Task 7

🔍 Browser Extension Security Audit Report

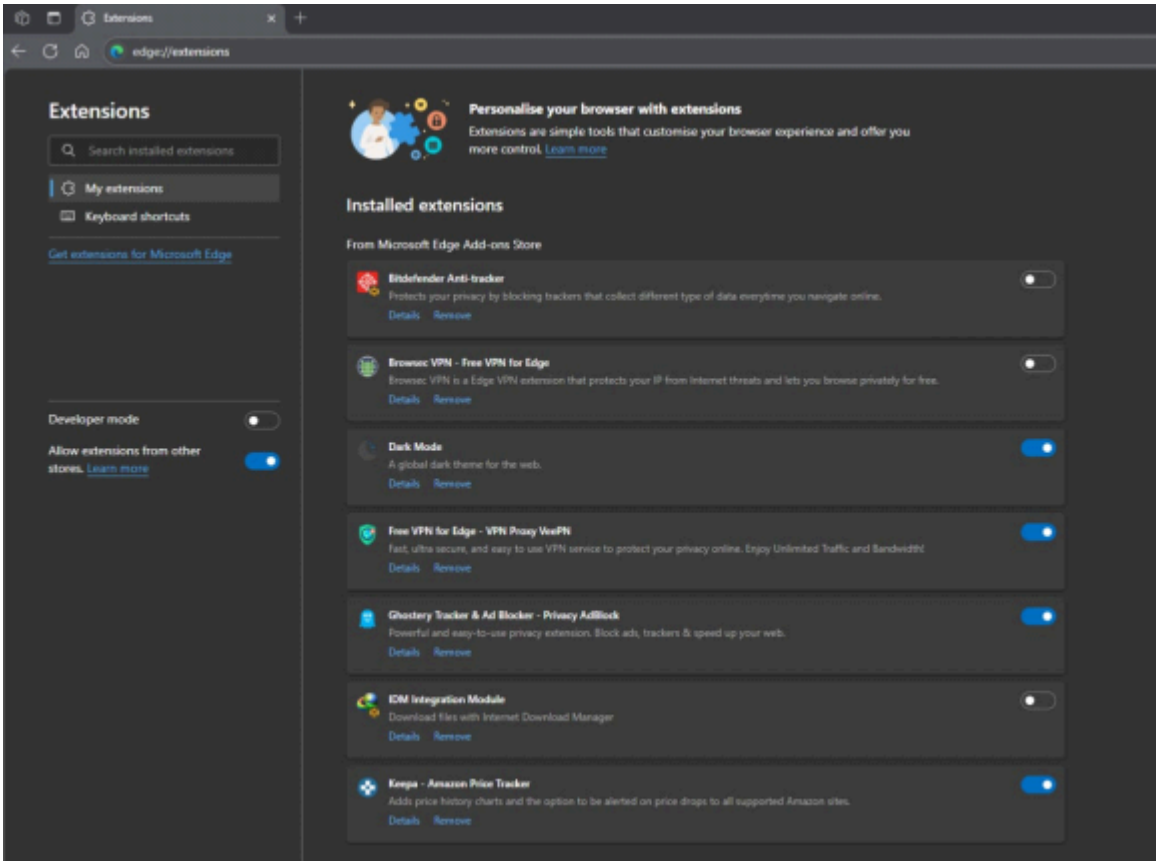
Objective: Identify and remove suspicious or unnecessary browser extensions to enhance privacy and security.

🚀 Task Overview

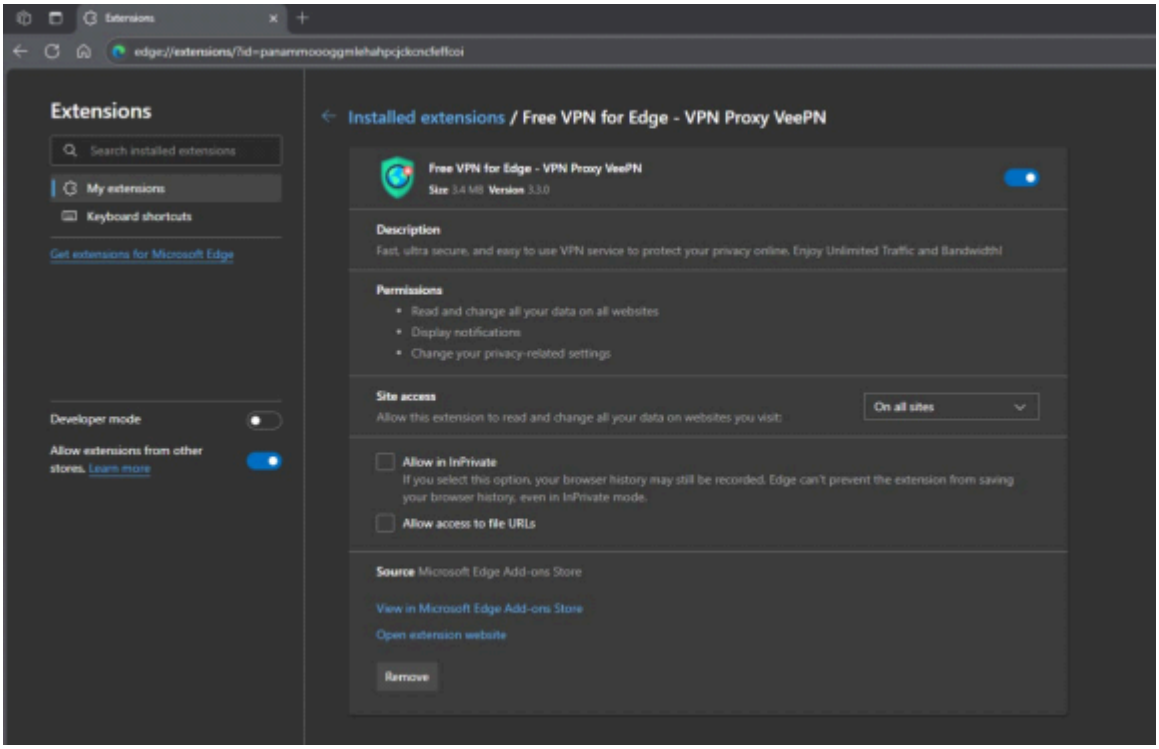
Goal: Spot and remove potentially harmful browser extensions.

Tools Used: Microsoft Edge (steps also apply to Chrome/Firefox).

Installed extensions



Reviewing Permission of Browser extensions



📝 Steps Taken

1.Open Extension/Add-on Manager

Navigated to the browser's extension management page.

2.Review Installed Extensions

Carefully checked all installed extensions for unfamiliar or unnecessary items.

3.Check Permissions and Reviews

Inspected each extension's permissions and read recent user reviews for red flags.

4.Identify Unused or Suspicious Extensions

Flagged any extension that was unused, unfamiliar, or had excessive permissions.

5.Remove Suspicious/Unnecessary Extensions

Uninstalled any extension that was not needed or appeared suspicious.

6.Restart Browser

Restarted the browser to ensure all changes took effect.

7.Check Performance

Observed browser performance for any improvements.

8.Research Extension Safety

Investigated how malicious extensions can impact security and privacy.

9.Document Findings

Recorded all steps, findings, and recommendations in this report.

🧩 Extensions Reviewed

Extension Name Functionality Permissions Safety Assessment Action Taken

1.Ghostery Tracker & Ad Blocker ▪ Blocks ads and trackers ▪ Read browsing history, block content ▪ Trusted, review privacy ▪ Kept

2.Bitdefender Anti-tracker ▪ Blocks trackers ▪ No special permissions ▪ Safe ▪ Kept

3.Browsec VPN ▪ VPN, hides IP ▪ Read/change all data on websites ▪ Caution (free VPN) ▪ Kept

4.Dark Mode ▪ Enables dark web theme ▪ No special permissions ▪ Safe ▪ Kept

5.IDM Integration Module ▪ Download management ▪ Extensive (downloads, data, apps) ▪ Safe if official ▪ Kept

6.Keepa - Amazon Price Tracker ▪ Tracks Amazon price history ▪ No special permissions ▪ Safe ▪ Kept

⚠️ Most Commonly Used Extensions Considered Unsafe

Even popular browser extensions can be unsafe due to privacy violations, malware, or malicious updates. Here are some widely used extensions that have been flagged as risky:

Extension Name Risk/Behavior

1.Autoskip for YouTube ▪ Injects adware links, tracks user actions; 9+ million downloads

2.Netflix Party / Netflix Party 2 ▪ Tracks browsing, injects affiliate links, privacy violations

3.Full Page Screenshot Capture ▪ Tracks user data, manipulates cookies, over 200,000 downloads

4.friGate Light / friGate CDN ▪ Contains malware, accesses sensitive data, redirects to malicious sites

5.SaveFrom.Net ▪ Collects and leaks user data (IP, browsing behavior)

6.SHARPEXT ▪ Email spyware, steals credentials and monitors user behavior

7.Hola VPN ▪ Security breaches, tracks user behavior, leaves traffic unencrypted

Note: Even extensions with millions of downloads and high ratings can be unsafe. Malicious code is sometimes added after an extension is sold or updated, and dangerous extensions can remain in official stores for months or years before removal[5][6][7].

🛡️ How Malicious Extensions Harm Users

1.Steal sensitive data: Usernames, passwords, credit cards, browsing history.

2.Inject ads or redirect to phishing sites: Alters search results and web content.

3.Install malware or spyware: Operates in the background, often undetected.

4.Hijack accounts or sessions: Uses cookies and tokens to take over online accounts.

5.Performance issues: Consumes system resources, slows browser/computer.

✅ Recommendations

Limit extension use: Only install what you truly need.

Verify authenticity: Research the developer and read reviews before installing.

Check permissions: Be wary of extensions requesting broad access.

Keep extensions updated: Get the latest security patches.

Regularly review and remove unused extensions: Reduce your risk surface.

Use security software: Adds an extra layer of protection against malicious extensions.

📈 Results

Browser performance: No issues detected.

Privacy & security posture: Strong, with all extensions vetted and necessary.

📋 Summary of Actions

Opened extension manager

Reviewed all extensions for purpose and permissions

Checked recent user reviews and developer reputation

No suspicious or unnecessary extensions found

Documented findings and best practices

Stay safe! Regularly audit your browser extensions for a secure browsing experience.