Martian Defense Research: White Paper

Social Engineering: Modern Techniques

By @Martian

Security Researcher

Introduction

Social engineering is used to describe a host of malicious activities accomplished during human interactions. Against the backdrop of information security, it encompasses the psychological manipulation of people into taking actions or revealing confidential information. All forms of social engineering are based on the characteristics of the human decision-making process—otherwise known as cognitive biases. A good example of social engineering is when a criminal calls an individual via their cellphone informing them that their bank account is on the verge of being closed. Once the alarmed individual seeks advice on what is the best course of action to take, the criminal asks them for their passwords and IDs in an effort to steal money from the victim.

As illustrated in this example, social engineering occurs in steps. The perpetrator often starts by investigating the intended victim to collect vital background information including potential points of entry or weak security protocols, which they could exploit to facilitate an attack. In other cases, the attacker proceeds to gain the victim's trust and offer stimuli for upcoming actions that compromise information security, such as providing sensitive information or access to critical databases. What is unique about social engineering is that it preys on human error instead of vulnerabilities in software or operating systems. This makes the vice less predictable, more difficult to identify, and even harder to prevent in comparison to malware–based attacks.

This paper will explore the common modern social engineering techniques that have been successful.

6 Common Modern Social Engineering Techniques

Phishing

Phishing is a type of social engineering whereby malicious individuals send messages masquerading as a trusted person or entity. It is often used to steal user data such as login credentials and credit card numbers. The victim is first lured into opening an email, a text message, or an instant message. Soon after, they are duped into clicking a malicious link that prompts the installation of malware, the stalling of the system in the event of a ransomware attack, or the revealing of critical information. A common example of phishing occurs when an internet user receives an email alerting them of a policy violation and demanding immediate action from them, say, a required password change. A link to an illegitimate website—that looks similar to its legitimate variant—is contained in the email. This link allows the unsuspecting victim to enter their credentials and password; and upon submittal, the information is sent to the attacker.

Phishing facilitates unauthorized purchases, the stealing of funds, and identity theft against individuals. For corporate or governmental networks, it preludes an advanced persistent threat (APT) event. FBI's recent Internet Crime Report revealed that phishing, including vishing, SMiShing, and pharming is the most common form of social engineering attacks in the US, with 300,497 victims in 2022.

Quid Pro Quo

Quid Pro Quo is an attack during which a scammer uses false promises to lure a victim into a situation that allows them to either steal personal and financial information or wreak the system with malware. Quid Pro Quo is similar to a technique called baiting, which generally uses physical media to distribute malware and the fake promises revolve around goods. However, enticing ads that link up malicious sites are increasingly being used to entice users to download malware-infected applications—in what has come to be known as Quid Pro Quo attacks. Other promises that peg on user curiosity or greed online are free music or movie downloads, expensive gifts, or discounts on premium software.

To give an example, a potential victim may receive a text or an email from an anonymous source claiming that the online user has won a lottery! All they are required to do is to pass their personal information over—which is actually what the scammers are looking for. Tantalizing messages like “Congratulations! You are the lucky winner of…” and “Yay! We have a gift for you; download it now” are characteristic of a Quid Pro Quo attack. People are naturally excited about freebies, discounts, and special offers; and this explains why baiting has been very successful. Children and teenagers often fall victim to this type of social engineering attack because they are more likely to “take the bait” without considering the potential consequences that soon follow.

Scareware

Oftentimes distributed through a pop-up ad, scareware takes advantage of the victim’s fear, cajoling them into installing fake and malicious anti-virus software. The motivation behind scareware can range from selling useless, fake software to the distribution of damaging malware that exposes confidential information. It is, however, commonly known for luring online users to download a form of malware called ransomware that holds the user’s data hostage in exchange for a monetary settlement. In March 2019, Office Depot and its tech support provider. Support.com was embroiled in what constitutes scareware. The two entities were forced to pay the FTC a $35 million settlement for allegedly deceiving customers into downloading a free “PC Health Check Program.” In this case, scareware was used to sell unnecessary diagnostic and repair services. The two businesses were at fault with the FTC because they used false alarms to drive sales.

Similarly, Latvian national, Peteris Sahurovs, was arrested in 2018 for a 2010 scareware scheme that sold *Windows* users fake anti-virus software. Individual units of the software sold for $49.95 and Sahurovs had made sales exceeding $250,000 by the time he was apprehended.

6 Common Modern Social Engineering Techniques

Pretexting

Pretexting involves a false situation or pretext to trick victims into giving their private information. Unlike the other forms of attacks that involve deception, the scammer behind a pretexting formulates a story to fool the unsuspecting victim. It is regularly instigated by a perpetrator purporting to need confidential information from the victim in order to perform a critical task.

It is typical of them to start by building trust with their victim by assuming the role of someone in authority. They usually pretend to be a police officer, a co-worker, a tax official, or any other figure who has the right to access the information in question or may use the information to assist the victim.

An example of a message that a potential victim may receive reads: “Hi, this is tech support from your bank looking to confirm your account information.” Because a pretexting attack wholly relies on the victim’s belief in the perpetrator’s story, it is usually used against victims who are trusting, vulnerable, influential, less tech-savvy, or respectful to authority. This means that the perpetrator thoroughly plans the attack to come up with both the role to assume and a plausible situation that can emotionally appeal to the intended victim.

Water holing

Also known as a watering hole attack, water holing takes place when a perpetrator observes or guesses which websites an entity or individual regularly uses and inflicts one or more of them with malware. The overarching goal of this type of social engineering is to inflict at least one of the computers used by members of the target group and gain access to the network members of the group are known to visit. Alternatively, the perpetrator may create a website and then lure the victim to it. This attack was named after a hunting technique in which a hunter determines where the prey is likely to go, most commonly to a watering point, and then waits there ready for an ambush. It can also be achieved using a technique called typo squatting in which a threat actor owns a domain similar to a well-known domain to take advantage of common misspellings of legitimate websites.

Even though water holing is rare, it poses a serious threat to securing because it is difficult to detect and is commonly wielded against highly secure networks via unsuspecting employees, business partners, or vendors. In 2017, for example, this technique was used to compromise websites belonging to the Ukrainian government and inflict them with the ExPetr malware. One year before this attack, the Canada-based International Civil Aviation Organization (ICAO) was used to spread malware that infected the United Nations (UN) network.

Spear phishing

Spear phishing is a more targeted kind of phishing attack in that the perpetrator pursues specific individuals or entities. Like in the case of pretexting, they plan attacks based on the characteristics of the victims to lure them into the scam more easily. Therefore, planning this type of attack may take weeks or even months. Still, they are more difficult to detect and typically have better success rates.

A good illustration of spear phishing is CEO fraud. Otherwise called executive phishing or business email compromise (BEC), attackers spend long periods learning about a company's organizational structure and prominent figures of the executive team. Then, they exploit the trustworthiness of the character they impersonate to convince the target into action. For instance, they may pretend to be the CFO when asking a company's accountant to initiate a financial transaction or reveal vital information. In June 2015, an American network Technology Company for service providers and enterprises, Ubiquiti Networks Inc., was defrauded of $46.7 Million following a spear phishing e-mail. In addition, The FBI reported that BEC attacks cost organizations revenues exceeding $43 billion between 2016 and 2021. At the time of writing, they reported losses over $2.7 billion just in 2022 alone!

Conclusion

In summary, the six techniques used in social engineering covered in this paper point to the preying of human psychology, greed, and curiosity to compromise computer systems or access confidential information. These techniques are Phishing, Quid Pro Quo, Scareware, Pretexting, Water holing, and Spear phishing. Constantly being on the lookout for these techniques can help individuals, groups, and organizations protect themselves against the various kinds of malicious social engineers prowling the internet.

