Published on *University of Colorado* (https://www.cu.edu)

Avoid fake browser update scams [1]

July 8, 2024 by ES and UIS Communications [2]

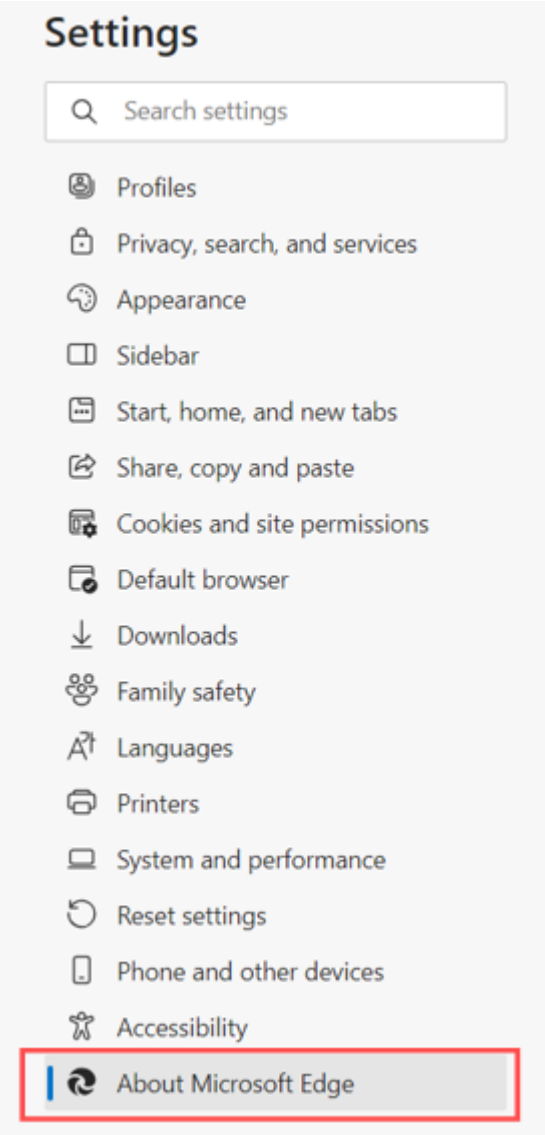
Be cautious if you ever receive an online pop-up urging you to update your browser or any software. It is likely an update scam. These scams often include a link to update your browser, which tricks you into downloading malware. You should never use a link from a browser pop-up to update your browser. Instead, close any window with a potentially malicious pop-up and follow these steps to update your browser.

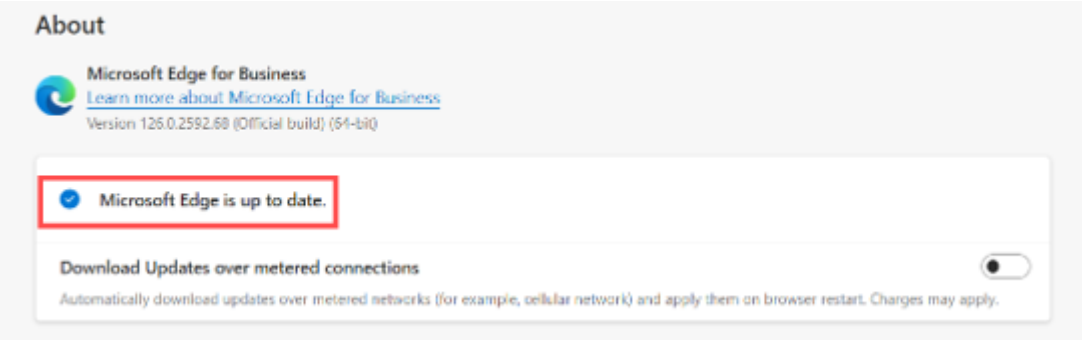
Microsoft Edge

Edge works seamlessly with OneDrive. It will automatically check for updates and apply them when you restart the web browser. However, many users rarely close all browser windows.

1. In Edge, click the three horizontal dots in the top right corner.
2. In the popup menu, click **Settings**.
3. Under Settings, click **About Microsoft Edge**

.



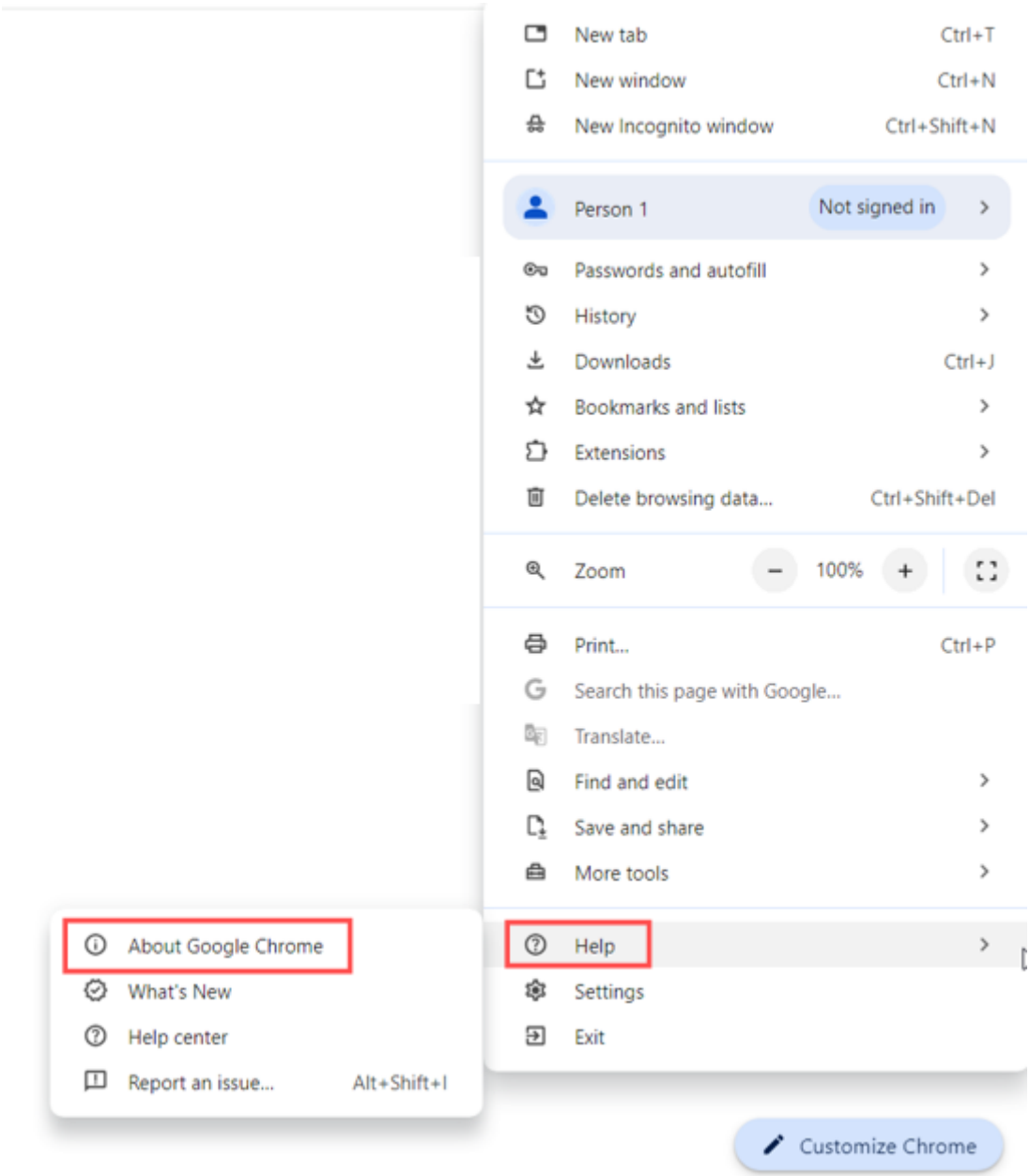


4. The About page shows whether Edge is up-to-date. If it shows an update is available, select **Download** and proceed to install.

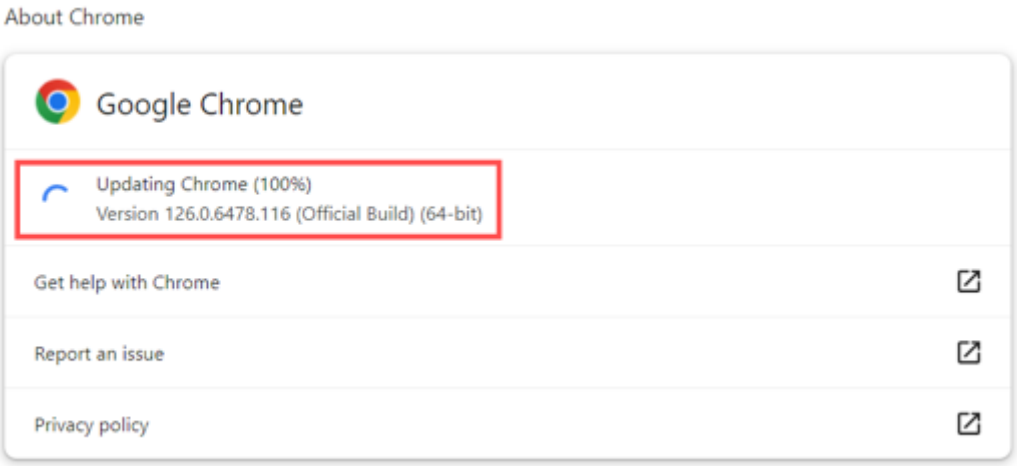
Google Chrome

1. In Chrome, select the three vertical dots on the far right of the taskbar.
    - If your Chrome version is outdated or has a pending update that needs your attention, the word “Update” will appear alongside the three vertical dots.
2. Select **Help** from the dropdown menu, then select **About Google Chrome**

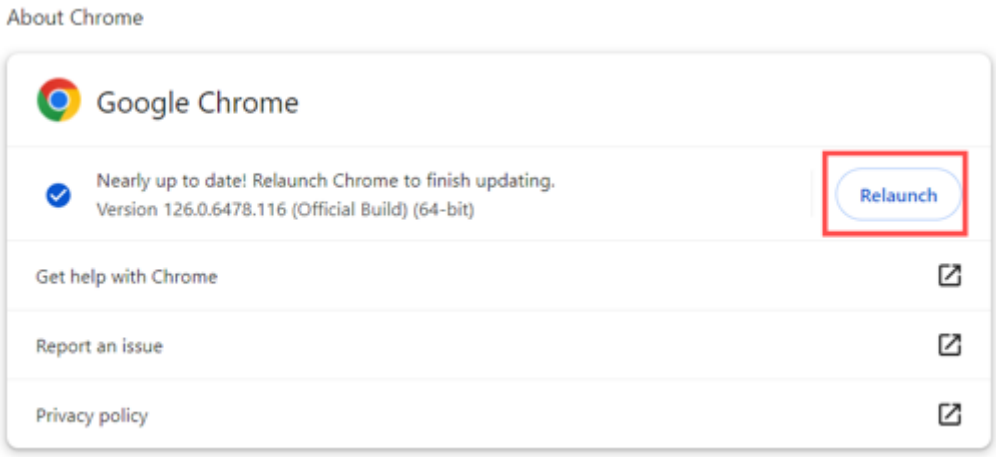
.



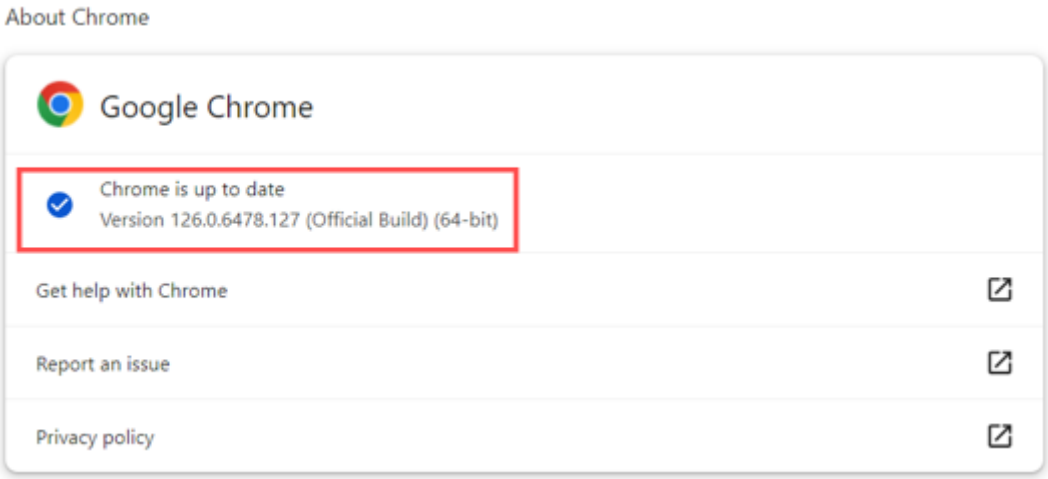
3. Chrome will begin to update automatically if your version is not up-to-date.



4. Once the updated version has finished installing, press **Relaunch** to finalize the update process.



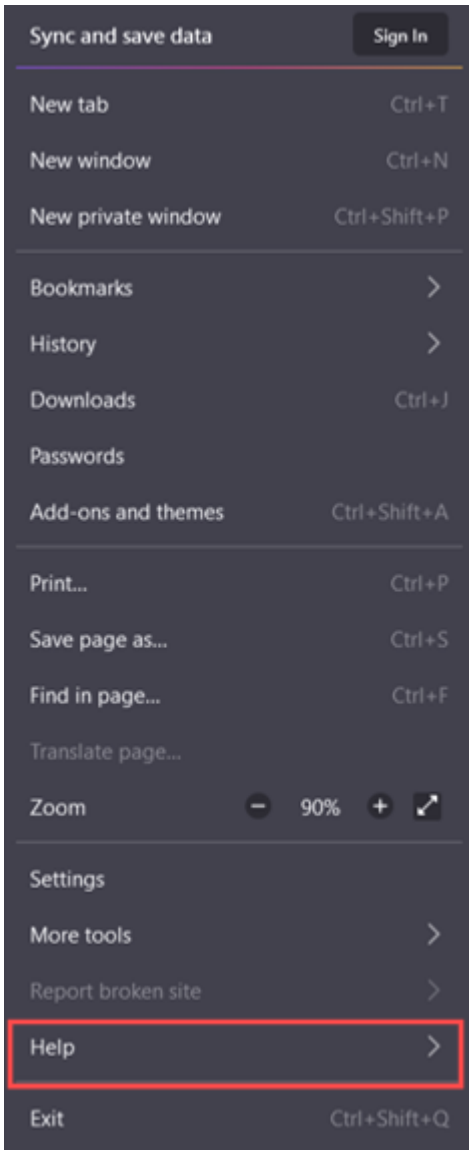
5. The About Chrome section will now reflect the up-to-date version.



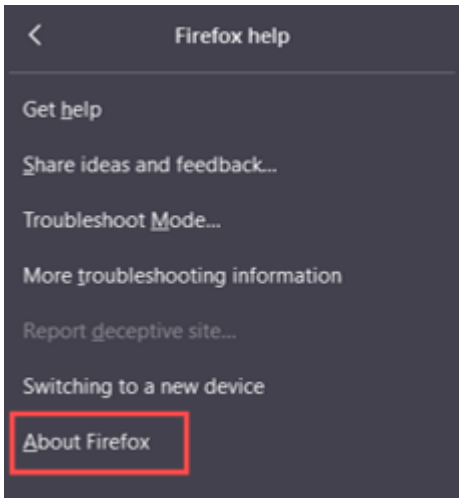
Firefox

1. In Firefox, select the three horizontal dots on the far right of the taskbar.
2. Select **Help**

.



3. Select **About Firefox**.



4. If your version of Firefox is outdated, it will update automatically. Click **Restart to Update Firefox**

to finalize the update.

Safari

1. Open **App Store**.
2. Navigate to the **Updates** section.
3. Check for available Safari updates.

Oh no, I opened a suspicious link or attachment! Now what?

Immediately report it as a possible incident. Reporting it immediately allows the information security team to act quickly, determine the level of impact and contain the incident. Visit the Report an Incident web page [3] to learn more.

Information security incidents can happen to anyone. No retaliation will be taken against anyone who, in good faith, reports a possible information security incident.

You can learn more about phishing scams from the Office of Information Security [4].

cybersecurity [5], computer help [6]
Display Title:
Avoid fake browser update scams
Send email when Published:
No

Source URL:https://www.cu.edu/blog/tech-tips/avoid-fake-browser-update-scams

Links
[1] https://www.cu.edu/blog/tech-tips/avoid-fake-browser-update-scams [2] https://www.cu.edu/blog/tech-tips/author/110439 [3] https://www.cu.edu/security/reporting-incident
[4] https://www.cu.edu/security/awareness/phishing-scams-faqs [5] https://www.cu.edu/blog/tech-tips/tag/cybersecurity [6] https://www.cu.edu/blog/tech-tips/tag/computer-help