Cyber Security

Lab 3 - Explore Social Engineering Techniques

Fullname: Amangeldi Zhanserik
ID: 22B030301
E-mail: zha_amangeldi@kbtu.kz
Date of submission: 05/02/2025
Class time: Thursday, 15:00–18:00

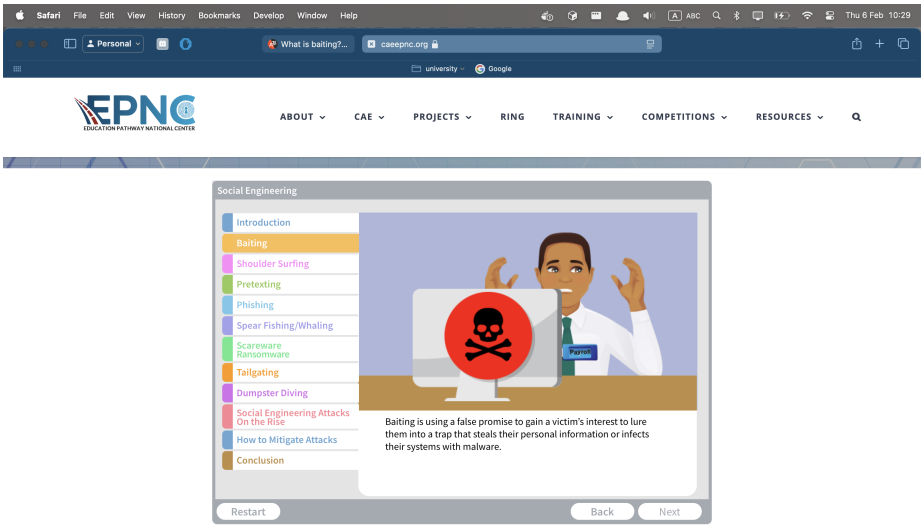
School of Information System and Engineering
Kazakh-British Technical University
Academic Year 2024-2025

Part 1. Explore Social Engineering Techniques

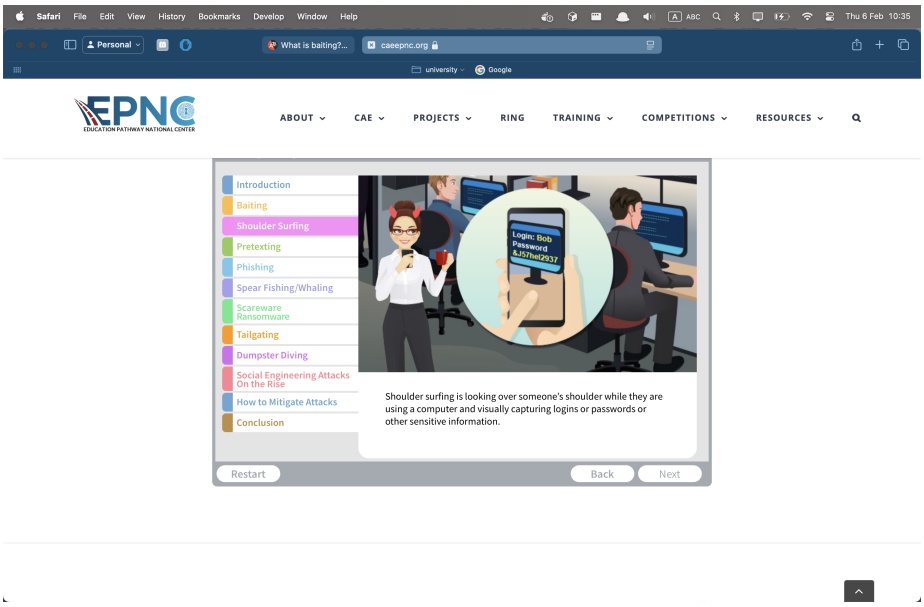
Step 1: Explore Baiting, Shoulder Surfing, and Pretexting.

Question 1: What is baiting? Did you click on the USB drive? What happened to the victim's system?

Answer: Baiting is a social engineering attack that relies on the curiosity or greed of the victim. In interactive game I clicked to the USB drive and it leading to the installation of malware on the victim's system.

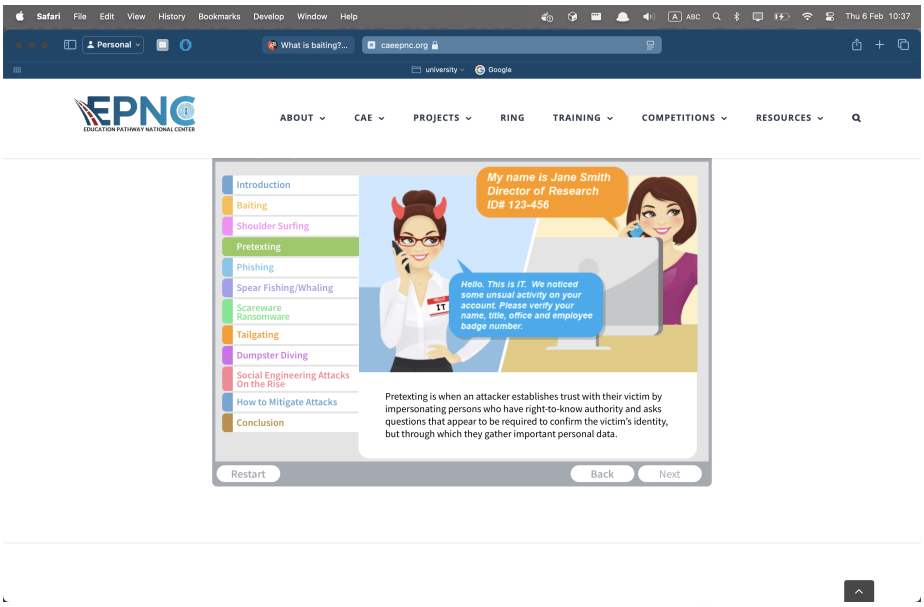


Question 2: What is Shoulder Surfing? What device was used to perform shoulder surfing? What information was gained?
Answer: Shoulder surfing is a social engineering attack that involves looking over someone's shoulder to get information. In the interactive game, a smartphone was used to perform shoulder surfing. The information gained was the victim's login and password.



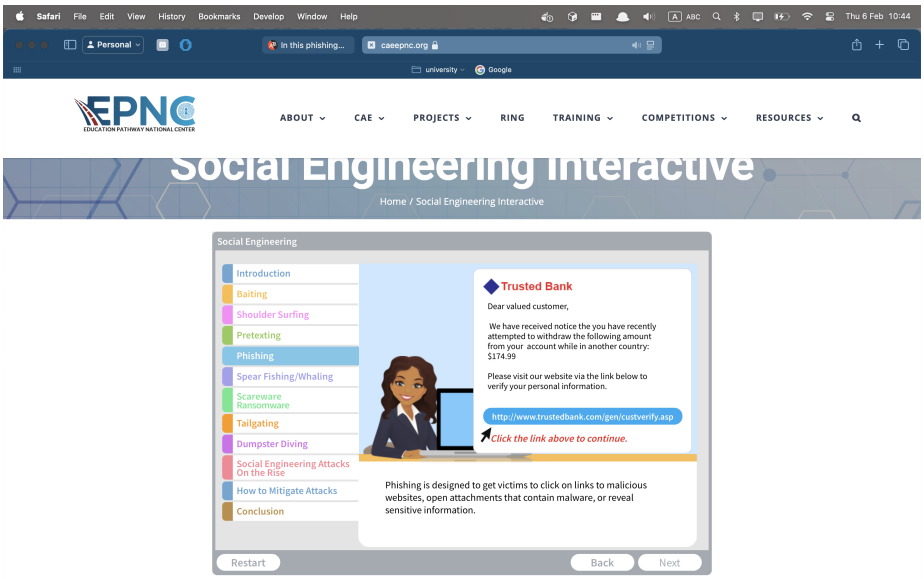
Question 3: What is Pretexting? What type of information did the cybercriminal request? Would you fall victim?

Answer: Pretexting is a social engineering attack that uses deception to create a scenario to convince victims to divulge information they should not divulge. In the interactive game, cymbercriminal requested the name, title, office and employee badge number. And yes I fall victim.



Step 2: Explore Phishing, Spear Phishing, and Whaling

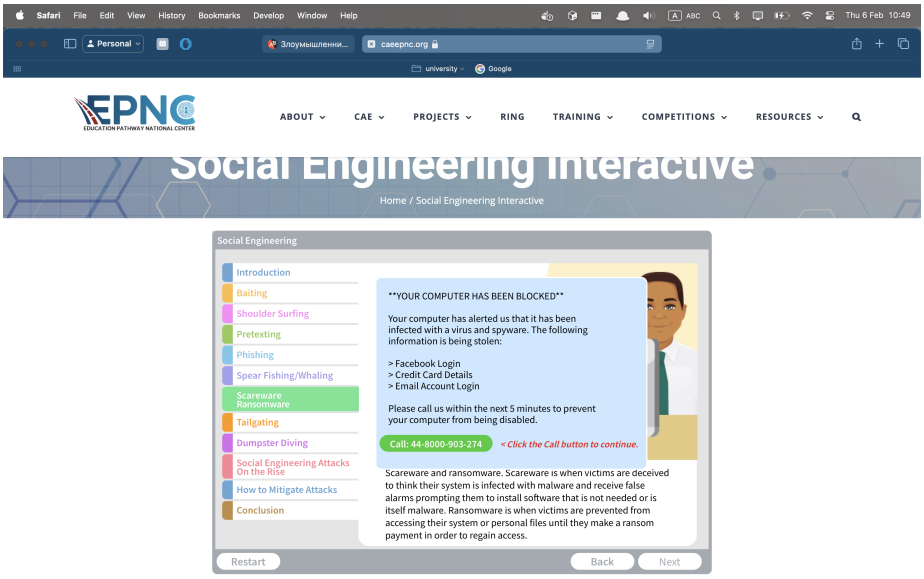
Question 1: In this phishing example, what is the ploy the attacker uses to trick the victim to visit the trap website? What is the trap website used for?
Answer: The attacker pretended to be a trusted bank and asked to confirm whether he would withdraw money from the account, the victim fell for it and went to the phishing site and entered his secret data from the bank account.



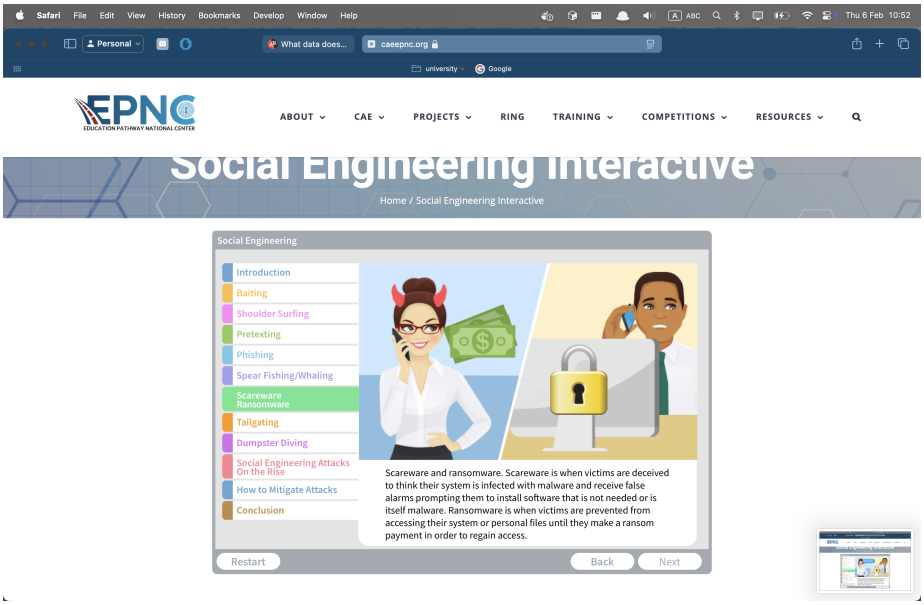
Question 2: What is the difference between phishing and spear phishing or whaling?
Answer: Phishing is a type of social engineering attack that targets a large number of people, while spear phishing is a more targeted version of phishing that targets specific individuals or enterprises. Whaling is a type of spear phishing that targets high-profile employees such as CEOs or CFOs.

Step 3: Explore Scareware and Ransomware

Question 1: What data does the attacker claim to have in this example? Would you fall for this deception?
Answer: Was claimed data about facebook login, credit bank account and email account. No i never fall for this deception.



Question 2: What is the attacker requesting the victim do to get the data back?
Answer: The attacker is requesting the victim to pay a ransom to get the data back.



Question 3: What is tailgating?
Answer: Tailgating is a social engineering attack that tricks the victim into helping the attacker gain unauthorized access to the organization's physical facilities.

Question 4: Give three ways to prevent social engineering attacks?
Answer:

1. Always verify the identity of the person requesting sensitive information, either through a phone call or in-person verification.

2. Do not click on links or download attachments from unknown or suspicious emails.

3. Regularly update and patch your software and systems to protect against known vulnerabilities.