

HOW SAFE ARE YOU?

Are you aware of who is behind you when using a Cash Machine?

Using free public Wifi access is like letting everyone view your PIN! Beware - your data is not secure and can be easily intercepted when using an untrusted Wifi point.

Would you let your kids talk to strangers?

They do on social media... Not everyone online is who they say they are.

Most social media sites include privacy and parental controls, make sure you know how they work!

Have you been offered a free iPad recently?

If it sounds too good to be true, it probably is!

Phishing emails are like pick pockets trying to steal your money. Think before opening emails with

attachments! Make sure your antivirus is up to date.

Do all your doors and windows lock? Who has access to your keys?

Make sure your devices are update with the latest security patches available!

You might be leaving a window open!

Cyber Safety Basics



Install Updates - All software vendors release updates for their products. Make sure all software is up to date, so your device is not vulnerable to hackers.



Use Strong Passwords - Passwords are the first defence against hackers. Poor passwords can be easily guessed and leave people vulnerable to identity theft. Make sure your passwords are more than 15 characters in length, include upper and lower case letters, with symbols and numbers. Never use the same password on another website.



Install & Update Security Software - Even today's smart phones have the option to install Anti-Virus software. Device protection does not have to be expensive.

Safety Continued...




Avoid Scams - If you do not believe everything you read in the papers, why would you believe what you read online? The internet is made up of open sources, which anyone can join. Always research what you find. Your best friend is a Search Engine.



Shop Online Safely - Always visit reputable Shopping Sites. If possible use a third party such as PayPal.com. Make sure the website is secure, by looking for the HTTPS padlock.



Monitor Your Online Privacy - Be careful what information you put on the Internet and Social Media. Do not leave yourself open to becoming a Victim of Cyber Bullying. If you  that you are flying away on Holiday, who else knows?



www.cyberstreetwise.com

< How to report Cyber Crime />

If you have been a Victim of Cyber Crime please report it directly to Action Fraud. This can be done by visiting www.actionfraud.police.uk or calling 0300 123 2040.



If there is an imminent risk to life please call your local Police Force on 999.

Action Fraud is the UK's national fraud and internet crime reporting centre.

< Where to get advice />

To get instant advice on how to protect yourself from becoming a Victim of Cyber Crime, visit www.cyberstreetwise.com

Cyber Streetwise is a HM Government website explaining Cyber Safety Basics to protect you and your family.

To access further information in relation to

Online Expert Advice, visit www.getsafeonline.org

THINK! Cyber Security is important...

West Midlands

RCCU

Regional Cyber Crime Unit

Cyber Crime Are you a Victim of it ?



Staffordshire West Midlands West Mercia Warwickshire

Working together to keep our communities safe