How to avoid, spot and report financial scams

Scams are getting more and more sophisticated, particularly when it comes to targeting you online and through mobile devices. In this guide we take a look at how you can recognise a scam, protect yourself and what to do if you're a victim or have been targeted

What is a financial scam?

A scam is a type of fraud that can take many forms, such as a text message, email, letter, phone call, or even a door-to-door visit. Scams are designed to steal your money. They do this by getting you to reveal your personal details, stealing your information, or even tricking you into willingly handing over the cash.

Scammers will pretend to be an organisation, your bank or even a family member or friend. Scams can take many different forms. So, it's important to know the warning signs to look out for and what to do if you have been targeted.

How to spot a scam

It's important to know how to spot a scam text message, call, or email and to learn to check whether any communication you've received is fraudulent.

While some scams can be easy to spot and avoid, others are much more sophisticated. Scammers keep up to date with things in the news and use government schemes that people might have heard of but aren't familiar with to create new scams.

Knowing what to be on the lookout for when it comes to scams is one of the best ways to protect yourself.

- Seems too good to be true? If the price seems too good to be true, it probably is.
- If you have not entered a competition you cannot win it.
- Being contacted out of the blue. You should be suspicious if you have been contacted out of the blue and asked for personal or payment details, either by phone, online, text, doorstep or by post.
- Asked for personal details? Legitimate organisations will unlikely contact you and ask for these details if you are not expecting it.
- Look at how you're addressed in the email. Scammers will use a general greeting such as Dear Sir, Dear Madam or Dear Customer. Legitimate emails will use your name.
- The email address the message has been sent from. Open the email and expand the pane at the top of the message and look at the email it was sent from. If it's a real message, it will come from a recognisable address – such as 'noreply @ bank.com(link sends e-mail)'. Scammers won't be able to send messages from a real domain name. So the email addresses will be filled in with random letters or

numbers, such as 'noreply @ 1234.bank.com(link sends e-mail)', or have deliberate spelling mistakes.
- The company you're dealing with is very hard to reach – they don't have a postal address and/or are nearly impossible to reach by phone.
- Asked to send money? Be wary if you are contacted out of the blue and asked to make a payment of any kind.
- You've been asked to pay for something in an unusual way – for example, via gift cards or vouchers.
- Feeling under pressure? Scammers often create a sense of urgency to pressure you into providing your details to try and rush you into making a decision. If something doesn't feel right, stop and think.
- Being asked to pay for something that usually doesn't require a payment – i.e. applying for a job and being asked to pay a fee.

While these are the most common ways to recognise or spot a scam, they are not the only ways, so it's best always to remain alert and vigilant.

The latest scams

As scams continue to be on the rise and take many forms, fraudsters will continue to target innocent people. But where you can, try to protect yourself and remain safe by learning more about the latest scams, such as the ones listed below.

- Romance scams – a scam that involves fraudsters adopting a fake online persona to build and gain a person's trust, usually for financial reasons. Find out more about romance scams at Action Fraud(link is external)
- Job scams – employment fraud when fraudsters 'hire' you for a job that doesn't exist or ask you to pay a fee once you've been 'hired'. Find out more about job scams at Action Fraud(link is external)
- Pension scams – a scam that involves a fraudster trying to gain access to your pension to steal it, usually by making false lucrative promises of unrealistic pension growth. Read more about how to spot a pension scam.
- Energy scams – some scammers are now pretending to be Ofgem, offering to save you money or help you switch to another energy provider. Learn more about Ofgem scams and how to report them(link is external).
- Bank scams – these involve the fraudulent use of a person's card to buy things to steal money. Read more about how to spot and avoid bank scams.
- Social media scams – a type of fraud that is committed online via social media sites or platforms such as TikTok, Whatsapp, Instagram and Facebook.
- Cryptocurrency scams – a cryptocurrency scam is a type of investment fraud involving a digital currency. Sometimes, scammers may impersonate new or existing businesses that offer digital currency. Read more about cryptocurrency scams or investment and scam risks with cryptocurrency.

While the above scams may be the most common, many more types exist. So, be careful and take a pause if you suspect something is dodgy or doesn't feel right.

How to protect yourself against scams

The best way to avoid scams is to know how to protect yourself both off and online. The tactics used by scammers and fraudsters can vary. So, it is best to always be vigilant.

The best way to stop a financial scam is to apply these important rules

1) Never click on links in text messages from someone you do not know
2) Never call or text suspicious numbers back
3) Never ever transfer money to someone you do not know or have not met
4) Always delete texts requesting personal or financial information or bank account details
5) Always forward scam texts to 7726 – the free scam text reporting service
6) Keep passwords strong and confidential for all of your accounts
7) Use safe and secure WiFi

For further information and advice on scams and how to avoid becoming a victim is available from -

- Consumer Council – Advice and Guidance
- Keeping yourself safe from scams - Consumer Council - bitesize recording
- MoneyHelper – Advice and Guidance
- Scams and Fraud | PSNI

What to do if you think you have been scammed.

If you've been scammed or suspect that someone is attempting to scam you or someone you know, you should always report it. Don't feel embarrassed or ashamed. If you report a scam, it gives important information to the authorities that can be used to warn other people.

How to Report a Scam

If you have been the victim of a scam, or feel that someone is trying to scam you, take immediate action.

Request a call for service from the PSNI (what is a call for service?)

You should ask for a call for service when any of these apply:

- a fraud is being committed or recently occurred (within 24 hours)
- you know the suspect and they live in Northern Ireland
- the victim is perceived to be vulnerable, through age, mental or physical impairment, or in need of care and support
- you believe it's important to report the incident to police so they can secure and preserve evidence or prevent loss (such as CCTV and recovering large amounts of money transferred from bank accounts before the criminal can remove it)

You can request a call for service report to the PSNI by phoning 101 or 999 in an emergency or report it to police online at https://www.psni.police.uk/report

Further information and support is available from -

- NI Direct website.(link is external)
- Scamwiseni | nidirect
- Investment Fraud | PSNI