Identify and Remove Suspicious Browser Extensions

CyberSecurity Internship

Reported By Thumma Kirnmai

Date: 05-06-2025

Browser Extensions

- Browser extensions are small software programs that enhance the functionality of a web browser. They integrate into browsers like Chrome, Firefox, Edge, and Safari, offering additional features beyond default capabilities
- Common uses include security enhancements such as ad blockers, password managers, and anti-malware tools Productivity tools like grammar checkers, session managers, and task organizers Development tools such as web profilers, API debugging tools, and SEO analyzers Entertainment and customization options including dark mode extensions, video downloaders, and theme modifiers E-commerce features like price comparison tools and automatic coupon finders
- Risks include malicious extensions that steal data or inject malware excessive permissions that allow access to browsing history, keystrokes, or personal details fake extensions from unverified publishers mimicking legitimate ones
- Best practices involve installing from trusted sources such as the Chrome Web Store and Mozilla Add-ons regularly reviewing permissions and removing unused extensions using technology profilers like Wappalyzer for analysis.

Tools Used

- Browser Extension Manager (Chrome, Firefox, or any other browser)
- Wappalyzer (To profile technology used by websites)
- BuiltWith (For additional extension analysis)
- Web Search (For research on extension risks)

Methodology

Step 1: Accessing the Extension Manager

- Opened the browser’s extension/add-ons manager to view all installed extensions.
- Observed all extensions listed, noting their permissions and descriptions.

Step 2: Reviewing Installed Extensions

- Checked the permissions requested by each extension.
- Reviewed user ratings and reviews to identify any complaints or security warnings.
- Used technology profilers (e.g., Wappalyzer, BuiltWith) to gather insights on lesser-known extensions.

Step 3: Identifying Suspicious Extensions

- Flagged extensions with excessive permissions (e.g., access to user data, keystrokes, or browsing history).
- Identified extensions with poor reviews, unverified publishers, or unknown developers.
- Noted extensions that were not used regularly and could be removed for better security.

Step 4: Removal Process

- Removed all unnecessary and suspicious extensions.
- Restarted the browser to ensure smooth performance post-cleanup.

PDF Converter Pro

- ➢ Status: Removed
- ➢ Reason: Requested permission to read/change all website data — unnecessary for a converter.

Weather Forecast+

- ➢ Status: Removed
- ➢ Reason: Redirected browser to suspicious external ad sites.

Recommendations

- Always verify the source before installing a browser extension.
- Regularly review and remove unused or suspicious extensions.
- Monitor extension permissions carefully to prevent data leaks.
- Use technology profiling tools like Wappalyzer and BuiltWith for analysis.