DNC Online Privacy Checklist

Updated: May 2026 by the DNC Security Team

Welcome!

★ People who work on campaigns and in elections may face greater risk on the internet both at home and at work when their digital footprint is used against them and exploited by bad actors. We want to help you mitigate these risks. Use this guidance to:

- Prevent manipulation and intimidation practices associated with doxing
- Discourage social engineering
- Safeguard your sensitive information against identity and location tracking

★ Don't try to complete all of these recommendations at once. Pick one or two at a time to avoid "privacy fatigue."

★ Questions? Email security@dnc.org.

Why do you need online privacy recommendations?

Our digital lives tend to get cluttered. Over time, we accumulate apps we don't use, permissions we don't remember granting, and accounts we've long forgotten. Safeguarding our privacy now requires more than just a "strong password." With the rise of massive data breaches, AI-driven phishing, and aggressive data scraping, our digital footprint can act as a map for bad actors. Instead of just guessing, they can use your data — geographic information, hobbies, and even information about your loved ones — to triangulate your vulnerabilities, leading to dangerous outcomes like doxing, swatting, or stalking.

This checklist includes a variety of recommended privacy topics to help you stay safe. The more steps you complete, the more you reduce your risk!

Click here for a print-friendly version of the checklist

Where to start: Protecting Personally Identifiable Information (PII)

You might not hear PII (Personally Identifiable Information) and SPII (Sensitive PII) every day, but these acronyms are key to your digital identity. Minimizing the public presence of these types of information is critical to protecting your online privacy.

PII can identify an individual (e.g., name, address, email) and is found in common data sources like social media, shipping labels and marketing databases. SPII is a subset of PII (e.g., SSN, credit card numbers, medical records) that, if compromised, can cause significant harm.

Who wants access to this information and why?

The market for personal data is massive, split between legal collectors (governments, employers, financial/healthcare institutions) and illegal collectors (cybercriminals, state-sponsored actors, scammers). These are only a few examples, but good to remember when deciding to provide any personal information to persons, forms, and websites.

PII can be used for a range of legitimate activities like identity verification, ad targeting, and personalization, to illegal activities like fraud, doxing, extortion and identity theft.

Step 1: Reduce Your Digital Footprint

Your digital footprint, the trail of data you leave online, can be a valuable resource for adversaries looking to exploit your information. Minimizing this footprint is a critical, ongoing process to limit the amount of PII available to data brokers and bad actors.

When identifying where to clean up your information, be sure to prioritize the accounts that you use daily that hold the most sensitive information, then work your way down the list.

Critical Defenses	Personal	Work
Apply all items from the DNC Security Checklist, including using a Password Manager and Phish-proof 2FA or Multi-Factor Authentication.	❑	❑

Updated 2026-05

The High Impact Essentials (Set & Forget)	Personal	Work
Enable Auto-Updates: Check operating systems (Windows/macOS), Browsers (Chrome/Firefox), smartphones, and log into your router admin panel to toggle "Auto-update firmware."	❑	❑
Freeze Your Credit: You must do this individually at all three credit bureaus: Equifax Experian TransUnion	❑	❑

Step 2: Data & Identity Thinning

Data and identity thinning is the process of removing your Personally Identifiable Information (PII) from the internet where it no longer needs to be, and consolidating your digital accounts to reduce your attack surface. By systematically cleaning up old, fragmented, or unnecessary personal data, you make it more difficult for adversaries to build a comprehensive profile of you.

Data Thinning	Personal	Work
Fight Against Data Brokers ***Paid Options***: DeleteMe Optery.com InCogni ***Free Options:*** Review the NYT Open Source Resource Guide Intel Techniques Extreme Privacy	❑	❑
Use Email Aliases ***Free Option:*** SimpleLogin ***Paid Option:*** iCloud+ Hide my Email	❑	❑

Data Breaches and Recovery

Before you can secure your digital footprint, you have to know what is already out there. Start by visiting Have I Been Pwned, a trusted industry-standard tool that tracks billions of leaked records. By entering your email address, you can see a list of which specific data breaches have compromised your information and, more importantly, what types of data (such as passwords, birthdates, or phone numbers) were exposed. Use this report as your roadmap: it will tell you which accounts need immediate password resets and which services you may want to close entirely.

1. **Discover**: Visit Have I Been Pwned to check if your email address or phone number has been part of a data breach.
2. **Triage**: Prioritize the most recent breaches and accounts involving financial data.
3. **Rotate**: Change passwords and use passkeys, focusing on any accounts that share the leaked password. If an account does not have MFA, add it now.
4. **Verify**: Check your "Sent" folder in your email and your "Recent Activity" on social media for any unauthorized posts or messages.

Step 3: Browser & Device Hardening

Devices and browsers are often the first points of attack for bad actors, as outdated software and lax settings can create critical security vulnerabilities. "Hardening" your device means taking proactive steps to configure your operating system, applications, and web browser for maximum defense.

Browser Hardening	Personal	Work
Auto Updates: Enable “Automatic Updates” on your Operating System, Browser and Router.	❑	❑
Browser Privacy Settings: Chrome Firefox Safari	❑	❑
Ad Blocker: uBlock Origin (if you use Chrome, then uBlock + Privacy Badger)	❑	❑

Updated 2026-05

Disable Your Ad ID: On your phone (iOS or Android) and Windows/macOS, go to Privacy settings and "Reset/Disable Advertising ID." This prevents apps from linking your activity to a specific "buyer profile." Chrome iOS Android	❑	❑

Smart Device & IOT (Internet of Things) Hardening	Personal	Work
Use a Strong, Unique Password. Change the factory-set name and password on all new smart devices (security cameras, smart speakers, routers). Never use the default password.	❑	❑
Separate Your Smart Devices from Work. If your router has a "Guest Wi-Fi" option, connect your smart devices (like TVs or speakers) to it. This keeps them off the same network as your primary personal or work devices.	❑	❑
Turn Off Features You Don't Use. Go into your device settings or router menu and disable unnecessary functions, like remote control access or "Universal Plug and Play (UPnP)," which can open up security holes.	❑	❑
Audit Microphone and Camera Settings. Check the privacy settings on devices like smart speakers and cameras. Limit how long they keep recordings and restrict which apps, and when they can access the microphone or camera.	❑	❑
Install All Security Updates. Make sure your IOT device apps or settings are set to automatically install updates. If they don't, manually check the manufacturer's website for security patches often.	❑	❑

Updated 2026-05

Step 4: Mobile Device Hardening

Your mobile devices (smartphones and tablets) are perhaps the most critical assets to secure, as they are constantly connected and hold a vast amount of sensitive personal and work data. "Mobile Device Hardening" focuses on taking additional, specific steps to lock down the security and privacy settings on these devices and the apps installed on them. This proactive approach ensures that even your most portable technology is resilient against threats like phishing, data scraping, and location tracking.

Mobile Device Hardening	Personal	Work
Turn off location tracking or precise location unless needed Android iPhone Samsung	❑	❑
Cell Phone Carrier Pin: Enable a carrier login pin to prevent SIM card swaps. AT&T: Set in your Profile (instructions) T-Mobile/Sprint: Set at Customer Care or call 800-937-8997 (more info) Verizon: Set at Security (instructions)	❑	❑
Enable remote lock and remote wipe: Android Phone Samsung	❑	❑
Set app location permissions to “while using” or “never” Android iPhone Samsung	❑	❑
Limit or block apps from accessing your contacts Android iPhone Samsung	❑	❑
Turn off Microphone/Camera on apps that don't need it Android iPhone Samsung	❑	❑
Disable background app refresh for apps that don't need it	❑	❑

Updated 2026-05

Turn off auto-join for public networks	❑	❑
Disable Bluetooth when not in use and make sure the device is not in "discoverable" mode If Bluetooth is enabled, restrict AirDrop and file sharing capabilities. iPhone AirDrop Google Play Store - Quick Share	❑	❑
Note: If you work in a highly sensitive position or role, utilize Lockdown Mode on iPhone or GrapheneOS on Android. Android iPhone	❑	❑

Privacy Settings	Personal	Work
iOS: Remove location data from your photos. Perform a Safety Check to review and update sharing with people and apps.	❑	❑
Paid Option: Deep clean your social media accounts with Block Party. Note: Federal campaigns and committees are eligible for a free one-year subscription. Check out defendcampaigns.org.	❑	❑
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.	❑	❑
Strava: Review your privacy settings. Hide portions of your exercise activity by editing map visibility.	❑	❑

Updated 2026-05

X (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.	❑	❑
Venmo: Make your transactions private.	❑	❑
Enter your commonly used handles into https://namecheckr.com to see where that handle is being used to discover old accounts you may have set up, as well as keep an eye out for impersonation accounts.	❑	❑

Congratulations, you made it to the end of the DNC Online Privacy Checklist! Scroll down to read more about some of the concepts listed above and best practices. Please return to this page from time to time for any updates.

Stay safe and secure,
DNC Security Team

Updated 2026-05

Dive Deeper: Appendix

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 Apple Device.

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.

Freezing Your Credit

Freezing your credit is a free and easy way to restrict access to your credit reports. When you do this, creditors cannot access your credit report, which stops them from opening new credit accounts in your name. If your social security number is compromised, bad actors can't use it to open credit cards in your name. You can always temporarily lift the freeze to open a new credit account yourself!

This can also be done with any minors and dependents.

Fight Against Data Brokers

Each time you go online or use a digital service, you leave a trail of information behind you. This data is often sold and used by third parties. Services like DeleteMe, Optery, and Incogni help to systematically remove your data from data warehouses that typically broker your information.

You can also do this at no cost by locating the opt-out link for all of the most popular data warehouses. Keep in mind that data brokers frequently refresh their databases, meaning your personal information can reappear within months of being removed. You will want to revisit opt-out links every three to four months.

Email Aliases

Your personal email address is a fundamental part of your digital identity. Just like with your phone number, you don't want to give it to everyone you meet. Many websites and online services use email addresses as your identifier. Using aliases makes it more difficult for interested parties to gather information on you.

If your aliased email starts receiving emails from a site you didn't sign up for, it is an indicator that an entity has either suffered a data breach or has sold your information. In these cases, you can simply delete the email alias. Additionally, if you use the same email address for all of your logins and there is a breach, your email address will likely be leaked.

What are PII and SPII, and where are they found?

Not all data is created equal. Security professionals categorize information based on how much damage would occur if it were leaked.

PII (Personally Identifiable Information) is any data that can be used to identify a specific individual, either alone or when combined with other relevant info.

- Examples: Full name, home address, email address, and phone number.
- Where it's found: Social media profiles, shipping labels, marketing databases, and public records.

SPII (Sensitive Personally Identifiable Information) is a subset of PII that, if lost or compromised, could lead to significant harm, such as identity theft or financial loss. It usually requires higher levels of encryption and legal protection.

- Examples: Social Security Numbers (SSN), credit card numbers, biometric data (fingerprints), and medical records.
- Where it's found: Human Resources (HR) databases, hospital records, banking portals, and tax filings.

Your PII/SPII May be Collected by:

- Federal, state and local Governments: For taxation, law enforcement, and providing social services.
- Employers: For payroll, benefits administration, and background checks.
- Financial Institutions: To verify identity for loans and prevent money laundering.
- Healthcare Providers: To maintain accurate medical histories and process insurance claims.
- Private Companies: To provide services and software for public and private access.

PII can be used for illegal or nefarious gains by:

- Cybercriminals: To sell on the dark web or use for identity theft.

- State-Sponsored Actors: For espionage, surveillance, social engineering or gaining leverage over foreign citizens.
- Scammers: To craft "spear-phishing" attacks that look incredibly convincing because they include your real details.

PII can be used for:

- Verification: Confirming you are who you say you are when logging into a bank or applying for a job.
- Ad Targeting: Advertisers use PII to show you products they think you'll buy based on your location and history.
- Fraud: Using SPII to open "ghost" lines of credit, claim your tax refund, or steal your medical insurance.
- Personalization: Streaming services or retailers use your data to remember your preferences and shipping info.

Are You a High Risk Individual?

Depending on your role and the work you do for Democrats, you could face higher risks than your average internet user. Calculating an individual's risk is nuanced, so we always want to be more cautious, instead of less. Some characteristics to consider when thinking through your risk factors:

- Do you have a high-profile or high-visibility role?
    - If you say yes to this, you are at high risk because of who you are. Bad actors want to compromise our Democratic message and reputation and may try to do so by targeting you.
- Do you have access to confidential data, or data that could be considered useful to bad actors?
    - If you say yes to this, it's possible you will be the target of an attack because of what and who you have access to.

Glossary of Terms

Data Breaches: A data breach is a security violation in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.

Data Minimization: The principle that only the minimum amount of personal data necessary to fulfill a specific, legitimate purpose should be collected, processed, and retained. It is a core tenet of modern privacy frameworks.

Data Scraping: Data scraping is the process of using automated tools to extract large amounts of data from websites and online sources. How Websites and Apps Collect and Use Your Information | Consumer Advice

Data Warehouses: These companies specialize in gathering data from a vast number of sources, including public records, social media, consumer purchase histories, and other online activity. They combine this fragmented data to build comprehensive profiles on billions of people. What To Know About People Search Sites That Sell Your Information | Consumer Advice

Digital Footprint: The trail of information you leave behind every time you use the internet, from websites you visit and posts you share, to purchases you make and apps you use. Some of it you share on purpose, while some of it is collected automatically without you realizing it. Think of it like footprints in the sand, except these don't wash away.

Passkeys: A passkey is a secure way to log in to apps and websites without needing a password. Instead of typing a secret word or phrase, you simply use your fingerprint, face, security key or device PIN to prove it's you.

People Search sites: These websites act as the public-facing storefronts for the data brokers. They allow anyone to search for an individual by name, phone number, or address, and for a fee, they will display the compiled personal profile.

Phishing: This is a specific type of social engineering attack carried out primarily through electronic communications, such as email, text messages (smishing), or phone calls (vishing). The goal is to fraudulently acquire sensitive information like usernames, passwords, credit card details, or other personally identifiable information (PII).

PII (Personally Identifiable Information): It is any data that could potentially be used to identify you. Examples of PII include:

- Full name
- Home address
- Email address
- Phone number

Social Engineering: This is a manipulation technique that exploits human error to gain access to private information, systems, or accounts. It relies on psychological tactics — such as creating a sense of urgency, fear, or trust — to trick a victim into performing an action or divulging confidential data.

SPII (Sensitive Personally Identifiable Information): Examples of SPII include

- Social Security Number
- Passport number
- Driver's license number

Swatting: This is a dangerous and illegal harassment tactic where someone makes a deceptive 911 call to trigger a massive police response, specifically a SWAT team, to an innocent person's address. The goal is to trick law enforcement into believing a high-stakes emergency is in progress, such as a hostage situation, a bomb threat, or a murder, forcing them to arrive with weapons drawn.

Underground Economy: In the context of online privacy and data, the underground economy specifically refers to the cybercrime ecosystem where stolen data and illegal services are

bought and sold. This marketplace is crucial to how PII (Personally Identifiable Information) ends up being exploited after a data breach or phishing attack.