

Blue Badge Copycat Website Warning

Warwickshire residents wishing to apply for or renew their blue badges online are being warned about new copycat websites that have appeared on web searches.

The websites may appear official, but are not. Instead, they take an additional fee for processing a blue badge application or renewal, making the process more expensive than if using the official website. At least 4 Warwickshire residents have recently contacted the council to complain about this.

Top Tip

The official blue badge application or renewal webpage is located at <https://www.gov.uk/apply-blue-badge>



Improve Your Internet Safety At Home

Future Learn are offering a free online course on Cyber Security at home, online and in life in its latest FREE course. Three one-hour long sessions will cover privacy online, payment safety and security at home.

For more information, and to enrol on this course, visit

<https://www.futurelearn.com/courses/cyber-security/1>



Warwickshire Police Issue Phone Scam Warning

Warwickshire Police are advising residents to be aware of a scam phone call which has been reported to them recently.

They have received reports from several residents in Rugby who have had phone calls claiming that they owe money to HMRC Inland Revenue.

The automated message will state to press a key on their phone for more details. This is a scam and HMRC, banks and the police would never ring people in this manner or ask for personal information or bank details over the phone.

Top Tips

- If you receive a call of this type, hang up immediately and report it on 101 using another phone.
- Call 999 in an emergency or if a crime is in progress.
- If you have elderly friends or relatives who may be vulnerable to this scam, please talk to them and make them aware.



SEPTEMBER'S TOP TIP: Install & Update Anti-Virus Software

- Download anti-virus software for **all** of your internet enabled devices.
- Regularly update the software if it does not do so automatically.
- [Get Safe Online](#) has advice on what to consider when buying anti-virus software

British Gas Scam Email

Fraudsters are spamming out fake British Gas utility bill emails that link to a virus that takes over victims computers.

Action Fraud has received hundreds of reports of these emails cleverly designed to look like a seamlessly harmless utility bill.

The emails entitled "Your summer gas & electricity bill" contain links that take people to a website where they are told to download a file in order to view their bill. After downloading the file, the virus locks you out of your computer and directs you to an online payment page.

Top Tips

- If you receive one of these emails do not click on any links or attachments.
- If you do need to pay a bill, go directly to the British Gas website and log in from there.
- You should always update your Anti-Virus software and operating systems regularly.
- If you have downloaded the virus, do not pay any money and get in contact with Action Fraud (details below) to report the crime and get advice on what to do next.



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](#).

Rise In Facebook Scam Offers

Throughout the summer, Facebook users were becoming increasingly inundated with scam offers for family days out to venues such as Alton Towers and Vue Cinema.



Top Tips

- If you see an unsolicited offer – contact the company the offer is apparently for to verify whether this is true.
- Do not click on any links or attachments which the unsolicited posts ask you to click on – doing so could download a virus to your device.



New School Year, New Shopping Scams

Buying the latest gadgets and tech for your children or grandchildren for the new academic year?

Be aware: criminals may profit at this time of year by appearing to offer the latest devices for reduced prices – only these devices do not exist, and they are trying to con you out of money.



Top Tips

- Buy online? Only enter your personal details on a site with **https** and the padlock in the address bar.
- Do your research – not heard of the company you are buying from? Google reviews, and search on social media to see what other buyers' experiences have been.

If you would like to have an advice session with Warwickshire County Council's Cyber Crime Advisors, contact them alexgloster@warwickshire.gov.uk or kierenhagan@warwickshire.gov.uk

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**.

Beware Of Banking Trojans

Banking Trojans are a growing concern for Warwickshire residents.

Trojans are a form of virus which gets onto your device when you download software from a non-legitimate email or website.

This software may look legitimate, but can allow criminals to access your bank accounts and steal your money.

If you have a Trojan on your device:

- run your anti-virus and follow their instructions on what to do next
- take your device to an IT specialist, who will clean it of the virus
- report the incident to Action Fraud



Top Tips

- Install and update your anti-virus software.
- Be wary when downloading software from unsolicited emails & potential copycat websites.

Reporting A Scam

Make a scam complaint to Warwickshire Trading Standards via [Citizens Advice Consumer Service](#) on 03454 040506.

'Amazon' Spam Emails

Email messages, claiming to be from Amazon, have been distributed as part of a widespread attack. They have been designed to trick computer users into opening an attachment disguised as information about an order for an unnamed item.

These emails are not from Amazon, with the danger being in the file attached to the emails. The emails carry an attached file called "Your Order Details with Amazon.zip" which contains a Trojan horse, a virus which allows criminals access to your online bank account.

 More information on Banking Trojans.



Top Tips

- Keep your device software up to date.
- Install and regularly update your anti-virus software.
- Be suspicious of any unsolicited email arriving in your inbox – it could be a scam or contain a virus.

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

COMING THIS OCTOBER
CYBER SAFE IN WARWICKSHIRE WEBSITE