

Identify and Remove Suspicious Browser Extensions

Objective

To learn how to identify, analyze, and remove potentially harmful browser extensions to improve browser security, privacy, and performance.

Tools Used

- Google Chrome Web Browser

Step 1: Open Browser Extension Manager

The Chrome Extensions Manager was opened using:

Menu (:) → Extensions → Manage Extensions

Step 2: Review All Installed Extensions Carefully

All installed extensions were reviewed by checking their names, purposes, status (enabled/disabled), and whether they were genuinely needed. Chrome's built-in **Safety Check** section was also reviewed for warnings.

Step 3: Check Permissions and Reviews for Each Extension

Permissions requested by each extension were examined, especially access to:

- Browsing data
- Website content
- Background activity

Chrome safety warnings and policy messages were used to assess extension reliability.

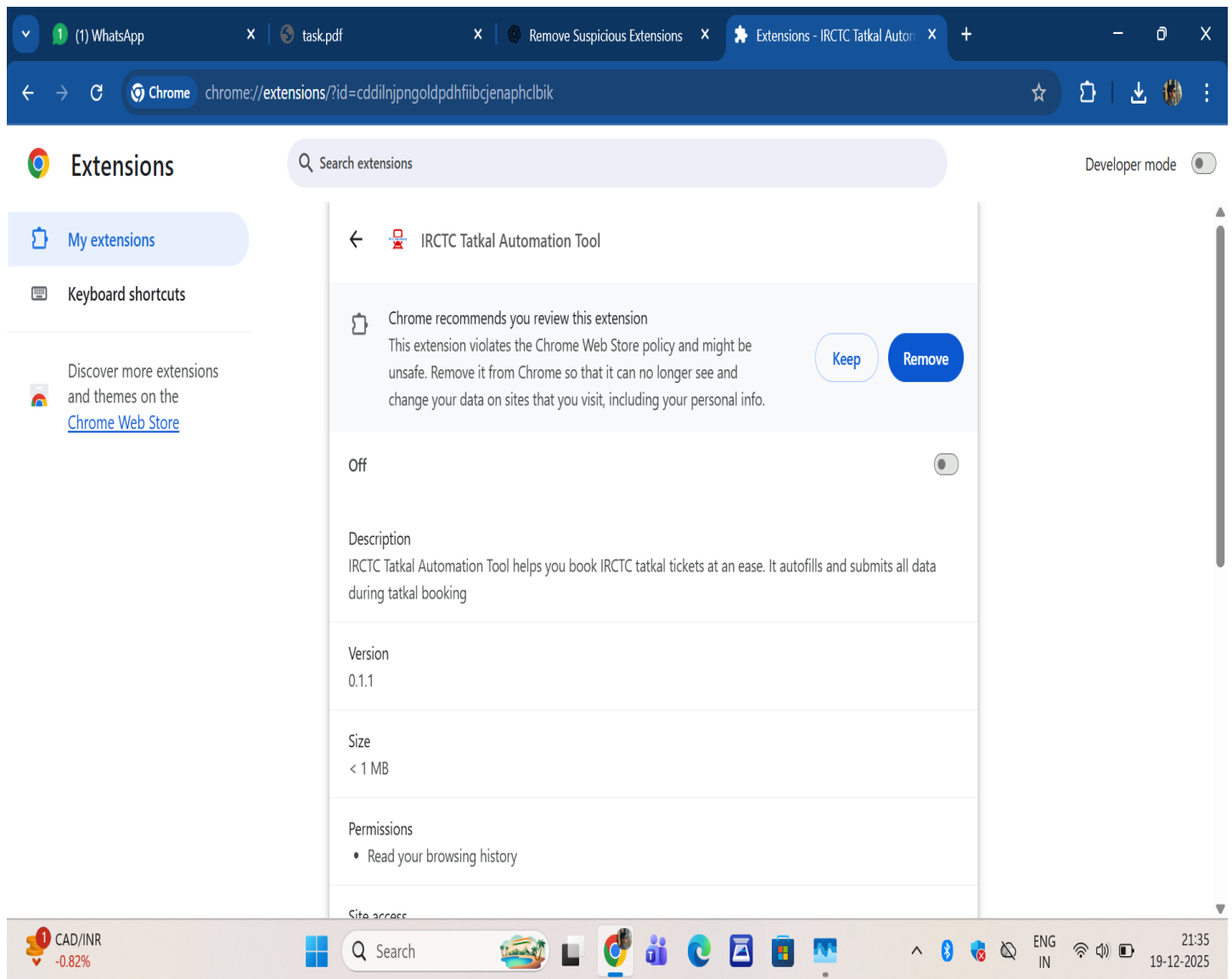
Step 4: Identify Unused or Suspicious Extensions

Chrome flagged **two extensions as unsafe**, indicating potential security risks:

Extension Name	Status	Reason
Free VPN ZenMate – Best VPN for Chrome	Disabled	Chrome cannot verify the source
IRCTC Tatkal Automation Tool	Disabled	Violates Chrome Web Store policy

These extensions were identified as suspicious due to policy violations and unknown sources.

A screenshot of the Google Chrome browser's 'Extensions' page. The address bar shows 'chrome://extensions'. The left sidebar has 'My extensions' and 'Keyboard shortcuts'. The main area has a 'Safety check' section with a warning: 'Review 2 extensions that may be unsafe'. It lists 'Free VPN ZenMate-Best VPN for Chrome' (Off - Chrome can't verify where this extension comes from) and 'IRCTC Tatkal Automation Tool' (Off - This extension violates the Chrome Web Store policy). Below this is the 'All extensions' section, showing 'Adobe Acrobat: PDF edit, convert, sign tools' and 'Foxified' (Emulate firefox extensions in Chrome, Opera and other Chromium based browsers). Each extension card has 'Details' and 'Remove' buttons and a toggle switch.



Step 5: Remove Suspicious or Unnecessary Extensions

The suspicious extensions were **disabled and removed** using the **Remove** option as recommended by Chrome to reduce security risks.

Step 6: Restart Browser and Check Performance

After removing the suspicious extensions, the browser was restarted.
Result observed:

- Improved browser stability
- No unexpected redirects or warnings
- Faster page loading

Step 7: Research How Malicious Extensions Can Harm Users

Malicious browser extensions can:

- Steal personal data and passwords
- Track browsing activity without consent
- Inject unwanted ads or redirects
- Slow down browser performance
- Install additional malware

Step 8: Documentation of Actions Taken

Suspicious Extensions Removed

Extension Name	Action Taken
Free VPN ZenMate – Best VPN for Chrome	Removed
IRCTC Tatkal Automation Tool	Removed

Safe Extensions Retained

Extension Name	Purpose
Adobe Acrobat PDF Tools	PDF viewing and editing
Foxified	Firefox extension compatibility

Conclusion

Regularly reviewing browser extensions is essential for maintaining security and privacy. Chrome’s safety check helped identify unsafe extensions, which were removed to ensure a safer and more efficient browsing experience.