**CYBER-CRIME – HOW TO PROTECT YOURSELF**

****

**Tip 1 – Have Strong Passwords.** Your password is the key to your online life; make sure it’s strong. Don’t use words personal to you (sports teams, pets, family names, birth dates etc.) and never share them with anyone! Always have a different password for your email.

To create a strong password simply join three random words together. You can add uppercase letters, numbers and symbols to make it more secure. You can store passwords in your browser or use a password manager such as Keeper (www.keepersecurity.com); this is particularly useful for those with multiple passwords for work and personal use.

**Tip 2 – Use Antivirus.** Antivirus is your first line of defence. Make sure you use it, and it’s kept up to date. Viruses and malicious software (malware) can infect any device (computers, phones etc.). Once malware is on your system it can lock you out, steal your information, or even watch you in your home! Antivirus software protects against malware.



Most systems have antivirus built in, so make sure you’re using it. Also, consider installing extra antivirus software on all of your devices (this can be free). These check everything coming into your device and will alert you if anything tries to infect your system. There are many options available on the market at varying price ranges; the following were voted top 3 in 2020 by TechRadar.com: Bitdefender, Norton, and Kaspersky.

**Tip 3 – Don’t Click on Links or Attachments.** Clicking on unverified links or attachments can give criminals access to your devices. Emails or texts you receive may contain attachments or links you are asked to click on. If you do, you’re instantly bypassing the security measures you already have in place.

Don’t click on links unless you can verify where they came from. Call the sender to check it’s genuine. If in doubt don’t click it. To ‘hard’ delete from your system press the shift key and the delete button (noting that this will permanently delete the message from your inbox).

**Tip 4 – Turn on Two-Factor Authentication (2FA).** 2FA proves you are who you claim to be online. Passwords can be stolen by cyber criminals. However, accounts that have been set up to use 2FA will require you to input an extra ‘factor’. This will be something only you can access like a code sent to you by text or generated by an app on your device. So, even if a criminal knows your password, they won’t be able to access your accounts.

Wherever available turn on 2FA on any accounts that contain important information. Go to www.turnon2fa.com for instructions on how to set up 2FA across popular online services.

Report all fraud and cybercrime to ‘Action Fraud’ online at [www.actionfraud.police.uk](http://www.actionfraud.police.uk) or by telephone on 0300 123 2040.