CRYPTO-PARTY:

SECURING YOUR COMMUNICATIONS

WHEN TO TAKE SECURITY SERIOUSLY?

- Oppositional efforts
- Groups (listservs, group texts) with access to confidential info
- Future oppositional efforts
- Close proximity to individuals in oppositional efforts

THREAT MODELING

1) **Identify security objectives: What do you want to protect?**
    a) Personal Info: home address, phone number, school info etc.
    b) Operational Info: details of direct actions, etc.
    c) Communication Security: contents of messages, etc.
    d) Information Security: contents of documents, membership lists, etc.
2) **Identify threat actors: Who do you want to protect it from?**
    a) Federal: DHS, FBI, DEA, NSA, DOJ, ICE
    b) State/ Local: CPD, State Police, Sheriff's Office
    c) Private: Private security, rogue cops, PIs
    d) Individuals: White nationalists, pro-misogynists
3) **Identify threat capabilities: How will they try to get it from you?**
    a) Federal: Full internet monitoring, 0-day exploits, PRISM, Full phone monitoring, Targeted wiretaps, Street surveillance, Lawful hacking against TOR and VPN users, GPS trackers, Financial transactions, subpoenas against cloud providers
    b) State/ Local: State ID databases, Intelligence fusion centers, Stingray interception, cell tower dumps, social media monitoring, auto-license plate recognition
    c) Private: Physical surveillance, credit history checks, "pretexting", cell phone pinging, skip tracing, Stingray/ DRT box/ IMSI catcher
    d) Individuals: Accessing online accounts (guessing password, security questions, phishing attacks, malware, local software vulnerabilities, server vulnerabilities), doxing

RESOURCES - BASIC STEPS TO TAKE

- Update to latest OS version (all devices)
- Disable all browser plugins, including and especially flash and java
- Set phone and computer to auto-lock after a short period of inactivity
- Enable strong passwords on phone and computer (alpha-numeric, 9+ characters)
- Android Specific:
    - Turn on encrypted file system
    - Need to charge battery to 85 percent or higher before enabling
    - Install and register *Signal* (app)
- iOS Specific:
    - Disable all iCloud syncing (use "sync this iPhone over Wi-Fi")
    - Turn off Location Services
    - Turn on Erase Data after 10 attempts
    - Turn on encrypted iPhone backups in iTunes
    - Install and register *Signal* (app)

- Mac

    - Enable FileVault in System Preferences > Security & Privacy
    - Optional hardening for FileVault (run these common in Terminal):
        - sudo pmset -a darkwakes 0
        - sudo pmset -a standby 0
        - sudo pmset -a standbydelay 0
        - sudo pmset -a destroyfvkeyonstandby 1
        - sudo firmwarepasswd -setpasswd -setmode command
    - Disable iCloud backup (ideally disable iCloud entirely)
- Windows
    - Install Veracrypt and enable full disk encryption

GENERAL RESOURCES AND APPROACHES TO TECH SECURITY

Security Culture

- Don't say anything you wouldn't want used against you in a courtroom
- Actively call out -isms; undercover agents frequently exhibit sexism, homophobia, racism, classism
- Collect as little data as possible (avoid video recording, notes, photos)
- You can say no whenever and to whomever you want
- Avoid "over-paranoia" when it comes to possible infiltrators
- More: http://www.crimethinc.com/texts/atoz/security.php

Device Security

- ALWAYS, above all, keep your web browser, phone, apps, office suite, and desktop operating system up-to-date within 24 hours of the latest update
- WiFi router: use WPA2-PSK (AES) authentication only; no TKIP/WEP/WPA; disable WPS
- Never enter any password on a device you do not own (such as public computers or computer cafes)
- Never double-click files that people email you (including files shared via google drive, dropbox, or any other website)
- Make logging out a habit

Precautions against non-state actors

- Fortify "cloud" services (Podesta hack)
- For all services: turn on all email security alerts
- Gmail: use Two-Step Authentication with Google Authenticator app (prevents number-porting attacks)
- Facebook: turn on Login Approvals (SMS-based)
- Twitter: Account Security: "Require a verification code when I sign in" (SMS-based)
- Skype: link account w/ Microsoft to enable two-factor authentication; keep your Skype handle secret and don't use it with untrusted people
- iCloud (if you truly need it, otherwise disable it): turn on two-factor authentication
- Dropbox: turn on two-step verification
- Audit all online accounts to avoid password reuse
- Use a password manager such as lastpass, duo, keepass, clipperz
- Don't click random links sent in private (emails, Twitter DMs, Skype, private FB msgs/posts): could give away your IP address / location / browser details
- Don't give out your phone number to websites or untrusted people; use a google voice number
- Don't leave clues about your personal life: where you live, work, roommates, family, work/travel schedule
- http://crashoverridenetwork.tumblr.com/post/114270394687/so-youve-been-doxed-a-guide-to-best-practice