6 ways to ensure Chrome extensions are safe

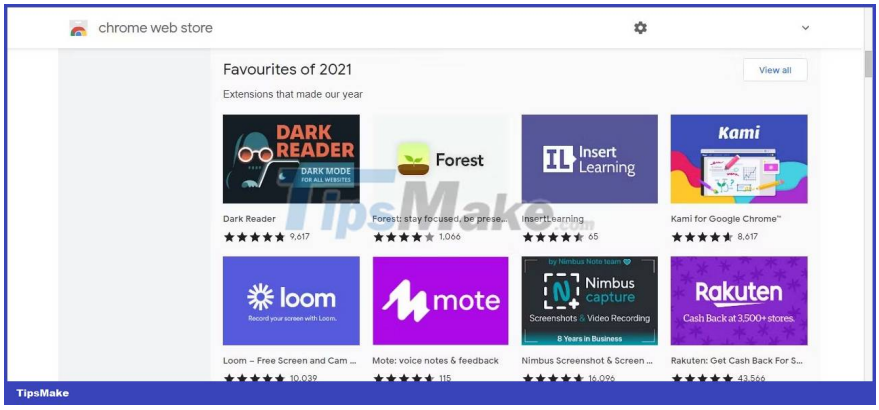
Choosing Chrome extensions carefully is important, so here are the best ways to make sure your Chrome extensions are safe.

Most Chrome extensions are safe to use, but malicious extensions with broad permissions can access the content of the websites you view, copy session tokens, or even access your payment information. Friend.

Choosing Chrome extensions carefully is important, so here are the best ways to make sure your Chrome extensions are safe.

6 ways to ensure Chrome extensions are safe

1. Use Chrome Web Store



The safest way is to use the Chrome Web Store, which is the safest place to install Chrome extensions. According to Chome Stats, the Chrome Web Store has more than 125,000 extensions and web apps. Whether you're looking for a password manager or an extension to enhance your creativity, you can find something suitable.

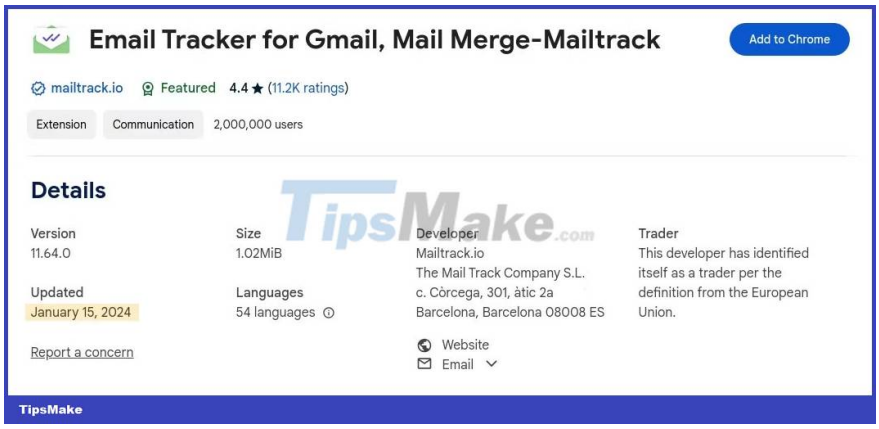
The main drawback of using the Chrome Web Store is that there will still be shady Google Chrome extensions that you should not install. And so, you should still verify the reliability of the extension before installing it. The advantage is that if you accidentally download a malicious Chrome extension and Google removes it, you will be notified and the extension will be disabled on your machine.

2. Research the developer

Before installing an extension, research the developer's legitimacy. To help you differentiate between a professional developer and a security risk, check whether the developer has a full website or a public profile. If you trust the developer, you can ensure that the Chrome extension you're downloading is legitimate by downloading it directly from their website.

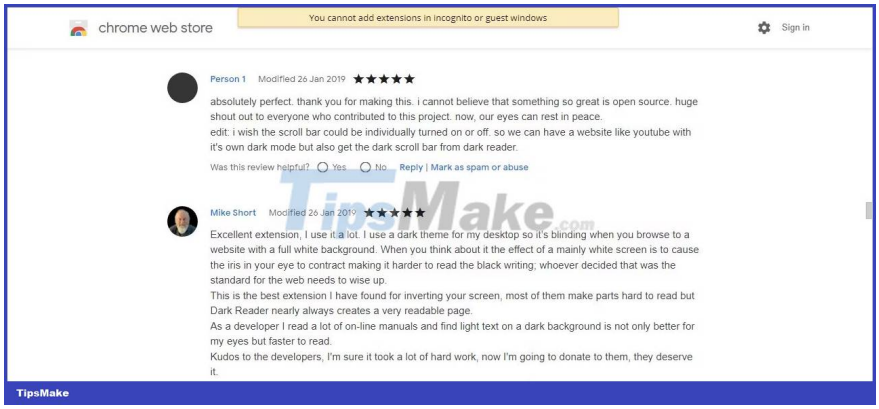
The only drawback is that some developers create malicious extensions months or years after initially releasing them or discovering compromised accounts and adding malicious code. Trust your intuition and use a different browser extension if something doesn't seem right.

3. Make sure extensions are updated regularly



You should also make sure the extension is regularly updated before installing it. If an extension is out of date, it is less secure than an updated extension. There is no point in using an extension if it contains vulnerabilities that put your browsing at risk.

4. Check reviews



Reviews are the best companion! Checking reviews from people who have used the browser extension will help you better understand the service based on other people's experiences. You can also evaluate the average user experience and whether they consider the Chrome extension safe.

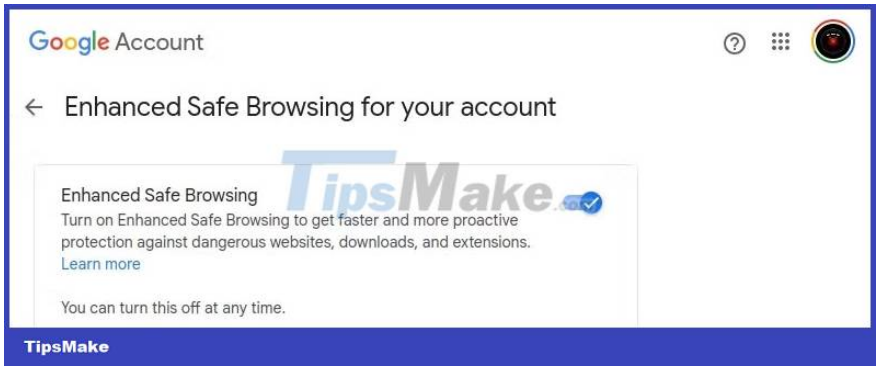
If the majority of reviews are negative, look for a similar extension with more positive reviews. You can read reviews of Google Chrome add-ons on the Chrome Web Store.

5. Regularly perform virus scans

With reliable antivirus software, you can monitor everything that enters your browser. Known malicious Chrome extensions, PUPs (Potentially Unwanted Programs), and any unknown but recognizable malicious internal or network activity will be detected by a reputable antivirus program such as Bitdefender or Malwarebytes.

However, antivirus software can only do so much to protect you online, and Chrome viruses and PUPs will always try to stay undetected for as long as possible. To avoid overwhelming your browser with too many extensions, only install the ones you really need.

6. Use Chrome's Enhanced Safe Browsing feature and surf the web safely



You may consider using Chrome's Enhanced Safe Browsing feature to protect yourself from malicious browser extensions. Enhanced Safe Browsing is a powerful browsing mode that essentially acts as an antivirus for your browser and protects you from dangerous downloads, extensions, and websites. You can enable Chrome Enhanced Safe Browsing by visiting your Google account settings at Security > Manage Enhanced Safe Browsing > Enhanced Safe Browsing.

4 signs that Chrome extensions are malicious

If you're particularly tech-savvy, you can help keep yourself safe in your digital world by investigating the Chrome extensions you use. You can start with methods like checking extension permissions, checking network traces, and using Chrome Extension Source Viewer.

1. Check the extension in CRXcavator

CRXcavator evaluates Firefox, Edge, and Chrome extensions and calculates risk scores based on factors like weak security policies and excessive permissions. By searching for an extension using CRXcavator (or entering the extension ID from the URL - a string of letters or numbers), you can see reports about the extension and make an informed decision about whether to download that extension or not.

2. Review the Chrome extension's permissions

CRXcavator provides great insight into the reliability of Google Chrome add-ons, but it's only useful depending on the context. Once you know what permissions your web browser requires, you should consider whether it

reasonably needs that permission. Despite the risks, the Chrome password manager extension will need to have access to the website's content and fill out forms. Those same permissions would not make sense for a weather browser extension.

3. Check network footprint in developer tools

In addition to CRXcavator, you can gain incredible insight into whether a Google Chrome add-on is malicious by monitoring its network activity. You can get more information about your network activity by logging a network trace file through your browser, as IBM explains.

4. Use Chrome Extension Source Viewer

You can best know the functionality of your browser extension by analyzing the source code generated by Chrome Extension Source Viewer. Analyzing source code is undeniably a difficult task, but your chances of success will improve if you understand how to create browser extensions.

Chrome extensions are convenient because they can make online browsing much easier, but it's also important to make sure that all Chrome extensions you install are safe to use.