

1. HOW ATTACKERS TARGET YOU

Cyber criminals use increasingly sophisticated methods, including AI, to trick people.

2. AI-GENERATED CONTENT

Convincing phishing emails, documents, images, chat messages and fake websites

3. DEEPFAKE MESSAGES

Cloned voices or videos in calls, voice notes or chats to impersonate colleagues and executives.

4. EXECUTIVE IMPERSONATION

Fake requests from senior leaders to create urgency, approve payments or share sensitive information.

5. QR CODE PHISHING (QUISHING)

Malicious QR codes that lead to fake websites or trigger unwanted downloads.

6. FAKE LOGIN PAGES

Lookalike websites that steal your credentials.

7. SOCIAL MEDIA INTELLIGENCE

Information from LinkedIn and other platforms is used to personalise attacks and make them more convincing.

THINK BEFORE YOU TRUST

*Modern cyber attacks target people, not just technology.
Recognise the tactics. Take simple steps. Keep our organisation safe.*

8. HOW YOU STOP THEM

Simple actions make a big difference.

9. VERIFY REQUESTS

Always confirm unusual requests through a second channel (eg. call the person directly).

11. CHECK LINKS AND QR CODES

Hover over links, inspect URLs and be cautious with QR codes before you click or scan.

10. USE MFA

Enable multi-factor authentication and never share your authentication codes.

12. PROTECT SENSITIVE INFORMATION

Keep customer, company and personal data confidential, including in AI tools.

13. BE ALERT TO URGENCY

Attackers create pressure to force quick decisions. Take a moment to think.

14. REPORT SUSPICIOUS ACTIVITY IMMEDIATELY

If something feels wrong, report it to the security team. You could stop an attack.

Remember: People are the primary target of modern cyber attacks.
Stay alert. Verify requests. Protect information. Report concerns.