September Cyber Scam Update

Identity Theft At An 'Epidemic Level'

Identity theft is reaching "epidemic levels", according to fraud prevention group CIFAS. ID fraudsters obtain personal information before pretending to be that individual and apply for loans or store cards in their name.

A total of 89,000 cases were recorded in the first six months of the year by UK anti-fraud organisation CIFAS.

This is a 5% rise on the same period last year and a new record high. According to our latest Warwickshire Cyber Crime Survey, there were an estimated **9,900** cases of identity fraud in the county over the last 12 months.

4 in 5 identity frauds committed now take place online, and is affecting every one of all ages. In order to commit identity fraud, a criminal only needs your name, date of birth and address.

TOP TIPS

- Limit the amount of personal information you give away on social networking sites. Your real friends know where you live and your birthday, so this doesn't need to be on social media.
- Consider updating the privacy settings on your social media too.
- Update your computer's firewall, anti-virus and anti-spyware programmes; up to 80% of cyber-threats can be removed by doing this.
- Never share passwords or PINs (personal identification numbers) with others.
- Use strong passwords and PINs - don't use your date of birth or your child's name, include a mix of upper and lower case letters, numbers and punctuation marks
- Do not use the same password or PIN for more than one account
- Shred all your financial documents before you throw them away

More information about staying safe from fraud online can be found on the Cyber Safe Warwickshire website.

EasyJet 'Free Flights' Offer Takes Off On Social Media

EasyJet is warning Facebook users not to be taken in by a "free flights" scam that has gone viral on social media. The scam claims to offer 2 free tickets to everyone that participates in an online survey, in celebration of the airline's 22nd anniversary.

When users click on the link, they are taken to a malware site that asks for their Facebook details. The scam has rapidly spread as it says that users must share the post in order to claim their free tickets. The post said there were just "332 remaining so hurry up!"

TOP TIPS

- Genuine competitions of this nature will only be hosted on the official EasyJet Facebook page.
- Don't click on links to alleged vouchers, competitions or offers on social media adverts – if you need to 'share' the offer in order to register, it may not be genuine
- Always go directly to the website the offer is claiming to be from to redeem these.

GOOD NEWS: Cold-Calling Ban On Pension Companies To Include Texts & Emails

A ban on cold-calling by pension companies will include texts and emails, the Government has announced, as it cracks down on scammers who target savers' retirement funds.

The ban will prevent all cold calls, emails and texts about pensions, and will be enforced by the Information Commissioner's Office (ICO). The ICO has powers to fine companies up to £500,000 if they break its rules.

TOP TIPS from The Pensions Regulator to avoid becoming a victim of a pension scam:

- **Hang up!** If you are cold called about your pension, hang up.
- **Check** the credentials of the company and any advisers – who should be registered with the Financial Conduct Authority.
- **Ask** for a statement showing how your pension will be paid at retirement and question who will look after your money until then.
- **Speak** to an adviser that is not associated with the deal you've been offered, for unbiased advice.
- **Never** be rushed into agreeing to a pension transfer.

For more information about pension scams, visit www.thepensionsregulator.gov.uk. Before you sign anything, call **The Pensions Advisory Service** on **0300 123 1047**.

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.

September Cyber Scam Update

LinkedIn Account Email Update Warning

An email, which has the subject “LinkedIn Update” claiming that LinkedIn is updating its “Services Agreement and Privacy" is being used by criminals to access your personal information.

The message warns that your account will be deactivated if you do not click the link and update your account. LinkedIn did not send the email, and your account will not be deactivated if you don’t click the link. The email is a scam designed to steal your LinkedIn account login details. If you click the link, you will be taken to a fraudulent website that has been built to look like the real LinkedIn login page.

On the fake site, you will be asked to enter your email address and password to log in. After entering your details, you’ll see a message claiming that you’ve successfully completed the 'update'.

Online criminals can now use the information you provided to hijack your **real** LinkedIn account. Once they have gained access to the account, the criminals can use it to send scam messages to your LinkedIn contacts in your name.

Criminals can still use information entered even if you do not have a LinkedIn account. If your password is the same across other websites, the criminals may then be able to access these, not just LinkedIn accounts.

TOP TIP

• Change your LinkedIn password, as well as passwords for ANY site with the same one, or ones which are very similar.

Action Fraud Reissues Courier Scam Warning

Action Fraud have issued a new warning about Courier Fraud, after one victim had £6,200 stolen from a criminal claiming to be a 'Sergeant Douglas'.

Courier scams work when you are called by someone pretending to be from your bank, building society or even the Police. They convince you to tell them your card details over the phone after they claim fraudulent activity has appeared on your account, or that your card is about to expire. They then arrange for a courier to pick up your card to take it away for evidence, or to have it destroyed.

In reality, the card is collected by the fraudsters to withdraw money from your account.

TOP TIPS

• Banks & the police will never call you to ask you to verify your personal details or PIN by phone or offer to pick up your card by courier. Hang up if you get a call like this.
• If you need to call your bank back to check, wait five minutes; fraudsters may stay on the line after you hang up. Alternatively, use a different line altogether to call your bank.
• Your debit/credit card is yours – don’t let a stranger take it off you. You should only ever have to hand it over at your bank. If it’s cancelled, you should destroy it yourself.

Spot The Signs

• Someone claiming to be from your bank or local police force calls you to tell you about fraudulent activity but is asking you for personal information, or even your PIN, to verify who you are.
• They try to offer you peace of mind by having somebody pick up the card for you to save you the trouble of having to go to your bank or local police station.

Follow Us On Social Media For The Latest Cyber Crime News

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

SEPTEMBER’S Top Tip: Watch Out For Text Scams

- It’s not just emails which criminals will use to scam people out of money, or to get their personal details.
- Text messages and social media are becoming increasingly popular methods used.
- Always double check before responding to a text – Google the phone number used to see if others have reported issues with it.
- Just because it comes from a friend, doesn’t mean it is always genuine – if it looks suspicious, don’t click on the link, and don’t reply with your personal details.
- Contact your mobile phone provider if you fall victim to a scam of this kind

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.