**Stay safe online tips**

Use **strong and unique passwords** and ***never*** share your passwords with anyone, unless you’ve designated someone you trust to manage your accounts. One reason for this precaution is to prevent someone from using your account to impersonate you — perhaps asking your friends and family to “help you out” by wiring “you” money in an “emergency,” which is a common scam.

Make sure your **passwords are long** — at least eight characters — and include numbers, upper and lowercase letters and symbols; avoid using names or dictionary words.

**Use privacy settings**. Most services have settings that let you control who can see what you post. Facebook, for example, has extensive controls, letting you post to only friends, your friends and their friends, or everyone on Facebook. You can also limit specific posts to a smaller group like only family members or specific people. Some services give you a choice between private and public posts, with private going just to people you designate. Before posting to any service, it’s good to get to know its privacy policies and settings. There are also privacy settings for smartphones that can restrict who has access to your location, contacts, and other personal information.

**Think before your post**. Whether it’s a picture, video, or comment, what you post and what you share is a reflection on you. Make sure you feel good about being associated with anything you say online and be sure not to post anything that you wouldn’t want to share with the world. Even if you’re using privacy settings to limit the audience, there is always a chance that what you post can be copied and shared by others.

Dealing with **“spam”** or unsolicited email can be challenging. It’s pretty common to be plagued by junk email. Simply getting these messages isn’t necessarily dangerous, but it can be annoying. In some cases they can be from companies you’ve interacted with in the past and, if they are legitimate companies, there is probably a link to a page where you can safely ask to be removed from their list. But if they are truly “spammers,” they won’t stop, even if you ask them to. The best thing to do is make sure you’re using whatever spam filter is provided by your email service. Avoid clicking on links in unsolicited email, as there is a chance they could link to sites designed to scam people or infect computers with malicious software.

**Report abuse from anyone**, including friends, family and caregivers. We hear a lot about children being “cyberbullied,” but it also happens to adults, including seniors. If you are getting messages on social media or in email that are threatening, mean, extremely angry, accusatory or in any way abusive, don’t respond; reach out for help and support from someone you trust or from adult protective services or law enforcement, and report the behaviour to the site or service. All major social media companies, and online and mobile service providers have employees that respond to **abuse complaints.**

**Staying Safe Online**

1. Don’t post any personal information online – like your address, email address or mobile number.
2. Think carefully before posting pictures or videos of yourself. Once you’ve put a picture of yourself online most people can see it and may be able to download it, it’s not just yours anymore.
3. Keep your privacy settings as high as possible
4. Never give out your passwords
5. Don’t befriend people you don’t know
6. Remember that not everyone online is who they say they are
7. Think carefully about what you say before you post something online
8. If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell a trusted party/family member about it.

**Top 7 tips for mobile phone safety**

1. Do not reply to a text from someone you don’t know.
2. Keep the messages you have been sent so you can show them to a trusted party/ family member and make a note of the time and date of the messages or calls you receive.
3. Do not answer calls from withheld numbers or numbers you don’t recognise, let it go to voicemail.
4. Block numbers from people who are sending you nasty messages.
5. Do not give your mobile number to someone you don’t know.
6. Do not send pictures to someone you don’t know.
7. If the problem is serious you can report it to the police.

Scams!

Fraudsters use the Internet to scam unsuspecting consumers. If an offer, email, or message sounds too good to be true or just seems plain fishy, go with your gut and do some additional checking. Here’s a roundup of common scams:

**Personal emergency scam**:

* Scammers email or post social media messages that appear to be from someone you know saying they are in distress, such as having their wallet stolen or having been arrested.
* If you get such a message, find another way to verify if it’s true, such as reaching out directly to the person. If you get such a message from a friend, there is a good chance that their account was hacked and that it’s a criminal who is out to steal your money.

**You owe money scam**:

* Be wary of emails that claim you owe money.
* If you hear from a bill collector or a government agency about money “owed” by you or a family member, don’t respond unless you are certain it’s legitimate.
* It’s pretty common for scammers to send “bills” to people who don’t actually owe them money.

**Online dating scam**:

* Many people have found love via dating websites, but others have been scammed out of money by online con artists.
* For tips on safe online dating and a list of red flags, see “Meeting new friends and romantic partners.”

**Infected computer scam**:

* You might get a call from “Microsoft,” saying your computer is infected or vulnerable to hacking, with an offer to fix it for you. **HANG UP.**
* Microsoft and other reputable companies never make these calls. These are criminals trying to steal your money and plant viruses on your machine.
* Also be suspicious of any messages in email or that pop-up on your computer, in your Web browser or on a mobile app warning you of a virus or a security risk.
* If you have reason to suspect that your device is at risk, consult a trusted expert but never download software or apps that you aren’t certain come from legitimate sources.

**Speak out and don’t be ashamed if you’re victimized**.

* Criminals are very good at what they do and there have been lots of very smart people who have been victimized online. If it happens to you, report it to a trusted person and, if appropriate, law enforcement.
* Even if you let your guard down, ***it’s not your fault if something bad happened to you.***

**5 Tips To Spot Fake News**

1. **Simplicity doesn’t equal truth** - it is surprisingly easy to mask a lie in the veil of credibility, by making it sound so obvious it must be true.
2. **Don’t be fooled by images** - With the use of software such as Photoshop, images can be easily altered. You may not realise just how easily this can manipulate your memory of history.
3. **Use critical thinking** - we are constantly surrounded by information, this can lead to over confidence and a belief we know more than the average person, as a result, our use of critical thinking is effected and leads to the risk of dismissing anything that disagrees with us.
4. **Look beyond your bubble** - It's important to engage in conversation with people that hold different views from our own, and explore news sources outside our usual routine. You may be surprised to find information that questions the facts you took for granted.
5. **Be curious** - Look at existing evidence in a more balanced way to ensure you are not blinded by pre-existing beliefs.

**Privacy settings for my computer and smartphone**

On your computer, you can protect against privacy invasion in your web browser. On your smartphone, you use the phone's settings.

**Computer Privacy**

Take a look at the privacy settings offered in your browser (Firefox, Chrome, Explorer) - usually found in the **Tools menu**- to see whether you can fine-tune them to keep the good and block the bad.

Tools > Customise and Control > Settings> Advanced Settings> Privacy and Security

**Smartphone Privacy**

Settings on smartphones vary, but you can tighten up privacy with these precautions:

Turn off location services. That prevents apps from tracking your location.

Don't let apps share data. Some apps want to use information stored on your phone (your contact list, for example). **Say no**.

Enable privacy settings on apps you download. Make sure you are using strict privacy settings on services such as Instagram and Facebook.

