



Top 25 Cyber Scams Affecting UK Households

Examples of common scams and practical advice on how to recognise and avoid them.



10 Signs a Message is a Scam

- 1 Unexpected urgency or pressure
- 2 Requests for personal or financial information
- 3 Suspicious links or attachments
- 4 Unknown sender address or phone number
- 5 Poor spelling or grammar
- 6 Requests for secrecy
- 7 Payment requests outside normal processes
- 8 Offers that seem too good to be true
- 9 Requests to move money quickly
- 10 Unexpected account warnings



1. Fake Royal Mail Delivery Text

How the scam works

Text messages claim a parcel cannot be delivered until a small fee is paid.

What to do

Do not click the link. Check the courier website directly.

2. Courier Delivery Fee Scam

How the scam works

A message claims a delivery charge must be paid before a parcel is released.

What to do

Use the courier's official website to check tracking.

3. Missed Delivery Email

How the scam works

Emails claim delivery failed and ask you to click a link to reschedule.

What to do

Avoid clicking email links and visit the courier site directly.

4. Fake Bank Security Alert

How the scam works

Messages claim suspicious banking activity and request login confirmation.

What to do

Banks never request passwords via text or email.

5. Fraud Department Phone Call

How the scam works

A caller claims to be your bank and asks you to move money to a safe account.

What to do



Hang up and call the bank using the official number.

6. Card Verification Scam

How the scam works

Messages ask you to confirm card details to prevent suspension.

What to do

Never provide full card details through email or unsolicited calls.

7. Facebook Marketplace Fraud

How the scam works

Fake buyers send false payment confirmations.

What to do

Only trust payments confirmed in secure platforms.

8. WhatsApp Family Emergency Scam

How the scam works

A message claims to be a relative urgently requesting money.

What to do

Call the relative directly to confirm.

9. Fake Investment Groups

How the scam works

Online groups promise high profits from crypto or trading.

What to do

Be cautious of guaranteed returns.

10. Fake Online Shops



How the scam works

Fraudulent websites sell popular products cheaply but never deliver.

What to do

Check website reviews before buying.

11. Too Good To Be True Deals

How the scam works

Advertisements offer expensive goods at unrealistic discounts.

What to do

Compare prices and verify retailers.

12. Counterfeit Goods Websites

How the scam works

Websites sell fake branded products.

What to do

Purchase only from authorised retailers.

13. Fake Microsoft Support Call

How the scam works

Scammers claim your computer is infected and offer remote support.

What to do

Legitimate companies do not call unsolicited.

14. Fake Antivirus Warning

How the scam works

Popups claim your computer is infected.

What to do

Close the browser and run your own antivirus.



15. Browser Hijack Popups

How the scam works

Popups lock the screen and demand payment.

What to do

Restart the browser or device.

16. Fake HMRC Tax Refund

How the scam works

Emails claim you are owed a tax refund.

What to do

Access HMRC via the official website.

17. Fake DVLA Licence Renewal

How the scam works

Messages say your driving licence must be renewed urgently.

What to do

Use the official DVLA website only.

18. Energy Rebate Scam

How the scam works

Messages claim eligibility for energy rebates.

What to do

Verify through official government sources.

19. QR Code Scams

How the scam works

QR codes redirect to fake websites.



What to do

Only scan codes from trusted sources.

20. Fake Charity Appeals

How the scam works

Fraudsters request donations after disasters.

What to do

Donate through recognised charities.

21. AI Voice Impersonation

How the scam works

Scammers mimic a family member's voice asking for money.

What to do

Verify requests through another contact method.

22. Crypto Investment Scams

How the scam works

Fraudsters promise guaranteed profits.

What to do

Be cautious of investment offers.

23. Ticket Resale Scams

How the scam works

Fake tickets are sold for events.

What to do

Use official ticket platforms.

24. Subscription Trap Websites



How the scam works

Free trials secretly enrol users into subscriptions.

What to do

Read terms carefully before signing up.

25. Fake Job Offers

How the scam works

Fraudulent recruiters request upfront fees.

What to do

Legitimate employers do not charge application fees.



About Wellis Technology

Wellis Technology provides practical cyber security awareness guidance for businesses, organisations and home users.

www.wellis-technology.co.uk

wellis.technology@gmail.com