24/7 SECURITY SERVICES
Personal • Integrated • Effective

# PERSONAL SAFETY BULLETIN

October 2023

# October is Cyber Security Month

## Keep software up to date

Installing software updates for your operating system and programs is critical:

- Always install the latest security updates for your devices.
- Turn on Automatic Updates for your operating system.
- Use web browsers that receive frequent, automatic security updates.
- Make sure to keep browser plug-ins up to date.

## Avoid phishing scams

Phishing scams are a constant threat - using various social engineering ploys, cyber-criminals will attempt to trick you into divulging personal information such as your login IDs and passwords, banking or credit card information. Phishing scams can be carried out by phone, text, or social networking sites - but most commonly by email. Be suspicious of any official-looking email message or phone call that asks for personal or financial information.

## Practice good password management

We all have many passwords to manage - and it's easy to take short-cuts, like reusing the same password. Create strong passwords or opt for a password manager that can help you to maintain strong, unique passwords for all of your accounts.

## Be careful what you click

Avoid visiting unknown websites or downloading software from untrusted sources. These sites often host malware that will automatically install and compromise your computer. If attachments or links in the email are unexpected or suspicious for any reason, don't click on them.

## Never leave devices unattended

The physical security of your devices is just as important as their technical security. If you need to leave your laptop, phone, or tablet for any length of time - lock it so no one else can use it. If you keep protected data on a flash drive or external hard drive, make sure they are encrypted and password protected.

## Use mobile devices safely

- Lock your device with a PIN or password
- Never leave it unprotected in public
- Only install apps from trusted sources
- Keep the device's operating system up to date
- Avoid transmitting or storing personal information on the device
- Don't click on links or attachments from unsolicited emails or texts


## Cyber Security Tips for Kids

- Never give out personal information such as your address, telephone number, and parents' work address/telephone numbers without your parents' permission.
- Tell your parents immediately if you come across something that makes you feel uncomfortable.
- Never agree to get together with someone you 'meet' online without first checking with your parents. If your parents agree to the meeting, make sure that it is in a public place and take a parent along.
- Remember that not everyone online is who they say they are, do not befriend strangers. Do not post pictures or any content online that your parents consider to being inappropriate. Never respond to any messages that are mean or in any way make you feel uncomfortable.
- Do not give out your passwords to anyone (even your best friends) other than your parents.
- Check with your parents before downloading or installing any software or doing anything that could possibly hurt your computer or mobile device or jeopardise your family's privacy.
- Do not buy anything online without talking to your parents first. Some advertisements may try to trick you by offering free things or telling you that you have won something as a way of collecting your personal information.