# Task 7: Identify and Remove Suspicious Browser Extensions

For this task, I am going to take screenshots of installed Brave browser extensions on my PC. Then I will provide information about the installed extensions.

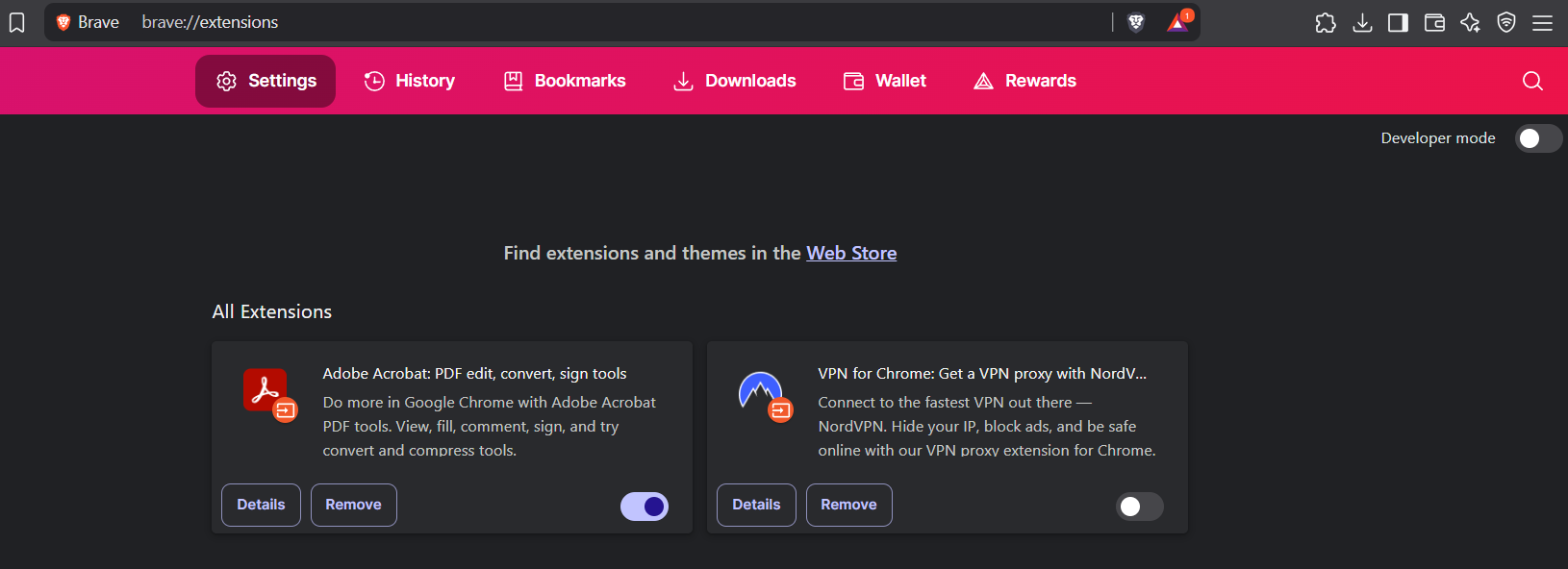


Figure 1 - Extensions installed in Brave browser

## There are two available web extensions on my PC:

1. Adobe Acrobat: PDF edit, convert, sign tools
2. VPN for Chrome: Get a VPN proxy with NordVPN

Now we are going to learn more about these extensions sequentially.

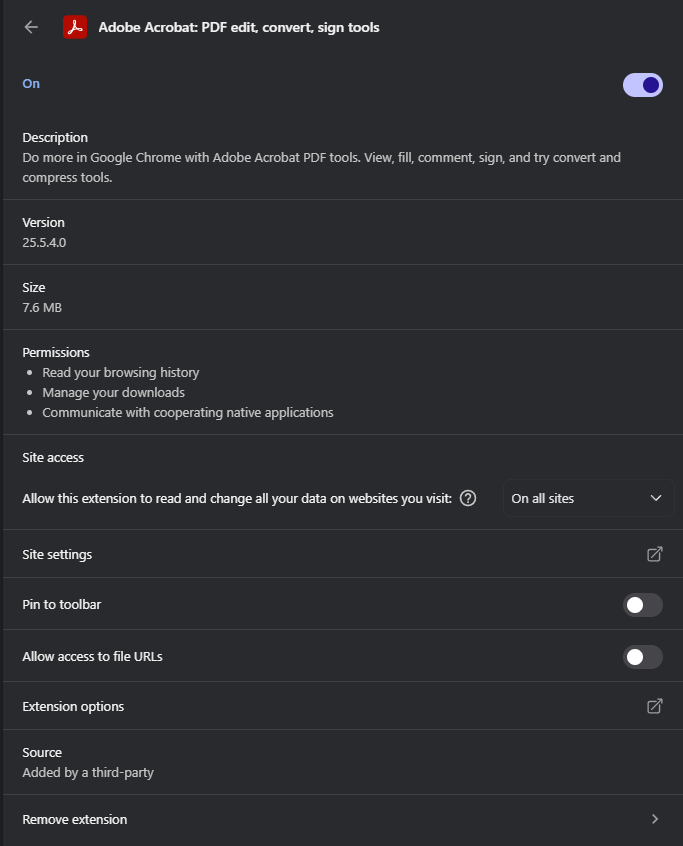


Figure 2 - Adobe Acrobat extension details with settings

A screenshot of a computer

AI-generated content may be incorrect.

Figure 3 - Adobe Acrobat extension preference via ‘extension options’

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4 - Site setting for Adobe Acrobat extension

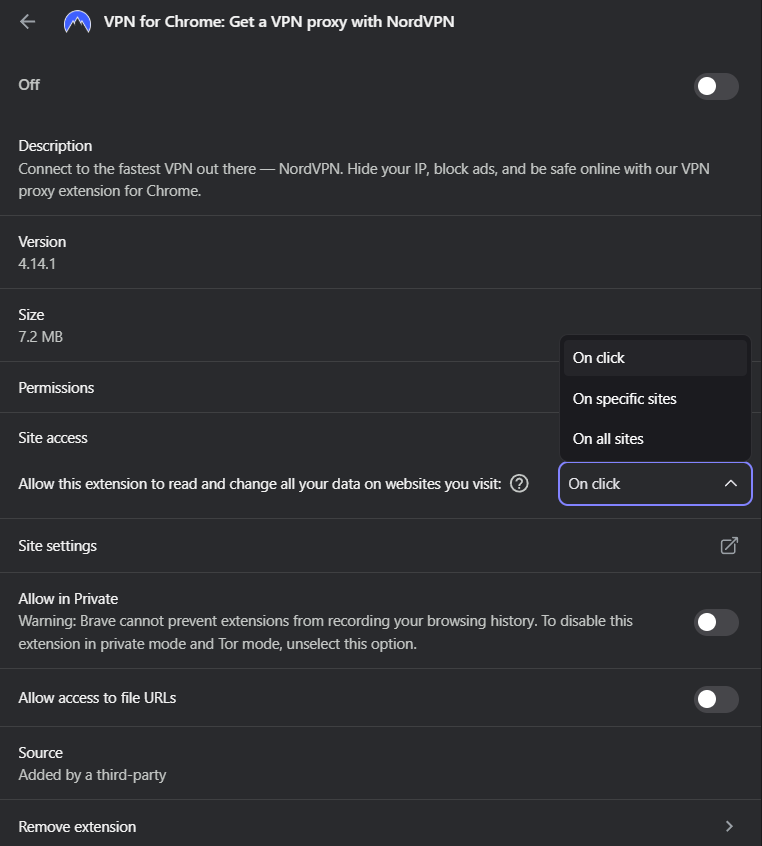


Figure 5 - VPN for Chrome extension settings with details

A screenshot of a computer

AI-generated content may be incorrect.

Figure 6 - Site Settings for VPN for Chrome

As we can see from the given extensions settings and details information are similar in some ways, but use of the extension is different. Also, site access to the extension can be configured in three ways, on click, on specific sites, on all sites. Site settings give us controls for service access on the browser i.e.: sound, camera access, file sharing, serial ports, USB devices, notifications, google auto sign-in, etc.

I have kept the browser neat and clean from multiple browser extensions. You should only download extension if it is important and can make surfing/working in web easy.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 7 - Removing unused extension

## How Malicious Browser Extensions Can Harm Users

Malicious browser extensions can significantly harm users by exploiting the wide-ranging permissions granted to extensions. Here’s a breakdown of how they can be dangerous:

### Stealing Personal and Sensitive Information

Malicious extensions can:

* Log keystrokes (keylogging): capturing everything a user types, including passwords and credit card info.
* Access cookies and session tokens, allowing attackers to hijack logged-in sessions (like your Gmail or bank account).
* Harvest autofill data, like saved names, emails, addresses, and card details.

### Spying on Browsing Activity

They can:

* Track every website you visit.
* Collect your search history.
* Monitor your interactions with pages (like clicks, scrolls, or form inputs).

This data can be sold or used to build a profile for targeted phishing or scams.

### Injecting Ads and Malware

* Ad injection: Adds unauthorized ads into legitimate websites, often leading to scam sites.
* Redirects: Force your browser to redirect to phishing or malware-hosting websites.
* Drive-by downloads: Trigger automatic downloads of malicious files.

### Impersonating Legitimate Services

* Spoof login pages to steal credentials.
* Modify content on trusted sites (like changing payment addresses on shopping sites).
* Appear as productivity or security tools but act as spyware or adware.

### Backdoor Access and Remote Control

* Connect to command-and-control (C2) servers to receive malicious instructions.
* Act as a backdoor into the system, allowing hackers to install other malware or exfiltrate data.

### Privilege Escalation

* Some extensions exploit browser bugs or user trust to escalate privileges and gain deeper access to your system or network.

### Bypassing Security Measures

* Disable browser security features (e.g., disabling Content Security Policy).
* Prevent antivirus or ad blockers from functioning.

#### Real-World Examples

* DataSpii Incident: Browser extensions leaked sensitive data from major companies.
* Fake VPN extensions: Several Chrome VPN extensions were caught harvesting user data.
* YouTube Ad Fraud: Extensions injected video ads and profited from fake views.

#### How to Protect Yourself

* Install from official stores (Chrome Web Store, Firefox Add-ons) and check reviews.
* Limit extension permissions (e.g., avoid “Read and change all your data on all websites”).
* Use as few extensions as possible.
* Regularly audit and remove unused extensions.
* Keep your browser and extensions updated.