Internet & Social Media Safety

Older Adult Advisory Committee (OAAC)

2022

What is the Internet?

The internet is an interconnected series of servers and computers spread across the world. This allows instantaneous communication across the entire globe. The good new is, you can quickly get in touch with anyone, either a person or a company. The bad news is, **anything you put on the internet is potentially available to anyone in the world!**

Social Media

What is Social Media?

Social media is the use of internet websites or applications (apps) to help you share personal information, opinions, photos and experiences, and enable you to keep in touch with family and friends.

Some examples of social media include: Skype, Facebook, Instagram, Google+, Twitter, WhatsApp, Pinterest, Tumblr, text and audio messaging, and video calls.

Caution! Do not allow social media to become your main source of information and/or personal contact. The information put on social media represents the posting of a person's unsencored point of view and may or may not be factual. Confirm anything you see or hear using other trusted sources.

Using Social Media

Here are some tips that you can follow to use social media wisely.

Choosing a social media application

- Research with trusted friends and media about their experience with various apps.

Protecting your privacy

- Take time to understand the provider's privacy policy. Ensure you are well-informed about how securely the personal information you provide will be protected.
- Understand and use the privacy settings. Most services have settings that allow you to choose the level of privacy risk you are willing to assume. Some apps also let you choose who will see the information you release.
- Confirm your privacy settings regularly (for example, an application update could alter your privacy settings).
- Exercise caution when accepting a "friend" on social media. Make certain the profile is real and that you know the person you are accepting.
- Consider using a virtual email address (for example, Hotmail or Gmail), instead of an ISP email address (for example, Cogeco, Bell, etc.) for all online activity.

Managing your social media account

- Limit the amount of personal information you provide to an absolute minimum. Once released, personal information cannot be taken back.
- Avoid posting your full birth date and place of birth and be cautious when asked to enter any other personal information, such as your home address.
- If you stop using your account, deactivate it. Don't risk leaving personal information in an inactive account.

Password tips

- Passwords should contain at least eight characters and include numbers, upper and lowercase letters and symbols.
- The more complex the password, the less likely someone will be able to hack your account.
- Change your passwords regularly and store them in a secure location.
- Never share your passwords.
- Never include personal information in your passwords (for example, street address, date of birth, social insurance number, personal financial information, bank account numbers, credit card numbers).

Other tips

- Never disclose your social insurance number, personal financial information, bank account numbers, credit card numbers or related passwords to any social media site or anyone contacting you through social media.
- Never make reference to your address or "living on your own" on social media. Such references could attract unwanted attention or criminal activity.
- Be wary of clicking on a link even if it is passed along by someone you know. Confirm with the person who sent you the link that it is valid.
- Be cautious when posting photos that include license plate numbers or other information that will make it easy to discover where you live. Sometimes this information can be used by identity thieves to answer security questions.
- Avoid posting information about spending time away from your home. Doing so suggests to others that your house will be left unattended.
- Turn off the GPS setting on digital cameras for photos that you will be posting. Embeded photo information may reveal more information that you want.

Social Media Etiquette

Use the social media golden rule: only post about others what you would have them post about you.

- Never post comments when experiencing strong emotions. Assume that whatever you post (comments, photos, images, etc.) will exist forever. Once posted, your words and pictures cannot be erased.

Report Abuse

Report abuse from anyone, including friends, family and caregivers. If you are receiving messages on social media, in emails or text messages, that are threatening, mean, accusatory or abusive, do not respond. Reach out for help from someone you trust, from protective services organizations or law enforcement, and report the behavior to the site or service. All major social media companies and online or mobile service providers have staff that respond to abuse complaints.

Fraud & Scams

Unscrupulous people may try to use the information you put on the internet to steal your money and/or identity. Seemingly harmless things you put on the web can be used for fraud, blackmail, extortion and bullying. The only sure way to avoid this is to **never put any personal information on the internet unless you are absolutely sure you know who is receiving it**.

Common Scams

Below are some of the more common internet scams being used today. For a comprehensive list, please visit https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/azindex-eng.htm.

Air Duct Cleaning

Phone calls offering deeply discounted prices on air duct cleaning or other home improvement services. Once you have paid, you will receive a very poor service or no service at all. The work has to warranty and no standards. You have no recourse at the end. It is generally true that *"you get what you pay for"*.

Emergency Call

Someone purporting to be a relative, such as a grandchild, will tell you they have been in an accident and/or are in jail. They will ask you for money for bail or lawyer fees. They prey on seniors since they tend to be more trusting. They will usually call in the morning when you are less alert.

Delivery Services

Someone calls or emails purporting to be from the large wholesaler or delivery companies such as Amazon, Wayfair, UPS, FedEx, etc. They claim to need more information in order to complete the delivery. You may not even be expecting anything. If they contacted you they must have your information. **Never** given them any additional information.

Canada Revenue Agency (CRA)

A caller claiming to be from the CRA and that you have unpaid taxes, threatening you with fines, penalties and even that a warrant has been issued for your arrest. Remember the government will never call you like this. They have all your information and do not require you to supply anything.

Business Opportunities and Cryptocurrency

They will ask you for an investment so you can get in at the low end of an incredible opportunity with promise of huge returns.

Remember: If something seems too good to be true, it usually is!

Other Possible Dangers

Computer virus or worm

A malicious program that is spread via infected email attachments, downloaded files, or insecure websites. A computer virus can destroy data, other programs or computer hardware. They can also disable security settings and even steal personal information and passwords.

How to protect yourself:

- Install a reputable antivirus program on your computer. Some of the most reputable include TOTALav, Norton, Kaspersky, McAfee, and Bitdefender. These apps are contstantly being kept up-to-date by the supplier.
- Regularly install updates to the antivirus program, if needed.
- Never open an email attachment or click on a website link unless received from a trusted sender.

Spyware and adware

Malicious programs that collect personal data from your computer. Spyware passes the data to an external person. Adware uses the personal data to launch ads (most commonly pop-up ads) on your computer.

The information can be used to gain access to email and social media accounts, bank and credit card accounts and other private, password-protected services.

To protect yourself:

- Install a trusted ad blocker program on your computer.
- Never download “free” programs or games unless you are certain that you can trust the source.

Wi-Fi eavesdropping

This occurs when another individual monitors the data exchanged over the wireless network you are using.

To protect yourself:

- Never exchange personal or financial information using “free” Wi-Fi.
- Never use a shared or public computer to access websites that require login passwords and other personal data.
- Secure your personal Wi-Fi network by using a complex login password. For extra security, change your login password regularly.

Unsolicited help

People call to say they have detected issues with your device, offering to fix it if you grant them remote access to your device. Never allow remote access. This gives access to all information stored on your computer.

Protect Your Data

- A web address may begin with the letters HTTP or HTTPS. If the website begins with HTTPS, it is using secure coding to keep your personal information safe.
- Use complex passwords that would be difficult for someone else to replicate. Do not put personal information in your passwords (for example, names, phone numbers, addresses, etc.).
- Regularly update the operating system for your computer. These updates often include program changes to prevent unwanted access to your computer. Beware that updates will often change your settings back to a default.
- Regularly check the network security of your computer to ensure it has not been changed by malicious access to your computer.
- Regularly change the password for financial institutions, shopping websites and other websites that have your personal information on file.
- Some services give you a choice between private and public posts. Only people who you designate or accept, such as your “friends” or “followers” are able to see posts that are private.
- Confirm your privacy settings regularly as applications commonly alter their privacy settings.

Telephone Safety

All of the information in this fact sheet applies to telephone communication as well as tablets, cellphones and computers. Remember to take everything with a grain of salt – sometimes we are too trusting and that can be used against us. The best thing to do, if you can, is to consult with a trusted source before making decisions online and **never allow yourself to be rushed**.

Reporting Potential Cyber Crimes

If you know of a potential cyber crime or feel someone has attempted to defraud you, you should report this to the authorities. This will serve the purpose of not only protecting you personally but also allowing police to amass data on crime trends to help others and organize responses to fight these crimes.

The first point of contect for reporting should be the Halton Regional Police Service. They will direct your report to the appropriate place.

Halton Regional Police Service: 905-825-4777

Police have special units at the municipal, regional, provincial and federal levels to deal with this rapidly growing threat to public safety.

References

The **Canadian Anti-Fraud Centre** gathers information on frauds and scams across the country. You can report potential frauds to them directly by calling 1-888-495-8501.

www.antifraudcentre.ca

The Little Black Book of Scams

www.competitionbureau.gc.ca

RCMP Cybercrime and Fraud Reporting System

https://www.rcmp-grc.gc.ca/en/new-cybercrime-and-fraud-reporting-system

Financial Consumer Agency of Canada

www.fcac.gc.ca

Get Cyber Safe Canada

www.getcybersafe.gc.ca