The Fraud & Scam Bulletin

JANUARY 2025

Your monthly update direct from West Mercia Police on the latest scams and frauds

NEW YEAR RESOLUTIONS

At the start of another New Year, what better time to make a new resolution to examine how we can protect ourselves from Fraudsters, strengthen our protection and do all we can to avoid being a victim of the scammers in the coming months.

There is no doubt the criminals will be planning their next moves to defraud any unsuspecting members of the public, and their methods are becoming more sophisticated and harder to spot. The use of AI to generate messages, images and clone voices increases the need for greater vigilance in all we do online.

What can we do?

3 SIMPLE STEPS TO PROTECT

1. Use strong and separate passwords for each of your online accounts. 3 Random Words with at least 8 characters and a combination of upper and lower case, numbers and symbols.
2. 2 Step Verification (2SV) – Also known as 2 Factor Authentication (2FA) for your online accounts adds an extra layer of security by requiring a code or PIN to confirm your identity when you log in.
3. Take time to stop and think before continuing a phone call, or clicking on a link from an unknown source. Never be pressurised into making a quick decision. Always check the email address before opening emails claiming to be from bona fide organisations such as your Bank, Government organisations or other businesses.

OTHER SIMPLE WAYS TO PROTECT YOURSELF

1. Install the latest Software and App updates on your devices as these often contain security patches to protect you from hackers
2. Back up your data regularly, by storing your important files in a separate location such as an external hard drive or on the Cloud. This way all is not lost if you experience a ransomware attack, device loss or damage.
3. Be careful when using public Wi-Fi networks as they are often unsecured and can expose your activities to others. Using a Virtual Private Network – VPN – can protect your privacy.

4. Protect your personal information online, and do not share too much information about yourself on social media, online forums and other similar platforms. This is how you could become a target for scammers and identity thieves. Check your privacy settings on Social Media to make sure only your real friends see your posts.
5. Beware of your Digital Footprint – every time you go online you leave a digital "footprint" which can show where you are and what you are doing. Once you post a file or photo online it may stay there forever and be used by others, so do not share anything that may cause you problems or embarrassment in the future.
6. Educate yourself and your family about online safety by learning how to spot common online scams, and how to avoid them, and use the internet responsibly and respectfully to protect you and your family.

Please feel free to share these messages with any vulnerable friends, relatives or neighbours

---

If you've fallen for a scam, report it to **Action Fraud on 0300 123 2040** or via actionfraud.police.uk.

Scam Text messages can be forwarded to 7726 to help phone providers take early action and block numbers that generate spam on their networks. Scam mobile calls can also be forwarded to **7726**, followed by the word "**CALL**", then the **scam phone number**

Forward **Fake Emails** received to report@phishing.gov.uk

For further information visit:

https://www.actionfraud.police.uk/ https://takefive-stopfraud.org.uk/