



TELUS Wise seniors

Empowering you to stay safe
in our digital world.



telus.com/wise

Contents

Introduction	1	Social media safety tips	20
Protecting yourself from scams and identity theft	2	1. Keeping an eye on your privacy and permission settings.....	20
1. Common scams	3	2. Thinking twice before connecting.....	20
2. Signs of identity theft.....	5	3. Logging off	21
3. Limit your risk with these tips	6	4. Keeping your digital household clean	21
4. What to do if you're a victim	7	Online dating	22
Internet safety tips	8	1. Creating a separate email account	22
1. Setting strong passwords	8	2. Choosing an appropriate website.....	22
2. Software upgrades.....	10	3. Researching a website's terms and conditions	23
3. Illegitimate software update requests	11	4. Looking out for romance scams....	23
4. Keeping your browser in check	12	Social gaming tips	24
5. Sharing personal information online	13	1. Thinking carefully before sharing your contact or friends list with an app	24
6. Thinking before you click.....	14	2. Chatting with caution	24
7. Shopping online.....	15	3. Being mindful of screen time.....	24
8. Taking and sharing photos.....	16	4. Being aware of cyberbullying	25
Smartphone and tablet safety tips	17		
1. Setting up remote locate/lock/wipe services	17		
2. Being careful when using free public Wi-Fi.....	17		
3. Wiping your phone before recycling it or giving it away	18		
4. Managing location services settings	18		
5. Choosing apps carefully	19		
6. Turning off geo-tagging	19		





Introduction

This guide was created for seniors who are already using the internet and want to learn more about participating in our digital society safely.

Are you new to using digital technology?

Check out telus.com/WiseOnlineBasics.

Developed in partnership with MediaSmarts, TELUS Wise online basics helps people who are just getting started with digital technology to learn basic, everyday digital skills. This free video series, designed for seniors, newcomers and non-digital natives, covers topics including how to connect to

the internet, use a search engine, keep yourself safe using social media and more.

If you're interested in booking a free-of-charge TELUS Wise seniors workshop for your community group or additional resources to help you stay safe in our digital world, visit telus.com/wise.

Throughout this guide, you'll see a series of QR codes like the one below.

QR codes give you quick access to websites without having to type or remember a web address. You can use the Camera app on your phone to scan a QR code.

1. Open the Camera app from the Home Screen, Control Center or Lock Screen.
2. Select the rear-facing camera. Hold your device so that the QR code appears in the viewfinder in the Camera app. Your device will recognize the QR code and show a notification indicating where the QR code points to.
3. Tap the notification to open the link associated with the QR code.



**Try it for
yourself!**



Protecting yourself from scams and identity theft

In our digital world, we're 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 and loans)
- Assumed identity (criminal records)

What information do cyber criminals look for?

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

1 Common scams

Scammers and fraudsters are becoming more opportunistic. Here are the top scams to watch for:

Romance: Romance scammers establish a virtual relationship, offer abundant attention and affection, gain trust and then ask for money or ask you to receive money on their behalf and then send it to them. Even though it may seem far-fetched, romance scams are real and many fall prey to them.

Cryptocurrency: Fraudsters, often impersonating an investment professional, will offer you cryptocurrency buy-ins, promising a high rate of return in a short amount of time. Before investing in crypto or sending anyone money online, do your research and remember that once you've sent money online, it's hard to get it back.

Fake social media accounts: Fake social media accounts are used by scammers to imitate people (or organizations) for their personal gain. For instance, they may copy someone's profile picture, create a new Facebook or Instagram account, and begin sending messages or bad links under the cover of someone else.

Phishing (email) and smishing (text): With this scam, you receive an email or text from what appears to be a reputable or recognizable company asking you to click on a link (which is malicious and often installs a virus/malware on your device) and/or provides them with personal or financial information. These messages are becoming trickier to spot.

Did you know?

If you receive a smishing text, you can report the text by forwarding the message to **7726** with the word **"SPAM"** in the body of the message.

Extortion: This is where a scammer unlawfully obtains money, property or services through coercion.

Spoofing: Spoofing is when scammers try to obtain personal information by pretending to be a legitimate business or another known trusted source.

Emergency grandparent scam: This occurs when a senior receives a phone call from someone who impersonates their grandchild in order to gain credibility with the victim. The caller will claim to be in trouble and request money right away from the victim.

Phone scams: Scammers call posing as financial services companies, phone companies, insurance providers, or to offer tech support, immigration or other services. Their goal is to obtain your personal financial information and/or secure payment for services that go undelivered.

Social insurance number: Fraudsters allegedly calling from government agencies alert potential victims that their SIN has been blocked, compromised or suspended. They then ask for personal information to remediate the issue.

Email scams are becoming increasingly common and more sophisticated. Watch this TELUS Wise video on how to spot common email scams.

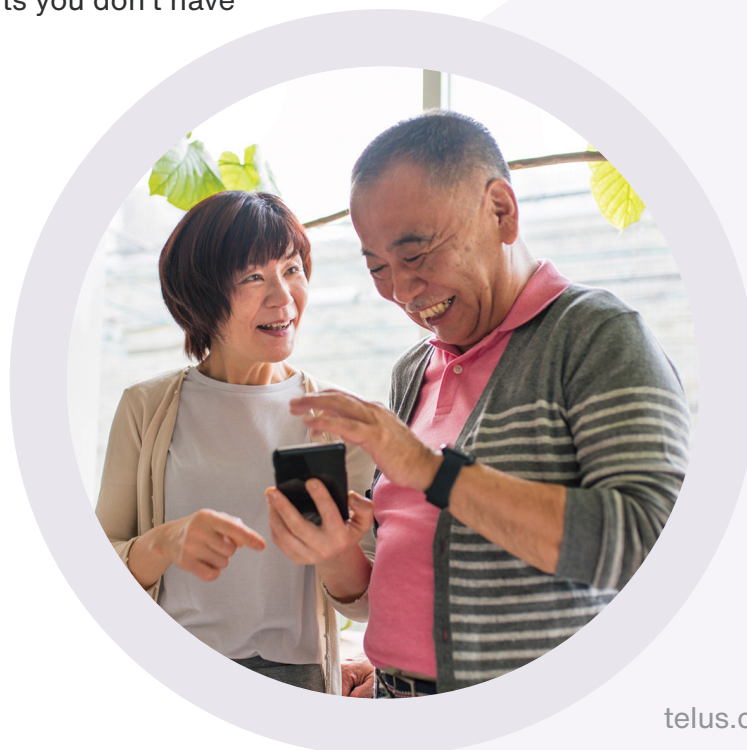


2 Signs of identity theft

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

Watch for these signs:

- 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



3 Limit your risk 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.
- Limit the personal and private information you share online.
- 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.
- 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.

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 with personal information when you no longer need them.

4 What to do if you're a victim

- Step 1:** Contact your local police force and file a report.
- Step 2:** Contact your 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 on scams, and what to do if you're a victim can be found on the Canadian Anti-Fraud Centre website:
antifraudcentre-centreantifraude.ca



To learn more, visit
telus.com/WiseOnlineBasics
and watch episode 11: Keeping yourself safe: Avoiding online scams.





Internet safety tips

1 Setting strong passwords

A strong password can stop someone from hacking into your email, social media and other accounts. Passwords should be at least **12 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: “Ican’trememberwhereIputmykeys yesterdaybutIremember2day!” or more simply ICRWIPMKYBIR2D!

Two-factor (2FA) and multi-factor (MFA) authentication: This account security feature requires you to authenticate 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’s recommended that you enable 2FA/MFA for optimal security for all of your online accounts.**

Don't use the same password for your computer, smartphone, email and all of your apps (e.g. online banking and Facebook). **This is a jackpot for hackers.**

According to Cybernews, **the top 6 worst passwords in 2023** were:



- password
- 123456
- 123456789
- 12345
- qwerty
- qwerty123

To learn more, visit
telus.com/WiseOnlineBasics and watch
episode 9: Keeping your devices and
accounts safe: PINs and passwords.



2 Software upgrades

It's 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're 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 on your Apple () and Android () devices.

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



3 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 — don't 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, Google and Apple).
- **Never click on links in emails that tell you to upgrade your software.** If you're unsure whether a link is legitimate, hover over it to see the destination address. If the website is not recognizable, don't 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 or smartphone to **automatically update** your operating system and apps when updates become available.



Did you know?
TELUS offers
Online Security with
all-in-one protection.



4 Keeping your browser in check

The web browser you use (e.g. Edge, Firefox, Chrome and 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.

Extensions and browser hygiene

Browser extensions add functionality to your browser (e.g. spelling or grammar checking extensions) and require you to download software. Often, extensions can be malicious or put your privacy at risk. To protect your safety, you may wish to avoid extensions. If you're going to download one, make sure it's coming from a reputable source, check reviews and take the time to research what information the extension will gather from your browser.

It's 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 Chrome").

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 identity theft and fraud risk.

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

- Contact information
(e.g. phone number and 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?

6 Thinking before you click

- **Never click on suspicious links or email attachments** even if they look interesting. Several scams and malware are spread through links, attachments and rogue apps.
- **Don't respond to emails that request personal or financial information**, especially those that use pressure tactics or prey on fear.
- Legitimate service providers like TELUS, Canada Revenue Agency and financial institutions. **won't ask you to provide or verify sensitive information through non-secure means such as email.**
- Apple, Microsoft, Google and other reputable companies **will never call to tell you that there is something wrong with your computer** or device. Don't 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 and newsletters, and maintain a separate email account for more professional uses, such as online banking, booking travel and communicating with friends and family.

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 uses encryption. Look for a tune or padlock icon in the address bar and click to view site information to ensure the connection is secure.



telus.com/en/wise

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 experiences a data breach.

To learn more, visit
telus.com/WiseOnlineBasics
and watch episode 20:
Shopping online.



8 Taking and sharing photos

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're 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 the apps you grant access to your camera roll. Always read the terms and conditions to understand how your photos will be used.





Smartphone and tablet safety tips

1 Setting up remote locate/lock/wipe services

Use these built-in services to **lock your device, track its whereabouts or remotely erase the information on your device if it's lost or stolen**. These services also allow you to remotely post a message on the device's screen, advising how you can be contacted if your device 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**, whereas on most Androids it's called **Find My Device**. You can set up these services in your device settings.

2 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** – don't 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 don't require login credentials** (e.g. general websites for browsing).
- **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.

3 Wiping your device 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 and photos?

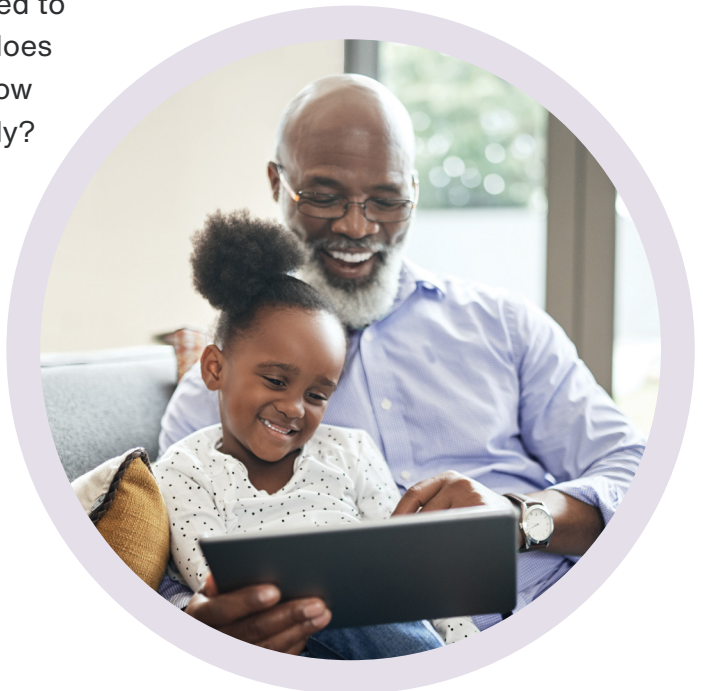
Before you dispose of any mobile device, ensure that you wipe all information by performing a factory reset on your device.

4 Managing location services settings

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

Turn off location services and Bluetooth features when you're not using them. This will help protect your privacy and save battery power.

You can find location services and Bluetooth in the settings section on your smartphone.



5 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.

To learn more, visit
telus.com/WiseOnlineBasics
and watch episode 10:
Downloading and installing apps.



6 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 don't want your location information to be captured with your images. Search Google.com for instructions specific to your device (e.g. "how to turn off geo-tagging on an iPhone").

TELUS Wise tip:

Before posting any photos or videos online, review them to ensure they don't inadvertently share private information such as street signs that may reveal your location or school signs that might reveal where your grandchild goes to school.



Social media safety tips

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 can't be accessed and shared about you by a social networking site or mobile app (e.g. your contact lists, photos and location).
- **Privacy settings** control who can and can't see your profile and posts (e.g. is your profile visible to only your friends 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 1.3 billion active users are fake accounts, potentially created by spammers.

3 Logging off

Remember to log off social media sites when you're done. If you don't log off, you can become vulnerable to security and privacy risks.

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

4 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.

To learn more, visit telus.com/WiseOnlineBasics and watch:

Keeping your devices safe:

- Episode 11: Avoiding online scams
- Episode 12: Managing your digital footprint
- Episode 13: Privacy on social networks
- Episode 14: Social media privacy settings
- Episode 15: Making good privacy choices
- Episode 16: Fixing privacy settings





Online dating

Seniors are increasingly looking for companionship or even a new life partner through online dating websites and apps. 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 Creating a separate email account

Similar to the tip shared previously about creating a different email account for social media, games, etc. It's recommended you use another email account when signing up for a dating website.

2 Choosing an appropriate website

Several traditional dating websites like eHarmony are now catering to the over 55 demographic. There are also specific dating websites designed for seniors, such as Silver Singles.



3 Researching 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 Looking out for romance scams

Below are some telltale 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 and be cautious if you plan to meet in person.

According to the Canadian Anti-Fraud Centre, romance scams cost Canadians more than \$59 million in reported losses in 2022.



Social gaming tips

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

1 Thinking carefully before sharing your contact or friends list with an app

Oftentimes, app or 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 your contacts.

2 Chatting with caution

Many games offer 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're 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 Being mindful of screen 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.

4 Being aware of cyberbullying

While most people have a positive social gaming experience, it's good to know what to do if things go wrong. If you're being harassed or cyberbullied online, report this behaviour to the social network and block the user.

Additionally:

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



Notes

Notes

Notes

Caring for seniors across Canada

At TELUS, we're working hard to ensure everyone has access to world-leading technology and healthcare through our **Connecting for Good®** programs.

Tech for Good

Helping to ensure the digital space is inclusive for all people, Tech for Good offers people with disabilities specialized training and support, including assistive technology in some cases, to empower them to independently use their smartphone or tablet.

Mobility for Good®, Internet for Good® and Health for Good™

If you're a low-income senior, you may be eligible for these additional

Connecting for Good programs:

Mobility for Good

- \$25/month (plus taxes) 5 GB of high-speed data
- \$35/month (plus taxes) 15 GB of high-speed data
- **Plans include:**
 - Unlimited data at reduced speeds
 - Unlimited Canada-wide talk & text
 - Choice of a free certified pre-owned device on a 2-year term or Bring Your Own Device. Alternatively, you can get a \$75 discount on the purchase of a phone of your choice from

Mobile Klinik.

Internet for Good

- Starting at \$10/month (plus taxes) in British Columbia, Alberta and some areas of Quebec
- Option to purchase a low-cost refurbished computer (no contract or cancellation fees)

Health for Good Medical Alert

- Live more confidently knowing that you're connected to 24/7 access to emergency support at the push of a button. Starting at \$10/month

Learn more about
**Connecting for
Good®** programs.





Learn more about staying
safe in our digital world.



- Book a TELUS Wise workshop at telus.com/Wise for your local seniors group.
- Visit telus.com/WiseWorkshops to complete the online seniors workshop.
- Check out telus.com/WiseOnlineBasics to watch and learn basic, everyday digital skills.