

REPORTING A SCAM

If you or someone you know has fallen victim to a scam, you should report it to the police on **101** and to Action Fraud on

0300 123 2040

Don't be embarrassed

If you did fall victim to the scam, do not feel ashamed, or think that you were to blame in any way. Victims of scams are just like victims of any crime – they have been targeted by criminals and bear no culpability for the crime.

The quicker you act, the sooner you might stop someone else becoming a victim.

You should also tell your Neighbourhood Watch coordinator, so that they can warn others in your area that this particular type of scam is being attempted. They will not reveal to anyone else that you have been a victim of it.



TELEPHONE SCAMS

Scammers will use any means to separate you from your money or your personal data – they operate over the phone, through the post, on the internet or face-to-face, often on the doorstep.

They will do their best to persuade you that they, or whatever it is they are offering you, are genuine — and will usually appear to be polite, friendly, and professional. It can be easy to be taken in by them — after all, they do this for a living!

However, there are also lots of signs that might indicate that all is not what it seems. Many scams follow certain patterns, and once you know what to look for, they can be easy to spot.

Here is one of the most common scams targeted at older people, and how you can avoid falling victim to it:

How does it work?

Telephone calls are a popular tool of scammers. They might call you pretending to be your bank, and ask for your PIN number or password, or tell you you've been defrauded and ask you to move your money to a safe new account.

They might even offer to send a courier to your house to pick up your bank card.

They might try to sell you investment opportunities in exotic offshore assets like diamonds or wine.

They might offer you a free review of your pension, suggesting they can convert some of it to a low-tax or tax-free lump sum.

They might say they are collecting for charity, and ask for your bank details to set up a direct debit.



Or they might claim your computer is faulty and that they can fix it, if you just tell them your password or give them access to it remotely.

All of these are scams. Just hang up the phone.

SPOT THE SIGNS!!

Any one of these signs could indicate it's a scam phone call:

- The caller asks you to transfer money to a new account for fraud reasons
- They phone to ask for your 4-digit PIN or online banking password.
 Even if they ask you to tap it into your telephone keypad rather than saying it out loud, it's still a scam
- The caller doesn't give you time to think, tries to stop you speaking to another householder or is insistent and makes you feel uncomfortable
- They say you've been a victim of fraud and offer to send a courier to your home to collect your cash, PIN, payment card or cheque book.



DON'T BE A SCAM VICTIM!

Next time you receive a phone call from someone you don't know, remember these rules to keep yourself safe from scammers:

- Never agree to anything over the phone. Just hang up if you feel at all wary of a caller.
- Don't assume a caller is genuine just because they already have some details about you, such as your name. Criminals will often already have some basic information about you.
- Remember: Your bank or building society will NEVER contact you out of the blue to ask for your PIN, full password or to move money to another account. If you receive a call from your bank requesting any of these, hang up immediately.
- Never give out any personal information over the phone, such as bank account or credit card details, unless you made the call.

- If you're not sure about a caller who claims to be from a legitimate bank or company, you can always end the call and then call the company back yourself, using a phone number from their official website or letters sent to you. Always wait five minutes before calling back though, to ensure the first caller has hung up it takes both sides to terminate a phone call.
- Never give control of your computer remotely to a third party over the phone.
- Register your phone numbers with the Telephone Preference Service.
- Mobile phone users can also send a simple text message to opt out of unsolicited sales and marketing calls. To add your number to the UK's official 'Do Not Call' database, text 'TPS' and your email address to 85095. They will then email you to confirm your registration.