Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Social Engineering in Cyber Security

Panya Sethi[a]

[a]Symbiosis Law School, Noida, India

Received 17 October 2022; *Accepted* 29 October 2022; *Published* 02 November 2022

Social engineering is a term used to describe a broad range of fraudulent activities that include interaction with real people. The goal of this strategy is to trick victims into disregarding security measures or providing sensitive information. Most social engineering attacks begin with the attacker conducting research and reconnaissance on the target. If the target is an enterprise, for example, the hacker may gather intelligence on the organizational structure, internal operations, industry jargon, and potential business partners, among other things. Social engineers frequently target the behaviour patterns of employees with low-level but initial access, such as a security guard or receptionist; attackers can scan social media profiles for personal information and study their behaviour online and in person. Social engineering might include a single step or several stages. Before launching an assault, a criminal profile he targets to learn details like access points and security flaws that would help them succeed. After gaining the trust of the victim, the attacker plants the seed for the victim to subsequently break security rules by, for example, disclosing sensitive information or gaining access to forbidden areas.

"Generally, social engineering attackers have one of two goals:

1. *Sabotage: Disrupting or corrupting data to cause harm or inconvenience.*

2. *Theft: Obtaining valuables like information, access, or money.*

Keywords: *hacker, behaviour, trust, sabotage, theft, fraudulent activities*

HOW DOES SOCIAL ENGINEERING WORK?

For many social engineering strategies to be successful, communication with the target is required. Instead of resorting to brute force to access your data, the attacker will likely use social engineering to trick the victim into compromising himself. Because of the assault cycle, con artists have a tried-and-true method of fooling you. Typically, a social engineering assault cycle will consist of the following steps:

- **"Prepare** by gathering background information on you or a larger group you are a part of.
- **Infiltrate** by establishing a relationship or initiating an interaction, starting by building trust.
- **Exploit the victim** once trust and weakness are established to advance the attack.
- **Disengage** once the user has taken the desired action."

The first step in any assault is for the attacker to do reconnaissance on the target.[1] If the victim is a company, for instance, the hacker could get knowledge about the target's organizational makeup, internal operations, jargon, and potential business partners. If the victim is a company, the hacker could pick up on the inner workings, jargon, and potential commercial relationships of the enterprise.

SOCIAL ENGINEERING ATTACKS LIFESTYLES

The risk of social engineering rests in the fact that it preys on human frailty rather than technical flaws in programs or systems. In contrast to an infiltration carried out by malware, human error is significantly more difficult to detect and counteract.

There is a wide variety of social engineering assaults, and they may be carried out anyplace where people interact with one another. Here are the most typical examples of social engineering used online.

[1] Linda Rosencrance & Madelyn Bacon, 'Social engineering' (*Search Security*, June 2021) <https://www.techtarget.com/searchsecurity/definition/social-engineering> accessed 9 October 2022

1. **Baiting**

Baiting assaults, as the term suggests, involve making a false promise to draw in the target. They set traps for their victims to fall into so that they may steal data or infect computers with malware. Physical media distribution of malware is a particularly dangerous kind of baiting. Example: perpetrators would strategically place the bait (often malware-infected flash drives) in locations frequented by their targets (e.g., bathrooms, elevators, the parking lot of a targeted company). There are seemingly authentic touches, such as a label pretending to be a payroll list, that lend credence to the scheme. People who are easily intrigued take the bait and enter it into their home or business computer, where malware is secretly installed. Con artists may be able to carry off a baiting scam without ever leaving their virtual territory. Online versions of baiting include appealing advertisements that direct viewers to harmful websites or promote downloads of malware-infected software.

2. **Scareware**

Scareware inundated users with false alarms about hypothetical threats. Users are tricked into installing useless (except to the perpetrator) or malicious software by pretending their machine is afflicted with malware. Deception software, rogue scanning software, and fraud ware are all names for what scareware is. Some forms of scareware, such as browser pop-up adverts claiming things like "Your computer may be infected with harmful spyware apps," may be rather deceptive. If you click on it, you will be sent to a bad website where malware might infect your computer, or the program will be installed automatically. Spam emails may also be used to spread scareware by giving out exaggerated warnings or trying to sell people useless or malicious software.

3. **Pretexting**

Here, an adversary gathers intelligence by telling a string of falsehoods. The scammer may approach the victim by professing to require private information to complete an urgent assignment. The perpetrator of a social engineering assault may often pose as a friend, coworker, law enforcement officer, bank official, or other trusted authority figure to gain the victim's

confidence and get access to sensitive information. The pretext asks the victim what seems to be legitimate identification verification inquiries to glean sensitive information. Information including social security numbers, home locations, phone numbers, vacation itineraries, financial data, and even details about the security of the actual building might be obtained through this scam.

4. Phishing

Phishing is a kind of social engineering in which the victim is duped into responding to an email or text message campaign by creating a false sense of urgency, curiosity, or fear. They are then coaxed into divulging personal information, visiting fraudulent websites, or downloading dangerous files. If a client of an online service violates the terms of service, the consumer may get an email urging them to take immediate action, such as resetting their password. There is a link to what seems like a legitimate website but is a phishing scam that asks for the user's current login details and a new password. As soon as the attacker sees the form submitted, they have access to the information. In the event of a widespread phishing campaign using almost identical messages, mail servers connected to threat-sharing systems have a far easier time detecting and blocking the assaults.

5. Spear phishing

This is a sophisticated kind of phishing in which a victim is a particular person or company. To conceal their assault, they personalize their communications depending on the information they learn about their targets, such as their interests, occupations, and social networks. Spearfishing is far more labor-intensive and time-consuming and might take weeks or months to finish. They are harder to detect and provide better results when carried out properly. A spear-phishing email sent to one or more employees might seem to come from the company's IT consultant, whom the attacker is pretending to be. The consultant’s signature and writing style make it seem as if it was authored by them. It requests that recipients change their passwords and provides a link to a malicious website where their data might be compromised.

6. Vishing

Voice phishing is a similar concept. Vishing is a sort of social engineering in which sensitive information such as a person's bank details or identity is gathered by phone.

7. Whaling

Whaling attacks are a subset of phishing attacks that specifically target high-ranking executives like the CFO or CEO of an organization to get access to confidential data.

8. Watering Hole

To get access to a network, the attacker compromises a select set of users by infecting websites they often use and trust.

9. Quid pro quo

To do this, the social engineer would often make false promises of compensation in return for the victim's cooperation. For instance, a hacker may phone several random extensions inside a company, posing as a technical support representative. The hacker will eventually discover a victim with a genuine technical problem, whom they will then pretend to assist. The hacker may trick the victim into typing in the instructions to activate malware or get sensitive information such as passwords via this contact.

10. USB Baiting

USB baiting may appear unrealistic, but it occurs more frequently than you might think. Essentially, cybercriminals install malware onto USB sticks and leave them in strategic locations, hoping that someone will pick up the USB and plug it into a corporate environment, unwittingly unleashing malicious code into their organization.[2]

[2] 'What Is Social Engineering?' (*Cisco*) <https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html> accessed 09 October 2022

CASES OF SOCIAL ENGINEERING

Frank Abagnale is widely regarded as a leading authority on social engineering techniques. In the 1960s, he impersonated at least eight people, including an airline pilot, a doctor, and a lawyer. During this time, Abagnale was also a check forger. Following his incarceration, he worked as a security consultant for the Federal Bureau of Investigation and launched his financial fraud consultancy. His experiences as a young con man were immortalized in his best-selling book Catch Me If You Can and the film adaptation directed by Oscar-winner Steven Spielberg.

Kevin Mitnick, dubbed "the world's most wanted hacker," persuaded a Motorola employee to give him the source code for the MicroTAC Ultra Lite, the company's new flip phone. It was 1992, and Mitnick, who was on the run from the police, was living in Denver under an assumed name. He was worried about being tracked by the federal government at the time. To hide his location from authorities, Mitnick used the source code to hack the Motorola Micro TAC Ultra Lite, then attempted to change the phone's identifying data or disable the phone's ability to connect to cell phone towers.

In 2013, a phishing scam led to the massive data breach of Target. A phishing email was sent to a subcontractor that was one of Target's business partners. The email contained the Citadel Trojan, which enabled attackers to penetrate Target's point-of-sale systems and steal the information of 40 million customer credit and debit cards. That same year, the U.S. Department of Labor was targeted by a watering hole attack, and its websites were infected with malware through a vulnerability in Internet Explorer that installed a remote access Trojan called Poison Ivy.

Cybercriminals gained access to John Brennan's personal AOL email account in 2015, the then director of the Central Intelligence Agency. One of the hackers described how he used social engineering techniques to pose as a Verizon technician and request information about Brennan's Verizon account. After obtaining Brennan's Verizon account information, the hackers contacted AOL and correctly answered security questions for Brennan's email account.

CONCLUSION AND SUGGESTIONS

Social Engineering Prevention

To accomplish their goals, social engineers use human emotions like curiosity and terror to lure unsuspecting people into their traps. You should exercise caution anytime an email alarms you, a website's offer piques your interest, or you find a random piece of digital material lying about. Most attempts at social engineering in the digital arena can be avoided with just a little bit of vigilance.

Even more so, the following advice might help you be more alert to social engineering tricks.

Don't open emails and attachments from suspicious sources – It is not necessary to reply to an email if you do not recognize the sender. Verify information from many sources, including the service provider's website or by calling them directly, even if you suspect the sender of the message is a friend or acquaintance. Keep in mind that email addresses are often faked, meaning that even emails that seem to have come from a known and trustworthy sender might have been sent by a malicious actor. Using secure email and web gateways, you may check incoming emails for harmful links and block them before they reach your employees' inboxes. You may use spam filters to go through your inbox and delete any unwanted messages. A spam filter may use many methods to identify and block potentially malicious emails, including blacklisting IP addresses and sender identifiers, scanning for malicious attachments and links, and analyzing message content.

Use multifactor authentication – User credentials are highly sought after by cybercriminals. Multi-factor authentication adds an extra layer of security to your login and reduces the risk of your account being compromised.

Be wary of tempting offers – Do not jump to conclusions just because something sounds good. You can immediately find out whether you are dealing with a genuine offer or a trap by doing a fast Google search.

Keep your antivirus/antimalware software updated – Whether you want to wait for updates to download automatically or check for new signatures first thing every day, make it a practice to do so. Scan your machine for malware and make sure the updates have been installed regularly.

It is imperative that IT teams routinely do penetration testing using social engineering methods. This information will aid managers in determining which staff need more training and which sorts of users offer the greatest danger of attack.

Use two-factor authentication (2FA) to get into your most important accounts (e.g., a text message confirmation code or voice recognition).