



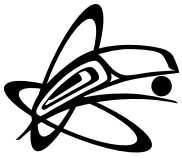
A Safer Way to Browse the Web

Prepared by Brian Burciaga
Intern, First Nations Technology Council

A personal report offering practical guidance for safer and more private web browsing. The views and recommendations are the author's own and do not represent an official position of the First Nations Technology Council.



First Nations
Technology Council



● Introduction

If you learn about the history of the Internet it wasn't built with security in mind. Everything was an open book. Years later there has been added tools and technologies to make the internet safer. However, it doesn't mean its fool proof.

In a report from the Canadian Government, they mentioned how the elderly are at risk of fraudulent attacks by scammers. They can be phone calls, emails, and ads on platforms like YouTube and Facebook. [1]

Adaptive Office Solutions claimed in an article that smaller entities, e.g. community and non-profit organizations, are vulnerable to Cyber Attacks. This is partly due to the lack of resources in having a robust security system for their organizations. [2]

Internet Service Providers collect information regarding your online activity. Rogers privacy policy mention collecting information about your devices identifiers like an IP address and IMEI, which are used to find your device. With WiFi usage they also track data regarding network traffic destinations from websites or mobile apps. The last one is all the URLs, i.e. websites, you visited on the web. [1]

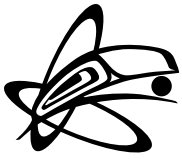
It's commonly known that Facebook and Alphabet (Google) use ads to make profits. However, bad actors have used their platforms to serve malicious ads to people. This results in phishing scams to steal peoples accounts, money, or identification. I've seen these types of ads on YouTube.

We give these organizations our data and let them serve us ads. However, with this data they train on it and sell it to the highest bidder. Yet we get malicious ads or no data ownership. [2]

People will say, "if you got nothing to hide, you have nothing to fear". However, I believe this is a wrong way to think. There was prohibitive legislation early in Canadian history. This led to the banning of some ceremonies like Powwows. However, Indigenous people in Canada decided to host them in order keep the tradition alive. It's not that they had nothing to hide, but were forced to hide it. They used any means necessary to keep our cultural history alive. Now we don't have to worry about that being an issue, but what if legislation dictated some information or messaging was deemed "dangerous". It may seem far-fetched. However, it wasn't long ago that Powwows were deemed an "Indian Offence". [3]

With this in mind I believe it's important to make an effort to help protect yourself from bad actors, either being scammers or large tech corporations.





● Web Browser

Google has been constantly working towards blocking ad blockers on the Chrome Browser. So usually, I go with other browsers because they can offer a more personalized or safer browsing experience. There are many options, but the main ones I focus on are Brave and Firefox.

Brave is a forked copy of Google Chrome, i.e. the foundations of the browsers are the same. However, the people behind Brave have added features to the browser to help with data privacy and safer browsing. They have a built-in ad blocker for the browser that will also block popups. A VPN is also attached to the browser which I will talk about later. They have their own Search Engine and AI tool with privacy and non-ad search results.

<https://brave.com/>

The other browser I recommend and use is Firefox or Firefox based browsers. For simplicity of this topic I will just talk about Firefox. Unlike Brave it is built on a different foundation. Firefox recently added a built-in free VPN to their browser, but you need to install an Ad blocker as an extension.

<https://www.firefox.com/en-US/>

● Ad Blockers: More Than Just Annoyance-Free Browsing

From the info above ads don't provide much value. Maybe you can get a good recommendation, but a lot of advertisements are malicious as well. Ads can be so egregious that the FBI has literally recommended people to install ad blockers for your safety. This is partly because Ads can include Popups in the browser, which can lead to more malicious sites. [6]

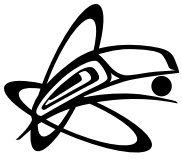
NOTE: The original FBI resource for their announcement was taken down, but there are articles talking about the announcement

The one Ad Blocker I choose is uBlock Origin. It allows for custom filters to also block unwanted sites and is available on the mobile version of Firefox.

<https://www.firefox.com/en-US/>

If you want a simple pick up and go option I would choose Brave, otherwise you can choose Firefox.





● VPNs: Encrypting Your Connection

Virtual Private Networks (VPNs) are not an end all be all to be "invisible" online, but it definitely does make an impact to your network traffic. A VPN is able to encrypt your traffic to websites from your ISP. This helps protect your data from being tracked by corporations. Another thing a VPN can do is hide your IP address. This adds an extra layer of protection for your device's location. Some VPN providers do however give your information to data brokers so you need to know which one to choose from.

VPNs can be useful for public WiFi locations like Coffee Shops or Hotels. Not all business's actually use standard network safety practices. This can be a concern especially if you need to log into your bank account or something important. Having an encrypted connection can circumvent these safety concerns.

Personally, I recommend two main providers. ProtonVPN is a subset of a larger suite of tools from Proton, but you can use their VPN as a guest user for their free access. They claim a no logs policy and I've been a customer of theirs for years.

<https://protonvpn.com/what-is-a-vpn>

Mullvad VPN mainly serves a VPN service to users. They don't ask for account registration, instead you generate a random account number. After, you are able to top up the number of months you would like to use for that account with any payment method. I've also used their VPN in the past and highly recommend.

<https://mullvad.net/en>

● Final Thoughts

I believe these topics are a good way to start your journey in taking back your privacy! Once you've set up some of these options, you'll be on your way to being able to browse the web in a safer way. They can't prevent all malicious attacks, but it can greatly reduce the risks of surfing the web.

● Resources

[1] <https://canada.ca/en/canadian-heritage/campaigns/harmful-online-content/what-we-heard-online-safety.html>

[2] <https://adaptiveoffice.ca/blog/cyber-security-awareness-for-canadas-indigenous-communities/>

[3] <https://rogers.com/support/privacy/rogers-privacy-policy#how-why-we-collect-personal-information>

[4] <https://cybersecuritynews.com/hackers-exploiting-companies-google-ads-accounts/>

[5] <https://thecanadianencyclopedia.ca/en/article/history-of-powwows>

[6] <https://tomsguide.com/news/the-fbi-now-recommends-using-an-ad-blocker-heres-why>