October Cyber Scam Update

Interested in working to combat cyber crime in Warwickshire? We are recruiting for two Cyber Crime Advisers! More details here- https://www.wmjobs.co.uk/job/40087/cyber-crime-advisor/

British Airways Data Breach

British Airways have announced that personal and financial details of customers making bookings had been compromised in a recent data breach. About 380,000 transactions were affected, but the stolen data did not include travel or passport details. BA said the breach took place between the 21 August and on 5 September.BA said all customers affected by the breach had been contacted. The breach only affects those people who bought tickets during the timeframe provided by BA, and not on other occasions.

TOP TIPS

- Change your password for your BA account, and any other accounts which have the same, or similar, passwords
- Monitor your bank and other online accounts for any suspicious activity. Alert your bank immediately if you suspect anything.
- Be aware that fraudsters may refer to the breach in scam emails. This could involve them asking you to click on links to enter personal or financial details.

MONTHS TOP TIP: PHONE SCAMS

Some fraudsters will call your landline or mobile, pretending to be from your bank, building society, a government agency or someone you do business with.

- If a phone call/voicemail asks you to make a payment, log in to an online account or offers you a deal, be cautious
- Don't assume anyone who's sent you an text message – or has called your phone or left you a voicemail message – is who they say they are. Verify the information through another way.

Fake Car Insurance Fraud

Figures from the City of London Police's Insurance Fraud Enforcement Department (IFED) has revealed that 17-24 year olds are most likely to fall victim to fraudsters selling fake care insurance, also known as 'ghost brokers'. The reported losses for these victims total £164, 993, with each individual losing on average £912. They typically carry out the fraud by one of three ways: they will either forge insurance documents, falsify the details to bring the price down or take out a genuine policy, before cancelling it soon after and claiming the refund plus the victim's money.

TOP TIPS

- Trust your instincts – if an offer looks too good to be true, then it probably is.
- Ghost brokers often advertise on student websites or money-saving forums, university notice boards and marketplace websites.
- Be wary of ghost brokers using only mobile phone or email as well as WhatsApp, Snapchat and Facebook
- If you are not sure about the broker, check on the Financial Conduct Authority or the British Insurance Brokers' Association brokers: register.fca.org.uk and biba.org.uk.

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.

October Cyber Scam Update

Computer Service Fraud

Computer Software Service fraud can start with a phone call, an email or a pop-up message appearing on your computer, stating there is something wrong with your computer or internet connection and that it needs to be fixed. However, there will either be a demand for payment to fix it, or they will install software on the computer which will allow the criminals to access personal and financial details.

In 2017/18, Action Fraud received 22,609 reports of Computer Software Service fraud with a total of £21,365,360 being lost to fraudsters. An intelligence report run by the City of London Police's National Fraud Intelligence Bureau has shown that men and women are equally susceptible to being targeted and the average age of a victim is 63

TOP TIPS

- Computer firms do not make unsolicited phone calls to help you fix your computer.
- Computer firms tend not to send out unsolicited communication about security updates, although they do send security software updates. If in doubt, don't open the email.
- Computer firms do not request credit card information to validate copies of software. Nor do they ask for any personally identifying information, including credit card details.

Fake Netflix Emails

The fake email reads: "We face some difficulties with the current billing information of your own. "We will try again, but please at the same time update your payment details." At the end of the email, there is a red button that tells you to "Update Account now".

TOP TIPS

- Never automatically click on a link in an unexpected email or text
- Always question unsolicited requests for your personal or financial information
- If they know your email address but not your name, it'll begin with something like 'To our valued customer', or 'Dear...' followed by your email address.

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

Fake TV Licensing

Fraudsters are sending out fake TV Licence refund emails that lead to convincing looking websites in a bid to steal bank account details. They claim that TV Licencing have been trying to get hold of recipients regarding an overpayment refund or that due to invalid account details a credit was not possible. The refund links lead to cloned TV Licencing websites that are designed to harvest bank account and credit card details.

TOP TIPS

- **Check the email contains your name** – TV Licensing will always include your name in any emails they send you.
- **Check the email subject line** - anything along the lines of "Action required", "Security Alert", "System Upgrade", "There is a secure message waiting for you", and so on, should be treated as suspect.
- **Check the email address** - does the email address look like one that TV Licensing use? For example donotreply@tvlicensing.co.uk. Look closely as often the address may be similar.
- **Never provide details by email** - TV licensing will never ask you to reply to an email and provide bank details or personal information.

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.