July Cyber Scam Update

Criminals targeting residents in council tax scam 'barrage'

Criminals posing as council staff are targeting people across the country in a new wave of council tax scams offering bogus refunds or threatening fines. Fraudsters are contacting residents by text, email and phone to con them out of money and access personal bank details. The scammers tell people they have either paid too much council tax and are due a refund which they offer to claim on their behalf for a fee. A similar scam demands payment for council tax arrears.

Another scam aims to convince people their property is in the wrong council tax band and offers to secure a refund, again in return for a payment – even though a council tax band reassessment is available for free. Fees of £150 have been quoted in the scams which falsely claim to be from local councils or the Valuation Office Agency in a bid to appear official and trick people into falling victim to them. Some also use the Government's GOV.UK branding in text messages and emails in a bid to appear more convincing, and often include a link to a fake official-looking website to claim the refund.

Top Tips:

- Anyone who receives an email, text message or phone call offering a council tax refund should not to give out any personal information, particularly bank account details, or debit or credit card details
- You should delete the email or text, block the sender and make sure they do not reply or click on any links, the LGA said. Any such phone calls should be brought to an end as quickly as possible.
- Residents, who wish to have their council tax band assessed, can do so for free by contacting the Valuation Office Agency. This information will have been supplied to residents with either a previous or current Council Tax bill.

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.

House buyers are being warned to be on their guard when purchasing new properties.

Conveyancing fraud is committed when criminals hack into the email chains between sellers and buyers and their solicitors and estate agents.

Waiting for the right time (usually on the day of sale completion) fraudsters send a spoofed or mimicked email informing the parties that bank account details have changed at the last minute and that money should be put into a different account.

The conveyancing process is particularly at risk because of the frequency of one-off and sizeable transactions.

Protection advice

- Get bank details from your solicitor either in person or over the phone at the start of the conveyancing process. Ask them to confirm the details by post.
- Always check the bank details and do not feel pressured into changing any details. If you receive an email stating a change in the bank details don't be afraid to question its authenticity.
- Avoid using public Wi-Fi systems to check emails when house purchases are being made.
- Avoid posting on social media about buying/selling your house or getting a mortgage.
- Make sure you have strong passwords for your accounts and have anti-virus installed on your devices.

What to do if you're affected

Victims should contact their bank as soon as they become aware that they've been tricked and ask them to contact the receiving bank and freeze the account.

July Cyber Scam Update

Google calendar scam puts strange events into people's schedule to trick them into being attacked

Strange invitations are showing up in people's calendars as part of a dangerous scam, cyber security experts have warned. The unwelcome events are actually ways of tricking people into cyber attacks that could see their data or money stolen.

Criminals are carrying out the exploit by inviting people to events through Google Calendar, which places that event into their schedule. That then serves as a link out to a URL – where a variety of different cyber threats might be lurking for anyone who clicks.

The invitations might appear with titles such as "You've received a cash reward," or "There's a money transfer in your name."

Top Tips:

- It is possible to ban people from adding invitations to your Google Calendar, which stops the scammers getting through at all.
- Doing so is relatively simple. Open up the site on a PC, head to the settings and click on "event settings", where an option for "automatically add invitations" should show.
- Switching that to "No, only show invitations to which I've responded" will stop people being able to add you to unwelcome events. It is also worth turning off the "show declined events" option, which will mean that any you do turn down will disappear rather than hang around.

MONTHS TOP TIP: Social Media

- Use a strong password. The longer it is, the more secure it will be!
- Use a different password for each of your social media accounts.
- Manage and regularly check your privacy settings.
- Never allow automatic logins. Don't have your computer's browser "remember" your login and password.
- Disable old accounts.
- Be selective when accepting friends, posting and clicking.
- Think twice before you post! Consider who will be seeing it.
- Avoid posting too much personal information.

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

Courier Fraud, Bogus Police and Bank Officials

Individuals have been receiving phone calls from people claiming to be a police officer or banking official

The suspect will say either:

- There has been fraudulent activity at the victim's bank and the staff at the bank are involved, the victim is then asked to withdraw money to either keep it safe or assist the police with their investigation
- The victim's card has been compromised and used to purchase goods by a suspect, the victim is requested to withdraw their money to keep it safe or hand over their bank card to the police
- Occasionally the victim will be told to dial a non-emergency extension of '161' to receive confirmation of the individual's bogus identity, the bogus official will advise the victim to lie about the reason for the withdrawal or purchase if challenged by staff, as the staff member is involved in the fraud
- A courier attends the victim's home address to collect the goods the same day, often the victim is given a code word for the courier as a way of authentication

Your bank or the police will never:

- Phone and ask you for your PIN or full banking password
- Ask you to withdraw money to hand over to them for safe-keeping
- Ask you to transfer money out of your account
- Send someone to your home to collect cash, PINs, cards to cheque books

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.