

# Online Privacy and Safety Checklist

This document contains suggested tips designed to enhance online and offline privacy. While it is impossible to completely anticipate or eliminate all possible privacy vulnerabilities, following the best practices outlined in this guide will help significantly improve personal online safety. The tips provided in this document are most effective when they are integrated proactively as part of an everyday online safety routine.

## Password Management

Strong password management practices are among the most important and simplest ways to improve online security.

- Ensure email accounts and other platform accounts have two-factor authentication enabled (if that service is available).
- Avoid recycling passwords across several accounts. If a password is breached or stolen, someone may be able to access other accounts that use the same (or similar) password with relative ease.
- Following the above point: consider using a reputable password manager to ensure unique and strong passwords can easily and conveniently be managed across all accounts. These services also send notification when username/password is part of a service's data breach. For example, *LastPass*® or *1Password*® are currently two popular and well-regarded password managers available for a small monthly fee.
- Consider using online services to verify if email address or password has been part of a previously reported data breach. The following is one example of a website that gathers data breach information and makes it searchable at no cost to the user:  
[haveibeenpwned.com](https://haveibeenpwned.com)
- If an online service such as the one noted above returns information that suggests username or passwords have been previously breached, it is strongly recommended to change each impacted password to a new, unique password.

- Tips for creating strong passwords:
  - i. Make password as long as possible (generally each platform or service has a character limit);
  - ii. Avoid using sequential characters such as “123”, “ABC” or “qwerty”;
  - iii. Avoid using some of the most used passwords, see here for a list of examples: [https://en.wikipedia.org/wiki/List\\_of\\_the\\_most\\_common\\_passwords](https://en.wikipedia.org/wiki/List_of_the_most_common_passwords)
  - iv. Avoid using passwords that are derived from obvious personal information such as maiden name, date of birth, or pet’s name; and
  - v. When possible include, non-letter characters such as numbers, symbols, upper and lower case letters.

## Social Media and Digital Presence

It may not be obvious to a platform user, but the repeated sharing of content on social media — images, videos, stories, anecdotes, check-in, comments, group associations, online resumé, etc — can collectively provide anyone in the public with enough information to build an accurate profile of a person.

- These seemingly innocuous “digital breadcrumbs” left behind by innocent people may enable any member of the public to easily determine:
  - i. Basic daily schedule based on the timing of online activity;
  - ii. Circle of friends, family, and broader social contacts;
  - iii. Hints contained in the background of images can reveal whereabouts or private residence (e.g., house number or street sign);
  - iv. Images or videos captured with smartphone’s camera application may include metadata about your location;
  - v. Names of a person’s children and the schools they attend;
  - vi. Entire work and academic history, and current employer.

- Consider the following steps to reduce the amount of information that can be used by others to exploit or harm someone.
  - i. Delete any old social media accounts (e.g., Facebook®, MySpace®, LinkedIn®, etc). It can be easy to forget about idle accounts that haven't been used in years, but may nonetheless contain identifying information;
  - ii. If the unwanted attention is expected to be short term, temporarily deactivate social media accounts until the issue has subsided;
  - iii. Lock down privacy settings and block public access to content;
  - iv. Review list of “friends” or “followers” who can view private content
  - v. Avoid accepting unknown “friends” or “followers”. Be wary of people impersonating a friend or creating a duplicate account masquerading as someone else;
- Consider cleaning up and deleting past posts or tweets. This will eliminate the amount of information that individuals can misuse;
- If tagged in a public post by another individual, deliberately untag. If the platform does not allow to untag, consider asking the poster to remove the tag;
- If pictures (including of children) are posted online by friends, family, the school, or daycare, consider reaching out and asking them to remove the images;
- Use a pseudonym as account name. Depending on the privacy risk, consider deleting original account and recreate a new account under a pseudonym;
- Remove any key personal information in profile or bio such as date of birth, age, phone number, email, home address, etc;
- Often image or video files—especially those taken with a smart phone—contain detailed metadata that may include information about the exact location of the image taken. Known as “Exif” data, this information has been used in the past to locate individuals who upload these images to the internet or shared them with someone else. When possible ensure the settings on smart phone’s camera application are such that location data is not being generated and associated with images. For existing images or videos on computer, before sending to a third party, it is good practice to use a metadata removal tool or application to first strip any possible identifying information. Several online resources can help guide through this process for specific operating systems.

## Public Records Access

In addition to online footprints, a great deal of information may also be found about an individual through public record searches. Consider the following steps to mitigate this risk:

- For property owners, information about home address and personal property may be accessible via your jurisdiction's land title or property registry office. Consider inquiring about the possibility of severing name from public searches. Certain offices will grant these requests if there is evidence of a safety risk;
- Any public submission, petition, or variance application (e.g., a request to vary a zoning by-law) that may have been filed with a local or provincial/state government may contain home address or contact information. If this applies to you, consider contacting the local government clerk and request the information be redacted;
- Public court records (e.g., from a divorce proceeding) may contain significant private information. However, because most jurisdictions have what is called an "open court principle" (i.e., court proceedings are by default accessible to the public), it may be unlikely that any of these records will be made inaccessible to the public upon request. However, depending on the situation and the types of harm experienced, there may be options. If involved in litigation, consult a lawyer to see if there is any way to have personal information redacted or sealed against public access;
- Obituaries often contain a great deal of information related to a family unit. These publications can easily allow an individual to recreate a family tree and identify close members of a person's inner circle. Depending on the level of risk, consider contacting the website or publication as a family member and requesting a name removal or changed to a nickname, middle name or pseudonym.



## Other Considerations

- Consider using an email address that is not constructed using actual name. This makes it far more difficult to confirm identity. Using a nickname, middle name, or other terms are good ways to make email address less identifiable;
- Accept update prompts from apps or operating system to protect computer or device from viruses or malware attacks;
- A growing type of privacy attack is what is known as a “SIM swap.” A SIM swap is when someone convinces cellphone carrier to switch a person’s phone number over to a SIM card they own. To protect against this, it is advisable to contact cellphone provider and notify them that you do not plan to port your number or change providers. If possible, ask that your account security be enhanced in some fashion – this could involve adding an additional password requirement on account when dealing with customer service;
- If you suspect your phone number has been disclosed publicly, consider contacting your provider to create a new phone number and disclose it only to trusted family and friends;
- Occasionally vet internet presence by searching yourself using various search engines. This may reveal long-forgotten information that exists online. Examples include school, church, or community websites that may contain your contact information;
- Online privacy is only as strong as your weakest link. If the necessary steps are taken to increase protection, but your network of friends and family haven’t adopted best practices, they may be inadvertently compromising your personal safety (e.g., tagging you in images). Consider discussing these issues with them.

## Conclusion

While the internet has many pitfalls, it’s an important (and unavoidable) part of everyday life. Becoming aware of the risks involved in navigating this digital space is a key skill that everyone can benefit from.



Legal Language:

© 2022, Canadian Centre for Child Protection Inc., 615 Academy Road, Winnipeg, Manitoba, CANADA. Information current as of April 06, 2022. All rights reserved, except you may download and print copies for personal use, and if you are directly assisting another person, you may download and print copies for use for you and the person you are assisting.

“CANADIAN CENTRE for CHILD PROTECTION” is registered in Canada as a trademark of the Canadian Centre for Child Protection Inc. All other trademarks are the property of their respective owners.

Safety and privacy tips, and all other information provided herein, is intended as general information only. Readers should consider and assess all information in light of their own circumstances and seek external advice as needed.

Any external website or service referenced in this document is not owned, controlled or in any way associated with the Canadian Centre for Child Protection Inc. (“C3P”). C3P does not make any representations or warranties as to the accuracy or security of these websites or services. Use of the site or service is at the risk of the user.

