Cyber Security – Social Media

This October brings Cyber Security month. The month is dedicated to creating resources and spreading awareness about staying safe online.

For this newsletter we are going to talk about social media and how to use it safely.

You forever see posts online about people being hacked or receiving scam messages and while most of them seem very obvious, some are not. Some have more detail and look more believable.

There are all kinds of ways to keep your data protected. For example:

- Enabling multi-factor authentication.
- Using strong passwords.
- Using a password vault.
- Updating software.
- Keep personal information limited.
- Be careful and aware of who you are talking to online.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is one of the easiest and widely available ways to protect your social media accounts and beyond.

Hackers have gotten very good at compromising passwords but with MFA means attackers with a stolen password still can't access the online service.

The majority of sites give you the option to enable MFA and some even prompt you to set it up after signing up and logging in.

Content of Your Posts

One of the biggest things you will or will have been taught about social media in school or work etc is to be wary of what you post online. Posting to social media is part of the fun and how you interact with others but being careful is so important in keeping you safe.

Posting personal information that can tie you to a school, workplace or a place that you frequently visit could be potentially dangerous, especially on accounts that aren't private unless set as such, for example a Twitter/X account. If the information lands in the wrong hands, you could face being doxxed or have someone you don't know turn up at these locations.

Doxxing is the act of revealing identifying information about someone online, such as their real name, home address, workplace, phone, financial, and other personal information.

Setting your profiles to private is a great way to be able to control who you're engaging with online, but it is important to remember that everything can be shared and once posted online, nothing is truly private.

Another great way to protect yourself is to block people who are causing any trouble to you.

Fake Accounts and Scams

While you can't control what others do, you can be aware of it, especially when it comes to being online.

Quite frequently on Facebook there are fake accounts pretending to be you or your family/friends in order to try and message people and convince them to send money.

They take the same name and profile picture of the person they are impersonating to try and look convincing however they almost always have no friends or posts.

If you are unsure, the best way to find out if they are real or not, besides asking the person being impersonated is to ask the fake account about things that don't exist. For instance, ask how their son or daughter are if they have no children. The scammers usually respond saying they are well etc.

A good way to secure your social media accounts is to periodically log out your account from all devices, which is an option you can usually find in settings.

This is how to find it on Twitter/X
Settings -> Security and Account Access -> Apps and Sessions -> Sessions

If you ever find yourself in a position where information has been leaked or someone is threatening to leak information that would put you in danger, please seek help from the police.