



How to spot a scam email or text

Scammers want you to act before you think. Run through these checks first.

1. Is it rushing you?

"Your account will be closed today." "Act now." Real banks and shops do not panic you. If your heart races, stop and breathe first.

2. Is it asking for something private?

Banks, the tax office and the police never ask for your PIN, your full password or a one-time code. Nobody genuine will ask you to move money to a "safe account".

3. Does the sender look right?

Check the actual email address, not just the name. On a phone, press and hold the name to see the address behind it. Scammers copy an address you know with a small change: joebloggs@gmail.com might become joebloggs@gmail@something-else.com.

4. Fake payment requests

"My bank app isn't working right now. Can you please send the payment via PayPal instead?" Do not send money until you have checked it is really them, using a number you already know. The same goes for invoices with new bank details: ring the person on a number you know before you pay. That includes Tim, who never emails asking you to pay a PayPal invoice or link.

5. PayPal: three golden rules

- ☐ **Check the name before you send.** PayPal shows the real full name of the account holder on the final screen.
- ☐ **If you do not know and trust the name, do not press send.** Cancel the payment.
- ☐ **Never use "Friends and family" for purchases.** It removes PayPal's Buyer Protection. Use "Goods and services".

If something looks wrong on PayPal

Contact PayPal through its own app, or sign in at paypal.com and use Help. Never ring a number or click a link from an email or text. Have your 17-character transaction ID ready (Activity, then open the payment).

6. Do not use the links in the message

Close it and go to the company yourself: type their website, use their official app, or ring the number on the back of your card.

7. Telephone bank scams

Scammers can fake your bank's number on your phone's display. They pretend there is fraud and rush you into moving money to a "safe account" (banks never have one), giving away PINs or codes, or installing remote access software.

If anyone calls claiming to be from your bank or PayPal about a security problem, stop and hang up. A real bank will never mind. On a landline, wait at least 5 minutes before ringing out, or

use a mobile.

8. You never need to install anything to open an email or a PDF

Your device already has a web browser and a way to open PDFs. **If an email, pop-up or website says you must install a new browser, "PDF viewer", "player" or "update", it is a scam.** Tim recently found unwanted programs called "Wavesor" and "SWUpdater", and a "browser" called Wave, on a customer's computer. It came by email, installed itself and allowed outside access. Do not open attachments or download programs from emails you were not expecting. Scammers also ring pretending to be your bank, broadband company, Microsoft or the police and ask you to install a remote access app such as AnyDesk, TeamViewer or RustDesk, so they can see and control your screen. **If anyone asks, hang up.** If you have already installed something, turn off Wi-Fi or unplug the internet cable, then ring your bank on the number on your card. Do not log in to your bank on that device until it has been checked.

9. Never give out personal information

If someone contacts you first, do not give them your date of birth, address, full card number, PIN, passwords or any code sent to your phone. A real company will let you ring it back on a number you trust.

10. When in doubt, ask someone

Show a family member, a neighbour or Tim before you click. Forward scam emails to **report@phishing.gov.uk** and scam texts to **7726** (free).

If you have already clicked or paid

- ☐ **Ring your bank straight away** on the number on your card, or dial **159**.
- ☐ **Change the password** of the account involved, and any other that uses the same one.
- ☐ **Do not be embarrassed.** Clever people get caught. What matters is acting quickly.

Need a hand? Ring Tim on **07746 655324** or visit **techmadesimple.uk**.