

How to Bypass the HTTPS Warning for Self-Signed SSL/TLS Certificates

Learn how to safely bypass HTTPS warnings for self-signed SSL/TLS certificates with step-by-step instructions for different browsers and security considerations.

Contents

01	Introduction	3
02	Firefox	3
03	Safari	4
04	Chrome	6
05	Brave	8
06	Edge	9
07	Opera	9
08	History	10

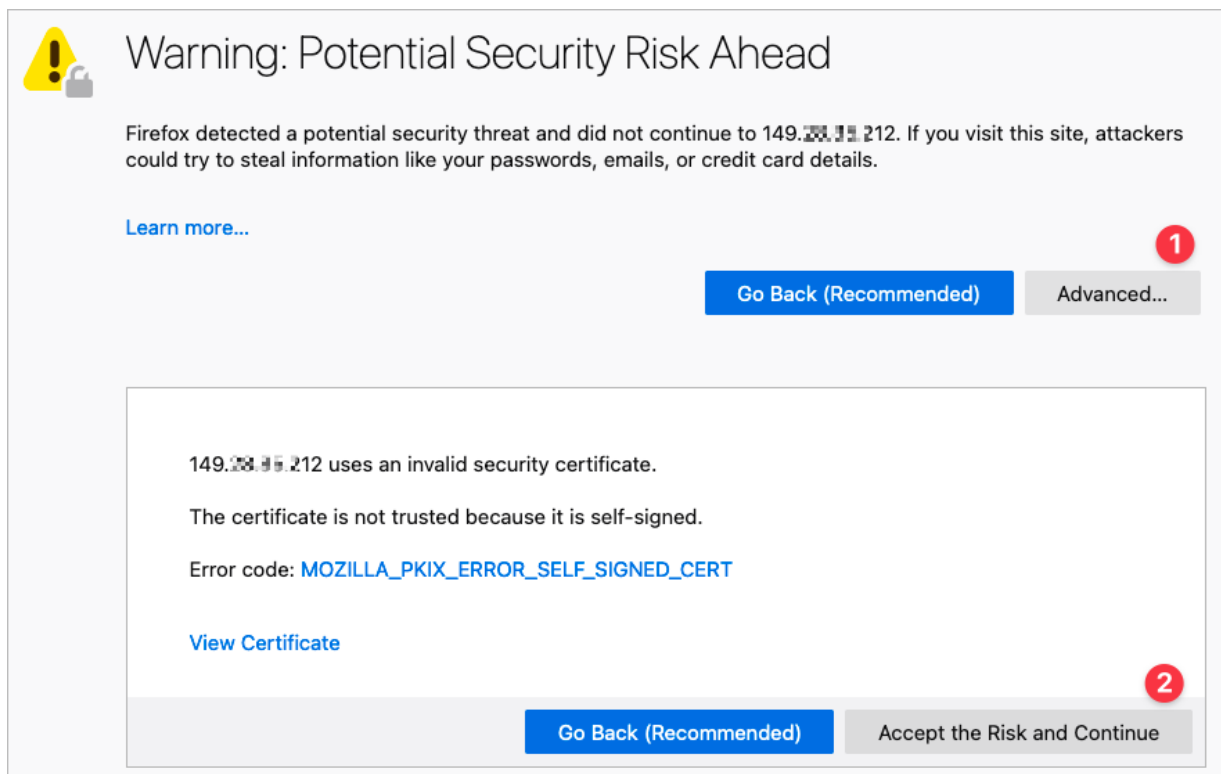
Introduction

Many applications, including some Vultr [One-Click apps](#) deploy with self-signed TLS/SSL certificates to protect your traffic when performing the initial configuration. When you connect, you may encounter a browser warning. This guide explains how to move past the browser warning and connect to the site.

Firefox

Firefox has the most straightforward warning screen to navigate.

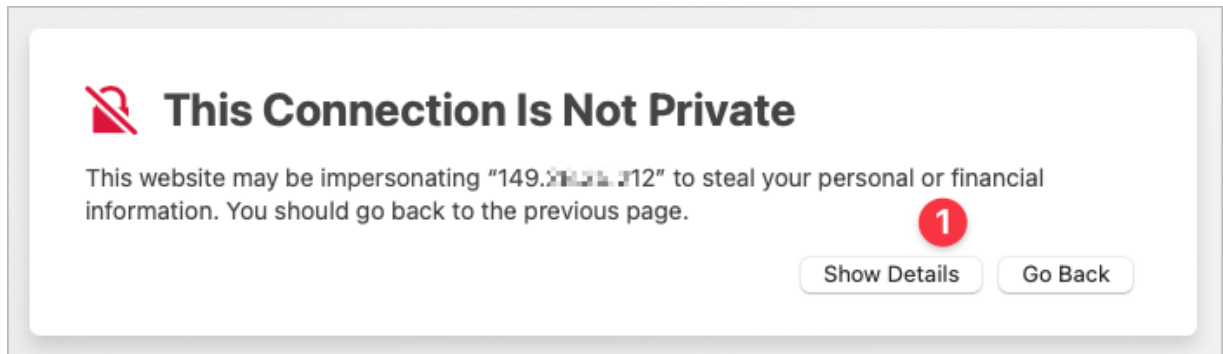
1. Click the **Advanced** button.
2. Click **Accept the Risk and Continue**.



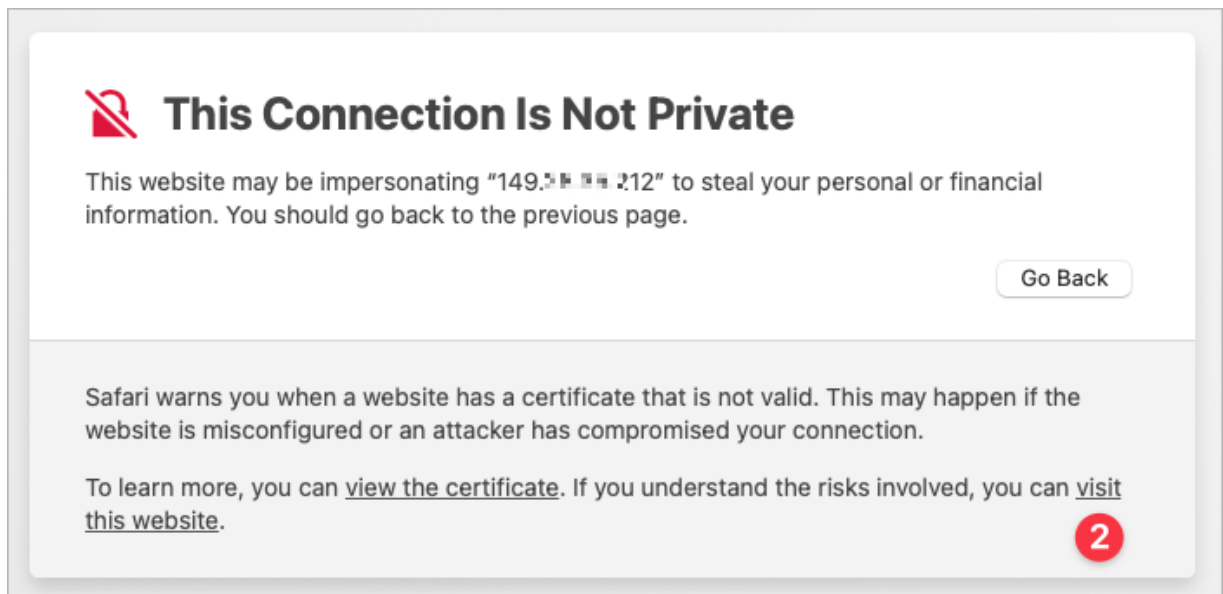
Safari

You can bypass the security warning in Safari with a few mouse clicks.

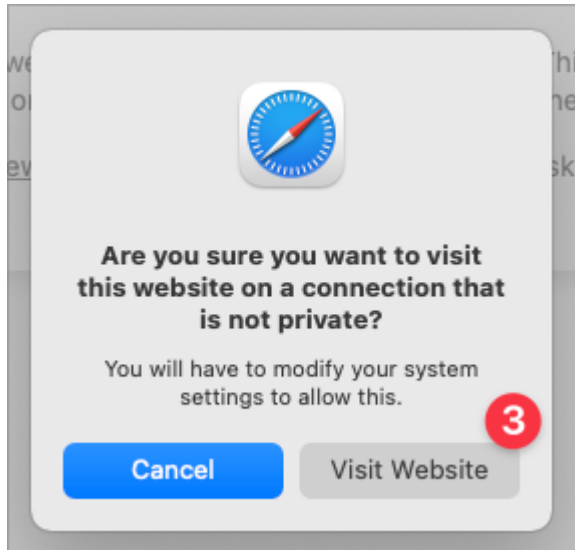
1. You'll see a dialog titled **This Connection Is Not Private**. Click **Show Details** to expand the dialog.



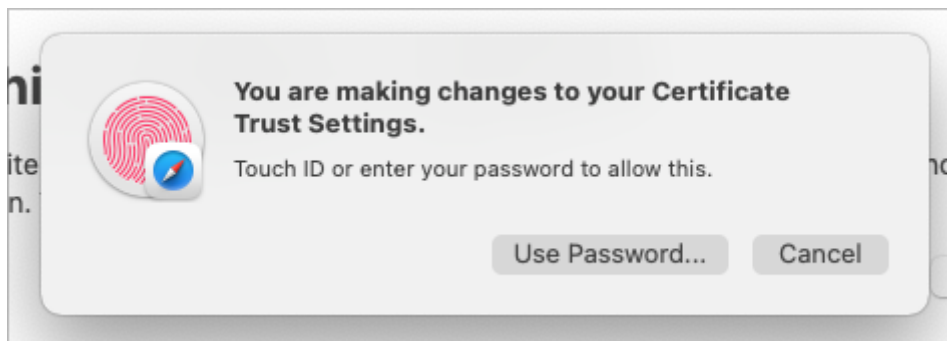
2. Click the **visit this website** link.



3. A new dialog appears. Click **Visit Website**.

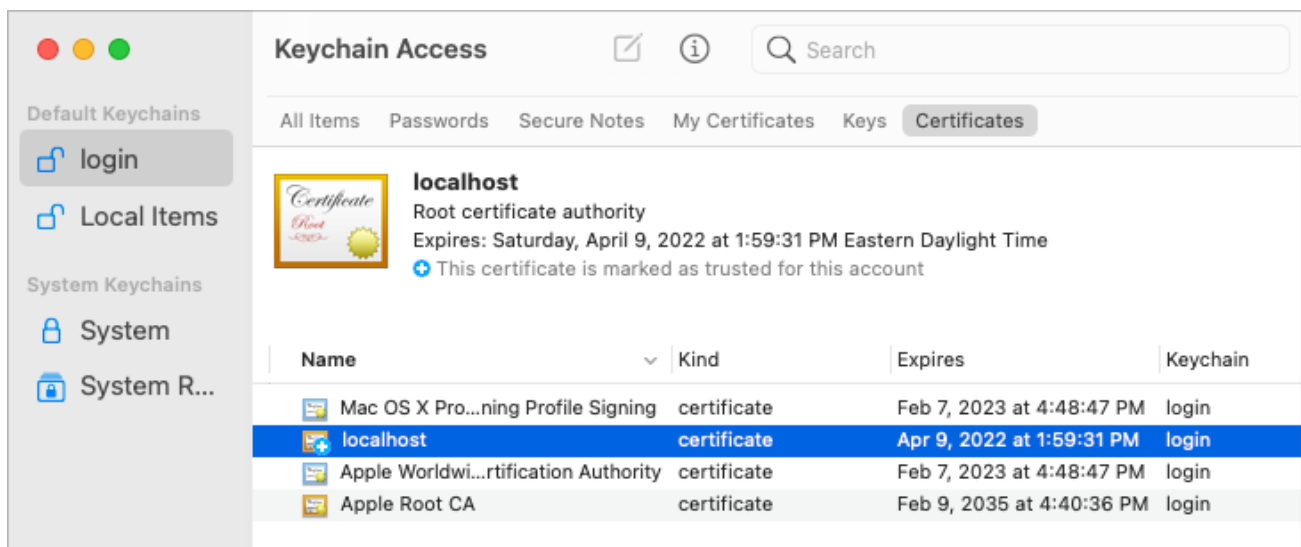


4. You'll be prompted to make changes to your Certificate Trust Settings. Use your Touch ID or enter your password.



You'll be able to proceed to the site.

If you want to revoke the certificate, launch **Keychain Access** and delete the certificate in the **login** keychain.



Chrome

In the last few versions, Chrome has made it more difficult to bypass the invalid certificate warning. On Windows you may still have a **Continue to ...** link when you click the **Advanced** button, but on macOS there is no button or link to bypass the warning.

Instead, you have to type a magic phrase. There's no input field; just click the page to make sure it has focus, then type: `thisisunsafe`



Your connection is not private

Attackers might be trying to steal your information from **149.28.21.212** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_INVALID



To get Chrome's highest level of security, [turn on enhanced protection](#)

Hide advanced

Reload

149.28.21.212 normally uses encryption to protect your information. When Google Chrome tried to connect to 149.28.21.212 this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be 149.28.21.212, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Google Chrome stopped the connection before any data was exchanged.

You cannot visit 149.28.21.212 right now because the website sent scrambled credentials that Google Chrome cannot process. Network errors and attacks are usually temporary, so this page will probably work later.

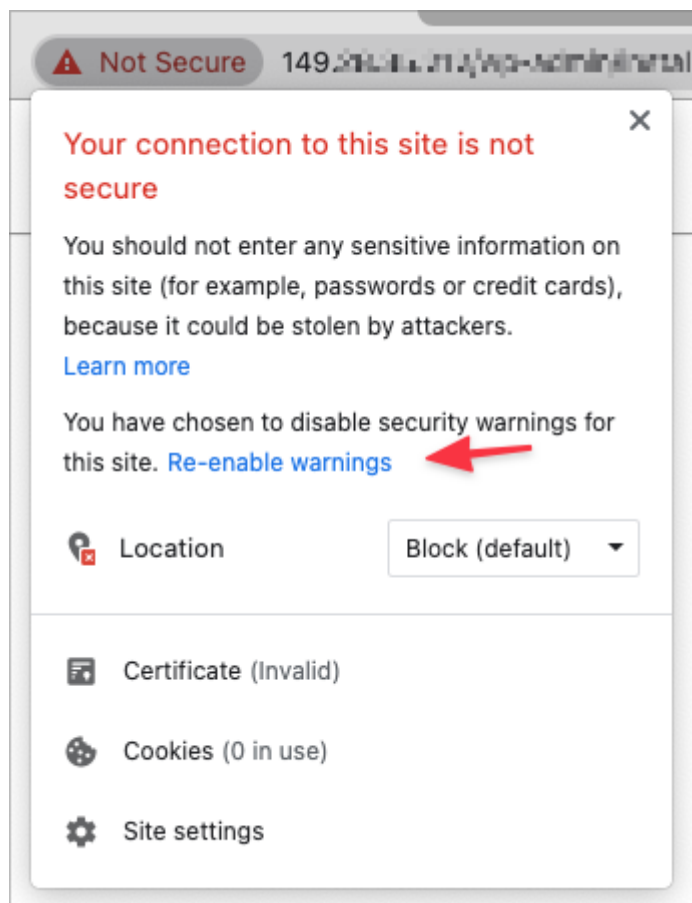
This magic phrase isn't officially documented, but you can find it [buried in the Chromium source code as a base64 encoded string](#).

```
19  const BYPASS_SEQUENCE = window.atob('dGhpc2lzdW5zYWZl');
```

At one point in the past, the magic phrase was `badidea`, and the Chromium developers may change it again in the future. If you discover that `thisisunsafe` has stopped working, please [let us know](#).

Re-enable Warnings

If you've used the `thisisunsafe` trick and need to re-enable the warnings, click the **Not Secure** flag in the address bar, then click **Re-enable warnings** in the information panel.



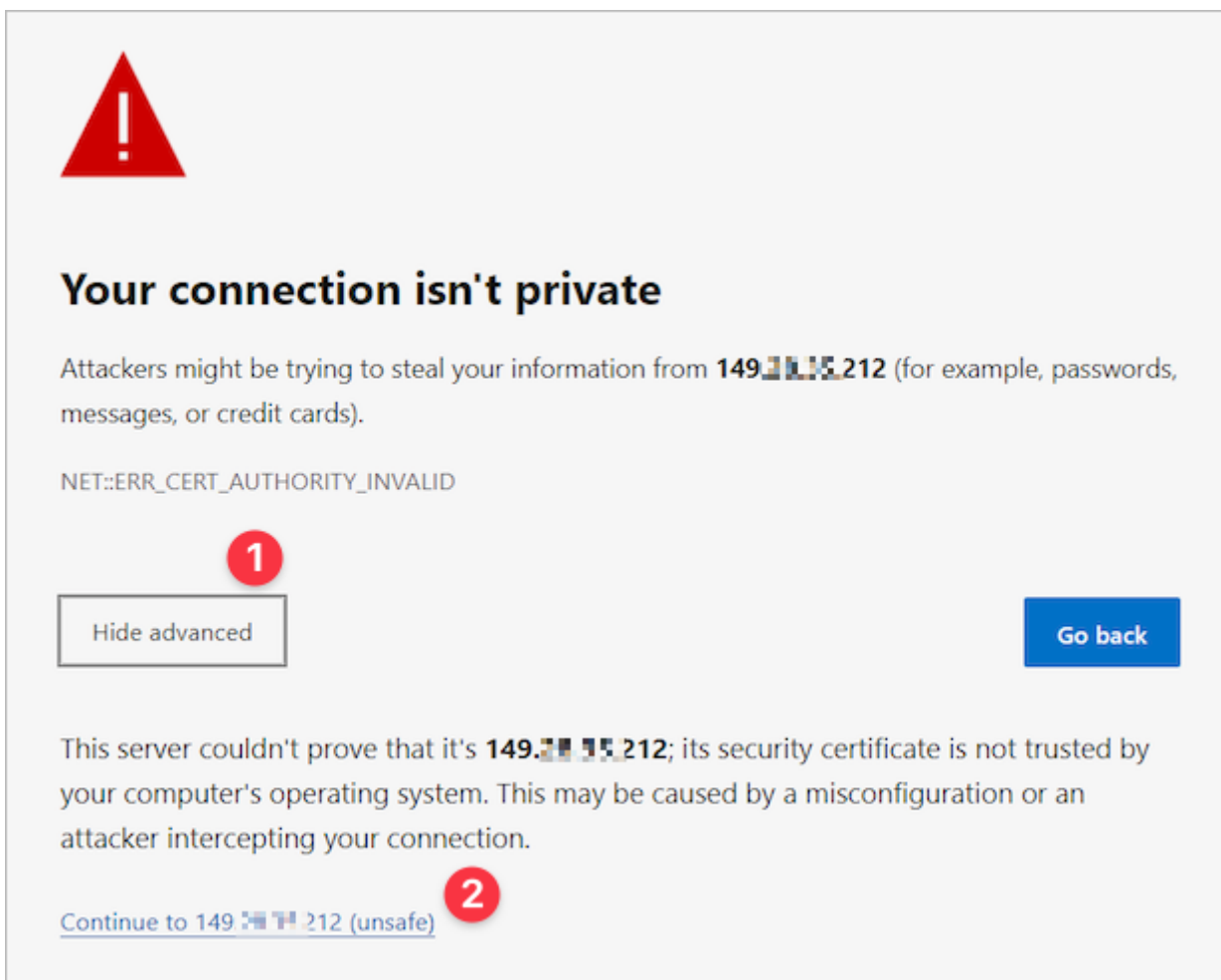
Brave

Brave is a Chromium-based browser. The warning looks the same as Chrome, and the magic phrase is the same: `thisisunsafe`.

Edge

Edge is a Chromium-based browser with a slightly different screen. You can still click a link to bypass.

1. Click the **Advanced** button.
2. Click the **Continue to...** link.



You can also use the magic phrase: `thisisunsafe`

Opera

Opera is a Chromium-based browser. The warning screen looks a little different but uses the same magic phrase: `thisisunsafe`.



Your connection is not private

Attackers might be trying to steal your information from **149.23.25.212** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_INVALID

Reload

▼ Help me understand

149.23.25.212 normally uses encryption to protect your information. When Opera tried to connect to 149.23.25.212 this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be 149.23.25.212, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Opera stopped the connection before any data was exchanged.

You cannot visit 149.23.25.212 right now because the website sent scrambled credentials that Opera cannot process. Network errors and attacks are usually temporary, so this page will probably work later.

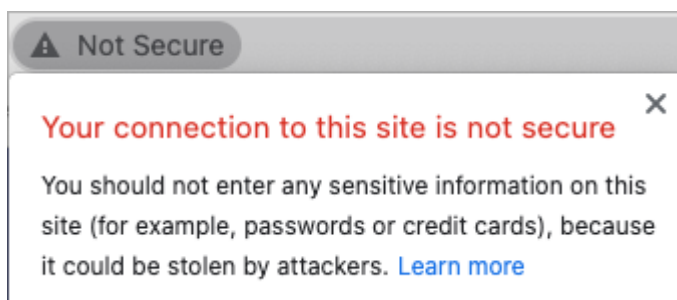
History

HTTPS requires a TLS/SSL certificate, and if you have a domain name for your site, you can get a free Let's Encrypt certificate. However, some sites don't have domain names, or maybe you haven't set it up yet. In those cases, you can use a self-signed certificate. Self-signed certificates allow the server to encrypt the web traffic, but a certificate authority hasn't signed them.

At one time, HTTPS protocol was unusual enough that popular browsers would warn, You are about to view pages over a secure connection. To turn this warning off, you had to check the do not show this warning box.



Fortunately, we've moved past that. Most websites use HTTPS by default, and modern browsers will warn you if they don't.





VULTR

