



Phishing & Social Engineering

A practical guide to spotting and stopping phishing attacks. One-page summary.

The 10 things to remember

- 1 The attacker is hacking you, not the computer: a strong feeling plus a call to action is the signature of social engineering.
- 2 Urgency is itself a red flag; legitimate organisations give you time to think.
- 3 The display name on an email proves nothing; always check the real sender address.
- 4 Read domains right to left: the registered domain just before the final ending is what counts.
- 5 Hover or long-press to preview links, and when in doubt go direct via a typed address or official app.
- 6 Never share passwords or MFA codes; no genuine organisation will ask for them.
- 7 Verify any change of bank details or unusual payment by phone on a number you already hold.
- 8 Never approve an MFA prompt you did not trigger; deny it and tell IT.
- 9 If you click, report to IT within minutes; speed matters more than certainty and nobody is blamed.
- 10 Forward suspicious emails to report@phishing.gov.uk and scam texts to 7726.