University of halabja

College of science

Computer science Department

Forth stage- First semester

Social engineering
Chapter 2

Prepared by:
karzan kamaran & muhamad star

Supervised and Editor:
Bilal H.Ali

Outline

- **Social engineering**
- **How Does Social Engineering Work?**
- **Traits of Social Engineering Attacks**
- **Types of Social Engineering Attacks**
- **How to Spot Social Engineering Attacks**
- **Social engineering prevention**

Social engineering

What is social engineering?

- Social engineering is the act of exploiting human weaknesses to gain access to personal information and protected systems. Social engineering relies on manipulating individuals rather than hacking computer systems to penetrate a target's account.

Generally, social engineering attackers have one of two goals:

- Sabotage: Disrupting or corrupting data to cause harm or inconvenience.
- Theft: Obtaining valuables like information, access, or money.

The five Phases of Social Engineering

- **Attack formulation:** The first phase consists of identifying the goal and in accordance, identifying the target necessary to fulfill the goal.
- **Information gathering:** In this stage, social engineers assess and identify potential information sources and begin the information gathering and assessment.
- **Develop a relationship:** In this stage, the social engineers establish a line of communication and begin to build a relationship.
- **Exploit the relationship:** In this phase, the target is “primed”. The exploitation stage uses different methods of manipulation to evoke the right type of emotions and prime the target to the right emotional stage. Once the target is in the right stage, the social engineer will start bringing out information from the target.
- **Execution:** During the execution phase of the attack, Generally, it is better to act in the stage of the attack in such a way that the intended person (victim) feels that he has done a good job for another person (attacker) and there is a possibility of further interactions in the future.

Types of Social Engineering Attacks

1. Old-Fashioned Types of Social Engineering Techniques:
   - Direct approach
   - Social media –Facebook
   - Mail-outs

5. Mail-outs

- 6. Social media

1. Direct approach

Types of Social Engineering Attacks

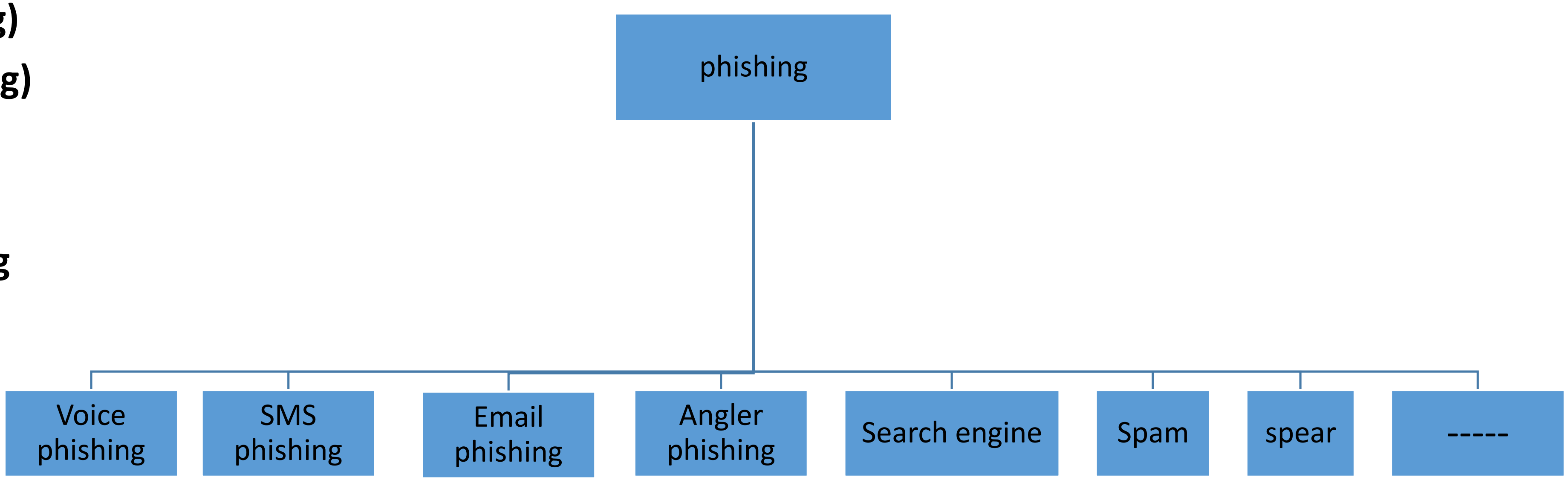
New-Fashioned Types of Social Engineering Techniques:

1. Phishing Attacks
2. Baiting
3. Quid pro quo
4. Scareware (Ransomware Attacks)
5. Physical Breach Attacks
6. Pretexting
7. Piggybacking
8. Tailgating
9. Pop-Up Windows
10. And other (Robocall attacks, ……)

Types of Social Engineering Attacks

1. **Phishing Attacks:** Phishing attacks occur when scammers use any form of communication (usually emails) to “fish” for information. These messages look identical to ones from trusted sources like organizations and people you know.

   - **Voice phishing (vishing)**
   - **SMS phishing (smishing)**
   - **Email phishing**
   - **Angler phishing**
   - **Search engine phishing**
   - **URL phishing**
   - **In-session phishing**
   - **Spam phishing**
   - **Spear phishing**



Types of Social Engineering Attacks

1. **Phishing Attacks:**
   - **Voice phishing (vishing):** phone calls may be automated message systems recording all your inputs. Sometimes, a live person might speak with you to increase trust and urgency.
   - **SMS phishing (smishing):** texts or mobile app messages might include a web link or a prompt to follow-up via a fraudulent email or phone number.
   - **Email phishing:** is the most traditional means of phishing, using an email urging you to reply or follow-up by other means. Web links, phone numbers, or malware attachments can be used.
   - **Angler phishing:** takes place on social media, where an attacker imitates a trusted company’s customer service team. They intercept your communications with a brand to hijack and divert your conversation into private messages, where they then advance the attack.
   - **Search engine phishing:** attempt to place links to fake websites at the top of search results.(SEO) These may be paid ads or use legitimate optimization methods to manipulate search rankings.

Types of Social Engineering Attacks

1. **Phishing Attacks:**

- **Spam phishing,** or mass phishing, is a widespread attack aimed at many users. These attacks are non-personalized and try to catch any unsuspecting person.
- **Spear phishing** and by extension, **whaling** , use personalized info to target particular users. Whaling attacks specifically aim at high-value targets like celebrities, upper management, and high government officials.
- **URL phishing:** links tempt you to travel to phishing websites. These links are commonly delivered in emails, texts, social media messages, and online ads. Attacks hide links in hyperlinked text or buttons, using link-shortening tools, or deceptively spelled URLs.
- **In-session phishing:** appears as an interruption to your normal web browsing. For example, you may see such as fake login pop-ups for pages you're currently visiting.

Types of Social Engineering Attacks

2. **Baiting**:
   - As its name implies, baiting attacks use a false promise to pique a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.

   Popular methods of baiting can include:
   - USB drives left in public spaces, like libraries and parking lots.
   - Email attachments including details on a free offer, or fraudulent free software
3. **Quid pro quo** is a term roughly meaning "a favor for a favor," which in the context of phishing means an exchange of your personal info for some reward or other compensation. Giveaways or offers to take part in research studies might expose you to this type of attack.
4. **Scareware** is a form of malware used to frighten you into taking an action. This deceptive malware uses alarming warnings that report fake malware infections or claim one of your accounts has been compromised.

A Ransomware attack involves six stages: (1) creating the malware; (2) deployment; (3) installation; (4) command and control; (5) destruction; and (6) extortion.

5. **Pretexting** Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

Types of Social Engineering Attacks

6. **Piggybacking and tailgating:** both refer to a type of attack in which an authorized person allows an unauthorized person access to a restricted area. This form of social engineering may happen at your place of work if you let someone follow you into the building. Or, it could happen at your apartment building as you're leaving for the day.

7. **Physical breaches** involve attackers appearing in-person, posing as someone legitimate to gain access to otherwise unauthorized areas or information. Attacks of this nature are most common in enterprise environments, such as governments, businesses, or other organizations. Attackers may pretend to be a representative of a known, trusted vendor for the company. Some attackers may even be recently fired employees with a vendetta against their former employer.

They make their identity obscure but believable enough to avoid questions. This requires a bit of research on the attacker's part and involves high-risk. So, if someone is attempting this method, they've identified clear potential for a highly valuable reward if successful.

8. **DNS spoofing** manipulates your browser and web servers to travel to malicious websites when you enter a legitimate URL. Once infected with this exploit, the redirect will continue unless the inaccurate routing data is cleared from the systems involved.

Unusual Social Engineering Methods

Unusual Social Engineering Methods: In some cases, cybercriminals have used complex methods to complete their cyberattacks, including:

1. **Fax-based phishing:** When one bank's customers received a fake email that claimed to be from the bank — asking the customer to confirm their access codes – the method of confirmation was not via the usual email / Internet routes. Instead, the customer was asked to print out the form in the email, then fill in their details and fax the form to the cybercriminal's telephone number.

2. **Traditional mail malware distribution:** In Japan, cybercriminals used a home-delivery service to distribute CDs that were infected with Trojan spyware. The disks were delivered to the clients of a Japanese bank. The clients' addresses had previously been stolen from the bank's database.

How to Spot Social Engineering Attacks

- Message Arrives Unexpectedly

There is almost never a time when the potential victim is expecting the message from the sender and certainly not about the involved subject. There are plenty of legitimate emails that arrive unexpectedly each day, but this is a key trait of most social engineering attacks.

- sender Asks Something Out of the Ordinary

In most cases, social engineering requests ask the potential victim to do something they have never done before.

- Requested Action is Potentially Harmful

Being asked to open documents, execute programs, send information or put in passwords, are all examples of potentially harmful actions.

How to Spot Social Engineering Attacks

- Attacker Attaches an Unusual File or URL

Most digital social engineering attacks include a rogue link the user is told to click on or a document or program they are instructed to download

The most common types of file formats used maliciously include: EXE, DLL, URL, SCR, HTA, HTM, HTML, MSI, SYS, ZIP, 7Z, BIN, CAB, CPL, and Microsoft Office document types (e.g., DOCX, XLSX, PPTX, etc.). You can find lots of "potentially dangerous file type lists on the Internet, including here. Attachments of fairly safe types of file formats (e.g., TXT, PDF, etc.) which do not include embedded URL links or "active content" are considered safer than others.

- Attacker Includes a Sense of Urgency

Most scams include a heightened sense of urgency.

How to Spot Social Engineering Attacks

- Are my **emotions heightened**?
- Did this message come from **a legitimate sender**?
- Did **my friend** actually send this message to me?
- Does the **website** I’m on have **odd details**?
- Does this **offer sound** too good to be true?
- Attachments or links **suspicious**?
- Can this person **prove their identity**?

Social engineering

- Mitigation Techniques
- **Prevention Techniques:**

Mitigation Techniques

- Human-based mitigation:Mitigating techniques for social engineering attacks aim at decreasing the attacks' impact on the individuals or the companies. They aim at saving what can be saved after a human is already attacked or a company's system is already hacked. (Build a positive security culture)

Human-based mitigation techniques are a must for companies to mitigate the social engineering attacks and minimize their impacts in exploiting employees' weaknesses and vulnerabilities. They are mainly related to the effective in decision making and acting to classify an activity as malicious and act as necessary. However, human decisions are relative and thus not efficient as the human judgment is subjective even with strong awareness of social engineering attacks

- Technology-based mitigation: Technology-based mitigation techniques are required to enhance the accuracy of the human-based mitigation techniques. There are four technology-based mitigation techniques: biometrics, sensors, artificial intelligence, and social honeypot. Biometrics-based techniques aim at counteracting physical impersonation attacks, Biometrics distinguish real employees from fake profiles through their biological traits. These unique traits can be fingerprint, facial recognition, eye print, and voice. Sensor-based technique entails using sensors to identify individuals.

Social engineering

- Prevention Techniques:

A list of defense procedures for social-engineering attacks include:

- security education and training.
- increasing social awareness of social-engineering attacks.
- providing the required tools to detect and avoid these attacks.
- learning how to keep confidential information safe.
- reporting any suspected activity to the security service.
- organizing security orientations for new employees.
- advertising attacks' risks to all employees by forwarding sensitization emails and known fraudulent emails.

For email-based attacks, some companies use the **honeypot** email addresses, also called **spamtraps**, to collect and publish the spams to employees. When an email is sent from one of the spamtraps list, the server considers it as malicious and bans it temporarily.

- being aware of unexpected and unsolicited calls
- For phishing attacks, anti-phishing tools have been proposed to **blacklist** and block phishing websites. Examples of these tools are McAfee anti-phishing filter, Microsoft phishing filter, and Web sense

Kali Linux: Top 5 tools for social engineering

- Maltego

Maltego is an OSINT (open-source intelligence) investigation tool that shows how different pieces of information are interlinked. With Maltego, you can find relationships between people and various information assets, including email addresses, social profiles, screen names and other pieces of information that link a person to a service or organization.

- Social Engineering Toolkit (SET)

Social Engineering Toolkit (or SET) is an open-source, Python-driven toolkit aimed at penetration testing around social engineering. SET has various custom attack vectors that enable you to set up a believable attack in no time.

SET includes a website tool that converts your Kali box into a web server with a range of exploits that can compromise most browsers. The idea is to send your target a link that routes them through your site, which automatically downloads and executes the exploit on their system.

Kali Linux: Top 5 tools for social engineering

- Wifiphisher

Wifiphisher is a unique social engineering tool that automates phishing attacks on Wi-Fi networks to get the WPA/WPA2 passwords of a target user base. The tool can choose any nearby Wi-Fi access point, jam it (de-authenticate all users) and create a clone access point that doesn't require a password to join.

- Metasploit MSF

Metasploit Framework is a penetration testing tool that can help you identify, exploit and validate vulnerabilities. It delivers the content, tools and infrastructure to conduct extensive security auditing along with penetration testing.

- MSFvenom Payload Creator (MSFPC)

MSFPC is a user-friendly tool that makes it easy to create basic payloads. It helps users avoid the need to write long msfvenom commands to generate payloads. With this generator, you can create payloads with a minimum of one argument.