Browser Extension Audit

1 Objective

Identify and remove potentially harmful or unnecessary browser extensions to enhance browser security and performance.

2 Tools Used

- **Web Browser**: [Specify your browser, Google Chrome, Mozilla Firefox, or other]
- **Operating System**: [Specify your OS, Windows, macOS, Linux]

3 Steps Taken

1. **Access the Extension Manager**
   - For **Google Chrome**: Click the three-dot menu (top-right) > Extensions > Manage Extensions.
   - For **Mozilla Firefox**: Click the three-line menu (top-right) > Add-ons and Themes > Extensions.

er browsers if applicable

2. **Review Installed Extensions**
   - Listed all installed extensions and noted their names, developers, and purposes.
   - Checked the source of each extension (Chrome Web Store, Mozilla Add-ons, or third-party sites).
   - Identified extensions that were unfamiliar, unused, or installed without consent.
3. **Check Permissions and Reviews**
   - Reviewed permissions for each extension (access to all website data, clipboard, or downloads).
   - Visited the extensions page on the official store to check user reviews, ratings, and developer information.
   - Flagged extensions with excessive permissions (access to all tabs or sensitive data) or poor/no reviews.
4. **Identify Suspicious or Unused Extensions**
   - Criteria for suspicion:
     - Unknown or unverified developers.
     - Excessive or unnecessary permissions (reading all browsing data for a simple tool).
     - No clear purpose or functionality.
     - Installed without user knowledge (potentially bundled with other software).
   - Identified unused extensions (not used in the last 3 months).
5. **Remove Suspicious or Unnecessary Extensions**
   - Removed extensions that met the suspicious criteria or were no longer needed.
   - Confirmed removal by checking the extension manager after deletion.
6. **Restart Browser and Check Performance**

- Restarted the browser to ensure changes took effect.
- Observed browser performance (speed, memory usage, or unexpected behavior).
- Noted any improvements or issues post-removal.

7. **Research on Malicious Extensions**
   - Malicious extensions can harm users by:
     - **Data Theft**: Stealing browsing data, cookies, or login credentials.
     - **Adware/Malvertising**: Injecting unwanted ads or redirecting to malicious sites.
     - **Cryptojacking**: Using browser resources to mine cryptocurrency.
     - **Tracking**: Monitoring user activity for unauthorized profiling or data sales.
     - **Phishing**: Displaying fake login pages to capture sensitive information.
   - Sources: General knowledge of browser security and common threats associated with malicious extensions.

4 Findings: Suspicious Extensions Identified and Removed

Extension Name	Developer	Permissions	Reason for Suspicion	Action Taken
Web Speed Booster	Unknown Dev	Access to all tabs, read/write data	Unfamiliar, no clear purpose	Removed
Coupon Finder Pro	ShopEasy Inc.	Access to all browsing data	Excessive permissions for coupon tool	Removed
Quick Search Enhancer	NoDevListed	Modify search results	Installed without consent	Removed
[Add rows as needed]				

5 Observations

- **Post-removal performance**: [Browser feels faster, no pop-ups observed]
- **Any issues encountered**: [None, or describe any problems]
- **Additional notes**: [Plan to monitor browser for a week to ensure no residual effects]

6 Recommendations

- Regularly review installed extensions (every 3 months).
- Only install extensions from trusted sources like the Chrome Web Store or Mozilla Add-ons.
- Use antivirus software to scan for bundled malicious extensions.
- Keep browser and extensions updated to patch security vulnerabilities.

7 Outcome

Awareness of browser security risks and managing browser extensions.