November Cyber Scam Update

Courier Fraud Is On The Rise

Courier fraud is on the rise and it's often the elderly and vulnerable that fall victim.

This scam involves criminals ringing you, claiming to be your bank or the police. Often the call will claim that fraud has been suspected on your account. Part of their 'identity check' often involves asking for details such as your address and PIN.

If these details are given, a courier is then sent to your address to collect your card, or cash (depending on the exact nature of the call).

TOP TIPS

- No one will ever phone and ask you for your PIN or full banking passwords.
- Nor would anyone ask you to withdraw money to hand over to them for safe-keeping, or send someone to your home to collect cash, PIN, cards or cheque books if you are a victim of fraud.
- Don't assume an email or phone call is authentic.
- Just because someone knows your basic details (such as your name and address or even your mother's maiden name), it doesn't mean they are genuine.

More Customers Caught Up In British Airways Breach

185,000 BA customers have been told their personal details were also stolen in a data breach first revealed last month.

Hackers may have stolen 77,000 customer details such as names, addresses, email address, and card numbers, expiry dates & CVV numbers (the 3 digits on the back of your card). This data would allow purchases to be made by the criminals.

An additional 108,000 customers are thought to have had these details stolen, but not the CVV, which acts as an extra layer of protection for online transactions.

The company have said that all affected customers have been informed.

TOP TIPS

- Be vigilant about any suspicious activity on your accounts, and alert your bank if you suspect anything.
- Be aware of any unsolicited calls, emails or messages asking for your personal information (especially if in relation to this breach).
- Alert your bank if your card details have been compromised in this, or any other, data breach.

Goodbye Cyber Sam

Cyber Sam has moved on to pastures new, and we want to take the opportunity to thank him for all his hard work with Cyber Safe Warwickshire, and wish him all the best for his future ventures!

(But don't forget you can still enjoy his Cyber Samta videos on YouTube!)

Follow Us for the Latest Cyber Crime News

Facebook: facebook.com/cybersafewarwickshire
Twitter: @CyberSafeWarks
Instagram: Cyber_Safe_Warks
Visit www.cybersafewarwickshire.com

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.

November Cyber Scam Update

Brits At Risk of Fake Invoice Scams

Research has revealed that more than a quarter of Brits would be caught out by email invoice scams due to not checking the details.

More than a quarter (28%) of Brits admitted they could be caught out, as they would go ahead with a request for payment received by email without calling the supplier directly to check the details. This tactic is becoming increasingly popular, as fewer Brits (5%) say they couldn't spot a rogue doorstep trader.

It is younger people who are more likely to be caught out by these scammers, too.

While more than one in five (22%) of those aged 55 and above would be at risk by not checking an email invoice via a phone call to the supplier, over a third (37%) of those aged 25-34 would take the same risk.

TOP TIPS

- Don't rush to get work done by someone knocking on your door - take your time and do your research and look out for neighbours who may be more likely to feel pressurised.
- Fake invoices received by email can be very convincing; check personally using separate contact details before parting with your money.

New 'Smart Devices' Guide Launched

Everything from our phones to our fridges, (even bathroom taps) can connect to the internet nowadays.

Now, the Government have produced consumer guidance around smart devices in the home to help manage the security of these products and protect your privacy. To view the guidance, click on the image below.

NOVEMBER'S TOP TIP
Cut Out The Junk Email

Is your inbox always full of junk email?

Try flagging them as 'Junk' or 'Spam', rather than simply ignoring or deleting them

This will let your email provider know that these are getting past their filters

The more these junk emails are reported as such, the less likely you will have to see them in your main inbox

Government Warns Against Poppy Scams

The Government has warned of rogue traders selling fake poppy merchandise, which won't benefit charities.

The Intellectual Property Office has teamed up with the Royal British Legion to urge consumers to 'buy responsibly' ahead of Remembrance Day on 11th November.

Genuine poppy merchandise, featuring the two or four-petal official poppy design, can be bought through the Royal British Legion, its eBay or Amazon pages, or one of its official corporate partners.

The profits support members of the Armed Forces, veterans and their families – whereas money spent on fake poppy products will only benefit the scammers.

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.