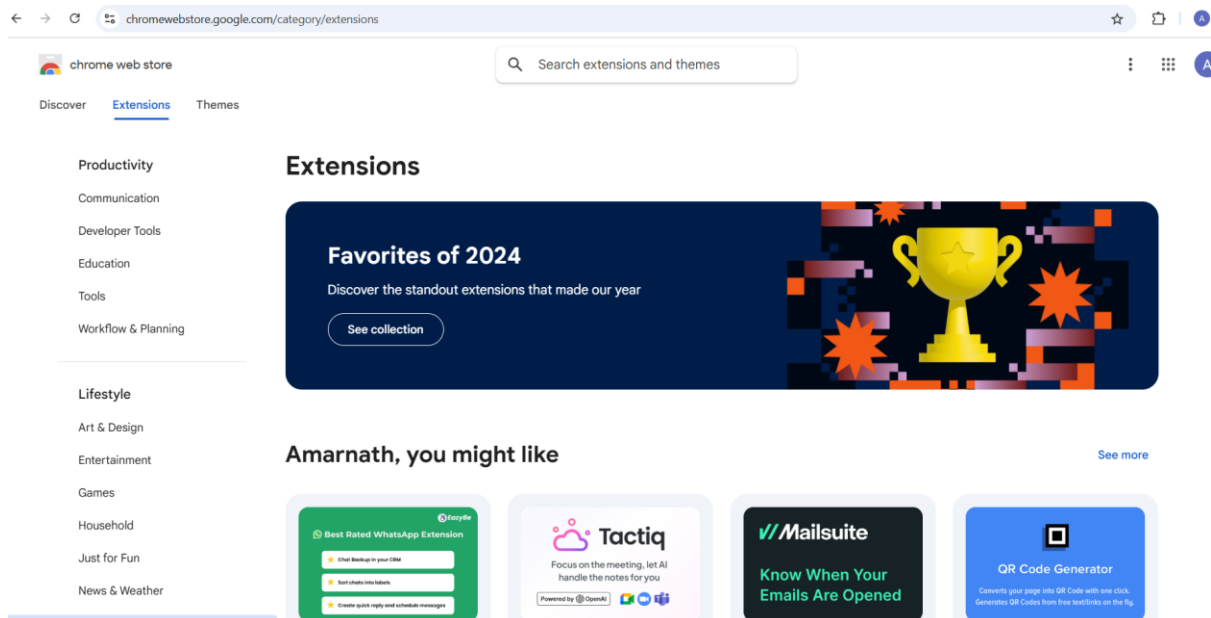# Identify and Remove Suspicious Browser Extensions

Objective: Learn to spot and remove potentially harmful browser extensions.

Tools: Any web browser (Chrome, Firefox)

Deliverables: List of suspicious extensions found and removed

STEP 01: Open your browser's extension/add-ons manager.

STEP 02: Review all installed extensions carefully.

I have verified this page , it gives a 4.5 ratings and overall users list is 60,000 . Above screenshot gives a detail about the page and version, size and developer .

STEP 03: Check permissions and reviews for each extension.

All the reviews to be provided positive and its true to the website .

- If any suspicious things happened remove the extension immediately .
- Remove the low rated apps like 2.5 ratings, 2 ratings apps.

STEP 04: Research how malicious extensions can harm users.

DATA THEFT

1. Access to browsing history: Malicious extensions can read the URLs of websites you visit.
2. Credential stealing: They can capture login credentials by monitoring login forms or capturing keystrokes.
3. Clipboard monitoring: Some can read copied data (like passwords, bank details, or crypto wallet addresses).

SPYWARE AND SURVEILLANCE

1. Track your location
2. Record your mouse clicks and keystrokes
3. Monitor behavior to build a profile of your habits.

PHISHING AND FAKE CONTENT INJECTION

1. Inject malicious ads, banners, or popups on legitimate websites.

2. Replace real website content with phishing pages to trick you into entering passwords or card numbers.

3. Redirect you to fake login pages that resemble real websites (Google, Facebook, banking, etc.).

STEP 05: Document steps taken and extensions removed.

Browser used: Chrome://extensions

QR CODE GEBERATOR

Ratings: 4.9/5

Permissions: All checked

Reviews: All to be checked and positive reviews.