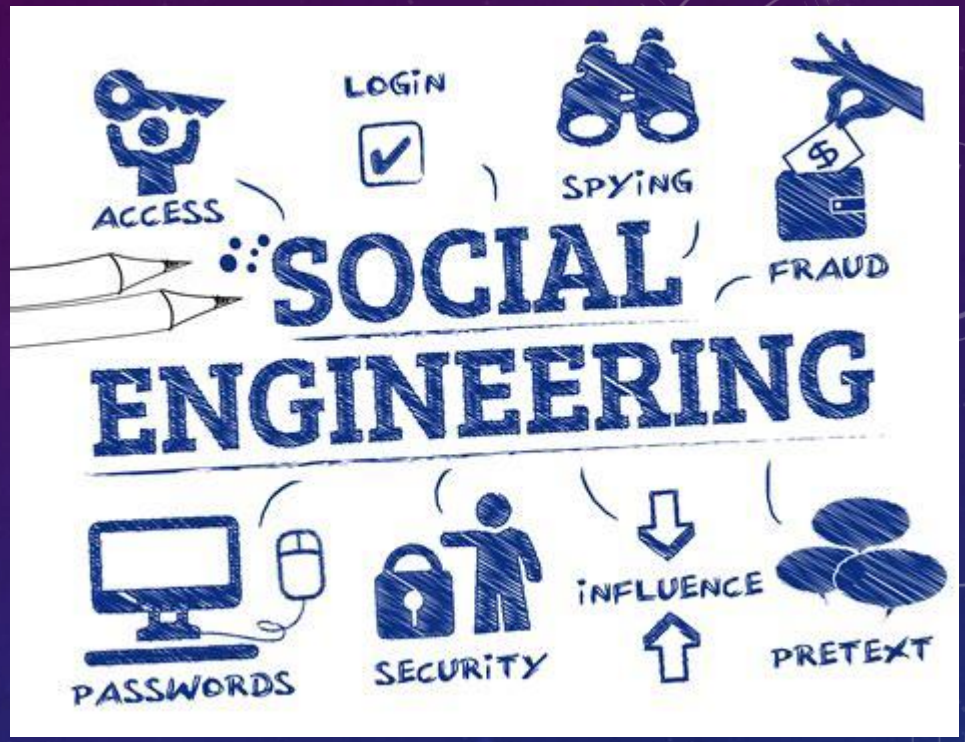
CYBERSECURITY AND SOCIAL ENGINEERING

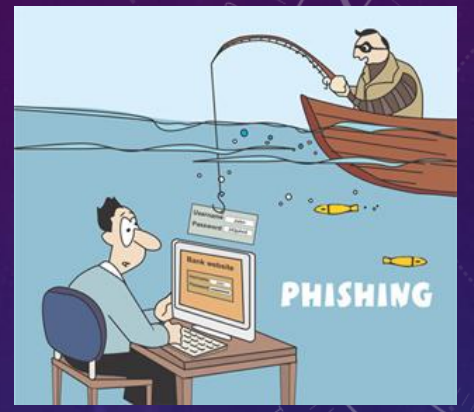
BY STEPHEN PRICE

INTRODUCTION

Social engineering is a tactic used by cybercriminals that exploits human psychology rather than technical vulnerabilities. Cybercriminals manipulate people into exposing their personal information to them like passwords and banking information.



TYPES OF SOCIAL ENGINEERING ATTACKS



The most common types of social engineering attacks include:

Phishing: Attackers deceive people through emails to seek their information and data.

Pretexting: Offender impersonates a person with power (police officer or boss) trying to get information.

Baiting: Attackers exploit human curiosity or desire by offering them something like free software or infected USB drives to trick them into compromising their security.

Tailgating: Someone follows a person physically into a space and steals their personal information.

Smishing: Attackers deceive people through text messages to seek their personal information.

Vishing: Attackers deceive people through voice messages to seek their personal information.

References: CYSE201S MODULE 10 Powerpoint

HOW ATTACKERS EXPLOIT HUMAN BEHAVIOR

Authority: Victims of social engineering attacks tend to comply when request come from authority figures.

Scarcity: Victims may be offered something that's they need, or it's limited without taking into consideration.

Reciprocation: Victims feel like they got to return the favor if someone offers them something.

EXAMPLES OF SOCIAL ENGINEERING ATTACKS IN THE REAL WORLD

- Phishing: Attackers had exploited google calendar's default setting that automatically adds events, so they send calendar invites to people to baited them into revealing their personal information to attackers.
- Reference: Arntz, P. (2025, November 21). *Fake calendar invites are spreading. Here's how to remove them and prevent more*. Malwarebytes. https://www.malwarebytes.com/blog/news/2025/11/fake-calendar-invites-are-spreading-heres-how-to-remove-them-and-prevent-more
- Pretexting: An HR Staff member who worked for snapchat was targeted where the attacker impersonated Snapchat's CEO and request employee payroll information from the HR staff member. The attacker was successful in deceiving the HR staff member and gains access to their personal data.
- Reference: *Snapchat falls hook, line & sinker in phishing attack: Employee data leaked after CEO email scam - Tech Monitor*. (2016, February 29). Tech Monitor. https://www.techmonitor.ai/hardware/data-centres/snapchat-falls-hook-line-sinker-in-phishing-attack-employee-data-leaked-after-ceo-email-scam-4824852?cf-view
-

SOCIAL ENGINEERING IMPACT ON SOCIETY AND RELATIONS TO SOCIAL SCIENCE

- Social engineering is related to social science theories like psychodynamic theory, behavioral theory, and cognitive theories. It's possible that criminals who engage in social engineering attacks can be influence from experiences in their early childhood or they learn it from somebody depending on the environment they are around.
- It can impact victims of social engineering causing them to have stress, anxiety, identity theft, and financial loss.
- References: CYSE 201S Module 5 Powerpoint

WAYS TO PREVENT SOCIAL ENGINEERING ATTACKS

Implement least privilege access

Implement multi factor authentication

Firewalls

Cyber hygiene through early education

Training in the workplace that raises awareness

Regular Security Audits

Incident Response Plan

References: CYSE 201S Module 10 Powerpoint

THANK YOU FOR YOUR TIME!