June Cyber Scam Update

Scam BT Emails being sent

Fraudsters are using the global WannaCry ransomware attack to get people to click on links within a BT-branded phishing email.

Several convincing emails that claim BT has launched preventative measures to protect your data on an international scale have been sent. The domains in the emails appear very similar to genuine BT addresses, and this could easily catch out those who are concerned about the security of their data after the global attack.

Cyber criminals have been known in the past to take advantage of situations like this to design new phishing campaigns. If you receive one of these emails **do not** click on any links. Instead, go to the BT website directly and log in from there to monitor your accounts activity.

TOP TIPS

- Always update software on all devices and install an antivirus.
- Do not click links in emails you are not expecting
- Do directly to the website concerned to check details

NHS Ransomware Attack

Computers at hospitals and surgeries across the UK were among tens of thousands hit by a global ransomware attack.

Ransomware blocks access to any files by locking the screen on a PC until a ransom is paid. It states on screen that you will only have a limited period of time to pay the ransom before the files are lost. The unprecedented NHS attacks exploited a security weakness in old Windows systems.

Microsoft released a patch – a software update that fixes the problem – for the flaw in March, but computers that had not installed the security update were vulnerable.

TOP TIPS

- Ensure you have effective and updated antivirus/antispyware software and firewall running before you go online.
- Don't click on links or open any attachments you receive in unsolicited emails or SMS messages. Remember that fraudsters can 'spoof' an email address to make it look like one used by someone you trust. If you are unsure, check the email header to identify the true source of communication.
- Always install software updates as soon as they become available. Whether you are updating the operating system or an application, the update will often include fixes for security weaknesses.
- Back-up your files to an external physical hard drive or online cloud storage provider. It's important that any physical device you back up to isn't left in an insecure location, or left plugged into the device you have backed up once complete.

Greater Manchester Fund Raising Scams

In the wake of the Manchester attack, Greater Manchester Police (GMP) is warning people to be cautious of online fundraising pages as it has emerged that fraudulent pages are being set up which request donations to support the families of the victims.

Fraudulent fundraising websites often use topical events to make it look like their charity has been created recently in response. Their website may also be badly written, and have spelling or grammatical mistakes throughout.

When you go to a donation page, fraudsters can record your credit or bank account details, so if you are unsure, seek further advice before donating any money.

TOP TIPS

- If you do wish to donate to this cause, visit the official Just Giving page set up by the Manchester Evening News in partnership with the British Red Cross.
- If you believe you have been a victim of fraud, report to Action Fraud, and seek support from Warwickshire Victim Support (contact details below).

If You Are Affected

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or 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.

Make a scam/rogue trader complaint to Trading Standards via Citizens Advice Consumer Service on 03454 040506.

June Cyber Scam Update

Smishing Scam Looking For Card Details

Smishing – a term used for phishing via SMS text messaging – is an activity which enables criminals to steal victims' money or identity (or both) as a result of a response to a text message.

This scam involved fraudsters purporting to be from the person's credit card provider, stating a transaction has been approved on their credit card.

The text message further states to confirm if the transaction is genuine by replying 'Y' for Yes or 'N' for No.

Through this method the fraudster would receive confirmation of the victim's active telephone number and would seek the victim's credit card details.

TOP TIPS

- Always check text messages by contacting your credit card provider through a number provided at the back of the card or on a credit card/bank statement.

- Beware of cold calls purporting to be from banks and/or credit card providers.

- If the phone call from the bank seems suspicious, hang up the phone and wait for 10 minutes before calling the bank back, or use a different telephone line.

Fraud Warning As Wedding Season Approaches

Whilst weddings may not seem the most obvious event for fraudulent activity, there are a number of ways fraudsters may operate to take your money.

TOP TIPS

- Complete researches on each vendor, ensuring you are dealing with a bona fide person or company.
- Pay by credit card. This will provide you with protection for purchases above £100 and below £30,000.
- Consider purchasing Wedding insurance.
- Some companies run their businesses entirely on social media. Whilst many are genuine, some may not be insured, or may even be fraudulent. Make sure you obtain a physical address and contact details for the vendor and verify this information.

JUNE'S Top Tip: Back Up Your Files

There are two main ways in which your personal data can be backed up; physical hard drives and online via a 'cloud based system'.

Physical Hard Drives: these are plugged into your computer and can back your data up as and when you choose to do so.

Cloud Based System: The cloud is becoming very popular nowadays due to its ease of use and the unlimited space available. The cloud almost kills two birds with one stone in that it can act both as back up and primary storage.

More information on backing up your personal data, can be found on the Get Safe Online website.

'Microsoft Tech Support' Scam

Action Fraud has received reports of Tech-Support scammers claiming to be from Microsoft who are taking advantage of the global ransomware attack.

One victim fell for the scam after calling a 'help' number advertised on a pop up window. The window, which wouldn't close, said the victim had been affected by WannaCry Ransomware.

The victim granted the fraudsters remote access to their PC after being convinced there wasn't sufficient anti-virus protection. The fraudsters then installed Windows Malicious Software Removal Tool, which is a free tool, and took £320 as a payment for installing this.

It is important to remember that Microsoft's error and warning messages on your PC will **never** include a phone number.

TOP TIPS

- Don't call numbers contained in pop-up messages.
- Never allow remote access to your computer.
- Always be wary of unsolicited calls.

Keep up to date with the latest updates Community Safety in Warwickshire.

Like us on **Facebook**: www.facebook.com/SafeinWarwickshire

Follow us on **Twitter**: @SafeInWarks

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

If You Are Affected

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or 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.

Make a scam/rogue trader complaint to Trading Standards via Citizens Advice Consumer Service on 03454 040506.