

LOCK DOWN YOUR BROWSER IN UNDER 10 MINUTES.

SETTINGS TO CHANGE

- ❑ **ENABLE HTTPS-ONLY MODE.** Forces secure connections. Chrome: Settings > Privacy > Always use secure connections.
- ❑ **BLOCK THIRD-PARTY COOKIES.** Stops cross-site tracking. Chrome: Settings > Privacy > Block third-party cookies.
- ❑ **ENABLE ENHANCED TRACKING PROTECTION.** Firefox: Settings > Privacy > Strict. Blocks trackers by default.
- ❑ **TURN OFF PASSWORD SAVING IN BROWSER.** Use a password manager instead; browser password stores are more exposed.
- ❑ **DISABLE AUTOFILL FOR PAYMENT AND ADDRESS.** Reduces risk if the browser is compromised or an extension is malicious.

EXTENSIONS TO INSTALL

- ❑ **UBLOCK ORIGIN.** Best ad and tracker blocker. Free, open-source. Works in Chrome, Firefox, Edge.
- ❑ **PRIVACY BADGER (EFF).** Learns and blocks invisible trackers automatically. From the Electronic Frontier Foundation.
- ❑ **BITWARDEN.** Open-source password manager extension; fills passwords without auto-save risk.

WHAT TO AVOID

- ❑ **AVOID GOOGLE CHROME ON HIGH-RISK ACCOUNTS.** Chrome sends more data to Google than Firefox or Brave. Use Brave or Firefox for anything sensitive.
- ❑ **NEVER INSTALL EXTENSIONS YOU DON'T RECOGNIZE.** Malicious extensions can read all your browsing data and steal passwords.
- ❑ **DON'T SAVE PASSWORDS TO THE BROWSER.** If malware runs on your computer, saved browser passwords are easy pickings.
- ❑ **AVOID CLICKING "ALLOW NOTIFICATIONS" FROM UNKNOWN SITES.** Push notification spam is used to deliver scam ads and malware.

Ten minutes, five settings, three extensions. That's the whole browser fixed.

→ rexcalloway.com/free-tools

Educational content only. Not financial, legal, tax, or professional cybersecurity advice. No professional-client relationship is created. Consult a qualified professional for your specific situation. Full disclaimer at rexcalloway.com/disclaimer.