

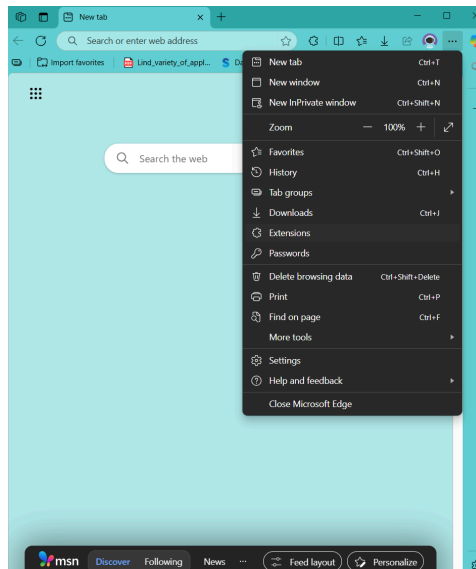
# Identify and Remove Suspicious Browser Extensions

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

## 1) Open the Extensions manager :

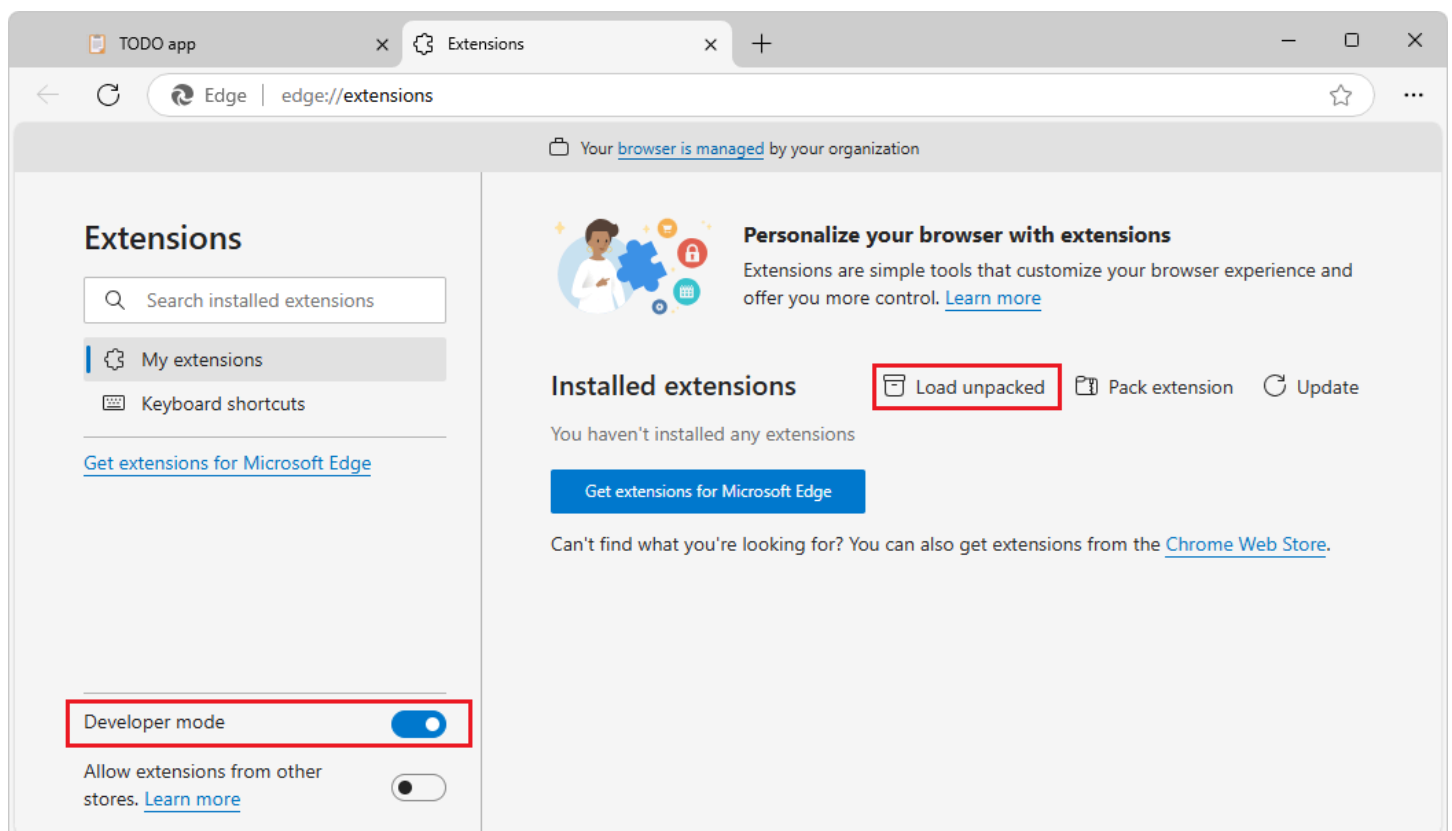
Open Edge → click the three-dot menu → Extensions → Manage extensions.

You can also type **edge://extensions** in the address bar.



## 2) Review what's installed :

On the “Extensions” tab, scan the full list. Note any you don’t recognize, don’t use, or that look outdated. Use the toggle to quickly disable one for testing.




### 3) Check permissions & reviews :

Click **Details** on an extension and look at **Permissions** and **Site access**.

Then click **Get extensions for Microsoft Edge** (store page) to read ratings, installs, and recent reviews.

A “Featured” badge on the store listing signals Microsoft’s recommended practices for security/privacy.

[← Installed extensions](#) / Office

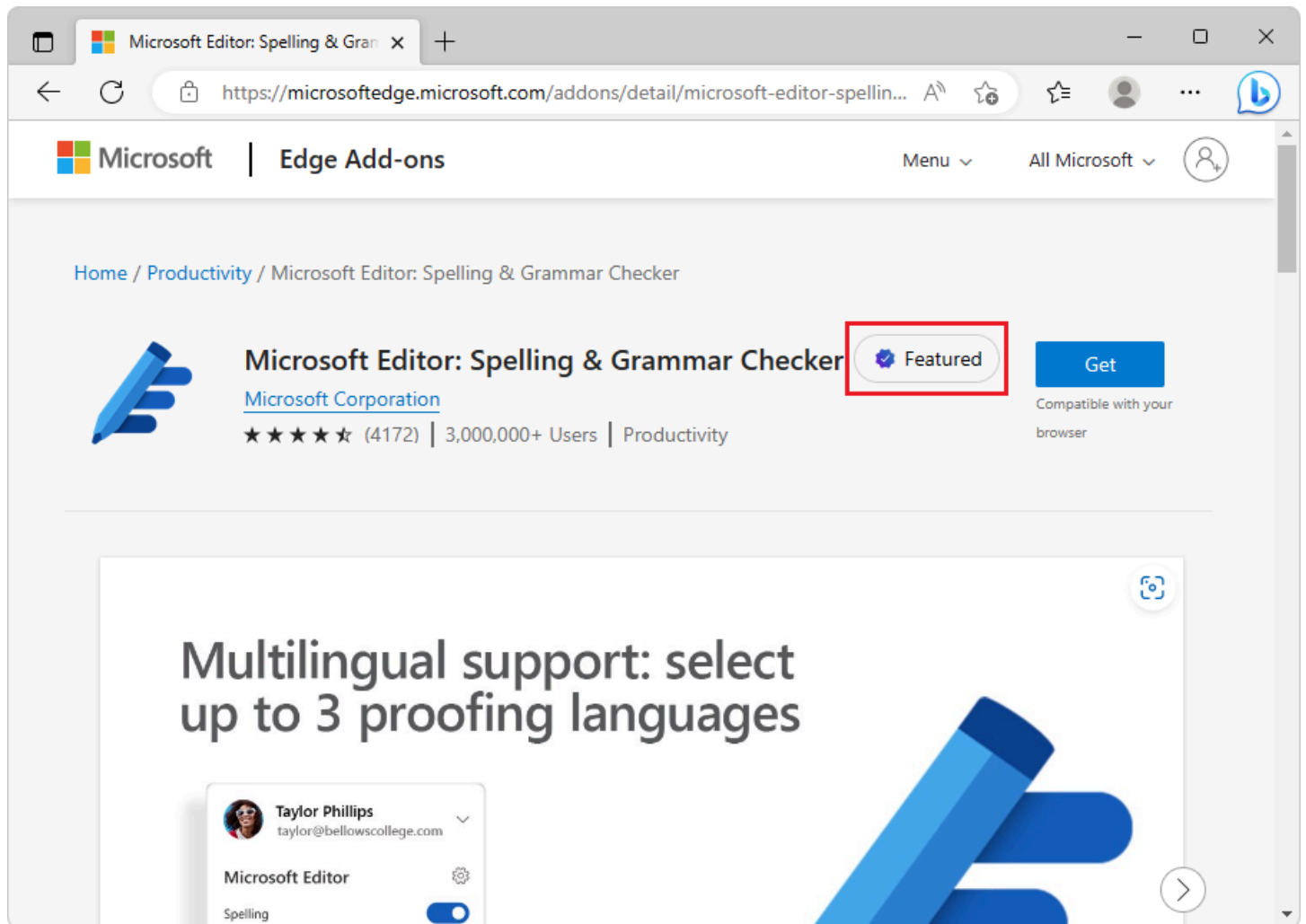


**Office**  
Size 5.1 MB Version 2.2.4

**Description**  
View, edit, and create Office documents in your browser.

**Permissions**

- Read your browsing history
- Display notifications
- Read and modify data you copy and paste
- Communicate with cooperating native applications



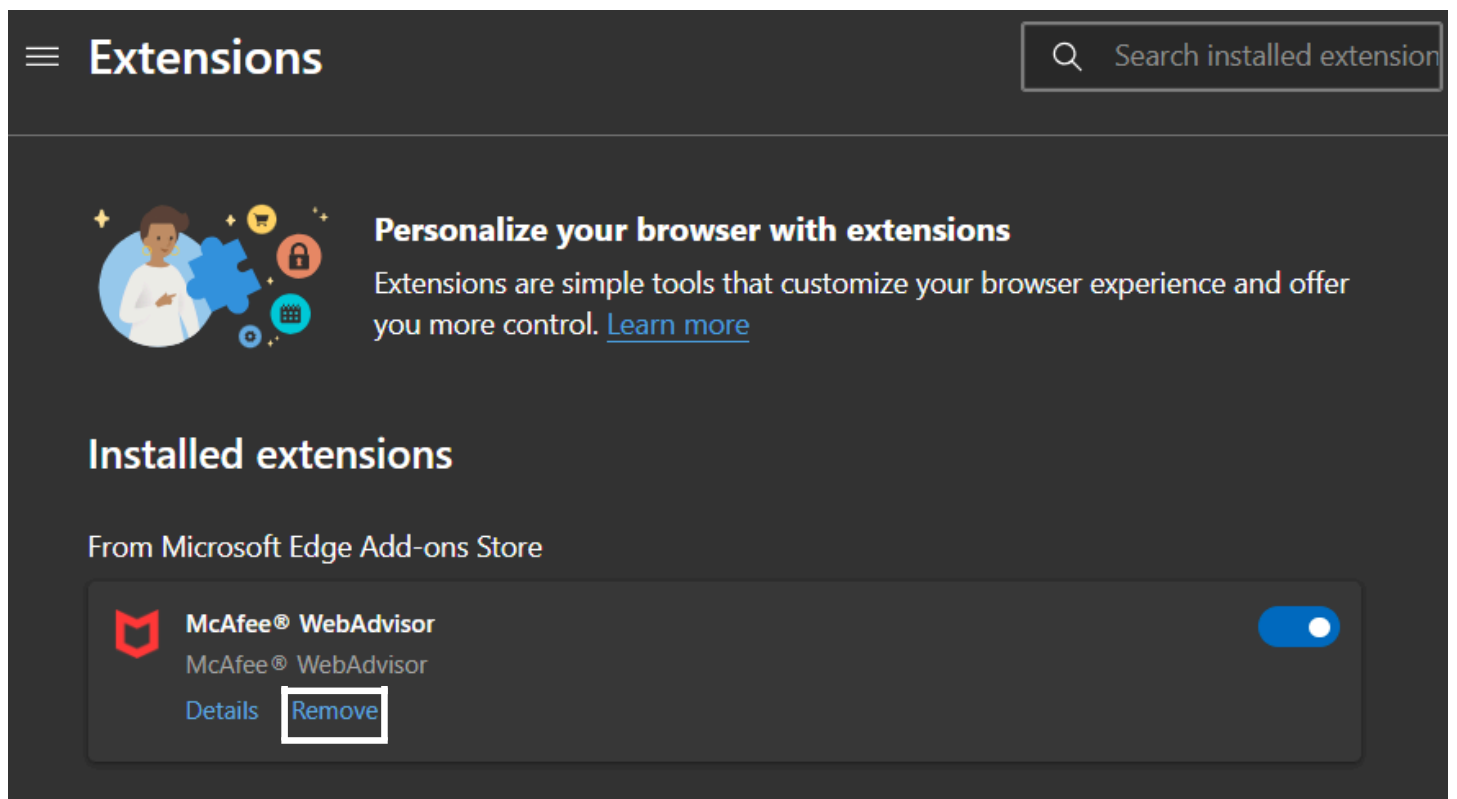
#### 4) Identify unused or suspicious items:

Flag extensions you haven't used in a month, ones asking for broad access like "Read and change all your data on all websites," or those with poor/negative recent reviews.

(Host/device permissions let extensions view/modify sites or interact with your device—treat broadly-scoped ones cautiously.)

#### 5) Remove what you don't need :

Method A: right-click the extension's toolbar icon → **Remove from Microsoft Edge** → **Remove**.



Method B: at **edge://extensions**, click **Remove** under the item → **Remove**. You'll see a brief "Extension removed" confirmation.

## 6) Restart Edge & check performance:

Close all Edge windows and reopen. Browse normally and see if page loads feel snappier and if CPU/RAM use drops.

## 7) Research: How Malicious Extensions Harm Users:

### 1. Data Theft & Privacy Invasion

- **What happens:** Malicious extensions can read everything on the web pages you visit if given broad permissions like *"Read and change all your data on the websites you visit"*.
- **Risks:**
  - Stealing login credentials (usernames & passwords).
  - Collecting browsing history, cookies, and personal info (names, addresses, phone numbers).
  - Selling data to advertisers or cybercriminals.

### 2. Ad Injection & Redirects

- **What happens:** The extension modifies web pages to show extra ads or redirect you to specific websites.
- **Risks:**
  - Unwanted pop-ups or banners.
  - Links to phishing sites.
  - Slower browsing experience due to extra scripts.

### 3. Account Hijacking

- **What happens:** Some extensions capture your active login sessions through cookies or tokens.
- **Risks:**
  - Attackers log in to your accounts without needing your password.
  - Identity theft or financial fraud.

### 4. Malware Delivery

- **What happens:** An extension downloads malicious files or injects harmful code into websites you visit.
- **Risks:**
  - Installation of ransomware, spyware, or keyloggers.
  - Exploitation of system vulnerabilities for deeper access.

### 5. Browser Manipulation

- **What happens:** Extensions can change browser settings without permission, like altering your homepage or default search engine.
- **Risks:**
  - Search results are hijacked for ad revenue.
  - Trusted pages replaced with lookalike phishing sites.

### 6. Persistent Surveillance

- **What happens:** Malicious extensions remain active in the background, even if you rarely use them.
- **Risks:**
  - Continuous tracking of online behavior.
  - Building a detailed profile of your interests, habits, and connections.