Name: satya chaitanya yerninti

Email: satyachaitanya21@gmail.com

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

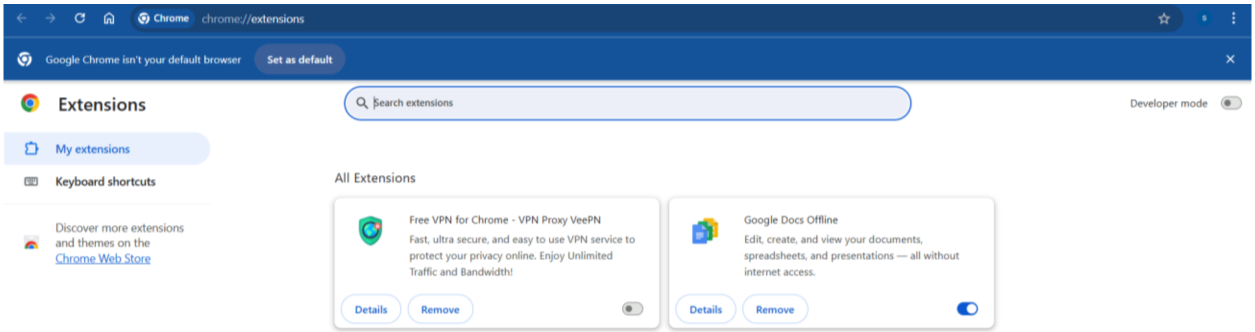
Browser used: google chrome

Harmful browser extensions can steal your data, including passwords and cookies, spy on your activity through keylogging and screenshots, inject malicious ads or malware, redirect you to phishing sites, and even perform unauthorized actions like financial transactions. These extensions can be disguised as legitimate tools, and a major risk is their ability to access and manipulate data on all websites you visit.

What harmful extensions can do

- **Data theft:** They can harvest sensitive information such as names, addresses, phone numbers, email addresses, and login credentials.
- **Session hijacking:** Some extensions steal session cookies, allowing attackers to log into your accounts without needing your password.
- **Surveillance:** They can monitor your browsing history, record keystrokes, and take screenshots of your screen.
- **Content manipulation:** Malicious extensions can inject unwanted ads or modify web content to trick you into divulging information.
- **Phishing:** They can redirect you to fake, but convincing, websites designed to steal your personal and financial information.
- **Malware delivery:** They can be a vector for delivering other types of malware to your device.
- **Performance issues:** Poorly designed extensions can slow down your browser and overall computer performance.
- **Unauthorized actions:** Some extensions can perform state-changing actions, such as changing your settings or submitting forms, without your consent.

Before installing harmful extensions



Google Chrome isn't your default browser

Discover more extensions and themes on the Chrome Web Store

Free VPN for Chrome - VPN Proxy VeePN

Fast, ultra secure, and easy to use VPN service to protect your privacy online. Enjoy Unlimited Traffic and Bandwidth!

Google Docs Offline

Edit, create, and view your documents, spreadsheets, and presentations — all without internet access.

Some harmful browser extensions are

- **Emoji keyboard online (kgmeffmlnkfnjpgmdndccklfigfhajen)**: Identified by Malwarebytes as a Chrome extension that could spy on users.
- **Free Weather Forecast (dpdibkfpbaadnnjhkmmnenkmbnhpobj):** Also flagged by Malwarebytes.
- **The Great Suspender:** A once popular extension that, in 2021, was updated to include malicious code that stole data.
- **SessionManager:** An extension that was updated in 2022 to steal session cookies and other data.
- **Fire Shield Extension Protection:** A Chrome extension with hundreds of thousands of users, identified by Kaspersky as being suspicious.

How to protect yourself

- **Be selective:** Only install extensions from trusted sources, and check their developer information and reviews before installing, suggests the University of California, Berkeley.
- **Review permissions:** Look for extensions that request unnecessary or invasive permissions, and be wary of those that request access to all your browsing data.
- **Regularly audit your extensions**: Periodically check your list of installed extensions and remove any you no longer use or that seem suspicious, says the University of Illinois System.
- **Use security software**: Install and maintain antivirus and anti-malware software that can detect and block malicious extensions.