Privacy resources

View this tipsheet online at https://github.com/mhkeller/privacy-resources/

Many folks have compiled lists of different security software, some are listed below. This small tipsheet is an attempt to point to useful reading on the subject and pick out the tools people are most likely to install, given that security software is [notoriously difficult to get going and use](http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it).

Why use privacy tools / encryption?

This question warrants more discussion than can be fully given here. But, if you're reading this, you're most likely a journalist or someone worried about privacy vis-à-vis consumer technology. The most basic answer to this question is "Why should everything on the web default to public?" Encryption can be a way of thinking more critically about much information is being collected and exerting some agency over what can be public.

Some also argue for wider adoption of security tools so that those who rely on them — activists, political dissidents, journalists etc. — don't stick out, thus flagging their behavior as suspicious.

Reading material & Guides

* [Digital Security For Journalists](https://www.gitbook.com/book/susanemcg/digital-security-for-journalists/details) — A report by Susan McGregor at the Tow Center for Digital Journalism at Columbia University
* Jonathan Stray's two part guide "Security for Journalists" — [Part one: the basics](https://source.opennews.org/en-US/learning/security-journalists-part-one-basics/) and [Part two: threat modeling](https://source.opennews.org/en-US/learning/security-journalists-part-two-threat-modeling/)
* [Journalist Security Guide](https://cpj.org/reports/2012/04/journalist-security-guide.php) — A guide on reporting in dangerous areas by the Committee to Protect Journalists

Tools

As you'll see in any discussion of security tools, here's a disclaimer to say **they may not be 100% effective**. If you've skipped the top part of this guide and jumped right to tools, best to read through the top resources first. To quote the [Hacks / Hackers guide](https://github.com/hackshackers/hhnyc-crypto/):

> *The latest information we have is that these tools are likely to help protect your communications, but governments including the U.S. have made progress in breaking or circumventing some cryptographic technologies.*
>
> *If you or your source is truly a high-value target of a government, protecting yourself will require far more effort. To get an idea of what people do when they are really serious*

about security, please read this post first:
http://grugq.github.io/blog/2013/06/13/ignorance-is-strength/

Simple mobile practices

It's best to turn off Bluetooth and WiFi when you're in public or not using them. Bluetooth and WiFi signals can be used to identify your phone, for example, [when passing by a Bluetooth- or WiFi-enabled phone booth](http://www.buzzfeed.com/josephbernstein/exclusive-hundreds-of-devices-hidden-inside-new-york-city-ph - .yryawvdMa), or [shopping in a store with WiFi](http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?_r=0).

Web-browsing tools

A few simple browser extensions exist to limit your digital footprint around web trackers and sending insecure information. **Disclaimer: Using these extensions can cause some sites to not load properly and appear broken. Sometimes disabling them or whitelisting certain domains is required to find a happy medium.**

* [HTTPS Everywhere](https://www.eff.org/https-everywhere) — From the Electronic Frontier Foundation browser extension automatically sends your traffic over the more secure HTTPS protocol instead of by HTTP.
* [Privacy Badger](https://www.eff.org/privacybadger) — Another EFF browser extension, this tool blocks different domains from putting cookies and other trackers on the pages you visit.
* [Self-destructing cookies](https://addons.mozilla.org/en-US/firefox/addon/self-destructing-cookies/) — A Firefox-only plugin that destroys cookies after you leave any website, unless you whitelist certain ones.

Encryption tools

Hacks / Hackers New York City has an installation [guide](https://github.com/hackshackers/hhnyc-crypto/) and [tipsheet](https://github.com/hackshackers/hhnyc-crypto/blob/master/tipsheet.md) that lists many different tools you can use.

The easiest to set up is **secure instant messaging** with Adium. You can find instructions in the [tipsheet](https://github.com/hackshackers/hhnyc-crypto/blob/master/tipsheet.md - adium-mac-os-x). Secure IM is a non-intrusive way to keep your instant message conversations private. You can think of this technology as, "if my casual chats are just that, why do they need to be logged forever?" Or, if you're working in a newsroom and your conversations with colleagues could potentially veer into non-public information, your best bet is to simply encrypt everything by default.

The next level up is creating a **private/public key pair for encrypted email** with [GPG Tools](https://gpgtools.org/). The tipsheet [has instructions](https://github.com/hackshackers/hhnyc-crypto/blob/master/tipsheet.md - thunderbird--enigmail) for configuring with Thunderbird but it can work with Apple Mail. For Gmail or other web mail services you can use [Mailvelope](https://www.mailvelope.com/).

For **phone security**, the iPhone app [Signal - Private Messenger](https://itunes.apple.com/us/app/signal-private-messenger/id874139669?mt=8) provides both encrypted text messaging and encrypted calls. Read more about how to use it on [their website](https://whispersystems.org/).

More resources

* This [Mozilla compilation](https://github.com/mozilla/DropItLike) points to a whole bunch of other tools and guides if you want to jump in further.

LICENSE

Michael Keller, May 2015