News, Resources and Useful Information for the Online Investigative and OSINT Professional from Toddington International Inc.

Toddington International Inc.

Online Research and Intelligence Newsletter

FEBRUARY 2019 EDITION

In This Edition

Welcome to the Newsletter

Welcome to the February 2019 edition of the newsletter.

In this edition, we have a guest article contribution from Jacob Roach, the Deputy Editor of Cloudwards.net, who regularly writes about today's Web technology, with a main interest in online privacy. In his article, "*Anonymous Browsing Guide: Silent Online Runnings in 2019*," he explains the importance of anonymous browsing in today's online climate, including how our online activities are tracked by browsers. More importantly, he explains how we can secure our browser, social media, and internet connection.

Also in this newsletter, we share our monthly round-up of online investigative and security tools, and our favourite industry-related articles that our team has found to be of particular interest.

E-Learning Graduates

Congratulations to the following students who are among the latest to have

TODDINGTON INTERNATIONAL eLEARNING
INTERNET RESEARCH SKILLS FOR FINANCIAL INVESTIGATORS
USING THE INTERNET AS AN INVESTIGATIVE RESEARCH TOOL

- Barbara Bieniek
- Lydia Chang
- Patricia McGratton
- Cat Williams
- Michael Thomas
- Selene Spence
- Rick Hamilton
- Megan Leigh
- Jeff McLachlan
- Faye Arsenault
- Khauola Barakat
- Kim Yiu
- Mark Summers
- René Cote

"This course as a whole has completely exceeded my expectations. I thought it would either be aimed at a lower, very basic level that I might not learn much from, or that it would be too technical and I would struggle to grasp the content. Instead, the content was extremely relevant to me and I have learnt valuable skills that are already in demand within my organisation. All detectives and intelligence officers would benefit from this course."

Congratulations to the following students who have successfully completed our 40-hour online Intelligence Analysis Methods training this month:

- Elizabeth Martin
- Brianne Todd

Important Note: As we respect the privacy of our students, we only publish the names of students who have provided express permission to do so. Many of our students are unable to share their completion due to the nature of their employment, or due to online privacy concerns. If your name did not appear in the above list and you wish to announce your completion of an online course with TII, please contact us.

Anonymous Browsing Guide: Silent Online Runnings in 2019

By Jacob Roach, Deputy Editor – Cloudwards.net

As our world of tech becomes more interconnected, and messier as a result, privacy becomes a bigger concern. With tech titans such as Facebook playing fast and loose with people's data, the integrity of the companies we trust with our data has to be questioned. That's even ignoring the obvious privacy issues that come with internet service providers and government spying, too.

In this anonymous browsing guide, we're going to arm you with the knowledge and tools to protect your personal data from dubious collection practices and shady sales. After taking the steps we suggest, you'll not only be able to enjoy a more open internet, but also one in which you don't have to look over your shoulder.

Before diving into the specifics, you need to know this: there is no bulletproof way to be anonymous online. Though we're here to help protect you from the malicious data collection and exploitation that exists in our online world, the fact that you're using the internet means that you can't be safe from everything.

If you want true anonymity, close your browser and throw away your computer.

Though you can't be safe from everything, you can be safe from most things. True anonymity is a pipe dream, but you can block malicious advertisements, tracking beacons, network snooping and more. The purpose of this guide is damage control.

Why You Should Browse Anonymously

Though it’s easy to chuckle at the ridiculous questions congressmen and women ask tech titans, such as Mark Zuckerberg and Sundar Pichai, they aren’t on Capitol Hill without reason. Most websites, including Facebook and Google, use trackers to log how you interact with them. Those trackers can even follow you across websites.

Companies use the data to better sell advertisement space, get a hold on their demographic or just see what features may be useful on their website. Of course, the collection is usually outlined in the privacy policy and you’re agreeing to the privacy policy by using the service.

It seems wholesome when put in that light. The line between simple audience research and malicious data mining is blurry, though. A viral story on Forbes, for example, shared how Target knew a young girl was pregnant before her father did.

After shopping online and buying certain products from Target, its automated system determined the girl may be pregnant and started sending advertisements to her home, where she lived with her father. Outraged, the father stomped down to Target, claiming its marketing team was encouraging his daughter to get pregnant. It turned out that she already was.

That type of data mining and profile attribution is underscored in the New York Times article “how companies learn your secrets.” Marketers want the dirty details about you and they want to gather them without your knowledge. Privacy policies are hard to decipher, rife with legalese and designed to let organizations build as detailed a marketing profile about you as they want.

no one has held the U.S. National Security Agency accountable during the six years since. Some European countries have better privacy laws, but many are just as bad if not worse.

Plus, it's creepy. Even without the world of Philip K. Dick looming above, data collection and tracking is immoral and gross. To make matters worse, even your browser tracks more data than you may think.

How Browsers Track You

Most people are familiar with cookies. On the web, cookies are meant to provide a mechanism for websites to remember information about a user and log their browsing activity. For example, cookies are used to store your email address at login or remember certain attributes about when you last browsed the website.

First-party cookies, which are made and implemented by the website you're browsing, are exclusive to the party that runs the website. That said, you'll also find cookies from third parties that track you across multiple pages. Usually, they are injected through ad networks.

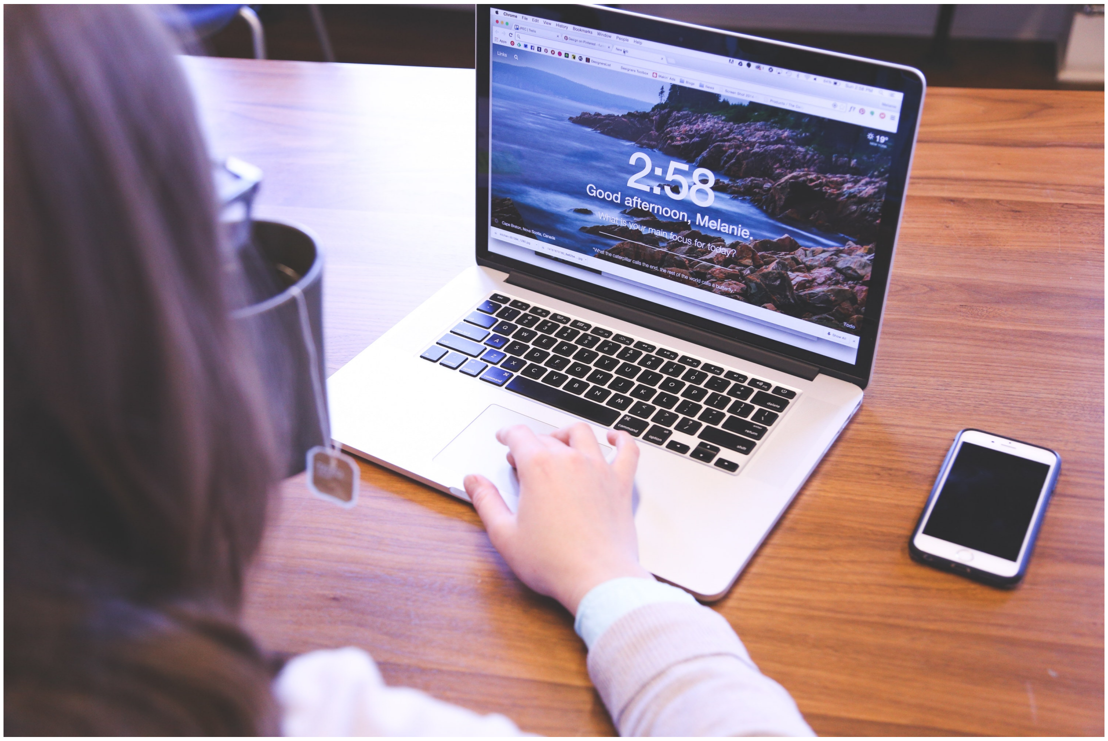
For example, let's say you go to a website that had Google AdSense ads in the sidebar. You then leave that website and go to one that sells audio equipment. That company sells advertisements to Google AdSense, so, for a week afterward, you see a sale from that company before every YouTube video you watch.

name, credit card information, address, age and much more. If you want to know the details about what your browser sends, we recommend running a scan with Panopticlick.

Even without giving away personal data, you can be identified through browser fingerprinting. Your browser sends a lot of metadata with each request, including your operating system, browser plugins, screen resolution, language, platform, system fonts, time zone and more. Combined with your IP address, that can be used to determine where and who you are.

We ran a test with all privacy protection turned off for this guide. Panopticlick found that our browser fingerprint was unique among the 154,045 tests ran during the prior 45 days.

Securing Your Browser



The first step toward browsing anonymously is securing your browser. Though doing so won't protect you from the spying done by the government and your ISP, it can protect you from the malicious data collection by websites around the web.

Block Browser Data

If you want to go easy mode, it's worth it to ditch your browser and use a secure one, such as Brave. However, Chrome is still the most secure browser out of the big three, and there are tools you can install to help make it even more so.

The first tool is an ad and tracker blocker. You can read our guide to the best stores. Though it does what it does well, uBlock Origin also shows the fewest number of privacy leaks out of top ad blockers.

uBlock Origin isn't the prettiest or easiest ad blocker to use, though. If you're looking for more options, read our piece on 99 free tools to protect your privacy.

There are a few other extensions you can install besides an ad blocker. For example, Privacy Badger is a tool for blocking invisible trackers across websites. It was developed by the Electronic Frontier Foundation — the creator of Panopticlick — and sends a Do Not Track signal whenever a cookie attempts to track you.

EFF also provides HTTPS Everywhere, which forces websites to load encrypted pages. Many websites default to unencrypted HTTP pages or redirect requests to unsecure domains. HTTPS Everywhere changes the requests you're sending to only load encrypted webpages.

There are a lot of privacy extensions, but most boil down to ad and tracker blocking. Experiment with different ones if you want and double-check if they're working with Panopticlick. If you don't want to go through the hassle, our recommendations should serve you well.

Hide your Kids, Hide Your Passwords

Browsers have become more sophisticated as the number of accounts users stored with them has increased. That said, your browser's built-in password manager is the worst thing you could be using. Though Safari's integration with iCloud Keychain is better than Chrome's password storage, a dedicated password manager is better than both.

Password managers let you store, organize and fill your passwords online. They provide convenient access to your account credentials and help you stay more secure online by avoiding cybercrime. Because you have a dedicated spot to store your passwords, you can use long, unique combinations for your accounts, making it much harder for a hacker to access them.

The best password managers store your information in encrypted form, too, so it's next to impossible for a hacker to break in. Our top choice is Dashlane for its ease of use, superior password security and slew of features. You can learn more about it in our Dashlane review.

If you don't have the money, LastPass is the best free password manager. It comes close to Dashlane — you can see how close in our Dashlane vs. LastPass comparison — but, as you can read in our LastPass review, there are security breaches on record.

There are many reasons to delete your search history, but it’s an annoyance and can easily fall into the category of things you wish you did but never kept up with. Instead of doing it manually, the better option is to use a search engine that doesn’t keep your history in the first place.

Search engines are among the most data-hungry services on the web, with Google being a particularly terrible offender. Privacy-focused search engines usually use Google, Yahoo and Bing to combine results and display them for you. Because nothing is gathered about you, the results aren’t personalized, either.

Perhaps the most famous privacy-focused search engine is DuckDuckGo. In addition to providing its services for free, DuckDuckGo is a strong defender of privacy and has donated over $1 million to various privacy organizations over its 11 years in business. You can make it the default search option in Safari and Firefox, but, unsurprisingly, Google has not integrated it.

Securing Your Social Media

If you want to be anonymous, you shouldn’t have social media. If you run a business or want to connect with friends and family, it’s a necessary evil, though. Most of the steps for securing social media are the same as securing your browser, so make sure you start there.

If you’re using a tracker-blocking plugin, you should be covered on social media.

Phony security answers, birth dates and addresses are good ways to throw a wrench in the data collection machine.

There’s a unique aspect to social media, though: external links. There’s a ton of — wave your hands with us — fake news on social media. Though the Zuckerbergs of the world are cracking down on it, you’ll still have to use your judgment to separate what’s real and what isn’t.

Thankfully, there are tools that can help you do that. Windscribe, which is the best free VPN, includes a tool that allows you to check links before clicking them. It will show you information like the number of ads and trackers on the page, and give you an overall score for privacy. You can learn more about that in our Windscribe review.

Securing Your Internet Connection

Now that your browser and social media are locked down, it’s time to secure the source. No amount of browser extensions and tracker-blocking can protect the data that flows through your ISP and, with internet providers selling user browsing history, that’s a scary thought.

Many people think using a proxy is the best way to secure your connection, usually because free ones are available. As explained in our VPN vs. proxy vs. Tor guide, proxies are best when used for low-risk web tasks where you want to mask your IP address. They’re a bad option, though, because they don’t provide encryption and can come with unintended consequences.

the request to your ISP and the larger web. VPN security is a complex topic, but for the purposes of this guide, it's the best way to secure your internet connection.

The best VPN providers offer top-notch AES 256-bit encryption and strict no-logging policies. In short, instead of routing requests to your ISP's DNS servers, the requests are sent to the VPN provider for routing. Since no logs are kept there, you essentially become invisible when using the internet.

Unfortunately, it's not as simple as choosing a VPN that claims it keeps "no logs." Providers such as HideMyAss and IPVanish claimed not to, then were found to be lying in court. You can learn about those incidents in our HideMyAss review and IPVanish review.

The providers we rank highly in our VPN reviews, have proven that they don't keep logs, though. Our top pick is ExpressVPN for its ease of use, security and strong stance on privacy. You can learn more about it in our ExpressVPN review.

Final Thoughts

Though using the internet is going to compromise your anonymity, you can take steps to secure most of your personal data. The most offensive practices are cross-website tracking and data collection by ISPs and government agencies. Thankfully, you can fight against both.

Ad and tracker blockers will take you some of the way, but a VPN is an essential tool for online privacy. It protects everything at the source, so you won't have to worry about requests slipping through the cracks and exposing your identity.

What steps are you taking to protect your browsing?

***About the Author:** Jacob Roach is the Deputy Editor of Cloudwards.net, who regularly writes about today's Web technology, with a main interest in online privacy. To learn more, visit Cloudwards.net or email Jacob. To view the original article at its original post location, please visit www.cloudwards.net/anonymous-browsing-guide.*

Upcoming Select Public Courses

Advanced Internet Intelligence & Online Investigations

Aimed at managers, frontline investigators, researchers, and analysts alike, this advanced training program will provide detailed instruction on effectively using the Internet as an Open Source Intelligence, research, and investigation tool. Demonstrating advanced search and analysis techniques for mining Web-based and social media information, this comprehensive training program will also examine a number of essential privacy tools for ensuring data, communication, and online security. Techniques being used by the criminal element to conceal their identity, location, and illegal behaviour will also be introduced.

March 18-19, 2019, Toronto, ON

March 25-26, 2019, Vancouver, BC

September 8-11, 2019, Cambridge, UK
(3-day course and evening social, in partnership with the International Chamber of Commerce, Commercial Crime Services)

Social Media Intelligence & Investigation

To recognize, collect, and leverage the value of social platform-sourced information, research and investigative professionals must fully understand the restrictions and implications of obtaining and utilizing such information in a manner that does not violate user privacy expectations, license agreements, and other legal limitations. This course will introduce research and investigative professionals to a variety of innovative tools and techniques that will enable you to locate, collect, and utilize social platform-sourced information, while considering the implications of leveraging this type of information safely, quickly, and appropriately.

May 16-17, 2019, Vancouver, BC*

**Only a limited number of seats are available at the early-bird rate, based on a first come, first served basis. Sign up early to receive the discounted pricing.*

Australia- & Asia-Based Training

We will also be in Australia, Hong Kong, and Singapore for training in the upcoming months. For dates, locations, and pricing information, please contact us.

TII is pleased to offer a number of specialized and customizable in-house training programs for both the public and private sector in a variety of formats. We also have available a number of expert speakers available. To learn more about what we can do to empower your workforce, contact us.

Resources for the OSINT Professional

https://www.lastpass.com – Generate strong passwords for all of your accounts to ensure account security and manage them with LastPass, the password manager used by over 16.5 million people

https://hide.me/en/proxy – Free, web-based proxy/VPN for anonymous browsing

https://brave.com – Privacy-based browser that does not view or store browsing data, protects against malware, and prevents tracking

https://justice.gov.bc.ca/cso – BC Court Services Online: search traffic, criminal, civil, and appeal court records in British Columbia

https://www.scrible.com – Ad free website annotation tool that allows you to save and bookmark pages and mark up as needed

https://signal.org – Secure messaging app available as an alternative to chat apps like WhatsApp from malware, viruses

https://adblockplus.org – Browser extension that blocks ads, pop-ups, and trackers, available for Firefox, Chrome, and Operator

https://search.disconnect.me – Search engine that does not track searches or share user data, with built in DuckDuckGo search

https://browserleaks.com/webrtc – Find out what identifying or personal information your browser is leaking

https://wetransfer.com – File sharing website that allows users to send unlimited files, up to a maximum of 2GB at a time

https://scholar.google.ca – Google's search tool for locating only scholarly literature

https://10minutemail.com – Disposable email service, perfect for confirming online accounts

https://www.zamzar.com – Free online file converter, available for extensive file formats

Follow us on Twitter for our "resource of the day", or visit our Free Open Source Intelligence Resources page to see more resources like these.

More Online Training

Open Source Intelligence for Financial Investigators

40-Hour E-Learning Program

Essential for all financial institutions and corporations required to comply with the *European Union Fourth Anti-Money Laundering (AML) Directive* and similar legislation, or otherwise engaging in enhanced due diligence activities, this comprehensive training provides financial and business professionals with the latest tools and techniques required to effectively gather online OSINT, with the aim of enhancing compliance activities and minimizing potentially detrimental risks to an organization — both quickly and accurately. **Sign up or learn more here.**

This course was tremendously beneficial and relevant. It provided me with a robust set of skills to assist our member countries in fighting all types of illegal

Introduction to Intelligence Analysis

40-Hour E-Learning Program

This program provides a rich and interesting opportunity to explore the key concepts and intellectual foundations which inform intelligence analysis activity. Students will develop awareness of, and experience in, using common tools and methodologies to conduct analysis assignments, as well as learn how to fashion one's insights and ideas in a way that communicates effectively to clients and other intelligence consumers. **Sign up or learn more here.**

Criminal Intelligence Analysis

40-Hour E-Learning Program

This program is designed to equip aspiring and inexperienced analysts, as well as other interested law enforcement and investigative professionals, with the knowledge and skills required to undertake criminal intelligence analysis work, and to understand criminal intelligence analysis products when encountered. **Sign up or learn more here.**

Strategic Intelligence Analysis

40-Hour E-Learning Program

This program is intended for professionals working in public sector enforcement, intelligence, national security, and regulatory compliance roles, or those aspiring to do so. Students will be equipped with the skills and knowledge required to effectively conceive, plan, and implement strategic analysis projects, and deliver impactful strategic advice to clients and other end users. **Sign up or learn more here.**

"How-Tos" and Articles of Interest for the OSINT Professional

"How to Visualize Your Google Location History"

"A handy list of ways Facebook has tried to sneakily gather data about you"

"Facebook Privacy Setting: A Quick & Easy Guide for 2019"

"Google+ is Officially Shutting Down on April 2nd"

"What Does Your Credit Card Company Know About You?"

"The best VPN services: Our 10 favorite vendors for protecting your privacy"

"WhatsApp restricts message-sharing to fight fake news"

"Study: On Facebook and Twitter your privacy is at risk -- even if you don't have an account"

"How to Delete Your Online Accounts but Keep Your Data"

"Five Ways to Easily Convert Audio Files to Text"

Fake news spotter: How to enable Microsoft Edge's NewsGuard

“Google Chrome to Warn Users About Imposter Sites With Lookalike URLs”

Google to give political parties anti-hacking tools in time for EU elections

Facebook to integrate WhatsApp, Instagram and Messenger

"Why I'm Worried About Google"

Four out of five Americans distrust mainstream social media sites like Facebook

Follow us on Twitter for daily articles and other interesting industry updates.

follow on Twitter | friend on Facebook | forward to a friend