Malton Women Council

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

Cyber Fraud

Tip Sheet

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

Malton Women Council

Table of Contents

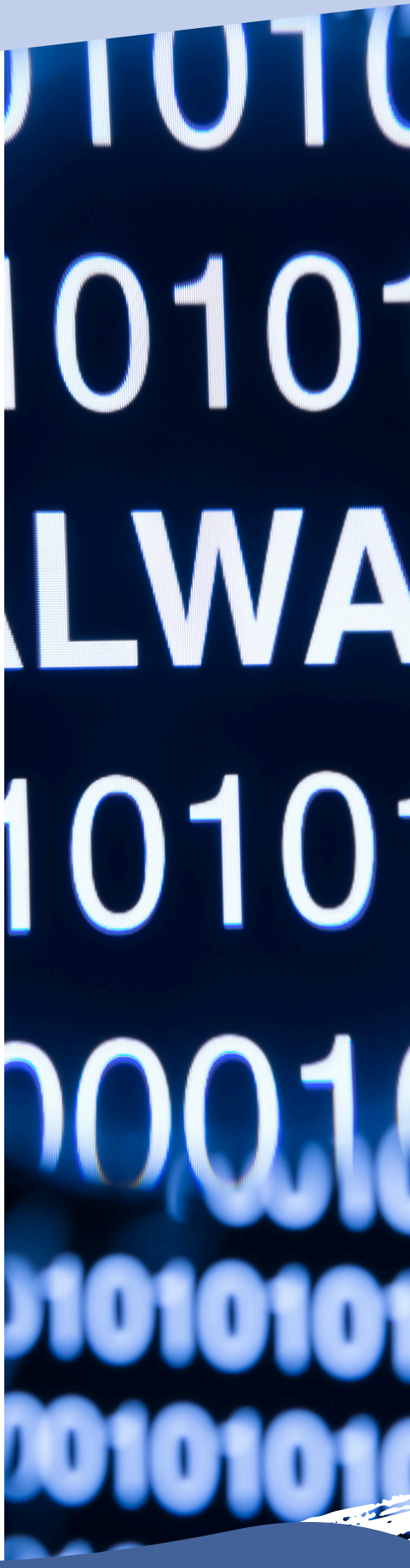
Fraud and Cyber Fraud

As society advances, so do the fraudsters and their tactics. Keep reading to learn more about how you can protect yourself from fraud.

Common Types of Frauds

Malware

- Malware is malicious software that damages your computer system without your consent. Examples of malware include viruses, worms, Trojans, spyware, and adware. Malware can steal sensitive information such as passwords, delete your files, monitor your activities and keystrokes, and take control of your computer.
- You may get malware on your computer if you accidentally download a suspicious program (even if it looks legitimate), open or download problematic attachments in emails, click on bad links in emails or texts, or visit a suspicious website.
- To protect yourself, never click on suspicious attachments, links, or emails. Install security software and regularly scan your computer and external drives, and USBs.
- If you fall victim to malware, scan your computer with security software to remove the malware, change your passwords, and enable two-factor authentication. You can seek help from a professional when necessary.



Identity Theft

- Identity Theft involves using your personal information (date of birth, name, credit card, etc.) to make purchases, obtain funds, and create social media and banking accounts in your name.
- To protect against identity theft, avoid sharing your personal information, keep your social insurance number, passport, and birth certificate in a safe place, ensure a website is secure when making transactions, regularly check your bank statements for errors, and review your credit history yearly.
- If you are a victim of identity theft, contact your bank, credit card company, police, and Equifax or TransUnion Canada to place a fraud alert on your credit reports.

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

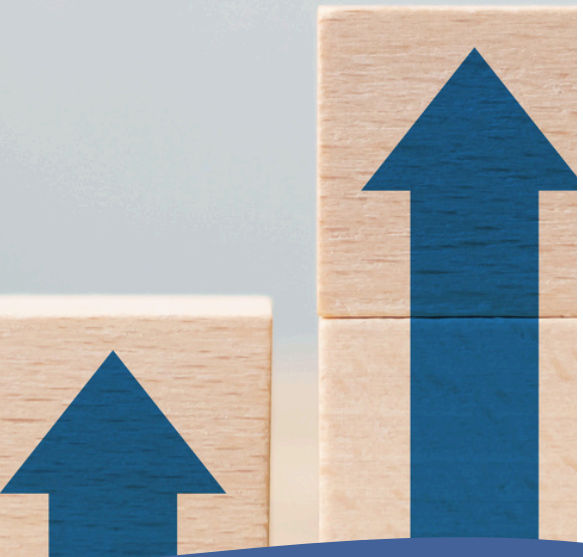
Online Shopping

- Social media, texting tools, and online websites may advertise fraudulent products and offer malicious links to products.
- To prevent fraud while shopping, follow the following tips:
- Research before clicking on deals, discounts, and products that seem too good to be true.
- Do not click on links in messages; visit the vendor's website in another browser.
- Buy from reputable sources.
- Be wary of online retailers that redirect to a third-party source during checkout.
- Monitor your credit card statement transactions.
- Note red flags in websites such as poor design, missing return and privacy policies, and missing contact information.

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

Canada Revenue Agency (CRA) Fraud

- Fraudsters may phone, email, or text you claiming they are from the CRA or Immigration, Refugees, and Citizenship Canada. They may demand immediate payment or claim you have a refund. They may seek your personal and banking information to process the transaction.
- The CRA will never send refunds by e-transfer or text. They will never demand payment by e-transfer, bitcoin, prepaid credit cards, or gift cards. They will not threaten to deport you or put you in jail. They will never ask for your personal or financial information in a voicemail or email.

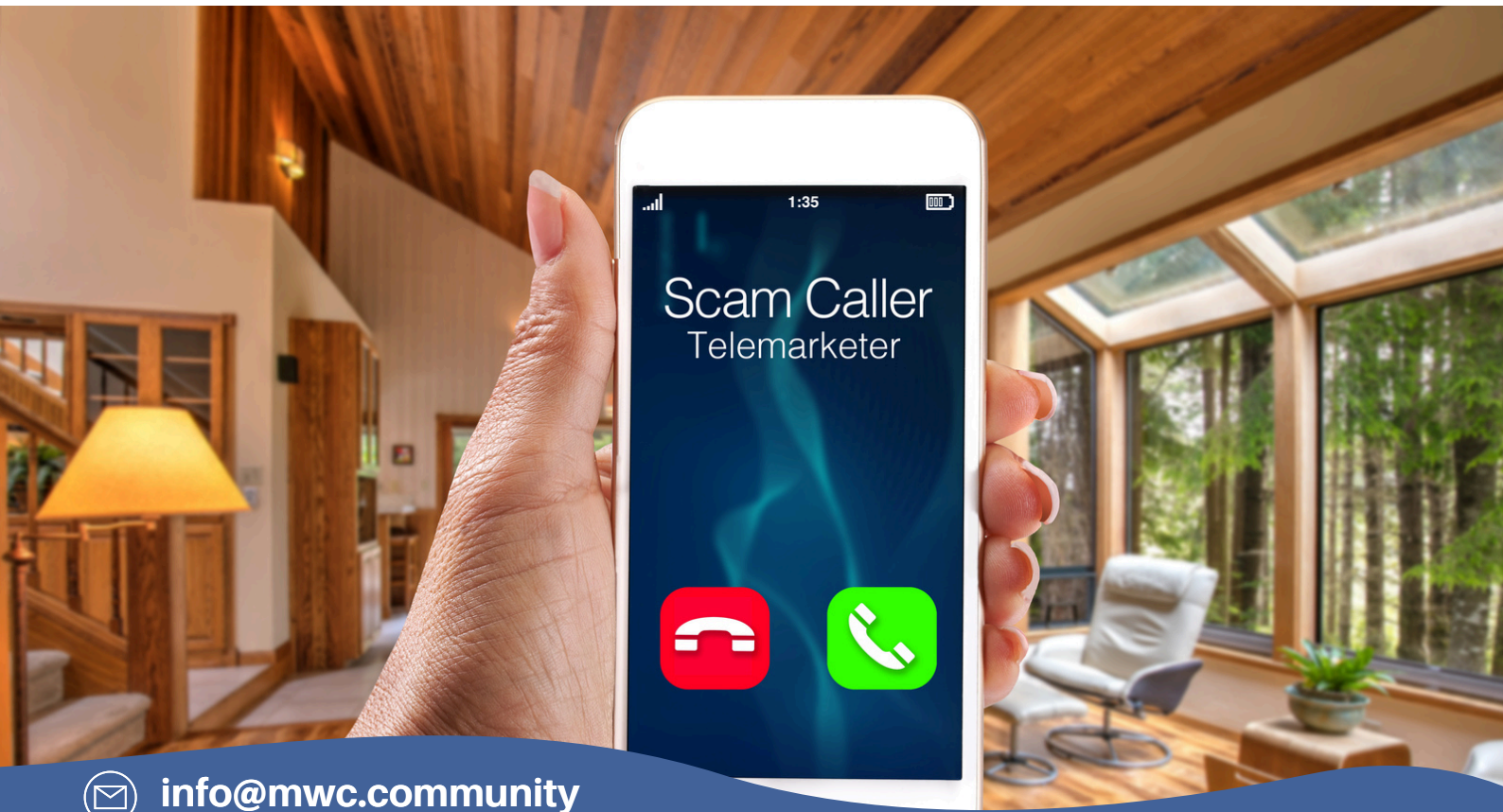


Financial Institution Scams

- Beware of calls, emails, and texts that claim to be from your financial institution. They may ask for your personal and financial information or ask you to click on a link. If you get such a call, tell them you will call them back. Wait for 10 minutes, use another phone, and call the number listed on the back of your credit or debit card instead to confirm who was calling. Never click on links in emails or texts.

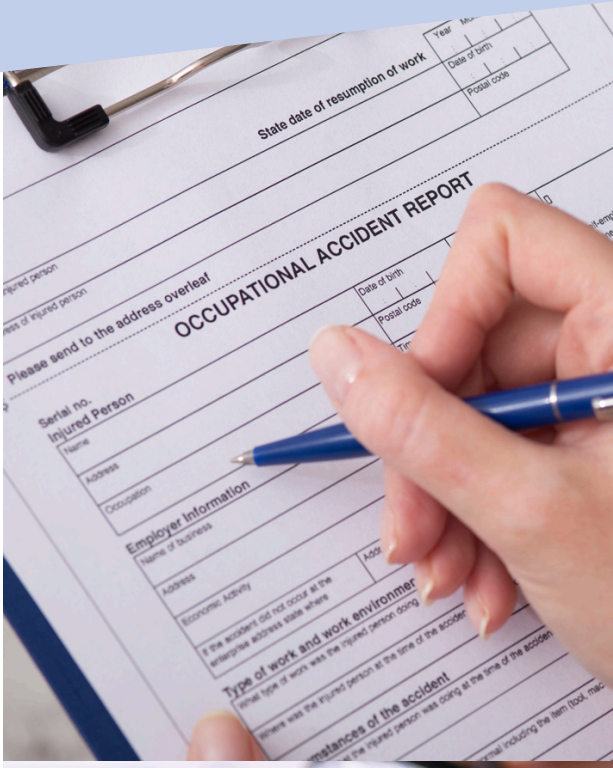
Emergency Scams

- You may receive a call saying your loved one, such as your grandchild, is in an emergency. The caller will pretend to be your loved one, they may claim to have the same name, they may even sound the same as a result of technology.
- A second person claiming to be a police officer or lawyer will give you instructions on how you can transfer money to help with the situation.
- Never transfer or give money. Call your family member or their parent instead from a different number to confirm.

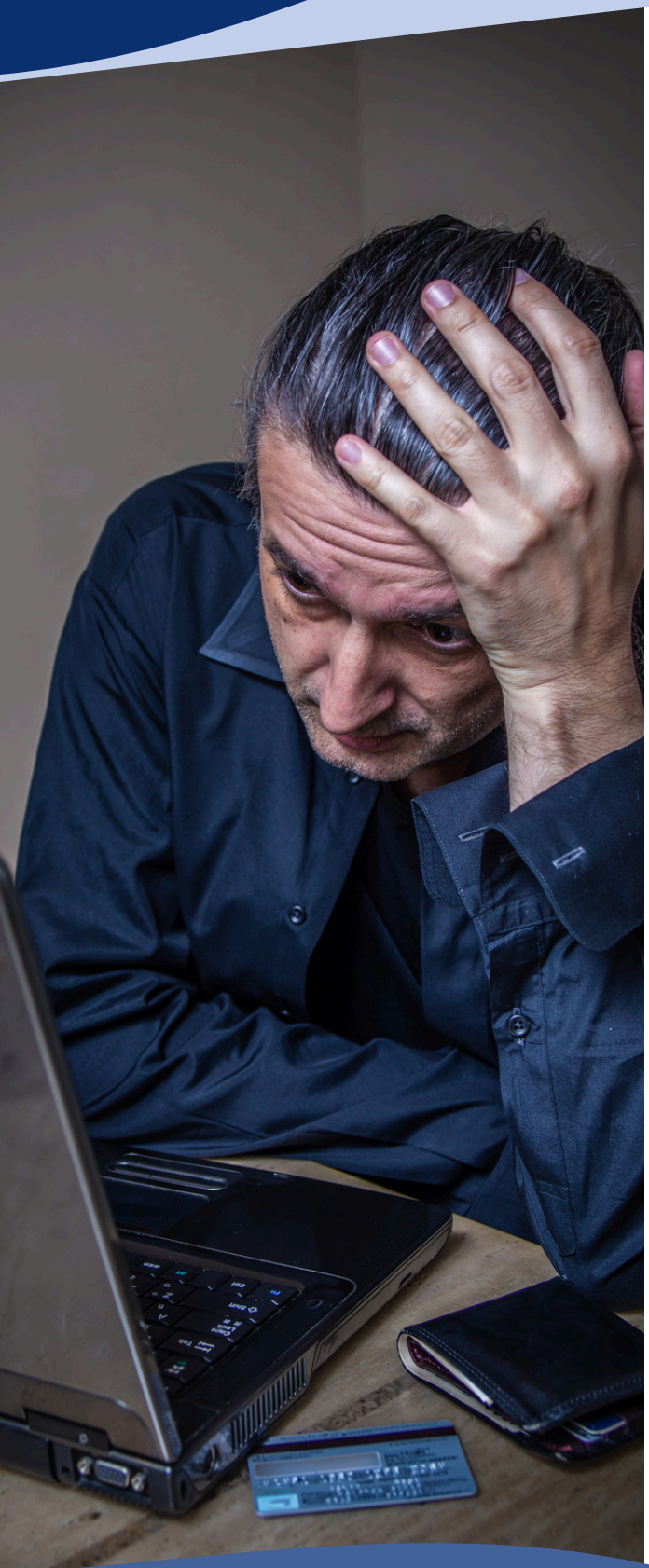


info@mwc.community
www.mwc.community
+1 647-391-9668

Reporting Fraud



- To take action against fraud:
- Visit your nearest Peel Regional Police Division/Community Station to file a Fraud Report. Reports are not taken over the phone.
- For inquiries about fraud and scams, contact the Peel Regional Police non-emergency line, Fraud Bureau 905-453-2121 ext. 3335 https://www.peelpolice.ca/en/who-we-are/contact-us.aspx#fraud
- If you have received an email, text, or call from a scammer and have not provided personal information or lost money, contact the Canadian Anti-Fraud Centre at 1-888-495-8501 or www.antifraudcentre.ca to file a report.



If you are a Victim of Fraud

- Stay calm. Gather all information about the fraud such as documents, receipts, emails, and texts.
- Contact financial institutions.
- If you face identity fraud, place flags on all accounts, change all passwords, and report the fraud to both credit bureaus – Equifax and Trans Union Canada.
- Contact the local police. Get a file number. If you find suspicious activity on your credit report, contact the police to update the file.

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

If you are a Victim of Fraud

- Report the incident to the Canadian Anti-Fraud Centre toll-free at 1-888-495-8501. Depending on the fraud, you may also want to report it to other institutions. Find details here: https://antifraudcentre-centreantifraude.ca/scams-fraudes/victim-victime-eng.htm
- Protect yourself from future fraud. Scammers may target you again. Do not send recovery money to scammers in an attempt to recover from fraud. Share updates with the Canadian Anti-Fraud Centre, police, and financial institutions.
- Share your experience with others. You may prevent future fraud.

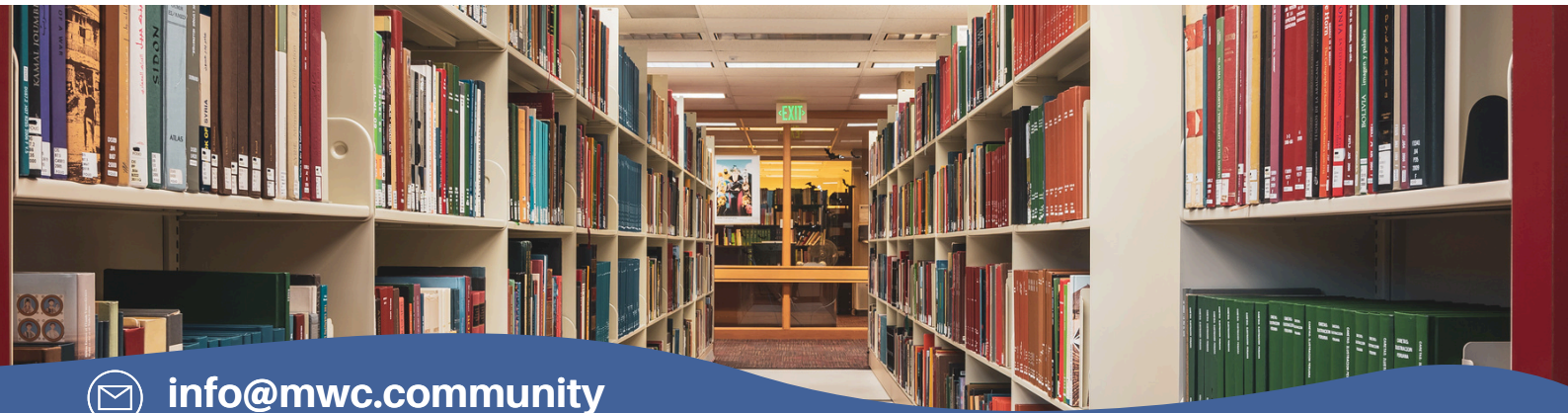
info@mwc.community
www.mwc.community
+1 647-391-9668

Resources

- Canadian Anti-Fraud Centre https://antifraudcentre-centreantifraude.ca/index-eng.htm
- Equifax https://www.equifax.ca/personal/ and TransUnion Canada https://www.transunion.ca/ for credit reports and scores

References

- Peel Police Common Frauds and Scams https://www.peelpolice.ca/en/safety-tips/fraud-and-scams.aspx
- Peel Police Cyber Crime https://www.peelpolice.ca/en/safety-tips/cyber-crime-computer-and-internet-safety.aspx
- Get Cyber Safe. https://www.getcybersafe.gc.ca/en
- Malware https://consumer.ftc.gov/articles/malware-how-protect-against-detect-and-remove-it
- Canadian Anti-Fraud Centre: Victim of Fraud: https://antifraudcentre-centreantifraude.ca/scams-fraudes/victim-victime-eng.htm



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