Identify and Remove Suspicious Browser Extensions

1. **steps taken**

- Open your browser's extension/add-ons manager.
  (edge: edge://extensions/)
- Review all installed extensions carefully.
  Look for unfamiliar names, recently added items, or anything you did not install knowingly.
- Check permissions and reviews for each extension.
  Extensions requesting access to "read and change all your data on the websites you visit" should be reviewed carefully.
- Identify any unused or suspicious extensions.
  Consider extensions with:
  - No clear purpose
  - Poor reviews
  - Excessive permissions
  - Reports of adware or data tracking
- Remove suspicious or unnecessary extensions.
  Use the browser's built-in "remove" or "uninstall" option.
- Restart the browser and check for performance improvements.
  Verify whether issues like pop-ups, redirects, and slow performance have stopped.

2. **extensions removed**

- google docs offline
  - This extension can read and change your data on sites you open. Control how this extension can access your data on sites from the below settings.

Security Incident Matrix — Malicious Browser Extension

- **Details**
- Incident Name: Malicious / Suspicious Browser Extension
- Incident Type: Browser-based malware, Adware, Data exfiltration, Unauthorized access
- Severity Level: Medium to High
- Detected By: User report / Alerts
- Systems Affected: Browser, User profile, Session data
- **Indicators of Compromise (IoCs):-**
- Pop-ups, redirects, homepage change
- Suspicious outbound traffic
- Unknown extension with high permissions
- **Immediate Response:-**
- Disconnect internet if severe
- Identify and disable suspicious extensions
- Reset browser settings
- Clear cache, cookies
- Notify IT/SOC team
- **Containment: -**
- Block malicious domains
- Disable syncing
- Enforce extension policies
- **Eradication: -**
- Remove residual files
- Scan system with Defender/Malwarebytes
- Check DNS/proxy settings
- **Recovery:-**
- Restart system
- Re-enable trusted extensions
- Monitor for 48 hours

- **Prevention: -**

- Allowlist extensions
- User awareness training
- Browser security tools

3. how malicious extensions can harm users.

Malicious or poorly designed browser extensions can act like miniature malware inside your web browser. Because extensions often request powerful permissions (like reading or modifying all websites you visit), they can abuse this access to perform harmful activities without the user noticing.

Below are the major security risks:

1. Data Theft

Malicious extensions can collect sensitive browsing information such as:

What they can steal:

- Browsing history
- Search queries
- URLs visited
- Personal data from websites
- Autofill data (emails, phone numbers, personal info)
- Cookies and session tokens (in some cases)

How it harms users:

- Privacy invasion
- Targeted ads or profiling
- Selling data to third parties
- Tracking user across websites
- Possible account takeovers if session data is captured

2. Browser Redirection

Malicious extensions often modify browsing behavior to redirect users.

Examples of harmful redirects:

- Redirecting search queries to unsafe or ad-filled search engines
- Sending users to phishing websites
- Redirecting to websites with malware downloads
- Hijacking new tab pages or homepage

Impact on users:

- Exposure to scams and phishing
- Loss of control over browsing experience
- Increased risk of downloading malware
- Confusion and reduced productivity

3. Ad Injection (Adware Behaviour)

Some extensions inject unwanted advertisements or pop-ups into normal webpages.

What they can inject:

- Banner ads
- Pop-up ads
- Fake warnings (“Your PC is infected”)
- Affiliate links
- Pop-under ads

Why it happens:

- Extensions generate revenue for their creators through ad impressions
- They modify webpage content to show their own ads

Impact on users:

- Slow browsing
- Cluttered webpages
- Higher CPU/Memory usage
- Exposure to malicious or deceptive ads
- Increased chance of clicking harmful content

4. Credential Harvesting

The most dangerous capability: stealing usernames, passwords, and authentication tokens.

How extensions can steal credentials:

- Injecting scripts into login forms
- Keylogging input fields
- Extracting data from browser autofill
- Capturing cookies or session tokens
- Redirecting users to fake login pages (phishing)

Impact:

- Full account takeover
- Financial fraud (banking logins stolen)

- Email and social media compromise
- Business email compromise (BEC)
- Identity theft

3(a). Why Malicious Extensions Are Dangerous

- They *look legitimate* and install like normal apps
- Users trust them and grant powerful permissions
- They run continuously in the background
- Browsers sync extensions across devices silently
- Many bypass antivirus or firewall detection
- Attackers use them for long-term spying
-

3(b). How to Protect Yourself

- Only install extensions from trusted developers
- Avoid extensions requiring excessive permissions
- Regularly remove extensions you no longer need
- Enable browser security protections
- Use antivirus/EDR tools that monitor browser activity