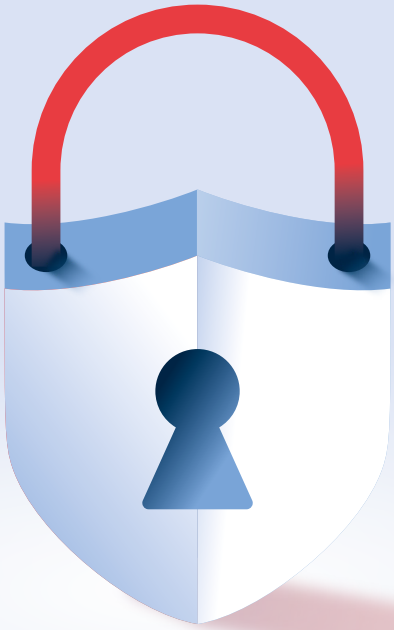
How to spot a scam



Together we'll keep your money safe

We're committed to protecting your money and your personal information. But there are things you need to do too. So, to help you, we've put together this handy guide to spotting the latest scams. We've also listed our 5 top tips on how best to protect your money from scammers.

The most common scams (and how to spot them)

Important numbers and contact details

Nationwide Scam Checker service - **0800 030 40 57**. See page 11 for details.

Concerned that you've fallen victim to a scam? Call us straight away on **0800 055 6622**. If you're abroad, call **+44 1793 656789**

For credit card fraud, call **0800 055 6622.** If you're abroad, call **+44 2476 438997**

Report suspicious emails, texts, and messages that refer to Nationwide by emailing: **phishing@nationwide.co.uk**

You can also forward any other suspicious emails that refer to another organisation to **report@phishing.gov.uk** and suspicious texts to **7726**.

Get smart to the scammers' tricks

Most scams rely on people being tricked into sharing their personal and financial information through cold calls, emails and texts. If you learn to recognise the tell-tale signs that it's a scammer at work, you'll keep your money safe. And remember, suspicion is your best asset.

So, always be suspicious of...

...cold calls pretending to be from Nationwide or other respectable organisations.

It's a fact that we will **NEVER** ask you to disclose your card reader codes or one-time codes over the phone. And we'll **NEVER** ask you to move money to a 'safe account'. No genuine organisation including banks, building societies, the police or government ever would.

...emails and texts that ask you to click on a link to log in or update information.

We'll **NEVER** ask you to log into the Internet Bank, directly from a link in an email or text.

Nationwide have signed up to the new **Stop Scams UK 159 Service.**

So if you think you're being scammed, stop, hang up and call this number: **159**

159 is the secure number that you can call to be connected straight to your banking provider.

You can find out more at **stopscamsuk.org.uk/159**

STOP SCAMS UK

Take Five – Stop. Challenge. Protect

We're proud to be supporting the industry fraud awareness campaign Take Five, which encourages you to take five minutes to:

Stop:	Taking a moment to think before parting with your money or information.
Challenge:	Ask yourself whether it could be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
Protect:	Keep your money safe. Always contact us immediately if you think you've fallen for a scam.

Look out for our tips on spotting scams throughout this leaflet, but you can find out more about how protect yourself at **takefive-stopfraud.org.uk**

Did you know...

It is still a huge issue where criminals continue to defraud people. In 2024, more than **179,115** confirmed cases were reported and in total **£365.7 million** was lost to scammers from personal (non-business) accounts alone. Average lost per case **£2,041.21**.

£85.1 million was lost through impersonation scams, **£126.4 million** through investment scams, and **£76.4 million** through purchase scams.

Source: UK Finance | Annual Fraud Report 2024

Impersonation scams

How it works

You're convinced to make a payment or give personal and financial details to someone claiming to be from a trusted organisation, person or someone you know. This could include the police, your financial provider, a delivery or utility company or a government department such as HMRC, or DVLA or even a friend or family member.

The scammer will claim a payment is owed, your account or money is at risk and needs to be moved to a safe account or that they've accidentally refunded you too much. They might claim to be someone you know texting from another phone or messaging from another profile.

These scams often begin with a phone call, text or email that appears to be from a trusted organisation or person. Scammers can make their calls, texts and emails look like they're from an organisation or person you trust. This is a tactic called 'spoofing' – see also email hack scams on page 9. In some cases scammers even trick you by sending couriers to collect your cards, PINs or valuable items in person.

Always ask yourself

- How do I know they're who they say they are?

Keep your money safe

You never have to do anything to fix a problem someone else created or move your money to a safe account. That's always a scam. Legitimate organisations will never put you under pressure to act urgently. Call the company back on the number from their official website or any original letters. If they claim to be somebody you know, call them back on a number you trust or speak to them in person.

...If someone asks you to lie to your bank, **this is a scam** – don't engage with them, report them immediately.

Investment & cryptocurrency scams

How it works

With investment scams, scammers convince you to move money into a fake investment opportunity. They may contact you, often by phone, but also by email or on social media, offering unusually high returns on investments. They frequently ask you to invest in something like property, gold or cryptocurrency.

Some pretend to be from genuine investment firms by cloning details like the name and address. Some often set up convincing social media posts or websites with fake reviews.

It may seem legitimate, and some criminals even pay their victims a return at the start, but the investment doesn't exist, and your money will be stolen.

With cryptocurrency scams, scammers typically offer a fake, but convincing opportunity to make a profit by investing in cryptocurrency, a virtual currency. There's no physical money.

They may also target you after you've asked about a crypto asset investment advertised online. To access the investment, you may be told you need a crypto-wallet. Criminals offer to set these up, but then empty them of your money.

Always ask yourself

- How do I know this is a legitimate opportunity or that I'm giving money to the genuine company.
- If this is such a good opportunity, why do they need to phone me out of the blue?
- Is it just too good to be true?

Keep your money safe

Be wary of promises of high returns.

Do plenty of research and get impartial advice before you take out any investment. If the company is registered in the UK, you can also check them out on Companies House. If you don't understand how it works, don't invest in it.

Many cryptocurrency investments aren't regulated by the FCA, which means they're not protected by the UK's Financial Services Compensation Scheme, so you're unlikely to get your money back if you're scammed. The FCA's website will tell you if the firm is registered on the Financial Services Register. It's a good idea to check the FCA warning list for known scams and firms to avoid.

...If someone asks you to lie to your bank, **this is a scam** – don't engage with them, report them immediately.

Romance scams

How it works

This is a particularly cruel scam that exploits our emotions and willingness to trust the intentions of other people. Typically, scammers will carefully build an online relationship with you to gain your trust. Eventually, they will steer the conversation round to money and how they need 'help' for things like 'medical fees for an ill relative' or to pay to come and visit you from abroad.

Always ask yourself

- Do I really know this person well enough to trust who they say they are?
- Why can't they video chat with me or meet in person?

Keep your money safe

Talk about your relationships with friends and family that you trust - they may spot something you haven't. **NEVER** send money to, or accept money from, someone you've only ever met online.

...If someone asks you to lie to your bank, **this is a scam** – don't engage with them, report them immediately.

Purchase scams

How it works

Goods ranging from trainers to holidays to cars will be offered for sale online. You'll be asked to pay via bank transfer. Your money will disappear and the thing you've paid for will never arrive.

Always ask yourself

- Can I trust this advert?
- Why is it so cheap?
- Am I 100% sure the goods exist?
- How do I know I'll receive the items I've paid for?
- Why are they refusing to send more photos?

Keep your money safe

Use the secure payment methods recommended by reputable online retailers and online marketplaces. For larger items, like a car, arrange to view it before paying money. Carefully read the description and small print. Do your research on the company or seller you're buying from and read reviews.

Payment in advance scams

How it works

Scammers ask you to pay an upfront fee for things like goods or services, lottery wins, delivery fees or a loan that will never materialise. Sometimes the initial fee is very small. But then they'll keep asking for more and more money.

Always ask yourself

- Why am I being pressured to pay in advance for goods or a service I've never asked for?
- How did I win a lottery I never even entered?
- What confirmation do I have that I'll get what I've been promised?

Keep your money safe

As ever, if an offer sounds too good to be true, it probably is.

You should never pay upfront fees for things you've not ordered.

...If someone asks you to lie to your bank, **this is a scam** – don't engage with them, report them immediately.

Money mule scams

How it works

You'll see advertised what looks like a genuine job, a chance to earn easy money by accepting money into your bank account and then paying it on. This is money laundering.

If you accept the job, criminals will use you as a 'money mule'. Even if you're not fully aware of what's happening, you're still committing a crime. You could face prosecution, be branded as untrustworthy by banks and building societies and have your accounts frozen.

Your credit rating will be severely affected and you'll struggle to get such things as loans or phone contracts.

Always ask yourself

- Why are they asking me to look after or transfer money on their behalf?
- If this a genuine job, why would I be paid to move money for them?

Keep your money safe

No reputable company will ask you to use your own bank account to transfer their money. Don't accept any job offers that ask you to do this. Be especially wary of job offers from people or companies overseas – it'll be harder for you to find out if they are genuine.

Email hack scams

How it works

Scammers will hack the email account of a person or company you have a business relationship with, often solicitors and builders. They will then send you a message telling you a payment is due but that their bank details have changed. Because you're expecting to make a payment, you think nothing of it and follow their instructions.

Always ask yourself

- If you've paid them before, why am I being asked to pay money into a different account?
- Has the account name flagged up as a 'no match'?

Keep your money safe

All you need to do is speak to your supplier either over the phone or in person, ensuring you use their original contact details, to check the account details you are paying belong to them.

Rogue trader scams

How it works

Rogue tradespeople will knock on your door and say that urgent building or roofing work is needed on your property.

They may overcharge you for unnecessary work, or convince you to make full payment for partially completed work and then never return to finish it. They may rush you to make a payment for something you don't need.

Always ask yourself

- Why do I have to make a decision right now?
- Do I trust this stranger to do a good job and not overcharge me?
- How do I know this work needs doing?

Keep your money safe

Don't feel rushed to get work done by someone knocking on your door. Take your time and do some research. Get quotes from several tradespeople first. Ask friends and family you trust for advice too. They may have had similar work done or know a good tradesperson.

...If someone asks you to lie to your bank, **this is a scam** – don't engage with them, report them immediately.

Recovery scams

How it works

If you've ever been scammed, or lost money to an investment, scammers may contact you pretending to be a legitimate company, offering to recover any money you previously lost, for an up-front fee. They may even say that, with your help, they can make an arrest.

Always ask yourself

- How do I know this offer is legitimate?
- What guarantee do I have that I'll get any money from them in return?
- How do they know I was a victim of a scam?

Keep your money safe

Check the Financial Services Authority site to see if the company is authorised to carry out recovery services.

...If someone asks you to lie to your bank, **this is a scam** – don't engage with them, report them immediately

Five top tips to beat the scammers

1. Don't be rushed

Only scammers will try to rush or panic you. A genuine organisation or someone you know won't mind waiting, or even you phoning them back on a number you trust.

2. Don't assume...

...an email request, text, or phone call is genuine just because it looks as you'd expect. Scammers are experts at faking the real thing.

3. Don't ever disclose...

...your security details like your PIN or one-off card reader code: we would **NEVER** ask you for this information.

4. Don't be afraid to say no.

Saying NO can feel uncomfortable sometimes, but it's ok to reject, refuse or ignore requests.

5. Don't ignore your instincts.

If something doesn't feel right, if the offer's too good to be true, then trust your instincts and don't be fooled by the scammers.

Nationwide Scam Checker Service – if you're not sure about a payment, we can help

Our Scam Checker Service

Our Scam Checker Service can help whenever you're **in branch** or using our **Banking app**, **Internet Bank** or **Open Banking** to make a payment to someone else in the UK from your Nationwide current account.

Not sure about a payment?

Call us anytime on **0800 030 40 57** or come into your local branch.

We'll ask you about the payment, check the details and tell you if we believe it might be a scam.

Scam Protection Promise

You can find out more about our Scam Protection Promise, including the full terms and conditions on our website. Just visit **nationwide.co.uk/banksafely**

Call **0800 055 6622**
Email **phishing@nationwide.co.uk**
Visit **nationwide.co.uk/help/fraud-and-security**

Need a copy of documents in Braille, large print or audio format? Just ask in branch or call **03457 30 20 11**.

This literature is printed in the UK with biodegradable vegetable inks on paper from FSC® certified and other controlled material.

FSC www.fsc.org MIX Paper from responsible sources FSC® C003270

recycle When you have finished with this leaflet please recycle it

P3743 (September 2025)