How to spot, avoid and report scams

Information on the different types of scams that you should look out for and how to keep yourself safe.

Scammers are always looking for new ways to catch you out. Scams can happen in many ways, such as via phone, on your doorstep, online or by email. If you know what to look out for, you can help to keep yourself safe.

How to spot a scam

Follow these top tips to spot scams.

- 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.
- Asked to send money? Be wary if you are contacted out of the blue and asked to make a payment of any kind.
- 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.

Types of scams and how to avoid them

Scammers are always looking for new ways to catch you out. Scams can happen in many ways, such as via phone, on your doorstep, online or by email. If you know what to look out for, you can help to keep yourself safe.

Email and text message scams

Phishing emails and text messages are used by scammers to get your personal details. The text message or email might ask you to click a link to visit a website. The email address and content can also look like it is from a real company.

Ways to protect yourself from email and text scams

- Never reply to this type of text message or email with information such as your bank sort code, account number or password.
- Do not click on links in an email or text message if you are suspicious of the sender.

- Check if the greeting is personal - does it include your first and last name? If not this is a sign it is probably a scam.
- Watch out for spelling and grammar mistakes as this is often a sign of a scam.
- Forward suspicious text messages to 7726. This is free and will report the message to your mobile phone provider.
- Forward suspicious emails to report@phishing.gov.uk.

Telephone scams

This is when fraudsters cold-call you and make you believe you are speaking to a member of staff from a trusted organisation such as the bank or a government department. They may try and persuade you into thinking you have been a victim of fraud and ask you to share personal and banking details.

Scammers can also make the caller display on your phone show an official telephone number. This is known as 'number spoofing'. This can make you think the call is from a real organisation, like your bank, utility company or HMRC.

Ways to protect yourself from telephone scams

- Register with the Telephone Preference Service to opt out of unsolicited sales and marketing calls.
- Never give out your personal and banking information if you are unsure of the sender.
- If you are in doubt, hang up the call and call the organisation directly using the contact details on their website.
- If possible, call the organisation back from a different telephone as scammers can stay on the line without you knowing.
- If it is not possible, wait a short while before returning the call.

Online scams

This type of scam can include romance scams, holiday scams, ticketing scams and copycat websites. Scammers use online marketplaces and social media to target sell you fake goods or goods that do not exist.

How to protect yourself from online scams

- Check the web address of the website you are being directed to. Most shopping websites end with ‘.co.uk’ or ‘.com’. Official UK Government or public body websites end with 'gov.uk' and 'org.uk'
- Is the advert offering expensive items at a low price? Stop and think – is this too good to be true?
- Check if the web address has ‘https’ and a padlock icon in the browser bar. The ‘s’ stands for secure and together with the padlock are an indication the website is safe.
- Never make payment for goods by bank transfer. When paying by credit or debit card you have some rights to get your money back.
- If using a third-party payment processor, be wary of additional discounts being offered if you are asked to pay by an alternative method to avoid fees.
- Avoid sellers who only want to converse by email/text message and are reluctant to engage by phone.
- Do your research before buying from a website you have not used before. Read reviews of items and previous customer feedback.
- Never use public Wi-Fi to access your personal information. This is an easy way for scammers to get hold of your details.

Doorstep scams

This is when someone calls to your home, pretending that they represent an organisation and try to sell you something. They may pretend to represent law enforcement, utility companies, or fake charities. The aim is to take your money or steal your valuables. Doorstep selling is still a thing and there are genuine sellers out there.

Ways to protect yourself from doorstep scams

- Always treat cold callers with caution.
- Keep your home secure and do not let strangers in.
- Use the PSNI Quick Check Scheme by calling 101 to check the identity of anyone calling on behalf of a utility company.
- Ask the caller to show you ID.
- Set up a free password scheme offered by utility companies like NI Water and NIE Networks
- Do not hand over cash or feel pressured into buying something.
- If you are an older person, make use of the PSNI Nominated Neighbour Scheme

Postal scams

Postal scams are when you receive a letter and the sole purpose is to get your money. There are many types of scam mail including fake lotteries and prize draws, pyramid schemes, investment scams, and hard luck stories.

Ways to protect yourself from postal scams

- Register with Mail Preference Service to have your name taken off direct mailing lists.
- Watch out for bad spelling and poor grammar as these are often signs of a scam.
- If it sounds too good to be true, it probably is. If you have not entered a competition you cannot win it.
- Do not reply with personal or financial information.

How to report a scam

If you have been a victim of a scam, or feel that someone is trying to scam you, take immediate action. Information on what to do is available here on the NI Direct website.

Other scams information

Business and agricultural scams

Types of scams that are specifically targeted at business owners and agriculture.

Educational scams activities

We have developed a range of educational activities that consumers of all ages can get involved in.

Become a Scamwise Champion

Inclusive programme to help people with learning difficulties avoid scams.