Social engineering

Social engineering is a cyberattack where an attacker manipulates people into performing actions or divulging confidential information.

How Does It Work?

Attackers often employ psychological tactics to gain trust and manipulate their victims.

Common techniques include:

Phishing: Sending fraudulent emails or messages to trick recipients into revealing sensitive information.
Pretexting:Creating a believable scenario to deceive the victim into providing information or granting access.
Baiting: Offering something enticing, like a USB drive, to lure victims into compromising their systems.
Tailgating: Physically following someone into a secure area without authorization. Why is it

Why is it a Threat?

Social engineering is a highly effective attack method because it relies on human error, which is often harder to prevent than technical vulnerabilities.

Data breaches: Theft of sensitive information like credit card numbers, social security numbers, or intellectual property.

Financial loss: Unauthorized access to bank accounts or fraudulent transactions.

Identity theft: Misuse of personal information for criminal purposes.

Reputational damage: Loss of customer trust and confidence**.**

How to Protect Yourself?

While it's impossible to eliminate all risks, you can significantly reduce your vulnerability to social engineering attacks.

Be skeptical: Be wary of unsolicited emails, phone calls, or messages, especially those creating a sense of urgency or fear.

Verify information: Double-check the authenticity of requests by contacting the organization directly using a verified phone number or email address.

Protect your personal information: Avoid sharing sensitive information online or over the phone unless you initiated the contact.

Educate yourself: Stay informed about the latest social engineering tactics and how to recognize them.

Implement security measures: Use strong passwords, enable two-factor authentication, and keep software up-to-date.