BILL'S HOME TECH

Home & Small Business Tech Solutions

AN EXTENDED GUIDE · NO. 2016

Updated November 2026

Browser Privacy Settings Worth Changing — Chrome, Safari, Edge, Firefox

A few switches in Chrome, Safari, Edge, and Firefox for more privacy and less tracking

Tech Made Simple. Service Made Personal.

Bill Davis — Bill's Home Tech

(330) 200-8042 · bill@billshometech.com · Atwater, Ohio

Book a visit · billshometech.com/book

What's Inside

Everything in this guide, with page numbers. Skip to whichever chapter answers your question right now.

The 60-Second Version 3

What 'Tracking' Actually Means 3

The Three Changes That Matter Most 4

Chrome and Microsoft Edge 5

Safari on iPhone, iPad, and Mac 6

Firefox 6

Taking Back Site Permissions 7

The Browser's Password Help 8

Keeping the Danger Warnings On 9

A Few Habits Beyond the Settings 9

What Private or Incognito Mode Really Does 10

A Simple Privacy Tune-Up 11

Everyday Cheat Sheet 12

A Picture to Follow Along 13

A Second Look 14

A Note From Bill 14

Your Visit — and My Promise 15

THE 60-SECOND VERSION

1 The 60-Second Version

The whole idea in a minute.

Every major browser has a Privacy section in its settings, and a few changes there make a real difference. The big one is blocking the cross-site cookies and trackers that let advertisers follow you from page to page. After that, it is worth reviewing which websites can use your location, camera, and microphone, keeping the safe-browsing warning on, and clearing out old data now and then.

- Turn on the browser's tracking protection.
- Block third-party (cross-site) cookies.
- Review and trim site permissions, and clear old browsing data occasionally.

GOOD TO KNOW

These settings do not make you invisible, and they are not about hiding anything. They simply stop the quiet, constant following that advertisers do by default — a reasonable bit of tidying for anyone.

WHAT TRACKING IS

2 What 'Tracking' Actually Means

Why pages seem to follow you.

You have surely noticed it: you look at a product on one site, and suddenly ads for it follow you around the web for days. That is tracking, and it works through little files called cookies — specifically 'third-party' or 'cross-site' cookies, which belong not to the site you are visiting but to advertising companies whose code rides along on it.

These cross-site cookies act like a tag that lets advertisers recognize you from one website to the next, quietly building a profile of what you look at, buy, and read. None of it is dramatic or dangerous in the way a scam is, but many people find the constant, invisible following unsettling — and it is entirely reasonable to want less of it. Blocking cross-site cookies is the single change that curtails the most of this, which

is why it tops the list in every browser.

Blocking cross-site cookies is not about hiding — it is about declining to wear the advertisers' tracking tag everywhere you go online.

THE BIG THREE

3 The Three Changes That Matter Most

True for every browser.

Whatever browser you use, these three changes give you most of the benefit. The exact wording differs, but the ideas are the same everywhere, and none of them will break your everyday browsing.

Change	What it does
Tracking protection	Stops hidden trackers following you between sites
Block cross-site cookies	Removes the main tool advertisers use to track
Review site permissions	Takes back location, camera, and mic from sites

A fourth, gentler habit — clearing your browsing data occasionally — clears out accumulated cookies and history for a fresh start. You do not need to do it often, and you can choose to keep the saved passwords and logins you rely on while clearing the rest. The chapters that follow show exactly where these live in each of the four major browsers, so you can make the changes in whichever one you use.

CHROME & EDGE

4 Chrome and Microsoft Edge

Close cousins under the hood.

Chrome and Edge are built on the same foundation, so their privacy settings look and work much alike. You reach them from the three-dot menu, then Settings, then a Privacy section. If you use one of these — and most people on a Windows computer use one or the other — the steps below take only a few minutes.

In Chrome

1. Open the three-dot menu and choose Settings.
2. Click Privacy and security.
3. Open Third-party cookies and choose to block them.
4. Visit Site settings to review location, camera, and microphone access.
5. Use Clear browsing data to tidy up history and cookies when you like.

In Edge

1. Open the three-dot menu and choose Settings.
2. Click Privacy, search, and services.
3. Set Tracking prevention to a stronger level such as Strict.
4. Review Cookies and site permissions for location, camera, and mic.
5. Use Clear browsing data as needed.

> **TIP**
>
> Edge's Strict tracking prevention blocks the most trackers. If a site you trust misbehaves, you can ease it for that one site rather than turning the whole protection off.

SAFARI

5 Safari on iPhone, iPad, and Mac

Private by default, with extras.

Safari, Apple's browser, already blocks many cross-site trackers out of the box, which is one of its quiet strengths. It also offers a couple of extra switches worth knowing, and — for those with iCloud+ — a feature that hides even more of your browsing.

1. On a Mac, open Safari then Settings; on an iPhone or iPad, open the Settings app and scroll to Safari.
2. Confirm Prevent Cross-Site Tracking is on.
3. Turn on Hide IP Address from Trackers for an added layer.
4. Review Camera, Microphone, and Location under Settings for websites.
5. Use Clear History and Website Data to tidy up.

Because Safari leans toward privacy by default, there is less to change than in some browsers — but it is still worth confirming the cross-site tracking protection is on and reviewing which sites you have granted camera, microphone, or location access. Those site permissions accumulate quietly over time, and trimming the ones you no longer need is good housekeeping.

> **GOOD TO KNOW**
>
> Apple customers with iCloud+ also get Private Relay, which hides more of your browsing from your internet provider and the sites you visit. It is worth turning on if you have it.

FIREFOX

6 Firefox

Strong, straightforward privacy.

Firefox has long made privacy a selling point, and its controls are clear and generous. Its main feature is called Enhanced Tracking Protection, which is on by default and can be turned up for even more protection.

1. Open the menu (three lines) and choose Settings.
2. Click Privacy & Security.
3. Set Enhanced Tracking Protection to Standard or, for more, Strict.
4. Review Permissions for location, camera, and microphone.
5. Turn on the option to alert you about breached passwords, and clear data when you wish.

For most people, Firefox's Standard protection strikes a good balance, blocking the common trackers without breaking sites. The Strict setting goes further and suits those who want maximum privacy, at the small risk of the occasional site needing to be eased. Firefox also makes its breach alerts easy to find, warning you if a password you saved has turned up in a known data leak.

WATCH OUT

Firefox's Strict mode is very protective but can occasionally break a page's login or video. If a trusted site stops working, switch that one site back rather than abandoning the protection entirely.

Rather not do this yourself? I'll come to your home and set it up for you — a flat $99 first visit across Portage County, Ohio and nearby communities. Outside the area? I also help remotely by phone or screen-share. Book at billshometech.com/book or call (330) 200-8042.

SITE PERMISSIONS

7 Taking Back Site Permissions

Who can use your camera and location.

Over time, as you visit websites, you grant little permissions — a site asks to know your location, or to use your camera for a video call, and you say yes. Those grants persist, and it is worth occasionally reviewing them, much as you would review app permissions on a phone.

- Location: few sites genuinely need to know where you are; revoke it from ones that do not.
- Camera and microphone: should belong only to sites where you truly make calls or recordings.
- Notifications: many sites beg to send you pop-up notifications — turn off the ones you did not want.
- Each browser gathers these under Site settings or Permissions in its privacy section.

The notifications permission is the one most people are glad to clean up. Countless sites ask to send you desktop alerts, and if you have absent-mindedly allowed a few, they can clutter your screen for months. Reviewing site permissions and switching off the location, camera, and notification grants you never meant to give is a satisfying bit of tidying that makes the browser feel calmer and more private.

PASSWORDS

8 The Browser's Password Help

A security feature worth using.

All four browsers can remember your passwords and, importantly, warn you when one of them has turned up in a known data breach. This is a genuine security benefit, not just convenience, and it is worth turning on.

- Let the browser save your passwords so you can use a different, strong one for each site without memorizing them all.
- Turn on breach alerts, which tell you if a saved password has appeared in a known leak so you can change it.
- Heed those alerts promptly — change the flagged password on the real site, and anywhere else you used it.
- Protect the device itself with a passcode, since the saved passwords live behind it.

Reusing the same password everywhere is one of the biggest everyday security risks, because a leak at one site then unlocks all the others. Letting the browser remember a different password for each site solves that without burdening your memory, and the breach alerts act as an early warning when one of them is exposed. It is one of the most useful, least-used features sitting right there in your browser.

SAFE BROWSING

9 Keeping the Danger Warnings On

Your browser as a guard.

Beyond privacy, every major browser includes a safety feature that warns you when you are about to visit a known dangerous or fraudulent site — a fake bank page, a malware trap, a phishing site. It is on by default, and you should leave it on.

- Safe browsing warns you before you load a site known to be dangerous or deceptive.
- It helps catch phishing pages that imitate real banks and services.
- It is found in the same privacy and security settings, usually on by default.
- Heed its warnings — if the browser says a site is dangerous, do not click through.

This feature quietly protects you from a whole category of online harm, stepping in with a full-page warning before you reach a site known to steal logins or install harmful software. There is no good reason to turn it off, and every reason to respect its warnings. Think of it as a guard at the door who recognizes the known troublemakers and turns them away before they reach you.

GOOD HABITS

10 A Few Habits Beyond the Settings

Privacy is also behavior.

The settings do most of the work, but a few habits round it out across any browser, and cost nothing but a moment of attention.

- Let the browser warn you about dangerous or fake sites — keep safe browsing on.
- Use the browser's password manager and heed its breach alerts.
- Be cautious about browser add-ons; install only ones you trust, from the official store.
- When a cookie pop-up offers 'reject' or 'necessary only,' choose it rather than 'accept all.'

- Clear your data if a computer is shared or before you pass a device on.

Browser add-ons deserve a word of caution: a useful-looking extension can also watch everything you do online, so install only ones from reputable makers through the official store, and remove any you no longer use. And those endless cookie pop-ups, annoying as they are, usually offer a 'reject' or 'necessary only' choice — taking it rather than 'accept all' declines the extra tracking with a single click.

PRIVATE BROWSING

11 What Private or Incognito Mode Really Does

Useful, but commonly misunderstood.

Every browser offers a 'private' or 'incognito' window, and it is widely misunderstood. It is genuinely useful for one thing: it does not save the history, cookies, or form entries from that session on your device, so it is handy on a shared or borrowed computer, or for a one-off login.

- Private mode forgets the session on your device — no saved history or cookies afterward.
- It is useful on a shared computer, or to sign in to an account without leaving traces locally.
- It does not make you anonymous online — websites and your internet provider can still see your activity.
- It is a local tidiness tool, not a cloak of invisibility.

The common myth is that incognito mode hides you from the whole internet. It does not — the websites you visit, and your internet provider, can still see what you do. What it does is keep that particular session off the device you are using, which is exactly what you want when borrowing a friend's laptop or using a library computer. Understanding that limit lets you use it for what it is good at without a false sense of security.

PUTTING IT TOGETHER

12 A Simple Privacy Tune-Up

Fifteen minutes, once.

You can do the whole thing in one sitting of fifteen minutes or so, in whichever browser you use, and then mostly forget it — the settings stay put and keep working.

1. Open your browser's Privacy section.
2. Turn on tracking protection and block cross-site cookies.
3. Review site permissions and revoke location, camera, mic, and notifications you did not mean to grant.
4. Confirm safe browsing is on, and turn on password breach alerts.
5. Clear old browsing data for a fresh start, keeping the logins you rely on.

None of this makes browsing harder day to day; you will scarcely notice a difference except perhaps fewer ads that eerily follow you around. What you gain is a browser that quietly declines to be tracked, keeps a guard against dangerous sites, and warns you if a password leaks — a reasonable, self-respecting default for anyone who spends time online.

CHEAT SHEET

Everyday Cheat Sheet

Keep this page handy. It points you straight to what to do for each task.

I want to…	Do this…
Block trackers	Turn on tracking protection so sites can't follow you around
Limit cookies	Block third-party (cross-site) cookies, the main tracking tool
Control sites	Review which sites can use your location, camera, and mic
Safe browsing	Keep the warning for dangerous and fake sites switched on
Manage passwords	Let the browser flag passwords exposed in a breach
Tidy up	Clear old browsing data now and then for a clean slate
Get help	Call Bill: (330) 200-8042

AT A GLANCE

A Picture to Follow Along

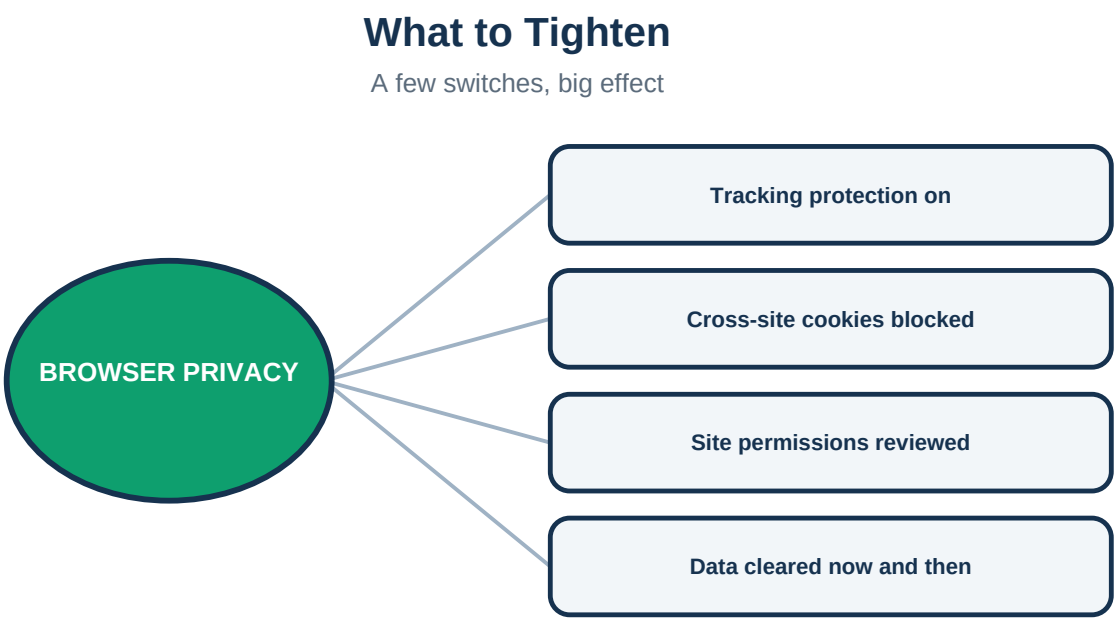


Illustration — a schematic. Set-up screens differ; each takes only a few minutes.

AT A GLANCE

A Second Look

Tightening Your Browser

The same idea everywhere

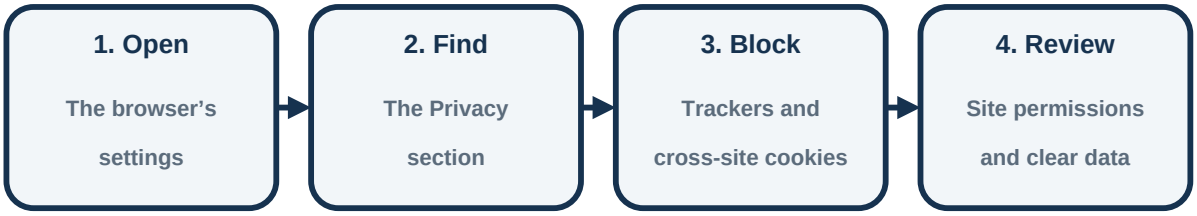


Illustration — a schematic. The order is a suggestion; do one box at a time.

A schematic of the plan — company steps vary; the order does not have to.

BEFORE YOU GO

A Note From Bill

A quick note from Bill. I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results.

HOW I CAN HELP

Your Visit — and My Promise

You don't have to remember all of it — just that a friendly, patient person is one call away, whenever you'd rather have a hand.

KEY SPECS

In your home — $99 flat for the first visit, no contracts and no surprises, with a 30-day come-back-free follow-up. In-home visits cover Portage County, Ohio and nearby communities.
Outside the area? Remotely — $49 for a screen-share session (free for Support Plan members, $39/mo), refundable if I can't fix it — and credited toward a visit if you'd rather have me in person. Book either at billshometech.com/book.

GOOD TO KNOW

My promise — If you're not 100% satisfied with your visit, I'll come back at no charge, or refund the full $99. No questions, no awkwardness. That's how I'd want to be treated.

Whenever you're ready, I'll come to your home anywhere in Portage County, Ohio and nearby communities, at your pace. Too far for a house call? I also help remotely. Book at billshometech.com/book or call (330) 200-8042. — Bill

Call or text (330) 200-8042 · bill@billshometech.com

This free guide is for general information only — not professional advice, and no substitute for your device's own manual. Any prices or outside products mentioned can change; please confirm current details before you buy. Please use your own good judgment and follow it at your own risk — for anything involving electricity, gas, water, or heights, stop and call a licensed professional. Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results. © 2026 Bill's Home Tech, LLC.