even today, AI tools have the capability to analyze various publicly available data sources, such as social media content, job offers, websites, and online behaviors to create highly convincing and personalized scams. The use of AI among cybercriminals will increase to automate these social engineering processes, like creating phishing emails, fake support messages, and even real-time conversations that appear to be real. [22]

AI can also create chatbots that interact with the victim through messaging apps, websites, or customer services. [23] Before trying to get the expected sensitive information such as login credentials, bank details, or security codes, these AI chatbots can carry out convincing conversations to gain the trust of the victim. As systems learn about human conversation patterns more effectively, the difference between a real person and an AI-powered scammer will become extremely hard to identify.

Emotional manipulation can be mentioned as one of the most dangerous and more effective methods behind social engineering where AI can be used to customize attacks based on the victim's emotional state. [22] For example, when someone shares content on social media that might indicate his/her emotional state, such as stressful events or financial difficulty, AI can predict that person is vulnerable; and then deliver a customized attack to exploit that vulnerability.

For example, during the COVID-19 period, many attackers used AI-generated phishing emails that appeared to come from health organizations, government agencies, or employees**.** [24] These emails were personalized with the victim's name, workplace information, and even health statistics, making them much more convincing than traditional phishing attempts.

In the future, AI-driven social engineering will deliver faster and large-scale attacks with a high success rate. Also, AI will be a powerful tool for cybercriminals because of the personalized content, emotional manipulation, and realistic conversation abilities. To defend against such threats, individuals and organizations will need to adapt new security mechanisms that detect AI-based attacks and will need to invest heavily in awareness training to recognize these attacks and resist them. [25]

B. Deepfake Advancements and Risks

The Rise of Deepfake Technology can be mentioned as another major development in the future of social engineering. Deepfake uses artificial intelligence (AI) to create fake audio, video or images that look exactly like real ones. Allowing attackers to impersonate someone's voice, face or, even body movements, which can create an entire video conversation, makes deepfake an extremely powerful tool for carrying out more convincing and dangerous attacks in the future. [26]

In the future, social engineering may include fake video meetings with the advancement of deepfake technology. For example, an attacker can set up a video call where they impersonate a trusted manager or business partner. During the call, they could ask for sensitive information, authorize money transfers, or even approve fake contracts. Since modern businesses now heavily rely on these kinds of video conferences, this type of attack can happen more in the future. [26]

A deepfake scam on a Hong Kong company in early 2024 can be shown as one of the great real-world examples of modern video conference attacks. An employee at a multinational company in Hong Kong was tricked during a live Zoom meeting, where attackers impersonated the company's CFO and other senior executives using deepfake technology. The deepfake video looked extremely real by showing faces, voices, and even body movements. An employee who believed it was a legitimate meeting, transferred $25 million to the scammer's bank account. This incident is one of the first deepfake scams using fake live video calls, not just voices. This shows how dangerous and believable this deepfake scam has become. [27]

Deepfake technology is not only targeting the business world. It's also used to spread false information, support election campaigns, or damage reputations. For these purposes, they use fake videos by impersonating politicians, celebrities, or public figures. [28] A close example of this happened in 2019, when a video of U.S. speaker Nancy Pelosi was edited to slow down, making her appear drunk while speaking. This video spread across social media platforms quickly, which misled thousands of viewers. [29]

As deepfake becomes more advanced, detecting these attacks will be more difficult. Even though new security measures are introduced to detect these attacks, cybercriminals are also improving their techniques to adapt these measures just as fast. What this growing threat indicates is that in the future people may not be able to believe what they see or hear online. Individuals and organizations must implement strong verification methods and stay aware of the risks posed by deepfake-driven social engineering. [30]

C. IoT and New Attack Vectors

The Internet of Things (IoT) is going to be another major development in the future of social engineering. The IoT refers to smart devices that connect to the internet, such as smart speakers, security cameras, smart TVs, and home appliances etc. As more people and organizations adopt these technologies, attackers are eyeing them for use in social engineering. [31]

Many IoT devices don't have strong security compared to computers or smartphones. Attackers can hack into these devices to gather sensitive information about individuals, such as their daily routines, habits, and especially personal preferences. Using this data, they can create highly personalized scams. For example, an attacker can hack into a smart speaker and learn about the victims' travel plans. And then send a fake email by pretending to be a travel agency offering a fake "Flight offer". [31]

Real-world incidents have highlighted that attackers often hack a smart doorbell camera to monitor if the house is empty, then they send fake emergency service alerts to homeowners, tricking them into giving away personal information or granting remote access to their home systems. [32]

In 2019, hackers accessed a ring camera in a child's bedroom in Mississippi, USA. The attacker used the two-way communication feature to talk to the 8-year-old girl and tried to influence her behavior by pretending to be Santa Claus. [33] Another series of incidents occurred when hackers accessed multiple doorbell cameras across the U.S. These hackers posed as police officers over the speakers, giving fake warnings. [32]

As IoT devices continue to grow, the opportunity for social engineering attacks will also increase. Future attackers might combine digital and physical tactics, using smart devices, phishing, deepfake, and psychological manipulation tricks to create attacks that are hard to detect.

The challenges of social engineering will keep evolving with advancements in technology like AI, deepfake, and IoT devices. However, defense strategies will keep pace with these changes and adapt to them in the future. Among these future defense strategies will be an AI-based detection system that can outstrip human judgment in the speed of detection of fake emails, deepfake videos, or patterns generated by AI. Big companies like Facebook, Microsoft, and Google do put a lot of money into deepfake detection technology. [34]

Apart from the technical solutions, public awareness and training will play a critical role in the future. [35] Regular awareness programs for employees and the public will be necessary to teach people how to detect these social engineering attacks and how to avoid them. Organizations also should update their security policies. For example, including multifactor authentication steps for sensitive transactions. [36]

Finally, governments around the world have started to introduce new laws and registrations to address these social engineering violations. A strong legal framework will be needed to punish these cybercriminals to protect individuals and organizations. [37]

IV. CONCLUSION

In conclusion, social engineering attacks have metamorphosed over the years in ways that are interesting, if not astounding; attacking general audiences with no intention has long ago given way to highly sophisticated methodologies directed at specific individuals and organizations. The attacks have evolved with advances in technology, methods of communication, and changed behavior of human beings. The frontal assault commenced with low-level impersonation in the form of phishing emails or telephone calls; today, it has transformed and turned in the other direction with respect to incentive precursors, psychologically prolonged attacks, and empathy-based human vulnerabilities. Active changed challenges arise from human behavioral sciences and the psychology sustaining conduct, upon which an attack is dependent, as applied to cybersecurity in situations where humans are viewed as the weakest security link. The expeditious growth of technology and the overreliance on the internet exploit these same vulnerabilities, which, in turn, create a favorable environment for social engineering to become one of the most potent strategies in modern cyber-attacks.

Traditionally, social engineering attacks drew upon broad strategies: e-mailing mass phishing campaigns or cold calling potential victims to acquire sensitive details. Although attacks made evident to the victim were becoming more difficult to perpetrate, this posed no concern for attackers, who-only venture-few-in-any forays decided to weave these into expansive-hurdle scenarios misleading the average user-victims over the past decade. The nature of these attacks changed to a more systematic approach, from targeting one or a few victims to employing people inside organizations: these were the highest targets possessing access to data of value to the company or finance. An emergence of new forms of attacks in social engineering spear phishing, whaling, and business email compromise (BEC) ushered in a new era in which cybercriminals researched the people they targeted and tailored their attacks to make them more convincing. Attackers could then put together emails and messages to match their impersonated persona streamlined through publicly available information and navigate through established security parameters.

With algorithms capable of simulating speech and sequence in human conversations, deep learning technology will allow attackers to craft AI-generated voice calls to converse with victims, hence giving a whole new dimension to social engineering attack operations. It successfully automated the processes whereby the attacker lures victims into their trap. It can analyze information on social networks, job history, and online behavior to design hyper-personalized messages that originate from a legitimate user, e.g., a colleague, friend, or trusted service provider. AI corruption activities will ultimately achieve a very high scale that will be difficult for individuals to distinguish whether the communication is authentic or fraudulent.

A deepfake technology presents some very legitimate concerns regarding the future of social engineering. Deepfake refers to the use of artificial intelligence to synthesize audio and video recording that are realistic enough to be used to mimic real. Deepfakes are becoming almost indistinguishable from real, hence represent grave threats to many human beings and organizations. Threat actors can generate deepfake videos, impersonating top executives, colleagues, or even public figures, to set up fake meetings, give announcements, etc.

V. RECOMMENDATIONS

This report has shown that social engineering will also remain a great threat in the future. Therefore, it is now only essential that both individuals and organizations take proactive measures to minimize vulnerability and build defenses for the long haul. The recommendations made are:

Individuals: [38]

- Stay informed and aware about the latest tactics in social engineering, such as phishing or AI-generated scams and deepfakes.
- Avoid posting excessive personal information on social media, which attackers can use for creating targeted scams.
- Always verify with regard to any unexpected message or call, particularly when something urgent is involved, more so if it has monetary value or sensitive information.
- Use multi-factor authentication (MFA) wherever possible to protect accounts from unauthorized access.

Organizations: [39]

- Conduct periodic training sessions for employees regarding evolving techniques of social engineering.
- For financial transactions, as well as sensitive requests, it is better to have stringent validation processes in place.
- Implement an artificial intelligence-security systems, which detect phishing as well as deepfake content.
- Keep updating IoT devices and network security configuration regularly to minimize loopholes in vulnerabilities.

Reducing the threats from social engineering attacks and the improvement of digital infrastructure in both personal and professional lives could rely mostly on these recommendations.

VI. REFERENCES

[1] TeamPassword, "TeamPassword," 2021. [Online]. Available: https://teampassword.com/blog/what-happened-during-the-twitter-spear-phishing-attack#what-information-was-compromised-in-the-july-2020-twitter-hack.

[2] Verizon, "Verizon," 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[3] PurpleSec, "PurpleSec," 2024. [Online]. Available: https://purplesec.us/resources/cybersecurity-statistics/.

[4] D. P. C, "Unmasking the Evolution of Social Engineering in Cybersecurity: Techniques, Vulnerabilities, and Countermeasures," International Journal of Engineering and Management Research, p. 6, 2024.

[5] gcohen, "Control Engineering," 2023. [Online]. Available: https://www.controleng.com/throwback-attack-the-first-phishing-attack-is-launched-on-aol/.

[6] M. Hofman, "Sans Technology Institute," 2011. [Online]. Available: https://isc.sans.edu/diary/10912.

[7] A. Clark, "The Guardian," 2006. [Online]. Available: https://www.theguardian.com/business/2006/sep/07/2.

[8] Imperva, "Imperva," 2019. [Online]. Available: https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Baiting,Scareware.

[9] M. E. A. B. A. R. Robert Larson. [Online]. Available: https://www.ieee-security.org/TC/SP2015/posters/paper_15.pdf.

[10] Anon, "Wikipedia," 2023. [Online]. Available: https://en.wikipedia.org/wiki/2014_Sony_Pictures_hack.

[11] Anon, "MYRA Security," 2025. [Online]. Available: https://www.myrasecurity.com/en/knowledge-hub/whaling/.

[12] Vignesh, "Zoho Workplace," 2023. [Online]. Available: https://www.zoho.com/workplace/articles/facc-ceo-fraud.html#:~:text=Legal%20and%20regulatory%20implications,who%20fell%20for%20the%20scam..

[13] Anon, "Preception Point," [Online]. Available: https://perception-point.io/guides/bec/business-email-compromise/.

[14] E. Woods, "use cure," [Online]. Available: https://blog.usecure.io/social-media-the-key-ingredients-for-social-engineering-attacks.

[15] J. Stathis, "Reader's Digest," 2025. [Online]. Available: https://www.rd.com/article/linkedin-scams/.

[16] S. Klappholz, "ITPro.," 2025. [Online]. Available: https://www.itpro.com/security/cyber-attacks/linkedin-social-engineering-attacks.

[17] C. Owens-Jackson, "Social engineering in the era of generative AI: Predictions for 2024," IBM, 2024. [Online]. Available: https://www.ibm.com/think/insights/social-engineering-generative-ai-2024-predictions.

[18] S. C. Ali F Al-Qahtani, "The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19," NCBI, 2022. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC9349804/#:~:text=Notable%20phishing%20attacks,and%20communication%20platforms%20%5B7%5D..

[19] B. Lenaerts-Bergmans, "What is a Deepfake Attack?," Crowd Strike, 2025. [Online]. Available: http://crowdstrike.com/en-us/cybersecurity-101/social-engineering/deepfake-attack/.

[20] Anon, "Unusual CEO Fraud via Deepfake Audio Steals US$243,000 From UK Company," Trend Micro, 2019. [Online]. Available: https://www.trendmicro.com/vinfo/mx/security/news/cyber-attacks/unusual-ceo-fraud-via-deepfake-audio-steals-us-243-000-from-u-k-company.

[21] B. Kovacs, "Cyber Mirage: How AI is Shaping the Future of Social Engineering," BISHO FOX, 2025. [Online]. Available: https://bishopfox.com/blog/cyber-mirage-deepfake-ai-social-engineering.

[22] M. James, "AI's role in future advanced social engineering attacks," Security Magazine , [Online]. Available: https://www.securitymagazine.com/articles/99989-ais-role-in-future-advanced-social-engineering-attacks.

[23] R. Lakshmanan, "Top 5 AI-Powered Social Engineering Attacks," The Hacker News, 2025. [Online]. Available: https://thehackernews.com/2025/01/top-5-ai-powered-social-engineering.html.

[24] CISA, "COVID-19 Exploited by Malicious Cyber Actors," Cybersecurity and Infrastructure Security Agency CISA, 2020. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-099a.

[25] "Defending Against AI-Driven Cyber Attacks and Advanced Social Engineering," Pro Checkup, 2024. [Online]. Available: https://www.procheckup.com/blogs/posts/2024/may/defending-against-ai-driven-cyber-attacks-and-advanced-social-engineering/.

[26] "The Rise of Deepfake Detection Technologies in 2025," DETECTING-AI.COM, 2025. [Online]. Available: https://detecting-ai.com/blog/the-rise-of-deepfake-detection-technologies-in-2025.

[27] H. C. a. K. Magramo, "Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’," CNN, 2024. [Online]. Available:

https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html.

[28] I. Group®, "Targets, Objectives, and Emerging Tactics of Political Deepfakes," Recorded Future , 2024. [Online]. Available: https://www.recordedfuture.com/research/targets-objectives-emerging-tactics-political-deepfakes.

[29] CBS, "Doctored Nancy Pelosi video highlights threat of "deepfake" tech," CBS, 2019. [Online]. Available: https://www.cbsnews.com/news/doctored-nancy-pelosi-video-highlights-threat-of-deepfake-tech-2019-05-25/.

[30] N. P. a. W. E. F. G. Bueermann, "How can we combat the worrying rise in the use of deepfakes in cybercrime?," World Economic Forum, 2013. [Online]. Available: https://www.weforum.org/stories/2023/05/how-can-we-combat-the-worrying-rise-in-deepfake-content/.

[31] S. Blanton, "IoT Security Risks: Stats and Trends to Know in 2025," Jump Cloud, 2025. [Online]. Available: https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025.

[32] M. Grigutytė, "Ring hacked: Doorbell and camera security issues," NordVPN, 2024. [Online]. Available: https://nordvpn.com/blog/ring-doorbell-hack/.

[33] E. W. a. B. Ries, "A hacker accessed a family's Ring security camera and told their 8-year-old daughter he was Santa Claus," CNN, 2019. [Online]. Available: https://edition.cnn.com/2019/12/12/tech/ring-security-camera-hacker-harassed-girl-trnd/index.html.

[34] A. Alford, "Facebook, Microsoft, and Partners Announce Deepfake Detection Challenge," InfoQ, 2019. [Online]. Available: https://www.infoq.com/news/2019/09/facebook-microsoft-deepfake/.

[35] "Social Engineering Awareness Training for Employees: The 2025 Framework," Defendify, 2025. [Online]. Available: https://www.defendify.com/blog/social-engineering-training-for-employees-the-framework/.

[36] "MFA: Your best defense against social engineering attacks," EnterSEKT, [Online]. Available: https://www.entersekt.com/resources/blog/tpost/mpckujb9p1-mfa-your-best-defense-against-social-eng.

[37] I. Atrey, "Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence," 2023. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4789133.

[38] "Ways to avoid social engineering attacks," Kaspersky, [Online]. Available: https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks.

[39] "How To Protect Your Organization From Social Engineering," 360 Advanced, 2025. [Online]. Available: https://360advanced.com/how-to-protect-your-organization-from-social-engineering/.