DO NOT LET ATTACKERS TRICK YOU

SOCIAL ENGINEERING

A social engineering attack is a type of security threat where an attacker manipulates or tricks individuals into divulging confidential information or performing actions that compromise their security.

Social engineering attacks use psychological manipulation to exploit human emotions, such as trust, fear, or curiosity.

How to prevent a social engineering attack?

Keep software and operating systems up to date

Regularly update software, including the web browser, antivirus program, and operating system to prevent attackers from exploiting vulnerabilities.

Be cautious with emails

Avoid clicking on links or downloading attachments from unknown or suspicious sources. Verify the sender before opening an email and look out for signs of phishing, such as poor grammar or spelling.

Use strong passwords and security measures

Use a combination of letters, numbers, and symbols to create strong passwords and never reuse passwords for multiple accounts.
Enable two-factor authentication where possible.

Keep personal information private

Do not share personal information such as social security numbers, credit card numbers, or passwords with anyone online or over the phone.

Think before you act

Take the time to think before clicking on links or downloading attachments from unknown sources. If something seems too good to be true, it probably is.

6388014 Waris DamKham 6388087 Chanisara Kotrachai 6388101 Jittiwat Sanit