October Cyber Scam Update

ALERT REMINDER: Test and Trace scams remain a threat

Residents should remain vigilant after being alerted to new reports of fraudsters posing as people from the NHS Test and Trace programme, launched to help control the COVID-19 virus.

There are concerns that the system is being targeted by scammers, who are pretending to be contact tracers in a bid to trick people into parting with their personal information.

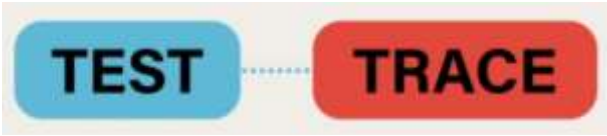
People will be alerted by the NHS Test and Trace service if they have been in close contact with someone who has tested positive for coronavirus.

Contact tracers will:

- call from 0300 013 5000
- send text messages from 'NHS' · ask people to sign into the NHS test and trace contact-tracing website
- ask for full name and date of birth to confirm identity, and postcode to offer support while self-isolating
- ask about the coronavirus symptoms
- ask people to provide the name, telephone number and/or email address of anyone they have had close contact with in the two days prior to symptoms starting (as with your own details these will be held in strict confidence and will be kept and used only in line with data protection laws)
- ask if anyone they have been in contact with is under 18 or lives outside of England

They will not ask:

- for bank details, or payments
- for details of any other accounts, such as social media
- set up a password or PIN number over the phone
- to call a premium rate number, such as those starting 09 or 087



Find out more about the NHS Test and Trace service by visiting - https://www.nhs.uk/conditions/coronavirus-covid-19/testing-and-tracing/nhs-test-and-trace-if-youve-been-in-contact-with-a-person-who-has-coronavirus/

If you have been a victim of fraud or cybercrime, please report it to Action Fraud at action.fraud.police.uk or by calling 0300 123 2040.

Victims of a courier fraud scam have lost almost £419,000

Courier fraud is when criminals call people impersonating banks or the police in order to convince them to hand over their cash, bank cards, or high value items, to a courier that's been sent to their home. Recent reporting to Action Fraud has highlighted that an increasingly popular tactic is for criminals to instruct the unsuspecting victim to purchase high value items such as gold coins and gold bullion. In the last three months, Action Fraud has received 13 reports relating to this particular M.O, with losses totalling almost £419,000.

TOP TIPS:

- Your bank or the police will never call you to ask you to verify your personal details or PIN by phone or offer to pick up your card by courier. Hang up, wait a few minutes and call your bank on a number you know to be genuine, such as the one on the back of your card
- Your bank or the police will not contact you out of the blue to participate in an investigation in which you need to withdraw money from your bank or to purchase high value goods, such as gold bullion.
- Your bank will never send a courier to your home to collect your card, PIN, or other valuables, therefore any requests to do so are a scam

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.

October Cyber Scam Update

Fake penalty charge emails reported over 1,000 in 24 hours

Action Fraud has received more than 1,400 reports about fake emails purporting to be from HM Courts & Tribunal Service. The emails state that the recipient has been issued a penalty charge for "the use of a vehicle on a road in the charging area which a charging scheme applies without payment of the appropriate charge." The link provided in the emails lead to genuine-looking phishing websites that are designed to steal personal and financial information.

TOPS TIPS:

- Your bank, or any other official organisation, won't ask you to share personal information over email or text. If you need to check that it's a genuine message, call them directly.
- Spotted a suspicious email? Forward it to the Suspicious Email Reporting Service (SERS) – **report@phishing.gov.uk**

THIS MONTHS TOP TIPS:

Protect yourself from Viruses and 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

Watch out for HMRC tax refund scams

Action Fraud are aware of scammers claiming to be from HMRC offering financial support as a result of coronavirus.

TOP TIPS:

- Don't click on the links or attachments in suspicious emails, and never respond to messages that ask for your personal or financial details, including requests to send images that prove your identity.
- HMRC will **never** text, email or phone you to ask for bank details, PINs or passwords.