TELUS WISE®

Wise Internet and Smartphone Education

Get wise about Internet and smartphone safety and security

Find out more by joining the TELUS WISE virtual community where you can access great resources, media articles and courses on this important topic. Register at **telus.com/wise**

TELUS

the future is friendly®

Tips for wise smartphone use

Help keep your family safe online by following these tips on Internet and smartphone safety and security.

Google yourself

Put a Google Alert on your name so you can track what is being said about you online. Just go to. **google.com/alerts** and type in your name in quotation marks. 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.

- **Parents' tip:** You can set a Google Alert for your kids names as well.

Set strong passwords

A password can prevent someone from gaining access to your device and doing things like circulating your pictures or sending messages in your name. A good password or other form of authentication can also stop someone from hacking into your social networking accounts or changing passwords on your applications. Set the security settings on your device so that it automatically locks after a specific period of inactivity. Remember to use a difficult password; easy-to-guess passwords are less secure.

- **Parents' tip:** Your children should understand that passwords should not be shared with their friends. While parents have a legitimate reason to know their children's passwords, others do not.

Turn off most geo-tagging

Photos taken from most smartphones include a geotag - the exact location of where the picture has been taken. Think of it this way – if you take a picture of your child's first day at school and share this picture or post it to your favorite social networking site anyone can find the exact location of where this picture is taken. To turn of geotagging – go to 'camera settings' on you smartphone and turn geo-tagging off.

- **Parents' tip:** Ensure geo-tagging is turned off on your kids smartphones.

Install and/or activate remote locate/lock/wipe software and install security software

Some smartphones come with an optional service that will help you locate your phone if it's lost. Take advantage of this free service and set it up or purchase one of the many similar applications. Security software on your mobile device can protect you if you erroneously download a malicious app or click a bad link.

Profile settings:

Privacy settings are configurable on almost every site and app where you can create a profile. Review them regularly.

- **Parents' tip:** Sit down with your kids and check their profile settings on Facebook and other social media sites and ensure that they are set to the desired levels of privacy and security.

Keep your browser in check

The web browser 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.

Be cautious in using Wi-Fi

Be careful about using "free" Wi-Fi in public places – it can be an easy way for hackers to access personal information. Stop and think about how secure the Wi-Fi might be before accessing it. Don't share personal or financial information over an unsecure network unless you are confident that they will be effectively encrypted.

- **Parents' tip:** Teach your children about the risks of using open Wi-Fi in public places.

Visit us at **telus.com/wise**. Join the conversation online with **@TELUS** on Twitter and usir

Choose applications carefully

Only purchase/download applications from your smartphone or service provider's "app store." Steer clear of applications that ask for access to data like your address books, picture gallery, etc. Rule of thumb: be wary of free applications. Often, free is too good to be true.

- **Parents' tip:** Kids often don't realize that the game "everyone is playing" on their phone comes in an ad-filled free version and to unlock it costs real money. Help your child understand what you'll pay for and what is coming out of their allowance.

Be aware of risks of using Bluetooth

If you are using Bluetooth-activated devices, there is a risk of others accessing information on them or making unauthorized connections with them. Only enable connections with trusted devices.

- **Parents' tip:** Always switch your child's Bluetooth device to "undiscoverable."

Save battery power

Manage your phone's power consumption by turning off unneeded features and turning down adjustable features:

- Dim your screen
- Turn off Bluetooth when it's not in use
- Turn off Wi-Fi when it's not in use

Digital house cleaning

Set 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, check/reset passwords and ensure you are using the latest web browser. Make it a family activity.

ng **#TELUSWISE**.

What do I do if I suspect my child or someone I know is being subjected to cyberbullying?

Discuss the options for blocking messages from specific numbers or user accounts with your kids. Third-party applications are available for smartphones and some built-in tools enable users to block calls or text messages from specific numbers.

If blocking doesn't eliminate the problem, or is not feasible, and the abuser is known, then a parent-to-parent discussion may be called for. Indeed, school authorities may require you to take this step before they will consider getting involved.

In more serious cases and where other alternatives are ineffective, victims or their parents should contact their local law enforcement agency. Some schools have (or have access to) a police community liaison officer who might be able to help. Harassment is a crime under the Criminal Code, and defamation law may also provide a legal means to stop harassment.

How can I get my kids to share their user names and passwords with me in case of an emergency?

MediaSmarts recommends having your kids write down their user names and passwords for their smartphone, laptop and social media groups (e.g. Facebook) on a piece of paper and date it. Have them place this information in a sealed piggybank that you agree to access only in the case of an emergency.

List your emergency contacts

Ensure you have emergency contacts stored on your phone.

- **Parents' tip:** Make sure your contact numbers are stored on your kids' phones

Erase your personal information when you upgrade to a new smartphone

Use the manufacturer's approved method to reset your device to factory settings before recycling it. Performing a security wipe is a secure way to delete your personal data, passwords, files, and emails. Remember, manually deleting your information may not be as thorough as resetting the device.

GPS applications

Various applications access your phone's GPS to provide services ranging from finding nearby restaurants to checking you in on social networks. As a user, you can revoke these applications' access to your phone's GPS. When you install them, many applications will ask you for permission to use your location. When in doubt, say no.

Back up often

Frequently back up the information you store on your smartphone, in case it is lost, stolen or breaks.

How you can participate in TELUS WISE

- Visit us at **telus.com/wise**
- Contact us at **wise@telus.com**
- Join the conversation online with **@TELUS** on Twitter and using **#TELUSWISE**

TELUS
the future is friendly®