ONE PAGE SUMMARY

IT & Software › Ethical Hacking › Social Engineering

Introduction to Social Engineering

Mastering Social Engineering: The Art of Deception in Cybersecurity

DEFINITION

> Social engineering is the manipulation of people to gain confidential information or access. It exploits human psychology rather than technical vulnerabilities.

KEY CONCEPTS

Phishing

A deceptive attempt to obtain sensitive information by pretending to be a trustworthy entity.

Pretexting

Creating a fabricated scenario to persuade a target to divulge information.

Baiting

Offering something enticing to lure victims into a trap, often involving malware.

Tailgating

Gaining unauthorized access by following someone into a restricted area.

Impersonation

Pretending to be someone else to gain trust and access to information.

EXAMPLES

→ An email claiming to be from a bank asking for account verification.

→ A person posing as IT support to request a password.

→ Leaving a USB drive labeled 'Confidential' in a public place to entice someone to plug it in.

MEMORY TIPS

★ Remember the acronym 'PBIT' for Phishing, Baiting, Impersonation, and Tailgating.

★ Visualize a phishing hook to recall phishing attacks.

★ Associate pretexting with 'pretend texting' to remember its deceptive nature.

COMMON MISTAKES

✗ Underestimating the power of human error in security.

✗ Failing to recognize social engineering attempts in everyday situations.

✗ Neglecting to verify the identity of individuals requesting sensitive information.

QUICK RECAP

Social engineering relies on psychological manipulation to access confidential information. Key techniques include phishing, pretexting, and baiting. Always verify identities and be cautious of unsolicited requests.