LEMUEL OKECHUKWU

VEPH/20B/CY082

TASK 25B

SOCIAL-ENGINEERING

**TASK 25B:**

* Provide a comprehensive explanation of various social engineering attack techniques—including phishing, vishing, smishing, whaling, spear phishing, impersonation, pretexting, tailgating, dumpster diving, typosquatting, and watering hole attacks—and discuss the mechanisms behind each method as well as best practices and technical controls for their prevention?"

[](https://www.knowbe4.com/what-is-social-engineering-old)

Social engineering attacks exploit human psychology rather than technological weaknesses to gain unauthorized access to sensitive information or systems.

**How Did Social Engineering Attacks Evolve?**

Despite the existence of so many modern social engineering examples, the practice actually has a long history—dating back to the 18th century.

**French noblemen**

After the French Revolution, prisoners in France falsely claiming to be valets for French noblemen sent out letters that claimed they had hidden their master's vast treasure and would provide a map to help the recipient find it. In return for this “priceless” information, they would request a modest amount and hoped for a little preferential treatment.

While computers were centuries from being invented, this kind of scam certainly fit the common social engineering definition.

**European nobleman**

These kinds of early social engineering attacks continued with a similar prison-based scam involving someone incarcerated in Spain.

The convicted would write a letter claiming to be a European nobleman who had been wrongly imprisoned. The bars not only kept him from freedom but also from his impoverished daughter, who needed him free to survive. The letter would ask the recipient for enough money to secure the prisoner’s release while promising a handsome payment—far more than what the recipient provided—as soon as the prisoner saw the light of day.

**Nigerian prince**

What is social engineering today?

As time passed, the technologies and text changed but the psychological manipulation did not—as could be seen in the Nigerian Prince scam.

The social engineering toolkit for this scam simply involves an email account and some faked documents. Someone pretending to be a Nigerian prince claims there is money locked away that they cannot access without help. If the recipient gives them the cash they need to bribe officials or pay the fee needed to gain access to the funds, the “Prince” will share the loot with the recipient. Of course, there never is any money at all, and anything the target wires never gets returned.

To defend against **social engineering attacks,** it’s crucial to understand **3 main steps**attackers follow:

**1. Discovery and Investigation**: Attackers start by gathering information, often through social media, public records, or even dumpster diving. They collect details like email addresses and job roles to make their attack more convincing.

**2. Deception and Hook.**: Using that information, attackers craft a scenario that plays on emotions—like a fake urgent email from your bank or a coworker in need. The goal is to make you act without thinking.

**3. The Attack.**: Finally, they get you to take action, like clicking a malicious link or sharing sensitive data. This can lead to **data theft, financial loss**, or a [cybersecurity breach.](https://keepnetlabs.com/blog/lessons-from-5-of-the-biggest-cybersecurity-breaches-in-history)

**Common Types of Social Engineering Attacks**

**Phishing: R**emains one of the most dangerous and prevalent **social engineering** methods. Attackers send fraudulent emails, often appearing to be from trusted sources like banks or colleagues, to trick users into providing sensitive information. These phishing attacks usually direct victims to fake websites where their credentials are harvested.

**Spear Phishing:** Unlike regular phishing, [spear phishing](https://keepnetlabs.com/blog/what-is-spear-phishing-and-how-to-prevent-it) is more personalized. Attackers research their targets and tailor the message to appear more credible. For instance, the attacker might mention specific company projects or impersonate someone familiar to the target, making the scam harder to detect.

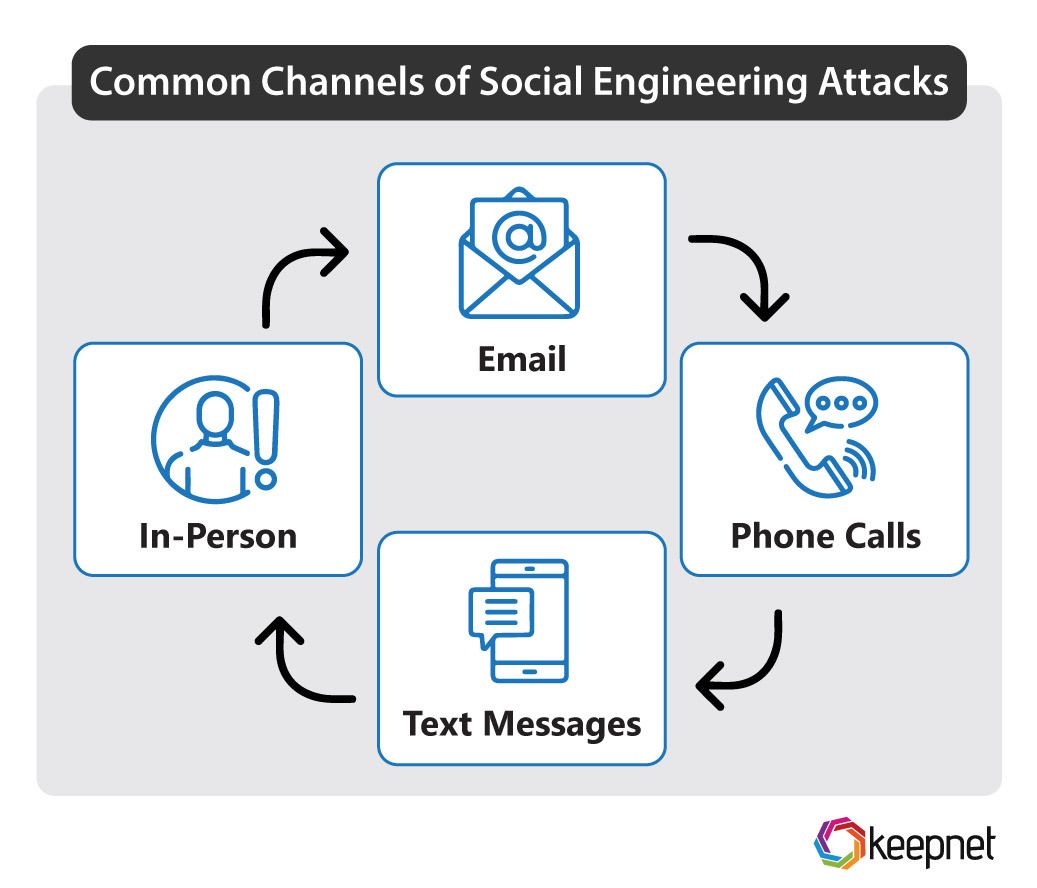
**Vishing:** Short for **voice phishing**, involves attackers using phone calls to deceive individuals. The caller often poses as someone from a trusted entity, such as your bank or IT department. They may claim there’s an urgent security issue and persuade you to reveal personal information, such as passwords or social security numbers.

**Smishing:** Similar to vishing, [smishing](https://keepnetlabs.com/blog/top-7-examples-of-smishing-attacks-and-how-to-stay-safe) involves **social engineering attacks** via text messages. Attackers may send an urgent message pretending to be a financial institution or delivery service. Clicking a link in the text can lead to malware installation or direct victims to a fake website to steal credentials.

**Pretexting:** Attackers create a fabricated scenario or pretext to obtain personal or organizational information. For example, the attacker may pose as an HR representative requesting sensitive details from employees. The strength of **pretexting**lies in the attacker’s ability to create a plausible scenario that appears genuine.

**Baiting: C**apitalizes on human curiosity by offering something enticing—like free software downloads or USB drives left in public places. Once the victim takes the bait, malicious software is installed, compromising their systems. **Baiting** often results in malware infections or unauthorized access to corporate networks.

**Tailgating:** Also known as **piggybacking,**[tailgating](https://keepnetlabs.com/blog/what-is-a-tailgating-attack)is a **social engineering attack**that exploits physical security flaws. In this case, the attacker physically follows someone into a restricted area without proper authorization. This method is particularly dangerous in secure facilities where unauthorized access could lead to data theft or sabotage.



**Watering Hole attacks:** A “watering hole” attack infects frequently visited websites of a specific industry or user group, leading them to a malicious site.The term “watering hole” originates from the presence of predatory animals that loiter around them, preying on unsuspecting targets.Although watering hole attacks, also known as strategic website compromise attacks, are subject to chance, they can be significantly more effective when combined with email prompts that entice users to the targeted websites. Attacks on watering holes are not common; they have a high success rate.

**Dumpster diving**: May be the least sophisticated attack of them all, but it's a form of social engineering nonetheless. It involves going through a target company's garbage to find discarded information, like bank account statements or old hardware, that can be used to gain unauthorized access or information.

**Typosquatting**: This involves registering domain names that are similar to legitimate websites, often with slight misspellings, to trick users into visiting the malicious site instead of the intended one. Typosquatting can be used to distribute malware or steal sensitive information.

**How to Protect Yourself from Social Engineering Attacks?**

* Set up reliable data backups and regular repair for important data repositories. Set up thorough backup methods to protect important data effectively.
* Encryption should be the top goal when improving security for sensitive data.
* Even though your business probably already has a firewall, a next-generation web application cloud-based firewall is made to protect against social engineering attacks in the best way possible.
* A common part of social engineering is creating a sense of urgency. The attacker hopes that the target won’t think much about what’s going on. So, taking a moment to think can stop these attacks or show them up as fakes for what they are.
* If your email program doesn’t flag suspicious emails or screen out enough spam, you may need to change the settings.
* Effective spam filters use many different kinds of information to figure out which emails are likely to be spam. Even if hackers get a hold of your data, emails, and other forms of contact, they won’t be able to read the information in them. You can do this by getting SSL certificates from sources that people trust.

Social engineering attacks exploit human vulnerabilities to gain unauthorized access to networks or sensitive data, resulting in identity theft, financial loss, and system compromise. To safeguard against such threats, businesses should implement measures like strong passwords, two-factor authentication, encryption, network activity monitoring, and employee training.