HALTON REGIONAL POLICE SERVICE

Avoiding Online Frauds and Scams

Smart online usage means taking steps to avoid falling victim to online fraud, which occurs when criminals try to obtain your personal information, such as credit card and account numbers, get you to pay for items that are either non-existent or misrepresented to you and/or steal your identity. It may also include infecting your computer with a virus. The Halton Regional Police Service offers the following safety tips to help keep you and your family safe:

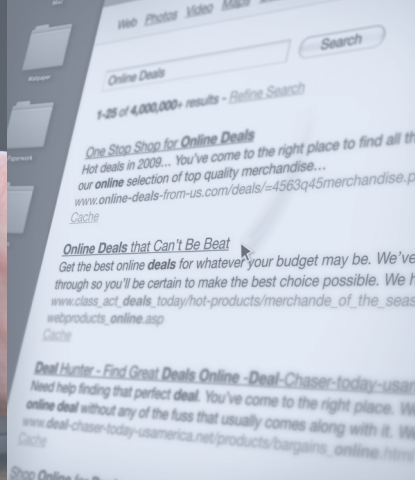
E-mails:

- Do not respond to offers of money, threats of legal action or warnings about "compromised security".
- Be watchful of phishing e-mails that ask for personal or financial information.
- Never provide personal or financial information to anyone in an e-mail.
- Do not click on links in e-mails from senders you don't know. The link may take you to a fraudulent website where you will be asked to enter your passwords or other personal information.
- Be suspicious of e-mail attachments from unknown sources. If you do not know the sender of an e-mail, do not open the attachment. Attachments may contain viruses or malware designed to infiltrate and harm your computer.
- Do not set your e-mail program to "auto-run" attachments. Always run your anti-virus software to check that e-mails you receive do not contain viruses.

Online Passwords:

- Choose unique, yet memorable passwords that you do not have to write down, but that are difficult for others to guess. A combination of letters and numbers is recommended.
- Disable AutoComplete or other memorized password functions that may be available on your computer.
- Do not save passwords on your computer, on the Internet or on any software. Anyone who has access to or compromises the security of that information can potentially impersonate you.
- Never disclose your passwords to anyone, especially online.
- Change your password at least every 90 days, to help protect the security of your information.





E-Commerce:

- Shop only from your home computer and not on public ones. It is much safer.
- Deal only with reputable companies you know and do your research. Legitimate merchants will have easy-to-find information about themselves, their location and contact numbers.
- Don't be pushed or rushed into buying an item, especially by "limited supply" or "limited time" warnings.
- Know what you are paying for and all costs involved. Read the terms and conditions of all contracts before buying.
- Ensure the merchants you deal with online have secure transaction systems (indicated by a padlock symbol at the bottom of your browser) before providing credit card or other sensitive information.
- Consider using a credit card with a low credit limit or single use payment card.
- Always print and save the confirmation page when completing online purchases.
- Monitor all bank statements and activity online. Report discrepancies to your financial institution immediately.
- Never provide your Social Security Number, date of birth or a driver's licence number to a seller.
- Clear your browser's cache after visiting secure sites to ensure nobody else can view any confidential information you may have transmitted.
- Always remember that if it sounds suspicious or too good to be true, it probably is.

Viruses and Malware:

- Always use up-to-date anti-virus and anti-spyware software from a reputable vendor that is capable of scanning files and e-mail messages for malevolent software. Most anti-virus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for them as soon as they are discovered.
- Register new anti-virus and anti-spyware software immediately, and sign up for automatic notification of product updates if available.

Firewalls:

A firewall filters information transmitted through your Internet connection into your computer, permitting communication only with sources you know and trust. It helps prevent unauthorized access, protecting your home network and family from potential hackers and offensive websites.

- Restrict traffic that travels through your firewall by only granting access to those programs and/or traffic that you are familiar with.
- Disable the File Sharing feature if you do not share files or documents with other computers on your network. Doing so will prevent others from being able to download or view your files or documents.

FOR MORE INFORMATION, PLEASE CONTACT:

Halton Regional Police Service
Regional Fraud Unit
905-465-8741
https://www.haltonpolice.ca/about/specializedunits/fraud.php