Gone phishing: fraudsters want your money

Financial scams are on the increase.
The Trustees of the ITV Pension Scheme want you to be vigilant to protect yourself. This handy leaflet explains how fraudsters work and what you can do to avoid becoming the victim of fraud.

Be vigilant

Fraudsters use a method called phishing to trick you into handing over sensitive information or downloading something harmful to your computer or mobile device. Phishers will typically pretend to be a well-known company or organisation. Their emails or text messages will ask you to verify some personal details or log on to a fake website.

Spot the signs

There are a few things you can watch out for:

- Emails that don't address you by your name, only your email address.
- Messages that contain errors and poor grammar.
- Website addresses that look similar but are fake.
- An offer that sounds too good to be true, such as a tax refund from HMRC.
- Being asked to do something quickly to get a good deal or avoid a service being disconnected is usually a sign of a scam.

If in doubt, close and delete the email or text message. Contact the organisation using a different method using a phone number you've looked up yourself.

If we call you, we'll never ask for your full bank details. We'll never talk to you about ITV shares.

If we need to call you and you're not sure a call is from us, just call us back. Our number is:

01772 884488

Your pension savings are very attractive to fraudsters. Find out how you can protect them by reading the enclosed leaflet ***Don't let a scammer enjoy your retirement.***

Replace passwords with passphrases

Use upper and lower case and add punctuation.
For example: *!WANTtoStaySafeOnline*

Keep it secret

Don't tell anyone your passwords or passphrases and never give secure information to cold callers.

Go direct

Visit websites directly rather than clicking a link in an email.

Be alert

Fraudsters can mimic an organisation's name in an email, so make sure you check who an email is really from by clicking the sender's name. They can also mimic the number you see on your phone display to make a call seem genuine. If your 'bank' calls and asks you to call them back the call is probably a scam. If you want to check with your bank, wait a while before calling them and, if you can, call from another phone.

Trust your instincts

or get a second opinion

If something doesn't feel right, stop and check. If in doubt, speak to family or friends, and only ever contact a company using details you know are real.

Do I know you?

Be wary of emails from unknown senders and don't click links in suspicious emails or respond to unknown mobile texts or messages.

Remember, fraudsters target everyone. Don't be tricked into handing over personal information or giving your money away.

If you've received a suspicious email or been the victim of a scam, report it to Action Fraud at

www.actionfraud.police.uk

December 2020
(2961)