

Phishing & Messaging

Staying safe when clicking, chatting, or sharing links.

Why It Matters

Phishing and fake messages are the most common way cyber criminals reach people. They look real — pretending to be friends, banks, or delivery services — but one quick click can give them access to your accounts or money.

Knowing what to look for makes every message safer to open.

What It Looks Like

-  **Emails** | “Your account needs attention” — urgent, official-looking notices.
 -  **Texts (SMS or WhatsApp)** | Delivery updates or refund offers with dodgy links.
 -  **Social messages** | “Is this you in this photo?” — from hacked or fake profiles.
 -  **Links** | URLs that look almost right but lead somewhere risky.
 -  **Attachments** | Files or forms asking for login details.
-

How to Stay Safe

-  **Pause before you click.** Urgency is the scammer’s favourite tool.
 -  **Check who it’s from.** Hover over links or inspect the sender’s address.
 -  **Don’t open attachments** unless you’re expecting them.
 -  **Go direct.** Log in through the official app or website instead of the message link.
 -  **Report it.** Forward phishing emails or texts to **report@phishing.gov.uk** or text **7726** (free in the UK).
-

If You’ve Clicked or Replied

-  **Disconnect immediately.** Close the message or hang up the call.
-  **Change your password** if you entered any details.
-  **Turn on MFA** to secure your account.
-  **Run a quick antivirus scan** on your phone or computer.
-  **Report it** to your workplace IT team or Action Fraud (UK).