Tor

• Anonymized internet access so websites don’t know where you are
  • Great for research so websites don’t know you visited them & your ISP doesn’t know either.

• Relays your web traffic through random computers before trying to access the website

• Caveats:
  • Slower than normal browsing
  • Relays may see your browsing (if not HTTPS), since they are relaying it on behalf of you. (Be careful with logins!)
Tor

PC/Mac: https://www.torproject.org/

iOS: Onion Browser (disclosure: I work on this)

Android: Orbot
Chat: OTR Encryption

• “Off The Record” encryption protects messages between you and someone else.
  • Not the same as Google “Off The Record” mode

• Use an existing account (like GChat or others) & use an OTR plugin to encrypt.
  • You can register an account at other chat services too, to avoid Google knowing about your chats.

• Caveats:
  • Metadata – who you are talking to and when – is still seen by the chat service.
OTR Encryption

Jeremy B. Merrill

Mike Tigas

Jeremy B. Merrill
**OTR Encryption**

- **Tor Messenger** provides OTR encryption and lets you use accounts on many messaging services (Google Chat, Twitter DMs, XMPP/Jabber).
  - In addition to OTR, it uses Tor to mask your IP address.
- **ChatSecure** is similar, but for iPhone and Android.

Remember: to use OTR, your friend also needs to use Tor Messenger (or another app that does it).
Encrypted Texts

- **Signal** (iOS & Android)
- iMessage (iOS) **claims to encrypt messages**, but Apple may have access to the messages.
  - Phone provider doesn’t see messages anymore, but Apple has the metadata of who you communicate with.
Phone Calls

- **Signal** (iOS & Android)
- **SilentCircle** ($$$, iOS & Android)
- **FaceTime** (iOS): Like iMessage.
  - Prevents cell provider from knowing who you call. But again, Apple may have access to the metadata and actual call.
PGP

Also known as GPG — for “GnuPG”, one of the programs that does this

Public and private keys, you have to know someone's public key to send them an encrypted message.

Also lets you “sign” messages so recipient can tell whether it was tampered with while in transit.
PGP

- Mac:
  Thunderbird+ Enigmail
  or GPGTools + Mail app

- Windows:
  Thunderbird+ Enigmail
  or GPG4Win + Outlook

- Setup guides:
  Hacks/Hackers NYC
  Freedom of the Press Foundation
  Security in a Box
But what about other tools?

• New tools come out all the time.
• We don’t necessarily know what’s secure. Follow a lot of security experts to see what their consensus is.
• Consider the encryption, metadata-masking capabilities, and transparency of how tools work:
  • https://projects.propublica.org/graphics/privacy-tools
Further reading

- Freedom of the Press Fdn. encryption guide
- Threat Modeling guide on OpenNews Source