TASK-7

Official Report: Identifying and Removing Suspicious Browser Extensions:

Objective:

To detect, analyze, and remove suspicious or unnecessary browser extensions, ensuring improved browser performance and enhanced cybersecurity.

Mini Guide Implementation Steps:

Step 1: Open Browser's Extension Manager

- Navigated to the extensions page:
    - Chrome: chrome://extensions/
    - Edge: edge://extensions/

Step 2–4: Review and Evaluate Installed Extensions

Below are five selected extensions reviewed during the audit:

Extension Name	Permissions Requested	User Reviews Summary	Suspicious?	Notes
Honey	Access to all browsing data, change webpage content	Mostly positive, trusted company (PayPal)	❌ No	Safe and widely used
Grammarly	Reads and modifies text input on websites	Positive reviews, millions of users	❌ No	Well-reviewed productivity tool
Dark Mode - Night Eye	Modifies appearance of websites, access to all pages	Some mixed reviews, performance issues reported	✅ Yes	Causes lag on some systems
Easy PDF Converter	Access all website data, change content on all pages	Very poor reviews, flagged on multiple forums	✅ Yes	High-risk, flagged as malware
Weather Extension Pro	Location access, change browser behavior	Poor rating, aggressive popups and redirects	✅ Yes	Classified as adware

---

Step 5: Removal Actions Taken

Extensions Removed:

1. **Easy PDF Converter**
   - Reason: Poor reviews, overreaching permissions, potential malware risk.
2. **Weather Extension Pro**
   - Reason: Adware behavior, location tracking, and intrusive pop-ups.
3. **Dark Mode - Night Eye**
   - Reason: Performance degradation, possible conflict with other apps.

Step 6: Browser Restart

- The browser was restarted post-removal.
- Noted a **significant improvement** in:
  - Tab load speed
  - Reduced CPU usage
  - No more intrusive ads or redirects

Step 7: Research on Risks of Malicious Extensions

Common Threats from Malicious Extensions:

- **Data Theft**: Harvesting login credentials, credit card details, and browsing history.
- **Ad Injection**: Inserting unauthorized ads into websites.
- **Redirection**: Hijacking browser to lead users to malicious or phishing sites.
- **System Exploits**: Leveraging browser vulnerabilities to install further malware.
- **Surveillance**: Tracking user behavior across all websites.

Step 8: Documentation Summary

Extension Name	Action Taken	Justification
Honey	Kept	Trusted, useful, and well-reviewed
Grammarly	Kept	Productivity enhancer with good trust
Dark Mode - Night Eye	Removed	Performance concerns

Extension Name	Action Taken	Justification
Easy PDF Converter	Removed	Malware warnings, unnecessary access
Weather Extension Pro	Removed	Identified as adware

Conclusion:

Three suspicious extensions were identified and removed. Browser performance improved noticeably. This exercise highlights the importance of regularly auditing extensions to protect against malware and privacy breaches.