CYBER CRIME PROTECT

GUIDE TO STAYING SAFE ONLINE

GREATER MANCHESTER
POLICE

cyber.protectprevent@gmp.police.uk

Before we get to the "Techy stuff" let's talk...

PHYSICAL SECURITY!

- Don't leave devices unattended
- Secure ALL devices with a pin code/password where possible.
- Be aware of who is around, and could look over your shoulder at your device.
- Be careful of damage – Drops/spillages and transport devices like laptops in waterproof carriers.
- If you commute to work or school with any devices (phones/ laptops) then store them securely and out of sight.
- NEVER plug in a found USB device as it could transfer a virus or other malware to your system.
- If you log-in to any account/school/work system, log-out and secure the device as soon as your session is complete.
- When you are out-and-about, try not to have your head down in your phone, pay attention to possible dangers around you - especially when its dark, don't be lighting up the street with your phone!

Let's talk about the importance of...

PASSWORDS

- Ensure that all of your accounts are protected with a STRONG password! We advise THREE RANDOM WORDS.

THREE RANDOM WORDS
CandleBottleSweet4!

- Do not disclose passwords to anyone else.
- Ensure that all of your accounts have different passwords.
- Create a SUPER strong AND separate password for your email account.
  *Your email account is the hub that connects ALL of your other online accounts; gaming accounts, online shopping orders, online banking, social media etc.
- Statistically, if your password is 12 characters or longer, you are safer from being hacked.

The magic number is…12

- Use 2-factor authentication where possible.
  *this improves the security of accounts as it means that a password alone is not enough to access your account.
- Save your passwords in a password manager or to your internet browser.

  *This will help you to have strong and different passwords on ALL of your accounts, and remember them.

Installing and backing up

Install the latest software and app UPDATES!

Software and app updates contain vital security updates to help protect your devices from cyber criminals.

Always have BACK UP!

Back up all important files regularly, whether it's an external hard-drive, memory stick, or cloud-based storage.
*If using cloud-based storage log out after each use, disconnect any hard drive/ removable memory.

Install TRUSTED anti-virus security software!

Always research any additional products, and make sure they meet YOUR requirements. Don't pay a fortune for fancy software if it's not necessary.
* There are many free products available, and free trials/versions of paid services.

Let's talk about being...

SOCIAL MEDIA SAVVY!

- Check the security settings of your social media profiles to make sure they are set to **PRIVATE**.

  *You don't need 1000+ followers/friends that you **DO NOT** know, especially if one is somebody dangerous!

- Not everyone using social media is necessarily who they say they are. Take a moment to check if you **KNOW** the person, and if the friend/follow is genuine.

- Consider what your followers and friends **NEED** to know, and what detail is unnecessary (but could be useful for criminals).

- Once something is posted, it is there **FOREVER**...Even if it is DELETED! **THINK before you click!**

- Make sure your LOCATION SERVICES are switched **OFF!** It is your responsibility to check the location settings of **ALL** apps that you download.

- Once your Location Services are **OFF**, make sure you don't share your current location via Instagram stories, TikTok videos, Facebook check-ins, tags etc.
  *post any pictures and videos taken, once you get home.

Let's talk about sensitive information...

PUBLIC WI-FI

Don't send sensitive information over public Wi-Fi. Data sent over public Wi-Fi can be accessed by others/criminals.
OR
Criminals can create their own Wi-Fi access point to gain access to your device and your details.

PHISHING

This is a type of social engineering where attackers influence users to do 'the wrong thing', such as disclosing information or clicking a bad link.

Phishing is commonly carried out via email, text and phone calls.

Don't click on the links or attachments in suspicious emails, and never respond to messages that ask for your personal or financial details.

SUSPICIOUS EMAILS CAN BE FORWARDED TO;
report@phishing.gov.uk

SUSPICIOUS TEXTS CAN BE FORWARDED TO;
7726

INDECENT IMAGES

Creating, possessing, or sharing sexual images or videos of a child under 18 is illegal, even if the person doing it is a child.

When sharing pictures/videos online, we advise anyone under 18;

- Never take a picture without clothes on (REPORT if asked to!)
- Do not to wear revealing outfits or school uniform.
- Keep accounts PRIVATE and share with real FRIENDS only.

TO ANONYMOUSLY REPORT ANY INDECENT IMAGES OF CHILDREN UNDER 18: www.iwf.org.uk

BULLYING

REMEMBER: Be as kind as possible with your words and actions, and also be aware of those of the people around you!

Online comments, messages, likes, and group chats can get out of hand. You never know how your actions can affect someone else, so always BE KIND.

If you are being bullied online, UNFRIEND the person, BLOCK the person, REPORT the comments/messages to the platform used, and DO NOT respond.

If you are a child, speak to an adult that you trust, or call CHILDLINE on 0800 1111.

REPORT NON-EMERGENCIES ONLINE

REPORT ONLINE	REPORT ONLINE	REPORT ONLINE	CONTACT US	REQUEST
				
A CRIME	NON-INJURY ROAD TRAFFIC INCIDENT	ANTI-SOCIAL BEHAVIOUR	VIA LIVECHAT	AN UPDATE

SCAN ME

REMEMBER, IF IT'S NOT 999, REPORT ONLINE!

GREATER MANCHESTER POLICE

www.gmp.police.uk