International Journal of Engineering and Management Research
e-ISSN: 2250-0758 | p-ISSN: 2394-6962
https://ijemr.vandanapublications.com

Peer Reviewed & Refereed Journal
Volume-14, Issue-1 (February 2024)
https://doi.org/10.5281/zenodo.10686537

Unmasking the Evolution of Social Engineering in Cybersecurity: Techniques, Vulnerabilities, and Countermeasures

Dr. Paravathi C[1], Dhanyashree G[2], Yeshaswini R[3] and Lisha S[4]
[1]Associate Professor, Department of Computer Science and Engineering, BGS College of Engineering and Technology, Bangalore, INDIA
[2]Student, Department of Computer Science and Design, BGS College of Engineering and Technology, Bangalore, INDIA
[3]Student, Department of Computer Science and Design, BGS College of Engineering and Technology, Bangalore, INDIA
[4]Student, Department of Computer Science and Design, BGS College of Engineering and Technology, Bangalore, INDIA

[1]Corresponding Author: parvathi.cse@bgscet.ac.in

Received: 14-01-2024 Revised: 02-2-2024 Accepted: 18-02-2024

ABSTRACT

This research explores the historical evolution, tactics, and classifications of social engineering in the realm of cyber security. Tracing its roots back to the 1990s when attackers would exploit human vulnerabilities through phone calls, the paper highlights the shift towards sophisticated techniques targeting individuals to transfer substantial sums or disclose sensitive information. The term "social engineering" was coined in 1894, gaining prominence in cybersecurity in the 1990s and evolving with the proliferation of the internet. The attackers meticulously research their targets, utilizing human-based and computer-based social engineering tactics.

The classification section delineates human-based social engineering techniques, including impersonation, posing as an important user, using a third person, calling technical support, shoulder surfing, and dumpster diving. Computer-based social engineering involves fake emails, email attachments, pop-up windows, and other deceptive practices. The paper delves into various types of social engineering attacks, such as manipulating conversations, piggybacking, tracking, baiting, phishing, smishing, Trojan horse attacks, water hole attacks, and reverse social engineering.

The document emphasizes the need for self-protection measures, providing guidelines to recognize and thwart social engineering attacks. It also discusses real-time examples like email phishing scams and suggests multi-factor authentication as a potential solution. In conclusion, the research underscores the significance of understanding and combating social engineering, offering insights into its dynamics and countermeasures to fortify cybersecurity in an ever-evolving digital landscape.

***Keywords*—** Attack Techniques, Cybersecurity, Multi-Factor Authentication, Phishing Scams, Social Engineering

I. HISTORY OF SOCIAL ENGINEERING

Tricking users into divulging sensitive information is nothing new in the world of cybersecurity. The only thing that has changed is the attack techniques, intelligence collection stories, and sophisticated attacks by organized groups that include other threats such as phishing. The term social engineering was first used by Dutch businessman J..C..van Marken in 1894, but it has been used as a cyberattack technique since the 1990s.

In the 1990s, social engineering consisted of calling users to reveal their credentials or provide a dial-in number that connected the threat actor to a company's internal servers. Currently, attackers are using social engineering to trick targeted users into transferring millions of dollars to offshore bank accounts, costing companies. In some cases, the impact and damage may result in employees losing their jobs. [1][2]

According to the website www.worldwidewebsize.com, the number of indexed websites is over 4.48 billion. This does not apply to things that are not indexed, such as sites on the dark or deep web. Annual global Internet traffic has reached 1.3 zettabytes (or 1,300,000,000,000,000,000,000 bytes). According to some sources, the Internet can contain a total of 10 yottabytes of data. [3]

II. INTRODUCTION

Social engineering is a tactic that manipulates, influences, or deceives victims in order to gain control of computer systems or steal personal or financial information. They use psychological manipulation to trick users into making security mistakes or divulging sensitive information. Social engineering attacks occur in one or more steps. The perpetrator first researches the intended victim and gathers the necessary background information, potential entry points and weak security protocols needed to carry out the attack. The attacker then uses pretexts such as impersonation to gain the victim's trust and encourage subsequent actions that violate security practices, such as disclosing sensitive information or granting access to critical resources. [4][5]

Peer Reviewed & Refereed Journal
Volume-14, Issue-1 (February 2024)
https://doi.org/10.5281/zenodo.10686537

III. SOCIAL ENGINEERING OVERVIEW

Social engineers use a variety of tactics to carry out their attacks. The first step in most social engineering attacks is for the attacker to research and scout the target. For example, if the target is a company, hackers can collect information about the organizational structure, internal processes, terminology used in the industry, potential business partners, etc. A common tactic used by social engineers is to focus on the behaviours and patterns of employees with basic but initial access, such as security guards and receptionists. Attackers can search your social media profiles for personal information and examine your online and in-person behaviour. From there, social engineers can design attacks based on the information they collect and exploit vulnerabilities discovered during the reconnaissance phase. A successful attack allows the attacker to gain access to sensitive information such as social security numbers and credit card or bank account information. Earn money from your goals or gain access to a protected system or network. [7]

IV. CLASSIFICATION

Human Based Social Engineering

Human-based social engineering refers to human-to-human interaction to obtain needed or desired information.

An example would be calling the help desk and trying to find out your password.

1. Impersonating an Employee or a Valid User: "Spoofing" (e.g., impersonating an employee of the same organization) is probably the best technique social engineers use to deceive people. Social engineers "exploit" the fact that most people are generally kind, such as by telling someone who seems lost the location of a computer lab or by asking someone who has "forgotten" their ID. Entering a building or impersonating an employee appears to be harmless or any valid user in the system.

2. Posing as an Important User: An attacker impersonates a key user, such as a CEO or senior manager, who needs immediate assistance to access the system. Attackers use blackmail to allow lower-level employees, such as help desk employees, to gain access to the system. Most low-level employees don't ask questions of people who appear to be in positions of authority.

3. Using a Third Person: The attacker pretends to have permission to use the system from an authorized source. This trick is useful if the authorized person is on vacation or cannot be reached for verification.

4. Calling Technical Support: Calling technical support for assistance is a classic example of social engineering. Help desk and technical support staff are trained to assist users, making them easy targets for social engineering attacks.

5. Shoulder Surfing: This is a technique that collects information such as usernames and passwords by looking over a person's shoulder while they are logged into a system, thereby allowing an attacker to gain access to the system.

6. Dumpster Diving: This involves searching through trash for information written on pieces of paper or computer printouts. [8].

Computer Based Social Engineering

Computer-based social engineering is an attempt to use computer software/Internet to obtain desired/desired information.

For example, fake email is sent to the user asking them to re-enter their password on the website for confirmation.

1. Fake emails: An attacker sends fake emails to a large number of users so that the users recognize them as legitimate emails. This behaviour is also known as "phishing." It is an attempt to trick internet users (netizens) into disclosing sensitive personal information such as usernames, passwords, credit card details, etc.by impersonating trusted and legitimate organizations or individuals. Banks, financial institutions, and payment gateways are common targets. Phishing is typically carried out via email or instant messaging, and often asks users to enter information on their websites. The website is usually designed by the attacker to maintain the appearance of the original website. Therefore, phishing is also an example of social engineering techniques used to deceive Internet users. The term "phishing" arose from the analogy of Internet scammers using email as bait to "phish" or extort financial information from large numbers of Internet users (i.e., Internet users).
2. Email Attachments: Email attachments are used to send malicious code to a victim's system that is automatically executed (such as a keylogger password capture utility). Viruses, Trojan horses, and worms can be cleverly inserted into attachments to trick victims into opening the attachment.
3. Pop-up windows: Similar to email attachments, pop-up windows are also used. Pop-up windows that display special offers or free items can unintentionally install malware. [9]

V. TYPES OF SOCIAL ENGINEERING

Manipulating conversation - The attacker brings the group conversation to the topic of security, with one of the attackers disclosing his password and discussing whether the password is secure enough. If most other participants (or attackers) also start revealing their passwords, the target can be manipulated into revealing passwords and other sensitive information.

Piggybacking - An authorized person holds a secure door open for assistance or other reasons and provides

Peer Reviewed & Refereed Journal
Volume-14, Issue-1 (February 2024)
https://doi.org/10.5281/zenodo.10686537

entry to an unauthorized person. Most employees don't know all their colleagues in a (large) organization, they leave the door open to be polite, and it goes without saying that the attacker is well-dressed and has no shoes, polished, with perfect hair, polite and smiling. Victims are less likely to become suspicious. Subsequently attackers pose as lunch rushers at large companies and gain access to facilities by following employees wearing security badges. Security guards and clerks make eye contact, but they're accustomed to it.

Tracking **-** In some organizations, lazy security guards leave access cards on desks for people who forget them to retrieve themselves. Attackers impersonate employees of the target organization using appropriate disguises, such as uniforms and printed badges, to convince management of them supposed role in accessing buildings and restricted areas. If you only have one caregiver, your caregiver is more likely to provide assistance.

Baiting **-** Attacker leaves her USB stick containing malicious code in a location where the victim is likely to find it. The outside of the USB flash drive is painted with the target organization's logo or an attractive symbol to entice the victim to pick it up and insert it into their computer. Once malicious code is injected, it can be executed automatically.

Phishing **-** An attacker sends a phishing email using a fake address (or via a pop-up her window) offering very cheap discount coupons on groceries (or tickets to a sports event) for a limited time only.Notify the target that something is going on. The email includes an appealing food image (or a passionate sports poster). This trick targets you to click on malicious links or leak your privacy information. The attacker determines that there is dissatisfaction among the target organization's employees based on text, images, videos, etc. Posted on social media , and sends an email containing malicious code to some employees, falsely claiming it to be a hoax virus. You can send it to someone else and forward it anonymously to someone else. This can put many people within your organization at risk.

Smishing **-** The attacker blocks the target CEO's cell phone signal and sends an SMS message to the secretary spoofing the CEO's phone number: ``I'm in a meeting in another city, so I can't call you.'' Please encrypt your bill of organization and contract files into a zip file with the *** key and send it to xxx@xxx.xxxnow! Otherwise, you will lose important business.

Trojan Horse Attack, Honey Trap **–** The attacker provides a URL and suggests that it is a porn site or offers free software (malware) that you can download to watch pom videos. "The seductive image is not displayed. If the victim opens the link or installs the software, the attacker's computer or mobile device is compromised. [10]

Water Hole **–** The attacker determines that the target regularly visits or is likely to visit certain websites and infects those websites with malicious code that waits for the target to trigger, e.g., download software (malware), or click on a (malicious) link, the target is compromised.

Reverse Social Engineering – Attackers send emails containing fake addresses to new employees. ``We have recently run a network test. If you experience network problems, please contact us at xxx." The attacker causes a network error and waits for the new employee's request. After you help resolve the issue, the attacker says in good faith: "Would you please do a little bit to help us develop a security awareness training program for new employees by taking a survey? "Nearly 80% of our employees are already doing this." "Okay, thank you." "Are you aware of our email policies?... It's dangerous to open unwanted attachments... We need to know your password.", to be able to evaluate the safety awareness of new employees. That's for sure." ``Okay, that's..."

Pretext **-** Attacker poses as a cable installer, pretends to be wiring 200 pairs of terminals for the police, and requests sensitive information. Who would want to refuse an office worker the slightest bit of cooperation in accomplishing this difficult task? She sympathises with him, and she herself has had bad days at work. I'm going to change the rules a bit to help a colleague who has a problem. Vishing and pretexts. The attacker poses as a new employee and convinces the target that if their demands are not accepted, they will suffer significant harm. Example: Ask technical support (e.g. Paul) to reset the password for a specific account to complete an urgent task, and also ask for a VPN for external access. [11]

Vishing and Pretexting **-** Attacker calls a technical support representative and informs him that the CEO has approved a request for an emergency VPN channel for a project presentation in another city, and that this has already been completed. I will also tell you that. by other employees, e.g. Paul.

Shoulder Surfing- Attackers pose as delivery drivers, maintenance workers, or consultants to gain access to targeted workplaces and make contact with victims. If the victim is not careful, the attacker can peer over the victim's shoulder or look at visible areas such as sticky notes, papers, and computers to collect information such as usernames and passwords. Manipulate the conversation. The attacker steers the group conversation to the topic of security, with one of the attacker's girlfriends revealing her password and discussing whether it is secure enough. If most other participants (or attackers) also start revealing passwords, the target can be manipulated to reveal passwords and other sensitive information. [12]

VI. SELF PROTECTION METHODS

Remove all requests for financial information or passwords. Asking people to respond to messages containing personal information is a scam.

Refuse a request or offer of help- No reputable companies or organisations will contact you to provide

Peer Reviewed & Refereed Journal
Volume-14, Issue-1 (February 2024)
https://doi.org/10.5281/zenodo.10686537

support. Unless you specifically ask the sender for help, consider any offer of "assistance" to rebuild your credit, refinance your home, answer your questions, etc. to be a scam. If you receive a request for help from an unaffiliated charity or organisation, remove it. To donate, search for reputable charities yourself to avoid falling for scams. [13]

Set spam filters too high- All email programs have spam filters. To find the spam folder, check the settings option and set it to "High". Don't forget to check your spam folder regularly to make sure legitimate emails aren't accidentally stuck there. You can also search for your email provider's name and the term "spam filter" for detailed instructions on setting up a spam filter.

Protect Your Computing Devices- Install and keep antivirus software, firewalls, and email filters up to date, and set your operating system to update automatically. If your phone doesn't update automatically, update it manually every time you receive a notification. Use your web browser or an anti-phishing tool provided by a third party to alert you to the risk of the websites. [14][15]

VII. SOCIALENGINEERING PROTECTION TECHNIQUES

The most common attack techniques behind social engineering scams are:

1. Surveillance -Social engineering attacks such as business email compromise (BEC) and spear phishing rely heavily on pertinent information from the target. This allows cybercriminals to create highly customized attacks. For example, in a BEC crime, fraudsters can spend months intercepting emails to learn which suppliers receive payments on a regular basis. As part of the scam, invoice details are changed to force payment into the scammer's bank account.[18]

2. Grooming Social -grooming is often an integral part of social engineering attacks. Building trust and creating empathy among targeted employees will help ensure a successful scam. Grooming is closely related to surveillance, which is often performed as part of an attack. Fraudsters prepare for the endgame by building relationships with all employees involved in carrying out the attack: B. Someone from the finance department.

3. Deepfakes and AI- According to CSO Online, "Deepfakes are fake video or audio recordings that look and sound exactly like the original." Cybercriminals, like the rest of the business world, are constantly trying to optimise the process. Automation of cybercrime in the form of deepfakes is beginning to see the fruits of the cybercriminals labor. Deepfakes use artificial intelligence (AI) technology to trick people into thinking they are seeing or hearing someone other than the imposter. In a recent example, a CEO was tricked into believing he was speaking to the head of his parent company using a deep fake audio call. The CEO thought the request was legitimate and he transferred $243,000 to the scammer's account. [16]

4. Psychology of Social Engineering-Psychology of Social Engineering is low-tech in spirit, but it can use high-tech to perform tricks. Social engineering is based on the manipulation of natural human characteristics such as trust, empathy, the need to do a good job, and urgency. Simple, deep-rooted behaviours such as reciprocity. The process “if you pat me on the back, I'll pat you" process goes a long way toward successful cybercrime. Scammers are masters of manipulation, and the resulting excitement of financial gain is their specialty. They use all sorts of tricks to trick you into clicking on malicious links, downloading infected attachments, and transferring money from your corporate account to a fake account at your provider. [17]

VIII. REAL TIME PROBLEM EXAMPLE

An Email Phishing Scam

Let's say your bank sends you an email alerting you to any questionable behaviour on your account. You are directed to click on a link in the email in order to confirm your account information and guarantee its security. You click on the link out of fear that your account may be compromised, not realizing that it takes you to a phony website that is set up to steal your login information. You are sent to a confirmation screen after inputting your password and username, which appears to validate the security of your account. But your login credentials have been successfully taken by the attackers, giving them access to your bank account and maybe your whole balance.

Multi

Factor Authentication as a Potential Solution Multi-factor authentication, or MFA, has become popular as a means of thwarting phishing attempts and shielding consumers from illegal access. Applications that create one-time passwords and need input in addition to the login and password are known as authenticator applications.

Hardware tokens

To finish the login procedure, these tangible objects produce special codes that need to be physically input into the computer.

Application of MFA

Using multi-factor authentication (MFA) on a variety of online platforms, such as social networking accounts, e-commerce sites, and banks, can dramatically lower the success rate of phishing assaults. Without the extra verification step offered by MFA, an attacker will not be able to access an account even if they manage to get their hands on the user's login credentials.

In Summary

Social engineering assaults are a serious danger to cybersecurity, especially phishing schemes. Organisations may greatly improve their security posture and shield their users from monetary losses and unlawful

Peer Reviewed & Refereed Journal
Volume-14, Issue-1 (February 2024)
https://doi.org/10.5281/zenodo.10686537

access by using multi-factor authentication. Users may engage with online platforms with more confidence thanks to MFA's additional security layer, as their accounts are safeguarded by an additional line of defence.

IX. CONCLUSION

In conclusion, this research emphasizes the strategies and historical evolution of social engineering in cybersecurity, emphasizing the field's significance in the digital era. Understanding the various approaches taken by attackers can be gained by categorizing social engineering tactics using computers and humans.

The significance of self-defence techniques, such as awareness, spam filters, and device security, is emphasized in the document. Examples from today, such as email phishing, emphasize the importance of being cautious. Suggest multi-factor authentication as a suitable remedy that aligns with contemporary cybersecurity protocols. Anticipating the future, the objective is to create sophisticated instruments for identifying and stopping fraudulent activity, guaranteeing a safer online environment.

The future scope entails developing a website that can recognize and prevent fraud in messages, emails, and phony websites. Creating intelligent algorithms to evaluate the authenticity of content on the internet will be essential to improving cybersecurity protocols and making the internet a safer place.

REFERENCES

[1] Dabke, Viyan, Dabke Yanik & Gadgil, Dr. (2023). *Social engineering as a driving force for innovation in cybersecurity*. DOI: 10.36227/techrxiv. 24226411.v2. https://www.researchgate.net/publication/374662175_Social_Engineering_as_a_Driving_Force_for_Innovation_in_Cybersecurity

[2] *Social engineering*. proofpoint [online]. Available: https://www.proofpoint.com/us/threat-reference/social-engineering.

[3] Zuoguang Wang, Hongsong Zhu & Limin Sun. (2021). *Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods*. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China. DOI: 10.1109/ACCESS.2021.3051633.

[4] Nanda, Ipseeta & Dey, Rajesh. (2022). Social engineering: An introduction. *Information Management and Computer Science, 5*, 36-37. DOI: 10.26480/imcs.02.2022.36.37.

[5] *Information security offices, computing services*[online]. Availabe:https://www.cmu.edu/iso/aware/dont-take-the-bait/social engineering.html

[6] Khan, Salal Ali. (2023). *Social engineering*. Conference: Computer and networks security - Final's Presentation At: ST.FX University, Antigonish, NS. Available at: https://www.researchgate.net/publication/376266487_Social_Engineering.

[7] Linda Rosencrance and Madelyn Bacon. *Social engineering, tech target*. Available at: https://www.techtarget.com/searchsecurity/definition/social-engineering.

[8] https://www.ques10.com/p/49012/classification-of-social-engineering/#google_vignette.

[9] Abbas, Asad. (2024). Social engineering attacks: Techniques, impacts, and mitigation strategies. https://www.researchgate.net/publication/377382644_Social_Engineering_Attacks_Techniques_Impacts_and_Mitigation_Strategies.

[10] Choi, Young. (2023). Social engineering cyber threats. *Journal of Global Awareness, 4*, 1-12. DOI: 10.24073/jga/4/02/08. Available at: https://www.researchgate.net/publication/376880801_Social_Engineering_Cyber_Threats.

[11] David, Udochukwu & Bode-Asa, Ayomide. (2023). An overview of social engineering: The role of cognitive biases towards social engineering-based cyber-attacks, impacts and countermeasures. DOI: 10.13140/RG.2.2.12421.12003. Available at: https://www.researchgate.net/publication/376450802_An_Overview_of_Social_Engineering_The_Role_of_Cognitive_Biases_Towards_Social_Engineering-Based_Cyber-Attacks_Impacts_and_Countermeasures\.

[12] Zuoguang Wang, Hongsong Zhu & Limin Sun. (2021). *Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods*. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China. DOI: 10.1109/ACCESS.2021.3051633.

[13] Omullah, Hamza. (2023). The art of social engineering. DOI: 10.13140/RG.2.2.20647.73124. https://www.researchgate.net/publication/374117752_THE_ART_OF_SOCIAL_ENGINEERING.

[14] Webroot by opentext[online]. Available at: https://www.webroot.com/in/en/resources/tips-articles/what-is-social-engineering.

[15] Heartfield, Ryan & Loukas, George. (2018). Protection against semantic social engineering attacks. DOI: 10.1007/978-3-319-97643-3_4. https://www.researchgate.net/publication/322476901_Protection_Against_Semantic_Social_Engineering_Attacks.

[16] Hitachi System Security Inc . Available at: https://hitachi-systems-security.com/common-

Peer Reviewed & Refereed Journal
Volume-14, Issue-1 (February 2024)
https://doi.org/10.5281/zenodo.10686537

social-engineering-examples-attack-techniques/.

[17] Hao, Tan. (2024). Combating social engineering attacks in the age of deepfakes: A multi-layered approach using explainable ai and user education. https://www.researchgate.net/publication/377326123_Combating_Social_Engineering_Attacks_in_the_Age_of_Deepfakes_A_MultiLayered_Approach_Using_Explainable_AI_and_User_Ducation.

[18] Olusanya Akinola, Adeniji Oluwatosin, Ayobami Afolake & Adekanla Oluwaseun. (2023). *Analysing social engineering attacks and its impact*. 10.13140/RG.2.2.16300.85120. https://www.researchgate.net/publication/376443039_Analysing_Social_Engineering_Attacks_and_its_Impact.

[19] Breda, F., Barbosa, H. & Morais, T. (2017). Social engineering and cyber security. *Proceedings of the International Conference on Technology, Education and Development, Valencia*, pp. 4204-4211. http://dx.doi.org/10.21125/inted.2017.1008.

[20] Winkler, I.S. & Dealy, B. (1995) Information security technology? Don't rely on it a case study in social engineering. *5th USENIX UNIX Security Symposium, Salt Lake City*, pp. 1.