November Cyber Scam Update

Two-Thirds Have Received 'Fix Scam Phone Calls'

- If you have ever been called from a person claiming to be from Microsoft or any similar company, to tell you they are aware of a problem with your computer – you have been targeted by what is called a fix scam.
- The caller will ask you to turn on your computer and follow their instructions so they can gain access remotely to your computer.
- The criminal will make it seem as if they are resolving the issue which they have mentioned. You will then be asked to pay a fee and told the problem has been resolved.
- Once the initial payment has been processed, it is not uncommon for additional, larger payments to be taken from the victim's account without permission.
- In some instances, programs and malware are also installed that allow the fraudsters unlimited access to the computer without the victim's knowledge.
- This permits them to have access to information, such as personal data, as well as view online transactions so that further illegal activity may to be carried out.
- 69% of UK residents have been affected by this kind of scam.

TOP TIPS

- Microsoft has said they will NEVER proactively reach out to users to offer technical support.
- If you receive a phone call like this, hang up the phone - do not follow their instructions to turn your computer on.
- NEVER give out your passwords or PIN to anybody – no company needs this information from you.

Regional Cyber Crime Survey 2016

- Warwickshire, West Mercia and the West Midlands have joined forces to launch a Regional Cyber Crime Survey.
- This latest survey will seek to examine how the picture has changed across Warwickshire over the past 12 months and whether residents are more aware of the dangers that can be posed online and the things that they are able to do to minimise these risks.
- To fill in the survey, please visit https://www.surveymonkey.co.uk/r/RegionalCyber16

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.

Court Summons Scam Emails

Fraudsters are sending out a wave of scam emails purporting to be from the Crown Prosecution Service (CPS) that claim you have to appear in court.

We have received several reports from concerned members of the public who have received the email entitled "You've been witness summoned to court".

The email entices people to click on a link to view their start time/case details. This link is likely to lead to malware.

TOP TIPS

- This email has no connection to the CPS.
- Anyone receiving the email should not download any attachments or click any links and report it to Action Fraud (details below).
- The CPS is aware and has said that they "never email witnesses in order to summons them to court".

NOVEMBER'S TOP TIP: BEWARE OF LINKS & ATTACHMENTS IN EMAILS

- In unsolicited emails:
- Links may ask for personal details, so criminals can scam you out of money.
- Attachments which you have to download may place viruses and malware onto your device.
- If you are unsure about an email, research online and on social media to see if others have been affected by a possible scam.
- If in doubt, throw it out!

COMING SOON

CYBER SAFE WARWICKSHIRE WEBSITE

November Cyber Scam Update

Scam Sainsbury's & Topshop WhatsApp Voucher Links

Fraudsters are sending out fake Sainsbury's and Topshop voucher deals through WhatsApp that appear to have been sent by a trusted contact.

The fake WhatsApp messages appear as if they have been sent by someone in your contacts – such as a friend or family member.

However the recipient name is false and is designed to trick you into clicking on a link to claim the alleged Sainsbury's or Topshop voucher.

If you click on the convincing looking link, you will be taken to a fake website designed to trick you into handing over personal information.

According to security researchers, once you click on the malicious link, fraudsters also collect personal information from your device by installing items on your phone that tracks you, or add browser extensions that can be used to show you advertisements, which may also be scams.

Sainsbury's have confirmed that they are aware of the fake offers, and are "advising customers to delete the message".

TOP TIPS

- Install security software on your device and keep it up to date.
- Never click on unsolicited links in messages that you that receive, even if they appear to come from a trusted contact.

Improve Your Online Security Knowledge Today

A new e-learning package has been made available for you to increase your knowledge about cyber crime and security.

It has been made by subject experts at Warwickshire County Council, and takes a Warwickshire focussed look at how people can become safer while online.

To access this e-learning, visit the following links for modules on Cyber Crime and Cyber Security.

Have you been a victim of Cyber Crime?

Would you like to share your story to raise awareness of Cyber Crime issues in Warwickshire?

If so, get in contact with Warwickshire County Council's Cyber Crime Advisor
Email: alexgloster@warwickshire.gov.uk

If your community group would like an advice session with Warwickshire County Council's Cyber Crime Advisor, contact alexgloster@warwickshire.gov.uk

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

ALDI Voucher Scam Warning

Aldi is warning its customers about a 'fraudulent' voucher that is being circulated online.

The supermarket chain issued a statement on its Facebook page saying that the offer of an £85 voucher is a 'hoax' and is 'being fully investigated'.

Aldi's warning read:

"ALERT: We have been notified that there is a hoax £85 Aldi voucher being circulated online.

Please be aware that this voucher is fraudulent and cannot be redeemed in our stores. Aldi UK will never ask you to share your personal details via a website to redeem a genuine voucher offer.

This hoax is currently being fully investigated. Thank you, Aldi UK."

TOP TIPS

- It is always advised to be vigilant of any offer or voucher from a social media platform.
- Check the verified account for any company to check whether the offer is legitimate.

Reporting 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.