How to spot a scam

Your handy guide

Nationwide
Building Society

Contents

Your security is a priority for us

At Nationwide, we're committed to protecting you from fraud. One of the best ways to keep your personal data and money safe is to make you aware of what to look out for. Here's a pocket guide outlining the latest scams with our top tips on how to recognise and combat them.

There are lots of ways fraudsters can try to trick you. But by building your defences against them and arming you with the knowledge you need to protect yourself, together we can stop fraud.

Safe account scam

What to look out for:

Fraudsters will phone to try to convince you that your money is at risk, and that you need to move it to a 'safe account'.

They might also impersonate the police, the Financial Conduct Authority, or Nationwide.

Ask yourself:

How do I know the caller is who they say they are?

Is my money really at risk?

Top tip:

Never act on a call out of the blue or transfer money at a caller's request. A genuine organisation would never ask you to do this.

Purchase scam

What to look out for:

Fraudsters will advertise goods, holidays, or cars on a website online. They'll ask you to pay via bank transfer but never send the advertised item.

Ask yourself:

Can I trust this advert?

How do I know the goods exist?

Top tip:

Only buy goods through a reputable website/app. For larger purchases (for example, a car) make sure you see what you're buying before parting with any money.

Refund scam

What to look out for:

Fraudsters will phone, posing as a trusted organisation, and tell you there's an issue with your computer, requesting remote access to fix it. They'll say you're due compensation for the inconvenience, and ask you to log on to your Internet Bank.

They'll claim they've refunded you too much (as they have access to your computer, they'll actually have remotely transferred money from your savings account to make it look like they've credited your current account). Then they'll ask you to return the difference to them.

Ask yourself:

Is it safe to give this caller remote access to my computer?

Why do I need to pay back the overpayment right now?

Top tip:

Don't allow yourself to be rushed into allowing remote access. Be sure who you're dealing with. And never log on to your Internet Bank account while allowing someone remote access.

Investment scam

What to look out for:

Fraudsters will phone to try and sell you investments in emerging markets, claiming they'll make you money. For example: wine, diamonds, and alternative energy.

But the investment doesn't exist and you won't see any return on the money you put in.

Ask yourself:

How do I know this is a genuine company?

Top tip:

Always visit the Financial Conduct Authority's Scamsmart website – **fca.org.uk/scamsmart** – which offers a warning list. Here, you can check the risks of a potential investment. You can also search to see if the company that has contacted you is known to be operating without authorisation.

Email hack scam

What to look out for:

Fraudsters will hack service providers' (often solicitors and builders) mail accounts and use them to send messages advising you to send payments to a different account.

Ask yourself:

Why am I being asked to pay money into a different account?

Top tip:

Be vigilant – fake email invoices can be very convincing. Use your supplier's original contact details to check if any changes are genuine.

Rogue trader scam

What to look out for:

Rogue traders will knock on your door and say they're working in the area and that urgent work needs doing to your property.

They may overcharge you for unnecessary work, or convince you to make full payment for partially completed work and never return to finish it.

Ask yourself:

Why do I have to make a decision right now?

Do I trust this person to do a good job and not overcharge me?

Top tip:

Don't feel rushed to get work done by someone knocking on your door – take your time, do your research, and get quotes from several tradesmen before making any commitment.

Courier scam

What to look out for:

Fraudsters will phone you – impersonating your bank, building society, or the police – to try and dupe you into revealing your PIN. Then they'll attempt to convince you that, as part of an investigation, you need to hand over your debit/credit card.

They'll arrange for a courier to pick up your card. They might also ask you to hand over a large sum of money to help with 'the investigation'.

Ask yourself:

Do I know this person is from a genuine organisation?

Is this a real investigation?

Top tip:

Don't give out your banking information or take out money/buy goods for someone who claims this is necessary for an investigation. A genuine organisation would never ask you to do this.

Romance scam

What to look out for:

Fraudsters will build an online relationship with you to gain your trust and start asking for money for things like ‘medical fees for an ill relative’.

Ask yourself:

Do I trust this person is who they say they are?

Top tip:

Keep conversations through a reputable dating agency. Never send money to – or receive money from – someone you’ve only met online.

Money mule scam

What to look out for:

This involves unknowingly helping fraudsters move stolen money. You'll see what looks like a genuine job, but the earnings are from crime. This could result in criminal prosecution, your account being frozen, and being branded as untrustworthy by banks.

Ask yourself:

Is this a genuine job?

Why are they asking me to transfer money on their behalf?

Top tip:

A reputable company will never 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/companies overseas – it'll be harder for you to find out if they are genuine.

Things to remember

We'll never ask you to:

- **transfer your money to a safe account**
- log directly into the Internet Bank via a link in an email, text or social media message
- update your details directly from a link in an email or text
- use, re-enable, or re-sync your card reader over the phone.

Don't:

- be rushed – a genuine organisation won't mind waiting
- assume an email request, text, or phone call is genuine
- disclose security details like your PIN or generated card reader code.

Do:

- listen to your instincts – you know if something doesn't feel right
- stay in control – don't panic and make a decision you'll regret.

If you're concerned or just want more information

Visit our security centre on our website at:
nationwide.co.uk/fraudaware

Think fraudsters might have access to your money?
Call us straight away: **0800 055 6622**
If you're abroad: **+44 1793 656789**

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

By being aware and staying vigilant, we can stop fraud. Report suspicious emails, texts, and messages by emailing: **phishing@nationwide.co.uk**

Let's build a safer society, together.

TAKE FIVE TO STOP FRAUD™

P3743_A (June 2021)