Smishing & vishing

Smishing = SMS phishing
- A fraudulent message sent to your phone via text message

Vishing = voice phishing
- A fake voicemail or phone call, either using a pre-recorded message or AI to impersonate someone's voice in real time

The most common red flags to watch out for:

- An unfamiliar or hidden number
- Requests for payment
- Prompts to click on a link
- An unfamiliar style of conversation

What an attack might look like:

Smishing – attacks tend to follow the same pattern as phishing

- Text message received claiming to be someone else/a trusted organisation
- Emotive or urgent language used
- Prompt to click on a link or a demand for payment

Vishing – aim to trick you into disclosing private information

- Call received from unfamiliar phone number
- Pre-recorded message played or AI utilised to impersonate a familiar voice
- Caller can become increasingly assertive
- Request for private information