October Cyber Scam Update

Scammers Using A Simple Con To Get Into Online Bank Accounts

Residents are being warned of a scam involving some simple techniques which criminals are using to access online banking accounts. The scam begins with a phone call, claiming to be from your bank, stating that suspicious activity and unusual transactions have taken place on your account.

Security checks are then made to verify your details, similar to those made by genuine phone calls from a bank. The caller then claims that they are noticing money transfers are taking place between your accounts. Next, the caller says they are sending over a verification code to your mobile phone (the number of which they received as part of the security checks). They ask the number to be read out loud to verify the correct number has gone through to the right phone.

The scammer uses this code to set up the banking app on their phone in YOUR name.

Further details are then verified, with callers asking for the certain letters in your password. This is used to sign into your account. By this point, they are able to claim it is not a scam, by referring to recent transactions you have made, as they have managed to successfully log into your account.

The final part of the scam involves asking you to delete any mobile banking app which you may have. This is to ensure you do not see what the criminals are doing on your accounts; and to make sure you do not log in to the account, and log them out of it in the process.

TOP TIPS To Avoid This Scam:

- **Never** read verification codes over the phone - this should just stay with you.
- The bank will **never** get you to use a card reader to generate a pin or code.
- If the bank rings you, ask them what they want and call back from a different phone; using the number on the back of your credit or debit card.

Become A Cyber Champion & Help Others In Your Local Area

The Cyber Crime Advisors are offering YOU the opportunity to receive free training to help spread awareness of cyber crime.

Cyber Champions are trained to spread awareness of cyber crime, how to prevent it and where to report such issues and seek support. As a Cyber Champion, you will be in a better position to protect yourself, friends, family and your community. You don't have to have any prior knowledge of IT or the internet to be a Cyber Champion.

The only thing we ask in return is that you use the training to help spread awareness in your own way. This can be anything from giving advice to a friend/family member or sharing articles on social media about how to keep safe, to helping educate groups you work with. There is no pressure or formal requirement to do anything.

If you're interested in becoming a Cyber Champion, or to find out more information, email: samslemensek@warwickshire.gov.uk

Watch Out For MORE Scam PPI Emails, Phone Calls & Text Messages

Fraudsters are posing as the Financial Conduct Authority (FCA), to cold call customers stating that they are eligible for a PPI claim. They are also using text messages and emails to convince the intended victims that their PPI claim is legitimate - but this may not be the case. The fraudsters tell you *how much* PPI you can claim back but emphasise a need for an advance fee payment in order to make a successful claim.

An increase in these types of frauds is expected, as the FCA launched a new campaign urging people to make a decision relating to PPI, before the deadline on 29th August 2019. If you use third party organisations to assist with your claim, you can check to see if they are legitimate by carrying out independent research on them. You can also check the FCA's website for company details, as the FCA regulates the financial services industry.

TOP TIPS

- Never take up offers of PPI claims on the spot from cold calls, texts or emails.
- Check the FCA website for details of the company.
- Don't give your bank account details or sensitive information to any unsolicited message.

If You Are Affected

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or 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.

Make a scam/rogue trader complaint to Trading Standards via Citizens Advice Consumer Service on 03454 040506.

October Cyber Scam Update

Action Fraud Launches Counterfeit Goods Campaign

When shopping online, consumers part with personal details such as addresses and financial details which *could* allow fraudsters to set-up new websites selling counterfeit goods in their name.

400 people have been contacted by Police in the last 2 years to tell them that their identity is believed to have been stolen, with websites opened in their name, after purchasing counterfeit items online.

TOP TIPS:

- Trust your instincts: If an offer looks too good to be true, it probably is.
- Check the website: The spelling & grammar on the website, and in the web address, will look suspicious. Those behind the sites will try to deceive you by slightly changing the spelling of a brand in the website address.
- Look to see *where* the trader is based and if they provide a postal address – even if the web address contains 'uk'; do not assume the seller is based here. If no address is supplied, or it is only a PO Box, be wary.
- Only deal with reputable sellers & only use sites you know, or ones 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 web address begins 'https' at the payment stage – this indicates a secure payment.
- Ask the trader if there is a returns policy or guarantee. Many rogue traders do not offer this.
- Watch out for pop-ups appearing asking you to confirm your card details before you are on the payment stage.
- **Never** enter your PIN online.

Equifax Data Breach - How To Protect Yourself

Equifax has confirmed that around 400,000 UK consumers have been affected by its recent data breach. The main risk from this is a rise in targeted phishing emails.

Fraudsters can use the data released in the breach to make the phishing messages look more credible, **including using your real name** and statements such as:
'To show this is not a phishing email, we have included the month of your birth and the last 3 digits of your phone number'.

These phishing messages may be unrelated to Equifax, and may use more well-known brands. It is unlikely that any organisation will ask their customers to reset security information or passwords as a result of the Equifax breach, but this may be a tactic employed by criminals.

While in typical phishing emails your real name may not be used, in this case, the fraudsters are likely to have, and will use, your name. Extra caution is advised if you receive a message that claims to be from an organisation you deal with - especially when there are attachments or links which take you to sites asking for more personal information.

Fraudsters may also call. If you do receive a phone call that is suspicious, do not give over any information. Hang up the phone. You should then contact the organisation the caller claimed to be from – but never use the details they provided during the call.

Follow Us On Social Media For The Latest Cyber Crime News

Facebook: facebook.com/cybersafewarwickshire
Twitter: @CyberSafeWarks
Instagram: Cyber_Safe_Warks

Or visit www.cybersafewarwickshire.com

OCTOBER'S TIP OF THE MONTH: Strengthen Your Passwords By Using THREE RANDOM WORDS

- Some of the most common passwords used globally are 'password'; '123456', 'football' and 'password123'

- These are not strong, and allows criminals to access your online accounts with great ease

- Many now use names of pets, children, hobbies - and follow it up with a date of birth or anniversary to make a memorable number

- **ALL** of this information is online about us across websites and social media - so is easy for cyber criminals to find for themselves

- Get stronger passwords by combining THREE RANDOM WORDS (e.g. ChampionSupportUpdate)
- Keep the capitals in; add in a couple of numbers (e.g. 2017) - and for added strength, use a 'special character' at the end (e.g. ?)
- ChampionSupportUpdate2017? is much stronger, more unique and hopefully not too difficult to remember!

If You Are Affected

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or 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.

Make a scam/rogue trader complaint to Trading Standards via Citizens Advice Consumer Service on 03454 040506.