Integrity360
your security in mind

Stop Social Engineering in its tracks

Advice for Cyber security Awareness Month

Why it matters

Social engineering attacks target people rather than technology. Threat actors use manipulation, deception and urgency to trick people into revealing sensitive information, providing access or transferring funds. Awareness and proactive measures are key to stopping these attacks before they succeed.

1. Verify before you trust

Always double-check identities before sharing information or granting access. Use known contact details, official channels or internal verification procedures to confirm requests, especially those involving sensitive data or financial transactions.

2. Think before you click

Phishing emails, fake login pages and malicious links are common social engineering tools. Pause before clicking links or opening attachments. Look for subtle signs like misspellings, unusual requests or suspicious sender addresses.

3. Limit what you share

Attackers often gather information from social media, public profiles and conversations. Reduce your digital footprint by keeping sensitive company details, job responsibilities and project updates private or restricted.

4. Empower staff to speak up

Create a culture where employees feel confident reporting suspicious activity. Provide clear reporting channels and regular training so staff can recognise and respond quickly to potential attacks. Provide an easy-to-use reporting channel for suspicious emails or behaviour:

- Recognise and reward employees who flag potential social attempts.
- Run regular refresher sessions so staff know what to look for and how to respond.
- Make it clear that no action is too small to report — better safe than sorry.

Need help?

Get in touch with the experts with Integrity360 to help reduce the threats posed by Social Engineering to your organisation.