From phishing to smishing...

Ways to spot (and stop) a scammer

Email fraud – or 'phishing' – is where a scammer sends out a legitimate-looking email in an attempt to gather your personal and financial information. It can be very difficult to tell the difference between a real email and a scam email, but there are some common signs to look out for.

Phishing with friends

Scammers use different types of electronic messages to target their potential victims – so make sure you're aware of them all.

Vishing

Sometimes criminals obtain our phone numbers and call us to try and steal sensitive information. They may pretend to be from Microsoft, a bank or a phone company and will ask you to reveal personal details, passwords or bank details.

Smishing

Fake text messages are another thing to watch out for. You may even receive a text or a WhatsApp message from someone you know that seems genuine, but if they're asking for money or personal financial information, check before you respond. If in doubt, just block and delete.

Spear phishing

This is the most dangerous form of phishing. Instead of a generic message sent to thousands of people, the criminals go directly after you. They will seem to know you and will have already collected some of your personal information, typically through social media, to try and steal your confidential information.

Social media phishing

Scams on social media platforms like Facebook, X (formerly Twitter), TikTok and Instagram are becoming more common. Watch out for scams being sent through in-app messages.

Watch & learn

Here you can watch our video on keeping your pension safe. Or, scan the QR code.

Scan me

Here you can watch Action Fraud's video which has some useful tips on how to stay safe from scams. Or, scan the QR code.

Scan me

Don't get hooked...spot the signs

- Never download attachments or click on links from unknown senders. Clicking the link may send you to a fake site or install dodgy software (malware). Hover over links to see the destination web address (but scammers can sometimes superimpose real links over fake links, so be very careful). ***If it doesn't look right, don't open it.***
- Be cautious if someone you know sends a message with strange content. They may have been hacked.
- Poor grammar or spelling can indicate a phishing scam.
- Be cautious if someone you know calls you by your full name if you're normally known by a shorter version of it, such as Victoria instead of Vicky.
- Never give out personal or confidential information at the request of an email or phone call. No credible business will ask to receive information in this way (and Aptia will **never** contact you in this way to ask about your savings in the Sainsbury's Pension Scheme). If in doubt, call the sender on a trusted number to check.
- If you've received a phone call, watch out for the 'open line'. This is where scammers wait on the line, keeping it open after you've hung up. Some are even sneaky enough to have a dial tone playing when you pick up the phone again. They're hoping you'll call your bank or whomever straight away to verify the call. They'll then pretend to be that provider and the scam continues...
- Be wary of bogus traders or rogue traders who call uninvited at your home under the guise of legitimate businesses; sometimes the aim of the visit to distract you while their accomplice enters your property from another entrance looking for items to steal.

Top tip

Some home phone handsets have call-blocking technology pre-installed or you can buy a device that connects to your landline. There are also apps that filter spam and calls, or warn you about potential malware.
Scan the QR code or visit **this website** to read an Ofcom article that looks at how technology can help you spot – and avoid – a potential scam.

Scan me

How to stay safe when out and about

To stay safe when using free Wi-Fi, consider the following precautions:

- Only connect to networks that you trust
- Be aware of your surroundings and what people around you are up to
- Be careful what you click on. If it looks suspicious, don't click on it.

Powerful passwords

- Do not use obvious passwords that can be easily guessed from your social media feed, such as family or pet names, sports teams, town or street that you live in, date of birth etc.
- Create passphrases instead of passwords – it's proven we can remember phrases better than random words.
- Passphrases should contain at least three words – and you can add a few special characters to make it more secure.
- You can either remember the first letter of the words in your passphrase – eg, Tango was my first dog (Twm#1d) – or just remember the whole phrase: T@ngowasmy1std0g
- Never share your passphrases or passwords with anyone.
- Use the key chain function if you have an iPhone – this is a secure password management system that allows you to store and retrieve sensitive information, including passwords, secure notes, and even payment information.
- If you have an Android phone, you can use the approved password manager.
- Don't use the same password for different systems.

Report your suspicions

If you think you've been targeted by a scammer, report it right away.

- Call Action Fraud on **0300 123 2040** or report it at **actionfraud.police.uk**
- Call the Financial Conduct Authority on **0800 111 6768** or use their simple online reporting form at: **fca.org.uk/contact**
- Forward suspicious emails to **report@phishing.gov.uk** and texts to **7726**; this notifies the National Cyber Security Centre (NCSC), who have the power to remove scam email addresses and websites.

If you're worried that someone is trying to scam you out of your savings in the Sainsbury's Pension Scheme, please contact Aptia via their CAP service at **pensionuk.aptia-group.com**

Telephone: 0345 072 6772

Remember, despite what anyone claims, you **cannot** access the money in your pension before the age of 55* (unless you are in very poor health). Not only do you risk being scammed out of your life savings, you will also face a hefty fine from HM Revenue & Customs for unauthorised access.

*the minimum pension age is increasing to 57 from 6 April 2028.