March Cyber Scam Update

Dating & Romance Scams Warning

The majority of accounts on dating websites are genuine people looking for romance, but fraudsters may try to contact you by making fake profiles, getting in touch and building what feels like a loving relationship.

Once a fraudster using a fake dating profile is confident that they've won your trust, they will tell you about a problem they're experiencing and ask you to help out by sending money. They may have arranged to visit you, but need money to pay for the flight or visa.

They may tell you everything has been booked but their ticket has been stolen, and you need to send money quickly to get them on the next flight.

They might also state they or somebody else they know is ill and need money for medical treatment. Fraudsters will also try and obtain personal information from you so they can commit identity fraud.

TOP TIPS

- Avoid giving away too many personal details when dating online. Revealing your full name, date of birth and home address may lead to your identity being stolen.
- Never send or receive money or give away your bank details to someone you've only met online, no matter how much you trust them or believe their story.
- Use a reputable dating website and messaging service. Fraudsters will want to quickly switch to social media or texting so they aren't monitored by the website.

Trusted dating sites will monitor their own messaging services to stop dating fraud from occurring.

Storm Doris Cold Caller Warning

Rogue traders use unusually stormy weather as a way of persuading people that they need work done on their property – such as repairing loose roof tiles or removing damaged trees. You can't tell a good trader from a bad one on the doorstep.

TOP TIPS

- Avoid buying from unexpected/unknown doorstep traders.
- Also be aware of traders contacting you via phone or email out of the blue.
- If you are looking for an approved and vetted trader, consider using Warwickshire Trading Standards new approved trader scheme - No Rogue Traders Here

Streetlife Users Warned To Be Cautious Over Transfer To NextDoor.com

Many people across the UK have been using the useful community messaging site, Streetlife.

Now, with very little warning, users are being told they need to transfer to the US community messaging site Nextdoor.com, to which Streetlife has recently been sold.

There is widespread concern that NextDoor, unlike Streetlife, publishes not only people's names and their street but also their house number. It is possible to delete the house number if you go to their website but this company should not be compromising users' security in such a way in the first place.

Some locals have already unsubscribed; others are thinking of so doing. It remains to be seen whether NextDoor will respond positively to people's concerns.

streetlife.com
the local social network

National Cyber Security Centre Officially Opened

A new centre to protect the UK against cyber-attacks has been officially opened.

National Cyber Security Centre
a part of GCHQ

The National Cyber Security Centre (NCSC) in London is designed to improve Britain's resilience to attacks.

Among its projects, the NCSC is working on trial services to take down tens of thousands of phishing sites affecting the UK.

If You Are Affected

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.

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

March Cyber Scam Update

Tax Rebate Scam Warning

NHS members are being targeted by tax rebate companies that claim they offer services where they can get a tax rebate on the victim's behalf.

The fraudsters request the victim sign forms to give them permission to liaise with HM Revenue & Customs (HMRC) on their behalf, stating their fee will be charged after the rebate is received.

HMRC have confirmed that they have issued refunds to the companies in relation to requests received and authorised by the staff member. Once the refund is obtained all contact with the companies are broken and the victim does not receive their rebate.

The scam has affected NHS staff, Police, airline staff and teachers. However this list is not exclusive and **anyone** can be targeted.

TOP TIPS

- Do research online to ensure the company is reputable by checking the registration details are correct and by viewing feedback online.
- Do not feel pressured to sign documentation without doing some basic checks.
- Do not respond to unsolicited emails, texts or calls offering rebate services.
- Make sure that you are aware and agree to the commission that will be paid to a rebate company prior to signing any documents.

University Spear Phishing Emails

Fraudsters are sending out a high volume of phishing emails to university email addresses claiming to be from their own HR department. These email addresses are either spoofed, or in some cases using compromised university email accounts.

The email claims that the recipient is entitled to a pay rise from their department and to click on a link to claim the pay rise. This link then takes you to a spoof university website telling you to enter your personal details (including university login details and financial information). These financial details can then be used by criminals, and the login details are usually passed around and sold for future fraud campaigns.

It is advisable that all universities prompt all staff and students to change any password associated with their university email/IT accounts. Due to potential data breaches, it is recommended that universities discuss with the IT departments about issuing a mandatory password reset for all users.

TOP TIPS

- Don't click on links or attachments from email addresses you don't recognise.
- Use strong passwords which include a mixture of letters, numbers and special characters, and include both upper and lower case characters.
- If you think your bank details have been compromised, you should immediately contact your bank.

Facebook Scams Warning

Facebook scammers are making copies of legitimate profiles to trick users into revealing financial and personal details, in a tactic known as 'cloning'.

They do this by creating a new account using the exact same name, personal information and profile and cover photos included on your own profile – even going as far as copying your statuses.
This allows them to confidently approach your friends and family members, who could unknowingly accept a friend request from the clone account and eventually share private information with it, depending on how convincing their messages appear.

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

www.facebook.com/SafeinWarwickshire
@SafeInWarks
www.safeinwarwickshire.com

March's TOP TIP: Social Media Safety

Be aware against phishing scams, including fake friend requests and posts from individuals or companies inviting you to visit other pages or sites.

Be aware of what friends post about you, or reply to your posts, particularly about your personal details and activities.

Be aware of what friends post about you, or reply to your posts, particularly about your personal details and activities.

If You Are Affected

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.

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