SOCIAL ENGINEERING

What is social engineering

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Baiting

Baiting attacks use a false promise to pique a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.

Phishing

Phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

Quid Pro Quo

Quid pro quo involves a hacker requesting the exchange of critical data or login credentials in exchange for a service.

Pretexting

Attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task. The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data.

WHAT TO DO :

- Delete any request for personal information or passwords.
- Reject requests for help or offers of help.
- Set your spam filters to high.
- Secure your devices.
- Always be mindful of risks.

[COMNETS]
http://www.comnets.ilkom.unsri.ac.id

Department of Computer Engineering
University of Sriwijaya