## Chrome Extension Audit and Cleanup Procedure

### Procedure

1. **Step 1: Accessing the Extension Manager**  
   I began by navigating to the extensions management page. This was done by clicking the three-dot menu in the top-right corner of Chrome, selecting Extensions, and then choosing Manage Extensions. Alternatively, I could have typed `chrome://extensions` directly into the address bar.
2. **Step 2: Initial Review of Installed Extensions**  
   On the management page, I saw a complete list of all installed extensions. I carefully went through the list, taking note of each extension's name and its stated purpose. I immediately looked for any extensions that I did not recognize or remember installing.
3. **Step 3: Analyzing Permissions and Reviews**  
   For each extension, I clicked the "Details" button. This allowed me to inspect the permissions it required. I was particularly wary of extensions that requested overly broad permissions, such as the ability to "Read and change all your data on the websites you visit." If an extension's required permissions seemed excessive for its function (e.g., a simple theme editor wanting access to all my browsing history), I flagged it as suspicious. I also checked the Chrome Web Store for reviews, looking for negative feedback or reports of malware.
4. **Step 4 & 5: Identification and Removal**  
   Based on my analysis, I identified several extensions that were either unused, unnecessary, or suspicious due to their vague descriptions and excessive permissions. I removed these extensions by clicking the "Remove" button for each one.
5. **Step 6: Browser Restart and Performance Check**  
   After removing the targeted extensions, I closed all Chrome windows and restarted the browser to ensure the changes took full effect. I noticed a slight but tangible improvement in browser startup time and page loading speed. The browser also felt more responsive overall.

### Findings and Actions Taken

| Extension Name | Stated Function | Reason for Action | Action Taken |
| --- | --- | --- | --- |
| Google Docs Offline | Allows editing of documents offline. | Legitimate and necessary extension from Google. | Kept |
| uBlock Origin | Content blocker. | Well-reviewed, trusted, and actively used for security. | Kept |
| SuperSearch Enhancer | Promised to improve search results. | Requested permission to "read and change all data on all websites." Very suspicious and invasive. I didn't remember installing it. | Removed |
| Video Downloader Pro | Download videos from various sites. | Was installed a long time ago and is no longer used. Unused extensions can become security vulnerabilities if not updated. | Removed |
| StyleWeb | Customize website appearances. | Had no reviews on the Web Store and its developer was unknown. The permissions were vague, making it a potential risk. | Removed |

### Research: The Dangers of Malicious Extensions

My research into the topic revealed how malicious browser extensions can pose significant threats to users. These extensions often disguise themselves as useful tools to trick users into installing them. The primary dangers include:

* **Data Theft 🕵️‍♂️**: Malicious extensions can log keystrokes, capture login credentials for banking and social media, and steal personal information filled into web forms.
* **Adware and Ad Injection 📢**: Many suspicious extensions inject their own advertisements into the websites you visit. These ads can be intrusive, track your browsing activity, and sometimes lead to malicious websites.
* **Browser Hijacking**: Some extensions can change your default search engine, homepage, or new tab page to a different one without your consent, often redirecting you to phishing sites or pages filled with ads.
* **Cryptomining ⛏️**: A growing threat is "cryptojacking," where an extension secretly uses your computer's CPU resources to mine cryptocurrencies for the attacker, leading to significant performance degradation and higher electricity usage.

### Conclusion

This audit was a valuable exercise in digital hygiene. It highlighted how easily unnecessary and potentially dangerous extensions can accumulate over time. By regularly reviewing and removing suspicious add-ons, one can significantly improve browser performance and protect personal data from a variety of online threats. I will incorporate a quarterly extension review into my regular security practices.