# Scams

There are many different types of scams. Scammers may contact you in different ways – online, by telephone, by post or in person.

Their goal is to obtain personal details from you so that they can steal money by pretending to be you or convince you that what they are offering is so good that you hand over your details or your money willingly.

If you believe that someone is trying to scam you, you should never:

* Give them any personal information, like bank details, computer passwords or PIN numbers.
* Reply to their emails or click on any links within their emails.
* Download any attachments or files in their emails.
* Send them any money or give them any payment details.
* Call any numbers in emails or letters you receive.
* Allow them into your house if they’re at your door.

If you’ve lost money because of a scam, you can report it.

It’s easier to spot a scam if you know what to look for, so be careful if something:

* Comes out of the blue or from someone you don’t know.
* Sounds too good to be true - like you’ve won the lottery, or you’ve been invited to invest in a scheme which will pay huge dividends.
* Asks you to pay for something in advance - especially by bank transfer.
* Asks you for personal information - like your bank details, computer passwords or PIN numbers.
* Pressures you into buying something or making a decision quickly rather than giving you time to consider your options.
* Asks you to phone an expensive number - these start with 070, 084, 087, 090, 091 or 098.

You can [check recent scams](https://www.actionfraud.police.uk/news) on Action Fraud’s website - [www.actionfraud.police.uk](http://www.actionfraud.police.uk) and [common financial scams](https://www.fca.org.uk/consumers/protect-yourself-scams) on the Financial Conduct Authority’s (FCA) website;

[www.fca.org.uk](http://www.fca.org.uk)

If you’ve been contacted about making an investment, [check if the company is registered with the FCA](https://register.fca.org.uk/) on their website - [www.fca.org.uk](http://www.fca.org.uk). If it is not it is probably a scam.

If someone is offering to do building work for you, don’t let them start immediately and ask them for references - this will give you time to check if they’re reliable. Always get comparison quotations for work that needs to be carried out.

How to spot a fake email or website:

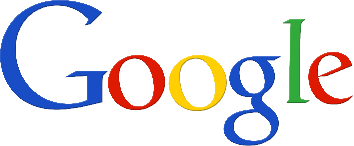
* Scam emails ask you for personal information like passwords or bank details to get money. This is called ‘phishing’.
* They often look like they are from a real company - like a bank or building society. Remember that your bank will never ask you to confirm personal details by clicking on an email link.

If you are not sure if it’s a scam, check:

* The email or website address - if it is a scam, it might have a strange address or come from a free email provider like Gmail.
* For spelling mistakes - trustworthy websites are less likely to have them.
* If the website starts with https:// - this means the information you send on the website is secure, but the website could still be a scam.
* If the website has a green padlock in the website address bar - this means the information you send on the site is private.

[Get advice on being safe on the internet](https://www.getsafeonline.org/)on Get Safe Online’s website:

[www.getsafeonline.org](http://www.getsafeonline.org)

They also have advice on [protecting your computer from viruses](https://www.getsafeonline.org/protecting-your-computer/) which can sometimes steal your details.

If you think you’re being scammed online:

* Don’t click on anything and leave the website. You might want to keep the email as evidence in case you report the scam.
* If you have received an email which looks like it is from your bank, contact your bank directly using the number on your card. You can also log into your account on their website - use Google to find the real one.
* You can also block the email sender or mark an email as ‘spam’ or ‘junk’ - this means that you will not see them in your inbox. Check your email provider’s help section for instructions on how to do this.

Scamming can affect us all, but what are the scams that you particularly need to look out for? For further information about how to recognise a scam and what you should do to avoid being caught out, visit the following links;

* GOV UK - [www.gov.uk/government/publications/frauds-tricks-and-scams/fraud-tricks-and-scams](http://www.gov.uk/government/publications/frauds-tricks-and-scams/fraud-tricks-and-scams)
* Citizens Advice - www.citizensadvice.org.uk/consumer/scams/spotting-a-scam
* Age UK - www.ageuk.org.uk/information-advice/money-legal/scams-fraud/phone-scams

**10 scams to watch out for and what to do about them**

Scamming can affect us all, but what are the scams that you particularly need to look out for? We explain the real danger scams and what you can do to avoid being caught out

Scams are everywhere. Popping up in your inbox, through your letterbox, and potentially inside any other kind of box that you might happen to have lying around.

A new report by the National Trading Standards (NTS) identified almost 200,000 potential victims who appear on so called "suckers lists". The average age of those on the lists is 74, pointing to a criminal delectation for preying on older and more vulnerable people.

Almost 11,000 of the identified victims lost an average of £1,184 each, just over £13 million in total. Work done by the National Trading Standards Scams Team (NTSST) has saved consumers more than £5million over the past three years, its figures show.

During their, Scams Awareness Month, the NTSST urged people to be vigilant and help those who may be vulnerable to mass marketing scams to avoid them. But what kind of scams should you be watching out for?

Here, we run through the top 10 scams to avoid, and how you should approach them if you do come across them.

**The pension scam**

Money Advice Service warns that since April 2015, it's become even easier to be scammed via your pension, owing to the additional ways in which you can access your pension pot. Now the rules have changed, fraudsters are aware that not everyone will be totally clued up. If you're not, that leaves you vulnerable to their advances.

These unpleasant individuals may promise you extra tax savings or higher returns on investments, claim to know of ways you can get more than the standard 25 per cent tax free cash, or say they have the power to unlock your pension before you turn 55. Scams in which companies claim to help you take your pension early are known as 'pension liberation fraud', and it's important to be wary of it.

**The lottery scam**

Lottery scams make up a huge amount of scams operating in this country. If you're a victim of one of these, it's likely you'll receive a letter saying you have won a large amount of money on an online, or overseas, lottery.

If this happens, ask yourself the obvious question: have I entered such a lottery? Most people that fall victim to the lottery scam, haven't. If you respond to it, you'll be asked for your personal information, and in order to 'receive' your money, you'll have to keep paying fees. Unfortunately, the money you have 'won' on the lottery will never materialise.

**The competition scam**

On a similar vein is the competition scam. 'Congratulations!' the email subject line will scream. 'YOU'VE WON!' Well, have you? Probably not. In many cases, the condition of having won these prizes is that you'll need to send money to claim them.

The prize that you have 'won', invariably won't turn up, probably because it doesn't exist. Consumer rights group Which? advise that 'any legitimate organisation will pay these upfront costs, so anyone asking for a fee in advance shouldn't be trusted.'

**The phishing scam**

Not fishing, but phishing. 'Phishing' is a clever but nasty practise in which internet sites pretend to be something they're not. They resemble legitimate organisations like eBay or PayPal, and draw you in to entering your username and password so they can access your account. If you receive an email 'from' a certain organisation, and there's a sudden and immediate need for you to confirm your identity with some classified information, ask yourself whether this is realisation.

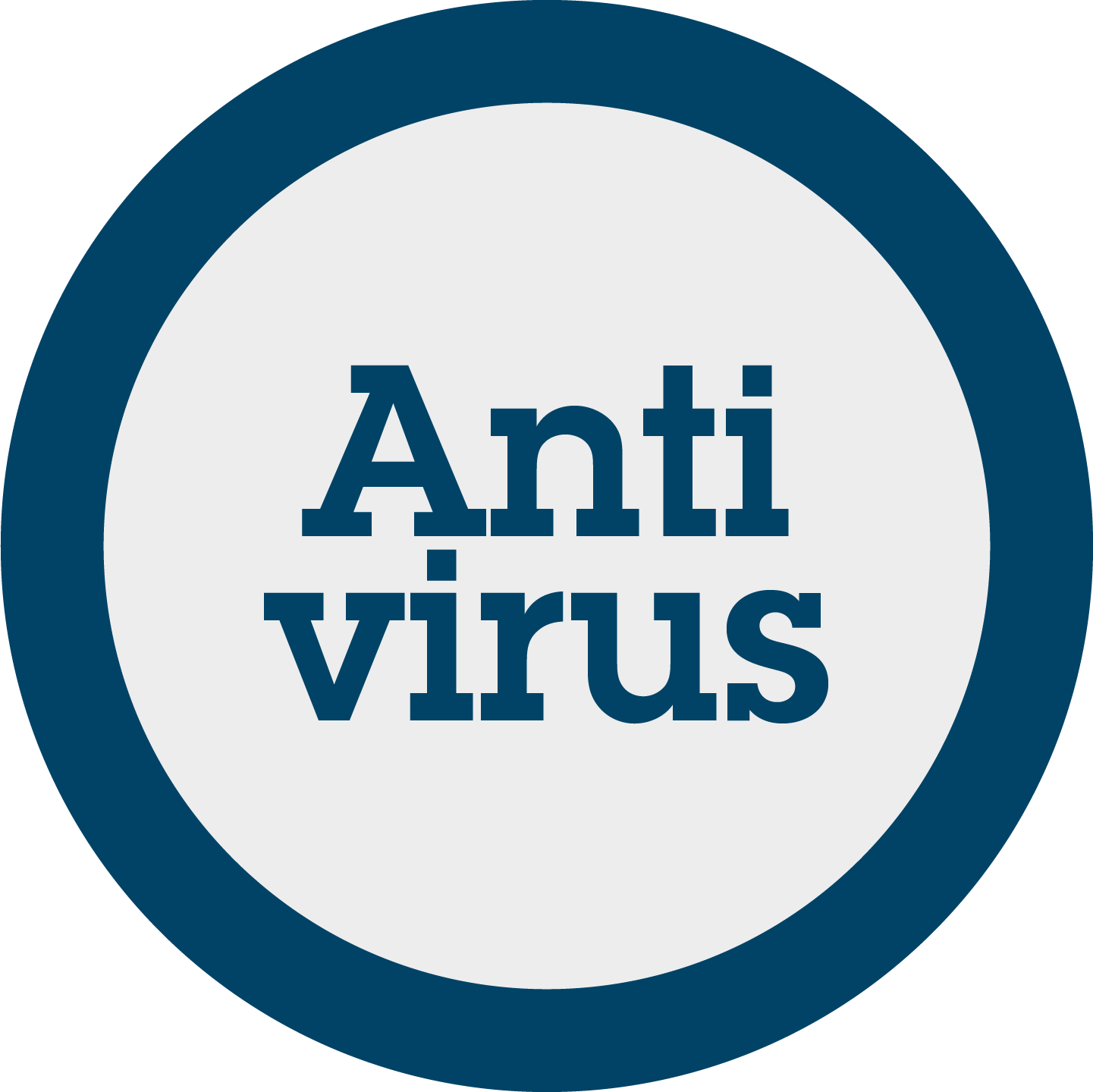
You might be told that your account has been hacked, and in order to fix it you must log in and enter your information. Don't fall for it. Avoid falling victim to phishing by checking that the web address is real. In the web bar, on a secure site, if there's a 'https://' present, its real; if not, and it reads 'http://' with no 's' it's fake as they come.

**The disaster relief scam**

It's obvious that the natural and manmade disasters that hit the world are devastating. They pull on your heart strings with some legitimacy, but what if you get an email asking you to help out with relief? Take a look twice, before proceeding. Sadly, some scammers are in the business of setting up fake charity websites to steal money donated by good willed people to these disaster funds.

If you receive one such request by email, then think twice before entering any information.

There's a chance it could be a phishing attempt, so do not click the link and offer up your bank account details. If you're keen on donating to whatever cause is being proffered, contact the organisation directly to be safe.



**The computer software scam**

These can come from Microsoft, or sometimes from Windows. You'll get a call or an email saying that you have a virus on your computer, and in order to combat it, 'the only way' is to pay some money up front to get a clever computer person to send it away. The problem is, the 'clever computer person' is actually a scammer,

and they are raking it in from the money that you are willingly offering them for their services. Make sure you have adequate antivirus software installed on your computer, bought via a verifiable source, and that should limit your concern. If you know that you've got enough protection installed on your computer, you shouldn't be tempted to read these software scam emails, or take their calls.

**The boiler insurance scam**

You might at some point have worried about your boiler. Although it's summer time now, during the winter it will suddenly come in useful, and you're naturally keen to keep it in good shape. As if to take advantage of your good nature, scammers can come along to hit on you and your boiler. Reports have surfaced in recent years of older people being pressurised into giving away their bank account details to cold callers who claim that they need to get insurance on their boiler. These can happen over the phone or on your doorstep, and largely occur during the day when the scammers know that older people are more likely to be at home.

**The 'Nigerian email' scam**

This usually involves a low email from 'your beloved' in some far away land. Astonishingly, this kind of scam dates back to the 18th century, and variants of it can be found in the memoirs of Eugène François Vidocq, a former French criminal and private investigator. These emails generally start with something that goes like this: "Hi Dear, Compliments to you and thanks for taking your precious time to reply to my mail. I am more than happy and grateful to you. I know you will be a good and honest friend..."

The ultimate goal is usually to get you to send them some money to 'release them' from whatever situation they have ended up it. It's what is called 419 fraud, and you can avoid getting caught up in it by simply ignoring it. Delete the message, and don't respond to it.

**The HMRC tax rebate scam**

[](https://www.google.co.uk/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwiC-oeQ05_hAhVmyoUKHYs4BwUQjRx6BAgBEAU&url=https://www.getsurrey.co.uk/news/surrey-news/hmrc-releases-list-most-outlandish-12503157&psig=AOvVaw331Vaq3lFKogYMhkPz728j&ust=1553684268916310)You might have received a fairly convincing email from our favourite Revenue and Customs officials saying that you are owed a tax rebate. It might go something along the lines of: 'We have reviewed your tax return; According to our calculations, a tax refund is due.' Sadly, it never is. Fraudsters purporting to be HMRC will often use email accounts with HMRC or revenue names in them, such as 'refunds@hmrc.org.uk', and this is done deliberately to trick you. Gov.uk says that HMRC will never contact you by email about your tax rebate.

If you think about it, that makes sense why would they discuss sensitive information with you by email? If you are concerned about your taxation, ring HMRC a call and verify your situation rather than trust an email. It's better to be safe than sorry.

**The PPI scam**

Everyone has heard of PPI the constant, annoying scourge on society that drops into your inbox, through your letterbox, and would, if it could, slide into every other kind of box you might happen to have hanging around. PPI means 'payment protection insurance', and refers to the insurance sold alongside credit cards and loans to insure payments are made if the borrower is unable to make them due to sickness or unemployment.

Typically, you'll get a call from an unknown number, or an email in big shouty capital letters saying that you have been missold PPI. What's really naughty about these scams is that if you've actually got a PPI policy, you might be eligible for compensation. And it's true that millions of people have been missold the product, having had it pushed on to them by unqualified financial advisors to customers who would never find a use for them. The banks have made billions in profits from these policies and so it's only right that if you have been missold something, you should be able to claim it back. But are the scammers trying to do you a favour? Definitely not.

They're making a neat and tidy profit of their own, and wasting your time in the same breath. While they're not trying to scam you out of your money, this is a different kind of scam: if you're concerned about having been missold some PPI, then get on the phone to your authorised insurance dealer, and see how you can resolve it without the 'help' of those pestering you by text, email, and on the house phone.



According to Age UK, nearly half of people in the UK have been targeted by a scam, but less than five per cent of victims are likely to report the crime to the authorities. If you do find yourself a victim of scam crime, then just follow these simple steps to make sure you're in the clear. Report it. Don't be afraid to do so remember, scammers are targeting millions of us, so it's in the public interest to get it known about. Report what has happened to Action Fraud this contributes to teams of effort catching the perpetrators, and prevents other people from falling victim to crime.

**Talk about it**

Talk about it if you are feeling embarrassed or uncomfortable about experiencing a scam, then it's really important to get it out of your system. Explain to a sympathetic friend who won't judge you, or contact Victim Support or Think Jessica, organisations set up to help people in similar situations understand what they have been through. The Samaritans are also there if you need a kind listener, you can get in touch on 08457 90 90 90.

Get some advice if you have lost money or racked up some debt as a result of a scam, contact your local Age UK. They are best placed to help you find out what to do next. Your local Citizens Advice Bureau will be helpful if you are having trouble paying your bills, or are worried about what to do next.

How can you help? NTS and the Royal Mail are working together to train postal staff to recognise spamming tactics before they get through your letterbox, and to identify households who may be at risk. Louise Baxter, team leader of the NTSST says, "We really need the public to help us with this by being vigilant about mass marketing scams themselves, but also looking out for relatives or neighbours, particularly those who are elderly or vulnerable."

If you spot something that could be fraudulent, report it to Royal Mail on 03456 113413 or email scam.mail@royalmail.com

Ultimately...

The lesson to be learnt with all types of scams is that you shouldn't respond to them. If you are asked at any point for any personal information, follow it up with a phone call to the organisation that the email, letter or phone call purports to be from, to verify that it is legitimate. It's better to be safe than sorry.

