# ELEVATE LABS INTERNSHIP

## Day-07

Name : Mohamed Riyas

Role: Cyber Security Analyst

Task: 07

Title: Identify and Remove Suspicious Browser Extensions

Date: 03-07-2025

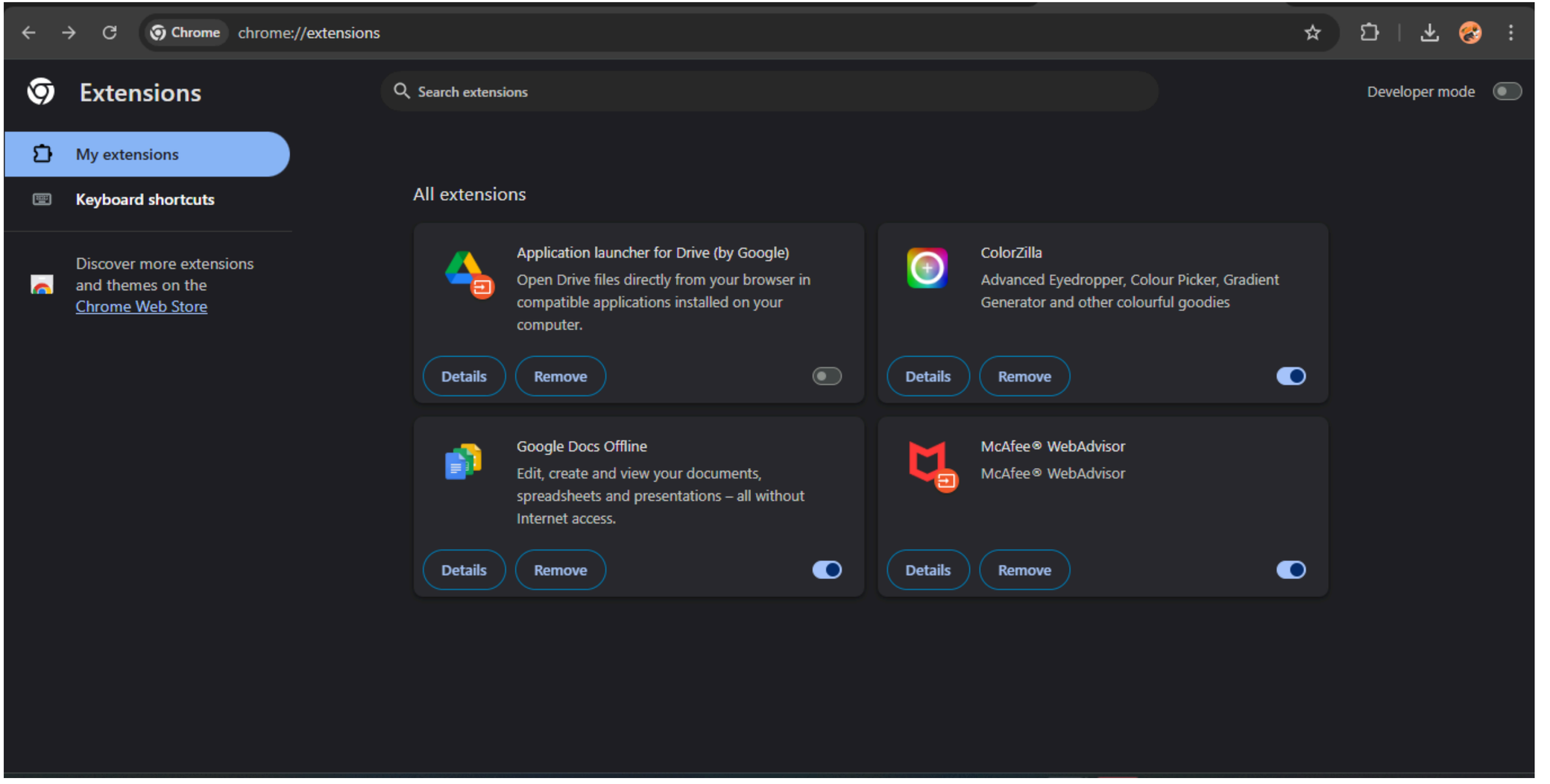
**Objective:** Learn to spot and remove potentially harmful browser extensions.

**Tools:** Any web browser (Chrome, Firefox)

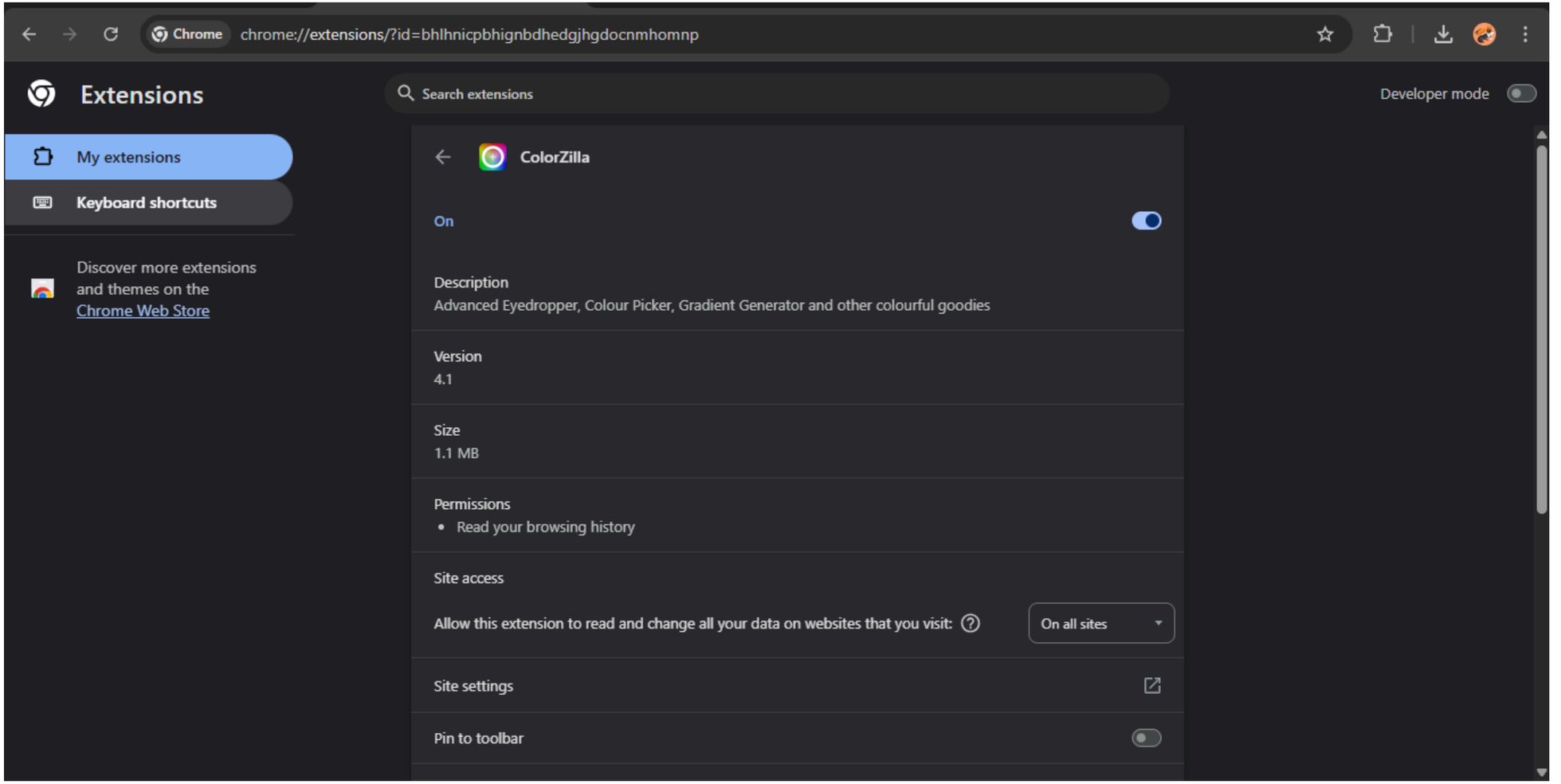
**Deliverables:** List of suspicious extensions found and removed

## Step by step procedure to complete the task

### 1 .Review all installed extensions carefully.


Chrome
chrome://extensions
Extensions
Search extensions
Developer mode
My extensions
Keyboard shortcuts
Discover more extensions and themes on the Chrome Web Store
All extensions
Application launcher for Drive (by Google)
Open Drive files directly from your browser in compatible applications installed on your computer.
Details
Remove
ColorZilla
Advanced Eyedropper, Colour Picker, Gradient Generator and other colourful goodies
Details
Remove
Google Docs Offline
Edit, create and view your documents, spreadsheets and presentations – all without Internet access.
Details
Remove
McAfee® WebAdvisor
McAfee® WebAdvisor
Details
Remove

# 2 Remove suspicious or unnecessary extensions.




Am just remove this extension from my browser because this extension have capability to read and change all your data on websites that you visit.

# 3. Research how malicious extensions can harm users.

How Malicious Extensions Harm Users:

**1. Steal Sensitive Data**

- Some extensions can access:
  - Login credentials
  - Credit card info
  - Emails & chats
- Example: If you log in to your bank, the extension may capture the username/password.

**2. Spy on Browsing Activity**

- They track all websites you visit.
- Create a user profile and sell your data to advertisers or attackers.

**3. Inject Ads and Redirects**

- Replace real ads with fake ones.
- Redirect you to fake or phishing websites.

Example: You search on Google, but it takes you to a scam site.

**4. Install Malware**

- Some extensions download harmful files or backdoors silently.
- They can:
  - Encrypt files (ransomware)
  - Turn your system into a botnet

**5. Bypass Security Settings**

- They can disable your browser security protections or antivirus extensions.