Cybersecurity and Social engineering

By, David P, Ryan H, Ryan S, Zack, Gavin H.

What is Social engineering

- Social engineering is a way for cyber criminals to gain access to a controlled or closed system they shouldn't be able to.
- Social engineering is not a cyber attack in a traditional sense it does not deal with computers or hardware typically but it can, but usually instead with persuasion and psychology.
- The Aim of social engineering is to gain the trust of your target and use the trust you've built in order to get them to either divulge information they shouldn't normally tell anyone or perhaps taking unsafe actions such as clicking an external unverified link or opening an attachment of the same type.
- An aspect of social engineering that makes it very dangerous is that it does not need to be successful in a large scale, a single person falling for the lies of a cyber criminal can compromise a system no matter how safe everyone else involved is.

Types of Social engineering “attacks”

- The most common types of social engineering attacks are, Phishing, Water Hole attacks, Compromised or impersonated emails, Physical social engineering, and USB baiting
- Phishing attacks are usually an email or text message or some sort of communication that looks like it is coming from an official source but is really a cyber criminal trying to get the victim to disclose information or even login information that can be used against their company
- Water hole attacks are when a cyber criminal compromises or uses a fake website that a target might frequent in order to either gather data or compromise the targets device
- Compromised or impersonated emails are usually different from phishing attempts in that it’s the compromised email or impersonation of a higher up or C-suite executive being used to get a lower position employee to carry out what might seem like a normal function of the company but in reality is opening the door to the cyber criminal
- A physical social engineering attempt might look like just charming or convincing a security guard or secretary to let you into an area with sensitive data or servers hosting such data
- And finally USB baiting is simply the act of leaving a USB that has malware on it or device compromising software on it on hope that someone plugs it into their device or a corporate system

Who is usually targeted and effected?

- Generally speaking, the most common targets are CEOs of large companies, or positions that could have access to important information.
- The elderly, as they are usually not aware of best practices when it comes to analyzing text messages, phone calls or emails received.
- People who get successfully socially engineered tend to either have a lack of knowledge regarding cybersecurity, and are hence easy targets for bad actors.
- If an important member of a company who may have access to vast amounts of PII is targeted, all customers or owners of the PII will be affected, with their information possibly being sold through internet black markets or just used as ransom.

How is social engineering acted out at present?

- Software based social engineering attacks commonly take place via modern messaging services such as email, phone calls and direct messaging platforms. These types of attacks are prevalent on messaging apps like Discord, WhatsApp, and Messenger.
- Text messages or emails from government agencies asking for money are among the most common forms of social engineering, enticing a victim to pay an amount of money lest they risk ‘breaking the law’.
- Physical social engineering attacks are usually done through USB baiting, but can also be done through rogue APs.
- The modern ubiquity of smartphones has made WiFi attacks extremely popular by intercepting traffic by making a malicious device act as a trusted device.
- Preying on lower level employees as seen with recent attacks on a company Google has contracted with exposes the importance of proper cybersecurity training and safety practices being practiced by all within a company, no matter the level.

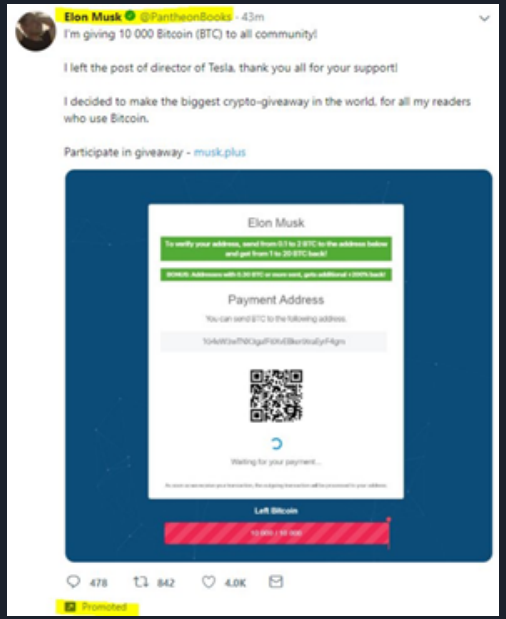
Case Study - 2020 Twitter Bitcoin Hack

The Attack

- On July 14th and 15th, a hacker group called Twitter IT Help Desk.
- Utilized social engineering methods like fraudulent websites to gain access to Twitter's network.
- Stole credentials to many coveted accounts and exchanged for bitcoin.
- Many important accounts were hijacked such as the National Weather Service account.

Total Loss

- Over $111,800 worth of bitcoin was lost in the attack
- Exposed a major vulnerability within Twitter, a major corporation during the hack.



Source: Twitter Investigation Report | Department of Financial Services

How to prevent social engineering

- Preventing social engineering requires a proactive blend of awareness, skepticism, and secure practices.
- The first and most critical step is education—individuals and organizations must understand the psychological tactics attackers use, such as impersonation, urgency, and emotional manipulation.
    - Regular training sessions and simulated phishing exercises help reinforce this awareness and prepare people to recognize suspicious behavior.
- Technical defenses also play a role: multi-factor authentication, email filtering, and access controls can reduce the impact of a successful attack.

However, technology alone isn't enough. People must be taught to verify identities before sharing sensitive information, avoid clicking on unsolicited links or attachments, and report unusual requests—even if they appear to come from trusted sources.

Cultivating a culture of caution, where employees feel empowered to question and verify, is essential.

Ultimately, the goal is to make every individual a strong link in the security chain, because even one person falling for a social engineering ploy can compromise an entire system.

Conclusion

- Social engineering is a leveraging of human interaction/emotions for an attackers benefit
- Targeted individuals include: CEOs, high rankings, and elderly people, but that doesn't mean YOU can't be targeted
- Common methods include texting, e-mail, and voice
- 2020 Twitter breach, which was caused by tricking users with a fake webpage
- Prevention includes education, hands-on training, MFA, e-mail filtering
- Make every individual a strong link in the security chain