CYBER CRIME PROTECT

TOP TIPS FOR PROTECTING AGAINST CYBER CRIME

USE A STRONG PASSWORD AND USE DIFFERENT PASSWORDS FOR EACH ACCOUNT

Use three random words for example, coffeetrainfish. Avoid using words which are easy to guess, such as onetwothree. Avoid using words which are closely related to you, such as the names of family members or pets.

INSTALL TRUSTED SECURITY SOFTWARE

Most computers will have a basic anti-virus and firewall software pre-installed. Make sure it is activated and don't ignore the prompts to update when they flash up – do it straight away.

KEEP SOFTWARE AND APPS UP-TO-DATE

If you get notifications of updates, don't ignore them. They often contain security fixes so update as soon as possible.

BE SOCIAL MEDIA SAVVY

Check the security settings of your social media profiles to make sure they are set to private. Be careful what information you post online. Once it is on the Internet, it is there forever!

BE WARY OF EMAILS AND TEXTS FROM PEOPLE YOU DON'T KNOW

Never click on links in emails from someone you don't know or trust. They could contain malicious software which could compromise your computer systems and your information. If a message seems suspicious or you don't recognise the sender, be cautious or delete it.

KEEP YOUR DATA SAFE

If you are sending confidential data or personal information, encrypting it will make it a lot more secure. For example compress the files and secure with a password.

USE 2-FACTOR AUTHENTICATION WHERE YOU CAN

2-factor authentication improves the security of your emails because it means your password alone is not enough to access your account, you have to have an extra piece of information that only you should know.

BACK UP ALL IMPORTANT FILES REGULARLY

Back up all important files regularly on to an external hard-drive, memory stick, or cloud-based storage or all three to be extra secure. If using cloud-based storage log out after each use.

DON'T SEND SENSITIVE INFORMATION OVER PUBLIC WI-FI

Data sent over public wi-fi can be accessed by others. It can be easy for a criminal to access personal data over public wi-fi or create their own wi-fi access point to gain access to your device and your details.

BEWARE OF FAKE WEBSITES

Cyber criminals are experts in tricking people. They can set-up fake websites almost identical to real website addresses where they can try to get you to share sensitive information, such as your bank account details or passwords, or download malware (malicious software) which can infect your devices, damaging or deleting your data. Keep a favourites list of websites you commonly use and avoid links on emails you are unsure of.

HELP YOUR FAMILY AND FRIENDS BY SHARING ADVICE ON HOW TO STAY CYBER SAFE AND PROTECT THEIR DEVICES, MONEY AND PRIVACY.

If you suspect a crime, call
Action Fraud on **0300 123 2040**
or the police on **101**

Further sources of help:
www.actionfraud.police.uk
www.getsafeonline.org

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

CYBER AWARE

GREATER MANCHESTER POLICE