How to Protect Your Privacy Online: FAQs

In this appendix, we answer some frequently asked questions about protecting your privacy online. Because Internet technologies constantly change, it is not possible to provide a comprehensive guide on this topic, but the answers below provide practical starting points.

Do websites collect personal information about me?

Most do. Certain websites make their policies very clear and collect information about you for a variety of commercial purposes, such as customizing the pages you view or deciding which advertisements to direct your way. Many websites bury their policies in hard-to-find and long-winded terms and conditions, while others collect your information without providing an opportunity for you to consent to or opt out of the collection.

What kinds of information do websites collect that I should be concerned about?

Websites may collect your name, physical address, phone number, credit card details, social insurance number, passwords, IP address, personal files
and folders, real-time activities, whereabouts, tastes, and preferences. Some of this information is supplied by you when you register for a service, but some may be gathered without your consent or awareness.

**Can I guarantee the protection of my personal information online?**

No. The best you can do is to constantly update yourself on measures (discussed below) that reduce the risk of your privacy being violated.

**Am I safe from an invasion of online privacy if I store personal information only on my computer and do not post any information online?**

Not necessarily. If you have not configured your computer’s security settings, it may be possible for information to be accessed by a third party or even uploaded to a public location without your consent. This can happen when you open email attachments or install software. Also, certain music players, calendar apps, or photo managers sort your files for you on your computer but also gather information from your computer that they store or sell to other parties.

**How do cookies work, and should I be concerned about them?**

Cookies are small strings of computer code that store information about you on your computer so that you can be identified when you return to a website. The most common way to tell whether you are being tracked by cookies is if, when you return to a website, details such as your personal preferences and profile information appear without you identifying yourself. On websites that you visit often, certain cookies make online browsing experiences more convenient by remembering information about you (such as your name and password) so that you do not have to enter it every time you return to the website. E-shopping websites, search engines, and video-sharing websites use cookies to customize your search results and to select advertisements that will, presumably, appeal to you. Similarly, certain email providers customize the advertisements that appear on your screen based on the content
of your personal emails. Disabling cookies in your browser will prevent such websites from placing them on your computer if that is your preference.

How can I reduce tracking of my online activity?

- Manage your cookies. Although certain websites only allow you to enter if you have enabled cookies, you should think carefully about a website before you grant this permission. All Internet browsers allow you to disable cookies. And some now have a “private browsing button,” which prevents cookies from being stored in the first place.
- Remove other tracking technologies from your browsing sessions with the use of third-party software. The Office of the Privacy Commissioner of Canada advocates the use of “Do Not Track,” a technology that allows people to opt out of much (but not all) online tracking.
- Use a number of different email accounts. Your primary account should contain your real name and be reserved for communication with individuals you know or groups with member-only affiliation. If you participate in news groups, chat rooms, or other public forums, then you should use a secondary account with a pseudonym. Names or email addresses that you type in public spaces are often gathered and targeted by spammers.
- Use search engines that do not collect your personal information, such as StartPage.

What is “phishing” and how can I minimize it?

Phishing occurs when a fraudster impersonates a legitimate organization and requests personal information. The request can appear in a pop-up message, on a counterfeit website, or in an email. For example, a fraudster could ask you to provide answers to common password challenge questions. What is your date of birth? What is your mother’s name? What is your pet’s name? Some phishing scams encourage you to click on a link; when you do, malware (malicious software) that gives the fraudster access to sensitive information,
such as your passwords or private banking details, is automatically installed on your computer.

To minimize the threat of phishing attacks:

- Avoid opening emails that appear suspicious (generally found in Spam or Junk Mail folders).
- Never click on links in suspicious emails or on suspicious websites.
- Keep your Internet browser up to date, since this will give you access to the most recent privacy options.
- Make sure your Internet connection is secure or scrambled. To identify this, look for “https” (as opposed to “http”) in the address bar. The symbol of a closed lock or unbroken key (usually in the address bar or in the bottom corner of the screen) also indicates that the web page is secure.
- Familiarize yourself with your Internet browser’s add-on software. There are many options available that help to encrypt the websites that you visit and reduce your exposure to phishing attacks.

How can I protect my privacy on social media websites?

Social media websites have become a regular part of our everyday lives. Many people update their tastes, preferences, and locations in real time and disclose their political, religious, and social views on these websites. If this information is publicly accessible, you increase the risk that others, such as employers or identity thieves, may collect your personal details.

To better protect yourself on social media websites:

- Use the privacy settings to limit who can see your personal information.
- Routinely check the privacy policy of your social media website for any updates and maintain your privacy settings accordingly. This is very important because many social media websites frequently update their privacy policies without informing their users of any changes.
- Think carefully about how you might regret—even years later—posting a photograph or comment. There are numerous cases in
which employers, in making hiring decisions, have relied on the
details of a prospective employee’s self-publicized private-public
life on social media websites. Do not post something that could
come back and haunt you.

• If you are posting a photo or comments that refer to someone
else, check with the person before you post it. Do not assume that
content that is seemingly trivial to you will not be embarrassing
or offensive to them. This will also encourage others to treat you
in the same way.

• If someone has posted information about you that you are
uncomfortable with, ask him or her to remove it. While this infor-
mation might still be stored by the social media website after it is
deleted, taking it down will reduce the risk of more people easily
accessing it.

What Internet connections can I trust and how do I keep my connection
safe?

Your safest Internet connection is usually your home connection. This is gen-
erally because there are fewer people using it. Here are some ways to make
your online experience safer:

• Update your network key (i.e., your password for connecting to
the network) often. Use combinations of random letters, punctua-
tion, symbols, and numbers.

• Use strong firewall hardware and software to reduce your vulner-
ability to system crackers.

• Disable your Internet connection when you are not using it.
System crackers search for unattended Internet connections in
order to gain access to consumers’ credit card details and other
sensitive information.

• Think about the websites that you visit at work as opposed to at
home. Employer monitoring, for example, often lets employers
record and see all Internet content sent within and from a specific
workplace computer. Even if you delete a file on your work com-
puter, your manager may still be able to see it from the back end.
How do I protect my child online?

• Become well informed about the issues your child faces online. Visit MediaSmarts.ca to learn more about online privacy, offensive content, cyberbullying, and identity theft.

• Talk to your child about the kinds of problems he might encounter and the types of websites he should visit. Although parental control software lets you block content that you deem inappropriate, either directly in your Internet browser or through your Internet provider, use this software carefully. The best way to protect your child online is to talk to him, make your expectations clear, and trust him to come to you when he makes mistakes.

• The most important thing is to establish a relationship of trust between you and your child. Relying on surveillance rather than communication can backfire. Actions like using parental control software, insisting that your child friend you on Facebook, or demanding that she give you the passwords to her social media accounts and cellphone, make it harder for her, especially as she approaches her teen years, to trust that she can come to you when she has a problem.

• Even though the vast majority of children talk online only to people they know, it never hurts to have the “stranger talk” at an early age. Teach a young child precautionary behaviour such as using a nickname; never disclosing phone numbers, addresses, or specific locations; never uploading photographs; and never agreeing to meet someone without your consent or supervision.

• Encourage your child to share his opinions in ways that are constructive and that promote creativity. Remind him that teachers and future employers may see what he posts.

• Let your child know that she can come to you if she encounters comments that are racist, homophobic, or misogynistic; that promote hate speech; and so on.

• Talk to preteens and teens about the consequences of sexting, that is, sending sexually explicit messages or nude or partially nude photos of themselves or others over a phone or the Internet. Once such a message or image is sent, the child can easily lose control over who can see it.
• Encourage your child to come to you for help if someone else has posted content about him that is hurtful, embarrassing, or offensive. Help your child to strategize solutions, such as confronting the person face to face and asking the person to remove the content. If the situation is serious, ask your child if he would like you to discuss the issue with the parents of the other child or with the school principal.

Can Canadian law help me protect my information from online corporations?

Yes, it can. Please see Appendix 1 for more information.

Who can assist me if my privacy is being violated online?

If you suspect that specific personal information (such as financial accounts) has been compromised, contact the relevant institution (such as your bank or credit-rating company) immediately to protect yourself from identity theft. The Office of the Privacy Commissioner of Canada can also help in these situations:

• If you suspect that your personal information is being used, collected, or disclosed improperly
• If you are having trouble getting an organization to correct inaccurate information about you
• If you have asked an organization for a record of the personal information it has about you and the organization is not giving you access to that information