WHAT IS SOCIAL ENGINEERING AND HOW TO PREVENT IT?

Alexandru TODOS

Departament of Software Engineering and Automatics, SI-221M, Faculty of Computers, Informatics and Microelectronics, Technical University of Moldova, Chisinau, Republic of Moldova

Corresponding author: Todos Alexandru, todos.alexandru1@gmail.com

Scientific coordinator: Rodica BULAI, university lector, Technical University of Moldova

Abstract. *When we think about cyber-security, most of us think about defending ourselves against hackers who use technological weaknesses to attack data networks. But there's another way into organizations that's taking advantage of human weakness. This is known as social engineering, which involves tricking someone into divulging information or enabling access to data networks.*

Keywords*: information security, privacy, security management, phising, vulnerability*

Introduction

Social engineering [1] is a cybersecurity attack that uses deception and manipulation to convince unsuspecting users to reveal confidential information about themselves such as social account credentials, banking credentials, etc.

The effectiveness of this attack does not necessarily need a high level of technical ability. Instead, social engineering preys on universal human psychological traits including civility, curiosity, credulity, avarice, carelessness, shyness, and apathy.

Social engineering can occur over the phone, through direct contact, or via the Internet. Attackers may seek to install malicious software on a victim's device, gaining full control over their computer and network, to achieve their goals of sabotage or theft.

Cybersecurity experts are concerned about social engineering attacks because no matter how robust the security stack is, users can still be tricked into providing their credentials to a hacker.

How does social engineering work?

Social engineering attacks rely on communication between attackers and victims. Attackers motivate users to compromise themselves, rather than using brute force methods to breach data.

The attack cycle consists of **preparation**, **infiltration**, **exploitation** and **disengagement**. Attackers collect information about victims through social media, telephone calls, email, text messages or other sources [2]. After that, they approach as reliable sources or authorities, use the information they have learned about victim to gain trust and persuade to give them sensitive information [3].

This process can take place in a single email or over months in a series of social media chats [4]. By studying the behaviour of the victim and playing on his weaknesses, the attacker can get the information he needs Thus, by studying the behaviour of the victim and playing on weaknesses, the attacker can get the information without writing a line of virus code.

Types of social engineering

Almost every type of cybersecurity attack has some kind of social engineering. Attackers that use social engineering often employ the following strategies [5]:

1. Phishing Attacks: attackers pretend to be a trusted institution or individual to persuade victim to expose personal data. Phishing scams are taking advantage of user trust. Methods used in phishing each have unique modes of delivery [6], including but not limited to:

Voice phishing – a sophisticated form of phishing attack. In this attack, a phone number is usually spoofed to appear legitimate. Attacker might disguise themself as someone trusted to trick victims into giving up sensitive information.

SMS phishing – a type of phishing attack that comes in the form of text messages. These types of attacks solicit immediate action from a victim, by including malicious links to click [7].

Email phishing – the most traditional type of phishing, using an email urging you to reply or follow-up by other means.

Search engine phishing – attempt to place links to fake websites at the top of search results. These may be paid ads or use legitimate optimization methods to manipulate search rankings. These links tempt you to travel to phishing websites.

2. Baiting Attacks: attacker leaves a malware-infected device, such as a USB drive, where someone is likely to find it. If a curious person picks up the device and plugs it into their own computer, they may infect their device with malware.
3. Physical Breach Attacks: attackers physically show up and pretend to be someone they are not to access restricted locations or information. These attacks take place in corporate settings, such as in enterprises, governments, or other organizations. Attackers pose as a representative of a reputable, well-known vendor for the business. Some attackers might even be ex-employees with grudges against their former employers. To avoid questioning, they provide an unremarkable but plausible identity.
4. Scareware Attacks: a form of malware used to frighten victim into taking an action. This malware uses alarming warnings that report fake infections or claim one of your accounts has been compromised. Usually, it appears in the form of pop-ups, claiming to help you remove a computer virus. As a result, scareware pushes victim to do thoughtless actions, like buying fraudulent cybersecurity software.

Why are people exposed to social engineering attacks?

Did you know that majority of social engineering attacks are successful because of human mistakes? [8] That is because of human emotions and psychological aspects that social engineers can use to their advantage. This includes emotions such as:

- Carelessness: most of us have unintentionally clicked a few links or opened an untrustworthy email attachment. The harm done may be trivial to severe, depending on how quickly we were able to stop such an act.

- Curiosity: victim mistakenly receives an email with intriguing content not meant for them. Despite potential risks, curiosity drives victim to download the attached file, only to discover it has a virus.

- Fear: according to Charles E. Lively, Jr. in the paper "Psychological-Based Social Engineering," [9] attacks that play on fear are usually the most aggressive form of social engineering because it pressures the target to the point of making them feel anxious, stressed, and frightened. Participants in such attacks are more likely to provide money, intellectual property, or other information.

- Empathy and sympathy: when crises or natural disasters occur, it is impossible to escape the urge to provide aid. Nowadays, it's far simpler to go online, type your card information into a website accepting donations, and hit "Enter" because many of us are unlikely to be able to quickly board a plane and fly to damaged areas to help. Not all those websites are legitimate. The associated feelings of sympathy and empathy are used by social engineers to steal money from individuals who are truly in need and put it directly into their own pockets.

Prevention techniques

For all mobile and computer users, understanding how to avoid social engineering assaults is crucial. Here are some important ways to protect against all types of cyberattacks:

1. Avoid clicking on links in any emails or messages**.** Type URLs manually and ensure that they are official and legitimate.

2. Use multi-factor authentication. Protecting your accounts with more than simply a password is safer.
3. Use strong passwords. Your passwords should be complicated employing a variety of character kinds, such as symbols, numerals, and uppercase letters [10]. Use a password manager to store and remember all your passwords.
4. Avoid sharing personal information such as name of your school, pet or other personal details. You could be unknowingly exposing answers to your security questions or parts of your password.
5. Never let strangers connect to your primary Wi-Fi network, make access to a guest Wi-Fi connection available. This allows your main connection to remain secure and interception-free.
6. Use a VPN (Virtual Private Network). A virtual private network are services that give you a private, encrypted "tunnel" on any internet connection you use. Your connection is not only guarded from unwanted eyes, but your data is anonymized so it cannot be traced back to you via cookies or other means.
7. Keep all network-connected devices and services secure. Be sure to protect commonly overlooked devices like home network routers. Data breaches on these devices could fuel personalization for a social engineering scam.

Most businesses are aware of cyber-attacks and have invested heavily in security measures to reduce security threats. Though, with all that in place, in the digital world, there is still an element called human. To prevent successful social engineering attacks in companies, consider implementing the following measures:

1. Conduct regular security trainings and simulate social engineering attempts [11].
2. Increase spam filtering and implement security policies. For example, require multi-factor authentication for employees.
3. Frequently check critical parts of the company.
4. Periodically execute penetration tests and do internal audits [12].

Conclusion

Social engineering is one of the most effective ways of gaining access to secure systems and obtaining sensitive information yet requires minimal technical knowledge. Social engineering works against technical barriers and exploits human vulnerabilities to gain access. The best defence is to educate users on the techniques used by social engineers. Even so, a determined attacker with sufficient skill, resources and ultimately, luck, will be able to retrieve the information they are looking for. For this reason, organisations and individuals should have measures in place to respond to, and recover from, a successful attack.

Acknowledgment. I express my sincere gratitude to professor Bulai Rodica from the Technical University of Moldova for assistance and guidance provided during the preparation of this scientific report.

References

1. CASTELLUCCIO, MICHAEL. *Social Engineering 101*. Strategic Finance, vol. 84, no. 6, Dec. 2002, pp. 57+.
2. *Investigators at State Key Laboratory of Mathematical Engineering and Advanced Computing Describe Findings in Social Engineering (A Risk Analysis Framework for Social Engineering Attack Based on User Profiling).* Obesity, Fitness & Wellness Week, 13 Mar. 2021, p. 278.
3. JACKSON, RUSSELL A. *PULLING STRINGS: High-level hackers are using social engineering tactics to manipulate employees into giving up vital information.* Internal Auditor, vol. 75, no. 4, Aug. 2018

4. ALBLADI, S.M., WEIR, G.R.S. *Predicting individuals' vulnerability to social engineering in social networks.* Cybersecurity 3, 7 (2020).
5. *WHAT IS SOCIAL ENGINEERING?* Internal Auditor, vol. 75, no. 4, Aug. 2018
6. ALABDAN, RANA. *Phishing Attacks Survey: Types, Vectors, and Technical Approaches.* Future Internet, vol. 12, no. 10, Oct. 2020, pp. 1h+.
7. ALAZAB, MAMOUN, and RODERIC BROADHURST. *Spam and criminal activity.* Trends & Issues in Crime and Criminal Justice, no. 526, 21 Dec. 2016
8. ADAMS, ANNE, and MARTINA ANGELA SASSE. *Users are not the enemy.* Communications of the ACM, vol. 42, no. 12, Dec. 1999, p. 40.
9. CHARLES E. LIVELY, JR, GSEC Option 1 version 1.4, *Psychological-Based Social Engineering* (2003).
10. DEALVARE, A.M. *How crackers crack passwords or what passwords to avoid.* In Proceedings of Unix Security Workshop II. (Portland, 1990).
11. WANG, ZUOGUANG. *Social engineering in cybersecurity: a domain ontology and knowledge graph application examples.* Cybersecurity, vol. 4, no. 1, 2 Aug. 2021
12. PYZI., KEN. *Shutting the door on social engineering: internal audit can help organizations thwart efforts to manipulate employees to gain system access.* Internal Auditor, vol. 72, no. 5, Oct. 2015