

4.1 Browser Hygiene

Core Concepts: Protect Yourself, Minimize Your Exposure

Your web browser and email are your primary gateways to the internet, and the primary ways attackers try to reach you. Most cyber attacks start with either a malicious website or a phishing email. Good browser and email hygiene can stop the vast majority of these attacks before they start.

You don't need to be a technical expert. Most protection comes from recognizing common patterns, adjusting a few settings, and building good habits about what you click.

4.1.1. Understanding Browser Threats

Common browser threats:

- Malicious websites that install malware
- Fake websites that steal passwords (phishing)
- Malicious browser extensions
- Tracking cookies and fingerprinting
- Drive-by downloads (downloads that start without your permission)
- Man-in-the-middle attacks on unsecured connections

4.1.2. The Basics

- Use a modern browser
- Look for HTTPS and the padlock icon
- Check URLs carefully
- Minimize browser extensions

Use a Modern, Updated Browser

Modern browsers have built-in security features that older browsers lack. Keep your browser updated to get the latest protections.

Recommended browsers:

- Google Chrome - Most popular, excellent security, but heavy on tracking
- Mozilla Firefox - Good balance of security and privacy
- Microsoft Edge - Good security, integrates with Windows
- Safari - Best for Mac/iPhone users, good privacy
- Brave - Privacy-focused, blocks ads and trackers by default

Enable automatic updates:

- Chrome/Edge: Updates automatically, restart when prompted
- Firefox: Settings > General > Firefox Updates > Automatically install updates
- Safari: Updates with macOS system updates

Look for HTTPS and the Padlock Icon

HTTPS encrypts the connection between your browser and the website. Always check for it, especially on sites where you enter passwords or payment information.

What to look for:

- Padlock icon in the address bar
- "https://" at the start of the URL (not just "http://")
- Modern browsers show "Not Secure" warning for HTTP sites

Warning signs:

- No padlock icon
- "Not Secure" warning
- Certificate error warnings - don't ignore these!

NEVER enter passwords or payment info on HTTP sites. Close the site and find a secure alternative.

Check URLs Carefully Before Clicking

Attackers create fake websites with URLs that look almost right. Always verify URLs before clicking or entering information.

How to check URLs:

- Hover over links to see the actual URL (bottom left of browser)
- Look for misspellings: "amaz0n.com" instead of "amazon.com"
- Watch for extra words: "amazon-login.suspicious-site.com"

- Check the domain name “https://amazon-login.suspicious-site.com/login”
- Be suspicious of shortened URLs (bit.ly, tinyurl) from unknown sources

Common tricks:

- Character substitution: "paypa1.com" (number 1 instead of letter l)
- Adding words: "secure-bankofamerica-login.com"

When in doubt, type the URL manually rather than clicking links.

Use Minimal Browser Extensions

Browser extensions have access to everything you do in your browser. Only install extensions you truly need from trusted developers.

Extension safety rules:

- Install only from official browser stores
- Check number of users (millions is better than dozens)
- Read recent reviews
- Review permissions ;if they seem excessive, don't install
- Uninstall extensions you don't actively use

Recommended extensions:

- Password manager extension (all, good password managers have them, install from their site)
- Privacy badger <https://www.eff.org/pages/privacy-badger>

See the Software and App Safety section for additional extension guidance.

4.1.3. Better Protection

- Configure browser for privacy
- Use a privacy-focused search engine
- Install a reputable add blocker

Configure Browser for Privacy

Browsers collect data about your browsing. Review and restrict this.

Chrome:

- Settings > Privacy and security
- Turn on "Send a 'Do Not Track' request"
- Cookies: Choose "Block third-party cookies"
- Safe Browsing: Use "Enhanced protection" or "Standard protection"

Firefox:

- Settings > Privacy & Security
- Enhanced Tracking Protection: Choose "Strict"
- Enable "Tell websites not to sell or share my data"
- HTTPS-Only Mode: Turn on for all windows

Safari:

- Settings > Privacy
- Enable "Prevent cross-site tracking"
- Enable "Hide IP address from trackers"

Use a Privacy-Focused Search Engine

Search engines track your searches and build profiles. Consider alternatives that don't track.

Privacy-focused options:

- DuckDuckGo: <https://duckduckgo.com/>
- Startpage: <https://www.startpage.com/>
- Brave Search: Privacy-focused, integrated with Brave browser

How to change default search:

- Chrome: Settings > Search engine > Manage search engines
- Firefox: Settings > Search > Default Search Engine
- Safari: Settings > Search > Search engine

Install a Reputable Ad Blocker

Ad blockers prevent malicious ads and reduce tracking. Choose carefully - some ad blockers themselves track you.

Recommended ad blockers:

- Privacy Badger - Made by EFF, learns to block trackers
- uBlock Origin - Free, open-source, highly effective, no tracking

Avoid: Adblock, Adblock Plus (these allow "acceptable ads," ads that pay them)

4.1.4. Extra Credit

- Use a hardened browser
- Use browser profiles or containers

Use Hardened Browser

For maximum privacy and security, use browsers with hardened default configurations.

Privacy-focused browsers:

- Brave - Chromium-based, blocks ads/trackers by default
- LibreWolf - Firefox-based, pre-configured for privacy
- Tor Browser - Maximum anonymity (but slow)

Advanced Firefox hardening:

- Use arkenfox user.js template
- Disables telemetry, fingerprinting, and tracking
- Warning: Can break some websites - not for beginners

Use Browser Profiles or Containers

Separate your browsing into different profiles or containers to isolate activities.

Browser profiles (Chrome/Edge/Brave):

- Create separate profiles for work, personal, shopping
- Each has its own bookmarks, history, passwords, extensions
- Prevents cross-contamination of tracking cookies

Firefox containers:

- Install "Firefox Multi-Account Containers" extension
- Isolate sites into containers (Facebook, Banking, Shopping, Work)
- Sites in one container can't see cookies from other containers