December Cyber Scam Update

Be on the lookout for “too good to be true” flight deals!

As we approach the holiday season, when it is expected that an increasing number of UK residents will be traveling overseas to visit friends and family, Action Fraud is warning people to be on the lookout for fraudulent travel websites and unsolicited phone calls from scammers promising “too good to be true” deals on flights.

As well as flights relating to holidays, fraudsters particularly target the friends and family market, with flights to Africa and the Indian subcontinent dominating the list of affected destinations.

Fraudsters use a variety of methods to target people, most commonly cold calling and pretending to be from a travel company after the victim has unknowingly entered their personal details on a bogus website. The caller appears to know that the victim has been recently searching online to book flights and after gaining their trust, will make a ‘too good to be true’ offer on flight tickets to lure them into making a payment.

After transferring the money, victims may receive a confirmation email but any further attempts to contact the company will be unsuccessful and enquiries with the airline will reveal that the booking does not exist.

Top tips to avoid becoming a victim of travel fraud:

- Stay safe online: Check the web address is legitimate and has not been altered by slight changes to a domain name – such as going from .co.uk to .org
- Do your research: Don’t just rely on one review – do a thorough online search to check the company’s credentials. If a company is defrauding people there is a good chance that consumers will post details of their experiences, and warnings about the company.
- Look for the logo: Check whether the company is a member of a recognised trade body such as ABTA. If you have any doubts, you can verify membership of ABTA online, at www.abta.com.
- Pay safe: Wherever possible, pay by credit card and be wary about paying directly into a private individual’s bank account.
- Check documentation: You should study terms and conditions and be very wary of any companies that don’t provide any at all. When booking through a Holiday Club or Timeshare, get the contract thoroughly vetted by a solicitor before signing up.
- Trust your instincts: If something sounds too good to be true, it probably is.
- Report it: Victims should contact Action Fraud. (https://www.actionfraud.police.uk/)
- Get free expert advice: For further advice on how to stay safe when booking or researching travel online, visit Get Safe Online (https://www.getsafeonline.org/)

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.

Criminals using fake gift vouchers to lure victims into scam

Action Fraud have received over 118 reports this month about fake messages purporting to be from Argos.

The messages state that the recipient has won gift vouchers. The links in the texts leads to malicious websites designed to steal personal and financial details.

Top Tips:

Don’t click on the links or attachments in suspicious emails and texts, and never respond to messages that ask for your personal or financial details.
December Cyber Scam Update

Watch out for fake emails claiming to be Action Fraud

We would urge people not to click on the links or attachments in suspicious emails, and to never respond to messages that ask for personal or financial details. Under no circumstances will Action Fraud, or a police force, ask you to make a payment in order to recover money that you may have lost.

At least one fake number has been identified relating to this scam and Action Fraud are working with their disruptions team to close this down. If you think you have been a victim of fraud, report it to Action Fraud on 0300 123 2040 or via their online reporting tool.

For more information on how you can protect yourself, visit takefive-stopfraud.org.uk

MONTHS TOP TIPS

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.

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.

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

Watch out for these fake emails about undelivered packages

Action Fraud have received over 100 reports about fake emails purporting to be from FedEx.

The emails state that a package couldn’t be delivered to the recipient due to incomplete address information. The “update my address” link in the emails lead to malicious websites designed to collect personal information.

Protect yourself:

- Remember, Action Fraud will never ask you to transfer money out of your account.
- It pays to stop and think anytime you receive a request for personal or financial information. Remember, if you feel uncomfortable or unsure about what you’re being asked to do, never hesitate to contact your bank or financial service provider directly, using a number you trust, such as the one listed on your bank statements or on the back of your card.
- Fraudsters sometimes re-establish contact with previous victims claiming that they can help them recover lost money, this is just a secondary scam. Hang up on any callers that claim they can get your money back for you.

Top Tips:

Don’t click on links or attachments in suspicious emails, and never respond to messages that ask for your personal or financial details.