DNC Security Checklist

Updated: March 2022 by the DNC Security Team

Welcome!

★ We strongly recommend anyone who works in politics, campaigns, or really anyone who has a device or an account on the internet, take these steps to secure them.

★ Complete the steps thoroughly. Prioritize the accounts that are the most critical to your daily life, which may be your email, social media accounts, financial/banking, and file storage.

★ Questions? Email security@dnc.org.

Step 1: Secure Your Devices

Adversaries frequently take advantage of personal and work devices and the applications on them, especially those that are not updated regularly. Always apply software updates as soon as they are made available.

Secure your devices	Personal	Work
Make sure your phones and laptops are running the most up-to-date operating system. iPhone/iPad, Android, Mac, PC	❑	❑
Gmail: Enroll in Google's Advanced Protection Program (APP) to reduce the risk of getting phished (Learn more).	❑	❑

Gmail: Complete the Gmail security checkup	❑	❑
Laptop disk encryption: Here are instructions for Macs and for PCs (***Note:*** *not included with Windows 10 Home)* to keep them safe even if lost or stolen. Chromebooks have disk encryption enabled by default.	❑	❑
Phones and tablets: Enable a PIN, fingerprint, or pattern to unlock the device. iPad/iPhone PIN, TouchID. Android: Screenlock	❑	❑
Web encryption: Install the HTTPS Everywhere extension on all web browsers like Chrome or Firefox.	❑	❑
Block ads: Install the uBlock Origin extension on your web browser.	❑	❑

Step 2: Use a Password Manager

Password manager	Personal	Work
Set up a password manager to generate, store, and auto-fill all of your passwords. Learn more. ***Paid Options we like:*** LastPass, 1Password, Dashlane ***Free Options:*** Google Password Manager, Apple Keychain	❑	❑
Create a 'master password' for your password manager that is longer than 16 characters, unique and memorable. ***Pro Tip:*** Create a strong master password by using a passphrase. *Sample strong passphrase: worshiper favoring visa nest*	❑	❑
Add strong two-factor authentication to your password manager. More below in Step 3. **Guides:** Lastpass, 1Password, Dashlane.	❑	❑
Download your password manager's mobile app.	❑	❑

Add your password manager's browser plugin. **If you use Chrome:** LastPass, 1Password, Dashlane	❑	❑

Caution: If someone obtains or guesses your master password, they may be able to decrypt all your individual passwords. Your master password must be *long, random,* and *unique*, but also memorable. This is something you will type every day.

Now change all your passwords and add them to your password manager (details in Step 3).

Step 3: Use Strong Two-Factor Authentication

Secure all personal and work accounts:

1. Let your password manager generate long, random, unique passwords and save it in your password manager. (See step 2)
2. Enable two-factor authentication (2FA) on all sites (Learn more). Select the strongest form of 2FA in the following priority order.
    a. **FIDO Security Keys. Use security keys whenever possible because *all other forms of 2FA are phishable*.** We recommend Yubikeys and Google Titan Keys. Make sure your security keys support NFC so that you can use them with your phone.
    b. Authentication App. We recommend using Authy since it allows for backups in case you lose, misplace, or get a new phone.
    c. Email is the next best option.
    d. Avoid SMS/text message as your 2FA unless it is the only option. Ensure you have a *long*, *random*, *unique* password if so.

You probably have many accounts and some may be more important than others. Prioritize the ones that you use daily and hold the most sensitive information and work your way down the list.

Update passwords and enable Two factor authentication	Personal	Work
Apple ID	❑	❑
Email: *Gmail*, *Microsoft Outlook*, *Yahoo!*, *AOL*	❑	❑
Facebook and *Instagram*	❑	❑
Twitter	❑	❑
Other Social: *LinkedIn*, *Pinterest*, *Snapchat*, *TikTok*, *WhatsApp*, *Skype* (*use your Microsoft account*), *Slack*,	❑	❑
File Storage: *Box*, *Dropbox*, *Evernote*	❑	❑
Financial services: *Banks*, *CashApp*, *credit cards, investment/401k accounts*, *PayPal*, *Square*, *Venmo*	❑	❑
Gaming: *Nintendo*, *Twitch*, *XBox* (*use your Microsoft account)*	❑	❑
Ecommerce sites: *Amazon*, *Etsy*	❑	❑
Health: Insurance, Fitness apps, Healthcare providers, *Strava, FitBit*	❑	❑
Streaming sites and music—*especially those you share with others— Disney+, HBO, Hulu, Netflix, SoundCloud.*	❑	❑
Travel: *Airbnb, airline accounts, Lyft, Uber, transit apps*	❑	❑
Miscellaneous sites: *Salesforce, Yelp, Untappd*	❑	❑

Pro tip*:* We recommend a passphrase for anything you have to type in frequently (like your Netflix password).

Step 4: Take Your Security Up a Notch

Use secure messaging.

Many of the tools we use every day to communicate (such as standard email and text messaging) are not secure from eavesdropping or interception. Furthermore, even when using a platform like Slack or Google Chat, you should consider that all messages including direct messages can be retained and subject to litigation holds. Only type things you would not be embarrassed about if they ended up on the front page of *The New York Times*.

If you need to send sensitive data or have sensitive communications, we recommend using messaging apps that are encrypted in transit and at rest and support disappearing messages. Some examples are Signal, Wickr or WhatsApp, though each has limitations, so a different product may work for different organizations.

Finally, avoid SMS (text messaging) when possible, especially when dealing with sensitive data.

Use a device that is secure-by-design.

A key technique to reducing the risk of a breach is to reduce your attack surface. To that end, consider using a Chromebook or an iPad. Both devices offer a number of key security features, and dramatically limit the options our adversaries have for running malware.

Set a PIN on your mobile phone.

Most phone carriers allow you to set a login PIN. If someone attempts to make any changes to your account, your carrier will be required to validate the request with your PIN. Enabling this feature makes it harder for adversaries to take over your account or conduct SIM swapping attacks.

- AT&T: Set in your Profile (instructions)
- TMobile/Sprint: Set at Customer Care or call 800-937-8997 (more info)
- Verizon: Set at Security (instructions)

Appendix

Mail providers

For email accounts, we strongly recommend using mail services hosted by Microsoft (Outlook.com/Outlook 365) or Google (Gmail/Workspace). Do not host your own mail server under *any* circumstances.

Dating apps

As political staff, your activities, both during work hours and after work hours, are reflections of your campaign or organization, and the Democratic ecosystem. As such, you may attract more attention on dating apps, and some of these contacts may not be as well-intentioned.

A few tips:

- Verify who you're communicating with. A quick Google search (if you can) can go a long way.
- Don't put anything out there that you wouldn't mind the opposition seeing. This includes video calls, text messages, emails, photos, or DMs - imagine that it was on the front page of the NYTimes.
- Notice when people are asking you more than a few questions about the election, the campaign, the candidate, and the opposition. Are they actually curious, or might they be pumping you for information? Think twice about saying things that could be taken out of context to the detriment of our collective efforts.

Swipe carefully!

Password managers

Password managers such as Dashlane, LastPass and 1Password help you create, store, and enter login credentials for you. They will create passwords that are *long*, *random*, and *unique*. When logging in to a website, they can autofill your user name and password in the correct field so you don't need to type them.

We recommend you have separate password manager accounts for your work and personal logins. (This is an example of keeping your work and personal accounts and

data separate, something we strongly recommend!) Group features of password managers like 1Password Families and LastPass Families can help securely share passwords with loved ones in case of an emergency.

To protect all of your individual website passwords, you need to supply a “master password”. To create a strong master password use a password generator such as this passphrase generator. A good passphrase might look something like: “sixth golf glean pact hassock”.

Pro Tip: *Be sure to add strong 2FA to your password manager, preferably a security key.*

Privacy settings

While not the same as cybersecurity, our online presence can raise many privacy concerns. While many in politics retain a public presence, there are still many aspects of our lives that we would not want to be displayed publicly in case they get into the wrong hands.

When using a campaign or candidate page, be sure that anyone who has access to edit those pages has completed the Security Checklist on their personal accounts.

Review privacy settings on the following sites and services:

- iOS: Remove location data from your photos.
- Facebook: Review privacy settings.
- Google: Make sure you’re not sharing your location with anyone you don’t know. Remove your personal information (like your address or birthdate) from your profile.
- Instagram: Consider setting your account to private. Go to Settings > Privacy > Select “Private Account.” Consider where you geotag your location for posts and stories.
- Twitter: Review your Privacy Settings. Uncheck the “Add location information to my tweets” feature. Go to Twitter's Security Settings and check the "Password reset protect" feature.
- TikTok: Consider setting your account to private. Consider where you geotag your location for posts and stories.

- Venmo: Make your transactions private. Go to Settings > Privacy > Select "Private" which makes your transactions "Visible to sender and recipient only." Make your friends list private. Go to Settings > Privacy > Friends List > Select "Private" which makes your friends list visible to only you.

Two-factor authentication

Two-factor authentication (sometimes called 2FA, "two step", "multi-factor", or MFA) adds an additional and critical step to a website's login process. Two-factor systems use your smartphone or a hardware device to identify you to the website.

Caution: Many websites offer SMS-based (text message) two-factor access. Unfortunately, it is possible to steal someone's phone number (called 'SIM-swap attacks'), and then to intercept two-factor codes sent via SMS. Avoid two-factor authentication based on SMS.

Use the strongest form of 2FA available on the services. In order of strength: Security keys > Push notification > Authenticator app > Email > SMS/text messages.

When you have enabled the strongest 2FA available, disable others. For example, when you enable security keys, go back and disable authenticator app and SMS forms of 2FA. When you enable an authenticator app, disable SMS/text message.

Security questions

A few websites still rely on using account security questions ('ASQ') to help identify you in the event that you forget your password to the site. They often ask for information like "*Where did you travel on your honeymoon?*" While that might seem like a harmless question, in a world of social media, many of these answers can be found on the internet or the dark web.

To that end, if you encounter a website that requires account security questions, you should use random words to answer those questions. Then store the random answers in your password manager. Be sure to use a passphrase generator like this one. For example, the answer to *"What was the name of your high school?"* might be "*mystique parterre virelay*".

VPNs

Using a personal VPN can do more harm than good. A VPN is a complex piece of software and several have had serious vulnerabilities. Some personal VPN providers collect data on their users and their activities. And there's very little need for most people to use one, most of the time.

To limit the leakage of private information, do not use a VPN, but instead, use the free plugin HTTPS everywhere, install an ad blocker like uBlock Origin, and set up secure DNS in your browser.

Web encryption

Some websites do not properly enable encryption for all connections. Luckily, there is something you can do to make sure your internet connections are secure. In your web browser, you should install the HTTPS Everywhere extension. HTTPS Everywhere is a Firefox, Chrome, and Opera extension that strengthens the encryption between your device and major websites.