SOCIAL ENGINEERING SAFETY TIPS



Think Before You Click: It is a good idea to pause and think before clicking on links or downloading attachments, especially if they come from unknown sources. If something seems too good to be true, it is likely a malicious email or message.

Double-Check the Sender: Always verify the sender's email address or phone number before responding to requests for personal information or urgent actions. Don't just trust the name; scammers can impersonate familiar contacts.

Protect Your Personal Information: Never share personal or financial information over the phone, email, or social media unless you initiated the contact and are sure about the recipient's identity. Legitimate institutions will never ask for PINs, passwords, or your credit card CVE number.

Trust Your Gut: If a request or offer feels odd or too pushy, be cautious and seek a second opinion before proceeding. Remember, once cybercriminals invoke emotion or fear, they can influence our ability to act rational.

Use Strong Passwords & Implement MFA: Use complex and unique passwords for all your important accounts. Implement Multi-Factor Authentication (MFA) wherever it is supported.

Stay Updated About Common Scams: Financial institutions often share examples of common social engineering scams. Educate yourself to avoid falling victim to similar scams.

Question Unexpected Requests: If someone asks for money, sensitive data, or any unusual favours unexpectedly, it's important to take a step back and verify the situation with a trusted source. For example, if you receive a message out of the blue on Facebook from a known contact asking you to borrow money, contact them on a different channel such as WhatsApp to validate.

GRANT HUGHES
SPEAKER - AUTHOR - ADVISOR

CyberAwareness
Influencing change, one message at a time