April Cyber Scam Update

Council Tax Scam Warning

Fraudsters have been phoning victims telling them that they are calling to let them know that they have been placed in the wrong council tax bracket for a number of years and that they are entitled to a rebate, they normally say that this rebate should be worth £7000.

Once the victim is convinced, the fraudster tells them that in order to receive the rebate they will need to pay an administration fee in advance; the payment they ask for varies between £60-350. The victim provides the details and makes the payment, but then is no longer able to make contact with the person they spoke to on the phone.

TOP TIPS

- Never respond to unsolicited phone calls
- Your local council won't ever phone or email out-of-the-blue to discuss a council tax rebate, if you receive a message of this nature, put the phone down straight away, and delete the email.
- No legitimate organisation will ask you to pay an advanced fee in order receive money; so never give them your card details.
- If you think you have been a victim of fraud, hang up the phone and wait five minutes to clear the line as fraudsters sometimes keep the line open. Then call your bank or card issuer to report the fraud.
- Where possible, use a different phone line to make the call.

Travel Firm ABTA Hit By Cyber Attack

The travel trade organisation, ABTA, says a cyber attack on its website may have affected about 43,000 people.

About 1,000 files accessed may include personal identity information of individuals who have made a complaint about an ABTA-registered travel agent.

It said the type of data which may have been accessed included:

- Email addresses and encrypted passwords of ABTA customers and members registered on the website
- Contact details of customers of ABTA members who have used the website to register a complaint
- Data uploaded to support a complaint made about an ABTA member since January 2017
- Data uploaded by ABTA members in support of their membership

ABTA said those who had uploaded contact details or documentation on the website should actively monitor their bank accounts, social media and email accounts, and "remain vigilant".
It has also offered people who may be affected a free-of-charge identity theft protection service.

The Ransomware That Targets Your Phones, TVs and Watch

Ransomware that targets mobile phones and smart TVs have been singled out by a report for its increasing risk. Ransomware makes a device unusable until a ransom is paid to the attacker - will target connected personal devices like phones, watches and TVs.

TOP TIPS To Reduce Your Risk

- update your device software as soon as it becomes available
- watch out for links in emails
- only download from websites which have HTTPS, an unbroken padlock or the word 'Secure' within the address bar

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.

April Cyber Scam Update

Over One Million Gmail & Yahoo Account Details Stolen

Log-in credentials for over one million Gmail and Yahoo accounts are being sold on a dark web marketplace.

Among the compromised accounts being offered are 100,000 Yahoo accounts. The information includes usernames, email addresses and **plain text** passwords.

A further 145,000 Yahoo accounts are also on sale, with details including usernames, email addresses and decrypted passwords.

950,000 Gmail accounts, with information including usernames, email addresses and plain text passwords have also been stolen from various sources.

TOP TIPS

Users worried about the security of their Gmail or Yahoo account, particularly if their accounts were compromised in any of the data breaches mentioned here, should **change their password immediately**.

Users can also **enable two-factor authentication** where it is offered, as it adds another layer of security to online services by sending a unique, one-time code to a mobile device, which has to be entered alongside the password.

April's TOP TIP: Watch Out For Ransomware

Ransomware is a form of malware that gives criminals the ability to lock a computer screen. The only way it says it can be unlocked is if you pay a ransom fee.

Avoid Ransomware getting onto your device by:
- not replying to, or clicking links in, unsolicited emails
- only visiting and downloading content from websites you know and trust (look for HTTPS, an unbroken padlock, or the word 'Secure' within the address bar)
- back up your files regularly to an external, physical hard drive

If you have ransomware on your computer:
- seek professional advice from an IT specialist, who may be able to remove the malware from the device
- report it to Action Fraud (see details below)

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

Banking Scam Text Message Warning

A warning has been issued to banking customers in the face of a new text message scam.

The scam sees fraudsters sending a text saying they are from your bank and they need you to update personal details or speak with you urgently.

The text can fall into previous genuine text threads, and will normally
ask customers to phone a number or click on a counterfeit website that
will then ask them to transfer money.

An example of the message can be seen below:

Santander advise that they have "measures in place" to detect this scam,
and ask customers who receive these messages to forward them to the
bank by entering smishing@santander.co.uk into the number field, but NOT to click on the link in the message, or reply to them.

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.