April Cyber Scam Update

City of London Police warns public to keep online accounts safe from hackers

Action Fraud, the national reporting centre for fraud and cyber crime, received 15,214 reports of email and social media hacking between February 2020 and February 2021 – 88 per cent of which were from individuals who had their personal accounts compromised by criminals. When analysing historic data, the NFIB found that during the financial year 19/20, Facebook, Instagram and Snapchat were the most reported platforms on which people had their social media accounts compromised.

Compromised Facebook accounts were commonly used to facilitate fraud, whereas compromised Instagram accounts were often used to obtain intimate images of the account holder. Similarly, compromised Snapchat accounts were often used for blackmail offences, such as sextortion. The NFIB say the most common tactic criminals use to facilitate hacking offences is phishing messages, where recipients will be asked to click on a link which is designed to harvest their log in details and passwords. Other phishing messages may include a malicious attachment.

How to protect yourself and keep your accounts secure:

- Use a strong and separate password to protect your email. You should also protect your other important accounts, such as banking or social media.
- Enable two-factor authentication (2FA). It will help to stop hackers from getting into your online accounts, even if they have your password.
- Be cautious of social media messages that ask for your login details or authentication codes, even if the message appears to be from someone you know.
- If you can't access your account, search the company's online support or help pages. You'll find information about how to recover your account.
- You can report suspicious emails you have received but not acted upon, by forwarding the original message to report@phishing.gov.uk. You can report suspicious texts you have received but not acted upon, by forwarding the original message to 7726, which spells SPAM on your keypad.

What to do if your account has been compromised:

If you cannot access your account as it has been compromised, follow the NCSC's guidance on how to recover a compromised account. If a demand for payment is made, do not pay any money to the suspect in order to regain access to your account. It's likely the suspect will continue to demand more money instead of giving you control of your account back. If you have paid any money, contact your bank immediately and report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040 as soon as possible.

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.

WARNING: National Insurance scam leads to surge in calls to Action Fraud

Victims have reported receiving an automated telephone call telling them their "National Insurance number has been compromised" and in order to fix this and get a new number, the victim needs to "press 1 on their handset to be connected to the caller".

Once connected to the "caller", victims are pressured into giving over their personal details in order to receive a new National Insurance number. In reality, they've been connected to a criminal who can now use their personal details to commit fraud.

How to protect yourself

If you receive an unexpected phone call, text message or email that asks for your personal or financial details, remember to:

STOP - Taking a moment to stop and think before parting with your money or information could keep you safe.

CHALLENGE - Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

PROTECT - If you have provided personal details to someone over the phone and you now believe this to be a scam, contact your bank, building society and credit card company immediately and report it to Action Fraud at www.actionfraud.police.uk or by calling 0300 123 2040.

You can also contact CIFAS to apply for protective registration. This means extra checks will be carried out when a financial service, such as a loan, is applied for using your address and personal details, to verify its you and not a fraudster.

April Cyber Scam Update

Action Fraud warning as demand for tickets increases ahead of lockdown easing

As a result of the high demand for tickets, the National Fraud Intelligence Bureau (NFIB) are warning buyers to take extra care when buying tickets online. We are urging people to be wary of fraudsters selling fake or non-existent tickets to events. NFIB have already started seeing reports of non-existent tickets being advertised for sale online, some at inflated prices.

In February 2021, Action Fraud received 216 reports of ticket fraud. This is an 62% increase on the previous month and the highest number of reports received since March 2020 when lockdown restrictions were first implemented. Victims reported losing £272,300 in February 2021 – an average loss of just over £1,260 per victim.

It is anticipated that increased demand for tickets following lockdown restrictions will lead to greater numbers of victims and higher losses as a result.

Spot the signs of ticket fraud and protect yourself:

- Only buy tickets from the venue's box office, official promoter or agent, or a well-known and reputable ticket site.
- Avoid paying for tickets by bank transfer, especially if buying from someone unknown. Credit card or payment services such as PayPal offer greater protection against fraud.
- Be wary of unsolicited emails, texts or adverts offering unbelievably good deals on tickets. If it sounds too good to be true, it probably is.
- Is the vendor a member of STAR? If they are, the company has signed up to their strict governing standards. STAR also offers an approved Alternative Dispute Resolution service to help customers with outstanding complaints. For more information: star.org.uk/buy_safe

Every report matters. If you have been a victim of fraud or cyber crime report it to Action Fraud online or by calling 0300 123 2040.

Pension schemes urged to step up reporting to stop scammers

Data from the national fraud and Action Fraud shows a steady fall in pension scam reports from 1,788 in 2014 to 358 in 2020 – an almost 80% reduction.

While there has been a slight rise in reporting so far in 2021, TPR is calling on industry to be on high alert for criminal or suspicious activity and to sign up to its Pledge campaign to help combat pension scams.

So far, more than 200 organisations have signed up to the Pledge campaign, which is designed in part to encourage better reporting. The campaign follows changes the regulator has made to protect savers in light of COVID-19 including the introduction of new scams training for all trustees, (as a new module of the Trustee toolkit), and a 'warning letter' for all those looking to transfer out of a defined benefit pension.

Action Fraud figures show pension scam losses can range from under £1,000 up to £500,000. But the true scale of the amount lost to pension scams, and the number of victims, is likely to be much higher as victims often don't realise they have been tricked until many years later. And with the COVID-19 pandemic impacting many peoples' finances – despite the unprecedented government support – there are fears scammers will use this to their advantage to steal hard-earned cash from savers.

Scammers often approach people about a pensions or investment opportunity out of the blue with genuine sounding investments. They use sophisticated techniques to win trust before stealing people's hard-earned retirement cash and can leave victims facing retirement with limited income and little or no opportunity to build back their savings.

TOP TIPS: Virus & 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