TELUS Wise

Digital safety and privacy tips.

TELUS Wise® is a free educational program that empowers Canadians to stay safe in our digital world.

Internet Safety

1. **Protect yourself:** use anti-virus, anti spyware, and firewall security solutions and remember to back up your data regularly.
2. **Keep software, operating systems and browsers up to date** so you're always protected against the latest threats.
3. **Set strong passwords** and change them often. 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*". You can even use a passphrase for added security.
4. **Scrutinize your email:** suspicious attachments/links, requests for personal information, typos and grammar errors are good indicators for a potentially harmful email.

Smartphone and Tablet Safety

1. **Lock your phone:** program your phone so it automatically locks after a period of inactivity. Don't forget to set and change passwords regularly.
2. **Lock, track, erase program:** use an app to lock, track or remotely erase the information on your phone if it is lost or stolen, for example, Find my Phone on iPhones, or Find my Device on some Androids. Remember to wipe your device before you trade it in or recycle it.
3. **Update your operating system** regularly to protect against the latest threats.
4. **Manage location settings:** only grant location access to apps that need to know your location, such as GPS or maps. Social media and many other apps can operate without location information.
5. **Research apps before downloading** to avoid malware from being installed onto your device.
6. **Be cautious of free Wi-Fi:** it can be an easy way for hackers to access personal information. If you do use free Wi-Fi in a public place, limit your activity to browsing only. Never share personal or financial information over public Wi-Fi.
7. **Be aware of Bluetooth risks:** hackers can potentially access information on Bluetooth-enabled devices. Only enable connections with trusted devices and/or turn Bluetooth off if it's not required.

Social Media Safety

1. **Keep an eye on permission & privacy settings:**
   - **Permission settings** control what can and cannot be accessed and shared about you (e.g. contact lists, photos, profile information).
   - **Privacy settings** control who can and cannot see your profile and posts.
2. **Create a Google Alert:** set up a Google Alert for your name at google.com/alerts so you are notified via email when your name appears online.
3. **Limit what you share:** sharing too much information such as your date of birth, address, and vacation details can increase your risk.
4. **Think twice before connecting:** only connect with people online who you know face-to-face.
5. **Be careful where you click:** don't click on offers that sound too good to be true.
6. **Turn off geotagging:** photos taken from most smartphones include a geo-tag (exact location details where the image was taken). Turn off this feature to enhance your privacy when sharing photos online.
7. **Don't forget to log off:** leaving social media accounts, apps or games open when not in use leaves you vulnerable to security and privacy risks.
8. **Keep 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.

Online Shopping Safety

1. **Verify the seller's reputation:** look for a privacy statement, physical address, phone number and return policy on the website, and look for positive reviews from other customers.
2. **Confirm security:** look for the lock symbol and the 'S' in "https" in the address bar.

3. **Protect your information:** don't shop on public computers or Wi-fi, and always decline the option to save your credit card information.
4. **When making a mobile payment using your phone or watch,** only use the payment app that came with the device (e.g. Apple Pay or Android Pay).

Stand against distracted driving

Make distracted driving socially unacceptable. Keep your hands on the wheel and eyes on the road with these tips:

1. Keep your phone out of sight, out of mind.
2. Put it on silent or turn it off.
3. Rely on a passenger to handle your phone.
4. Check messages and program GPS before you drive.
5. Pull over safely if you must use your phone.

IoT Safety

IoT, or Internet of Things, refers to smart or connected devices, such as home security systems, baby monitors, smart watches, etc., that connect to each other via the Internet. These devices revolutionize many aspects of our lives, but collect and transmit data, so it's important to consider the following:

1. Understand what data is being collected and how it is used.
2. Manage privacy settings so you share only what you intend to and what you are comfortable with.
3. Turn devices off when they are not in use (especially devices with camera/mic functionality).
4. Keep devices on a separate "guest" network, protecting your personal network in the event of a hack.

Put an end to cyberbullying and rise above it with these tips:

1. Stop engaging and leave the online space immediately; arguing back can escalate the situation.
2. Block all messages if you can, and report/block the person via the social media platform.
3. Record the messages in case they are needed later for an investigation; take screen shots to save evidence.
4. Talk to someone and decide on a course of action. If you are unable to resolve the situation or feel threatened you should contact your local law enforcement agency.

Join the **#EndBullying** movement and help ensure the digital space is a safe place.
Take the TELUS Wise Digital Pledge at **telus.com/digitalpledge**

Learn more at **telus.com/wise** or contact **wise@telus.com** to request a workshop.
Join the conversation online with **#TELUSWise**

Westminster Savings

TELUS