September Cyber Scam Update

5 million pension savers could put their retirement savings at risk to scammers

New figures show cold calls, exotic investments and early access to cash among most persuasive tactics used by fraudsters. As well as this, those who consider themselves financially savvy are just as likely to be persuaded.

The Financial Conduct Authority (FCA) and The Pensions Regulator (TPR) are joining forces again this summer to warn the public about fraudsters targeting people's retirement savings. This warning comes as new research suggests that 42% of pension savers, which would equate over 5 million people across the UK, could be at risk of falling for at least one of six common tactics used by pension scammers.

The likelihood of being drawn into one or more scams increased to 60% among those who said they were actively looking for ways to boost their retirement income. Pension cold calls, free pension reviews, claims of guaranteed high returns, exotic investments, time-limited offers and early access to cash before the age of 55 could all tempt savers into risking their retirement income.

Pension savers were tempted by offers of high returns in investments such as overseas property, renewable energy bonds, forestry, storage units or biofuels. However, exotic or unusual investments are high-risk and unlikely to be suitable for pension savings. Nearly a quarter (23%) of the 45-65-year-olds questioned said they would be likely to pursue these exotic opportunities if offered them.

Helping savers to access their pensions early also proved to be a persuasive scam tactic. One in six (17%) 45-54-year-old pension savers said they would be interested in an offer from a company that claimed it could help them get early access to their pension. However, accessing your pension before 55 is likely to result in a large tax bill for the saver.

Four simple steps to protect yourself from pension scams:

1. Reject unexpected pension offers whether made online, on social media or over the phone.
2. Check who you're dealing with before changing your pension arrangements – check the FCA Register or call the FCA contact centre on 0800 111 6768 to see if the firm you are dealing with is authorised by the FCA.
3. Don't be rushed or pressured into making any decision about your pension.
4. Consider getting impartial information and advice.

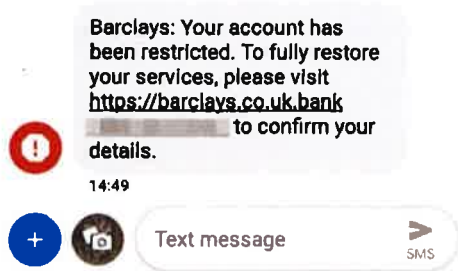
If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or http://www.actionfraud.police.uk

If you would like support as a result of becoming a victim of any crime, contact Victim Support on 01926 682 693.

Scammers target Barclays customers with fake texts

Action Fraud received over 50 reports about fake text messages purporting to be from Barclays bank. The texts state that the recipient's account has been "restricted" and asks the recipient to "confirm" their details in order to "restore" services.

The links in the messages lead to malicious websites that are designed to steal personal and financial information.



Top Tips:

- A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account. Only give out your personal or financial details to use a service that you have given your consent to, that you trust and that you are expecting to be contacted by.
- Don't be tricked into giving a fraudster access to your personal or financial details. Never automatically click on a link in an unexpected email or text.
- Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.
- Just because someone knows your basic details (such as your name and address or even your mother's maiden name), it doesn't mean they are genuine.

September Cyber Scam Update

The counterfeiting identity crisis: why buying fake goods online puts you at risk of fraud

Counterfeit goods websites often give the impression of using security authentication to give the site an air of authenticity. This includes the use of recognised images of reputable companies such as Visa, Mastercard and PayPal.

Additionally, many will also claim to have security software and secure transaction verification in place, again using reputable images such as Verisign and McAfee to give them a false 'trust seal'. These images are usually copied and embedded into the illicit website and the sites themselves will not have been approved by the firms.

The authenticity of these trust seals can be confirmed if the consumer attempts to click on any of them – original seals will direct you to the genuine security company. On counterfeit websites these links will not function, as they have no authorised hyperlink attached and will just be embedded images.

How to identify and avoid counterfeit websites:

- The site will usually have grammatical and spelling mistakes; the people behind these sites will try to deceive you by slightly changing the spelling of a well-known brand or shop in the website address;
- Images and web pages will fail or take a substantial amount of time to load;
- Images will have been copied and are usually edited to fit into certain website templates – the pictures may not look proportionate as they have been stretched or reedited;
- There's often lots of different fonts on the website and it won't have a professional finish;
- Hyperlinks to associated content will fail to work.
- Look to see where the trader is based and whether they provide a postal address – just because the web address has 'uk' do not assume the seller is based in the UK. If there is no address supplied or there is just a PO Box or email, be wary;
- Only deal with reputable sellers and only use sites you know or ones that have been recommended to you. If you have not bought from the seller before, do your research and check online reviews. People will often turn to forums and blogs to warn others of fake sites;
- Ensure the website address begins 'https' at the payment stage – this indicates a secure payment;
- Keep security software and firewalls up-to-date.

MONTHS TOP TIPS

Protect yourself from Viruses and Malware:

- Make sure your computer has a firewall and reputable anti-virus software. Without these, your computer has no defence to block infections.
- Take care downloading files. If you don't know someone who's sent you an email with an attachment, or you're not sure about a website offering a file to download, don't do it out of curiosity.
- Browse safely on the web. Get to know the risks and use the same level of caution as you would in the real world.

Keep up to date with the latest updates on Community Safety in Warwickshire.

Like us on **Facebook**: www.facebook.com/SafeinWarwickshire

Follow us on **Twitter**: @SafeInWarks

Visit our **site**: www.safeinwarwickshire.com

Phantom delivery scam warning as fraud cases increase dramatically across UK

The public are being warned about a new and confusing new delivery scam. Fraudsters obtain people's credit card details and then pose as them to order small, high-value items such as mobile phones.

They're delivered to the cardholder's address, so no red flags are raised with the card issuer or online retailer, but then the tricky part comes in.

The fraudsters visit the cardholder and explain that the parcel was "delivered in error" and ask for it back. The cardholder, in all innocence, hands over the item not realising that they have actually paid for it.

Top Tips:

- If you receive an unexpected high-value package such as a phone, contact the retailer immediately and arrange for it to be sent back, as the scammer may have attempted to intercept the delivery or will pose as a courier to collect the item.
- Check their credentials and call the company they claim to be representing. If you have any fears, contact the police.
- Identity theft is also on the rise so if you spot any suspicious activity on your account report it to your bank immediately.

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or http://www.actionfraud.police.uk

If you would like support as a result of becoming a victim of any crime, contact Victim Support on 01926 682 693.