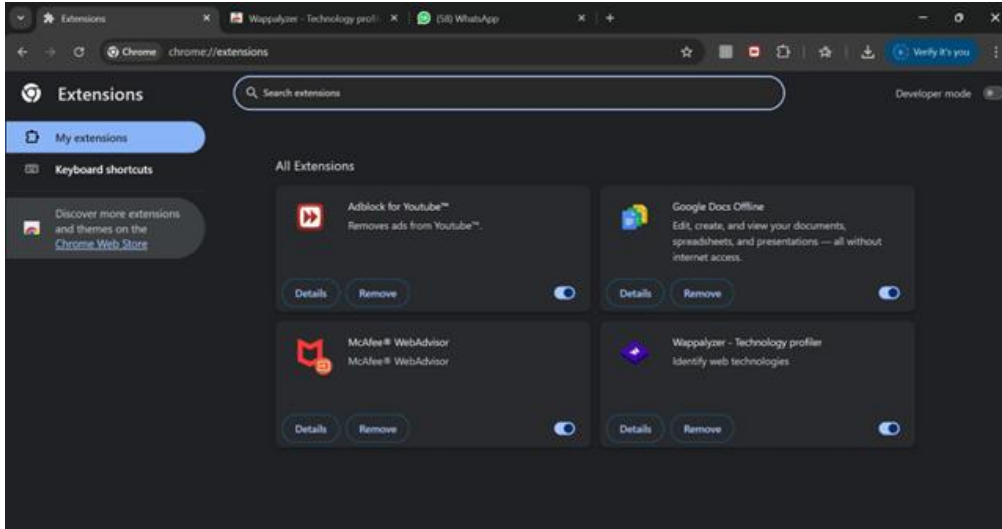


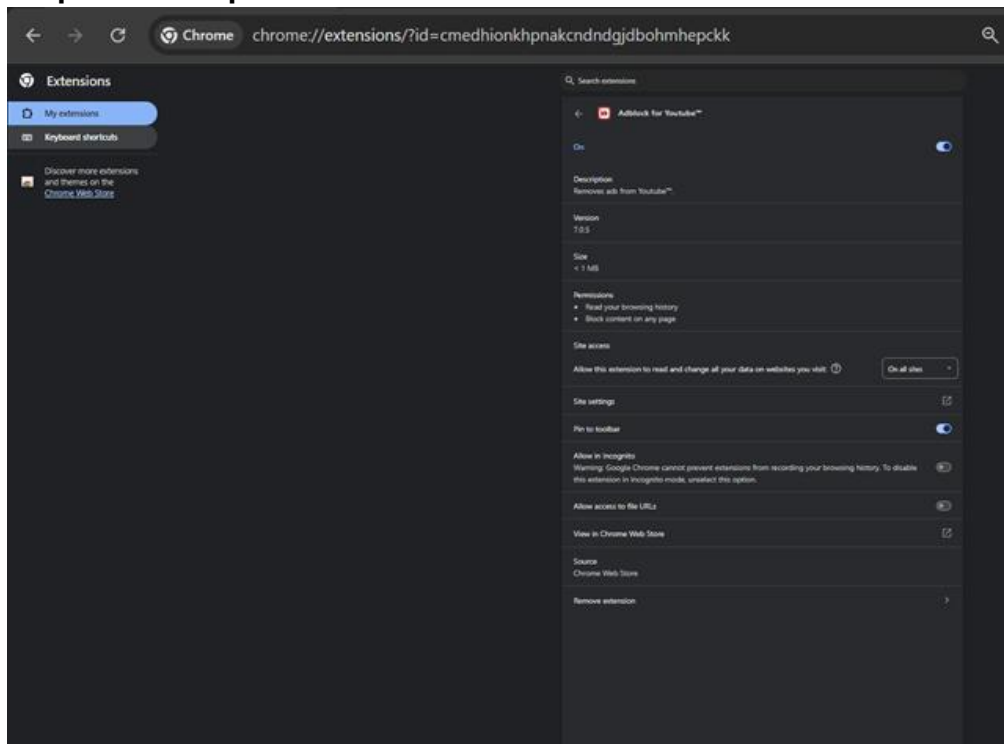
Task 7 - Browser Extensions Security

Step 1: Open your browser's extension/add-ons manager



Step 2: Review all installed extensions carefully

Step 3: Check permissions and reviews for each extension

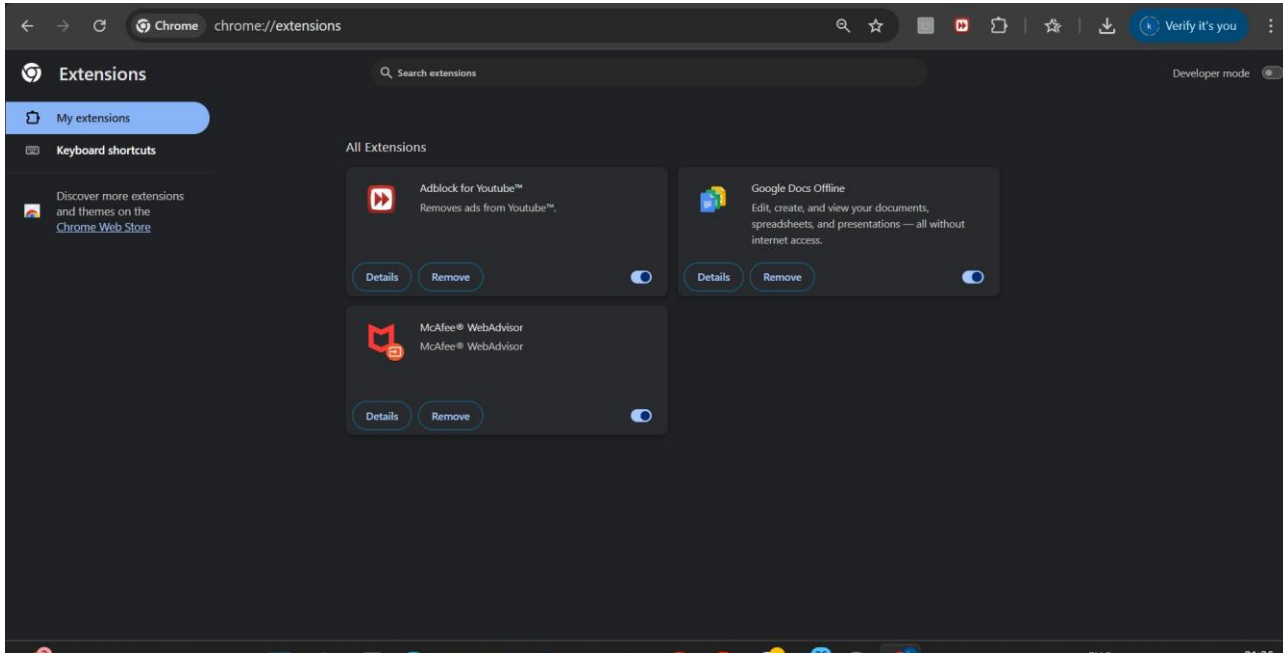


For the **Adblock for YouTube™** extension, it requested high-risk permissions such as “Read and change your data on all websites,” which is expected for an ad blocker but still poses potential privacy concerns. Reviews were mostly positive, though some users reported performance issues and occasional bugs.

Task 7 - Browser Extensions Security

Step 4: Identify any unused or suspicious extensions

Step 5: Remove suspicious or unnecessary extensions



Step 7: Research how malicious extensions can harm users

Malicious browser extensions can harm users by stealing sensitive data such as passwords, credit card details, and browsing history, hijacking online accounts, tracking browsing habits, and injecting malicious content or phishing pages into legitimate websites. They may also deliver malware, secretly mine cryptocurrency (cryptojacking), or bypass browser security through excessive permissions like “Read and change all your data on all websites.”

Step 8: Document steps taken and extensions removed