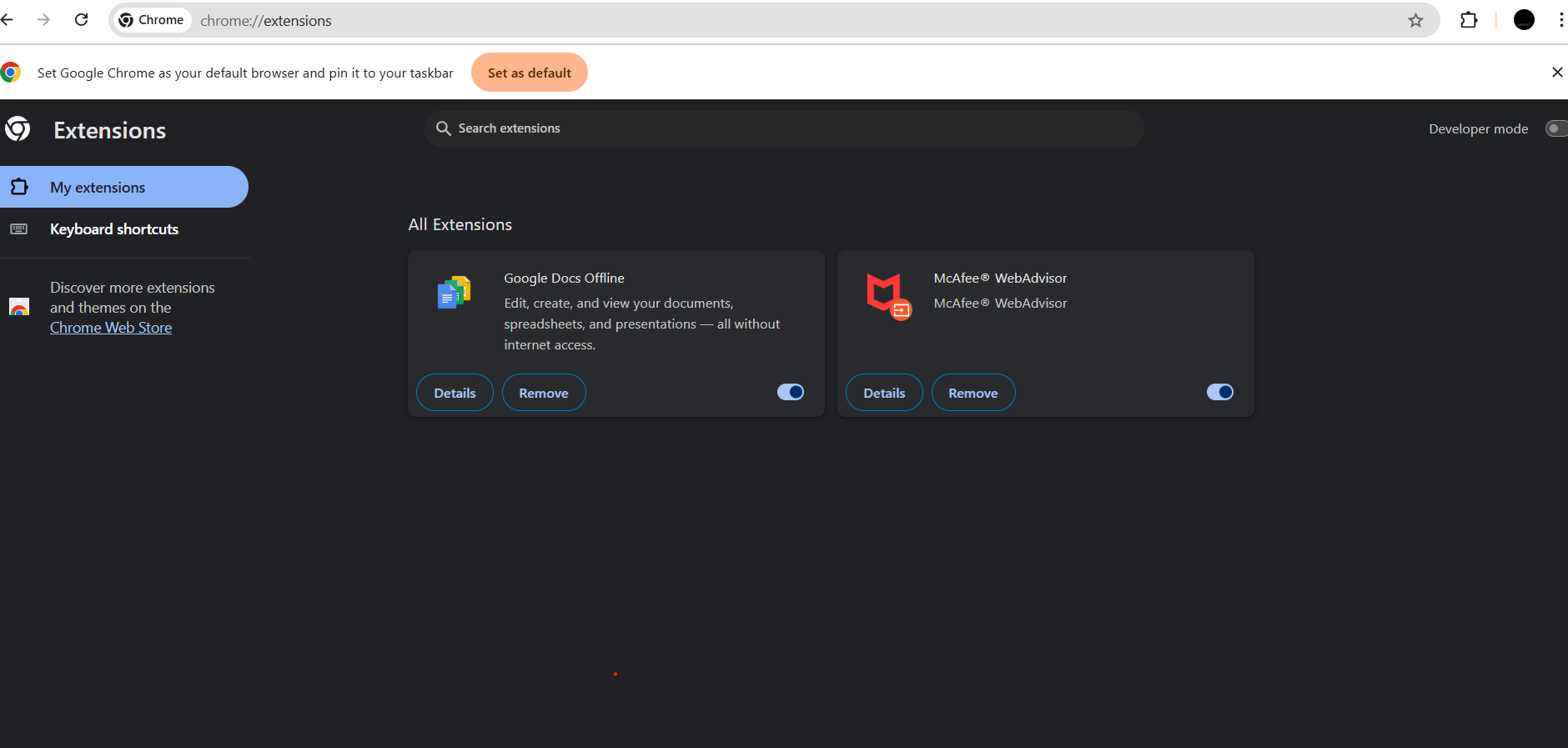
STEP 1:OPEN AND INSTALL BROWSER OR FIREFOX FROM THE WINOWS

STEP 2:Now Open your browser’s extension/add-ons manager.



##GO TO EXTENSIONS AND NEXT CLICK ON MANAGE EXTENSION AFTER CLICKING 3 DOTS ON THE CORNER.

STEP 3:AFTER YOU FOUND A SUSPICIOUS EXTENSIONS YOU CAN GO AND EASILY REMOVED FROM THE EXTENSIONS AND MANAGE YOU PC/LAPTOPS FROM ANY SUSPICIOUS ACTIVITY.

A screenshot of a computer

AI-generated content may be incorrect.

##THERE IS AN REMOVE EXTENSION THAT WE CAN REMOVE FROM YOUR PC.

STEP 4:REMOVE ALL UNWANTED EXTENSION FORM YOUR EDGE DEVICE AN ANY UNWANTED MALWARE CAN BE ATTACHED IN THE EXTENSION.

##HOW TO DETECT SUSPICIOUS EXTENSION

* **Name & Publisher** — does the publisher look legitimate? (e.g., a company name or a known developer)
* **Description & Version** — short description should match expected behavior.
* **Install date / last updated** — frequent updates by a known developer are normal; a suspicious extension may have a vague description and little/no updates.
* **Permissions summary** — often shown on the extension card or in **Details**.

**Store page / reviews** — click “Details” → click the extension name to open its store page and read reviews.

STEP 5: **Remove suspicious or unnecessary extensions**

**Safe removal steps**

1. On the extension’s entry: click **Remove** (Chrome)
2. If the browser offers to keep data/settings, choose **delete** if you suspect malicious behavior.
3. Restart the browser.

**If “Remove” is disabled / extension reappears**

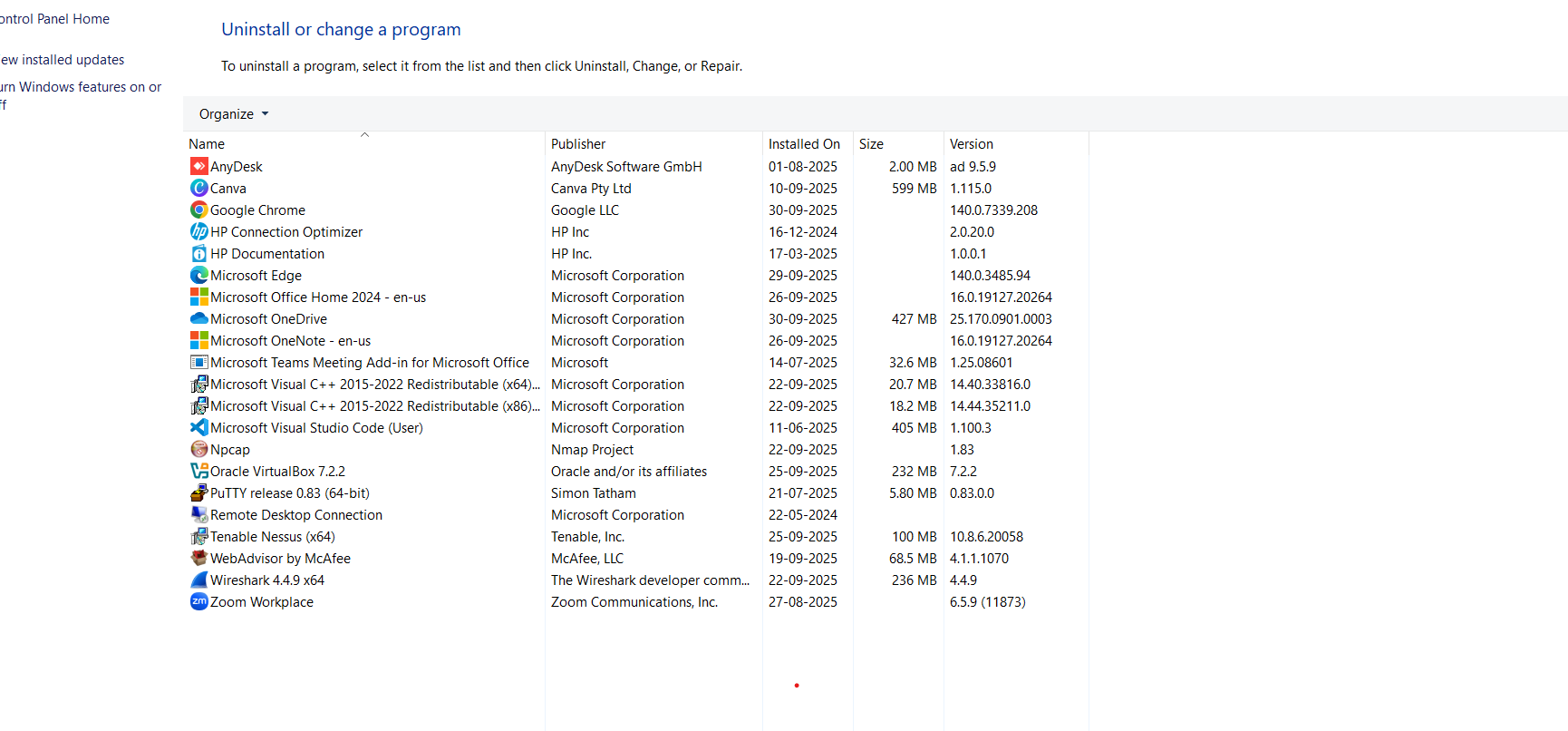
* The extension might be installed by external software or an enterprise policy:

**Windows:** check **Programs & Features** (Control Panel) for recently installed programs that might have bundled the extension and uninstall them.

* Run an anti-malware scan (see next section) to remove helpers that reinstall the extension.

**Reporting**

* After removing, go to the extension’s store page and use **Report abuse** / **Report this add-on** (store option) to notify the browser vendor.



I THINK ALL HAVE PROPER PUBLISER NAME AND ALL ARE SAFE EXTENSIONS THERE IS NO SUSPICIOUS EXTENSIONS IS FOUND.

**##Research how malicious extensions can harm users**

**Common malicious behaviors & technical mechanisms**

* **Ad injection / popups** — inject ads or trackers into pages; revenue generation for attacker.
* **Search hijacking / redirects** — change default search engine or redirect to affiliate sites.
* **Data exfiltration** — read page content and send it to remote servers (can capture form data).
* **Credential theft / session hijacking** — steal cookies or modify pages (man-in-the-browser) to intercept login credentials or alter transactions.
* **Keylogging / form capture** — capture keystrokes or form submissions.
* **Cryptomining** — run JavaScript miners in the background using your CPU.
* **Tracking & fingerprinting** — collect browsing behavior across sites to build profiles and sell them.
* **Supply-chain takeover** — legitimate extension maintained properly can be sold or its update channel hijacked; a benign extension can become malicious via an update.
* **Persistence tricks** — install companion apps or modify system settings so the extension reappears after removal.

**##steps taken and extensions removed (detailed template)**

Below is a robust template. Use this in Word/Excel or copy into a report.

**Header**

* **Report Title:** Browser Extension Audit
* **Auditor:** [Your name]
* **Date & Time:** [YYYY-MM-DD HH:MM, timezone]
* **Browser / Version:** e.g., Chrome 117.0.5938.132
* **OS:** e.g., Windows 11

**Summary (short)**

* Quick summary line: number of suspicious extensions found, high-level actions taken.

**Detailed table of extensions reviewed**

| **#** | **Extension Name** | **Publisher** | **Version** | **Installed On** | **Permissions** | **Why flagged?** | **Action taken** | **Removed (Y/N)** | **Notes / Evidence (screenshots, store link)** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Fast Coupon Finder | Unknown | 1.0.3 | 2025-09-10 | Read/Change all site data | Injected ads; user didn't install | Removed (chrome://extensions → Remove) | Y | Screenshot (before), store link, 1-star reviews noted |
| 2 | Awesome Theme | Theme Co. | 2.1.0 | 2024-02-05 | Not required but had full site access | Unused for >6 months | Disabled (kept for testing) |  |  |