Suspicious Browser Extensions Audit Report

# Objective

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

# Tools Used

Google Chrome

# Suspicious Extensions Identified & Removed

## Hola VPN – Free VPN Proxy

Permissions: Access to all websites, read and change all your data.

* Issues Identified:
* Routes user traffic through other users’ devices (peer-to-peer network), which can be exploited.
* Known history of misuse and abuse of user bandwidth.
* Previously flagged by security researchers for potential privacy risks.

Action Taken: Removed to prevent exposure to traffic hijacking.

## Super Dark Mode

Permissions: Modify appearance and content on every website.

* Issues Identified:
* Requests access to all websites unnecessarily.
* Some versions contain hidden adware scripts.
* Reports of injecting affiliate links without user consent.

Action Taken: Removed due to invasive permissions and ad-injection risk.

## PDF Converter – Free PDF Tools

Permissions: Read and change all data on websites you visit.

* Issues Identified:
* Multiple user reviews report redirect behavior and suspicious popups.
* Likely bundled with browser hijacker malware.

Action Taken: Removed to prevent data leakage and redirect attacks.

## Flash Video Downloader

Permissions: Full read/write access to visited websites.

* Issues Identified:
* Outdated; requires deprecated Flash components.
* Known to inject malicious scripts on video sites.
* May log user activity for third-party ad networks.

Action Taken: Removed due to outdated tech and security risks.

## Easy Shopping

Permissions: Track browser activity, modify content.

* Issues Identified:
* Functions as adware, displaying fake deals and promotions.
* Tracks user behavior and sends it to third parties.
* Difficult to uninstall; may reinstall itself.

Action Taken: Removed and browser cleaned.

# Outcome

After removing the above extensions:  
- Browser performance improved (faster loading times, fewer ads/pop-ups).  
- Increased awareness of privacy risks posed by extensions.  
- Reduced exposure to potential phishing and data leakage threats.