SOCIAL ENGINEERING IN CYBERSECURITY

Created by: Matthew Fox

WHAT IS SOCIAL ENGINEERING?

The term "Social Engineering" is used as an umbrella term that refers to various malicious activities done on the internet through the use of human interaction.

Most of the tactics used rely on taking advantage of the victim's emotions. Attackers make an attempt to force the victim to think one way in order to steal information from them while they are not thinking straight.

Breaking into physical places using Social Engineering is a common job; it helps prevent unauthorized people from walking into a building because they look like they belong.

There is no "main" way to do Social Engineering; the context of a situation matters, as someone may fall for one scam but not the other.

Some of the common ways people use Social Engineering are through Phishing, Fraud, Vishing, Deepfakes, and Scareware.

SOME EXAMPLES OF SOCIAL ENGINEERING ATTACKS

Phishing

Creating emails that look legit (or from a reputable source) to ease the guard of the victim and make them reveal personal information.

Scareware

Attempting to think that the victim was already hacked, so they are panicked and will not think correctly.

Vishing

Similar to phishing, this tactic uses voicemail or phone calls, and may also be backed up with AI.

Deepfakes

Using Artificial Intelligence to create realistic videos and images with the purpose of manipulating someone's way of thinking.

WHAT CAN BE DONE TO PREVENT FUTURE ATTACKS?

- For an organization, multiple things can be done:
  - Education is vital; knowing how to identify scams already is a big boost
  - Multiple authentication features like 2FA or Duo Mobile
  - Maintaining logs of activities can help identify interlopers
- Having a secure physical building is key too. Nobody should be able to walk into a building.
- Encryption of data can prevent potentially sensitive information from being leaked
- Always updating your systems will reduce the amount of exploits that can leak through

CONCLUSION AND REFERENCES

- Although Social Engineering may look easy to identify, the criminals know this and will attempt to force you into a certain state of mind to easily take advantage of you.
- There are many methods that criminals use to gain access to your sensitive information; however, if you keep calm and think twice, many of these incidents can be avoided.

References

What is Social Engineering? | IBM

The 13 Most Common Types of Social Engineering Attacks in 2025 + How to Defend Against Them

What is Social Engineering? Working, Types, Prevention, and Impact - GeeksforGeeks