TELUS Wise seniors

Helping Canadian seniors navigate their digital world.

telus.com/wise

TELUS®

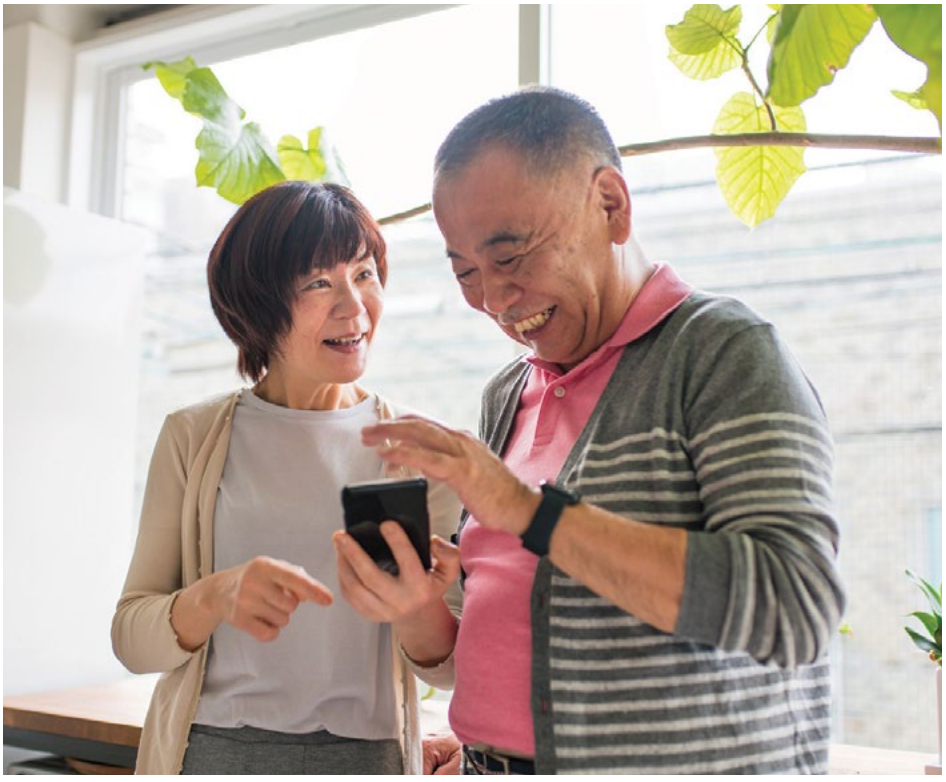
Contents

Introduction

This guide was created for Canadian seniors who are already using the Internet and want to learn more about participating in our digital society safely. The guide can be used as a personal reference and is also used as the basis for TELUS Wise® seniors workshops.

If you are interested in booking a free-of-charge TELUS Wise seniors workshop for your community group or have questions about the contents of this guide, please contact **wise@telus.com.**

For additional resources to help you safely navigate our digital world, visit **telus.com/wise**.



You may be more connected than you think.

Take a few minutes to think about how active you are online by answering the questions below.

Do you use any of these?

Email ☐ **Yes** ☐ **No**

Twitter ☐ **Yes** ☐ **No**

Facebook ☐ **Yes** ☐ **No**

Instagram ☐ **Yes** ☐ **No**

YouTube ☐ **Yes** ☐ **No**

Do you send **text messages?** ☐ **Yes** ☐ **No**

Do you **download apps?** ☐ **Yes** ☐ **No**

Do you **bank online?** ☐ **Yes** ☐ **No**

Do you **shop online?** ☐ **Yes** ☐ **No**

Do you **share photos online?** ☐ **Yes** ☐ **No**

Do you **enter contests online?** ☐ **Yes** ☐ **No**

Do you play **games online?** ☐ **Yes** ☐ **No**

Do you use the **Internet for research?** ☐ **Yes** ☐ **No**

What else do you do online? _____

_____

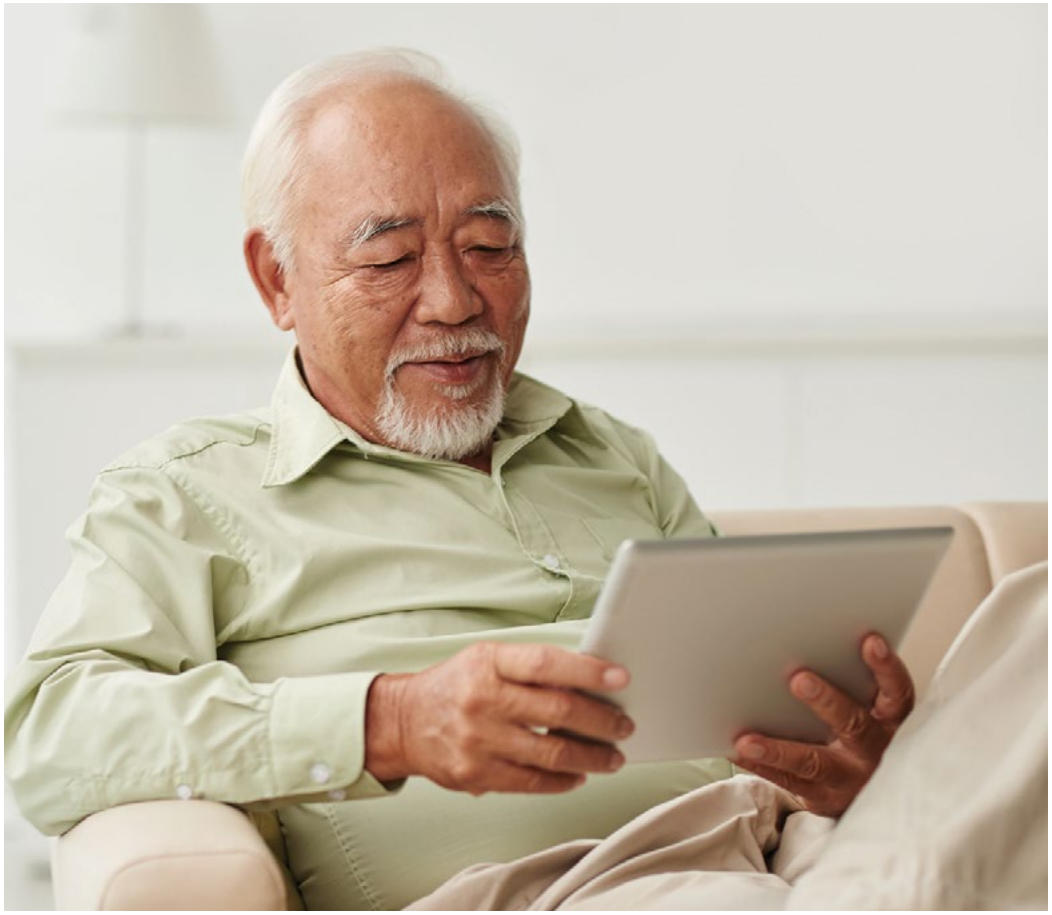
_____

_____

_____

Through this exercise, you may have discovered that you are more connected than you initially thought. But even if you only have an email account or do general web surfing, you are still a member of our growing digital society.

This guide offers safety tips to help protect your security and privacy online.



Notes

Internet safety tips

1. Setting strong passwords

A strong password can stop someone from hacking into your email, social networking accounts, etc. Passwords should be least **eight characters long and include numbers, letters and symbols.**

You can make your password stronger by using a **passphrase or the first letters of the phrase, instead of a word**. For example: “I can always remember my password 2*” or more simply ICARMP2*

Two-factor authentication (2FA): this account security feature requires you to authenticate yourself with something in addition to your username and password, such as a unique code that is sent to your device by text or a biometric verification like a fingerprint. **It is recommend you enable 2FA for optimal security for all of your online accounts**.

Do not use the same password for your computer, smartphone, email and all of your apps (e.g. online banking, Facebook). This is a jackpot for hackers!

According to SplashData **the top 6 worst passwords for 2018** were:

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111

2. Software upgrades

It is important to accept software upgrades, which include security patches, to protect your smartphone, tablet or computer from viruses. **Install these updates as soon as they are available to minimize your risk.**

For smartphones, the manufacturers (e.g. Apple and Android) will offer their own programs to update software and all have software managers that tell you if there is a new version of software available for your device or an app on your device. Software upgrades are found in the settings app, e.g. Apple ( ) and Android ( ).

Similarly, on your computer, all your software updates should come directly from the manufacturer of the software.

Notes

Protecting yourself from illegitimate software update requests.

Fraudulent software updates can cause a lot of damage if you click on them. Always remember to stop, take a close look, and **when in doubt — do not download or click**.

- Don't respond to software update requests when using **public Wi-Fi**.
- Only download updates directly from the software **manufacturer's website** (e.g. Microsoft, Apple).
- **Never click on links in emails that tell you to upgrade your software**. If you are unsure whether a link is legitimate, hover over it to see the destination address. If the website is not recognizable do not click.

- Review software update requests carefully, especially if they seem to have appeared out of nowhere or come from an unknown sender. Also look for **poor grammar and typos**.
- Set your computer/smartphone to **automatically update** your operating system and apps when updates become available.

Notes

3. Creating a Google alert

Create a Google Alert at **google.com/alerts** for your first and last name so you are notified via email if and when your name appears online. You can refine the search by adding the province or city where you live.

While this isn't a 100% guarantee, it is a good start to tracking your digital footprint and can help provide early warnings about identity theft.

To learn more about Google alerts, visit **https://goo.gl/Kh01N4**

4. Keeping your browser in check

The web browser you use (e.g. Internet Explorer, Firefox, Google Chrome, Safari) is your gateway to the Internet and the first point of defence against malicious activity. **Always use the latest version of the browser** and configure the browser settings with your security and privacy in mind. You can also use your browser in incognito or private mode for additional privacy.

It is also recommended that you clear your browser history and cache at least once a month.

Search Google.com for instructions specific to your browser (e.g. “how to delete browser history in Internet Explorer”).

Notes

5. Sharing personal information online

Always limit the amount of personal information you share about yourself online. This will help protect your privacy and reduce your susceptibility to identity theft or fraud.

Think twice before posting the following personal information on a public forum (e.g. social media profile):

- Contact information (e.g. phone number, email address)
- Full name and date of birth
- Home address
- Full names of your children or family members
- Dates and details of trips, vacations and time spent away from home

Think twice about participating in online social media quizzes, too. The information you share about yourself through these quizzes may reveal answers to security questions for your online accounts.

Before sharing any information online, always ask yourself:

1. How will my information be used?
2. Why is this information needed?
3. Who will have access to my information?
4. How will my personal information be safeguarded?

Notes

6. Thinking before you click

- **Never click on suspicious links or email attachments** even if they look interesting. A lot of scams and malware are spread through links, attachments and rogue apps.
- **Do not respond to emails that request personal or financial information,** especially those that use pressure tactics or prey on fear.
- Legitimate service providers like TELUS, the Canada Revenue Agency, banks, etc. **will not ask you to provide or verify sensitive information through non-secure means** such as email.
- Apple, Microsoft and other reputable companies **will never call to tell you that there is something wrong with your computer** or device. Do not agree to visit a website given to you by a caller to help you fix your computer — this is a scam!
- **If something seems too good to be true, it probably is!** If you receive a suspicious email offer, call your service provider or financial institution directly to verify the offer or request for account information. **Never dial the number found within the offer email**.

TELUS Wise tip: create an email account for things like social media, online games, contests, mailing lists, etc., and maintain a separate email account for more professional uses such as online banking, booking travel, communicating with friends and family, etc.

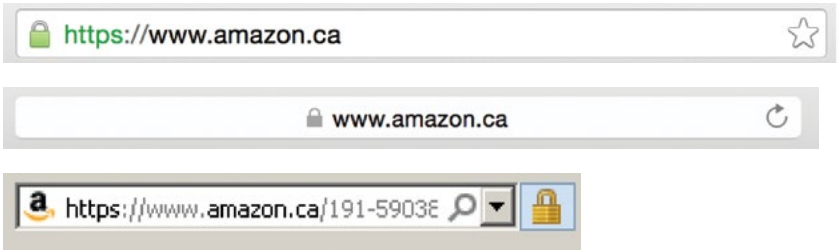
Notes

7. Shopping online

Use reputable websites for online shopping, and check with friends, family or read online references (not affiliated with the site) to get a feeling for reputability.

Ensure the website where you're shopping uses encryption. Look for the "s" in the **http** at the beginning of the address bar, and the **lock symbol** – this indicates that the website uses encryption to protect your payment information.

By way of example, see the Amazon.ca web address below. It starts with **https://** and also has a lock identified in the web address bar.



Always **decline the option to save your credit card information** for future purchases. While it may provide some convenience for your next purchase, your saved data is at risk if the organization is breached.

8. Taking and sharing photos

Many of us love to take pictures and share them online with family and friends, but there are privacy and safety concerns to consider.

If you share pictures online:

- **Ask for permission before posting pictures of other people.** This extends to grandchildren and children in your life – make sure you have the parents' approval before you post or share a picture online with a child in it.
- **Think about your audience.** Adjust social media privacy settings to limit your audience to only those who you are comfortable seeing your photos. Alternatively, use a reputable cloud storage service to store your pictures, and set up folders to share with specific people directly.

TELUS Wise tip: be selective about which apps you grant access to your camera roll. Always read the terms and conditions to understand how your photos will be used.

Notes

Smartphone safety tips

1. Turning off geo-tagging

While most social media sites strip photos of geo-tagging or location data, keep in mind that location details are still attached to images that are shared via email or text message.

You can **turn off geo-tagging** on your device if you do not want your location information to be captured with your images. Search Google.com to for instructions specific to your device (e.g. “how to turn off geo-tagging on an iPhone”).

2. Setting up remote locate/lock/ wipe services

Use these built-in services to **lock your smartphone, track its whereabouts, or remotely erase the information on your device if it is lost or stolen**. These services also allow you to remotely post a message on the smartphone’s screen advising how you can be contacted if your phone is found, or make your device play a sound if you have simply misplaced it nearby.

On Apple devices, the service is called **Find My iPhone**, whereas on most Androids it's called **Find My Device**. You can set up these services in your device Settings.

3. Being careful when using free public Wi-Fi

Hackers can access other users' personal information over public Wi-Fi (e.g. at a coffee shop). There are some steps you can take to minimize the risk:

- **Always confirm the Wi-Fi network before connecting to it** – do not rely only on the name of the network. If there are multiple Wi-Fi networks listed for the same venue, ask a staff member which one to use. Similarly, be sure to read the venue's Terms of Service so you know what you're agreeing to before connecting.
- Only use public Wi-Fi to **browse websites that do not require login credentials** (e.g. general web sites for browsing). If you need to access sensitive data or enter login credentials when using public Wi-Fi only go to websites that start with https (see page 10 for more info on secure websites).
- **Never install or update software while using public Wi-Fi** as it could introduce malware into your computer. For example, a common attack is to inform the user that their browser is using outdated software and then redirect the user to a fake website that will install a virus.

Notes

4. Wiping your phone before recycling it or giving it away

Technology is advancing at an amazing pace and many people frequently upgrade their smartphones.

Have you ever thought about what happens to your old device when you dispose of it? More importantly, what happens to all of the private information that's stored within it such as contact information, passwords, photos, and more?

Before you dispose of any mobile device, ensure that you wipe all information.

For help with disposing of your mobile device safely, visit a TELUS Learning Centre. Find one near you at **telus.com/learningcentre.**

5. GPS

Manage location settings on your apps by understanding which apps need to know your location. Ask yourself, does Facebook or Twitter need to know my location in order to work properly?

Turn off GPS (or location settings) and Bluetooth features when you are not using them. This will help protect your privacy and save battery power!

You will find GPS/location and Bluetooth in the Settings section on your smartphone.

Social media safety tips

Notes

1. Keeping an eye on your privacy and permission settings

Always read the privacy and permission settings when signing up for a new social media account or downloading a new app - don't accept the terms blindly.

- **Permission settings** control what personal information can and cannot be accessed and shared about you by a social networking site or mobile app. (e.g. your contact lists, photos, location, etc.)
- **Privacy settings** control who can and cannot see your profile and posts online (e.g. is your profile visible to only your friends list, or also visible to the general public).

2. Thinking twice before connecting

It's a good rule of thumb to **only connect and share with people online that you know in real life**. By "friending" people online who are strangers, you open yourself up to privacy and security risks, scams and more. Also, **be careful what you post online**. For example, posting a picture of yourself while on vacation may inform others that your house is empty.

Did you know? Facebook estimates that 1% of their 2.38 billion monthly active users are fake accounts, potentially created by spammers.

Notes

3. Choosing apps carefully

Only purchase and download apps directly from your smartphone's app store. Before downloading an app, read reviews and do a search to make sure it's legitimate.

4. Logging off

Don't leave social media accounts logged in if you are not using them. If you do not log off, you can become vulnerable to security and privacy risks.

Also, you should always **unsubscribe from and deactivate accounts and apps that you are no longer using.** Dormant accounts can be hacked and this can compromise your identity.

Think about this – a dormant Facebook account of a Calgary teen was once hacked and used to lure teens over the Internet.

5. Keeping your digital household clean

Set time in your calendar every three to six months to check your privacy and permission settings, change passwords, review and verify your friends lists, and deactivate accounts you no longer use.

Protecting yourself from identity theft

Notes

In our digital world, we are at an increased risk of having our personal information stolen and used for criminal purposes, like identity theft and fraud, and should take precautions to protect ourselves.

- **Identity theft** refers to acquiring and collecting someone else's personal information for criminal purposes.
- **Identity fraud** is the actual deceptive use of someone's identity.

What is the potential impact on victims of identity theft and identity fraud?

- Damage to credit score
- Refusal of credit (mortgages, loans)
- Assumed identity (criminal records)

What information do cyber criminals look for?

- Full name
- Date of birth
- Social insurance number
- Full home address
- Mother's maiden name
- Usernames and passwords
- Driver's license number
- Bank account numbers
- Personal identification numbers (PIN)
- Credit card information
- Signature
- Passport number

Notes

1. Common identity theft scams

- **Phishing emails/text messages:** an attempt to access private information by sending illegitimate emails/messages that appear to be from reputable organizations. The intent is to trick recipients into clicking on links or replying to the email and providing personal information.
- **Pharming:** the act of redirecting someone from a legitimate website to a fraudulent site where your information is not secure and at risk of being used for illicit purposes.
- **Formjacking** is a term used to describe a scam where the information you submit in an online form (credit card and other personal information) is intercepted between your device and the website you are using.

Email scams are becoming increasingly common and more sophisticated. Watch this TELUS Wise video on how to spot common email scams.
https://bit.ly/2yS9MMu

2. Signs of identity theft

Many victims of identity theft don't realize they have had their identity stolen, and may only find out when they're denied credit despite having a good credit history.

Below are signs to watch for:

- Unfamiliar charges and transactions on your bank and credit card statements.
- Notifications from your financial institution about changes to your account.
- You stop receiving mail and statements that you usually get or you start receiving new statements for accounts you don't have.
- Calls from creditors about accounts and loans you don't have.
- Mysterious activities on your credit report, such as credit inquiries or requests for new accounts.

Notes

3. Limit your risk for identity theft with these tips.

- Use **strong passwords and two-factor authentication**. Don't share passwords, change them often, and don't use the same password for all your accounts.
- Set up a **separate email address for financial matters**.
- **Wipe your device** before selling or recycling it.
- **Scrutinize unsolicited emails** that ask you to provide or validate personal information. Be wary of emails (and calls) that suggest you've won a prize or request financial help.
- **Limit the personal and private information you share online**.
- Always check to **ensure you're on a secure website** before providing banking or payment information.
- Limit your online activities to **browsing when using a public Wi-Fi connection**.
- Set up a **Google Alert** for your name.

Additional steps to **protect your identity offline** include:

- Emptying your mailbox regularly.
- Protecting your banking PIN, ensuring nobody is watching you enter it at an ATM or while shopping.
- Shredding any documents which contain personal information when you no longer need them.

4. What to do if you are a victim of identity theft or fraud

Step 1: Contact your local police force and file a report.

Step 2: Contact your bank/financial institution and credit card company to make a report.

Step 3: Contact the two national credit bureaus to request a copy of your credit reports and place a fraud warning on your file:

- Equifax Canada Toll free: 1-800-465-7166
- TransUnion Canada Toll free: 1-877-525-3823

Step 4: Report the theft or fraud to your local police and notify the Canadian Anti-Fraud Centre at 1-888-495-8501
antifraudcentre-centreantifraude.ca

Additional information can be found on the RCMP's website (**http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm**)

Notes

Online dating

Canadian seniors are increasingly looking for companionship or even a new life partner through online dating websites and apps. While this may not be the case for all single seniors, those who are looking for love online should be aware of common romance scams, and be extra vigilant in protecting their privacy and security.

1. Create a separate email account

Similar to the tip shared previously about creating a different email account for social media, games, etc., it is recommended you use this email account when signing up for a dating website.

2. Choose an appropriate website

A lot of the traditional dating websites like **eHarmony**, are now catering to the over 55 demographic. There are also specific dating websites designed for seniors, such as **Senior Friend Finder**, **Senior Match** and **Senior People Meet**.

3. Research the websites' terms and conditions

Read the fine print before signing up. If you have a free trial, put a reminder in your calendar when the trial expires so you can decide if you wish to continue your subscription. Sometimes free trials auto-renew and you may incur unexpected expenses.

4. Create an engaging profile

Honesty is the best policy. Make sure your profile is up to date and accurate; however, be careful not to include too much personal information, like your exact date of birth.

5. Be cautious if you plan to meet

If you meet someone online and decide to meet in person, always arrange to meet in a public area. Remember, you haven't really met them yet and can't be 100% sure who they really are, so you need to be mindful of risks. Always listen to your gut.

6. Look out for romance scams

Below are some tell-tale signs that you're being romanced by a scammer:

- they claim they live near you, but are currently overseas
- they cancel plans to video chat or meet in person
- they profess their love early on before they've met you face-to-face
- they ask for you to send money to help them with an emergency situation or to cover their travel expenses to come and see you

Never send money, under any circumstances, to someone you've connected with online.

According to the Canadian Anti-Fraud Centre, romance scams cost Canadians more than $22 million in reported losses in 2018.

Notes

Social gaming tips

Online games that allow social interaction between players are becoming increasingly popular.

1. Think carefully before sharing your contact or friends list with the app.

Often times, app/game developers will request access to your friends lists in order for you to play the game. In addition, the terms and conditions may authorize the developers to send gaming-related messages to all of your contacts.

2. Chat with caution.

When gaming online, you may have the opportunity to chat with other gamers from all over the world. Beware of creating friendships online and sharing personal information, and think carefully about who you are talking to - the person on the other side of the screen may not be exactly who you think. Generally, it's best to only chat with people you know in real life.

3. Be mindful of screen time.

Because social games can be played on the go, you may find you are playing them regularly and for extended periods of time. To ensure online games form part of a healthy and balanced relationship with technology, it's important to take breaks and balance screen time with offline activities.

Notes

4. Be aware of cyberbullying.

While most have a positive social gaming experience, it's good to know what to do if things go wrong. Unfortunately, because of the social nature of many online games, cyberbullying can occur. If harassment does happen, report this behaviour to the social network and block the user.

Below are some additional tips to consider:

1. Be careful what you click on. Things you buy in apps or on gaming sites can cost **real money!**
2. Be aware of **advertising**. Some 'advergames' are designed to promote and sell a product.

My action plan

List 1-3 things you will start doing differently after today's workshop.

-
-
-

TELUS Learning Centre

Get hands-on support with your mobile devices.

TELUS Learning Centre® representatives can show you everything you need to know about your smartphone or tablet. Book a complimentary one-on-one meeting at a TELUS Learning Centre. Find a location near you at **telus.com/learningcentre**.

Learn more about staying safe in our digital world.

- Book a TELUS Wise workshop at **telus.com/wise**.
- Email us a **wise@telus.com**
- Join the conversation online with **#TELUSWise**

TELUS®