December Cyber Scam Update

This Christmas, Action Fraud and City of London Police are reminding shoppers to take extra care when shopping for gifts online. As consumers search online for bargains and gifts for loved ones, fraudsters are seeing this as an opportunity to trick people with the promise of great deals and big cash savings.

The latest report by Action Fraud shows that fraudsters conned 15,024 shoppers out of more than £11 million over the Christmas period last year.

People are being defrauded on popular social media websites and online auction sites. Action Fraud works together with platforms including Gumtree to combat fraud and to issue protect advice to consumers.

Don't get caught out by the Christmas rush.

Top Tips;

- If something seems too much of a bargain, it's probably poor quality, fake or doesn't exist.
- Don't pay for goods or services by bank transfer unless you know and trust the person. Payments via bank transfer offer you no protection if you become a victim of fraud.
- Make sure you've installed the latest software & app updates. Criminals use weaknesses in software to attack your devices and steal information, such as your payment details.

Cyber "Sam"ta Offers His Advice This December

This December across the Cyber Safe Warwickshire social media pages, Cyber "Sam"ta will be on hand to offer his top tips and advice for staying safe online over the festive period.

Follow us via:
facebook.com/cybersafewarwickshire; @CyberSafeWarks on Twitter; and Cyber_Safe_Warks on Instagram

…to keep up to date with #CyberSamta and his top tips for all to share.

Cyber Aware is warning the public that without using a strong and separate password for your main email account, you risk giving cybercriminals a wealth of information that could be used against you.

This comes after research from UK General Insurance in partnership with Cyber Aware reveals that people are storing sensitive information within their email accounts.

Storing this kind of information can be like 'gold dust' to criminals, who can use it to commit cybercrime including making phishing emails more convincing by including personal information or impersonating you or friends and family.

Top Tips

- Use a strong, separate password for your email.
- A good way to create a strong and memorable password is to use three random words. Numbers and symbols can be used to make it stronger.
- Use words which are memorable to you, but not easy for other people to guess. Don't use words such as your child's name or favourite sports team which are easy for people to guess by looking at your social media accounts or simple substitutions like 'Pa55word!'

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.

December Cyber Scam Update

Facebook admits bug allowed apps to see hidden photos.

A Facebook bug let app developers see photos users had uploaded but never posted, the social network has disclosed.

For two weeks in September, an error in the way Facebook shares photos with third parties meant that apps could see not only photos users had posted on their newsfeed, but also pictures in other parts of the site – on Facebook Stories or Facebook's Marketplace, for instance.

The bug also "impacted photos that people uploaded to Facebook but chose not to post"

For two weeks in September, an error in the way Facebook shares photos with third parties meant that apps could see not only photos users had posted on their newsfeed, but also pictures in other parts of the site – on Facebook Stories or Facebook's Marketplace, for instance.

The bug also "impacted photos that people uploaded to Facebook but chose not to post", a Facebook developer, Tomer Bar, said in a statement on Friday.

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

DECEMBER'S TOP TIP: Shop Safely Online This Christmas

Millions of shoppers head online for bargains in the run up to Christmas - giving criminals ample opportunity to try and con people out of their money.

Stick to trusted websites, with HTTPS and the padlock within the address bar. If a site does not have this when you are entering any personal details - DO NOT go ahead with the purchase.

https://

Be aware of scam emails, text messages and social media posts offering must have items for low prices; all these platforms allow criminals to share scams and viruses with great ease.

Action Fraud warns against fake TV licensing emails, as over 2,500 reports are made in two months alone.

Reports made to Action Fraud show that fraudsters are sending out fake TV Licence emails regarding refunds and payment issues to people across the UK.

When a victim clicks on the link, they will be led to a convincing looking TV Licencing website. The website is designed to harvest as much personal and financial information as possible from the victim.

Top Tips

- Never answer an unsolicited email from TV Licensing - the organisation will never email you, unprompted, to tell you that you're entitled to a refund or ask for bank details/personal information.
- Check the email contains your name – TV licensing will always include your name in any emails they send you.

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.