DSA

Democratic Socialists of America

75 Maiden Lane Suite 702
New York, NY 10038

INFORMATION SECURITY RECOMMENDATIONS

June 2017

Introduction

Maintaining security and privacy has always been a challenge for political organizers, long before personal computers and the Internet. Today, the combination of ubiquitous information technology and a radical right-wing authoritarian political climate has made digital security a top concern for politically active organizations and individuals.

Online harassment and surveillance are, sadly, ubiquitous and effective ways of creating chaos and fear. As DSA grows in membership and influence, we should be prepared for both state and non-state actors to use digital means to attempt to destabilize us.

Let us not be victimized when we can readily secure ourselves and our comrades as we organize for socialism. Good information security practices don't require computer wizardry. A few new habits and tools, consistently applied, will go a long way towards defending our collective work from digital assailants.

This document recommends steps DSA members and chapters can take to promote information security. We've concentrated on actions that are inexpensive and known to be effective. This document will evolve over time to respond to new threats and embrace new defensive tactics. Meanwhile, please contact us with any pressing security questions or concerns.

In solidarity,

DSA Tech Committee
Information Security Working Group

Part 1: Public, Private, and Secret Communications

What you think is secret online, probably isn't. What you think is private is probably more public than you realize. Understanding the difference between public, private, and secret communication is essential to maintaining a strong practice of information security.

Public communication

Consider most of the digital communicating you do to be public. Unencrypted data is public data, and most of what happens on your devices and the services they connect to is unencrypted. Text messages, email, Facebook, Instagram, Google Groups, Slack... yep, all public!

If you don't know for certain that the communication platform you're using is end-to-end encrypted, consider your communications public.

Private communication

Let's say you're logged in to your favorite social network. You've made your account "private" and your posts can't be found in search engines like Google. That means your communications on that social network are private, right? Nope. "Private" Facebook groups, Instagram accounts, or Twitter profiles are not private communication.

Only communication using end-to-end encrypted software whose code has been audited by independent security experts (ex: Signal) is private. Even when using recommended apps like Signal, keep in mind that the more people who can see your communications, the less private those communications are. Anyone who has access to your communications could copy or screenshot them, so keep your sensitive communications limited to small trusted circle.

Secret communication

Simply put, **there's no such thing as secret communication via digital devices**. Truly secret communication is only possible between as few people as possible in a trusted location and without any digital devices present. Fortunately, most, if not all, of DSA's work does not require total secrecy.

Part 2: Recommendations for DSA members

Use Signal for private communication (5 minutes)

Signal is an app that uses many current best practices in encryption and privacy to allow for private voice and text communications. **Use Signal instead of text messaging and phone calls.** It's free and available on Android and Apple devices for texting and calling. By habitually using Signal by default, you will be way ahead of the curve in terms of private digital communications.

Secure your mobile devices (10 minutes)

Take the following steps to keep your phone or tablet safe in everyday situations:

1. **Lock your screen with a long password**. 10 characters is ideal, but anything more than the usual 4 digits is an improvement. If you lose your phone or it is stolen, you don't want others to be able to access your contacts and data.
2. **Turn on automatic updates** to keep apps and system software current. The latest software has the latest security fixes, which helps keep your device secure. Tip: If you have a restrictive data plan, enable the setting to update apps using wifi only, as app updates can chew through a lot of data.
3. **Encrypt your device**. On newer devices running more recent versions of iOS and Android, encryption is enabled by default. On older devices you may have to change a couple of settings to ensure that the data on your mobile device is protected.

Best practices for bringing mobile devices to protests, strikes, and direct actions are a topic of much debate in the security/privacy community. Your best bet is to not carry a device at all, but that may not be practical when you need to coordinate with comrades during an event. Disabling fingerprint unlock ("TouchID" on Apple's iOS devices) will ensure that law enforcement can't physically force you to unlock your device. Powering off your device will make it far more difficult to extract data from it, assuming you've followed the steps above and encrypted your device.

Enable two-factor authentication (1 hour)

Two-factor authentication (often abbreviated "2FA") is a method of verifying identity by providing two separate pieces of evidence. By double-checking that you are who you say you are, **two-factor authentication helps keep you safe online**. You should use it everywhere it's available.

For example: when you try to log on to a website, after asking for your username and password, the website will contact you via text message, email, or phone call and provide you a code. Once you enter that code into the website, you can log on and continue about your business. This extra step helps to prevent your accounts from being compromised.

Turn On 2FA has quick tutorials on how to activate two-factor authentication for many popular websites and apps.

Create and manage strong passwords (2 hours)

Everyone has seen the stories in the news of companies, governments, and public figures getting "hacked" because they used an obvious, guessable password. Don't want that to be you? We've got a good solution.

We recommend that you **use a password manager**. A password manager is an application that stores your passwords for you. Using a password manager is much easier and faster than having a bunch of passwords written down or memorized. In fact, once you switch to using a password manager, you'll only have to ever remember one password again: the master password for your password manager.

The other big advantage of a password manager is that they can generate and store "strong" passwords for you. A strong password is one that's hard for both a human and a computer to guess. There are a number of ways of generating strong passwords, and most good password managers will let you dial in the "password recipe" that meets the requirements of the services you're logging in to.

To get started with a password manager:

1. **Create and memorize a strong master password** using the Diceware method. Write this password down and put it someplace safe so you don't forget!

2. **Choose a password manager** and enter your new master password during setup. Depending on your budget, we recommend the following tools:

- Superb, easy to use, $3/month: 1Password
- Not as polished, relatively easy to use, free plan available: LastPass
- Robust, hard to use, free: KeePassX

If you can afford it and are running macOS or Windows, we recommend using 1Password over the other two options.

3. **Enter all your passwords into the password manager.** It's worth the time, trust us!

User-friendly password managers like 1Password or LastPass will have you install an extension to your web browser (most likely Chrome, Firefox, Internet Explorer, or Safari). Once installed, whenever you visit to a website that's in the password manager's database, it will automatically fill out the username and password field for you. Isn't that handy?

Of course, you don't have to enter all your passwords into your password manager at once. The browser extension will ask you if you want to save your login information whenever it sees you signing in to a website. Eventually all your passwords will end up in your password manager.

4. **Change all passwords to be strong, random, and unique**.

Once the passwords you use most often are in the password manager, it's time to change all of them to stronger, random, unique passwords. Your password manager can generate new and strong passwords for you. Don't worry if the new passwords look complicated or hard to type – that's the point! As long as you remember the master password, you will always have access to the rest of your passwords, and the browser extension will do the typing for you.

Now that you've done all that work: **never send passwords over email.** Email is public communication and you never know who might be reading your email in the future. If you need to share a password, use Signal.

Access the Internet safely

A few simple steps will help keep you secure online.

First: **use the Chrome browser for everyday internet usage**. It's secure and supports most websites, since it's the browser most web developers use. Chrome should automatically keep itself update to date, but it's good to periodically double-check that you have the latest version.

If you're conducting opposition research and visiting sites like Stormfront, **use Tor Browser for extra privacy**. It's not practical or advisable to use Tor all the time because it slows down your browsing and can be interpreted by law enforcement as an indication of criminal activity. Use Tor Browser for sensitive research and then go back to your regular browser (which should be Chrome, per the above).

Don't connect to public wifi (airports, coffee shops, libraries, etc.) if you can help it, especially if you need to do anything sensitive online. If you must use a

public network, use a VPN service, described below. If you have no choice but to use public wifi, try not to access anything personally identifiable (ex: email, social networks) while on a public network.

Use a paid VPN service that doesn't store logs on all your devices, especially on public wifi. We recommend Mullvad and Private Internet Access but there are many VPN providers out there.

Don't click on weird looking links online, especially ones that have been emailed to you. If your gut says that a link or a site seems sketchy, close it.

Secure your computer

Let your computer update itself when it notifies you that updates are available. Software vendors are constantly fixing security vulnerabilities that have been brought to their attention. If you're not running the latest software, you're not getting the benefit of those security fixes.

Uninstall Flash completely unless a site you depend on requires it. Flash is notoriously vulnerable software and has historically been the source of many successful hacks. If you must use Flash, keep it up to date.

Be cautious about running antivirus software. Most antivirus software is more likely to make your computer insecure than it is to save you from malware. Antivirus software is entirely unnecessary on macOS and Linux. If you're running Windows, stay up to date with system releases and use the built-in Windows Defender.

Part 3: Recommendations for DSA Chapters

Host a “security night”

Get your members and community involved! Following all these recommendations by yourself can be tedious. As a chapter leader, implement all the member recommendations above, then hold a security night where you and other security-minded members can help others do the same.

Secure your chapter’s website

1. **Enable HTTPS (SSL encryption) on all pages of your site.**
   If you are going to set TLS/SSL up on your own, contact the Tech Committee for help. If you’re the DIY type, use Certbot, which simplifies setting up a solid SSL configuration for your site.

2. **Hide operator information.**
   When you purchase a domain name like dsausa.org, the personal information you provide during the domain registration process will often be exposed to the Internet. This is problematic because it exposes your full name, address, and phone number while also implying an association between you and a political organization. For those reasons, domain registration info has frequently been used to facilitate doxing, a form of online harassment with potentially disturbing real-world consequences.

   Enter your domain name into Whois to see if your personal information is exposed. If it is exposed, visit your domain registrar (GoDaddy, Hover, Gandi, Namecheap, etc.) and turn on privacy protection. Just about every domain registrar offers privacy protection, but some charge extra for it. Unfortunately, if this information is already exposed, there isn’t much you can realistically do to make it private again.

3. **Take a lesson from Hillary: do not run your own email server.**
   If you are considering running your own email server, please reach out to us and we will direct you towards email services that are as private as possible.

Protect your members by collaborating securely

Many chapters use tools like Google Groups, Slack, and Google Docs to collaborate and organize. The most important thing to remember about these services is that they are a form of public communication. All content and discussions you make on such services should be kept appropriate for the public. It’s a safe assumption that Google and most other service providers

will comply with all requests for documents from law enforcement. **Don't share anything on these services that you wouldn't want known and attributed to you by opposition groups, law enforcement, or journalists.**

As an alternative to Slack and other group chat services, consider using DSA Chat, which is run by DSA's own national Tech Committee (the same folks who brought you this document). Any dues-paying DSA member can register for DSA Chat. You should still be cautious about how you communicate on DSA Chat, but we strive to make it as private and comfortable an online space as possible for members.

As an alternative to a shared Google Doc, try Riseup Pad. While it should still be considered public, this tool is hosted by an activist service provider with a longstanding commitment to privacy.