

HOW SCAMS WORK

Scams are far more convincing than they once were, yet most rely on persuasion rather than clever technology. The scammer pretends to be someone you trust, such as your bank, HMRC, the police, a delivery company or even a member of your family, and then puts you under pressure so that you act before you've had time to think.

Anyone can be caught out. Scammers are skilled and well organised, and many of the people they deceive are sensible and careful. Fortunately, the warning signs change very little from one scam to the next, and once you know them, scams become much easier to recognise.

THE WARNING SIGNS

- **Unexpected contact.** A call, text or email you weren't expecting. Be especially wary if it's about your bank, credit card or mortgage, your internet service, computer or a parcel.
- **Pressure to act quickly.** You're told your account is about to be closed, that you'll be fined, or that an offer ends today.
- **Requests for codes or passwords.** An unexpected caller or message asks for a code sent to your phone, or for your PIN or password.
- **Unusual ways to pay.** You're asked to move money to a 'safe account', buy gift cards or vouchers, pay in cryptocurrency or hand cash to a courier.
- **Secrecy.** You're told not to discuss the matter with family or friends, or to give your bank a false reason for a payment.
- **Offers that seem too good to be true.** An unexpected refund or prize, a bargain price, or an investment promising high returns.

THE GOLDEN RULE

If you're contacted out of the blue and asked for money, personal details or access to your computer, stop. End the call or close the message, then contact the organisation yourself using a number or website you know to be genuine, such as the number on the back of your bank card.

EMAILS, TEXTS AND MESSAGES

Most scams now begin with a message. These are designed to look genuine, often copying the logos and wording of real organisations, and they usually ask you to click a link or call a number. The link leads to a convincing fake website, and any card details or passwords you enter there go straight to the scammer.

COMMON EXAMPLES

- **Parcel deliveries.** A missed delivery, or a small fee to pay before a parcel can be redelivered.
- **Fines and charges.** An unpaid parking charge, speeding fine or road toll. Genuine speeding and parking fines are never sent by text message or email.
- **Refunds.** A tax refund from HMRC or a rebate on your energy bill, which you're invited to claim by entering your bank details.
- **Account problems.** A warning that your bank, PayPal, Amazon or TV Licence account has a problem, that a payment has failed, or that an order or direct debit you don't recognise has been set up.
- **Messages from 'family'.** A message from an unknown number, apparently from a son, daughter or grandchild who has lost their phone, soon followed by an urgent request for money. Always call them on the number you already have.

BEFORE YOU CLICK

- Don't use the links or phone numbers in a message you weren't expecting. Type the organisation's web address yourself, use its app, or call the number on your statement or card.
- Check who the message is really from. Scam emails often come from addresses that have nothing to do with the organisation they claim to be.
- A scam text can even appear in the same thread as genuine messages from your bank or a delivery company, so this alone doesn't prove that it's real.

REPORTING SCAM MESSAGES

Forward scam text messages to **7726**, which is free, and scam emails to **report@phishing.gov.uk**, then delete them. Reporting them helps to get scam websites shut down quickly.

PHONE CALLS

Phone scams often cause the greatest losses, because a skilled caller can be very persuasive. They may already know your name, address and bank, and can even make your bank's genuine number appear on your screen.

WHAT GENUINE CALLERS WILL NEVER DO

- Your bank and the police will never ask you to move money to a 'safe account', or send a courier to collect your card, PIN, cash or valuables.
- Microsoft, BT, Virgin Media, Sky, TalkTalk and other internet providers will never call you unexpectedly about your computer, or ask to connect to it. Our [Guide to Remote Support](#) explains how to tell the difference.
- No genuine caller will ask for your PIN or full password, tell you to keep the call secret, or ask you to give your bank a false reason for a payment.

SECURITY CODES

A genuine organisation will never call you out of the blue and ask you to read out a code sent to your phone. Some banks and other companies do send a code to confirm who you are when **you** have called **them**, so only share one on a call you made yourself, to a number you know to be genuine. Even then, read the message first. If it mentions approving a payment, a new device or adding a card, don't share it with anyone.

VOICES CAN BE COPIED

Scammers can now use artificial intelligence (AI) to copy a family member's voice from a short recording found online. If a relative calls in distress asking for money, end the call and ring them back on the number you already have. Some families agree a code word for exactly this reason.

IF IN DOUBT, HANG UP

End the call and contact the organisation yourself on a number you know to be genuine. Use a different phone if you can, as scammers can sometimes keep a landline connected. Calling **159** will put you safely through to most of the major UK banks.

ONLINE SCAMS

Fake shops

Copycat websites use genuine logos and tempting prices, often with a countdown clock to hurry you. Buy from shops you know, type the web address yourself rather than following an advert, and avoid paying by bank transfer. A credit card gives you extra protection on purchases from £100 to £30,000.

Investment adverts

Adverts and news-style articles in which a celebrity appears to recommend an investment, often in cryptocurrency, are almost always fake. Be wary of anyone promising high or guaranteed returns, and before investing, check that the firm is listed on the Financial Conduct Authority's register at [fca.org.uk](https://www.fca.org.uk).

Online relationships

Be cautious if someone you've met online, but never in person, starts to ask for money, however genuine they seem.

Blackmail emails

You may receive an email claiming that you've been recorded through your webcam, sometimes quoting an old password, and demanding payment. It's a bluff sent to thousands of people at once. Delete it, and change that password wherever you still use it.

SIMPLE HABITS THAT HELP

- Take your time. A genuine organisation won't mind you ending the call and contacting it yourself.
- Turn on two-step verification for your email and online banking, so that a stolen password isn't enough on its own.
- Switch on payment alerts in your banking app, so that you know straight away when money leaves your account.
- Talk about scams with family and friends. A scam you've already heard about is much easier to recognise.

IF YOU'VE BEEN CAUGHT OUT

If you think you may have been scammed, act straight away, because the sooner you do, the more can be done. Please don't feel embarrassed: scams are crimes, and the people they catch out aren't to blame.

1. If you've shared your bank details or sent money, call your bank straight away on **159**, or on the number on the back of your card.
2. If you've allowed someone to connect to your computer, switch it off and contact us, so that we can check it before you use it again.
3. Change any password you've given away, starting with your email account.
4. Report the scam to Report Fraud on **0300 123 2040** or at reportfraud.police.uk.

GETTING YOUR MONEY BACK

If you were tricked into sending money by bank transfer, your bank will usually have to refund you, up to £85,000, as long as you report it within 13 months.

REPORTING SCAMS

If you receive	What to do
A scam text message	Forward it to 7726 , which is free
A scam email	Forward it to report@phishing.gov.uk
A scam call to your mobile	Text the word CALL to 7726 and follow the reply