Social Engineering

Dilpreet Singh Bajwa

Dated: 30-6-18

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access. (Wikipedia)

Social Engineering is one of the first tactic among hackers/attackers because it is always easy to take advantage of user's weakness than to find a vulnerability in the system and exploit it.

For example: Attacker might call you and pretend to be an official from bank and ask you to share your confidential information like pin or card number.

Various types of social engineering attacks possible like: Baiting, Phishing, Spear phishing, Vishing, Tailgating, Quid-pro-quo, Honey Trap etc.

How to prevent yourself from Social Engineering Attack:

- **Be alert and aware.**
- **Don't open emails and attachments from un-trusted sources.**
- **Always use multifactor authentication like password and OTP both for your online accounts.**
- **Always install software from trusted sources.**
- **Be alert from tempting offers, verify before opting.**
- **Keep your system and antivirus/antimalware software updated.**
- **Don't share your confidential information with strangers and on social networking sites.**

References:

https://en.wikipedia.org/wiki/Social_engineering_(security)
https://www.incapsula.com/web-application-security/social-engineering-attack.html
https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/