SOCIAL ENGINEERING

-SOHRAB ARDESHAR VAKHARIA

THE ART OF MANIPULATING HUMANS

- Social engineers are interested in gaining information they can use to carry out actions such as identity theft or stealing passwords, or in finding out information for later use.
- Social engineering is considered as an art of convincing the target to reveal information (vital information).

HOW SOCIAL ENGINEERING WORKS?

- Trust
- Moral Obligation
- Threat
- Unexpected rewards
- Ignorance

WHY IT WORKS?

- Lack of technical knowledge
- Insufficient security policies on online portals
- Less awareness
- It is difficult to detect
- Humans trust others (good and bad at the same time)
- Human routine and habits

IMPACTS OF SOCIAL ENGINEERING

- Loss of money
- Physical violence
- Privacy compromise
- Loss of goodwill
- Much more..

COMMON TARGET PLACE

The social Network

GAME TIME

- Password hack-game
- Social profile information gaining

PHASES OF SOCIAL ENGINEERING

- Select a target
- Footprinting
- Reconnaissance
- Analysing the information
- Planning the attack
- Attack
- Clearing the tracks

THE CASE OF ANNA KOURNIKOVA

- This particular scam is a tried-and-true mechanism for getting information from an individual or causing harm in other ways. A good example of another form of this type of attack is the Anna Kournikova computer worm from 2001. This worm lured victims by promising nude pictures of the popular model and tennis star; but when users opened the attachment, they executed a computer worm. The worm forwarded the message to everyone in the victim's Outlook address book and started the process all over again.
- Interestingly, the worm and its delivery mechanism were created with a shrinkwrapped malware maker downloaded from the Internet.

FEW EXAMPLES

- **Test Your IQ** This type of scam attracts you with a quiz. Everybody loves quizzes. After you take the quiz, you are encouraged to enter your information into a form to get the results. In other cases, the scam encourages you to join an expensive text-messaging service, but the price appears only in extremely small print.
- **Tweet for Cash!** This scam takes many forms. "Make money on Twitter!" and "Tweet for profit!" are two common come-ons that security analysts say they've seen lately. Obviously this scam preys on users' greed and curiosity, but in the end they lose money or their identities.
- **Ur Cute. Msg Me!** The sexual solicitation is a tactic spammers have been trying for many years via e-mail and is one that has proven wildly successful. In the updated version of this ruse, tweets feature scantily clad women and include a message embedded in the image, rather than in the 140-character tweet itself.
- **Amber Alert Issued!!** This one is not so much as scam as it is a hoax. Amber alerts are pasted into status updates that turn out to be untrue. Although such attacks don't gain information, they are designed to cause panic and concern as well as increase traffic among recipients.

TYPES OF SOCIAL ENGINEERING

- Computer based
  - Malwares
  - Online information gathering (social networks, readily available information, whois)
  - Deploying an online campaign (fake one)
  - Phising
- Non-computer based (Human based)
  - Shoulder surfing
  - Eveasdropping
  - Dumpster diving
  - Impersonation

FEW MORE ADDED ATTACKS

- Reverse Social engineering
  - Show a problem to victim
  - Impersonate as an authorised personnel
  - Gain trust and access sensitive information
  - Exploit
- Piggybacking or tailgating
  - Attacker waits for authorised person gain entry and tailgates behind or piggyback behind to authorised access. (session hijacking)

MOBILE APPS

- Fake apps
- Trojans applications
- In app advertising

SOCIAL ENGINEERING COUNTERMEASURES

- Delete any request for financial information or passwords.
- Reject requests for help or offers of help.
- Keeping spam filters
- Don’t open untrusted emails
- Lock your laptops and mobile phones
- Deploy a good paid anti-malware software
- Read privacy policies (which we usually just accept)
- Do not and never give away your passwords to anyone
- Do not trust anyone online blindly. Do verify

1. Shark Tank, 2020

- Shark Tank television judge Barbara Corcoran was tricked in a nearly USD 400,000 phishing and social engineering scam in 2020. A cybercriminal impersonated her assistant and sent an email to the bookkeeper requesting a renewal payment related to real estate investments. He used an email address similar to the legitimate one. The fraud was only discovered after the bookkeeper sent an email to the assistant's correct address asking about the transaction.

SOCIAL ENGINEERING INCIDENTS

Source: https://gatefy.com/blog/7-real-and-famous-cases-social-engineering-attacks/

2. Toyota, 2019

- Toyota Boshoku Corporation, an auto parts supplier, was the victim of a social engineering and BEC (Business Email Compromise) attack in 2019. The money lost amounts to USD 37 million. Using persuasion, attackers persuaded a finance executive to change recipient's bank account information in a wire transfer.

SOCIAL ENGINEERING INCIDENTS

Source: https://gatefy.com/blog/7-real-and-famous-cases-social-engineering-attacks/

3. Cabarrus County, 2018

- Due to a social engineering and BEC scam, Cabarrus County, in the United States, suffered a loss of USD 1.7 million in 2018. Using malicious e-mails, hackers impersonated county suppliers and requested payments to a new bank account. According to the investigation, after the money was transferred, it was diverted to several accounts. In the emails, the scammers presented apparently legitimate documentation.

SOCIAL ENGINEERING INCIDENTS

Source: https://gatefy.com/blog/7-real-and-famous-cases-social-engineering-attacks/

4. Ethereum Classic, 2017

- Several people lost thousands of dollars in cryptocurrency after the Ethereum Classic website was hacked, in 2017. Using social engineering, hackers impersonated the owner of Classic Ether Wallet, gained access to the domain registry, and then redirected the domain to their own server. Criminals extracted Ethereum cryptocurrency from the victims after entering a code on the website that allowed them to view private keys that are used for transactions.

SOCIAL ENGINEERING INCIDENTS

Source: https://gatefy.com/blog/7-real-and-famous-cases-social-engineering-attacks/

5. Sony Pictures, 2014

- After an investigation, the FBI pointed out that the cyberattack on Sony Pictures, in 2014, was the responsibility of the North Korea government. Thousands of files, including business agreements, financial documents and employees' information, were stolen. Sony Pictures was targeted by spear phishing attacks. It appears employees were lured by fake Apple emails.

SOCIAL ENGINEERING INCIDENTS

Source: https://gatefy.com/blog/7-real-and-famous-cases-social-engineering-attacks/

RANSOMWARE

- Ransomware is a form of *malware* that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.
- Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

PREVENTION

- Update your operating system periodically with all the essential security updates and patches
- Don’t install illegit soft-wares
- Use anti-malwares
- Backup essential data.
  - Use online secure back-ups

THANK YOU

-SOHRAB ARDESHAR VAKHARIA