CUNY J+ Online Security Workshop

May 11, 2016
Mike Tigas, ProPublica
@mtigas | https://mike.tig.as/

Full tipsheet, link to slides, links to all the software (and more software), and other tutorial resources: https://bitly.com/jplus-security

Mobile

Signal — encrypted voice calls and messaging for iPhone & Android

- https://whispersystems.org/ and in the App Store and Android Play Store

Safer web browsing

HTTPS Everywhere — a browser plugin that increases your use of encryption automatically

- Some sites have optional secure HTTPS version of the website. This plugin makes your browser use that version, whenever possible.
- For Chrome & Firefox
- https://www.eff.org/https-everywhere and in the Chrome Web Store and the Firefox Add-ons site

uBlock Origin — commonly used as an ad-blocker, but also useful for blocking more malware sites.

- In the Chrome Web Store and the Firefox Add-ons site

Tor Browser — an anonymizing web browser

- Hides your IP address from websites you're visiting. (Sometimes you don't want a site to know that you're researching them.)
- Bypasses filters if you are in a censored country or at an office that blocks websites
- https://www.torproject.org/download/download-easy.html.en

Messaging tools

Ricochet — encrypted chat

- https://ricochet.im/

Jitsi — encrypted video call website (like Hangouts, Skype)

- No download required
- https://meet.jit.si/

PGP / GPG / GnuPG — encrypts e-mails (you can use it to encrypt files, too)

- Still notoriously hard to set up, and lots of ways to do it.
- See https://github.com/mtigas/workshop-cunyjplus for more info