Internet Safety and Social Media Tips

This publication is intended to provide general information only and is not a substitute for legal advice.

Internet Safety

The Internet is an incredibly useful tool. Through it, we can connect with family and friends, find out more about the world, and complete everyday activities quickly and easily. Though entertaining and educational, the Internet can also be used by hackers and scammers to spy inside our computer and electronic devices to obtain our personal information.

To avoid unpleasant computer and Internet-related issues while continuing to enjoy easy and quick access to the Internet, consider the following tips:

- Keep your computers and electronic devices safe by installing the latest software and operating system updates and firewall protection. Systems can become outdated on a daily basis, leaving your computer and electronic devices vulnerable to malicious software, such as computer viruses, Trojan horses and spyware.
  - A computer virus is a program that will reproduce itself into other programs if it is allowed to run on your computer.
  - A Trojan horse is disguised to look like a normal program or one you want to install. Once inside your computer, the Trojan horse can reproduce itself, steal information, or harm your computer's operating systems.
  - Spyware can be distributed by a Trojan horse to observe your web browsing, show targeted advertising and pop-ups, and manage your browser to show specific websites or search results.
- Update your web browser regularly and adjust your browser settings to a higher security level.
- Clear your computer cache and browser's history immediately after you finish online banking. This will help keep your financial information and password secure.
- When you are not using your computer, consider turning it off and disconnecting your Internet access. Many spamming programs are designed to locate and infiltrate unprotected computers that are turned on and connected to the Internet.
- If you use a wireless network at home, make sure the wireless encryption is enabled and protected by a complex password made up of numbers, symbols, and capital and lower case letters.
- Back up your files and make multiple copies of anything of importance.
- Use a firewall program, especially if your Internet is connected 24 hours a day. The firewall stops unwanted visitors from getting to the information on your computer.
- Wireless device applications using Global Positioning Systems (GPS) can send promotional material to your phone. The applications can be enhanced to collect, use, and distribute your personal information without your knowledge. Your device's manual can tell you how to turn off this feature.

Mobile Devices

Mobile devices, such as Smart Phones and Bluetooth enabled phones, are easy to use and a wonderful way to keep in touch with the world. However, misplacing or losing your mobile device can put your personal information in jeopardy. Visit the Get Cyber Safe website for tips on how to keep your information private:

Using mobile devices
www.getcybersafe.gc.ca/cnt/rsks/nln-ctvts/mbl-eng.aspx

For more information, vist https://www.alberta.ca/fraud-awareness.aspx or call 1-877-427-4088

Alberta

Using web-enabled devices safely
https://www.getcybersafe.gc.ca/cnt/prtct-dvcs/mbl-dvcs/index-en.aspx

Things to keep in mind while banking on the go
www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-mn/bnkng-fnnc-eng.aspx

Voice over Internet Protocol (VoIP)

Talking to people over the Internet is made possible through Voice over Internet Protocol (VoIP) technology. VoIP is web-based and easy to use. However, with ease of use are some risks, such as voice phishing, eavesdropping and phone tapping. Visit the Get Cyber Safe website for more information on how to avoid common VoIP threats. www.getcybersafe.gc.ca/cnt/rsks/nln-ctvts/vp-eng.aspx.

Surfing in public

Use automatic lock functions with password protection on personal computers and tablets.

- Keep in mind that connecting to free public Wi-Fi Internet networks in public places, such as restaurants, hotels, airports, and stores, may be risky. Non-legitimate or rogue hotspots may be located in the same place as the establishment's hotspots and can be difficult to identify. Before surfing, ask management for the network name and, if available, the password.
- Always use a firewall when surfing.
- Beware of 'shoulder surfing'. Identity thieves will try to access your passwords and personal information by looking over your shoulder when you log in.

Web software

Install applications from sources you know. Research unfamiliar software and applications before downloading them.

- Read the security warnings, licence agreements, and privacy statements attached to software before starting the download. Spyware could be included with downloadable software and mentioned in the licence agreement or privacy statement.

Passwords

- Use complex passwords made up of numbers, symbols, and capital and lower case letters for your wireless networks, computer, and electronic devices.
- Create and use a different password for each of your online accounts, such as e-mail, Facebook, Twitter, and banking, and change them frequently.
- Memorize your passwords and never share them.

Shopping online

- When buying or selling online be cautious: of messages with spelling errors, awkward phrasing, and content you would not expect to read considering the context of the message.
- if the buyer is in a hurry and makes an emotional appeal to secure the deal.
- if the buyer lives in a different city or country and they plan to send a third party to receive the goods.

When selling an item online, always pay for the shipping to the purchaser and keep the official receipt. You will then have a paper trail should anything go wrong. Check your bank account to make sure you have received the funds before sending the product.

Online shopping in Alberta is regulated under the Internet Sales Contract Regulation. Read our *Internet Shopping* publication at https://open.alberta.ca/publications/internet-shopping to find out about the regulation's disclosure and cancellation requirements.

Emails

Delete e-mails from people you don't know.

- Think carefully before giving your business card in restaurants or giving your e-mail address in shopping mall contests or draws. Some of these organizations could sell collected information or share it with other companies, which may result in unsolicited e-mails.

- The option to receive products and services is often automatically selected when registering for online accounts. De-select this option to prevent receiving unsolicited e-mails.
- If you do open a spam message, do not respond to it or click on the “unsubscribe” link, as this could verify your e-mail address and result in more spam.
- Disable automatic download of HTML graphics in e-mails. Some linked graphic content could be downloaded from a web server used by spammers for tracking valid e-mail addresses. Disabling automatic HTML download and viewing messages in plain text helps prevent this from happening.
- Only click on links or download attachments in e-mails sent from people you know. You can further check if the link is authentic by hovering over it and seeing if it matches.
    - Clicking on a link in a message sent by someone you don’t know could take you to a phishing website that imitates a legitimate site, where you will be asked for personal information.
    - Downloading free files, programs, or software could give third parties the ability to hack into your computer system and retrieve personal information.
- Turn off the preview screen in your e-mail program. Preview screens are used to allow you to read the start of a message. The danger is that invisible spam codes in the message could be activated through this screen. The best practise is to delete spam and messages from unfamiliar senders before opening them.
- Use more than one e-mail address. Have one for family and friends, one for companies you deal with, and one for online activities.
- Keep in mind that the message may not be from its apparent sender. Should fraudsters gain access to your e-mail account, they can pretend to be a family member or friend and send messages.
- Never e-mail bank or personal information. Phishers send imitations of messages from legitimate businesses asking you for personal information or to confirm banking details. Once sent, your information is used for fraudulent activities.

Social media

It is important to take as many precautions as possible to protect your personal information when using social media sites. Once content is posted, you lose control over who uses, forwards, copies, or claims it as their own. It can be archived and its online lifespan is indefinite.

- Consider limiting the amount of personal information listed on your social media profile – you may want to keep your birthday, full name, phone number, and/or address private.
- Consider limiting status updates that indicate you are out of the house or out of town – these could increase the risk of a break-in to your vehicle or home.
- Carefully choose what images you post because they can be downloaded, shared, saved, and possibly manipulated without your knowledge. Images can be used against you and can hurt your reputation or future work opportunities.
- Geo-tags on digital photos can reveal where you live and where you are traveling. You can turn this feature off on your wireless devices or digital camera.

- Access social media sites in secure browsing mode (https:// rather than http://) – this helps you control who views your personal information.
- Ensure you follow the tips in the ‘Passwords’ section above when creating your password for a social media site.
- Be sure to always log completely out of a social media website. Don’t use the automatic login feature that saves your username and password for future use, and watch for sites that select this feature automatically.
- Read the social media site’s privacy statements and policy. Many sites default to allowing all members to view another member’s complete profile without asking permission. Protect your information by setting your profile to allow access to only contacts you know well.
- Only accept ‘friend’ or networking requests from users you are familiar with. Requests from unfamiliar parties might represent attempts to obtain your personal information for various purposes, including identity theft.

- Many social media sites host third-party applications. Even after these applications are deleted, the application's creator may still have access to your personal information.
- Always read the application's privacy policy before downloading, and only download familiar applications from trusted sites.
- Keep in mind that tweets are accessible using search engines and may be sold to data mining companies. Every Tweet is recorded by Twitter and is archived by the U.S. Library of Congress.
- Go through your posts and contacts periodically, and remove any that cause you concern.
- Delete your social media profile if you feel it has been compromised, and then report your concern to your local police.

For more information

Consumer Contact Centre
Edmonton: 780-427-4088
Toll-free: 1-877-427-4088
https://www.alberta.ca/service-alberta.aspx

King's Printer Bookstore
You may purchase Acts and regulations from the King's Printer Bookstore:
10611 - 98 Avenue, Edmonton, Alberta T5K 2P7
Edmonton: 780-427-4952
Toll-free in Alberta:
Dial 310-0000 then 780-427-4952

These are also free for you to download in the "pdf" or "html" formats at https://www.alberta.ca/alberta-kings-printer.aspx

Other referrals

Office of the Information and Privacy Commissioner of Alberta
Toll-free: 1-888-878-4044
www.oipc.ab.ca

Office of the Privacy Commissioner of Canada
Toll-free: 1-800-282-1376
https://www.priv.gc.ca/en/

Industry Canada Office of Consumer Affairs
http://www.ic.gc.ca/eic/site/icgc.nsf/eng/home

Fight Spam Quiz
Office of the Consumer Affairs
https://www.fightspam.gc.ca/eic/site/030.nsf/eng/00016.html

Service Canada
Toll-free: 1-800-622-6232
https://www.canada.ca/en/employment-social-development/corporate/portfolio/service-canada.html

Immigration and Citizenship Canada
Toll-free: 1-888-242-2100
https://www.canada.ca/en/services/immigration-citizenship.html

Passport Canada
Toll-free: 1-800-567-6868
https://www.canada.ca/en/immigration-refugees-citizenship/services/canadian-passports.html

Canadian Anti-Fraud Centre
Toll-free: 1-888-495-8501
http://www.antifraudcentre.ca/index-eng.htm

Get Cyber Safe
Toll-free 1-800-830-3118
https://www.getcybersafe.gc.ca/index-en.aspx

Consumer Protection Alberta Facebook
https://www.facebook.com/ConsumerProtectionAlberta/