IE2022 – Introduction to Cyber Security

An emerging topic in cyber security

Social Engineering

Individual Assignment

Sri Lanka Institute of Information Technology

Kandy Uni

Student Name
D.D.K ELESINGHE

Table of contents

Abstract

In today's digital age there are plenty of attack types to compromise the cyber security implementations of digital devices and information systems. Among those various types of attacks there is an attack type called *social engineering attack.* This is a manipulation technique that uses the human factor as the advantage and use human psychology to gain unauthorized access to digital devices in the digital landscape nowadays. Social engineering use psychological tactics such as, trust, authority, and urgency to bypass technical security implementations and target the human element, that widely recognized as the weakest link in cybersecurity. The effectiveness of *social engineering attack* depends on its ability to manipulate behavioral patterns and exploit vulnerabilities of information systems by using deception, Persuasion and exploitation techniques. To conduct this type of attack, attackers use various techniques such as phishing, vishing, baiting and pretexting, to trick human mind to reveal their sensitive data such as passwords and etc. The results of these attack types can be severe and can lead to financial loss, data breaches, and reputational damage not only for individuals but also for large corporations. This report provides an in-depth explanation of *social engineering attacks*, evolution of this type of attack from the recent past years to now and explanation of predicted future developments in the area and a conclusion about all of the above-mentioned key points.

Introduction to the social engineering

Social engineering, in the context of information security, is the use of psychological manipulation to influence people into performing actions or reveal their confidential information [1] .Unlike traditional way of hacking, social engineering targets the weakest link in cyber security which is the human factor. In the traditional ways of hacking attackers use technical vulnerabilities but in social engineering, attackers use human behavior-leveraging trusts, fear, obligation, or curiosity to trick individuals into breaking normal security protocols [2]. Attackers usually impersonate trusted entities or create fake scenarios that look like real scenarios to trick victims, aiming to gain unauthorized access to information systems, data or financial assets [3]. This type of manipulation tactics can be carried on through various channels, including emails, phone calls, social media, or even in-person interactions. Most common types of this social engineering attacks are conducted by phishing (email or message that impersonating as trusted entity), pretexting (fake scenarios that look like real that make victims reveal their sensitive information's), baiting (Uses fake digital/physical media like USB drives loaded with malware and lure victims into grab those malwares loaded devices and plug those into to their own devices and then gain access to those victims' devices. This is done by promise of a reward or access to unique content by clouding the user's judgment, leading to harmful downloads or unauthorized access), and by tailgating (also known as piggybacking, is a physical security breach where an attacker gains access to a restricted area by following an authorized person without their permission) [4].

In social engineering, attackers' goal is to bypass technical security implementations by doing any of above activity or other social engineering attack methods. The effectiveness of those social engineering attacks depends on attacker's ability to predict the human behavior and then choose the right attack method and execute it in right time. Hence the significance of this social engineering attack depends on the total effectiveness and adaptability. Studies have shown that nearly 98 percent of cyberattacks have used some form of social engineering either as primary method or as part of the attack [5]. As mentioned earlier this social engineering methods take parts in 98 percent of cyberattacks because of the human mind is the weakest link in any security system. While well-built high functioning technical security implementations like firewalls, encryption systems and antivirus software can block many technical threats , but those technical implementations are powerless against a phone call that convincing a victim to provide their sensitive information or install malicious software to their information system that cannot block from happening [6] [7].

Attackers who use social engineering attacks are very creative and adaptive. They change their tactics, tools and methods according to the rapidly evolving technology and the victim's technological environment [8]. They are highly adaptable because they have to take advantage of new technologies, society trends and emerging vulnerabilities. Otherwise they lack behind and their tactics will not be valid to exploit current security implementations. For example, phishing is the most well-known social engineering attack method for years and also it is still the most widespread attack type and this can be done by using emails, text messages, and even social media to reach the potential victims on a large scale.

What sets social engineering attacks apart from other cyberattacks is this attack mainly focus on human psychology. Social engineers find core human psychological loopholes such as the desire to be helpful, the human instinct to trust the authority and big corporations or the human impulsiveness to act quickly in urgent situations [9] [10]. Attackers may build trust with the victim overtime by friendly interaction, also attackers will use intimidation by making threatening consequences, also attackers will use flattery compliments to victims to win favor and also, they will create a sense of scarcity or fear to take immediate actions by from the user. For instance, an attacker might act as a bank representative warning of suspicious activity by making statements like "Your account is at risk", or as a coworker requesting urgent access to a shared document. By making scenarios like this, attackers can capture the responses that would otherwise be unthinkable in only by technical context.

Consequences of successful social engineering attack can be extremely damaging not only for individuals but also for large organizations and corporations. Victims of those attacks will suffer financial loss, identity theft, or exposure of sensitive data. Organizations will face risks like data breaches , regulatory penalties, reputational damage and operational disruption [5] [7].Studies have shown in many high profile cyberattacks, social engineering has taken the first step in exploiting the information systems and it has gained access for entry point to the system for much larger and more destructing cyberattacks, such as ransomware deployments or corporate espionage.

The digital environments where social engineering attacks operates are constantly evolving. Growth of digital communication platforms-email, instant messaging, social media and remote collaboration tools-has created number of various paths to attackers to reach and manipulate their targets [7] [9]. Also, there is a huge advantage for attackers and a disadvantage to victims which is the rapid pace of evolution in the technology makes many users unaware of the latest threats or the true value of information they consume. Attackers use this lack of awareness of users, by creating sophisticated tactics to blend in with legitimate communications and bypass the detection.

Given those realities, understanding of social engineering is more important than ever. It is not only a technical issue, it is an issue that is connected with human psychology, that required some percentage of awareness, skepticism, and vigilance to counteract. Education and awareness is more important than ever because of evolution of the technology. Organizations and the social media platforms also have to motivate users to recognize common social engineering tactics and resist manipulation. There must be a culture of security inside the organizations, where users have to question unusual requests and verifying identities is not only accepted but encouraged.

In summary, social engineering plays major role in cyberattacks nowadays, exploiting the core traits that makes us human. Its success is purely depending on human psychology, daily habits, and our trust in each other's. As attackers continue to improve their techniques of conducting those social engineering attacks, the need for a basic understanding of social engineering and an effective approach to defense has never been more important. By identifying various methods and attackers' motivations behind these attacks, individuals and organizations can better protect themselves in today's highly interconnected and vulnerable world.

Evolution of the social engineering

As mentioned earlier social engineering is the art of manipulating human psychology to breach security, has evolved from deception to digital domination over past century [3]. First it was begun as simple impersonation and phone scams, it now uses advanced technologies like artificial intelligence and social media to exploit vulnerabilities at countless scales. This evolution of the social engineering section of the report will discuss its early roots to its current sophisticated forms, highlighting key technological shifts, attack methodologies, and countermeasures [7].

The term social engineering was first coined in 1894 by Dutch industrialist J.C. Van Marken, who used it to describe the need for specialists to address human challenges in organizational settings, similar to how engineers mention technical challenges [11]. However, it was not until the 1990s that social engineering became associated with cybercrime, as attackers started to use psychological manipulation tactics to conduct social engineering attacks [3]. Studies have shown impersonation and phone scams; dumpster diving and shoulder surfing were some of the early tactics used for social engineering. In the 1970s-1980s, attackers have exploited analog telephone systems ("phreaking") to make free long-distance calls or access sensitive data. This is done by impersonating as an authorized person in a corporation and attackers have manipulated victims into revealing their sensitive information or bypassing protocols [12]. Dumpster diving is done by physically obtaining the victims data by gathering discarded documents that containing passwords or personal information. In early days this was quite common tactic that was used to gather intelligence even nowadays this tactic is used to some distance [13]. Shoulder surfing means looking at the victim's digital devices while they entering PIN or passwords in public spaces provided direct access to secured systems [14]. Those methods depend on human trust and the lack of verification processes.

From 1990s to 2000s the rise of the internet and email in the 1990s transformed social engineering into a significant and scalable threat. Attackers have minimized the using of physical interaction methods that needed physical interactions with users and focused more on digital channels, gaining the advantage from novelty of early internet users. Also, phishing was used in this era. Email phishing and trojan Horses were most used phishing methods in this era. The first recorded phishing attack was occurred in 1995, targeting AOL users via fraud emails impersonating as customer support. By 2003, phishing became a mainstream tactic, with attackers targeting banks and large corporations to steal credentials [13]. The trojan horse attack method was also used back in time by including some form of social engineering. This attack was done by including malwares in email attachments that looked like invoices or job offers became an easy way for data theft [14]. Attackers have increased their usage of psychological manipulation tactics by increasing the victim's urgency and fear. For example, fake virus warnings or "account suspension" alerts have lured users into clicking malicious links [13].

From 2010s that was considered as social media era has enabled attackers to gain countless amount of personal and professional information from those social media platforms which is then used to create highly targeted and personalized social engineering attacks not only for individuals but also for organizations like spear phishing. For

instance, social media is considered like "veritable gold mine of personal information that criminals can, and do, use to personalize emails to specific recipients-a practice known as spear phishing [15] " in social engineering. LinkedIn, Twitter, Facebook has countlessly increased the amount of available information for social engineering attacks. Similarly, academic studies have confirmed that social engineering attacks have conducted heavily on social media by targeting the individuals and corporations by using data and information that they post on social media platforms like Facebook and Twitter [16]. Reconnaissance and pretexting are first steps of any cyberattack. But in social engineering those two steps play a major role. In this social media era platforms like Facebook, LinkedIn and twitter in the 2010s have given a head start for this reconnaissance and pretexting steps by providing attackers with rich datasets for personalized attacks. Those two steps are done by profiling targets from platforms like LinkedIn by harvesting details such as job titles, colleagues' names, and work history to create pretexts that look like real [17]. A 2019 study found that 65% of spear phishing attacks are using social media to create personalize messages. Multi-channel attacks also used in this social media era because of that countless information available in social media about an individual makes it easy to carry out a well-organized attack. Multi-channel attack is followed by reconnaissance because of gathering useful information from social media platforms is essential when carrying out a multichannel attack. For instance, attacker is acting as a fake CEO that email an employee about an urgent online fund transfer, and at the same time attacker will call the victim from a spoofed number to verify the fund transfer [17] . Early phishing emails were easily detected and sophistication of those attacked has evolved because attackers have learned from their previous mistakes and corrected those mistakes. Baiting also used in this era because social media made famous about gift cards, free software and exclusive content because of those concepts' attackers lured victims into download malware through counterfeit download links [13].

Then in the 2020s and beyond artificial intelligence revolution has begun. The advantages of generative ai and machine learning has increased the power of the social engineering attacks making it nearly undetectable from legitimate communications. Hyper-personalized phishing is generated with AI-generated content. Artificial engineering algorithms like ChatGPT enable attackers to create very accurate email according to the victim's personal details. Those algorithms can study the writing style of the person that attacker try to impersonate and can write exact grammatically flawless emails. In 2023, a Hong Kong finance worker transferred $25 million after receiving a deep fake video call from "CFO" [18]. Voice Cloning also considered as a big concern because of AI.Voice synthesis tools replicate voices from short audio and video samples, that convince victims into voice phishing attacks. A 2024 experiment has found that 85% of participants in the experiment cannot separate the difference between a cloned voice and the real person [18]. Automated social engineering also improved in those times. Large-scale campaigns and Deepfake propaganda are some of the famous examples for automated social engineering. Large scale campaigns are carried out by using AI algorithms to analyze social media to identify and analyze high value targets and then auto generate content according to the those targets to phishing lures [18]. Deepfake propaganda is carried out by using AI-generated videos and audio to manipulate public opinion and view of political party and also creating black mark for trust in institutions [18].

In current landscape of social engineering which means from 2024 to 2025 time period. Lot of attacks and defense strategies have evolved throughout this time period because of Artificial Intelligence and other technical developments. Today, social engineering has accounted for 98% of cyberattacks. Those social engineering attacks have accounted for losses more than $10 billion annually in United States of America alone [17]. Those modern type of attack connect both technical implementations and psychological tactics. Which make the social engineering attacks more advanced and accurate according to those hybrid tactics. There are different words use for phishing when phishing is used in sms and voice calls. When phishing is done by short text messages word smishing is used and when phishing is done by voice calls the word vishing is used. Also, phishing is used with a QR code the (quishing) is used and those fake malicious qr codes will direct users to fake login pages. Supply chain attacks are also took major place in these area by hacking a popular software and then gain access to other larger networks from the previously hacked software [18].

Not only attacks but also defense mechanisms for all of above social engineering attacks has improved with Artificial intelligence and technical implementations. Some of the defense mechanisms are AI powered while some of them are not like threat detection, Multi Factor Authentication, zero trust architecture and employee training also has to conduct at the same time. AI powered detection for social engineering attacks are done by analyzing email metadata, user behavior, network traffic to flag anomalies. The BotGRABBER framework, for example, has used random ai algorithms to detect spear phishing with 94% accuracy [14]. Multi-Factor authentication can reduce the risk of attacker gain access to an individual or organizations data by only gaining one type of sensitive information or one type of authentication [13]. Zero-Trust architecture means having literally zero trust about other users and devices enforcing strict access controls. Employee training is also playing major role in defending the cyberattacks, because studies have shown that phishing exercises and cybersecurity awareness programs reduce susceptibility by up to 60% [13].

In conclusion over the time social engineering has evolved from basic frauds to a highly technical and sophisticated level. While early attacks exploited trust in basic systems nowadays modern campaigns have used artificial intelligence and big data to exploit human psychology with technology at large scale. Because of the human element remains as the weakest link in the cyber security world attackers have shifted their focus into normal technical fixes to deeply rooted human-centric strategies. As attackers continue to innovate, the help of AI has given them a high chance of creating successful attacks at the same time for the defense AI has given rigorous education for cyber security professionals and zero trust frameworks for defending those type of attacks.

Future Developments in the Social Engineering

As we advance further into the digital era, the background of social engineering has undergo rapid transformation, with the help of Artificial intelligence this transformation has become more high paced, evolving human behavior and the high motivation of cyber criminals. Future development of social engineering can't be predicted by only depending on the past data because of the technological field is constantly evolving, with the help of AI this evolution has become higher paced, making the social engineering attack a more dynamic attack in cyber security field. This topic explores the possible and predicted development in the social engineering attack field while explaining how the integration of AI will made those attacks more advanced and shifting strategies of attackers and defenders with emergence of the technology.

When talking about the future and technology artificial intelligence is a must include technological aspect. So as mentioned above this artificial intelligence generative AI (gen AI) will play a major role in the social engineering in cyber security. AI's ability to pass vast amount of big data and generate highly convincing texts, images, videos and audios and adapt its tactics in real time will give chance to attackers to launch highly personalized and scalable campaigns. According to studies AI excels at creating believable content and quickly tailoring messages to specific demographics, making it easier to cybercriminals to create fake scenarios and lies that looked like real scenarios and this will lure victims into huge amount of traps that are mentioned in social engineering. This scalability is now not limited to only one individual attacker, those attacks now can be automated and deployed on an industrial scale. [19] [20] [21].

Generative AI can do more than text phishing. Deepfake technology, which generates audio and video contents that looks and sounds real, is also used in social engineering scams. They can also impersonate executives, colleagues, or even members of your family. Detecting those kinds of highly accurate attacks becomes nearly impossible. Deepfake voice calls recently become interest of corporate employees for a fraudulent transaction authorization. This AI trend is expected to peak and improve more because of given the low costs and easy accessibility of the technology [21] [22] [23]. Nowadays in social media it is very hard to detect fake personas. These countless fake personas also have created this problem much worse. Attackers use this AI algorithms as an advantage and as a strong base for an attack while making trust with the victims' overtime from using these fake personas [24] [21].

AI also enables the automation of social engineering campaigns. Those autonomous agents can conduct reconnaissance, profile targets, and initiate contact with the target without a physical interaction with the target. These agents can analyze public data from social media, websites, and other various open sources in digital landscapes. This allow attackers have their hands on well-organized and detailed document on potential victims allowing highly targeted and contextually aware attacks. The result is a new era of social engineering where the capabilities of human and the technology is clearly divided in unprecedented levels [23] [24] .

Immersive technologies, including virtual reality (VR), augmented reality (AR), and wearable devices, are making the way into revolutionize practices of social engineering. The more these technologies become used in everyday life, the newer ways attackers will find to manipulate and directly interact with their targets. For an example, VR environments could create nearly realistic real-world scenarios, such as virtual meetings or training sessions, in which users might be more susceptible to letting their guard down. The improved quality of such environments may allow attackers to gain trust, replicate authority, or create a sense of urgency that convince victims fall into those traps [19].

Also new portable devices such as smart glasses, fitness trackers, and health monitors are being analyzed very much according to social engineer criteria. They are valuable because of sensitive personal information that they carry and connects individual to other digital services so that it becomes a target for intrusion. Trend Micro adds nowadays, as new devices have entered the market, cybercriminals are expanding without a effort and the attack surface has provided attackers more chances to damage exploitation of human vulnerabilities. For example, it could send attachment with malicious packaged notifications through the compromised wearable device or indeed tamper with the health information collected, or even digitally replace the wearer when impersonation was needed in some scenarios [19].

The integration of AI with highly advanced technologies further expand the risk. Because of technologies like AI powered chatbots, and AI powered virtual assistants can be programmed to engage users in natural way that create trust with users overtime before sending a malicious payload. As these technologies become more sophisticated, the potential for large scale, automated social engineering campaigns will grow, while making it much harder to cyber security professionals to create defending strategies for those type of attacks [19] [24].

Future social engineering attacks will not only be conducted through phishing emails and fake phone calls, it will also spread into other types of attacks. The deepfake technology will play a big role in enabling an fake persona to develop highly accurate audio and video from any trusted persons and use them into compelling narratives. For instance, a company executive can use a deepfake video to instruct all "employees" to transfer money or release sensitive information. Usage of deepfakes in social engineering is not only for corporate environments, but can also be used in political disinformation campaigns, financial fraud, or even personal blackmails [23] [22].

These types of attacks are increasingly emerging as AI is integrated, multi-channel-attacks targeting male and female victims across all platforms of communication with email, SMS (smishing), voice (vishing), and social media. The communication becomes more difficult for potential victims to assess whether this is the real authorized person or some attacker who used to impersonate the real authorized person when such multiple media are combined. It leads to an increase in possibilities of success for an attack. For instance, a phishing email could be sent, followed by a spoofed phone call, and finally, a deepfake video that would further reinforce the deception.

Everything appeals to the cognitive errors and emotional hooks upon which social engineering is based and makes an individual resist to manipulate [22] [24].

Doppelganger websites impersonate legitimate sites to gain personal and sensitive information of users. Another method of SIM swapping has become normal in which an attacker reroutes a victim's phone number to intercept the authentication code. Social engineering attacks will improve by combining the two partnered technologies which are AI and deepfake, making it more convincing, much more scalable, and awfully difficult to prevent [19] [24].

Using AI integrated with newest technologies, attackers have found that defenders have used AI themselves to identify, detect, and respond to social engineering threats. AI-based controls will analyze the patterns of communication, detect patterns in user behavior, as well as detecting real-time suspicious activity. An example of working the machine learning algorithms is identifying phishing emails based on patterns in language, sender information, or even embedded links-inserted, even though the content is highly personalized. The same goes for the AI detecting deepfake content subtle mismatches in audio, video, or text [24] .

But the application efficiency of the artificial intelligence for defense is not a matter of certainty. "AI will give social engineering wings," Kevin Tian, CEO of Doppel, says, meaning that AI will augment detection capabilities and thus not make detection flawless. Social engineering is dynamic and as adjusted as the ingenuity of the attacker; hence they will only keep coming up with new ways to bypass defenses, however sophisticated. The challenge, in an organization's capacity, would be to try to stay ahead all the time, constantly upgrading its security measures and training employees to recognize and resist threats that evolve continuously[19] [24].

Despite advanced technology, humans remain the weakest link in social engineering. Manipulating human interaction involves the attacker playing on psychological and emotional variables such as trust, fear, curiosity, or authority bias. The more easily these lies can be convincingly molded by technology and perpetrated against large numbers of victims, the more vitally important human vigilance and awareness will become [24].

The teaching programs regarding awareness on how to avoid social engineering risks will keep rolling. An organization needs to invest in complete cybersecurity education to teach the workers to identify signs of manipulation in a unique request and to let them learn to validate any soliciting made on the other side. Employee enriched in practice towards simulated phishing exercise will develop abilities and skills instinctive to resist social engineering tactics. [24]

Questioning the unexpected and verifying its authenticity must be the bedrock on which a culture is built. The employees must be encouraged to question the legitimacy of any communication that falls in the unexpected category, particularly when those calls are for sensitive information or some urgent action on their part. By ensuring

a technologically defensive approach along with a well-built human engagement, organizations may fortify themselves against attacks employing social engineering [24].

And since AI and deepfakes are becoming more prevalent in social engineering attacks, these technologies tend to compromise trustworthiness in digital communications, confidence in institutions, and ultimately lead to the destabilization of social and political systems in far-meaning ways. The psychological and emotional impacts of a successful attack-stress, anxiety, and reputational damage can be rather serious-and will be felt at the level of the attacked individual and organization and at the level of society [22] [21].

The sophistication of social engineering will find its way into the making of laws, regulations, and standards for the industries involved. Governments and regulatory bodies may confront new demand phases for greater authentication, transparency, and accountability pertaining to digital communication. Organizations must adopt a proactive, multilayered approach that encompasses the technical, organizational, and human aspects to prevent the emergence of new challenges [24].

In summary the interplay between technological innovation, human psychology, and the ever-evolving strategy of the attackers and defenders shapes the future of social engineering. AI, immersive technologies, and new attack vectors are redefining the threat landscape, making S.E. more persuasive, scalable and difficult to detect. While technological solutions are indispensable, the human element constitutes the path of weakness and the first bastion of defense; hence, with constant awareness, diligence, and proactivity, persons and organizations can prepare for holistically treading through this next threat wave of social engineering, thereby emerging victorious with their digital futures.

Conclusion

Historical investigations into the evolution of social engineering have explored the idea's of current manifestations and examined possible and predicted future developments that will shape the cybersecurity landscape in the years ahead.

The first forms of social engineering capitalized on the same fundamental traits that have always characterized mankind-trust, curiosity, and authority. In the absence of the digital age, culprits engaged in activities like impersonation, pretexting, and even dumpster diving to query the outflow of unauthorized information and systems. As email communications proliferated and with the introduction of the Internet, all these.

Email phishing, spear-phishing, and using social media as recon were widely used," as they bypassed geography and gave attackers a worldwide reach with minimum efforts. The 2010s were more important as social networks such as Facebook, LinkedIn, and Twitter opened up the very private access to both personal and professional data, paving the way for very targeted attacks that could be crafted around the deep knowledge of the social networks of victims, as well as their behaviors and preferences.

The primary social and technological trends that define the future of social engineering will all converge. AI will continue to enhance both offensive and defensive measures within social engineering. All sorts of scenarios will see attackers leveraging AI for automating reconnaissance, crafting super-personalized lures, and practical deepfakes barely distinguishable from real ones. Flashing the other side of the coin, defenders will leverage AI anywhere capable for anomaly detection, suspicious communication tagging, and identification of synthetic media. However, the arms race is likely to speed up between both parties, as they will constantly adapt toward the new changes the other side throws into the spin.

Immersive technologies such as VR, AR, and wearables are new frontiers that open up for social engineering. They'll not only spread attack surfaces, but set up brand-new psychological manipulation vectors. VR immersion may serve to establish trust or create a sense of urgency by the attacker, and bearing-usability on compromised wearables to manipulate health data or impersonate users during digital interactions.

Human factors notwithstanding, these technologies represent a prime angle of the social-engineering world. The major psychological triggers-Trust, Fear, Urgency, and Authority Bias-continue to be the mechanisms for social engineering attacks.

Even with all the technological advances these days, the most critical vulnerability remains the human element. Social engineering attacks continue to use intrinsic psychological triggers- trust, fear, urgency, and authority bias. With technology making it all the easier to create believable untruths and scale them to targets, human vigilance and

awareness become even more important. Extensive education and awareness initiatives, within a culture of skepticism and verification, have been essential to successfully mitigating these risks further.

Social engineering is far more than cybersecurity-deficient. With the rampant use of AI and deepfake technologies, it has a lot to do with social engineering campaigns undermining the degree of trust that communications may have among people in the digital space, leading people to lose faith in institutions and even the social and political systems. Successful attacks can have psychological and emotional consequences-stress, anxiety, and damage to reputation at all levels, as individuals, organizations, and society as a whole-much more than just financial.

Future Research Directions

Rapid changes in social engineering indicate that there are a number of areas that need to be looked at in future research.

AI-Supported Detection and Prevention: Research and development of AI-based detection and prevention tools for social engineering attacks in terms of deepfakes and other synthetic media must continue.

Human Factors and Behavioral Sciences: Additional studies into the cognition and emotions that predispose individuals to manipulations should be conducted to build effective training and awareness programs.

Policy and Regulation: As social engineering techniques evolve, so do laws and regulations. New research on the effectiveness of the existing policies toward devising novel standards on authentication, transparency, and accountability becomes a prerequisite.

Impact Assessment: Studies that examine the impact of social engineering attacks, including the societal, economic, and psychological dimensions, will complement defense strategies with holistic thinking.

To conclude, social engineering will be a permanent source of contention in this digital age. Such knowledge synthesis will require technology, psychology, and policy insights and investment in technical improvements as well as human-centered ones to better prepare society for future onslaughts of social engineering attacks.

References

[1] Wikipedia Contributors, "Wikipedia," 17 April 2025. [Online]. Available: https://en.wikipedia.org/wiki/Social_engineering_(security). [Accessed 1 May 2025].

[2] IBM, "What is social engineering," IBM, 15 April 2025. [Online]. Available: https://www.ibm.com/think/topics/social-engineering. [Accessed 1 May 2025].

[3] proofpoint, "What is social engineering? definition, types & more," Proofpoint, 2 December 2024. [Online]. Available: https://www.proofpoint.com/us/threat-reference/social-engineering. [Accessed 1 May 2025].

[4] Kelly Hammons, "LinkedIn," LinkedIn, 28 July 2024. [Online]. Available: https://www.linkedin.com/pulse/understanding-social-engineering-how-cybercriminals-human-hammons-pastc/. [Accessed 1 May 2025].

[5] Okta, "Okta," Okta, [Online]. Available: https://quillbot.com/citation-generator/folders/Bu5dhymqNFZaAmFXVvcyK/lists/cMsHRYyJvvAnS5F3GGo0c/sources/20y3HrBx19M6iwrbd1AKwj. [Accessed 25 April 2025].

[6] S. Yerushalmi, "Imperva," A Thales company, 20 December 2023. [Online]. Available: https://www.imperva.com/learn/application-security/social-engineering-attack/. [Accessed 28 April 2025].

[7] "Kaspersky," Kaspersky, 26 August 2020. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering. [Accessed 26 April 2025].

[8] TLP WHITE. (n.d.)., "Public intelligence.net," [Online]. Available: https://info.publicintelligence.net/UK-CERT-SocialEngineering.pdf. [Accessed 20 April 2025].

[9] D. Bloxberg, "eLearning," VIPRE, 19 November 2024. [Online]. Available: https://inspiredelearning.com/blog/how-social-engineering-attacks-exploit-data/. [Accessed 1 May 2025].

[10] cyberark, "cyberark," The identity security company, 2 August 2024. [Online]. Available: https://www.cyberark.com/what-is/social-engineering/. [Accessed 1 May 2025].

[11] wikipedia contributors, "Wikipedia," 27 February 2025. [Online]. Available: https://chatgpt.com/c/6812873d-1338-800d-8f89-d12f5988e776. [Accessed 28 April 2025].

[12] Indiana cybersecurity hub, "Indiana Cybersecurity Hub," 1 April 2024. [Online]. Available: https://www.in.gov/cybersecurity/blog/posts/social-engineering-how-its-evolved-and-how-to-avoid-it/. [Accessed 2 May 2025].

[13] vandanapublications, "vandanapublications," 2024. [Online]. Available: https://ijemr.vandanapublications.com/index.php/j/article/view/1513. [Accessed 28 April 2025].

[14] Bokhonko, O; Lysenko, S; Gaj, P Khmelnitsky National University, & Silesian University of Technology., "ceus-wr.org. Development of the social engineering attackk models.," 2024. [Online]. Available: https://ceur-ws.org/Vol-3899/paper26.pdf. [Accessed 1 May 2025].

[15] T. h. o. p. attacks, "cofense.com," cofense, [Online]. Available: https://cofense.com/knowledge-center/history-of-phishing/.

[16] T. M. Alotayan, "Awareness of Social Engineering Attacks and their Relation to the Ability to Persuade among users of Social Networking Sites," *Journal of echohumanism,* Vols. 3, No:7pp. 2580 – 2592, no. ISSN 2752-6801, p. 13, 2024.

[17] Fortra, "How Is the Digital Age Redefining Social Engineering's Playbook?," Fortra, 6 Novemebr 2023. [Online]. Available: https://www.terranovasecurity.com/blog/what-has-changed-in-social-engineering. [Accessed 26 April 2025].

[18] M. Samala, "Lumen," Lumen web page, 2019 December 2024. [Online]. Available: https://blog.lumen.com/the-evolution-of-social-engineering-and-phishing-in-the-age-of-artificial-intelligence/. [Accessed 2 May 2025].

[19] "trendmicro," trendmicro, 2025. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-future-of-social-engineering.

[20] KBI media, "KBI media," Independent Cyber News, 2025. [Online]. Available: https://kbi.media/press-release/tesserents-cyber-security-predictions-for-2025-rise-of-social-engineering-cyber-attacks-fueled-by-ai-and-more-attacks-on-critical-infrastructure/. [Accessed 25 April 2025].

[21] M. James, "AI's role in future advanced social engineering attacks," Security magazine.com, 09 October 2023. [Online]. Available: https://www.securitymagazine.com/articles/99989-ais-role-in-future-advanced-social-engineering-attacks. [Accessed 2 May 2025].

[22] K. Roer, M. Adjei, N. David, M. Aalto and P. Schaffer, "Security Week," securityweek.com, [Online]. Available: https://www.securityweek.com/cyber-insights-2025-social-engineering-gets-ai-wings/. [Accessed 26 April 2025].

[23] "Confronting social engineering in the age of artificial intelligence," Hogen Lovells, 19 February 2025. [Online]. Available: https://www.hoganlovells.com/en/publications/confronting-social-engineering-in-the-age-of-artificial-intelligence. [Accessed 28 April 2025].

[24] A. Pillal, "The Perfect Storm: How AI is Revolutionizing Social Engineering Attacks in 2025," Network Intelligence Digital Security Company, January 2025. [Online]. Available:

https://www.networkintelligence.ai/blogs/the-perfect-storm-how-ai-is-revolutionizing-social-engineering-attacks-in-2025/. [Accessed 24 April 2025].