Protect your pension

Fraudsters are always on the lookout for ways to get hold of your pension benefits.

You may receive a call, message, text, or email from someone who is not genuine, trying to access your money or sensitive data. They might even pretend to be from an organisation you trust, such as your bank, HMRC or the Police.

It is essential you know what to look for and think carefully about what your next steps should be to keep your pension safe. We've included some top tips below.

How to know if a message is suspicious

Here are some things to look out for:

- ✘ Messages with generic and non-personal greetings such as 'Dear Customer' or 'Dear Member'.
- ✘ Promises of a short-term offer, a prize or a deal that seems too good to be true. Fraudsters often look to exploit emotions such as fear, greed or pity and create a sense of urgency e.g. 'Pay Now', 'Big Cash Prize'.
- ✘ Content with errors, poor spelling, or grammar.
- ✘ Communications issued from unusual email addresses or websites. Check the address for subtle misspellings, additional characters, or other irregularities.
- ✘ A request for further information, such as your personal details or bank account, particularly if you're asked to follow a link to fill it in.

Ways to protect your pension

- ✔ Stop, think, and consider: if the request doesn't seem right, it might not be.
- ✔ If you're on a call and feel unsure, disconnect the caller then call back the organisation on a telephone number found from an official source such as a previous bill.
- ✔ Don't give away your online banking PIN, passcode, or password, especially out of the blue. Your bank will never ask for this, even if you want to move money from one account to another.
- ✔ Think about how you use social media – only connect with people you know and keep important information private.
  The National Cyber Security Centre (NCSC) has guides for setting privacy controls on the biggest social media platforms. Visit **https://www.ncsc.gov.uk**
- ✔ Create strong passwords/passphrases to protect your accounts. Never reuse the same password and try not to include information others might be able to guess or find out easily, such as your pet's name.
- ✔ Keep your devices secure by enabling the screen lock and passcode and installing software updates as soon as they become available. You can also use multi-factor authentication as a second line of defence.
- ✔ Look for a padlock in your browser address bar to confirm your web connection is secure.

For more information about scams visit **https://ukpensions.uniper.energy/support/pension-scams** or **https://www.fca.org.uk/scamsmart**

If you suspect that you've seen a scam, you can call Action Fraud on 0300 123 2040 or the FCA Consumer Helpline on 0800 111 6768.