Elevate Labs – Cyber Security Internship

Name:Srinivas Atta

Task 7: Identify and Remove Suspicious Browser Extensions

By: Ministry of MSME, Govt. of India

Objective

Learn how to spot potentially harmful browser extensions, remove them, and understand their security risks.

Tools Required

- Any modern web browser (e.g., Google Chrome, Mozilla Firefox)

Execution Steps / Guide

1. Open extension manager
    - Chrome: `chrome://extensions/`
    - Firefox: `about:addons`
2. Review installed extensions
    - Note each extension's name, purpose, and developer.
3. Check permissions
    - Watch for suspicious permissions like:
        - "Read and change all your data on all websites"
        - "Access browsing history"
        - "Capture clipboard data"
4. Verify extension authenticity
    - Check ratings, reviews, official developer info.
5. Identify suspicious/unused extensions
    - Examples: Unknown publisher, very high permissions, poor reputation, or not updated for years.
6. Remove suspicious extensions

    - Chrome: Toggle off → Click Remove.
    - Firefox: Disable/Remove via Add-ons Manager.
7. Restart browser
    - Ensure changes are applied.
8. Research malicious extension cases
    - Noted that malicious extensions can:
        - Steal account credentials
        - Redirect to phishing websites
        - Inject ads/malware
        - Track browsing activity

Findings / Results

- Extensions Reviewed: 6 (example)
- Suspicious Findings:
    - Extension requesting access to *all browsing data* despite being a simple wallpaper app.
    - One extension flagged as removed from Web Store.
- Actions Taken:
    - Removed unused extensions.
    - Kept only trusted ones from official developers (e.g., Adblock, Grammarly).
    - Restarted browser; browsing improved slightly in performance.

Security Analysis

Browser extensions pose serious threats if malicious:

- Can steal saved passwords, cookies, and form inputs.
- Can inject ads/spyware.
- May serve as backdoors for malware/ransomware.

Unused or shady extensions increase the attack surface unnecessarily.

Recommendations

- Only install extensions from official stores (Chrome Web Store, Firefox Add-ons).
- Regularly review installed extensions.

- Remove any that are unused or have excessive permissions.
- Keep extensions updated for security patches.
- Use browser security settings and enable warnings for suspicious behavior.

Outcome

- Successfully identified and removed unsafe/unused browser extensions.
- Learned how to evaluate extension permissions and authenticity.
- Gained awareness of how malicious extensions exploit users.

Key Concepts

- Browser security
- Extension permissions
- Malicious software risks
- Safe extension management
- Best practices for securing browsers