

Warning about fake Google Chrome on the rise: How to detect it?

Google Chrome's fake alerts are becoming increasingly sophisticated, tricking users into running malicious scripts that compromise their systems.

Here's how these fake alerts work and what you can do to protect yourself.

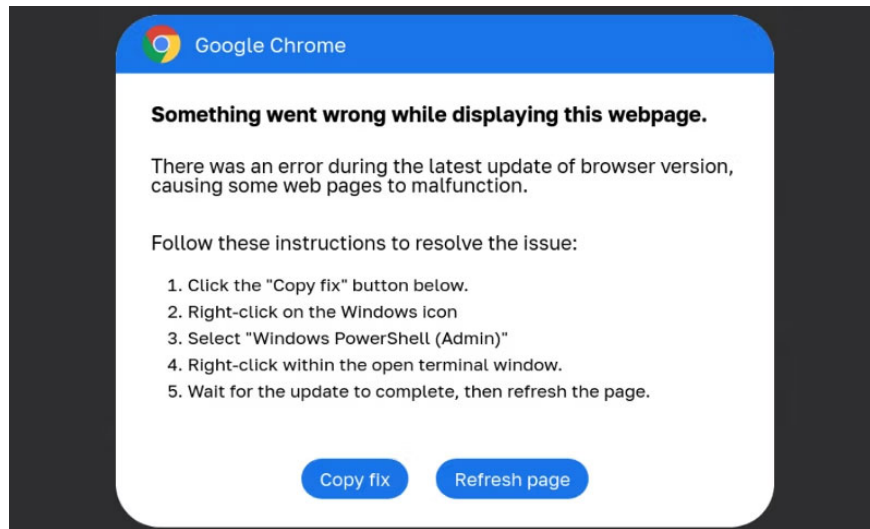
What is a fake Google Chrome warning? How do they work?

Google Chrome fake alerts are phishing notifications that mimic legitimate system notifications. Their main goal is to trick users into executing harmful commands.

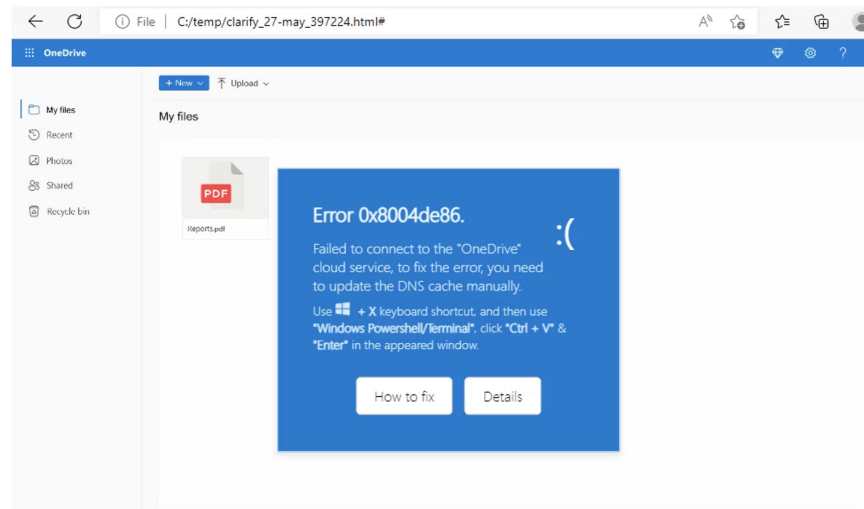
These warnings often appear as:

1. **System Error** : The message indicates that there is a serious system error that needs to be resolved immediately.
2. **Update notification** : A warning that the browser or other software is out of date and needs an urgent update.
3. **Virus alerts** : Fake alerts claiming that the device is infected with a virus and needs immediate scanning or repair.

Google Chrome's fake alerts use a number of different methods, suggesting different hacking groups use similar methods. For example, according to Proofpoint, the ClearFake attack uses a series of compromised websites and blockchain scripts to infect devices, while the ClickFix variant uses compromised websites and iframes to inject malware into the machine. Similarly, another attack uses malicious HTML attachments and fake error messages to trick you into copying dangerous commands and compromising your machine.



In each attack, users are prompted to open Windows PowerShell and copy and paste the code provided by the fake alert. As you might guess, if that happens, additional malware will be downloaded and installed on the device, leading to data theft, malware, and ransomware like DarkGate, Vidar Stealer, Matanbuchus and NetSupport. Furthermore, while Google Chrome phishing alerts are a serious problem, ProofPoint also noted phishing alerts in Microsoft Word and other Office programs, along with Outlook.



How to detect fake Google Chrome warnings

Google Chrome's fake alerts are convincing but there are a few ways you can try and detect them:

1. **Suspicious requests** : If the warning window makes unusual requests, such as running a PowerShell script or installing a root certificate, it's a clear sign of an infection. For example, Proofpoint has observed attacks where users were tricked into copying and pasting malicious scripts into PowerShell, leading to malware installation.
2. **Unexpected pop-ups** : Genuine Google Chrome warnings do not appear suddenly. So be wary of unexpected Chrome pop-ups, especially those that call for immediate action.
3. **Grammar and spelling errors** : Fake alerts often contain grammatical errors, which are rare in legitimate notifications. However, the advent of AI means that spelling and grammar errors in malware are

decreasing.

4. **Strange URLs** : Chrome phishing warnings often contain strange URLs. And in most cases, the URL is insecure, meaning it uses HTTP instead of HTTPS.
5. **Deals too good to be true**: Suspicious Chrome warnings can often claim to offer free software, such as malware removal tools.

Detecting a fake Google Chrome warning is surprisingly similar to detecting a phishing site and often leads to the same problems!

How to protect yourself from Google Chrome's fake alerts

You can also proactively defend against Google Chrome phishing warnings and other types of phishing and malware by taking these steps:

1. **Avoid scare tactics** : Fake warnings often use urgent language and scare tactics to prompt immediate action. So always take a moment to evaluate the warning before responding.
2. **Cross-check with Google** : Search for a warning message online to see if it's reported as legitimate. If you can't find it anywhere online, that's another warning sign.
3. **Use browser security features** : Turn on browser security features, such as enhanced safe browsing mode, to help protect against malicious websites and downloads.
4. **Avoid clicking on suspicious attachments** : Be cautious of links and attachments included in Chrome's suspicious warnings. These can often lead to malicious websites or trigger downloads of harmful software.
5. **Keep your software up to date** : Regularly update your browser and other software to ensure you have the latest security patches.

It's not always easy to spot a Chrome malicious warning (or any other warning for that matter). They are designed to be as realistic as possible. Otherwise, they will not be effective. But by taking a moment to double-check every warning, you can save yourself a lot of trouble later.

You finished reading the article "**Warning about fake Google Chrome on the rise: How to detect it?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.