January Cyber Scam Update

TV License Phishing Scam

A phishing scam using TV licence renewal as bait has been circulating email inboxes around the UK, driving 5,057 complaints. The email, which tricks people into opening it with headings about licence expiry and incorrect information, leads victims through to a page where they're required to enter their account number, sort code and card verification number – everything needed for scammers to steal money from innocent victims.

The emails themselves look worryingly convincing, and headlines like "correct your licensing information" and "your TV licence expires today" feel suitably formal, too. A spokesperson for TV Licencing was quite clear, however: "TV Licensing will never email customers, unprompted, to ask for bank details, personal information or tell you that you may be entitled to a refund."

TV Licensing will never:

- email you to tell you that you're entitled to a refund.
- ask you to pay additional money for our services, e.g. when you're buying a licence or changing your details.

Fake Tax Scam for students

Thousands of fraud reports have been received by the tax authority from students at university and colleges across the UK. Fake emails, which use university addresses in a bid to appear legitimate, may tell people that they are owed money and encourage them to send their personal details.

The recipient's name and email address may be included several times within the email itself and the email will include links that redirect the recipient to websites where their data is stolen. The emails often spoof the branding of HMRC, Gov.UK or credit card branding.

Anyone targeted should not click on any links but can report cases to HMRC on their website, or by texting 60599.

Pension cold-calling

A ban has been introduced in a bid to prevent people falling victim to pension cold call scams, however, cold calling is currently still by far the most common method used to initiate pension fraud. Other scam tactics include:

- Unexpected contact about your pension via post or email.
- Promises of guaranteed high returns and downplaying the risks.
- Offering unusual or overseas investments that aren't regulated by the FCA.
- Claiming to be able to unlock money from an individual's pension (which is normally only possible from age 55).
- The FCA and TPR are urging the public to be ScamSmart with their pension and always check who they're dealing with.

Top Tips from the HM Treasury:

If you receive a cold call about your pension, get any information you can, such as the company name or phone number, and report it to the Information Commissioner's Office via their website or on 0303 123 1113.s.

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.

January Cyber Scam Update

Whatsapp Gold Scam

The 'WhatsApp Gold' scam has being doing the rounds since 2016. It has surfaced again in the form of a new message claiming that there is a video which will be launched called 'Martinelli'. The video itself is a hoax and does not seem to exist. The message also warns of links being sent out to sign up for 'Whatsapp Gold'.

Previous versions of 'WhatsApp Gold' messages have included promises of free flights and 'exclusive' access to enhanced features such as the ability to make video chats, send 100 images at once and delete messages hours after they have been sent.

Victims are urged to sign up via a download link. After clicking on the link they are redirected to a fake page and their phone will become infected with malware.

Top Tips:

- Any updates to WhatsApp will usually happen automatically through the app. If you receive a request to download 'WhatsApp Gold' do not click the link.
- Always install the latest software and app updates.

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

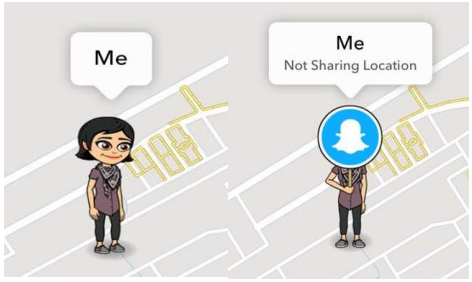
Follow us on **Twitter**: @SafeInWarks

Visit our **site**: www.safeinwarwickshire.com

Location Services on Snapchat

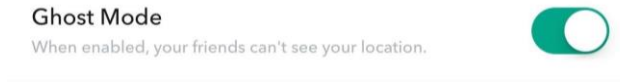
Opting out of Snap Maps:

Snap maps allow you to see where your snapchat friends are all the time, and allow them to see you.



All users are automatically sharing their location via Snap Maps, and need to opt out of it to hide your location:

- In photo taking mode, pinch the screen to open up Snap Maps
- When the map is open, tap on the settings cog wheel
- At the top of the settings, slide the bar on 'Ghost Mode' so it is coloured



- You can see if you are on Ghost Mode if there is a blue circle with a ghost covering your face on the map.

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.