

Scam Safety Red Flags Sheet

A calm checklist for suspicious emails, texts, calls, links, attachments, and urgent requests. The goal is not fear. The goal is a slower, safer next step.

Watch for these red flags

- The message creates panic, secrecy, or a tight deadline.
- Someone asks for gift cards, wire transfers, crypto, or payment apps.
- A caller asks for a password, one-time code, or remote access.
- The sender address is close to a real one but not quite right.
- A link is unexpected, shortened, misspelled, or unrelated to the sender.

More warning signs

- An attachment arrives without context or from someone you did not expect.
- The message says not to tell anyone else.
- The request involves health, money, legal rights, accounts, or identity documents.
- The voice, text, or email sounds convincing but the situation feels unusual.
- You are being pushed to act before you can verify.

Safer next steps

- Pause. Do not click, pay, reply, or share a code yet.
- Use a phone number or website you already trust, not the one in the message.
- Ask a trusted person to look at the message with you.
- Open the official app or bookmarked website directly.
- If money, health, legal, or account access is involved, verify twice.

Simple rule

If a message creates urgency and asks for money, access, passwords, codes, or private information, slow down and verify through a separate trusted channel.

Useful phrase

I am going to check this another way before I do anything.

Want guided practice? Ask about Level 1: Workplace Computer Confidence - bryanteachesai.com