Your Privacy and Security On-Line

Here are a few things you can do to protect your privacy and security on-line.

- Use a comprehensive (i.e. paid for full premier version) of a leading security suite such as Avast! (http://www.avast.com/en-ca/index). You can get a two year, 3 computer package from them for between $100 - $150 (depends on their current promotions, the tides and the phases of the moon). A full security suite has a great deal more than just anti-virus, including various security and privacy tools.

- In conjunction with the full security suite, use Microsoft Security Essentials. This is free from Microsoft (http://www.microsoft.com) and is designed to work with third party security software. DON'T use two or more security or anti-virus suites at once because they usually won't play well together.

- Ever inadvertently get stuck with one of those third party toolbars in your browser and can't seem to get rid of it? These toolbars are tracking devices. Avast! has a free utility called Browser Cleanup (http://www.avast.com/en-ca/store) that deletes these pesky and unwanted toolbars and plug-ins from your browser(s). Simply download and run the Browser Cleanup utility without the need to install anything. Once you run the utility, you will see a list of toolbars and plug-ins and be able to disable them with one click. When you download software from CNET, Download.com and many other places, be VERY careful during the software install not to install one of these toolbars or other things you don't want. As you go through the install steps, you usually have to uncheck one or more boxes to avoid installing this crap, and these boxes are sometimes very hard to see. Assume the boxes or buttons are always there, and don't press the final 'Install' button until you have found them.

- Use a comprehensive (i.e. paid for full premier version) of a security suite such as Avast! (http://www.avast.com/en-ca/index) for your SmartPhones. Even with the full security suite, don't put anything on your SmartPhone you don't want to share.

- Turn off the Wi-Fi on your laptop or SmartPhone when you are away from the home or office except when you are actually using it. Don't use free Wi-Fi unless you have your security suite in place and up to date.

- Be VERY careful of what you post to social networking sites. Don't put anything you don't want a future employer to see. Even if you post something using full privacy settings, you can't be sure that one of your friends or relatives that have rights to see it won't pass it along. Monitor your friend's and relative's pages and have them take down anything they post about you that you don't want the world to see, although once it has already been posted the damage may done. Especially, especially, especially council your kids about this. The pictures of their drunken party or them mooning that is so amusing now won't be so amusing when it costs them a job in a few years, and those naughty sexting pictures can land them in jail for child pornography. Continually monitor your privacy settings on the sites, because Facebook especially likes to change them regularly behind your back.

- The image file for your photographs contains a great deal of metadata, including GPS information if your camera is so equipped (Note: the camera in your cell phone or smartphone IS GPS equipped). Before you post your photos on line strip out the metadata. Many photo viewers and editors can edit the EXIF (metadata) information. Try FastStone Image Viewer (http://www.faststone.org) or IrfanView (http://www.irfanview.com). You can try using the following method in Windows Explorer, but this method doesn't work on many computers. Right-click on the picture's file inside Windows Explorer and choose 'Properties'. Now click the 'Details' tab and select the option that says "Remove Properties and Personal Information". Choose "Remove the following properties from this file" followed by "Select All" and click OK. All the private metadata tags are now erased from the photograph.

- Use encryption where possible, but it isn't easy. TrueCrypt (http://www.truecrypt.org/) is one good freeware choice. They have an on-line tutorial of how to use it. Keep in mind that if you have encrypted files or your entire laptop or SmartPhone you can be legally compelled to provide the keys or passwords by border officials.

- Set up false identities and accounts for websites that you do not want to give your real information to. If you are a G-Mail user you can have up to 5 email addresses. Set up one as your 'garbage' address. Even better, us MaskMe (https://www.abine.com/maskme), which sets up a phony email account that forwards to your real email account.

- Access the internet via a proxy server. This slows things down but it masks who you are and where you are. As a bonus you can pretend you are in another country for things like NetFlix where they won't let a user in Canada watch a movie but they will let a Canadian account holder watch the same movie if they are 'in' the US. There are free proxy server sites as well as paid for proxy server services. Do a bit of goggling to find out more. Avast! has a paid for service but it is a bit pricey ($75/year), but you can chose the proxy server site from several around the world.

- Use Disconnect (https://disconnect.me) or DoNotTrackMe (https://www.abine.com/maskme) to identify and disconnect web tracking services.

- Google and other search engines track your searches as part of their on-line profile of you. You can use a search engine such as Duckduckgo (https://duckduckgo.com) which doesn't track you or keep a browsing history.

- Major web browsers such as Google Chrome, Mozilla Firefox and Microsoft Internet ~~Exploder~~ Explorer have built in hooks to track your surfing history and clickstream. This information can be viewed by trackers and some of the sites you visit. There are several other security issues that can be fixed if you diligently go through all of the security settings in the browser. However, keep checking the security settings because Microsoft especially likes to re-set some of them during updates. Use the browsers "Incognito" or "InPrivate" browsing settings to further mask you. Even if you do all that, re-start the browser between sites that you do not want to be aware of each other. Better yet, use a security browser like White Hat Aviator (https://www.whitehatsec.com/aviator) where all the security and privacy safeguards all built-in, all activated, all ready-to-go.

- Change your passwords frequently for sensitive things like on-line banking. Good passwords contain a random combination of capital letters, small letters, numbers and special characters (!#$%&*), and are at least eight digits long (preferably longer). Every site should have a unique password. There are password tracking applications you can use, or you can use a password protected spreadsheet. Keep in mind the passwords on spreadsheets aren't all that hard to break. If you do use a password tracking application or a password protected spreadsheet, write THAT password down and put it somewhere safe, because if you lose that password you've lost them all (Note: a Post-It Note on the bottom of your keyboard is NOT a safe place for your passwords!)

- On-line shopping is great. ***Some*** of the bigger shopping sites like Amazon keep your credit card information on a server that is not directly connected to the internet and have other safeguards in place. Amazon also acts as a storefront for many smaller sellers, but Amazon itself manages the payment from your card and the storefront only gets your email and shipping info. Other sites, especially the smaller sites, may not have very good security in place. Be very leery of giving these sites your credit card number. Better yet, use a payment service like PayPal (https://www.paypal.com/) to keep your credit card info at arm's length. For those times you really, really need to give a small site a credit card number *("Only they have a speedometer for my 1947 Harley!"*), have a second card with a zero or a pre-pay credit limit that you can 'top up' before you make the transaction. This way there is no usable amount of money left if the card number is compromised.

- Not related to security, but when you're on-line shopping you will often find that an American website will not ship the item to Canada, or that the shipping costs to Canada are outrageous. You can use a service like My US Address (http://myusaddress.ca/). You can set up an account on-line for free. They will give you a unit number and address to have your stuff shipped to. When the shipment arrives at their depot they will email you.

You can pick the shipment up at their depot in Ogdensburg (O'burg is about an hour's drive from Ottawa on highway 416, and their depot is about half a kilometer from the US border crossing). It costs CDN$5 per shipment, and they will hold it for up to a year, so you can order lots and lots of stuff and pick it up every few months or so. Or for extra money ($25 for paperwork plus shipping costs) they will ship it to Canada. Don't forget you need a passport to cross the border, CDN$3 each way for the bridge toll, and you may have to pay the HST at Canadian customs coming back if they are in a bad mood, even on duty-free items.

In reality, if you have already used the Internet, social networking sites, credit cards, loyalty cards, etc. most of your information is already out there.