Malton Women Council

Cyber Safety

Tip Shet

Funded in part by
the City of Brampton's
Advance Brampton Fund

info@mwc.community
www.mwc.community
+1 647-391-9668

Malton Women Council

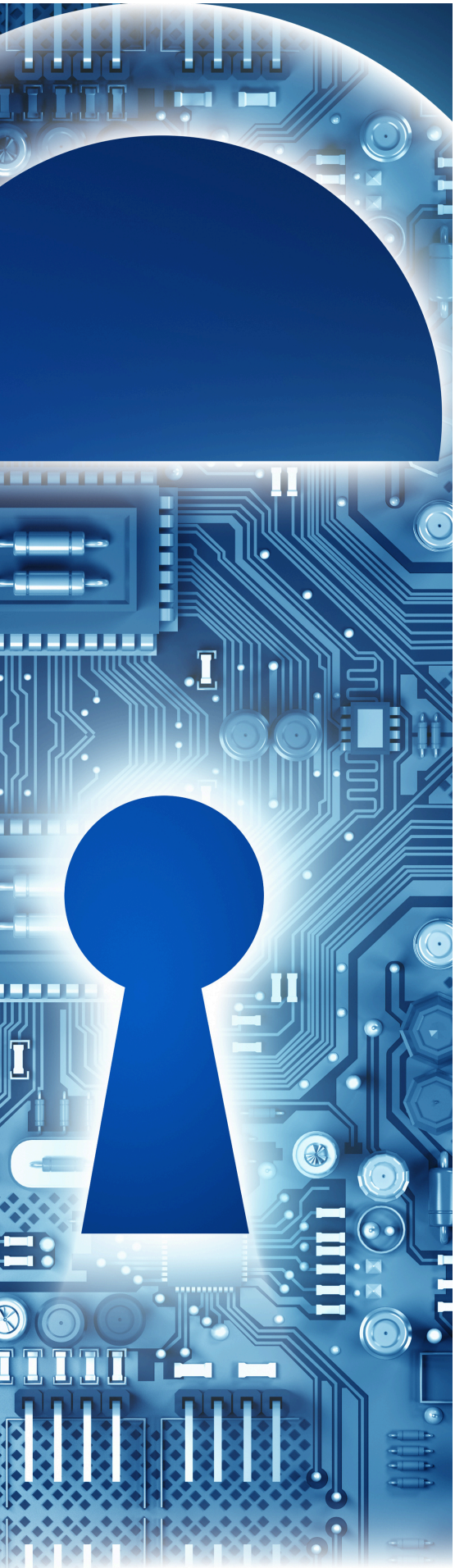


Table of Contents

Cyber Safety

As society becomes increasingly dependent on technology for school, work, and personal endeavors, it is important to learn to keep your data safe online. Keep reading to learn more about the different threats you may encounter in the online world.

Malware

Malware or malicious software refers to a program or code that can damage systems. Malware can steal your data, hijack your computer, and spy on your computer activity.

There are various types of malware, such as:

- Virus – A virus attaches to another program and, when executed, it replicates itself, modifies other programs, and infects them.
- Trojan – A Trojan often appears as a useful tool to trick you. It can steal financial information and install other malware on the computer.
- Keylogger – A keylogger can record your keystrokes to gather sensitive information such as passwords and banking details.
- Adware – Adware is unwanted software that shows you unwanted ads. It often piggybacks onto another program to trick you into installing it.
- Ransomware – Ransomware locks your device and/or encrypts files. To gain back access, you need to pay the cybercriminal.

info@mwc.community
www.mwc.community
+1 647-391-9668

Causes of Malware

Your device may become infected with malware when browsing suspicious websites (including those that look legitimate), downloading infected files, installing programs or apps from unfamiliar sources, opening malicious emails, or clicking on malicious links through websites, emails, texts, etc.

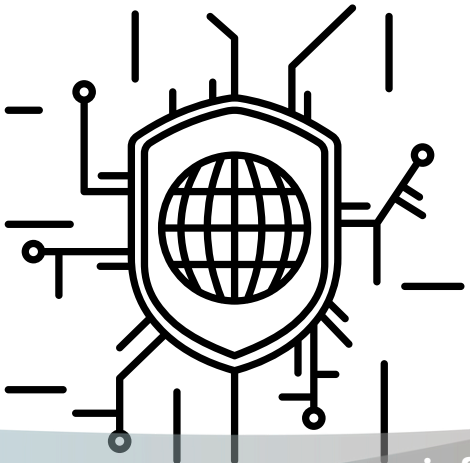
- Some common signs of malware include:
- Increase in pop-ups and advertisements.
- Confusing increase in data usage.
- Bogus charges on your bills.
- Suspicious texts and emails received by contacts.
- Hot phone caused by malware activity.
- Unknown apps.
- Wi-Fi and internet switch on by themselves.

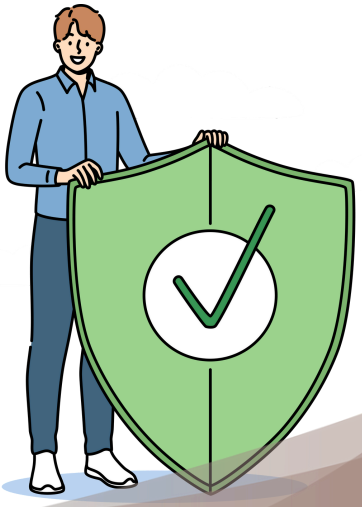
info@mwc.community
www.mwc.community
+1 647-391-9668

Malware Prevention Tips

To prevent your devices from becoming infected with malware, follow the advice below:

- Ensure the website domain name is recognizable, i.e., com, .ca, net, org, edu, .biz, etc., before clicking.
- Avoid clicking on pop-up ads.
- Use strong passwords and multi-factor authentication.
- Do not click on suspicious links in emails, texts, or websites.
- Do not download software from unknown sources or peer-to-peer file transfer networks.
- Do not open attachments from unknown senders.
- Delete programs and apps you no longer use or recognize.
- Back up data regularly.
- Use and install cybersecurity software.





info@mwc.community
www.mwc.community
+1 647-391-9668

- If your account or device has been hacked:
- Install and run a cybersecurity program to scan your computer for malware. Use the program to remove malware from your computer.
- Change the password for your device and all accounts (email, social media, banking, shopping, etc.).
- Change the password for the hacked account and related accounts with the same password.
- Check your email filter and forwarding rules. A criminal may have your account set up to receive a copy of your emails. This will allow them to reset your password.

info@mwc.community
www.mwc.community
+1 647-391-9668

What to do if I am hacked?

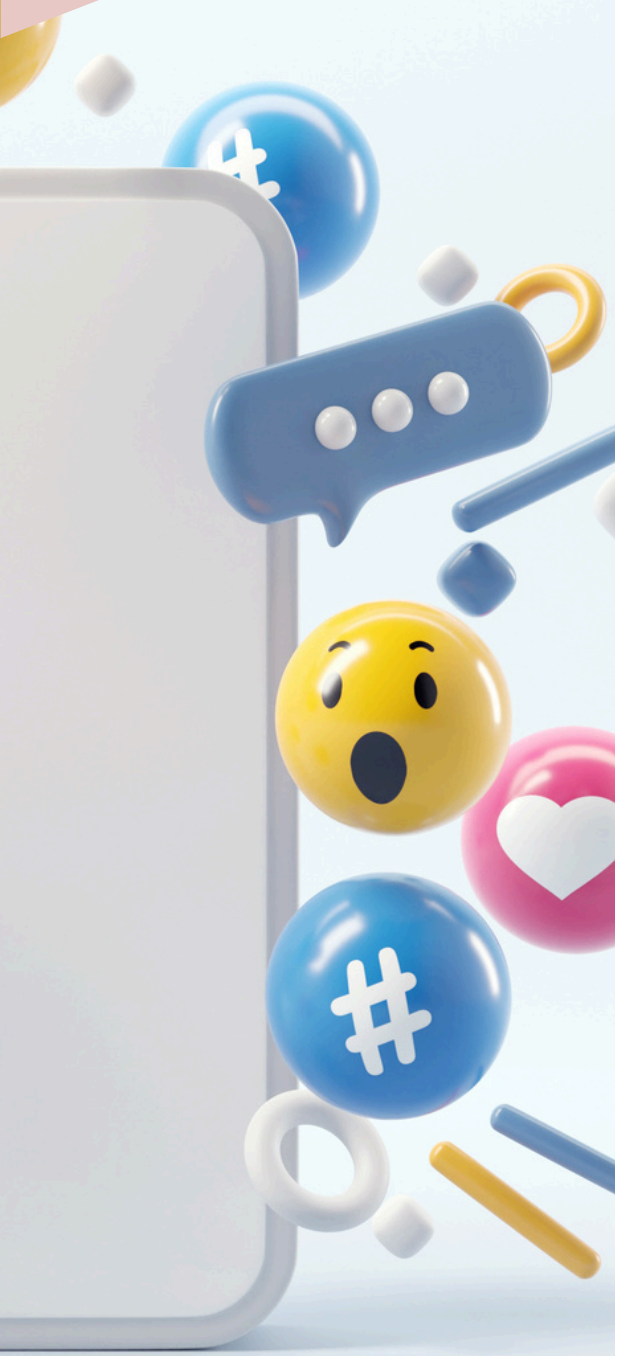
- Log out of all devices and apps that are currently logged into your account. This will prevent the criminal from accessing your account.
- Set up Multi-Factor Authentication.
- Update your apps and devices.
- Tell your contacts that you have been hacked and to avoid any suspicious messages they may receive from your account.
- Check your bank statements and online store accounts. If your email account is linked to these accounts, you may also find unrecognizable financial activity. Contact your bank if you need support.
- Report to your bank and local authorities if you have lost money.

info@mwc.community
www.mwc.community
+1 647-391-9668

How can I secure my Accounts?

- Use a strong password or passphrase. Passwords should be 12 characters or more with letters, symbols, upper and lower case, and numbers. They should not include names or birthdates. If creating a passphrase, choose a combination of four or more words and a minimum of 15 characters.
- Do not use the same password for all your accounts.
- Only log in from trusted sources.
- Never share your password.
- Enable multi-factor authentication. This involves having verification beyond a password, such as through a code provided by an app, text, email, or call.

info@mwc.community
www.mwc.community
+1 647-391-9668



Social Media

- Review your social media privacy and security settings.
- Avoid sharing personal information, financial information, vacation details, or big purchases and events on social media. This can result in fraud and robbery.
- Turn off geo-tagging.
- Review the background of photos (for license plates, street signs, etc.) before posting.

info@mwc.community
www.mwc.community
+1 647-391-9668

How can I secure my devices?

Laptops and Computers

- Install anti-virus and anti-spyware software. Run weekly scans.
- Update your software and operating system regularly. Turn on automatic updates.
- Customize browser security settings rather than accepting default settings. Balance security with user experience.
- Keep your browser updated. Some browsers update automatically.
- Clear your cache and browsing history. Log out of your accounts.
- Download files from trusted sources. Scan them with antivirus software before downloading. Delete suspicious files.
- Use a passphrase or a complex password for your computer. Lock files and documents.

info@mwc.community
www.mwc.community
+1 647-391-9668

How can I secure my devices?

Phones and Tablets

- Keep phones and tablets updated. Turn on automatic updates.
- Download apps from trusted sources like Google Play or the App Store. Apps with little to no information about the organization, contact details, website, etc., may not be trustworthy. Trusted sources may also host apps with security issues. Be careful.
- Review app permissions. Only enable permissions you are comfortable with.
- Avoid using public and unsecured wi-fi. If you must use public wi-fi, ensure it's from a trusted source. Never use public wi-fi for banking or accessing sensitive information.

How can I secure my devices?

Storage and Back-Up

- Back up data (photos, documents, videos, information, etc.) to an external hard drive or cloud system. Having another copy of your data can help you access it in case your device is infected with malware or stolen.
- Common cloud backup options include Apple iCloud, Microsoft OneDrive, and Google Drive. Secure your backup accounts using strong passwords and multi-factor authentication.
- Common removable media for backups include USBs, external hard drives, SD cards, and DVDs or CDs.
- Disconnect removable media when not in use. Malware infecting your device can also infect removable media.

info@mwc.community
www.mwc.community
+1 647-391-9668

How can I secure my connections?

Wi-Fi

- Change your network name and password from the default versions.
- Use a passphrase or a strong password.
- Limit area coverage by placing the router in the middle of the house rather than near a window.
- Update all devices on your network (computers, smartphones, routers, etc.) to protect your network.
- Turn public Wi-Fi off when not in use.
- Turn on the firewall and use a VPN when using public Wi-Fi.
- Avoid visiting sites with private information, such as banking websites, when using public Wi-Fi. Aim to visit secure sites using HTTPS only.

How can I secure my connections?

Firewalls

- Firewalls can act as extra protection for your device as your device contacts various pieces of information and other devices
- Your operating system will often have a firewall. Turn it on and keep it updated.
- Keep your operating system and software updated.
- Install a firewall from a credible source if you lack a firewall.

info@mwc.community
www.mwc.community
+1 647-391-9668

How can I secure my connections?

Bluetooth

Wireless devices such as printers, headphones, and keyboards can rely on Bluetooth to connect with phones and computers.

- Turn off Bluetooth to prevent strangers from connecting with your devices.
- Do not connect with strangers.
- Unpair devices. If one of your devices is lost, it can provide access to the rest of your devices. Delete the lost or stolen device from the list of paired devices on all your other Bluetooth devices.

info@mwc.community
www.mwc.community
+1 647-391-9668

How can I secure my connections?

Virtual Private Network (VPN)

- VPNs can help you browse privately when using public networks. They encrypt your internet traffic and disguise your identity. This can prevent others from tracking your online activity and stealing your data.

info@mwc.community
www.mwc.community
+1 647-391-9668

Resources and References

- To learn more about cyber safety, please visit the following resources
- Get Cyber Safe https://www.getcybersafe.gc.ca/en
- National Cyber Security Centre https://www.ncsc.gov.uk/
- VPN: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn
- What is Malware?: https://www.malwarebytes.com/malware

info@mwc.community
www.mwc.community
+1 647-391-9668