February Cyber Scam Update

Amazon Email Scams Warning

Amazon users are being warned of potential scams as numerous fradulent emails and compromised vendor accounts have left users vulnerable.

One of the scams was spoofed emails from “service@amazon.co.uk” claiming recipients have made an order online and mimics an automatic customer email notification. Items on the email say you have ordered an expensive vintage chandelier, Bose stereos, smartphones and luxury watches. The emails cleverly state that if recipients haven’t authorised the transaction they can click on the help centre link to receive a full refund. If you click on the link it sends you to an authentic looking website to enter your details.

Amazon customers beware have also been targeted by fraudsters creating seller accounts or taking control of genuine vendors to trick users into purchasing expensive items at unrealistically low prices.

One example of this was an over £2,000, 55-inch LG OLED TV was on sale for half its price and labelled as a “used-like new” article by a vendor called ScElegance Electronics. When the customer places the order for the TV, an error message appears asking the buyer to complete the purchase outside of the Amazon system. The user never receives the item and Amazon will not offer a refund as the payment was not made through their system.

Top Tips

- Do not click on links to websites that look like Amazon.co.uk, but aren’t Amazon.co.uk; go directly to Amazon’s website and log into your account from there instead.
- Do not open attachments or prompts to install software on your computer
- Watch out for spelling and/or grammatical errors

Boiler Scam Phone Call Warning

Warwickshire residents are warned to beware of persistent and unwanted phone calls from people claiming to be offering free boilers for householders on benefits.

Consumers are warned that these calls may be being made by people who actually want to sell you overpriced boiler cover or a boiler at a 'discount' which may not save you money at all!

Never agree to purchase goods or services from cold callers, or arrange for those callers to visit your home. It can be hard to tell a good trader from a bad one on the doorstep! If you are looking for a new boiler, consider using local businesses and where possible go on recommendation.

Some householders on certain benefits may qualify for free boiler grants funded by energy companies as part of the Energy Company Obligation (ECO).
Find out if you can benefit from ECO funding, by contacting the Energy Saving Advice Service on 0300 123 1234.

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.

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

February Cyber Scam Update

HMRC Scam Emails & Text Messages

Residents are being warned about phishing emails & texts claiming to be from HMRC concerning tax rebates.

Victims to the email scam have downloaded a word document attached to an email and unknowingly downloaded files from a hacked website which installs ransomware on their device.

When victims click on the link in the scam texts, they are redirected to a registration page requesting personal details. Victims who have provided their personal details have had direct debits, mobile phone contracts and new bank accounts set up using their personal details.

HMRC have advised on their website that this **is** a fraud and stressed they would **never** contact people using these methods.

If you have had a ransomware attack on your device, it is important to take the device to an IT specialist, who can ensure that the virus has been removed. You should install and update anti-virus software to the device, as well as back-up your files stored on there. Also be aware of any future possible scam emails which appear in your inbox.

TOP TIPS

- Don't click on links or open any attachments you receive in unsolicited emails or text messages.
- Remember that fraudsters can 'spoof' an email address to make it look like one used by someone you trust.
- If you are unsure, search online for the email sender's address to identify the true source of communication.

New PayPal Email Scam

The email resembles a receipt confirmation and guides you to click on a link to dispute a transaction. You won't recognise the name the transaction shows because it's fake and has been made up by the scammer.

Once you've landed on the sign-in page, you're guided to type in your email and password.

This information would then belong to the scammer and enable them to access your real account.

On the Personal Information Profile page, it asks you to enter personal information to verify your identity. Not only are you asked to enter your billing address and card details, you're also asked to enter in your mother's maiden name, branch code and account number for 'verification' purposes.

This is an attempt to capture as much financial information about you as possible, so accessing your account is easier for the scammers.

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

Safer Internet Day – 7th February 2017

To mark Safer Internet Day, Cyber Safe Warwickshire has also launched an e-learning module to residents to help them think about their online safety. This can be found here: www.safeinwarwickshire.com/elearning.

As well as this, a new campaign to ask residents to think about how they access free Wi-Fi connections when they are out and about in the county has been launched. More information on this scheme can be found at http://www.warwickshirebusinesswatch.co.uk/blog news/

FEBRUARY'S TOP TIP: Be Wi-Fi Savvy

Do you connect to free public Wi-Fi when out and about?

Cyber criminals can set up fake hotspots and see everything you are doing.

Avoid using public Wi-Fi for online shopping and banking to keep your details safe.

Use a trusted Virtual Private Network (VPN) service in order to secure your traffic.

By using a VPN when you connect to a public Wi-Fi network, you'll be encrypting all of your data that passes through the network.

For more information on staying safe on public Wi-Fi, please visit Warwickshire Business Watch's advice page.

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.