Understanding social engineering attacks

1. Impersonation:
2. hacker impersonate administrator
3. Hacker impersonate user
4. Hacker impersonates management

## **Phishing: A Breakdown of Common Types**

Phishing is a type of cybercrime where attackers attempt to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal details. Here are some common types of phishing attacks:

### **Whaling**

* **Target:** High-profile individuals, such as CEOs, executives, or celebrities.
* **Tactics:** Attackers often impersonate trusted individuals or organizations to gain access to sensitive information or financial assets.

### **Vishing**

* **Method:** Voice phishing involves phone calls from scammers posing as legitimate entities, such as banks or government agencies.
* **Goal:** To trick victims into revealing personal information or financial details.

### **Smishing**

* **Method:** SMS phishing uses text messages to lure victims to malicious websites or to trick them into revealing sensitive information.
* **Tactics:** Scammers often create a sense of urgency or create a false sense of trust.

### **Spear Phishing**

* **Target:** Specific individuals or organizations.
* **Tactics:** Attackers research their targets to tailor their messages and make them appear more legitimate.

### **Spam**

* **Method:** Unsolicited emails sent in bulk to a large number of recipients.
* **Goal:** To promote products, services, or scams.

### **Eliciting Information**

* **Tactics:** Attackers may use various methods to gather information about their targets, such as social engineering, pretexting, or online research.
* **Purpose:** To identify vulnerabilities and tailor their attacks accordingly.

### **Prepending**

* **Method:** Adding a prefix to a legitimate email address to create a fake one.
* **Goal:** To trick recipients into believing the email is from a trusted source.

**Remember:** Be cautious of unsolicited emails, phone calls, or text messages, especially those that ask for personal information or require urgent action. If you

suspect a phishing attempt, do not click on any links or attachments, and report it to the appropriate authorities.

**Identity fraud** occurs when someone uses another person's personal information without their knowledge or permission. Here are some common types and related threats:

### **Invoice Scams**

* **How it works:** Scammers send fraudulent invoices to businesses, often with a sense of urgency, hoping the recipient will pay without verifying the authenticity.
* **Related threats:** Financial loss, supply chain disruptions, and damage to reputation.

### **Credential Harvesting**

* **How it works:** Attackers use various techniques, such as phishing, malware, and social engineering, to collect login credentials for online accounts.
* **Related threats:** Identity theft, unauthorized access to sensitive information, and financial loss.

### **Reconnaissance**

* **How it works:** Attackers gather information about their targets, including their networks, systems, and personnel.
* **Related threats:** Targeted attacks, data breaches, and disruption of operations.

### **Influence Campaigns/Hybrid Warfare**

* **How it works:** States or non-state actors use a combination of traditional and non-traditional warfare tactics to influence public opinion, undermine democratic institutions, and destabilize governments.
* **Related threats:** Erosion of trust, political instability, and national security risks.

# **Comparing the Topics: A Brief Overview**

While each topic mentioned above is related to cybersecurity and digital threats, they have distinct characteristics:

### **Phishing vs. Identity Fraud**

* **Phishing:** Primarily focuses on tricking individuals into revealing personal information.
* **Identity Fraud:** Involves the unauthorized use of someone else's personal information.

### **Invoice Scams vs. Credential Harvesting**

* **Invoice Scams:** Target businesses with fraudulent invoices.
* **Credential Harvesting:** Aims to collect login credentials for online accounts.

### **Reconnaissance vs. Influence Campaigns**

* **Reconnaissance:** Gathering information about targets for potential attacks.
* **Influence Campaigns:** Using various tactics to manipulate public opinion or destabilize governments.

### **Whaling, Vishing, Smishing, Spear Phishing, and Spam**

* **Whaling, Vishing, and Smishing:** Specific types of phishing attacks targeting high-profile individuals, using voice calls, or text messages.
* **Spear Phishing:** Tailored phishing attacks targeting specific individuals or organizations.
* **Spam:** Unsolicited bulk emails.

### **Eliciting Information and Prepending**

* **Eliciting Information:** Gathering information about targets for future attacks.
* **Prepending:** Adding a prefix to a legitimate email address to create a fake one.

**In summary,** while there are overlaps and connections between these topics, they represent different aspects of cybercrime and digital threats. Understanding these distinctions is crucial for effective cybersecurity measures.

**Shouldering**

**Tailgating:**

Doortrap

**Hoaxes**: false story and asking the user to take some type of action.

## **Physical Attacks:**

* Malicious universal serial bus cable
* Malicious flash drive
* Card cloning : credit card stealing
* Skimming