HOW TO PROTECT YOURSELF FROM SOCIAL ENGINEERING

Verify requests

Always verify the identity of the person making the request. If an email, message, or call asks for personal information or financial transactions, contact the source directly using an official phone number or website.

Think before you click

Be cautious when clicking on links or downloading attachments, especially if the message is unexpected or from an unknown sender. Hover over links to check the actual URL, and avoid clicking if it looks suspicious.

Be wary of urgency

Social engineering attacks often create a sense of urgency to pressure victims into acting quickly. If something seems urgent, take a moment to pause and assess the situation. Fraudsters use time pressure to prevent critical thinking.

Educate yourself and others

Stay informed about social engineering tactics and make sure others, such as coworkers and family members, are aware of the risks. Awareness is a powerful tool in preventing attacks.

Enable multi-factor authentication

Multi-factor authentication (MFA) requires a second form of identification, such as a text message code, to verify your login. This adds an extra layer of protection, even if your login credentials are compromised.

Use strong passphrases

Strong, unique passphrases for every account make it harder for attackers to access your information. Consider using a password manager to securely store your passwords.

Report suspicious activity

If you suspect that a social engineering attempt has been made, report it to your IT or security team immediately. Fast reporting can prevent further damage.

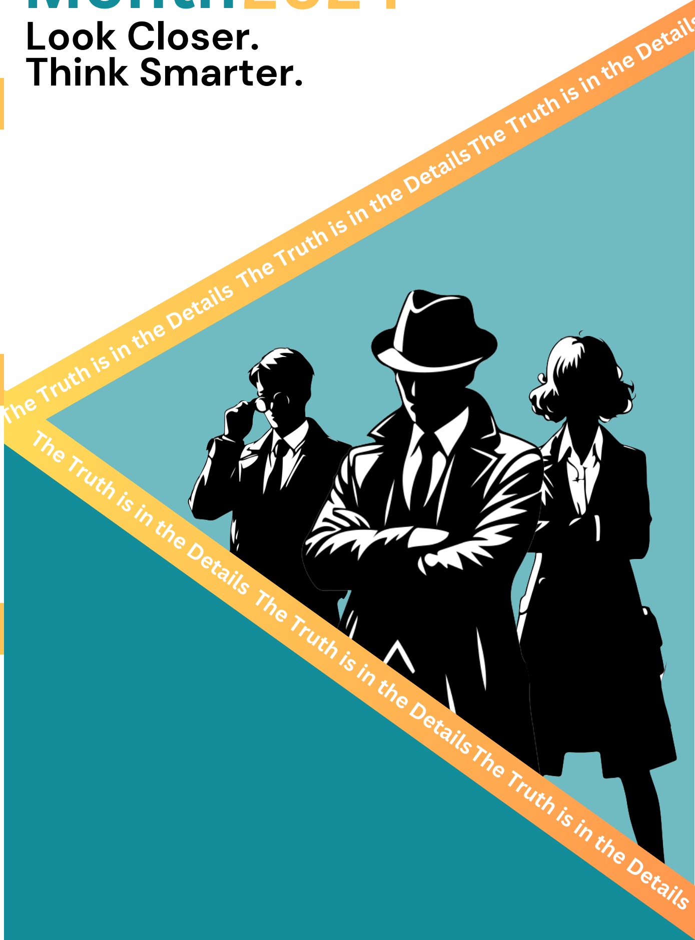
REMEMBER

Social engineering attacks rely on manipulating human behaviour.

Stay cautious, verify requests, and think before you act to protect yourself and your organisation from these deceptive tactics.

Cyber Security Awareness Month 2024

Look Closer.
Think Smarter.


The Truth is in the Details The Truth is in the Details The Truth is in the Details The Truth is in the Details
The Truth is in the Details The Truth is in the Details The Truth is in the Details The Truth is in the Details

Protect Yourself from Social Engineering

WHAT IS SOCIAL ENGINEERING?

Social engineering is the manipulation of people into giving up confidential information or performing specific actions.

Cybercriminals use tactics like phishing, impersonation, and deception to trick individuals into bypassing security measures.

Common types of social engineering

Phishing

Fraudulent emails or messages designed to steal personal information or login credentials by appearing as if they are from legitimate sources.

Pretexting

Creating a fabricated scenario to gain personal information, often pretending to be a trusted individual, like IT support or a colleague.

Vishing

This method uses phone calls to deceive victims. Attackers may pose as a legitimate business or authority figure, asking for confidential information, financial details, or access credentials.

Baiting

Offering something enticing, like free software, to lure individuals into clicking malicious links or downloading malware.

QUICK TIPS

- **Always verify** the identity of anyone asking for sensitive information.
- **Don’t click** on unknown links or download suspicious attachments.
- **Trust your instincts**—if something feels off, it probably is.
- **Enable MFA** to add a second layer of security to your accounts.
- **Report suspicious activity** to your IT or cyber team as soon as possible.

RED FLAGS OF SOCIAL ENGINEERING

- Unsolicited requests for personal or financial information.
- Emails or messages from unfamiliar sources asking you to click on links or open attachments.
- Requests that create a sense of urgency, such as “Act now!” or “Immediate action required!”
- Suspicious email addresses or URLs that do not match official sources.