Datacash

The Privacy Playbook

50+ Actionable Tips to Secure Your Digital Life

A Datacash Publication written by Devo Wright.

The Privacy Playbook: 50+ Actionable Tips to Secure Your Digital Life

Table of Contents

Introduction: Why Digital Privacy Matters Now More Than Ever

In the digital age, our lives are recorded in bits and bytes. Every click, every search, every purchase, and every conversation can be stored, analyzed, and monetized. While this data-driven world offers incredible convenience, it also presents unprecedented risks to our privacy.

Data breaches are becoming a daily occurrence, exposing the sensitive information of millions. Tech companies, advertisers, and data brokers are constantly creating detailed profiles about us to predict and influence our behavior. And governments are increasingly using surveillance technologies to monitor their citizens.

Digital privacy isn't about having something to hide. It's about having something to protect: your identity, your autonomy, and your security. It’s about controlling your own narrative and deciding for yourself who gets to know what about you.

That's why we at Datacash, a 501(c)(3) nonprofit dedicated to advancing data literacy, privacy, and digital rights, have created this playbook. We believe that everyone deserves the knowledge and tools to protect themselves online. This guide is a key part of our mission to make digital privacy accessible to all.

We’ll skip the dense technical jargon and focus on actionable, easy-to-implement steps you can take today to secure your digital life. You don’t need to be a cybersecurity expert to make a huge difference.

Welcome to the Privacy Playbook, a resource from your friends at Datacash. Let's get started.

Chapter 1: Securing Your Digital Foundations

Before you can build a private digital life, you need a strong foundation. This chapter covers the absolute essentials of digital security.

1.1 Mastering Password Management

Your password is the front door to your digital life. A weak password is like leaving that door unlocked.

- **Play #1: Use a Password Manager.** Stop trying to remember dozens of complex passwords. At Datacash, we recommend using a password manager (like Bitwarden, 1Password, or LastPass) to generate and store strong, unique passwords for every single account. You only need to remember one master password.
- **Play #2: Create a Strong Master Password.** Your master password should be long and memorable. A phrase or a series of random words (e.g., "Correct-Horse-Battery-Staple") is much stronger than a short, complex password.
- **Play #3: Never Reuse Passwords.** If one site gets breached, criminals will try that same password on every other popular service. A password manager makes using unique passwords easy.

1.2 Enabling Two-Factor Authentication (2FA) Everywhere

2FA adds a second layer of security to your accounts. Even if someone steals your password, they won't be able to log in without your second factor.

- **Play #4: Use an Authenticator App.** Instead of SMS (text message) 2FA, which can be vulnerable to SIM-swapping attacks, use an authenticator app like Google Authenticator, Authy, or Microsoft Authenticator.
- **Play #5: Enable 2FA on All Critical Accounts.** Start with your email, password manager, social media, and financial accounts. Go through your password manager and enable 2FA on every service that supports it.
- **Play #6: Store Your Backup Codes Securely.** When you enable 2FA, you'll be given backup codes. Print them out and store them in a safe place, like a safe or a locked drawer. Don't store them on your computer or phone.

1.3 Understanding and Using VPNs

A Virtual Private Network (VPN) encrypts your internet traffic and hides your IP address, making it much harder for your Internet Service Provider (ISP), public Wi-Fi networks, and websites to track you.

- **Play #7: Choose a Reputable VPN Provider.** Do your research. Look for a VPN provider with a strict no-logs policy, a good reputation, and servers in the locations you need. Avoid free VPNs, as they often make money by selling your data.
- **Play #8: Use a VPN on Public Wi-Fi.** Public Wi-Fi networks are notoriously insecure. Always use a VPN when connecting to Wi-Fi at a coffee shop, airport, or hotel.

- **Play #9: Understand the Limits of a VPN.** A VPN doesn't make you anonymous. It hides your IP address from the websites you visit, but they can still track you with cookies and other tracking technologies. It also doesn't protect you from malware or phishing scams.

1.4 Secure Your Home Wi-Fi Network

Your home Wi-Fi network is the gateway to all of your connected devices. It needs to be secure.

- **Play #10: Change the Default Router Password.** Don't use the default admin password that came with your router. Change it to something strong and unique.
- **Play #11: Use WPA3 or WPA2 Encryption.** Make sure your Wi-Fi network is using the latest encryption standard. WPA3 is the newest and most secure, but WPA2 is still a strong option.
- **Play #12: Create a Guest Network.** If your router supports it, create a separate guest network for visitors. This will keep their devices off of your main network and away from your personal devices.
- **Play #13: Disable WPS.** Wi-Fi Protected Setup (WPS) is a feature that's designed to make it easy to connect devices to your router, but it's also a major security vulnerability. Disable it in your router's settings.

Chapter 2: Taming Your Web Browser

Your web browser is your window to the internet. It's also one of the primary ways that companies track you online. This chapter will show you how to make your browser a tool for privacy, not a tool for tracking.

2.1 Choosing a Privacy-Focused Browser

Not all browsers are created equal when it comes to privacy.

- **Play #14: Ditch Google Chrome.** Chrome is a data-harvesting machine for Google's ad business. While it's a fast and convenient browser, it's not a private one.
- **Play #15: Use Firefox with Custom Settings.** Firefox is a great open-source browser with strong privacy features. Be sure to enable "Enhanced Tracking Protection" to its "Strict" setting for the best results.
- **Play #16: Consider Brave or DuckDuckGo.** Brave is a browser with a built-in ad and tracker blocker. The DuckDuckGo browser is a mobile browser that offers excellent privacy protection by default.

2.2 Essential Browser Extensions for Privacy

Browser extensions can add powerful privacy protections to your browser.

- **Play #17: Install an Ad Blocker.** UBlock Origin is the gold standard of ad blockers. It blocks ads and trackers, which not only improves your privacy but also makes web pages load faster.
- **Play #18: Use a Tracker Blocker.** Privacy Badger is a great extension from the Electronic Frontier Foundation (EFF) that learns to block invisible trackers.
- **Play #19: Always Connect over HTTPS.** HTTPS Everywhere is an extension that encrypts your communications with many major websites, making your browsing more secure.

2.3 Managing Cookies and Site Data

Cookies are small files that websites store on your computer. Some are useful, but many are used to track you across the web.

- **Play #20: Block Third-Party Cookies.** Third-party cookies are the primary way that advertisers track you from site to site. Your browser's settings should allow you to block them.
- **Play #21: Clear Your Cookies Regularly.** Get in the habit of clearing your cookies and site data every week or so. Some browsers can be set to do this automatically when you close them.
- **Play #22: Use Container Tabs (Firefox).** Firefox's Multi-Account Containers extension lets you isolate your web browsing into different color-coded tabs. This prevents websites from tracking you between, for example, your work, personal, and social media browsing.

2.4 The Power of Private Browsing (and Its Limits)

Private browsing modes (like Chrome's Incognito mode) have their uses, but they're not a silver bullet for privacy.

- **Play #23: Understand What Private Browsing Does.** Private browsing primarily prevents your browsing history and cookies from being stored on your computer. That's it.
- **Play #24: Understand What It Doesn't Do.** Private browsing does *not* hide your IP address from the websites you visit, nor does it prevent your ISP from seeing what sites you're visiting. It also doesn't protect you from malware or phishing.
- **Play #25: Use It for Specific Tasks.** Private browsing is useful for logging into your accounts on a shared computer or for looking up sensitive information that you don't want stored in your search history.

This is a start. I will continue to add more content in subsequent turns.

Chapter 3: Social Media Privacy Settings

Social media platforms are designed to get you to share as much information as possible. This chapter will help you take control of your data on the most popular platforms.

3.1 Auditing Your Facebook Privacy Settings

Facebook has a dizzying array of privacy settings. Here’s where to focus.

- **Play #26: Use the Privacy Checkup.** Facebook's Privacy Checkup tool is the best place to start. It will walk you through who can see your posts, what information is on your profile, and how people can find you.
- **Play #27: Limit Who Can See Your Past and Future Posts.** Set your future posts to "Friends" and use the "Limit Past Posts" tool to change the audience for all of your old public posts to "Friends" as well.
- **Play #28: Control How People Can Find You.** Do you want people to be able to find you using your email address or phone number? Do you want search engines to link to your profile? You can control all of this in the privacy settings.
- **Play #29: Manage Your Ad Preferences.** Facebook knows a lot about you, and it uses that information to show you targeted ads. You can see what Facebook thinks it knows about you and remove interests that you don't want to be used for advertising.

3.2 Locking Down Your Instagram Account

Instagram is owned by Facebook, so many of the same privacy principles apply.

- **Play #30: Make Your Account Private.** This is the single most important thing you can do to improve your Instagram privacy. With a private account, only people you approve can see your photos and videos.
- **Play #31: Control Who Can Interact with You.** You can limit who can comment on your posts, who can tag you in photos, and who can send you direct messages.
- **Play #32: Be Mindful of What You Share in Your Stories.** Instagram Stories are designed to be ephemeral, but they can still be saved and shared. Be careful about what you post, and use the "Close Friends" feature to share more personal moments with a smaller group of people.

3.3 Managing Your Twitter/X Data

Twitter (now X) has a more public nature, but you still have control over your data.

- **Play #33: Protect Your Tweets.** A protected account means that only your followers can see your tweets.
- **Play #34: Manage Your Location Data.** You can choose to add a location to your tweets, but it's generally a good idea to leave this turned off.
- **Play #35: Review Your "Interests and Ad Data".** Like Facebook, Twitter builds a profile of you for advertising purposes. You can review and edit this profile in your settings.

3.4 LinkedIn: Professional Networking with Privacy in Mind

LinkedIn is a professional network, but that doesn't mean you should share everything.

- **Play #36: Control Who Can See Your Profile and Network.** You can choose to make your profile visible to everyone, only your connections, or only people who have your email address.
- **Play #37: Manage How You Appear Off of LinkedIn.** LinkedIn has partnerships with other companies that allow them to show your profile information on other sites. You can opt out of this in your settings.
- **Play #38: Be Selective About Who You Connect With.** Don't feel pressured to accept every connection request you receive. It's okay to only connect with people you know and trust.

Chapter 4: Beyond the Desktop: Mobile & App Privacy

Our smartphones are with us all the time, and they're packed with sensors that can collect a huge amount of data about us. This chapter will show you how to lock down your mobile device.

4.1 App Permissions on iOS and Android: A Deep Dive

The apps on your phone are one of the biggest sources of data leakage.

- **Play #39: Be Mindful When Granting Permissions.** When you install a new app, it will ask for permission to access things like your location, contacts, and photos. Don't just click "yes" to everything. If an app doesn't need access to something to function, don't grant it.
- **Play #40: Regularly Review Your App Permissions.** Both iOS and Android have a privacy dashboard that shows you which apps have access to which data. Go through this regularly and revoke any permissions that you're not comfortable with.
- **Play #41: Delete Apps You Don't Use.** If you're not using an app, delete it. It's one less thing you have to worry about.

4.2 Secure Your Device: PINs, Biometrics, and Encryption

Your phone contains a huge amount of personal information. It needs to be locked down.

- **Play #42: Use a Strong PIN or Passcode.** A six-digit PIN is a good start, but a longer alphanumeric passcode is even better.
- **Play #43: Use Biometrics (Face ID or Fingerprint).** Biometrics are a convenient way to unlock your phone, but they're not a replacement for a strong PIN. Think of them as a convenience, not a security feature.
- **Play #44: Make Sure Your Device is Encrypted.** Modern smartphones are encrypted by default, but it's a good idea to double-check. On Android, you can find this in the security settings. On iOS, encryption is enabled as long as you have a passcode set.

4.3 Location Services: Who’s Tracking You?

Your phone's location is one of the most sensitive pieces of data it collects.

- **Play #45: Limit Which Apps Can Access Your Location.** Do you really need to give your weather app access to your location all the time? Probably not. Set location permissions to "While Using the App" whenever possible.
- **Play #46: Turn Off Location History.** Both Google and Apple keep a detailed history of your location. You can (and should) turn this off in your account settings.
- **Play #47: Be Wary of Geotagging Photos.** When you take a photo, your phone can save the location where it was taken as part of the photo's metadata. Be careful about sharing photos with this information online.

4.4 Secure Messaging Apps: Signal, WhatsApp, and Telegram

Not all messaging apps are created equal when it comes to privacy.

- **Play #48: Use Signal for Secure Communication.** Signal is the gold standard for secure messaging. It's end-to-end encrypted by default, and it's run by a nonprofit organization, which is a model we at Datacash strongly support.
- **Play #49: Understand WhatsApp's Privacy Policy.** WhatsApp is owned by Facebook, and it shares some data with its parent company. While your messages are end-to-end encrypted, your metadata (who you talk to and when) is not.

Chapter 5: Protecting Your Email

Email is one of the oldest forms of digital communication, and it's still one of the most important. It's also a major target for hackers and spammers.

5.1 Choosing a Secure Email Provider

Your choice of email provider has a big impact on your privacy.

- **Play #51: Move Away from Free, Ad-Supported Email.** Services like Gmail and Yahoo Mail are free because they scan your emails to show you targeted ads.
- **Play #52: Use a Privacy-Focused Email Provider.** Services like ProtonMail and Tutanota offer end-to-end encryption and are based in countries with strong privacy laws.
- **Play #53: Use Your Own Domain.** For the ultimate in control, you can use your own domain name with a privacy-focused email provider.

5.2 Spotting and Avoiding Phishing Scams

Phishing is a type of attack where a criminal tries to trick you into giving them your personal information, like your password or credit card number.

- **Play #54: Be Skeptical of Unsolicited Emails.** If you get an email from a company you do business with, don't click on any links in the email. Instead, go to their website directly and log in.
- **Play #55: Look for Red Flags.** Phishing emails often have poor grammar and spelling, a sense of urgency, and a generic greeting (like "Dear Customer").
- **Play #56: Check the Sender's Email Address.** Phishers will often use an email address that looks similar to a legitimate one, but is off by a letter or two.

5.3 Using Email Aliases to Protect Your Real Address

An email alias is a disposable email address that forwards to your real email address.

- **Play #57: Use a Service Like SimpleLogin or AnonAddy.** These services make it easy to create and manage email aliases.
- **Play #58: Use a Different Alias for Every Service.** That way, if one service gets breached, you can just delete the alias and the spammers won't have your real email address.
- **Play #59: Use Your Email Provider's Alias Feature.** Some email providers, like ProtonMail, have a built-in alias feature.

Chapter 6: Advanced Privacy Tactics

This chapter covers some more advanced privacy tactics that can help you take your privacy to the next level.

6.1 The Principle of Data Minimization

The less data you share, the less data there is to be breached.

- **Play #60: Don't Fill Out Optional Fields.** When you sign up for a new service, only fill out the required fields.
- **Play #61: Use a "Burner" Phone Number.** Services like Google Voice can give you a free phone number that you can use to sign up for services without giving out your real number.
- **Play #62: Be Mindful of What You Post Online.** Think twice before you post something online. Once it's out there, it's very hard to take back.

6.2 Performing a Personal Data Audit

Do you know what data is out there about you?

- **Play #63: Search for Yourself Online.** Use a search engine to search for your name, email address, and phone number. You might be surprised by what you find.
- **Play #64: Check Have I Been Pwned.** Have I Been Pwned is a website that will tell you if your email address has been compromised in a data breach.
- **Play #65: Use a Data Broker Removal Service.** Services like DeleteMe and OneRep can help you remove your personal information from data broker websites.

6.3 Requesting Your Data from Companies (GDPR/CCPA)

If you live in Europe or California, you have the right to request your data from companies.

- **Play #66: Know Your Rights.** The General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) give you the right to access, correct, and delete your data.
- **Play #67: Use a Service Like Mine.** Mine is a service that helps you discover which companies have your data and request its deletion.

6.4 A Word on Data Breaches and What to Do

It's not a matter of if, but when.

- **Play #68: Don't Panic.** If you find out that your data has been compromised in a breach, the first thing to do is to stay calm.

- **Play #69: Change Your Password.** If the breached service had your password, change it immediately. If you reuse passwords, you'll need to change them on all of your other accounts as well.
- **Play #70: Monitor Your Accounts.** Keep an eye on your financial accounts and credit reports for any suspicious activity.

About Datacash

Datacash is a 501(c)(3) nonprofit organization dedicated to advancing data literacy, privacy, and digital rights for the public benefit. We believe that your personal data is your property, and you should have the tools and knowledge to control it.

Our mission is to build a more equitable and informed digital world. We do this by:

- **Creating educational resources** like this playbook to make complex topics accessible to everyone.
- **Developing privacy-first technology** that helps you understand and manage your data.
- **Advocating for stronger digital rights** and a more transparent data economy.

Datacash was founded on the principle that privacy is a fundamental human right. We are a team of educators, engineers, and advocates committed to empowering individuals and communities.

Further Resources from Datacash

This playbook is just the beginning of your privacy journey. We offer a growing library of resources to help you along the way.

- **The Datacash Blog:** For the latest news, analysis, and tips on data privacy.
- **Community Workshops:** Join our free online workshops to learn from experts and connect with other privacy-minded individuals.
- **The Datacash App (Coming Soon):** Our upcoming app will give you a real-time view of your digital footprint and help you take action to protect your data.

Visit us at https://datacash.app to learn more and get involved.

Conclusion: Privacy is a Journey, Not a Destination

Protecting your digital privacy can feel like a daunting task, but it doesn't have to be. By taking small, consistent steps, you can make a huge difference in your digital security.

Don't try to do everything at once. Start with the basics, like using a password manager and enabling two-factor authentication. Then, work your way through the other plays in this playbook at your own pace.

The privacy landscape is constantly changing, so it's important to stay informed. At Datacash, we are committed to providing ongoing education and resources to help you on your privacy journey. We encourage you to visit our website, datacash.app, for more articles, guides, and tools.

Your privacy is worth protecting. It's your data, your life, and your story to tell. By working together, we can build a more private and secure digital world for everyone.

For more information, please contact:
Datacash
https://datacash.app
datacash@datacash.app