Proceedings of the 5th International Conference on Smart Systems and Inventive Technology (ICSSIT 2023)
IEEE Xplore Part Number: CFP23P17-ART; ISBN: 978-1-6654-7467-2

2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) | 978-1-6654-7467-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSSIT55814.2023.10061054

Comprehensive Assessment of Reverse Social Engineering to Understand Social Engineering Attacks

Ayush Bishnoi
Faculty of Computer Applications,
Manav Rachna International Institute of Research & Studies, Faridabad
vishnoiayush3@gmail.com

Garv
Faculty of Computer Applications,
Manav Rachna International Institute of Research & Studies, Faridabad
bhadu.garv@gmail.com

Sagar Bishnoi
Faculty of Computer Applications,
Manav Rachna International Institute of Research & Studies, Faridabad
bishnoisagar26@gmail.com

Neha Gupta
Faculty of Computer Applications,
Manav Rachna International Institute of Research & Studies, Faridabad
neha.fca@mriu.edu.in

Abstract:
This paper gives a systematic analysis of social engineering attacks, including their categorizations, methods of detection, and strategies for mitigating them. Digital technology has recently advanced, making human-to-human contact easier and faster than before. However, without the proper safeguards, social media platforms and internet services could reveal confidential and sensitive information. Malicious actors can easily access communication networks by employing social engineering techniques. Hackers use social engineering to obtain sensitive data from victims, such as bank account details, passwords, and medical histories, for their own gain. Social engineering poses a serious threat to network security because it preys on people's innate tendency toward trust. The paper carefully assesses reverse social engineering (RSE) and its impact on social engineering attacks.

Keywords: Social Engineering Attacks, Cyber Security, Phishing, Vishing, Scams, Spear phishing, Baiting.

1. INTRODUCTION

The phrase "social engineering" is used to describe a wide range of manipulative acts carried out via the manipulation of social relationships. It uses deceptive tactics to persuade people to breach security or divulge sensitive information. Attacks using social engineering may have several stages. A fraudster will investigate their intended victim to learn the specifics of the attack, such as entry points and security flaws. After winning the victim's trust, the attacker will use that rapport to convince the victim to violate security best practices such as revealing confidential data or granting access to necessary resources. And lastly, hackers frequently target novice users. Many customers and employees are unprepared for risks like drive-by downloads as a result of the rapid growth of technology. Users could discount the significance of data like their phone number. Many people are unaware of how to protect their data and themselves. [2]

II. LITERATURE REVIEW

The work of several researchers in the subject of social engineering is summarised in Table 1.

TABLE 1: Comparative Study of Social Engineering attacks by various authors

Author Name & Year	Title of the Paper	Methodology Adopted	Limitations
M. Hijji, G. Alam & 2021 [1]	A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pan- demic: Challenges and prospective solutions	Findings and professional viewpoints are combined in MLR.	Explanation flaws include the lack of a consultant's viewpoint on resource selection and a thorough explanation of the study findings.
J.W. Bullee, M. Junger & 2020 [2]	How effective are social engineering interventions? A meta-analysis	Analysed innovative strategies developed to lessen the susceptibility to social engineering assaults	More stringent study standards prevented the solution from being detected, which meant that the inquiry's goals were not properly attained.
P. Schaab, K. Beckers, S.	Social engineering	Reflects the viewpoints of	restricted to social

Pape & 2017 [3]	defence mechanisms and counteracting training strategies	social psychologists and data security professionals.	psychology-based defence
A. Yasin, R. Fatima, L. Liu, A. Yasin, J. Wang & 2019 [4]	Contemplating social engineering studies and attack scenarios: A review study	Merge numerous ideas to describe the execution of social engineering assault actions.	failed not outline the precautions that consumers should take to protect themselves from the many assaults and persuasion methods utilised by social engineering attacks.
F. Salahdine, N. Kaabouch & 2019 [5]	Social engineering attacks: A survey	Reviewed social engineering in four main areas: assaults, categorization, detecting techniques, and preventative methods.	didn't offer any technological or human-centered assault avoidance methods.
Z. Wang, L. Sun, H. Zhu & 2020 [6]	Defining social engineering in cybersecurity	To contrast the various theories now in use, benefits and drawbacks data is presented.	ignored the current methods of preventing social engineering attempts
Z. Wang, H. Zhu, L. Sun & 2021 [7]	Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods	Only emphasises the process of action and people's susceptibility to social engineering assaults, which are demonstrated via 16 situations.	didn't go over how to stop social engineering attacks, which is known to work
M. Fujikawa, M. Nishigaki & 2011 [8]	A Study of Prevention for Social Engineering Attacks using Real/Fake Organization's Uniforms	This is a pattern detection method that could be used to recognise objects, register them, and rebuild their three-dimensional (3D) shapes. This method was employed to evaluate the similarity among trustworthy and dubious sites.	The surfing procedure has lower resolution and a higher likelihood of incorrect matched points.
Monique Bezuidenhout & 2010 [9]	SEADM (social engineering attack detection model)	By dividing the task into easier to handle parts and providing rules for decision-making, this approach is based on decision trees. They characterise the person's inner feelings when he makes a choice during the social engineering assault procedure in here.	There is little understanding of this assault type. entirely rely on mental decision-making
Francois Mouton & 2014 [10]	Ontological model to detect social engineering attack	Inside this concept, we discuss an exploit structure, including how assailant reaches users with ease and the steps they must take. That model's approach is based upon Kevin Mitnic's loop of social engineering attacks.	Although this approach does not really guarantee cybersecurity, it does show us where to protect our material.
Zang etal 2007 [11]	Phinding phish: Evaluating anti-phishing tools	If those technologies were mainly precise in detecting malicious urls, users would still choose to disregard their warnings	Lack of understanding (many users are unable to comprehend that sort of warning)
Badra, Sawda, & Hajjeh, 2010 [12]	Phishing Attacks and Solutions	In order to disguise our identity, we employed steganalysis methods. The passcode shouldn't be too basic. According to this concept, the security flaw might be a picture used to identify the person throughout the authenticator.	No suitable construction is advised in social engineering regarding online security.

III. EXECUTING SOCIAL ENGINEERING ATTACKS

Interventions in social engineering can take many different shapes. In a typical social engineering effort, target research and reconnaissance come first.

For instance, if the target is a firm, the invader may learn about the organization's strategy, internal processes, lingo used in business, and potential business relationships [13]. As social engineers can monitor internet accounts for important information and analyse both virtual and actual behaviours, armed police officers and receptionists are desirable targets. With this knowledge in hand, the social engineer may plan an attack that takes advantage of the weak spots discovered during reconnaissance. In contrast, a hacker who uses an exploit can access secured systems or networks, steal personal data like Social Security numbers and bank account information, or profit from the victims.

IV. TYPES OF SOCIAL ENGINEERING ATTACKS

S.No	Social Engineering Technique	Explanation
1	Baiting	With a malware-infected USB flash drive, the attacker hides the "bait." The victim unwittingly instals the malware by connecting the device.
2	Phishing	Malicious actor attempts to steal information from a target by sending them an email that seems legitimate. Recipient may clicks on a link in an email & may install malicious software or reveal personal information.
3	Advanced Spear Phishing	It is quite similar to conventional phishing attempts, with the exception that it targets a specific people or organisation.
4	Voice phishing (or "vishing")	It is a kind of social engineering in which sensitive information such as a person's bank account number or Social Security number is extracted through telephone from an unwitting victim.
5	Whaling	Refers to a kind of phishing assault that especially targets high-profile persons, such as the chief financial officer or the chief executive officer, in an effort to get sensitive information.
6	Pretexting	It is possible to employ deception to gain access to private information. For instance, in a pretexting scam, the perpetrator poses as someone who is verifying the victim's identification and asks for private information under the guise of needing it to complete the verification process.
7	Scareware	It is a cyberattack in which the victim believes they have downloaded malware or unlawful content. The attacker claims to resolve a non-existent problem for the victim and pushes malware download.
8	Watering Hole	An attacker compromises a subset of users by infecting prominent, trustworthy websites they often visit.
9	Theft via diversion	When a delivery or courier business delivers a criminal to the wrong destination.
10	You may ask, "What's in it for me?"	This is a kind of social engineering in which the attacker provides a bribe in return for the victim's participation. A hacker may, for example, act as a technical support representative and phone a series of unconnected lines inside an organisation in an effort to address a problem. Over time, the hacker will discover a victim with a valid technical problem and pretend as a helper in an effort to resolve it. The hacker might use this communication to infect the victim with malware or collect information.
11	Honey Trap	The victim believes they've downloaded harmful software or unlawful content. The attacker encourages malware download by promising to fix the victim's fictitious problem.
12	Tailgating	An intruder uses a legitimate access card to enter a restricted location. The victim assumes an authorised user will hold the door open for them. This assumes they can join us.
13	Wrong Malicious Software	Malicious security software is a form of malware that induces users to purchase bogus protection against malware.
14	Dumpster Diving	Social engineering involves forcing people to trash dive. Individuals explore a company's garbage can for sensitive information, such as scribbled passwords and access codes. Employees may use these codes to access the internal network.
15	Pharming	A hacker installs malicious software on a server and leads the victim to a fake website. User may be misled into giving important information. [2]

V. REVERSE SOCIAL ENGINEERING:

Reverse social engineering is a common type of social engineering attack in which the victim is duped into giving the attacker access to their network system or personal data about them. They can only be stopped by highly developed security measures and trained security personnel [14]. Consider what would happen if you clicked on a phishing link that a hacker sent you in order to contact you and then installed malware on your computer. By emailing you in the guise of an officer, a hacker may try to persuade you that he can fix your device's issues for a reasonable price or even for free. Hackers create a back entry while simultaneously repairing any defects or flaws in your system after they have obtained access. This is done in order to track your online activity and steal sensitive information. In some cases, the perpetrator will trick the target into coming to you rather than making eye contact with their victim. The outcome of this would be greater confidence [15].

There is less cause to doubt the victim's genuineness if they did attempt to contact the offender. It gives the trespasser a more reliable appearance.

VI. REASONS FOR RSE:

a. Absence of safety training:

Overall majority of firms establish fundamental safety rules that include recommended practises including keeping credentials, identities, payment details, and certain other confidential material private. Unfortunately, not every worker is essential such regulations are and what happens if they are not

followed. Staff can expose firms to reverse social engineering and certain other assaults if they lack basic safety understanding.

b. Humans flaws:

There are several reasons why a person reveals personal data. Those human flaws can expertly easily program, resulting in anticipated to exceed social engineering assaults. Unfortunately, concern about hacking is another one of those weaknesses. Some technical support con artists claim that their customers have already been attacked before offering to remedy the issue.

c. Unproven policies & processes:

Unfortunately, not every company tests all of its applications, nor does it do so frequently. A further way businesses put oneself at danger of a reverse social engineering assault is by developing strong encryption and neglecting to practice regularly.

VII. Extraordinary Techniques of Social Engineering

Malware assaults are prevalent and may have far-reaching consequences; hence, they need careful study. Malware authors may use social engineering to entice naive users to open harmful files or visit dangerous websites. Numerous varieties of malware, such as email worms, use similar methods. Without a comprehensive security package for your mobile and desktop devices, you are susceptible to infection.

a. Problems with worms

To convince the user to click on the infected link or download the harmful file, the cybercriminal will attempt to capture their interest.

Several examples of this kind of attack are shown below:

1. As the year 2000 drew to a conclusion, many organisations' email systems were still infected by the LoveLetter worm. The victims got an email with an attached love note. When a victim opened the attachment, the worm created a duplicate of it and transmitted it to everyone in their contact book. Despite its extinction, this worm is still regarded as one of the most financially devastating.

2. The Mydoom email worm initially surfaced online in January of 2004, and propagated through messages that purported to originate from the mail server's technical assistance department.

3. The Swen worm purported to be a communication from Microsoft. It was said that the included patch will solve known Windows bugs. It's hardly surprising that many individuals trusted the story and attempted
to install the phoney security patch, which turned out to be a worm.

4. Hackers Link Distribution Channels: Email, ICQ, and other IM systems, as well as IRC Internet chat rooms, may be used to provide links to malicious websites. SMS messages play a major role in the widespread distribution of mobile infections.

Regardless of the channel, the message will often include exciting or attention-grabbing wording to entice the naïve user to click on the link. Using this kind of infection, dangerous software is able to circumvent the anti-virus defences of the mail server.

5. Peer-to-Peer (P2P) Network: Sometimes,P2P networks are used to propagate malware. The P2P system will be compromised by a worm or Trojan virus. The file will be labelled in a way that attracts people's attention and encourages them to download and run it. The following are some of the example:
The AIM and AOL Password Hacker.exe, Microsoft CD Key Generator.exe, PornStar3D.exe, PlayStation emulator crack.exe

To limit the possibility of infected persons exposing their infection, malware authors and distributors have access to a variety of techniques.

- Victims may behave in a number of ways when presented with a bogus promise of a free utility or guidance to illicit advantages.
- Free usage of the Internet and mobile phone services.
- A chance to obtain a generator of random numbers for use with credit cards.
- Methods used to falsely enhance a victim's online account balance.
- Naturally, the victim of a Trojan virus download will want to disguise their own illegal intent. Therefore, the patient is hesitant to disclose their condition to authorities.

A Trojan virus was once delivered to email addresses acquired from a recruiting website as an example of this practise. Members who joined the website were emailed fake job offers with Trojan malware. Businesses' email accounts were the primary target of the assault. Those responsible for the attack calculated that employees infected with the Trojan wouldn't want to inform their existing employers while hunting for new employment.[4]

VIII. Avoiding Social Engineering

Companies may take several precautions against social engineering assaults, including those mentioned below:

1. Ensure that your IT staff does vulnerability checks for social engineering. As a result, management will have a better understanding of who needs more training and which types of people are most vulnerable to certain types of assault.

2. Start a campaign to increase people's awareness of security issues. When people are informed about social engineering techniques, they are less likely to fall victim to them.
3. Using encrypted email and internet portals, you may scan emails for dangerous links and ban them, therefore decreasing the possibility that an employee would click on one.
4. To limit the danger of malware infection through phishing emails, it is vital to keep up-to-date antimalware and antivirus software.
5. It is vital to update the firmware and software on your devices.
6. Maintain a record log of people who have access to sensitive data and ensure that they are using strong authentication.
7. Utilize two-factor authentication (2FA) techniques, such as a one-time password (OTP) or voice synthesis, to access vital accounts.
8. Ensure that workers do not use the same password for personal and professional accounts.
9. Utilize a screening method to eliminate communications that are most likely to be spam. A spam filter may include the IP addresses or sender IDs of spammers on a blacklist. Additionally, you may determine if an email is fraudulent by opening any attached files or clicking on any links it may include.

IX. Conclusion

In order to obtain access to sensitive data, hackers use a variety of deception methods to trick users into making sloppy security choices or divulging sensitive information. There may be several steps to a social engineering assault. If the attacker is successful, they will get sensitive data such as SSNs and credit card information. Users may ignore the relevance of information such as their phone number. The user may be duped into revealing private information. Social engineering-based attacks are all too frequent. Social engineering relies significantly on the attacker's ability to elicit trust and confidence via their own persuasion. Social engineering is often used by malware developers to deceive users into opening a malicious file or clicking on a dangerous link.

Often, mobile viruses are spread through SMS text messages. Peer-to-peer (P2P) networks are used to distribute malware, which may evade detection by anti-virus software installed on the mail server. This will enable administrators in determining demographics of potentially vulnerable users. In addition, it will assist management in determining if any of their employees need more training. Businesses may use a number of tactics to combat social engineering initiatives. Perform penetration testing for social engineering in IT.

References

[1] Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. Ieee Access, 9, 7152-7169.

[2] Bullee, J. W., & Junger, M. (2020). How effective are social engineering interventions? A meta-analysis. Information & Computer Security.

[3] Schaab, P., Beckers, K., & Pape, S. (2017). Social engineering defence mechanisms and counteracting training strategies. Information & Computer Security.

[4] Yasin, A., Fatima, R., Liu, L., Yasin, A., & Wang, J. (2019). Contemplating social engineering studies and attack scenarios: A review study. Security and Privacy, 2(4), e73.

[5] Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89.

[6] Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. IEEE Access, 8, 85094-85115.

[7] Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. IEEE Access, 9, 11895-11910.

[8] Fujikawa, M., & Nishigaki, M. (2011, August). A study of prevention for social engineering attacks using real/fake organization's uniforms: Application of radio and intra-body communication technologies. In 2011 Sixth International Conference on Availability, Reliability and Security (pp. 597-602). IEEE.

[9] Bezuidenhout, M., Mouton, F., & Venter, H. S. (2010, August). Social engineering attack detection model: Seadm. In 2010 Information Security for South Africa (pp. 1-8). IEEE.

[10] Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014, July). Towards an ontological model defining the social engineering domain. In IFIP International Conference on Human Choice and Computers (pp. 266-279). Springer, Berlin, Heidelberg.

[11] Zhang, Y., Egelman, S., Cranor, L., & Hong, J. (2007). Phinding phish: Evaluating anti-phishing tools.

[12] Badra, M., El-Sawda, S., & Hajjeh, I. (2010, May). Phishing attacks and solutions. In 3rd International ICST Conference on Mobile Multimedia Communications.

[13] Burov, O., Lytvynova, S., Lavrov, E., Krylova-Grek, Y., Orliyk, O., Petrenko, S., ... & Tkachenko, O. M. (2020, February). Cybersecurity in educational networks. In International Conference on Intelligent Human Systems Integration (pp. 359-364). Springer, Cham.

[14] Aldawood, H., Alashoor, T., & Skinner, G. (2020). Does awareness of social engineering make employees more secure?. International Journal of Computer Applications, 177(38), 45-49.

[15] Tsinganos, N., Sakellariou, G., Fouliras, P., & Mavridis, I. (2018, August). Towards an automated recognition system for chat-based social engineering attacks in enterprise environments. In Proceedings of the 13th International Conference on Availability, Reliability and Security (pp. 1-10).