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.

Yahoo! Data Breach - Change Your Passwords Now
Yahoo says hackers have stolen information from an estimated 500 million users in what appears to be the largest publicly disclosed cyber-breach in history. The breach included swathes of personal information, including names and emails, as well as "unencrypted security questions and answers". 8 million UK Yahoo accounts are known to have been affected.

Top Tips
- Change your password and security questions for your online accounts. You should change passwords often and never use the same one twice. See below for some tips on how to create new passwords.
- Monitor your account for any suspicious or unexpected activity.
- Be very wary of any emails purporting to come from Yahoo, particularly if they prompt you to click on any links, download any attachments or give out any personal information.
- Be wary of anyone calling asking for personal information, bank details or passwords. If in doubt, just hang up.
- Contact your bank/credit card company, so that they can monitor for suspicious activity on your account.
- Watch out for signs of identity crime. Visit sites such as Experian, Equifax or Noodle (others are available) to check your credit rating to make sure no one has applied for credit in your name.
- Yahoo is also asking users to consider using Yahoo Account Key, a simple authentication tool that eliminates the need to use a password altogether.

Facebook Hack & PayPal Scam Warning
Fraudsters are hacking victims Facebook accounts through unknown means and changing their password and phone number.

The fraudsters then message the hacked victims’ friends to ask them to receive payments through PayPal for various reasons. They then ask for their phone number so they can communicate through WhatsApp.

The fraudsters try to convince the victim to receive funds into their PayPal account and transfer them into a bank account of the scammers’ choice.

A chargeback is then initiated through PayPal, leaving the PayPal account holder out of pocket as they have already sent the money to the fraudster’s bank account.

Top Tips
- If you receive a suspicious message from a friend on Facebook, contact them via other means to check the message is genuine.
- Create a strong password. You should change passwords often and never use the same one twice.
- Be wary of anyone calling asking for personal information, bank details or passwords. If in doubt, just hang up.
- Contact your bank/credit card company, so that they can monitor for suspicious activity on your account.
- Be aware of scam apps – read user reviews & see what the app wants to access before downloading it. THINK: Why would a ‘calculator app’ want to access your contacts or camera?

Need To Change Your Password?
- Make it long and complex
- Use a line from your favourite book/song/film
- Use the first letters of each word
- Change some of the letters for numb3r5 and punctuation
- Find it difficult to think of (and remember) new passwords? Download a password manager which does the hard work for you – make sure you have a secure password to access this!

October’s Top Tip: Be Safe Across All Of Your Devices
- Phones and tablets should not be ignored when thinking about online safety.
- Anti-Virus is available for, and should be installed on, mobile devices.
- Be aware of scam apps – read user reviews & see what the app wants to access before downloading it. THINK: Why would a ‘calculator app’ want to access your contacts or camera?

If You Are Affected
- If you receive a suspicious message from a friend on Facebook, contact them via other means to check the message is genuine.
- Create a strong password. You should change passwords often and never use the same one twice.
- Be wary of anyone calling asking for personal information, bank details or passwords. If in doubt, just hang up.
- Contact your bank/credit card company, so that they can monitor for suspicious activity on your account.
- Be aware of scam apps – read user reviews & see what the app wants to access before downloading it. THINK: Why would a ‘calculator app’ want to access your contacts or camera?
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.

Financial Scam ‘Every 15 Seconds’ In The UK
A financial scam was committed once every 15 seconds in the first half of this year.

More than one million cases of card, cheque, phone or online fraud were recorded from January to June, Financial Fraud Action (FFA) said. This was a 53% rise on the same period last year.

Losses are often refunded by banks, but not in every case. Many people are too embarrassed to admit they have been caught out.

Last year, financial fraud losses reached £755m – a 26% increase on the previous year.

Email deception, as well as phone and text-based scams, are now common tools in the modern-day bank robber’s trade – reflected in official crime figures which now include fraud data.

Top Tips
- Never disclose personal details such as PINs and passwords
- Don’t assume an email request or caller is genuine
- Don’t be rushed. Genuine callers allow time to return a call
- Have confidence to refuse unusual requests
- If you do fall victim – report it to Action Fraud

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 SOON
CYBER SAFE WARWICKSHIRE WEBSITE