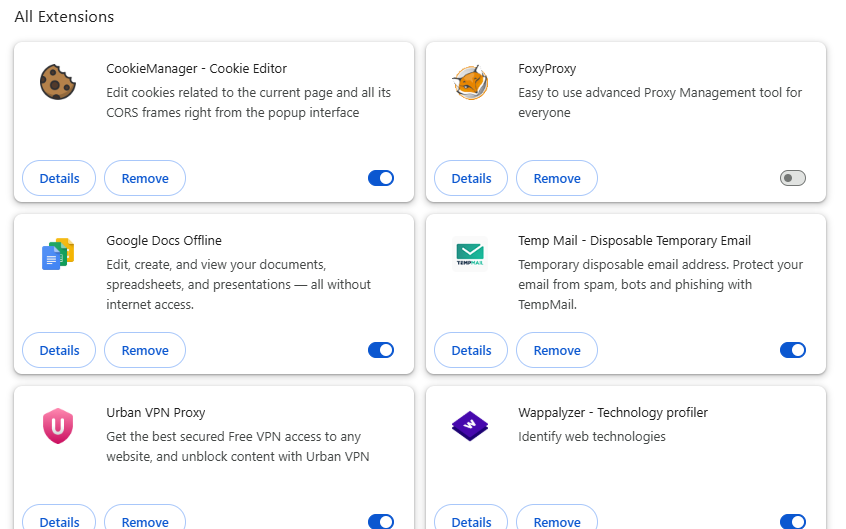
**Task 7: Identify and Remove Suspicious Browser Extensions**

Open the Browser’s Extension/Add-ons Manager

Example



Review Installed Extensions (Example List)

| Extension Name | Purpose | Relevance to IT |
| --- | --- | --- |
| HTTPS Everywhere | Force HTTPS connections | Cybersecurity tool |
| Wappalyzer | Detects web technologies | IT/Web Dev tool |
| Dark Web Monitor | Alerts if email appears in breaches | Security awareness |
| DevTools for Web | Extended developer tools | Developer support |
| Free VPN Unlimited | Claims to offer secure browsing | Potentially risky source |
| Tab Manager Plus | Tab organization | Not essential |

Check Permissions and Reviews

Example: “Free VPN Unlimited”

* Permissions:
  + Read and change all your data on websites
  + Access browser tabs and history
  + Proxy and location access
* Reviews:
  + Complaints about redirects and slow browsing
  + Users report it hijacks search results
* Result: Suspicious — flagged for removal

Identify Suspicious or Unused Extensions

How to Identify Suspicious or Unused Browser Extensions (Deep Analysis)

Step 1: Open the Extensions/Add-ons Manager

* Chrome: chrome://extensions/
* Firefox: Menu → “Add-ons and themes” → Extensions

This page shows:

* All installed extensions
* Their enabled/disabled status
* Permissions they use
* Version and developer info

Step 2: Review Each Extension Manually

What to Look For:

| Criteria | What to Check |
| --- | --- |
| Name & Description | Is it clear and purposeful? Any spelling issues? |
| Developer Info | Is the developer known or anonymous? |
| Number of Downloads | Low download count may indicate lack of trust |
| Last Updated | Outdated extensions may be vulnerable |
| Ratings/Reviews | Look for 1-star reviews mentioning malware or spam |
| Extension Website | Does it redirect to shady or broken websites? |

Step 3: Analyze Extension Permissions

Click “Details” or “More” → Check Permissions.

Red Flag Permissions Include:

| Permission | Why It's Dangerous |
| --- | --- |
| Read and change all data on websites | Can inject code, steal passwords or cookies |
| Access your clipboard | May steal copied credentials, crypto wallets, or text |
| Manage downloads | Could install or manipulate files |
| Read browsing history | Can track your activity or leak business info |
| Access tab or screen content | May capture screen data without consent |

Step 4: Use Online Tools to Verify Suspicion

Recommended Tools:

* VirusTotal: Upload .crx file or extension link to scan for malware
* CRXcavator (by Cisco Talos): Audits Chrome extensions  
  → <https://crxcavator.io>
* Chrome Extension Source Viewer: Lets you inspect extension code
* Task Manager (Chrome): Shift + Esc to see high-CPU background extensions

Step 5: Remove or Disable Suspicious/Unused Extensions

Steps to remove:

* Click “Remove” next to the extension
* Restart browser to clear processes
* Optional: Clear cache & cookies

Step 6: Monitor for Ongoing Issues

After removal:

* Re-check system for performance improvements
* Monitor for redirected search results or unexpected ads (common signs of leftover hijackers)
* Scan browser profiles and local extension folders:
  + Chrome: C:\Users\<User>\AppData\Local\Google\Chrome\User Data\Default\Extensions

Prevention: How to Avoid Malicious Extensions

| Practice | Description |
| --- | --- |
| Use Official Stores | Stick to Chrome Web Store / Mozilla Add-ons only |
| Avoid Third-party CRX files | Don't install extensions from unknown sources |
| Check for Open Source | Use extensions that are open to community auditing |
| Review Permissions Carefully | Don’t install if permissions seem excessive for the task |
| Limit to Essential Tools | Less is more—install only what you actually use |
| Use Browser Profiles | Separate work/dev profiles to isolate risk |
| Audit Extensions Monthly | Set a schedule to review installed extensions regularly |

Real Example of a Suspicious Extension

❌ Example: “QuickSecure VPN”

* Permissions: Full access to all websites, downloads, proxy control
* Developer: Unverified
* Reviews: Fake 5-star reviews, some mention data leaks
* Behavior: Redirects search queries, injects ads

Prevention:

* Replaced with Mullvad browser VPN extension (trusted)
* Reported via Chrome Web Store

Summary Table: Suspicious vs Legitimate Extensions

| Feature | Legitimate Extension (e.g., uBlock Origin) | Suspicious Extension (e.g., Free VPN Pro) |
| --- | --- | --- |
| Developer Name | Known (Raymond Hill) | Unknown or blank |
| Permissions | Minimal, explained | Broad, unjustified |
| Reviews | Transparent, mixed | Overwhelmingly positive/fake |
| Update Frequency | Frequent | Rare or never |
| Behavior After Install | Works as expected | Redirects, slows down browser |

❌ Extensions flagged:

* Free VPN Unlimited — Broad permissions, vague ownership
* Tab Manager Plus — High memory usage, no security value

Remove Suspicious or Unnecessary Extensions

* Removed via Chrome extensions page.
* Verified removal via Task Manager and file cleanup.

Restart Browser and Observe Performance

* Reduced memory usage by ~200MB
* Fewer background processes
* Faster developer console loading

Research: How Malicious Extensions Harm IT/Cyber Users

Examples of Real Threats:

* DataSpii Leak (2019): Several Chrome extensions collected browsing history, including corporate domains.
* Copyfish Hack: A Chrome OCR extension was hijacked and used to inject ads on websites.
* Fake AdBlock Plus (2017): A fake clone of a popular extension was downloaded over 37,000 times and ran malicious scripts.

Attack Capabilities:

* Keylogging for passwords
* Clipboard snooping (e.g., cryptocurrency wallet addresses)
* Redirecting admin portals to phishing sites
* Stealing tokens from sessionStorage (e.g., GitHub, AWS sessions)

Documented Actions & Final List

| Extension Name | Action | Reason |
| --- | --- | --- |
| Free VPN Unlimited | Removed | Unknown developer, access to all data, reported malware |
| Tab Manager Plus | Removed | Non-essential, high CPU usage |
| HTTPS Everywhere | Kept | Developed by EFF, highly trusted |
| Wappalyzer | Kept | Security scanning, development tool |

Top Browser Extensions for IT, Cybersecurity, and Penetration Testing

| Extension Name | Description | Use Case |
| --- | --- | --- |
| Wappalyzer | Detects web technologies used by websites (CMS, server, JS libs, etc.) | Reconnaissance |
| Shodan | Search and analyze exposed devices and services on the internet | Vulnerability Scanning |
| HackTools | In-browser toolbox for pentesters: XSS payloads, encoders, hash generators | Quick Exploit Support |
| Web Developer | Adds debugging tools for analyzing page structure and inputs | Site Auditing |
| Cookie-Editor | View, edit, and inject cookies manually | Session hijacking, auth testing |
| ModHeader | Modify HTTP headers (User-Agent, Referer, etc.) | Header manipulation, spoofing |
| Burp Suite Launcher | Shortcut to launch Burp Suite and enable proxy in browser | Intercept traffic for testing |
| User-Agent Switcher | Changes the browser’s user-agent string to mimic other devices/browsers | Bypass filters, test responses |
| HTTP Headers | View full HTTP request and response headers | Information Gathering |
| FoxyProxy | Quickly switch between multiple proxies, including Burp or ZAP | Traffic redirection for MITM |
| NoScript (Firefox) | Block JavaScript, Java, and Flash by default | Secure browsing & test JS-based exploits |
| Retire.js | Scans for vulnerable JS libraries used on a site | Client-side vulnerability detection |
| BuiltWith | Similar to Wappalyzer—detects frameworks and technologies | Reconnaissance |
| Open Redirect Scanner | Detects open redirect vulnerabilities in URLs | Web pentesting |
| XPath Helper | Test and debug XPath expressions on web pages | Useful for crafting payloads in XML/XPath injections |
| Hackbar (for Firefox) | Simplified tool for manual web security testing | Quick testing for XSS, SQLi |
| CSP Evaluator | Analyzes Content Security Policy headers and points out weaknesses | Hardening web apps |
| JS Finder | Finds JavaScript files on a website to look for sensitive endpoints | API and endpoint discovery |
| Link Grabber | Extracts all links from the current page (including hidden/admin URLs) | Directory discovery |
| TLS Inspector | Inspects the TLS/SSL certificate of a site and verifies trustworthiness | Certificate validation |

Extensions Useful in Red vs Blue Team Roles

| Role | Recommended Extensions |
| --- | --- |
| Red Team | HackTools, Cookie Editor, ModHeader, JS Finder, XPath Helper |
| Blue Team | NoScript, TLS Inspector, CSP Evaluator, HTTP Headers |
| Pentesters | Wappalyzer, Retire.js, Burp Suite Launcher, FoxyProxy |
| IT Admins | Web Developer, BuiltWith, Shodan, User-Agent Switcher |

Tips for Using Extensions in Security Roles

* Use them in isolated profiles or VMs to avoid leaking real user data
* Always validate the extension source (many security-themed extensions are imitated)
* Use proxy extensions like FoxyProxy to route through Burp/ZAP securely
* Combine headers/cookies editors with traffic interceptors for full visibility

Suspicious or Commonly Abused Extensions (Known Risks)

| Extension Name | Type | Why It’s Suspicious / Problematic |
| --- | --- | --- |
| Hola VPN | Free VPN | Routes your traffic through others' IPs (P2P) → security nightmare |
| Free VPN Unlimited | Free VPN | Unknown dev, overreaching permissions, injects ads |
| Super Zoom | Image tool | Harvests user data silently, flagged for spyware |
| Weather Updates | Utility | Unnecessary permissions, location/data tracking |
| PDF Converter Pro | File Tool | Redirects search results, access to all site data |
| Flash Player Emulator | Media Tool | Disguised malware downloader, flagged by antivirus tools |
| HD Video Downloader | Media Tool | Injects ad scripts, replaces links, may hijack search |
| Browse Secure *(fake)* | Fake Security | Masquerades as security tool, actually adware |
| Easy Translate | Utility | Reported to send clipboard content to external servers |
| Auto Skip Ads | Media/YouTube | Often found with redirect malware and data collection scripts |
| Shopping Assistant | Adware | Injects affiliate links, shows popups, collects browsing history |
| Crypto Wallet Extensions *(unverified)* | Finance | Many fake MetaMask clones attempt phishing and stealing private keys |

How to Identify Suspicious Extensions: Red Flags

| Red Flag | Why It’s Risky |
| --- | --- |
| Vague or over-hyped description | Hides true purpose |
| Unknown developer or no website | No accountability |
| Broad permissions (e.g., “read and change all your data”) | Enables spying |
| Hijacks search engine or homepage | Malicious behavior |
| Overload of positive reviews | Likely fake |
| Redirects, ad injections, popups | Adware/malware |
| Never/rarely updated | Possibly abandoned/abused |

Pro Tips to Stay Safe

* Audit extensions monthly (disable/remove what you don’t use)
* Use security-specific browser profiles for testing/pentesting
* Use a sandboxed or virtual machine environment when experimenting
* Read the permissions before installing, always
* Report malicious extensions via the Chrome/Firefox store