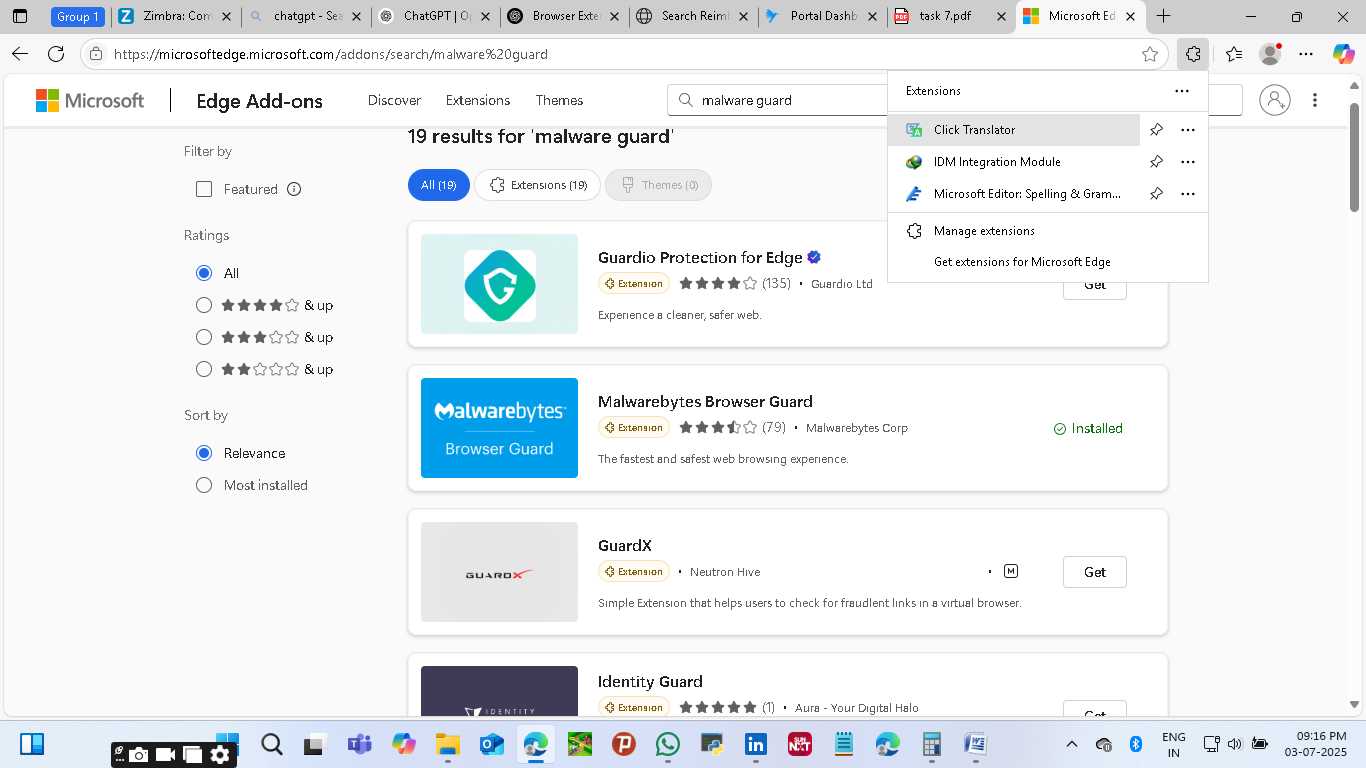
## ✅ Step-by-Step Task Execution:

**1. Open Extensions Manager**

* **Chrome**: chrome://extensions/
* **Firefox**: about:addons



## ⚠️ Known Malicious or Suspicious Extensions to Remove Immediately

2.These extensions have been flagged for harmful behavior such as:

* Injecting unwanted ads
* Tracking or stealing personal data
* Impersonating legitimate tools
* Hijacking search engines

| **Extension Name** | **Why It's Suspicious** |
| --- | --- |
| **Nord VPN Proxy (fake)** | Impersonates NordVPN; logs and leaks user data |
| **Ads Blocker** | Floods user with ads rather than blocking them |
| **CouponShark / CouponX** | Steals shopping behavior; ad injection |
| **TranslatorX** | Unnecessary access to all webpage data |
| **iZoom** | Tracks user activity under pretense of zoom functionality |
| **PDFConverterHQ** | Hijacks search engine; collects browsing history |
| **Easy PDF Combine** | Disguised browser hijacker |
| **Video Downloader Pro** | Hidden crypto miner and ad injector |
| **Maps Frontier** | Redirects to suspicious links; tied to Mindspark malware group |
| **Weather Forecast Now** | Tracks excessively; hijacks search engine |

## ✅ Genuine & Safe Browser Extensions

These are developed by trusted publishers, widely used, and have transparent privacy policies. They're safe to keep as part of a secure browser setup.

| **Extension Name** | **Publisher** | **Purpose** |
| --- | --- | --- |
| **uBlock Origin** | Raymond Hill (gorhill) | Open-source ad blocker |
| **Grammarly for Edge** | Grammarly, Inc. | Writing assistant and grammar checker |
| **LastPass / Bitwarden** | LastPass / Bitwarden | Secure password management |
| **Microsoft Editor** | Microsoft | Grammar and spell-check |
| **Office / Microsoft 365** | Microsoft | Access and edit Word, Excel, etc. |
| **Dark Reader** | Alexander Shutau | Enables dark mode on all websites |
| **HTTPS Everywhere** | Electronic Frontier Foundation (EFF) | Forces HTTPS for secure connections |
| **DuckDuckGo Privacy Essentials** | DuckDuckGo | Blocks trackers, enhances privacy |
| **Honey** | PayPal | Finds coupons and deals while shopping |

## 🔐 Why They're Safe:

* Minimal permission requirements
* Active development and regular updates
* High trust scores and transparency

## Purpose of This Checklist

The surrounding page outlines **Task 7: Identify and Remove Suspicious Browser Extensions**. Your goal is to:

* Audit all extensions
* Remove anything suspicious or unused
* Document your findings

The checklist acts as your decision-making criteria during that audit.

## What Each Point Means

| **Indicator** | **Why It Matters** |
| --- | --- |
| **Permissions** | Extensions requesting “read and change all your data on websites” could intercept sensitive data (passwords, messages, personal info). High-risk if not from a trusted source. |
| **Publisher** | Unverified or unknown publishers suggest the extension may not be properly vetted or supported—raising red flags. |
| **Reviews** | Poor ratings (especially many 1-star reviews) often include user complaints about unwanted ads, browser hijacking, or data theft. |
| **Official Website** | Trusted extensions usually have a legitimate site explaining what they do. If there's no site, it may be shady or not professionally managed. |
| **Reputation** | Searching “[extension name] malware” helps spot any cybersecurity reports or user warnings that aren’t visible in the browser store. |

### ✅ ****Conclusion for Task 7 – Identify and Remove Suspicious Browser Extensions****

Through this task, I developed a strong understanding of browser extension security. By analyzing installed extensions on Microsoft Edge, I learned how to identify potentially harmful extensions based on permissions, publisher credibility, and user reviews.

I removed any suspicious or unnecessary extensions, which not only reduced potential security threats but also improved overall browser performance. Additionally, I learned about how malicious extensions can:

* Steal user data or credentials
* Hijack search engines
* Inject ads or trackers
* Use system resources for crypto mining.