Basics of Digital Safety

Last updated 4/11/2018

Original Document Prepared by NYC DSA

1. Install Signal

Signal is an end-to-end encrypted text message app. End-to-end encryption means that when you send a message, it's protected in a way that only the person you sent it to can read it. Prevent snoops, cops, and feds from spying on your conversations. Just remember that anyone with access to your device can still see your messages. We recommend locking your device with a password, locking Signal down with a PIN, and setting messages to auto-delete. Remember, this doesn't just protect you, it helps protect your comrades.

Download Signal for Android, iOS, and your computer: https://whispersystems.org
What is encryption and other apps (EFF): http://bit.ly/2Bl7FzO

2. Install a Password Manager

A password manager creates an encrypted vault which you can use to store all your logins behind one master passphrase. Most people use the same emails/passwords over and over again, greatly increasing their risk of being hacked. Using a unique pw for every login prevents this. Since all your login info is stored in the password manager, it's also super convenient! Never struggle to remember (or type) a password again! We recommend using LastPass, which offers browser extensions for all major browsers and apps for both ios and android.

Download LastPass for Android, iOS, and your computer: https://lastpass.com

3. Use 2-Factor To Put a Lock On Your Accounts

Two Factor Authentication — or 2FA — provides an extra level of protection to your accounts. On login, you'll get a randomly generated code that you'll enter on your 2nd device (usually your phone) to verify your identity. 2FA can prevent damage if an account is compromised (DNC hacks would have been prevented by using 2FA). If a service offers it, you should turn it on! For managing your 2FA, we recommend Authy, which allows you to get codes through the app, which is more secure than via text message. Some services only offer text codes; this is still better than no 2FA at all!

Download Authy for Android, iOS, and your computer: https://authy.com/

4. Don't Get Doxxed — Lock Your Info Down

Don't let fash get the best of you. Set all your social media to private (or as private as possible). If you post about your activism online, use a pseudonym. Especially if you might be at risk from your boss or the authorities. Don't post personal info such as your email, phone number, address; even minor details like your birthday can be used against you, since security questions can bypass many account logins. You should also disable automatic geotagging / location tracking for Facebook, Instagram and any other apps. To get a sense of how exposed you are, try doxxing yourself—search for your name or use a person finding site like pipl or spokeo. If you find yourself, most of these sites will allow you to remove your entry.

Anti-Doxxing guide for activists (Medium): http://bit.ly/2FWzYYE
List of people finder sites, and how to remove yourself: https://www.abine.com/optouts.php

5. Finding More Help Online

EFF Security Self Design Guide: https://ssd.eff.org/en
How to protect your privacy at a protest (short video): http://bit.ly/2DV1lBE
Get more in-person training at a cryptoparty: https://www.cryptoparty.in/nyc
Questions about us? Reach out to us directly at nyc-dsa-infosec@protonmail.com
Concerned about digital safety for you or your org? Try our hotline at nyc-dsa-infosec-hotline@protonmail.com

NYC DSA