Cryptohippie's Guide To Online Privacy

The free Internet that many of us loved has become a surveillance web, serving governments and mega-corps, while abusing the rest of us. For those whose eyes are opening to this sad fact, we have assembled this guide.

This purpose of this document is to make Internet privacy as simple and concise as possible. Our intention is not just for you to understand, but for you to ***act upon*** the information we give you.

We will be giving you information that is as simple and clear as we know how to make it. We have included the minimum number of steps to take, but it will be up to you to **do** the things we explain to you.

We will be mentioning our own products in this guide, because they are relevant. We hope you like our stuff, but this document is not intended to push you into buying it.

Please do the things listed below. As we mentioned at the outset, the Internet has become a world-wide surveillance network. (And is becoming a manipulation network.) You need to protect yourself.

Let's get started:

Accept Software Updates: As much as there is reason to be leery of updates, it is necessary to take them. Every time a new security exploit comes along, operating systems (and some other programs) are upgraded to seal the hole. This is important.

Have a firewall: Your local machine needs to be guarded from local attacks. You don't have to pay big money for the "fix everything forever" firewalls, but you do need something. Zone Alarm makes a nice free firewall (including an outgoing firewall) and their upgrades provide anti-virus and protection for a very reasonable cost.

Have an outgoing firewall: If your regular firewall doesn't stop all outgoing data, get one. Little Snitch is an excellent outgoing firewall for Macs.

Have an anti-virus program: This is usually built into your firewall program, as it is in Zone Alarm.

Browser: Use Firefox as your browser. Also:

- Install and run the NoScript extension to manage your Java Script exposure. *In a Firefox window, follow this menu path: Tools > Add-ons > Extensions > search for NoScript*
- Install and run the Better Privacy extension to avoid nasty cookies. *In a Firefox window, follow this menu path: Tools > Add-ons > Extensions > search for Better Privacy*
- *Install and run the Priv3 extension to prevent cross-site tracking. In a Firefox window, follow this menu path: Tools > Add-ons > Extensions > search for Priv3*
- *Install and run the Certificate Patrol extension to manage SSL better. In a Firefox window, follow this menu path: Tools > Add-ons > Extensions > search for Certificate Patrol*
- Set Firefox to delete cookies on close. *From Firefox Preferences, choose Privacy, then Accept Cookies, then Until I Close Firefox*
- Set Firefox to NOT accept third-party cookies. *From Firefox Preferences, choose Privacy, then uncheck Accept Third Party Cookies*
- Set Firefox to Delete all browser data (except passwords) upon close. *From Firefox Preferences, choose Privacy, then Clear History When Firefox Closes. Be sure NOT to check Saved Passwords, Site Preferences or Offline Content*
- Turn off Geolocation: *Type* about:config *in the address bar, ignore the warning, scroll down to* geo.enabled*, double-click to change the default value to* False*.*

Email: Use the Thunderbird client for your email. STOP using webmail. Close your Google and Yahoo accounts. (Just do it.) Get a privacy-centered email provider. That means that they have no web interface (the one exception for webmail is Sciphered). They should not store or use your data, and they should clean your mail's headers. Use Cryptogroup, JumpShipMail, or Riseup.net.

You must also:

- Turn off Geolocation: *Get to* Advanced *settings (either via* Tools > Options *or* Preferences*), click the* Config Editor *button, ignore the warning, scroll down to* geo.enabled*, double-click to change the default value to* False*.*
- Do not load remote content. (Thunderbird will ask.)
- Don't allow add-ons.
- Do not allow delivery notifications.

- Don't let JavaScript run in your mail program: No plugins, no Java.

Hide your IP address: This requires:

- Tor, I2P or a good VPN.
- Multiple hops. (Not a cheap, single-hop VPN.)
- Out of band authentication.
- No single point of failure.

Full Disk encryption: If you run a Mac, use its File Vault disk encryption. If you run Windows you are are caught between a rock and a hard place. You could use Truecrypt version 7.1a, but there are serious doubts about its security. You could also use Bitlocker (which is included in most newer Windows versions), but it is unsure how secure it is, even against small institutional attackers. Instead of not using any fulldisk encryption, use one of these two. But please consider switching to Linux or BSD if your data is valuable and/or sensitive

Get text encryption: You can get PGP. It costs a bit, and you'll want to turn off all the extras, but it comes with support. Or you can get GPG (for Windows); it's free, and you can find install videos on YouTube.

Start using GPG and Enigmail: Thunderbird has a nice extension called Enigmail, that works with GPG to encrypt your emails, more or less automatically.

Chat: Stop using standard chat clients and use Pidgin. Enable OTR for chat, or chat inside of an anonymity network.

Change your machine address for mobile computing: Get Mac Changer to change your laptop's Mac address. For Windows.

Certificates: Firefox will handle these for you. Be careful, but not everything that gets flagged as an unknown certificate is dangerous. Read the warnings carefully; they usually explain the situation.

Voice: Ditch Skype, get Jitsi and sign-up with a free VoIP provider or with a provider that accepts anonymous payments.

Block Facebook and Twitter: Use the Priv3 extension to Firefox mentioned above.

Get ready to ditch Windows and even Apple: Both mega-corps are moving to the "walled garden" model. Move to Linux. It's not hard anymore.

Identity: Start using pseudonyms. You can get very detailed pseudonyms from Fake Name Generator.

Backing up: If you use an online backup, encrypt the data before you upload it. Lots of them say "we're encrypted," but that's only for transmission; they store your data in plain text.

Storage: Be careful where you leave your data. If it isn't under your control,

encrypt it.

DO NOT use Facebook, Google or Twitter.

Smartphones: Throw away your apps; their primary purpose is to spy on you. If think you can't, read their privacy statements. Stop doing everything from your Smartphones – they ALWAYS give the network your location. Cell phone are tracking devices that also allow you to make phone calls.

Stay up to date: Find a computer security forum and check in regularly. Understand the threats and stay current. (Shadowlife.cc is a good general privacy source.)

Commerce: Start paying for things with Bitcoin, cash and metals. All other methods double as a tracking tools.

Mesh networks: Learn how to build them and use them. It's cheap and easy, and may be very important one of these days. (PDF.) Think about packet radio afterward.

Educate yourself: Read and learn about liberty, that your life matters, and that you have a right to live it as you wish. Try these sites: Here, here, here, here, here, here, here and here.

**

Published March, 2013. Minor edit, June 2014.