DNC Security Checklist

Updated: March 2024 by the DNC Security Team

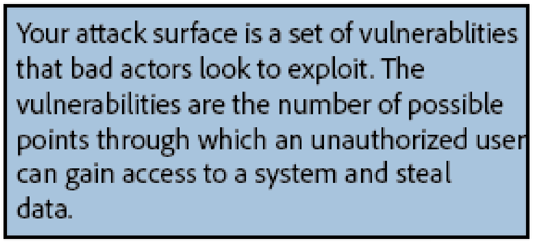
Welcome!

- ★ We strongly encourage anyone who works in politics, campaigns, or simply has a device or an account on the internet to take these precautions.
- ★ Prioritize the accounts that are most important to your daily life, such as your email, financial/banking, social media, and file storage accounts.
- ★ Questions? Email security@dnc.org.

Why do you need the Security Checklist?

The DNC Security Checklist's goal is to reduce your cyber attack surface. Your attack surface is a set of vulnerabilities that bad actors look to exploit, including computers, smart phones, hard drives, and even users themselves.

Vulnerabilities include weak passwords, no email security, software that isn't updated, and more. These all give attackers a way to target users and organizations.



Your attack surface is a set of vulnerablities that bad actors look to exploit. The vulnerabilities are the number of possible points through which an unauthorized user can gain access to a system and steal data.

This checklist includes a variety of security topics to help you stay safe. The more security settings you enable, the smaller your attack surface becomes!

Click here for a print-friendly version of the checklist

Step 1: Use Strong Two-Factor Authentication

Secure all personal and work accounts:

Enable two-factor authentication (2FA) on all sites (Learn more). 2FA adds a powerful layer of security to your accounts - if your password is hacked or phished, this second layer of approval helps keep your accounts safe. Select the strongest form of 2FA in the following priority order:

1. **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.
2. **Authenticator App:** These apps generate a 6 digit code that changes every 30 seconds and verifies your identity. Google Authenticator, Duo or Authy are some examples.
3. **Email:** Email is only recommended if your account has 2FA configured as well.
4. **SMS/text messages:** Avoid SMS/text message as your 2FA unless it is the only option. Ensure you have a *long*, *random*, *unique* password if so.

Prioritize the accounts that you use daily and hold the most sensitive information and work your way down the list.

Enable Two-Factor Authentication	Personal	Work
Operating System Profile: Apple ID Microsoft account (includes Skype & XBox accounts)	❑	❑
Email: Gmail Outlook Yahoo AOL	❑	❑
Campaign Tools (Examples): NGP/Votebuilder Action Network ActBlue Scale to Win	❑	❑
Social Media: Facebook TikTok Instagram Twitter	❑	❑
Other Social: LinkedIn Snapchat Pinterest WhatsApp Slack Skype (Microsoft account)	❑	❑

File Storage: Box Dropbox Evernote	❑	❑
Financial services: CashApp Venmo PayPal Square Credit Cards Investment/401k Accounts Banks Coinbase Wallet Bitcoin MetaMask	❑	❑
Gaming: Nintendo Twitch XBox (Microsoft account)	❑	❑
Ecommerce sites: Amazon Etsy	❑	❑
Streaming sites and music—especially those you share with others— Disney+, HBO, Hulu, Netflix, SoundCloud, etc.	❑	❑
Travel: Airbnb, airline accounts, Lyft, Uber, transit apps	❑	❑
Miscellaneous sites: Salesforce, Yelp, Untappd	❑	❑

Step 2: Use a Password Manager

Set up a password manager to generate, store, and auto-fill all of your passwords. (Learn more). These help keep you digitally secure by simplifying how you use and store strong passwords.

Password Managers	Personal	Work
Paid Options: 1Password Dashlane LastPass ***Free Options:*** Dashlane Apple Keychain LastPass Google Password Manager	❑	❑
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. We also recommend a passphrase for anything you have to type in frequently (like your Netflix password). *Sample strong passphrase: worshiper favoring visa nest*	❑	❑
Add strong two-factor authentication to your password manager, preferably a security key. Read more here: 2FA. **Guides:** 1Password, Dashlane, LastPass.	❑	❑
Download your password manager's mobile app.	❑	❑
Add your password manager's browser plugin. **If you use Chrome:** 1Password, Dashlane, LastPass	❑	❑

Step 3: Secure Your Devices

Adversaries 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. (Learn more)

Securing Your Devices	Personal	Work
Make sure your phones and laptops are running the most up-to-date operating system. Mac iPhone/iPad Android PC	❑	❑
Enable "Find My Device" features Apple Microsoft Android	❑	❑
Laptop disk encryption: Macs PCs (*not included with Windows 10 Home)* ***Note:*** 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	❑	❑
Cell Phone Carrier Pin: Enable a carrier login pin to allow changes to your account.		

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)	❑	❑

Step 4: Take Your Security Up a Notch

Take additional steps to protect yourself from bad actors.

Securing Your Gmail	Personal	Work
Gmail: Enroll in Google's Advanced Protection Program (APP) to reduce the risk of getting phished (Learn more).	❑	❑
Gmail: Complete the Gmail security checkup	❑	❑

Secured Messaging (Learn more)	Personal	Work
Use Secured Messaging Apps: Signal Wickr	❑	❑

Web Encryption (Learn more)	Personal	Work
Safe browsing: Enable "HTTPS only" mode on all web browsers like Chrome or Firefox.	❑	❑
Block ads: Install the uBlock Origin extension on your web browser.	❑	❑

Privacy Settings (Learn more) Review privacy settings on the following sites and services:	Personal	Work
iOS: Remove location data from your photos. Perform Safety Check to review and update sharing with people and apps.	❑	❑
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 turning off location services. ***Note:*** Consistent with previous guidance, if you’re using TikTok for campaign work, we recommend taking additional precautions, like using a separate phone and account.	❑	❑
Venmo: Make your transactions private.	❑	❑

Congratulations, you made it to the end of the DNC Security Checklist! Scroll down to read more about cybersecurity best practices. Please return to this page from time to time for any updates.

Stay safe and secure,
DNC Security Team

Appendix

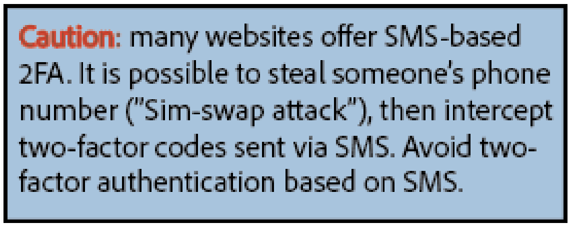
Two-Factor Authentication

Two-factor authentication (2FA) protects online accounts and data. Online accounts like email or social media can require two or more authenticators to verify your identity when 2FA is enabled. 2FA provides additional account security. Two-factor authentication reduces hacking risk. Why? Because even if a malicious cyber actor compromises one factor (like your password), they cannot meet the second authentication requirement, preventing them from accessing your accounts.

Whether you call it two-factor authentication, multi factor authentication, two-step verification, MFA, or 2FA, you use a combination of something you have, something you know, or something you are to verify your identity online.

Use the strongest form of 2FA available on each service.

1. **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.
2. **Authenticator App:** These apps generate a 6 digit code that changes every 30 seconds and verifies your identity. Google Authenticator, Duo or Authy are some examples.
3. **Email:** Email is only recommended if it has 2FA configured as well.
4. **SMS/text messages:** Avoid SMS/text message as your 2FA unless it is the only option. Ensure you have a *long*, *random*, *unique* password if so.



Caution: many websites offer SMS-based 2FA. It is possible to steal someone's phone number ("Sim-swap attack"), then intercept two-factor codes sent via SMS. Avoid two-factor authentication based on SMS.

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.

Additional resources:

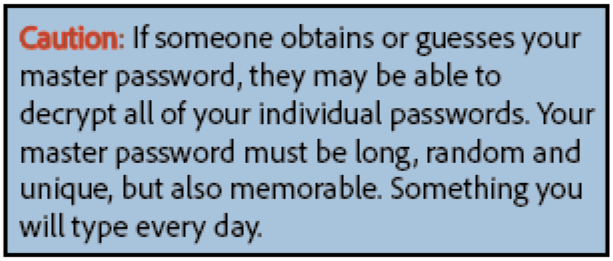
- CISA Multifactor Authentication
- Walk This Way to Enable MFA
- Multi-Factor Authentication (Fact Sheet)
- 4 Things You Can Do to Stay Cyber Safe

Password Managers

Password managers such as Dashlane, 1Password and LastPass 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 username 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. (We highly recommend keeping your work and personal accounts/data separate whenever possible!) Group features of password managers can also help securely share passwords with trusted friends and family.

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."



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

Security Questions
A few websites still rely on using account security questions 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. For example, the answer to *"What was the name of your high school?"* might be "*mystique parterre virelay*".

Secured Devices

Adversaries 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.

Use a device that is secure-by-design.
Secure-by-design is the concept that a software product and its capabilities have been designed to be secure at its foundation. Look for devices that are built with this in mind -

for example, consider using a Chromebook or an iPad. Both devices offer a number of key security features, and dramatically limit the options adversaries have for running malware.

How do I block all ads on my iPhone?

On your iPhone, iPad, or iPod touch, go to Settings > Safari and turn on Block Pop-ups and Fraudulent Website Warning. On your Mac, you can find these options in Safari > Preferences. The websites tab includes options to block some or all pop-up windows, and you can turn on fraudulent site warnings in the security tab.

Mobile Phone Pin

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.

Mail Providers

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

Secured 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. 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.

We recommend using messaging apps that are encrypted in transit and at rest and support disappearing messages. Some examples are Signal, Wickr, or WhatsApp - keep in mind each has limitations.

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

Web Encryption

Some websites do not enable encryption for all connections. Luckily, you can make sure your internet connections are secure. In your web browser, enable HTTPS by default in your browser. HTTPS strengthens the encryption between your device and major websites. Previously, the DNC recommended users install the *HTTPS Everywhere* extension to your web browsers, but major browsers now offer HTTPS Only Mode. As of January 2023 the browser extension is retired.

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. 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, enable HTTPS by default in your browser, install an ad blocker like uBlock Origin, and set up secure DNS in your browser.

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 DNC Security Checklist on their personal accounts.

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 public 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!

Crypto-Asset Protection

Blockchains now offer a variety of options for securing your cryptocurrency funds via crypto wallets. To keep your funds safe when trading, storing, and using them, it's best to trust in simple but effective ways and choose a storage medium with the benefits and drawbacks of each option in mind. Before depositing your money or cryptocurrency anywhere, make sure to thoroughly research all available information.

Personal information: Crypto-assets require separate accounts, such as email and phone numbers. It is critical to keep personal data out of the public eye on platforms like social media, messenger apps, or blogs.

Protecting your account: Your account will be more secure with two-factor authentication! It can significantly increase account security when used in conjunction with other security measures.

It always helps to use as many security features as possible:

- SMS confirmation
- anti-phishing code
- two-factor authentication
- email verification code

Seed-phrase authentication: Some people may frequently use the same password for all sites and applications. If your password contains publicly available personal information or is a simple digital password, an intruder can easily crack it using brute force or software. Wallet seed phrase, sometimes called a mnemonic code, recovery phrase, or mnemonic sentence, is a secret that can be used to restructure your crypto wallet and make transactions. A well-chosen seed phrase is a good way to protect your wallet because it can't be guessed. However, if someone comes up with a clever way to steal your seed phrase, they could rebuild your wallet and steal all of your crypto.

Asset allocation: To reduce the risk of losing more funds, we also recommend dividing your cryptocurrency portfolio into different vaults. Consider using a combination of crypto exchanges and crypto wallets, for example. Prioritize accounts that you use daily and hold the most sensitive information and work your way down the list.

QR Codes

QR (Quick Response) codes are a type of barcode that can be read by a smart device to direct users to a website, a PDF file, questionnaire, video, audio, and more. They have surged in popularity over the past few years. Originally used to track inventory in factories, they are now commonly used at restaurants and in retail.

The widespread adoption of QR codes means there are growing privacy and security concerns. Bad actors can create malicious QR codes to download malware onto your device, send users to a phishing site, or even track your geolocation on their phone.

Keep in mind some best practices. **Check the code** for suspicious elements. Are there dubious frame texts around the code? Does the logo appear legitimate in the middle of the code? Does the code design match the brand's colors and specifications? **Verify the URL.** When you scan a QR code with the camera on your smart device, you'll see a small notification pop-up on the screen. The confirmation prompt shows the URL you'll visit. You should check and verify the URL for malicious signs and only click if it is a secure and legitimate site (starts with https://).

Updated 2024-3