Social Engineering

Definition

The use of deception to manipulate Individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Types of Attacks:

PHISHING

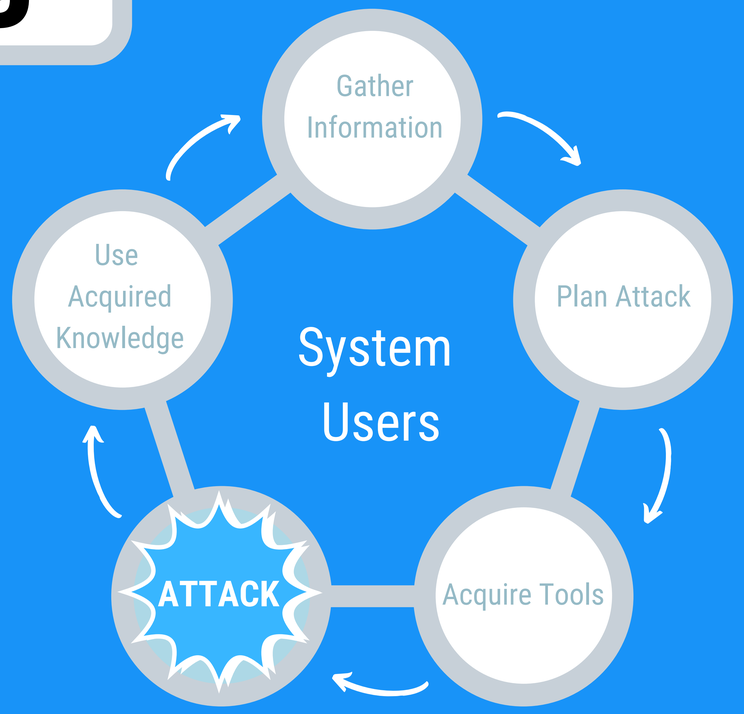
SPEAR PHISHING

VISHING

SMISHING

SOCIAL MEDIA MINING

Social Engineering Cycle



Social Engineering Stats

1. 3% of malware is meant to exploit a technical flaw. The rest is to trick a user through a scam.
2. 63% of data breaches come from internal sources, control errors, or fraud.
3. 15% of people successfully scammed will be targeted at least one more time within the year.
4. 97% of people aren't even able to recognize when they are being targeted in the first place!

27% of employees clicked an emailed phishing link, making it the most effective method of social engineering.

(www.techrepublic.com)

How you can help Princeton:

- Contact the SOC with questions.
- Utilize the power of the phish bowl.
- Never give out your credentials.
- Always verify sources are legitimate.

Tips for Avoiding a Social Engineering Attack

☑ **LIMIT PUBLIC INFORMATION:**
Limit the amount of personal information that you share online.

☑ **BE SKEPTICAL:**
Always question requests for sensitive information.

☑ **TRUST BUT VERIFY:**
Don't share information with people you don't know unless you can verify their identity.

☑ **CALL THEM BACK:**
Research and contact the company directly.

☑ **NO PASSWORDS OVER THE PHONE:**
Never share your password over the phone.