December Cyber Scam Update

Be Cyber Smart With Online Shopping This Christmas

Last Christmas, 12,142 people said that they had been a victim of online shopping fraud during the Christmas period. 133 people said that they had been defrauded on Black Friday, with a further 115 falling victim on Cyber Monday.

These figures amounted to a total loss of **over £10 million**.

TOP TIPS

- Use Trusted Brands & Websites

  Look for 'https' in the address bar (where you type in the website) whenever entering payment details online.

  If this is not there, do not continue with the transaction, as the details you enter may be seen by criminals.
- Look Out For Scam Emails

  If you get an email from a seemingly legitimate company, with a great offer, do not click on the link.

  Go directly to the company's website to see if this offer is genuine.

  If an email asks for any personal details or verification (unless the company has pre-warned you), do not enter any information, and delete the email.
- Look Out For Social Media Scams

  It's not just emails; adverts or messages on social media may also be scams too, so go directly to the company's website – don't click on the links.
- Be Wi-Fi Aware

  If you connect to any Wi-Fi, it is important to not do any online shopping or banking.

  A cyber-criminal can set up a fake hotspot, letting them see everything you do if you connect to it.

  Consider getting a Virtual Private Network (VPN) if you need to do any online shopping over Wi-Fi.
- Use Payments With Protection

  Credit cards offer great buyer protection, as do online payment systems such as PayPal.

  Legitimate retailers should have a clear returns policy which it will adhere to.

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.

How Safe Do You Feel Online?

- We want to know about cyber crime and online safety in Warwickshire.

- Whether you have been a victim or not, we want to hear from you.

- It should take 10 minutes to complete, and once you've finished, don't forget to share it to friends, families and colleagues.

- To complete the survey, please visit https://www.surveymonkey.co.uk/r/RegionalCyber16

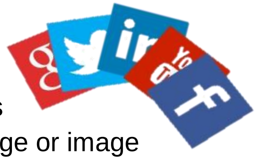
- The closing date for responses is Monday 9th January 2017.

Watch Out For Viruses On Social Media

There are new warnings concerning opening files received through social media, namely Facebook and LinkedIn.

Files being sent to users through social media messengers have been found to contain a virus which basically locks you out of your computer until you pay a fee.

This ransomware virus is being embedded in picture files and when the target opens them it opens the virus.



TOP TIPS

- Think before you click – does the person sending the message or image regularly contact you? Does the message or image look like something they would send you?

- Double check with the person that they have sent you the message or image before clicking on it.

- Back up your devices so if this does happen to you, you do not have to pay to get back any files.

December Cyber Scam Update

BT & Talk Talk Phone Scams Warning

- Warwickshire residents are being warned of a 'new' phone scam.
- A Rugby couple reported receiving a phone call from someone falsely claiming to work for BT.
- The caller informed them that the direct debit payment for their phone bill hadn't gone through.
- They confirmed the victim's name/address and asked who they banked with.
- They then informed them that their bank would call them back in 15 minutes to discuss.
- The "bank" (the fraudsters) then called back and tried unsuccessfully to obtain security question and other bank details from them.

Warwickshire residents have also received phone calls claiming to be from Talk Talk, informing them that their computer needs fixing – this too is a scam.

TOP TIPS

- If anyone cold calls you, hang up the phone.
- If you are unsure, ring the company on a different phone, using a phone number on a bill or other correspondence.
- Never provide any personal information such as banking details, PINs or passwords to anyone over the phone.
- Never give a caller remote access to your computer.
- Report any scam or rogue trader to Warwickshire Trading Standards via the Citizen's Advice Bureau on 03454 040 506.

Three & Deliveroo Accounts Breached

- Mobile and internet provider Three UK has confirmed that personal information of customers has been accessed by hackers in a cyber-attack.

- It has been suggested that financial details, including bank & credit card information, were **not** included in the breached data.

- 'Deliveroo' customers have also had their accounts breached as a result of people using the same password for this and previously compromised accounts.

TOP TIPS

- Change the passwords for all accounts - but make them strong and unique.
- Password managers can create and remember strong, unique passwords for each of your accounts.
- Be extra vigilant of any scam emails and cold calls if you think you may be affected by these.

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

National Lottery Accounts Hacked

Camelot say they did not believe its own systems had been compromised, but players' login details had been stolen from elsewhere – as people use the same username & password for most accounts.

It is recommended you **change your password** for this account, and **any others** which share the same password, to something strong and unique. The August & October Cyber Scam Updates have helpful tips for creating strong, unique passwords.

DECEMBER'S TOP TIP: Shop Safely Online

- A padlock symbol within the address bar should appear when you attempt to log in or enter any personal details. Do not enter any details if this is not there.

- The web address should begin with 'https://'. (The 's' stands for 'secure').

- If using the latest version of your browser, the address bar or name of the site owner will turn green.

- If you get an email advertising a great offer, go directly to the website to claim it – do not click on the email links.

- Using a company whom you have never heard of before? Check they are reputable before paying for anything by researching for them. Customer reviews on websites and social media may help you see if they are a legitimate company.

- Payments such as credit cards offer greater protection from fraud, guarantees and non-delivery than debit cards.

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.