TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

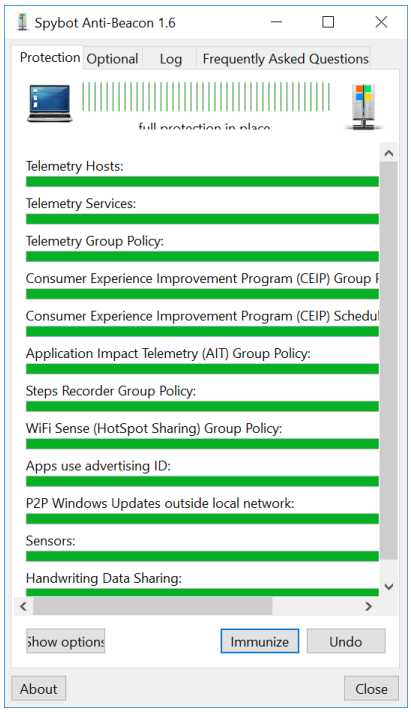
In the News:

- Blind Trust in Email Could Cost You Your Home
  - Krebs On Security
- Secure Messaging Showdown: Signal vs. Whatsapp
  - Lifehacker
- Senate Staffers' ID Cards have PICTURE of Smart Chip but no Security
  - Ars Technica
- 10,000+ Advanced Computer Infections Might be NSA Backdoor
  - Ars Technica
- Imposter Websites Now Harder to Detect Thanks to "PunyCode"
  - Ars Technica

Spybot Anti-Beacon

Defeating Windows 10 Telemetry

We have been disappointed in the tracking mechanisms that are built into Windows 10 and previously we have discussed **O&O ShutUp10** as a way to limit some of this tracking. Windows 10 introduced a number of telemetry tools that sends data about users back to Microsoft that is collected, analyzed, and used for a variety of purposes. Some of these purposes can be considered acceptable use, like improving product performance, but much of it is used to served targeted advertisements. We recommended opting out of this data collection to the maximum possible extent.



We recently tested a new anti-tracking tool from Spybot called Anti-Beacon. **Spybot Search & Destroy** is one of the more reputable anti-malware tools on the market for Windows computers. It has been around for a very long time and has a strong reputation for rooting out malware infections. With this in mind we had high hopes for how Spybot Anti-Beacon would do and we were not disappointed.

Spybot Anti-Beacon is a very simple tool. It requires very little interaction from the user. Download and install the application, and once it is installed it will begin working. To enable full protections, click the "Immunize" button at the bottom of the interface.

In addition to providing realtime protection against data tracking, SpyBot Anti Beacon also maintains a log of attempts to transmit data back to Microsoft. This provides a good visual indication of the data that is being collected behind your back. If you are running Windows 10 we recommend using SpyBot Anti-Beacon and **O&O ShutUp10**.

Wi-Fi Security & Privacy: SSIDs

Wi-Fi networks pose some risks to your security and privacy. They are incredibly convenient and most of us have them. The convenience that is so desirable for the user also makes it convenient to hackers and others trying to collect your data. In the next few issues we will cover all aspects of Wi-Fi security & Privacy, and we will begin this week by talking about the SSID.

The SSID (Service Set Identifier) is the name of your wireless network. This information is freely available to anyone coming into range of your network with a Wi-Fi enabled computer, tablet, or smartphone. The following are some basic security and privacy considerations you should take when choosing your SSID:

- Make sure it does not reveal information about you or your family members. You may be tempted to make your SSID something like "Johnson_wifi" but this reveals the last name of the occupants to anyone within range.
- Realize that Wi-Fi networks are mapped. Sites like **Wigle.net** map Wi-Fi networks into searchable databases. If your network has a distinctive SSID, it can be searched and located through such a database.
- If you would like to opt-out of network mapping totally, you can append the "_nomap" suffix onto your SSID. Using the earlier example, "Johnson_wifi" would become "Johnson_wifi_nomap"
- Understand the limits of hiding your SSID. You can make your SSID invisible to most devices, but it can be discovered with relatively simple tools.

Upcoming Events:

Law Enforcement Intelligence Units
May 1-5 2017, Bloomington, MN

Associated Locksmiths of America Expo
June 16-22 2017, Rosemont, IL

National Technical Investigators' Association (NATIA) Annual Conference
July 12-23 2017, Tampa, FL

BlackHat USA
July 22-27 2017, Las Vegas, NV

"Secret" Chrome URLs

Find Out What Chrome Knows About You

Google's Chrome browser is one of the most popular browsers in the world. We prefer Firefox and recommend it in our Data Protection and Non-Standard Communication courses because it can be easily configured for privacy and security. Chrome is very secure but is extremely difficult to optimize for privacy.

Some "secret" Chrome URLs were recently published that can give you access to the massive amounts of information that Chrome stores about you. This information is being collected at all times by the browser, but most users are really surprised to see it in black and white. The full list of URLs is available at: **https://fossbytes.com/complete-list-of-secret-chrome-urls-uses/**

The list of URLs is very long and we recommend you check all of them. We will point out a few that present some alarming information. To use these URLs, simply type the desired URL into the address bar and hit Enter.

⇒ **chrome://history**: This one isn't secret, but it makes your history easy to access and clear.

⇒ **chrome://device-log**: This can show you a list of serialized devices that have been attached to your computer. This is extremely sensitive information that makes your recognizable regardless of what other mitigations you are taking.

⇒ **chrome://view-http-cache/**: This will show the list of all the URLs you have visited, even if you are regularly clearing your history!

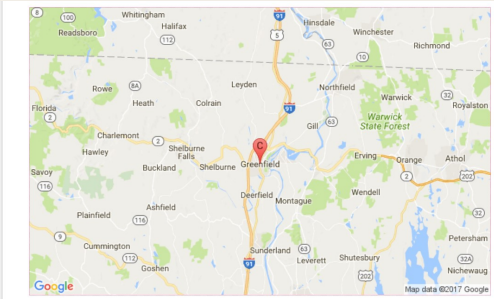
If you weren't aware of these "hidden" functions of Chrome, check it out. You might be surprised at what you learn!

Web Analytics

What Does Your Browser Know About You?

Last week we discussed three different websites that can be used to assess your exposure to data collection when you visit websites. We believe this kind of understanding is crucial. It helps you understand the collection that is happening on a daily basis, and it demonstrates how mitigations, like using a VPN and NoScript help to protect you. This week we are bringing you another website that provides information about what your browser knows. It is called "webkay" or "What Every Browser Knows About You". It is available at **http://webkay.robinlinus.com/**

This website is one of the most comprehensive of its kind and demonstrates the massive amount of data that can be collected when you visit a website. It will show you your geographic location (if you do not have a VPN enabled), the version of operating system, the browser you are using, and information about your computer's processor. It will also display your IP address, internet service provider, connection speed, and the previous page you were on. It can also display information about your social media accounts (if you are logged in), whether you are vulnerable to auto-fill phishing, and perform a scan of your entire network like some malicious websites will do.



Geo Coordinates: 42.587914999999995, -72.5994104
Location Name: 352-368 Main St, Greenfield, MA 01301, USA
Languages: English,
Local Time: Sun Apr 30 2017 11:29:46 GMT-0400 (Eastern Standard Time)

The site will also advise you on mitigations that will prevent them from seeing all of this information. In most cases a Virtual Private Network (VPN) and NoScript will prevent your information from leaking. The site actually recommends a web proxy, but we prefer the additional security afforded by a true, encrypted VPN. Just having an understanding of the information that is available to website operators is important to reclaiming your own digital privacy. Take a few moments to check out **http://webkay.robinlinus.com/** and see what information you are inadvertently giving up.

HTTPS Everywhere

Encrypt More of your Web Connections

The HTTPS (HyperText Transfer Protocol: Secure) is one of the most ubiquitous forms of end-to-end encryption on the web. Many sites have the capability to use this protocol. Using the updated Transport Layer Security (TLS), HTTPS is an incredibly effective tool for securing your traffic.

Unfortunately, many websites do not provide HTTPS connections by default. Many websites have the technology required to provide a secure connection, but it consumes slightly more bandwidth and resources to perform the encryption and decryption functions. With the **HTTPS Everywhere** browser extension you can force an HTTPS connection on any website with the required technology.

HTTPS Everywhere is available for Chrome, Firefox, Opera, and on Android. It also comes standard on the Tor Browser which is a testament to how respected it is. As HTTPS websites become more common, this protection will be come more and more important. The HTTPS Extension is free and is available at **https://www.eff.org/https-everywhere**. It is one of the most important browser extensions you can add to your suite of privacy-enhancing add-ons.

Over the next several issues we will use this section of the Digital Update to discuss the Firefox extensions that we recommend for security and privacy.

coming soon >>>

In Future Issues...

Internet Browser Comparison

⇒ ***Chrome, Firefox, Opera***

⇒ ***Mobile Browsers***

Firefox Setup Review

Browser Extensions