January Cyber Scam Update

New Year Scams & Shopping Tips

Shopping for discounted goods in the New Year sales? Keep in mind our top tips to keep you safe!

TOP TIPS

- **Use Secure Websites**

When buying items from websites look for 'https' in the address bar (where you type in the website), also look for a padlock symbol preceding this. When paying, some websites will redirect you to a third-party payment service (such as WorldPay). Ensure that these sites are secure before you make your payment.

- **Beware of Offers In Your 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.

- **Be Wi-Fi Safe**

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.

- **Additional Rights When Buying Online**

In most cases you can change your mind and cancel your order up to 14 days after delivery (you may have to pay the return cost).

Don't Forget!!!

Complete the new 2016/17 Cyber Crime survey, so we can see the full scope of Cyber Crime in Warwickshire & across West Mercia, West Midlands & Staffordshire: https://www.surveymonkey.co.uk/r/RegionalCyber16 Survey closes 31st January.

PayAsUGym Accounts Breached

The company, which sells passes for gyms around the UK, acknowledged that 300,000 email addresses and passwords of its members had been accessed. The website said it did not hold financial or credit card details of its users on its servers.

TOP TIPS

- Use a different password for every website. If you have only one password, a criminal simply has to break it to gain access to everything.
- Consider using a 'Password Manager' which stores all your passwords
- Customers have been advised to change their passwords and the company has also migrated to new servers.

JANUARY'S TOP TIP
Stay Safe When Looking For Love Online

Avoid posting details such as your full name, date of birth, or your home and work addresses on online dating profiles.

Never respond to any requests to send money, or have money transferred into your account by someone you don't know

Never reveal any of your financial details. If a user asks you for them, stop communicating with them immediately and report it to the dating site.

Trust your instincts - if you think something feels wrong, it probably is.

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.

January Cyber Scam Update

Lloyds Fraudulent Bank Letters

Action Fraud is warning of a letter which tells recipients there has been some "unusual transactions" on their personal account and asks them to call a number highlighted in bold to confirm they are genuine. When victims call the number, an automated welcome message is played and the caller is asked to enter their card number, account number and sort code followed by their date of birth.

TOP TIPS

If you are ever suspicious about correspondence from your bank you should call the customer service number on the back of their card.

Report to Action Fraud (See in Footer below).

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

Improve Your Cyber Knowledge

A new Future Learn online course 'Becoming a Digital Citizen: an Introduction to the Digital Society' launches 23rd January 2017.

For more information, and to enrol, visit https://www.futurelearn.com/courses/digital-society

WhatsApp Hacking Attempts To Steal Bank Details

Hackers are targeting unsuspecting users with a mobile virus that is distributed via legitimate-looking Word documents sent inside WhatsApp. Once opened, these documents are capable of taking sensitive information from users, including online banking credentials and other personal data.

The virus has also been disguised as a Microsoft Excel or PDF file, according to users.

Yahoo Account Breaches Affect One Billion

Yahoo has said more than one billion user accounts may have been affected in a hacking attack dating back to 2013.The internet giant said it appeared separate from a 2014 breach disclosed in September, when Yahoo revealed 500 million accounts had been accessed. Yahoo said names, phone numbers, passwords and email addresses were stolen, but not bank or payment data.

TOP TIPS

- If you think you have been affected, change your password and security questions for your online accounts.
- Monitor your account for any suspicious or unexpected activity.
- Be very wary of any emails purporting to come from Yahoo, particularly if they prompt you to click any links, download any attachments or give out any personal information.
- Be wary of anyone calling asking for personal information, bank details or passwords. If in doubt, just hang up.
- Visit Experian, Equifax or Noddle to check your credit rating to make sure no one has applied for credit in your name.

Report A Scam

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

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.