

Digital Security Tools

Cryptoparty Chicago
@cryptopartychi

Encrypted Emails

- **GnuPG:** A free implementation of OpenPGP that enables you to encrypt/sign messages
 - Windows: <http://gpg4win.org>
 - OS X: <https://gpgtools.org>
 - Linux: <https://www.gnupg.org>
- **Enigmail:** OpenPGP extension for the Mozilla Thunderbird email client
 - <https://www.enigmail.net>

Web Browsing

- **HTTPS Everywhere:** Browser extension that enables encryption by default while web browsing:
 - <https://www.eff.org/HTTPS-EVERYWHERE>
- **Tor Browser Bundle:** Web browser that allows you to browse the internet anonymously (this browser bundle uses HTTPS Everywhere)
 - <https://www.torproject.org>
- **Privacy Badger:** Browser extension that prevents advertisers and third-party trackers from tracking your web browsing.
 - <https://www.eff.org/privacybadger>

Instant Messaging

- **Pidgin and Adium:** Instant messaging clients which implement the Off-The-Record (OTR) protocol
 - Windows: <https://www.pidgin.im>
 - OS X: <https://adium.im>
 - Linux: <https://www.pidgin.im>
- **TextSecure and Signal:** User-friendly encrypted messaging for Android and iOS
 - <https://whispersystems.org/>

Phone Calls

- **RedPhone:** User-friendly encrypted phone calls for Android
 - <https://whispersystems.org/>
- **Signal:** User-friendly encrypted phone calls for iOS
 - <https://whispersystems.org/>

Operating System

- **Tails OS:** Linux-based live OS that you can use to protect your anonymity and privacy - has most of these tools already setup
 - <https://tails.boum.org>

Useful Guides

- <https://securityinabox.org/en/> : Website with simple guides and how-tos on topics like “How to use smartphones as securely as possible”
- <https://source.opennews.org/en-US/learning/security-journalists-part-one-basics/> : Basic computer security guide
- <https://source.opennews.org/en-US/learning/security-journalists-part-two-threat-modeling/> : Threat Modeling