SIMPLE STEPS TO PROTECT YOURSELF, YOUR INFORMATION AND YOUR MONEY

Keep up to date!

Quite simply, our first line of defence against cybercrime are the devices we use to access internet and email. So whatever devices, operating systems, software or apps you use, always ensure you are running the most up to date versions. Updates include security patches to fix vulnerabilities! If you can, select 'Auto Update'. If you are still using Windows XP, Vista or Windows 7 you need to upgrade ASAP.

Antivirus

Make sure you have up to date antivirus installed and running for all devices you use to access the internet and email – make sure you are always running the most up to date. If you can, select 'Auto Update'.

Passwords

In a nutshell, you need to have a different password for everything you log in to. Make sure you're using #ThreeRandomWords to create a strong, separate password for each account, adding uppercase letters and symbols for complexity. Consider installing a Password Manager App. You can save passwords in browsers, but this should only be where you are the only person using that device. https://www.ncsc.gov.uk/cyberaware/home#action-2

Protect your passwords

www.haveibeenpwned.com – check to see if your details have been compromised in known data breach incidents. Click on the three lines and opt for 'notify me' – you will be contacted anytime your passwords are found to available in a new breach allowing you to immediately change your passwords to protect your online accounts.

#2FA Turn it on!

Most email accounts, shopping and social media accounts will allow you to choose 2 Factor Authentication (2FA) in the security settings. It means you'll need to carry out an extra step to log in if you are using a different device or from somewhere new, but it means that ONLY you will be able to log in to your accounts!

For step by step instructions on how to set this up for different platforms, visit www.2fa.directory

If the worst should happen, here is some advice on recovering a compromised account https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account

BEWARE of phishing emails!

ALWAYS #TakeFive and REMEMBER! *– emails, texts and phone calls can all easily be spoofed. NEVER assume any contact is genuine until you have verified that it is.* ***Don't click*** *on links in emails or open attachments unless you are certain they are safe.*

If an email relates to an account issue of ANY sort, always log in via a browser or an app – ***NEVER*** *click on a shortcut in a text or email to log in or "resolve" an issue to ensure you avoid fake, copycat websites.*

Did you know that you can forward ANY suspected phishing emails **to** report@phishing.gov.uk; and suspicious texts can be forwarded to 7726 (spells SPAM on your keypad)

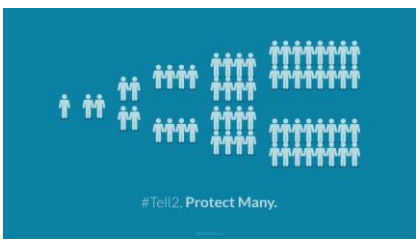
iTunes / Gift Card Scams

HMRC do not instigate debt collection via telephone, and Police do not give advance notice of exercising a warrant for arrest. **NO** legitimate debt can be paid in iTunes vouchers or any other type of gift card - *#HangUp* on that call

Courier Fraud

Neither the Police nor Banks will ever contact you to:

- transfer money to a safe account;
- withdraw funds for safekeeping;
- assist with a covert investigation;
- purchase high value items or jewellery;
- OR collect cash, bank cards or PIN numbers



Bank Accounts

REMEMBER it is a criminal offence to allow your bank account to be used for making payments on behalf of others! It's money laundering! https://www.moneymules.co.uk/

Cyber Aware Action Plan

Learn how to protect yourself with the Cyber Aware Action Plan. Answer a few questions on topics like passwords and two-factor authentication and get a free personalised list of actions that will help you improve your cyber security. https://www.ncsc.gov.uk/cyberaware/actionplan

Reporting Cybercrime and Fraud

Underreporting of incidents is still very high. Please report all incidents of cybercrime and fraud to Action Fraud – either online at www.actionfraud.police.uk or via 0300 123 2040.

Social Media

Social media is a great way to stay in touch with family, friends and keep up to date on the latest news. However, it's important to know how to manage the security and privacy settings on your accounts (turn that #2FA on!), so that your personal information remains inaccessible to anyone but you. The link below also contains links to specific platforms so that you can step up your security.
https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

CHOOSING ANTIVIRUS, Virtual Private Network Apps (VPN) ETC

Paid for solutions are always going to be superior to free versions

- Read reviews from other users – just as you would when researching restaurants or holidays!
- Search for articles on best products and visit GetSafeOnline, www.ncsc.gov.uk and 'Which?'
- Note the number of downloads and reviews left before downloading any apps or software (if not many, AVOID!)
- What score do other users give it?

Derbyshire Alert

Sign up to Derbyshire Police free Community Email Messaging Service, for local beat information, crime prevention, fraud and cyber advice visit www.derbyshirealert.co.uk and select "Sign up now".

Thinking of investing?

Sadly, there are many fake investment scams being offered via telephone, social media, email and the internet. **ALWAYS** check the FCA register BEFORE investing money https://register.fca.org.uk/s/

Samantha HANCOCK - Cyber Protect Officer
samantha.hancock@derbyshire.police.uk

Want to know more?

VISIT

www.cyberaware.gov.uk www.eastmidlandscybersecure.co.uk www.ncsc.gov.uk
www.getsafeonline.org www.actionfraud.police.uk www.saferinternet.org.uk
www.take-stopfraud.org.uk

For more advice follow @EMCyberSecure on Twitter and Facebook!

Why not visit www.eastmidlandscybersecure.co.uk for more advice and information.
DON'T ASSUME EVERYONE KNOWS – SHARE THIS INFO WITH OTHERS!