North Vancouver City Library

Intro to Online Privacy and Security

What is Online Privacy?

Online privacy relates to your online information. It involves how information about you is being displayed on the Internet. It also involves how your online information is being used. For example, is it being stored, repurposed and provided to third parties? You might be concerned about:

- What information is visible to your family and friends?
- What can your employers find out about you?
- What information does the government have access to?
- Which companies are selling information about your likes and dislikes?
- Is your data safe from hackers?

Your Online Identity

To get an idea about what personal information is available online, search for your name using the following tools:

- Google www.google.ca
- Facebook www.facebook.com/people-search.php
- Canada 411 www.Canada411.ca

Choose What You Share

Before you post anything on social media, think carefully:

- Is this something I want shared publicly
- What do people think about me when they see this?
- Who is my audience?
- What harm can it cause?
- Can something on social media really be removed?

Learn to Manage Your Privacy Settings

Instagram:

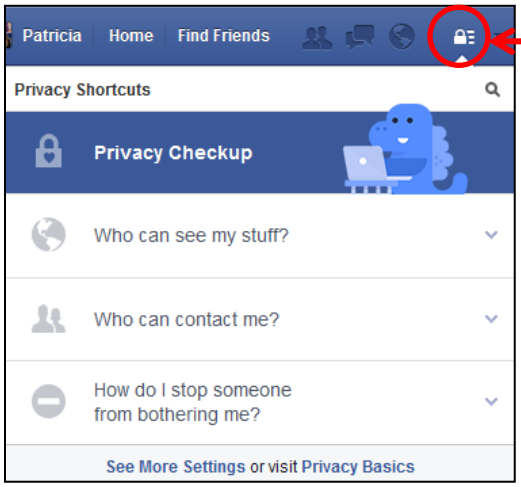
- Instagram is designed for use on mobile devices, so changes to account settings need to be made there.
- Setting your Instagram account to private will not affect existing followers – they will have to be blocked individually.
- Private posts you share to social networks will be visible to the public as per your privacy settings for those networks.

North Vancouver City Library

Pinterest:

For help with privacy settings for your Pinterest account, visit
https://help.pinterest.com/en/articles/edit-your-account-privacy

Facebook:



You can do a "Privacy Checkup" on Facebook. Simply click on the lock icon on the menu bar to start. From here, you can:

- Manage your audience
- Place limitations on who can contact you
- Block users who are bothering you

NOTE: Even if you are using the strictest of privacy settings, you should still consider anything you post on social media public, because you cannot control what your audience does with the information and images you post.

Terms of Use and Privacy Agreements

Whether we read them or not, by agreeing to the Terms of Service on a website we are:

1. Placing control over how we are represented in the hands of the service provider.
2. Agreeing to the rules / codes of conduct laid out by the service.

Typically, terms of use and privacy agreements contain information about how your data is used and distributed, and who owns the content you post.

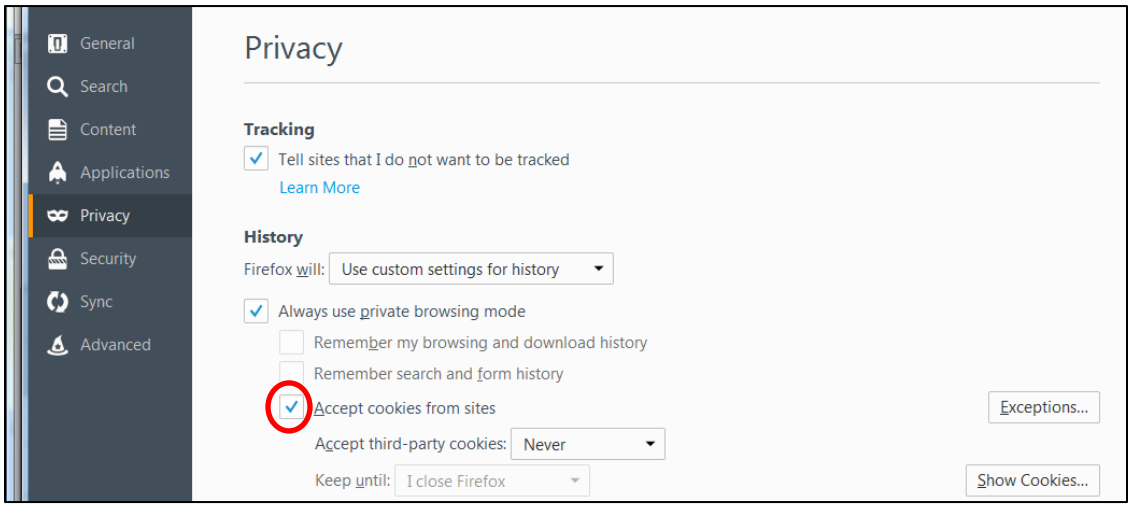
Cookies

A cookie is a "text file that is dropped on your web browser by a site you visit" (from *Do Not Track*, Episode 2). While not harmful itself, it can be used to track your activity on the Internet as you move between various sites. For this reason, it is important to know how to block (and unblock) cookies on your browser.

North Vancouver City Library

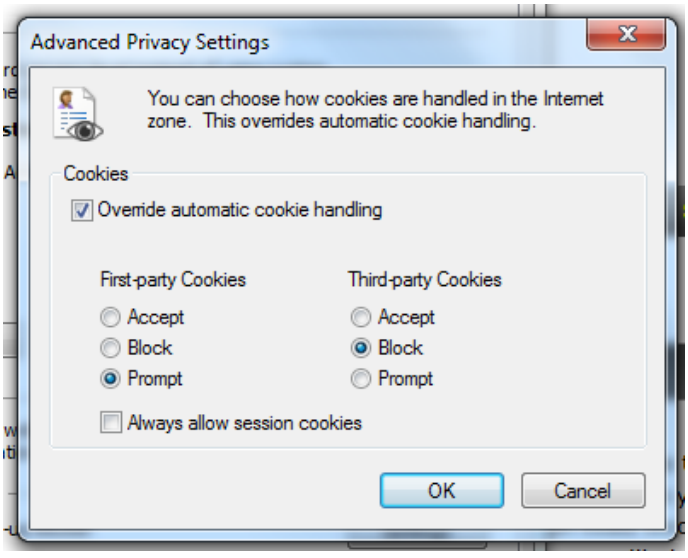
Block Cookies on Firefox

Menu-> Options -> Privacy tab -> Uncheck "Accept cookies from sites":

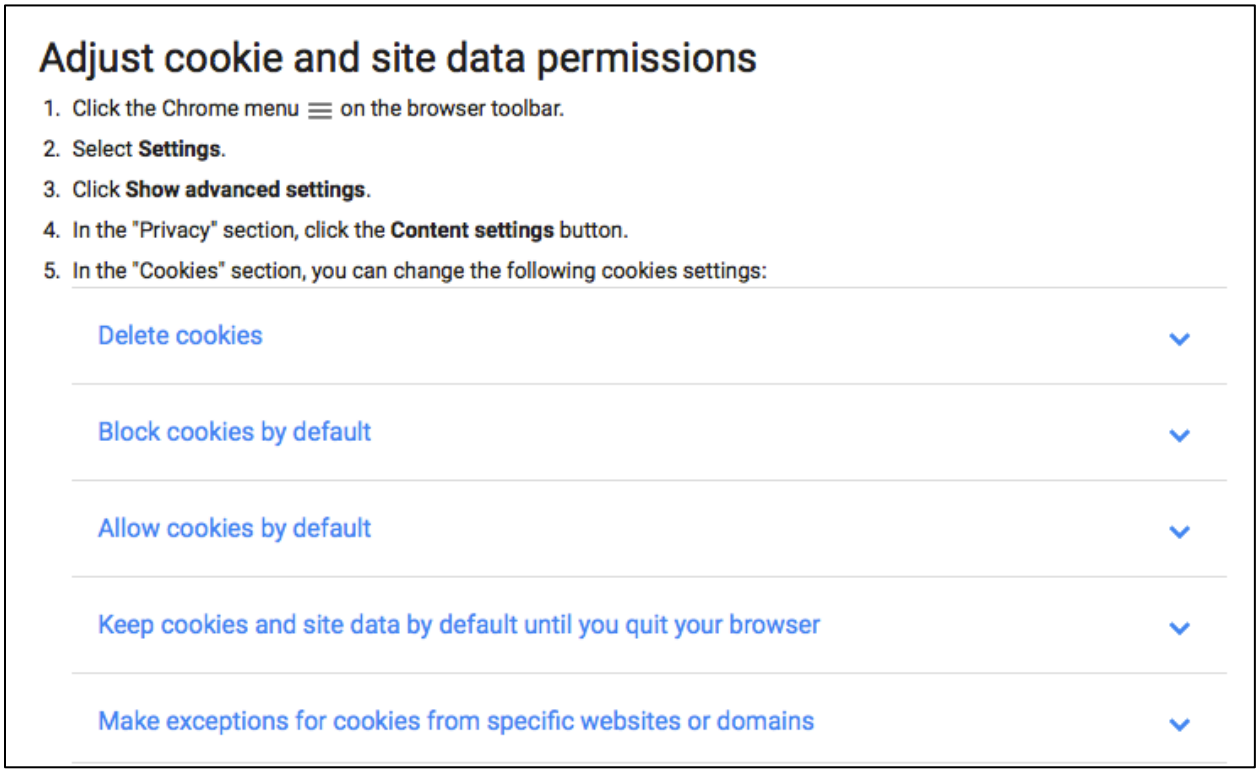


Block Cookies on Internet Explorer

Tools -> Internet Options -> Privacy tab -> Settings -> Advanced -> Uncheck "Override automatic cookie handling," customize your cookie handling -> OK



Block Cookies on Chrome



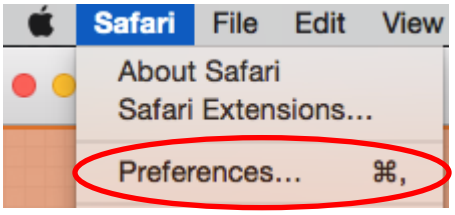
Adjust cookie and site data permissions

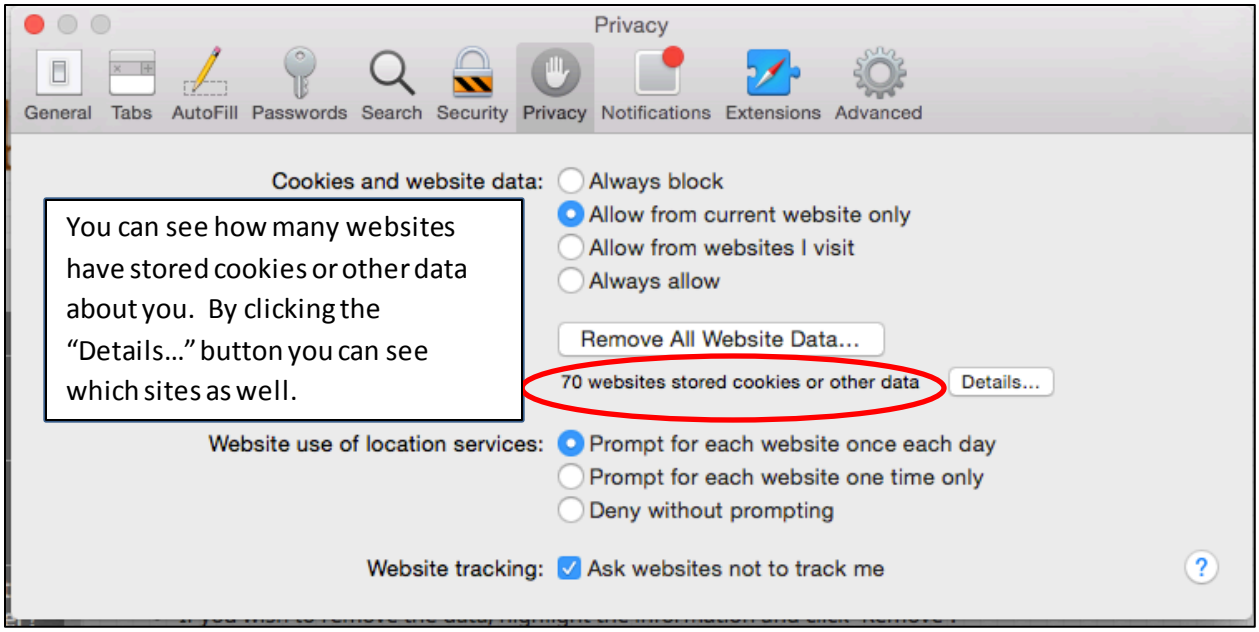
1. Click the Chrome menu ≡ on the browser toolbar.
2. Select **Settings**.
3. Click **Show advanced settings**.
4. In the "Privacy" section, click the **Content settings** button.
5. In the "Cookies" section, you can change the following cookies settings:

- Delete cookies
- Block cookies by default
- Allow cookies by default
- Keep cookies and site data by default until you quit your browser
- Make exceptions for cookies from specific websites or domains

Block Cookies on Safari

From the Safari menu, choose, Preferences. In the Preferences window, click Privacy and choose your desired settings.





What is Online Security?

- Protecting yourself from identity theft
- Protecting yourself from scams
- Online shopping safely
- Visiting secure websites

Passwords

Tips for creating passwords:

- They should include different kinds of characters: numbers, letters, capitals, special characters
- Don't use the same password for everything
- Change your passwords often

Here is a list of the most commonly stolen in 2014: http://gizmodo.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951 If you see your password on this list, CHANGE IT.

Protect Yourself From Online Identity Theft

Identity thieves are on the lookout for:

- Name
- Date of Birth
- Address

- Social Insurance Number
- Employment Information
- Driver's License #
- Credit Cards, Debit Cards
- PIN #s
- Mother's maiden name

Safe Online Shopping

- Make sure the you see **https** at the beginning of the address.
- Use PayPal or another payment gateway that hides your credit card number, if possible.
- Use a secured network when sharing personal information like your credit card.
- Online fill out mandatory fields.
- Do not "remember my password" when registering.
- Log out when you are finished.

Protect Yourself from Online Scams

- If possible, don't click links sent via email.
- Don't send financial information by email.
- If you receive an email from a company asking you to call a phone number, confirm the number before you call.
- Do not respond to texts or emails telling you you have won something or inherited something

Protect Your Smartphone

- Use a passcode: A PIN or password can prevent others from unlocking your device.
- A fraudster needs only three pieces of personal data to steal your identity. Don't put important data on your phone / device (this includes calendar / notes).
- Use encryption: Encryption scrambles phone data so it can't be read by unauthorized users. iPhones encrypt data by default when you turn on a passcode. On Android devices, you often have to turn on encryption separately.
- Scrutinize permission requests: Many apps, particularly on Android, ask for more permissions than they necessarily need. On iPhones, you can block apps' access to particular features or data. On Android, you may have to simply avoid certain apps. Don't let apps save your password.
- Stick to official app stores: Most smartphone malware is being distributed through third-party app stores, typically in places like Russia and China. Apple and Google, by contrast, have done a good job of keeping bad apps out of their stores.
- Use 'find my phone' features: Apple's Find My iPhone and Google's Android Device Manager help users locate lost phones and allow them to delete data from stolen ones.
- Run the latest OS. Updates will often make the device more secure.
- Add In Case of Emergency (ICE) information to your lock screen.

North Vancouver City Library

Resources for further help

- At NVCL:
  - www.nvcl.ca > Using the Library > Technology Training > Computer Classes > Intro to Online Privacy and Security > Class Resources
  - Online Books: www.nvcl.ca > Research & Learn > Databases A-Z > Safari Books Online *(look for "online privacy security")*
  - Set an appointment with a library staff member: 604-982-3941 or techconnect@cnv.org
- Online:
  - Media Smarts: www.mediasmarts.ca
  - Do Not Track (online documentary): https://donottrack-doc.com/en/intro/
  - CBC article: http://www.cbc.ca/news/technology/how-to-stay-safe-with-a-smartphone-1.2553592