July Cyber Scam Update

Computer Software Fraud Victims Being Contacted

There is concern that victims of previous Computer Software Service Fraud (CSSF) are being re-targeted for "owed money". This type of fraud involves the victim being contacted, told that there is a problem with their computer, and that for a fee this issue can be resolved. The aim of the fraudster at this point is usually to gain remote access to the victim's computer and subsequently look for bank account details. Fraudsters are now requesting that they pay money owed for a fake malware protection service they had previously been given.

The victims will often be cold-called or will receive a pop-up on their computer, prompting them to phone the suspect.

TOP TIPS

- If you receive an unsolicited call or pop-up, do not make a payment. If in doubt, hang up immediately.
- Do not allow remote access to your computer.
- Don't be rushed or pressured into making a decision. Under no circumstances would genuine companies or trusted organisation, force you to make a financial transaction on the spot.

Fake EE Text Messages

These fake text messages purport to be from EE and claim that you haven't paid a bill.

The link in the message leads to a phishing website designed to steal your EE account login details, as well as personal & financial information. Don't be tricked into giving a fraudster access to your personal or financial details.

TOP TIPS

- Never automatically click on a link or attachment in an unexpected email or text.
- If in doubt, check it's genuine by using an official app or going onto the official website on a web browser.

Action Fraud Warn of WannaCry Email Scams

WannaCry emails are designed to cause panic and trick you into believing that your computer is infected with Ransomware. In reality the emails are just a phishing exercise to try and extort money. The emails claim that all of your devices were hacked and your files will be deleted unless you pay a fine to the fraudsters in Bitcoin.

TOP TIPS

- If you receive one of these emails, delete it and report. Do not email the fraudsters or make the payment in Bitcoin.
- Always update your Anti-Virus software and operating systems regularly.

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.

July Cyber Scam Update

Fortnite Gamers Targeted by Scams

Action Fraud has seen reports of fraudsters who are taking advantage of Fortnite gamers.

In most reports, the gamer has seen an advert on a social media channel which claims that by following a web link and entering some information, they will receive free Vbucks (currency for the game). Fraudsters will ask the victim for information about their account which will then allow them to log in and create fraudulent charges.

Fraudsters are also asking for people's phone numbers in return for Vbucks to then sign the victim up to a premium rate subscription service, selling access to other people's Fortnite accounts, and offering VBucks for free then actually charging for it.

TOP TIPS

- Always question requests for personal or financial information. The promise of 'free' vouchers or credits is a common tactic.

- If it sounds too good to be true, it probably is.

Lost/Stolen Passports Campaign

Her Majesty's Passport Office and Action Fraud have teamed up to urge people to report their lost and stolen passports to prevent unrecovered and unreported documents from being abused and used to commit identity crime. On average people are waiting on average 73 days before making a report.

Once a passport is reported as lost or stolen, HM Passport Office cancel it, and share the information within 24 hours with the National Crime Agency.

TOP TIPS

- Report Lost Passports on the website here: https://www.gov.uk/report-a-lost-or-stolen-passport

Follow Us on Social Media for the Latest Cyber Crime News

Facebook facebook.com/cybersafewarwickshire
Twitter @CyberSafeWarks
Instagram Cyber_Safe_Warks
or visit www.cybersafewarwickshire.com

MONTHS TOP TIP:

Book Your Holiday's Safely:

- Always use websites which have a green padlock and HTTPS within the address bar when paying for a holiday online.
- Verify a company is genuine by checking their ABTA/ATOL numbers on the ABTA or ATOL websites.
- When you are on holiday – DON'T post on social media that you are away (you might be letting potential criminals know your house is empty).

Fake Football Kit Scams

Councils across the UK are warning fans of the potential risk of inadvertently spending money on fake kits and memorabilia as fraudsters look to take advantage of the excitement around the World Cup.

TOP TIPS

- Check the item description carefully and ask the seller questions if you're unsure of something.
- If something seems too good to be true, it probably is. Don't be fooled into thinking you're getting a great deal.

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.