

# Browser & Online Privacy Lockdown Guide

---

*Reduce Tracking, Control Browser Data, and Stop Giving Every Website Permanent Permission*

**Your browser knows far more about you than it needs to.**

Every search, cookie, extension, permission, saved login, autofill field, synchronized history entry, and tracking script is another piece of your digital trail. This guide helps you keep the useful parts without volunteering the rest.

**The Grumpy Sysadmin**

Version: August 2026

## How to Use This Guide

This guide is for people who want more privacy without turning normal web browsing into a part-time troubleshooting job. You are going to tighten the settings that matter, understand the tradeoffs, and use exceptions when a legitimate site actually needs one.

Chrome, Microsoft Edge, and Firefox use different names for similar controls. Menu names can move as browsers change, so this guide gives you both the current path and the privacy goal behind it. If a label has moved, search the browser settings for the feature name.

**Grumpy Rule:** *If your privacy plan requires twenty-seven extensions and every website is broken, you didn't create a privacy plan. You created a hobby.*

## The Five Questions to Ask About Any Browser Setting

- What information does this setting collect or expose?
- Who receives or can use that information?
- Does the feature actually need permanent access?
- What breaks if I restrict it?
- Can I make a site-specific exception instead of weakening everything?

## Table of Contents

- 1. Start With an Updated, Protected Browser
- 2. Tracking Prevention and Third-Party Cookies
- 3. Browser Accounts, Sign-In, and Sync
- 4. Lock Down Site Permissions
- 5. Extensions: Tiny Programs With Enormous Access
- 6. Passwords, Autofill, and Payment Data
- 7. Private Browsing: What It Does and Does Not Do
- 8. Search, Ads, Suggestions, and Diagnostic Data
- 9. HTTPS, Secure DNS, and Connection Privacy
- 10. Profiles, Containers, and Separating Online Identities
- 11. Downloads, Sessions, and Local Browser Data
- 12. Chrome Lockdown Walkthrough
- 13. Microsoft Edge Lockdown Walkthrough
- 14. Firefox Lockdown Walkthrough
- 15. Browser Privacy Worksheets
- 16. Maintenance and Final Verification

# 1. Start With an Updated, Protected Browser

Browser privacy doesn't matter much if the browser itself is missing security updates or its anti-phishing protections have been disabled. Start with the boring part because the boring part prevents expensive stories.

| Browser Foundation                                                    | Done                     |
|-----------------------------------------------------------------------|--------------------------|
| Browser updates install automatically or are checked regularly        | <input type="checkbox"/> |
| Built-in phishing/malware protection is enabled                       | <input type="checkbox"/> |
| HTTPS-first / secure-connection protection is enabled where available | <input type="checkbox"/> |
| Security warnings are not routinely bypassed                          | <input type="checkbox"/> |
| Unused or obsolete browsers are removed or retired from sensitive use | <input type="checkbox"/> |

## Keep Safe Browsing / SmartScreen / Protection Features On

Chrome Safe Browsing, Microsoft Defender SmartScreen in Edge, and Firefox phishing/malware protections are security controls, not advertising settings. Privacy-minded users sometimes disable anything that sends information to a vendor without considering what protection they're giving up. Review the privacy tradeoff, but don't casually turn off anti-phishing and malicious-download protection.

### Security and privacy are related, but they're not identical.

A setting can share limited data in order to protect you from malicious sites. Decide deliberately. "Send absolutely nothing anywhere" can create a less secure browser.

## 2. Tracking Prevention and Third-Party Cookies

Cross-site tracking works by connecting activity across different websites. Cookies are one mechanism, but fingerprinting, embedded content, advertising identifiers, and account sign-ins can contribute too. Blocking or isolating third-party cookies reduces one major tracking path, but no single switch makes you anonymous.

**Grumpy Rule:** *The “Accept All” button is usually the largest button for a reason. That reason isn’t your privacy.*

### Use the Browser’s Built-In Tracking Controls First

Start with built-in protection before stacking multiple overlapping privacy extensions. Edge offers Basic, Balanced, and Strict tracking prevention. Firefox uses Enhanced Tracking Protection and Total Cookie Protection. Chrome provides third-party cookie controls and separate Ad Privacy settings.

- Choose a stronger tracking setting if normal sites still work for you.
- Prefer a site-specific exception when one site breaks.
- Review exceptions periodically; temporary emergencies have a habit of becoming permanent configuration.
- Understand that blocking all cookies can break logins, shopping carts, embedded media, and federated sign-in.

### Cookies: First-Party vs. Third-Party

First-party cookies are created by the site you are visiting and often keep you signed in or remember preferences. Third-party cookies come from other domains embedded in the page and can be used to follow activity across sites. The practical goal is usually to limit cross-site tracking without destroying useful first-party site functionality.

#### When a site breaks

Temporarily allow what it needs, confirm that the privacy setting was actually the cause, and keep the exception as narrow as possible. Don’t disable tracking protection across the entire browser because one video player sulked.

### 3. Browser Accounts, Sign-In, and Sync

Signing into the browser can synchronize passwords, bookmarks, history, open tabs, addresses, extensions, and settings. That is convenient. It also means the browser account can become a very detailed map of your online life.

**Grumpy Rule: Sync isn't free storage from the privacy fairy. It's a deliberate decision to copy selected browser data to an account.**

#### Review What Is Synchronized

| Sync Review                                                      | Done                     |
|------------------------------------------------------------------|--------------------------|
| Browser account password is strong and unique                    | <input type="checkbox"/> |
| MFA is enabled                                                   | <input type="checkbox"/> |
| Only desired categories are synchronized                         | <input type="checkbox"/> |
| Old devices are removed from the account                         | <input type="checkbox"/> |
| Open tabs and history are synchronized only if useful            | <input type="checkbox"/> |
| Shared computers aren't signed into the personal browser account | <input type="checkbox"/> |
| Recovery email and phone are current                             | <input type="checkbox"/> |

#### Separate Browser Sign-In From Website Sign-In

Signing into Gmail, Outlook, or another website isn't always the same thing as signing the browser itself into an account. Pay attention to prompts that offer to turn on browser sync or connect the browser profile. Decide whether you want that relationship instead of clicking through it automatically.