



TELUS WISE seniors



Helping Canadian seniors
navigate their digital world.

Contents

Introduction.....	1	Social networking safety tips.....	15
How connected are you?.....	2	1. Keeping an eye on your permission settings	15
General Internet and smartphone safety tips.....	4	2. Keeping an eye on your privacy settings	16
1. Setting strong passwords	4	3. Thinking twice before connecting or posting	16
2. Software upgrades for your devices	5	4. Choosing applications carefully	16
3. Creating a Google alert for your name	7	5. Not forgetting to log off	17
4. Keeping your browser in check	7	6. Keeping your digital household clean	17
5. Being careful about sharing personal information online	8	Protecting yourself from identity theft.....	18
6. Thinking before you click	9	Internet fraudsters will find their victims online with minimum cost.	19
7. Shopping online	10	Some ways to protect your personal information and privacy online	19
8. Taking and sharing photos	11	Online dating.....	21
Smartphone safety tips.....	12	1. Create a separate email account	21
1. Turning off geo-tagging	12	2. Choose an appropriate website	21
2. Installing or activating remote locate/lock/wipe software for your smartphone	12	3. Research websites' terms and conditions	21
3. Being careful when using free Wi-Fi in public places	13	4. Create an engaging profile	21
4. Wiping your phone before recycling it or giving it away	14	5. Be cautious if you plan to meet	22
5. GPS	14	Social gaming tips.....	23
		Additional resources.....	25



Introduction

This guide has been created for Canadian seniors who are already using the Internet and **want to learn more about participating in our digital society safely**. This guide can be used as a personal reference and is also used as a workbook for participants of TELUS WISE® seniors' workshops.

If you are interested in booking a TELUS WISE seniors workshop for your community group please contact us at **wise@telus.com**. All elements of the program are free-of-charge and available to all Canadians.

For additional resources, including an electronic copy of this guide, please visit **telus.com/wise**.

Also if you have any questions don't hesitate to email us at **wise@telus.com**.



How connected are you?

Take a few minutes to think about how active you are online.

Do you use any of these?

Email Yes No

Twitter Yes No

Facebook Yes No

Instagram Yes No

YouTube Yes No

Do you **text**? Yes No

Do you **download apps** (e.g. games, mapping)
to use on your computer, tablet or smartphone..... 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 participate in **online games**
with others (social gaming)? Yes No

Do you use the **Internet for research**
(e.g. travel, health care)? Yes No

Now add up how many email accounts, social networking accounts (e.g. Twitter, Facebook, Instagram), mobile apps, online banking and online shopping accounts you have.

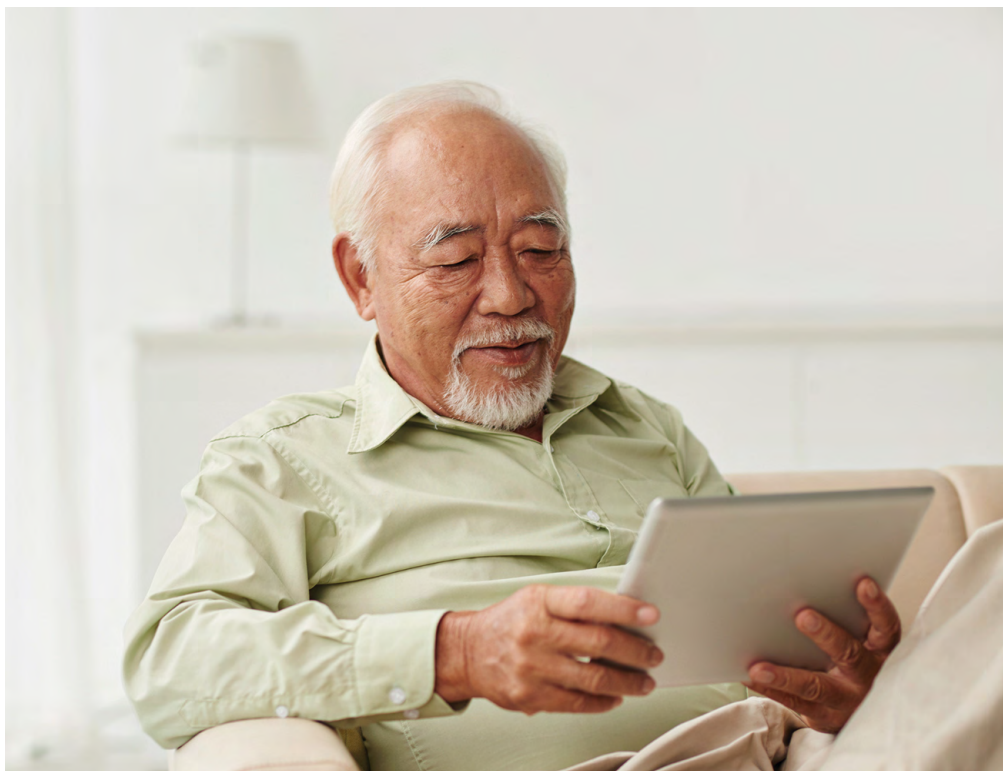
What does it add up to? **Your total here:**

Stop to think about how many Internet-enabled **devices** you have. Include smartphones, computers/laptops, tablets and game consoles.

What does it add up to? **Your total here:**

Even if you just have an email account and only do general web surfing **you are ‘connected’ and a member of our growing digital society.**

In the following sections of this workbook we will share online safety tips to help you protect your privacy, identity and more.



General Internet and smartphone safety tips



1. Setting strong passwords

A strong password can help stop someone from hacking into your email, social networking accounts, etc. **A good password is at least eight characters long and includes numbers, letters and symbols.**

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

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 for 2016 were:

1. 123456
2. password
3. 12345
4. 12345678
5. football
6. qwerty

Visit goo.gl/teu0vJ for the full list.



2. Software upgrades for your devices

It is really important to accept software upgrades which include very important 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. Blackberry, Apple and Android) will all offer their own programs to update the 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.

Similarly, **on your computer**, all your software updates should come from the manufacturer of the software. For example, Microsoft and Apple will manage a large majority of the updates for your devices.



Protecting yourself from illegitimate software update requests.

Fake software updates, no matter how legitimate they may seem, can cause a lot of damage if you click on them. **So always remember to stop, take a close look, and when in doubt — do not download.**

- Don't respond to software update requests when you're on a **public Wi-Fi** hotspot or **surfing a free media (e.g. news) or download site.**
- When in doubt, **download any needed updates directly** from the software vendor's website (e.g. Microsoft, Apple).
- **Never** click links in emails that tell you to upgrade your software.
- Get in the habit of **reviewing software update requests carefully**, especially if they seem to have appeared out of nowhere. Also look for poor grammar and typos.
- Set your computer to **automatically update your operating system** and applications.
- **Hover over links.** By far the easiest way to identify if an email is legitimate or not, is to simply hover your mouse over suspicious links. By doing so, you will be able to tell if the email is from a recognizable domain that is linked to the actual sender name. The first portion of the address (URL) is the 'domain name' (After the http:// and the subdomain). Many spammers try this when trying to get you to click on malicious links.





3. Creating a Google alert for your name

Go to google.com/alerts.

Enter your name in the search box to see any content with your name referenced. You can refine the search by adding the province or city you live in.

If you have a Google account you can create a permanent Google alert for your name. You will receive Google alerts via email when your name appears online. This is not a 100% guarantee but a great start to tracking your digital footprint, and the alerts may provide early warning of identity theft, etc.

Visit <https://goo.gl/Kh01N4> to find more information about creating Google alerts.



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. Make sure you have the latest version of the browser installed and that it is configured to provide the desired levels of security and privacy.

Also clear your browser history and cache at least once a month.

Visit <https://goo.gl/Q0cMuZ> to learn how to delete your browser history for all popular web browsers.



5. Being careful about sharing personal information online

In order to limit the amount of potentially sensitive information about yourself **online** — and to limit your susceptibility to **theft or abuse** — think twice before posting:

- Your contact information (e.g. phone number, email address)
- Your full date of birth
- Your social insurance number
- The names of your children or family members
- Your full home address
- Dates and details of trips, vacations and time spent away from home

When you are asked to share personal information online **ask yourself the following questions:**

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?
Remember it is YOUR information.

Think about creating a separate email account for your online activities (e.g. Google mail) — separate from your personal email that you use to connect with family and friends. If the email account you use for online activities is compromised, your personal email account will still be intact.



6. Thinking before you click

- **Never click on suspicious links or attachments**, even if they look interesting. A lot of scams (i.e. phishing) and malware in the social network world are spread through links, attachments and rogue applications.
- **Do not respond to phone calls or emails** that request personal or financial information, especially those that use pressure tactics or prey on fear.
- Legitimate service providers, banks, etc. **will not** initiate communication with you and then ask you to provide or verify sensitive information through a non-secure means, such as email.
- **If something seems suspicious or too good to be true**, it most likely is, so pick up the phone and call your service provider or financial institution directly to verify the validity of an offer or request for account information.
- **Read your monthly account statements thoroughly** as soon as they arrive to ensure all transactions shown are legitimate, and verify the transactions you expected to appear as well.
- **Microsoft or other companies will not call you** telling you that there is something wrong with your computer. How would they know if you haven't contacted them? The best advice is to hang up on this call as quickly as possible. Do not agree to visit a website given to you by caller to help you fix your computer — this is a scam!



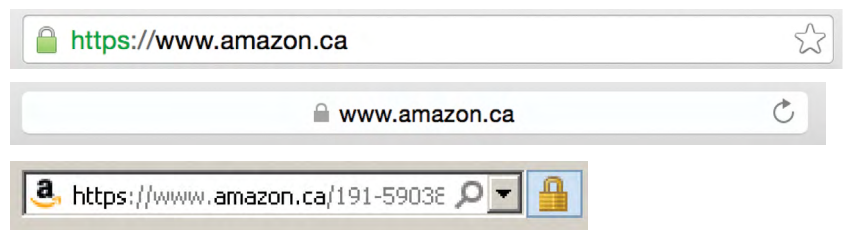


7. Shopping online

Generally, try to use reputable websites for online shopping. Check with friends or online references (not affiliated with the site) to get a feeling for reputability.

Next, ensure that the site that you enter your credit card information into uses encryption. **Look for the 's' in the http web link name, or look for the 'lock' symbol in your browser to indicate that encryption is being used.**

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



Also when shopping online, **do not let a computer or other electronic device remember your password.** Always decline this option.



8. Taking and sharing photos

Many of us love to take pictures and share them with family and friends. There are a couple of things we should think about before taking and posting and sharing pictures online:

- **Always ask someone's permission** before you take, post or share a picture. You should ensure someone asks your permission as well before they take, share or post a picture of you. This even extends to grandchildren and children in your life — make sure you have the parents' approval before you post or share a picture with a child in it.
- **Make sure geo-tagging is turned off** on your device (e.g. smartphone) or application (e.g. Instagram) when taking and sharing photos. See tip 1 in the next section for further details on how to turn off geo-tagging.



Smartphone safety tips



1. Turning off geo-tagging

Turn off geo-tagging on your smartphone and tablet, or even social networking sites like Instagram and Facebook, to enhance your privacy. When geo-tagging is turned on the exact latitude and longitude is included in photos and videos you take and post on social networking sites or share via email. Geo-tagging can be found in your location or camera settings.

The easiest way to find out how to turn off geo-tagging is to visit google.com and search 'how to turn off geo-tagging on an iPhone' or 'how to turn off geo-tagging on Instagram'.



2. Installing or activating remote locate/lock/wipe software for your smartphone

Another very useful tip is to install software that allows you to lock, track or remotely erase the information on your phone if it is lost or stolen. For the iPhone it's called **Find my Phone**, for the Blackberry its **Blackberry Protect** and for the Androids it's different for each manufacturer. For example, Samsung has what's called a **Mobile Tracker**.

With these programs, you can even remotely post a message on the screen advising how you can be contacted should your phone be found.





3. Being careful when using free Wi-Fi in public places

Be careful when using “free” Wi-Fi in public places — it can be an easy way for hackers to access personal information. Although you always run a certain amount of risk when connecting to public Wi-Fi, there are certain measures you can take to protect yourself:

- **Always confirm the legitimacy of a Wi-Fi network** before connecting to it; do not rely on the name alone. If there are multiple access points for the same venue (e.g. coffee shop), ask a staff member which one to use. Similarly, be sure to read that venue’s Terms of Service carefully to ensure that your privacy will not be breached.
- Ideally, you should **only use public Wi-Fi to browse websites that do not require login credentials** (e.g., general web sites, etc.). However, if you do need to access sensitive data or enter login credentials (e.g. your email account), only go to websites that start with HTTPS (‘s’ = secure, a more secure version of the standard HTTP web protocol). Just be aware that even if a website uses HTTPS for the majority of its content, the images on that website might still be distributed via HTTP since links are not typically encrypted. However, most current web browsers will warn you if this linked content is not secure or when the certificate from a secured HTTPS site is not valid or verifiable.
- **Never install software while using public Wi-Fi**, as it could introduce viruses 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 instead of the real software.



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

Technology is advancing at an amazing pace and new mobile devices with new features are coming out every month. Consequently, many people replace their smartphones or tablets almost every year.

Have you ever thought about what happens to your old device when you dispose of it? More importantly, what happens to all of your private information? After using your devices every day for so long, it has accumulated a significant amount of very private data.

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

If you require help, you can visit a TELUS Learning Centre for assistance.
Visit: goo.gl/g8WZJ2



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?

Turn off GPS (or location setting), Wi-Fi and Bluetooth features when you are not using them. You will protect your privacy and also save a lot of battery power!

You will find GPS/location, Wi-Fi and Bluetooth in the 'settings' section on your smartphone.

Social networking safety tips

It is really important that your permission and privacy settings on social networking accounts that you sign up for and apps that you download, **are set to where you want them to be**. You really need to pay attention to the privacy and permission terms and settings — just don't accept them blindly.

- **Permission settings** control what can and cannot be accessed and shared about you (e.g. contact lists, computer files including photos, and your profile) by a social networking site or mobile app that you subscribe to.
- **Privacy settings** control who can and cannot see your profile and posts.

Before reviewing these tips, write down all of the social network accounts (e.g. LinkedIn, Twitter, Instagram, Facebook) you have subscribed to and apps (e.g. weather, mapping) that you have downloaded.



1. Keeping an eye on your permission settings

Every time you download an app on your smartphone, tablet or computer, or sign up to a new social networking site, you could be allowing its developers to see and even take your personal information which could include your address book, your Facebook or Twitter account information, your location, or even your photos.





2. Keeping an eye on your privacy settings

Make sure you know what information is being shared publicly — and what information can be accessed by applications. You may be sharing more than you intended.



3. Thinking twice before connecting or posting

It's a good rule of thumb to only connect and share with people that you know in real life. By 'friending' people online that are strangers, you open yourself up to added privacy and security risks. Facebook estimates that 1 percent of their 1.86 billion monthly active users are 'false' accounts, potentially created by malware writers and spammers. Also be careful with what you post and share. For example, posting a picture of your son or daughter helping you in your yard when they were supposed to be at work can impact their job!



4. Choosing applications carefully

Only purchase/download apps from your smartphone or service provider's 'app store'. Steer clear of apps that ask for access to data like your address books, photos, etc. Rule of thumb: Before downloading an app, do a search to make sure it's legitimate.



5. Not forgetting to log off

Don't leave social media accounts (e.g. Twitter, Instagram) or apps/games (e.g. Angry Birds) open if you are not using them. If you don't log off you can become vulnerable to security and privacy risks.

Also unsubscribe from accounts and apps that you aren't using. Think about this — a dormant Facebook account of a Calgary teen, who stopped using it because it had been previously hacked, was used to lure teens over the Internet by a criminal.



6. Keeping your digital household clean

Book a time in your calendar every three to six months for you and your family to check your privacy and permission settings on the social media sites you subscribe to and apps you have downloaded. Also unsubscribe from email accounts and applications that you no longer use.



Protecting yourself from identity theft

What is Identity Theft?

Identity theft refers to **acquiring** and **collecting** someone else's personal information for criminal purposes.

What is Identity Fraud?

Identity fraud is the actual deceptive **use** of the identity information of another person in connection with various frauds.

What is the potential impact on victims?

- **Damage to credit history status**
- **Refusal of credit** (mortgages, loans)
- **Assumed identity** (offenders may incur criminal records or warrants)

What information is sought out by the fraudster?

- Full Name
- Date of Birth
- Social Insurance Number
- Full Address
- Mother's Maiden Name
- Username and Password for Online Services
- Driver's License Number
- Bank Account Numbers
- Personal Identification Numbers (PIN)
- Credit Card Information
- Signature
- Passport Number



How is your information used?

- Access your bank accounts
- Open new bank accounts
- Transfer funds
- Apply for loans, credit cards and other goods and services
- Lease cars or apartments
- Hide criminal activities
- Obtain passports
- Receive government benefits



Internet fraudsters will find their victims online with minimum cost.

Two common ways are:

- **Phishing:** the activity of defrauding an online account holder of personal and financial information by posing as a legitimate company
- **Pharming:** the act of domain name switching, where you will be redirected from a legitimate website to a fraudulent site where your information is not secure and at risk of being used for illicit purposes



Some ways to protect your personal information and privacy online

1. Wipe your device

Computers and smartphones contain a wealth of information that data thieves would love to get their hands on. Simply deleting your files and emptying the recycle bin is not enough; wipe or erase your hard drive before disposing.

2. Be aware of your surroundings

Shoulder surfers will look over a victim's shoulder while they are entering in their PIN or password. You should:

- Be aware of your surroundings and realize that shoulder surfers are actively seeking opportunities.
- Block your data. Shield the number pad to prevent someone from stealing your PIN.

3. Scrutinize emails

Be particularly wary of unsolicited e-mails, including those that identify you have won a prize or asking for financial help.

4. Manage your passwords carefully

- Choose passwords that will be difficult to crack.
- Use different passwords for all accounts.
- Change your passwords and PIN codes often.
- Memorize your passwords and PIN's.

What to do if you are a victim

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 and place a fraud alert on your credit reports:

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

Step 4: Always report identity theft and fraud.

Contact the Canadian Anti-Fraud Centre:

Toll free: **1-888-495-8501**

antifraudcentre-centreantifraude.ca

Online dating

1. Create a separate email account

Everyone you meet will not turn out to be a perfect match, so you want to keep it a little more anonymous than the everyday email you use with your family and friends.

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 websites' terms and conditions

Read the fine print before signing up. If you have a free trial, put a reminder in your calendar so that you can decide if you want to continue. A lot of the time with paid websites it is an automatic renewal. Investigate whether you have the option to opt out.

4. Create an engaging profile

Honesty is the best policy. You get a much better response having a photograph online and websites suggest having action shots. Make sure your profile is up to date and be specific about your interests and hobbies. It is difficult to talk about ourselves, so ask your friends for help.

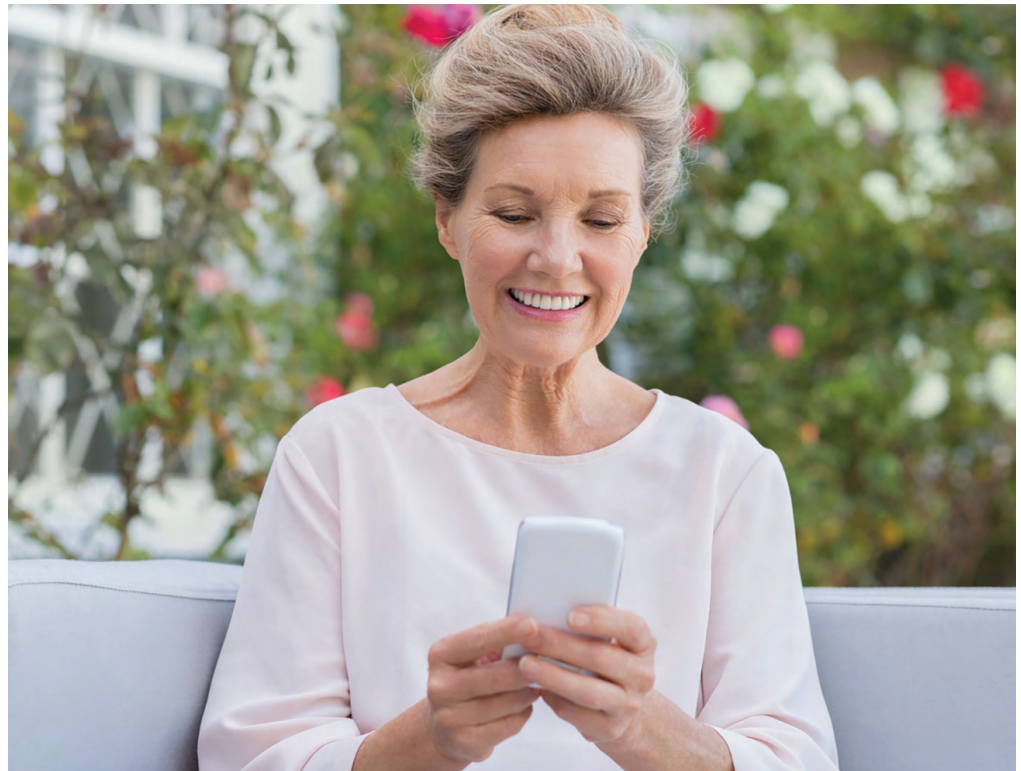
Also, don't include too much personal information, as this could give away your address, for example.



5. Be cautious if you plan to meet

If you do decide to meet someone, use your street smarts. Meet in a public area and don't tell them where you live. You haven't really met them yet, so you need to be mindful of those security risks. The big thing is to listen to your gut.

Source: '5 online dating tips for seniors looking for love in Canada', <http://goo.gl/RtJ98t>



Social gaming tips (online games)

Social games, online games that allow social interaction between players, have become hugely popular as they offer players a chance to play games on their smartphones or tablets through apps or on social networks, often for free! While providing a range of opportunities for engaging with friends and family, it is important that the same rules for staying safe online are applied to social games because the online risks.

If, when downloading an app, it asks to access your data, for example your location or contact list, think carefully about why it needs to do that and what information you are sharing.

Typically, social gamers will be playing directly against their friends or participating in leader boards within the app or via a social network. The ability to interact with people all over the world means it's important that gamers know how to protect their privacy and behave kindly to other gamers.

Fortunately most games and devices will have safety tools which can help protect players. If you are playing on a social network, **learn how to block other players and locate the means for reporting any issues** if you encounter them. When using online chats or sharing information, be careful never to give out any personal information, share pictures or agree to meet up with someone in person. Think carefully about who you are talking to and what you are sharing. Generally, it's best to only talk to people you know in real life, and to keep your personal information, such as your email address and passwords, private.

As social games can be played on the go, gamers may find they are playing them regularly and for extended periods of time. To ensure games form part of a healthy and balanced lifestyle it is important to take lots of breaks.



While many people experience social games and the Internet as a positive and integral part of their life, being aware that things can go wrong and knowing what to do when something does happen is essential to having a safe and positive experience.

Unfortunately, because of the social nature of social games, cyberbullying can occur. **If harassment does happen report this behaviour to the social network you are playing on and block the user. Always be aware of who you are talking and do not reveal any personal information.** Some tips to consider include:

1. When an app asks to access your data, such as your location, **think carefully about why it needs access.**
2. Think carefully about who you are talking to and what you are sharing. **Remember, never share personal information** with people you only know online and be cautious if you plan to meet with anyone face to face.
3. **Be kind and respectful** to anyone you interact with and follow the rules of the game.
4. **Take breaks.** It's fun to play lots of games but it's important to take lots of breaks too.
5. **Be careful what you click on.** Things you buy in apps can cost real money!
6. **Be aware of advertising** and that some 'advergames' are designed to promote and sell a product.
7. **Check your permission and privacy settings;** sometimes game apps will post information on your social media profiles about your gaming activity and send invitations to your contacts to get involved in the game.





How you can participate in TELUS WISE

- Visit us at telus.com/wise for more information or to book a free in-person TELUS WISE workshop for your group.
- Contact us at wise@telus.com
- Join the conversation online with [@TELUS](https://twitter.com/TELUS) on Twitter and use [#TELUSWISE](https://twitter.com/hashtag/TELUSWISE)