Share this guide! https://bit.ly/cryptochecklist
Managed by Derek Eder, Chi Hack Night
Suggestions & comments are welcome!

Better living through online security & encryption

This is a checklist and collection of resources for setting up encryption and good digital security practices in 2017. Following these steps will make your information and communications more secure from surveillance and malicious hackers.

Crypto-to-go: the short list for everyone (Easy)

New to online security? Do these 3 things and you'll be in good shape.

1. **Better password habits**
    a. Use a password manager like LastPass (free), 1Password (paid subscription ~$36 per year) or KeePass (free & open source)
    b. Turn on 2-factor authentication when available (list of supported sites)
2. **Use encrypted communication**
    a. Signal, replaces text messaging & chat (*Easy*)
    b. Semaphor, group chat similar to Slack (*Freemium service*)
        i. Join our chat room with this invite code: G2DDTI35MXKZRM2OJMU6JF2B7PARQDMVN4DG66KCKN5ZGWKOBL6Q
    c. Or pick something else from this list by the EFF
3. **Private web browsing**
    a. For Firefox & Chrome, install:
        i. HTTPS Everywhere, forces HTTPS whenever possible
        ii. Privacy Badger, blocks ads and trackers (this may break some sites when it's turned on)
        iii. uBlock Origin, adblocker
    b. Install and use Tor Browser (Windows & Mac)

The full online security & cryptography checklist (Advanced)

If you want to dig further into online security, we recommend reviewing this more comprehensive list.

1. Start thinking about digital security & risk assessment (sometimes referred to as threat modeling) - who are you protecting yourself from?

2. Switch to using encrypted messaging platforms

a. Signal, replaces text messaging & chat (*Easy*)
b. Semaphor, group chat similar to Slack (*Freemium service*)
c. Encrypted email services like Protonmail or Tutanota
    i. Disable email tracking on Google: General -> Images -> Ask before displaying
d. Longer list of encrypted services by the EFF

3. Change your online habits
    a. Routinely run computer software updates
    b. Learn about phishing and how to avoid it (see also spear-phishing)
    c. Get serious about passwords & logins
        i. Stop using the same passwords across different sites
        ii. Use a password manager like LastPass (free), 1Password (paid subscription) or KeePass (free & open source)
        iii. Turn on 2-factor authentication when available (list of supported sites)
            1. Use a USB key like YubiKey
        iv. Don't use your fingerprint to unlock. It's not secure. Use a password.
        v. Security questions are easy for adversaries to figure out.
    b. Protect yourself on social media
    c. Anonymous internet browsing
        i. 'Private' browsing mode is a myth. See http://panopticlick.eff.org/
        ii. For Firefox & Chrome, install:
            1. HTTPS Everywhere, forces HTTPS whenever possible
            2. Privacy Badger, blocks ads and trackers (this may break some sites when it's turned on)
            3. uBlock Origin, adblocker
        iii. Alternative browsers
            1. Tor - anonymous browsing
                a. Tor Browser (Windows & Mac)
                b. Install and use Orbot (Android)
                c. Install and use Onion Browser (iPhone)
            2. Brave - built in ad and tracking blockers
        iv. Start using a VPN like Algo, Riseup, OpenVPN or Mullvad
    d. Begin to break your dependence on cloud storage
        i. For sensitive messages and documents, don't share them unencrypted on 'the cloud' (Gmail, Slack, Dropbox, etc).
        ii. Switch to a fully encrypted cloud backup like Spideroak One (paid service)
        iii. Or, backup your data on an encrypted external hard drive

4. Protect yourself from your physical devices (more on why this is important)
    a. Encrypt your computer
        i. BitLocker for Windows

    ii. FileVault for Mac
    iii. Linux
b. Encrypt your phone
    i. iPhone 3S or greater, on by default in iOS8 (EFF's Guide)
    ii. Android on by default in Android 6.0
c. Cover your computer & phone cameras with tape
d. Consider ditching your phone during sensitive moments

Additional resources

More guides

- Surveillance Self-Defence, Electronic Frontier Foundation
- How to Protect Yourself From Government Surveillance and Criminal Hackers, ACLU
- Easy-ish privacy/security actions to protect against doxxing, Jason Reich, BuzzFeed
- Encryption Works, Freedom of the Press Foundation (out of date by over a year, update pending)
- Securing Your Digital Life Like a Normal Person, Martin Shelton, Open News
- How to encrypt your entire life in less than an hour, Quincy Larson, Free Code Camp
- Decent Security, Starter guide for better online security
- A 70-Day Web Security Action Plan for Artists and Activists Under Siege, Candace Williams
- Surveillance Self-Defense Against the Trump Administration, The Intercept
- Encryption Works: How to Protect Your Privacy (And Your Sources) in the Age of NSA Surveillance, Freedom of the Press Foundation
- The Smart Girl's Guide to Privacy (book/ebook; available at the Chicago Public Library)
- Security-in-a-box, a guide for activists
- DIY guide to feminist cybersecurity
- Beginner's guide to beefing up your privacy and security online, Ars Technica
- Digial Privacy Cheet Sheet, Karl Blumenthal
- Upgrade Your iPhone Passcode To Defeat The FBI's Backdoor Strategy, Micah Lee, The Intercept
- Transformers : Rescue Bots Exploring the security side of organizational, digital, and data transformation by Seamus Tuohy
- The Five Days of Privacy, Common Sense Education

Why is this important?

- We Should All Have Something To Hide, Moxie Marlinspike
- Why Privacy Matters, TED talk by Glenn Greenwald

Other resources

- CryptoParty, free security & crypto workshops around the world
- Library Freedom Project (collection of useful articles)

- Dear Clinton Team: We Noticed You Might Need Some Email Security Tips, The Intercept
- Crash Override Network for people suffering online abuse

On PGP email (*Advanced*)

- Mailvelope.com - PGP browser plugin
- PGP for Mac https://ssd.eff.org/en/module/how-use-pgp-mac-os-x
- PGP for Windows https://ssd.eff.org/en/module/how-use-pgp-windows
- PGP for Linux https://ssd.eff.org/en/module/how-use-pgp-linux
- Why Johnny Can't Encrypt (Usability study for PGP 5)
- Why Johnny *Still* Can't Encrypt (Usability study for PGP 9)
- Is Email Encrypted Yet? Talk by Tankred Hase
- GPG and Me, Moxie Marlinspike

Advanced security

- Mac OS Security and Privacy Guide

Reducing availability of public records

- How to Delete Yourself from the Internet, CNET article by Eric Franklin
- How to Remove Yourself from Google & Public Records, Reputation Defender (2014)
- There Are No Innocents: Data Rebroadcasting and Server-Side Responsibility, Karl Fogel (for those who work with public data)

On surveillance capitalism

- The Internet with a Human Face, Maciej Cegłowski
- What Happens Next Will Amaze You, Maciej Cegłowski
- The Terrifying Cost of "Free" Websites, Adam Ruins Everything

The Internet of Things

- Alexa and Google Home Record What You Say. But What Happens to That Data?, Tim Moynihan, Wired

Online Cybersecurity Courses

- Learn the Fundamentals of Cybersecurity, Sans Cyber Aces
- Journey into cryptography, Khan Academy