

CrimeBlocker protects you from the most common sources of cyber crime.

CrimeBlocker Protects You from Cyber Criminals

CrimeBlocker detects and blocks harmful links and attachments in apparently normal emails. They are the primary cause of ransomware attacks.

Stopping Ransomware Attacks

Without CrimeBlocker, ransomware attackers steal your client files and then lock them up with encryption on your computer. They demand a ransom in return for a key to unlock your files and a promise not to upload them, exposing them to anyone on the internet.

When it comes to web security, we use real-time analysis to stop access to innocent-looking, malicious websites. If a site is suspicious, CrimeBlocker doesn't open the webpage. Instead, it displays a warning and offers an option to see a graphic image of the page, explaining the reasons for suspecting it.



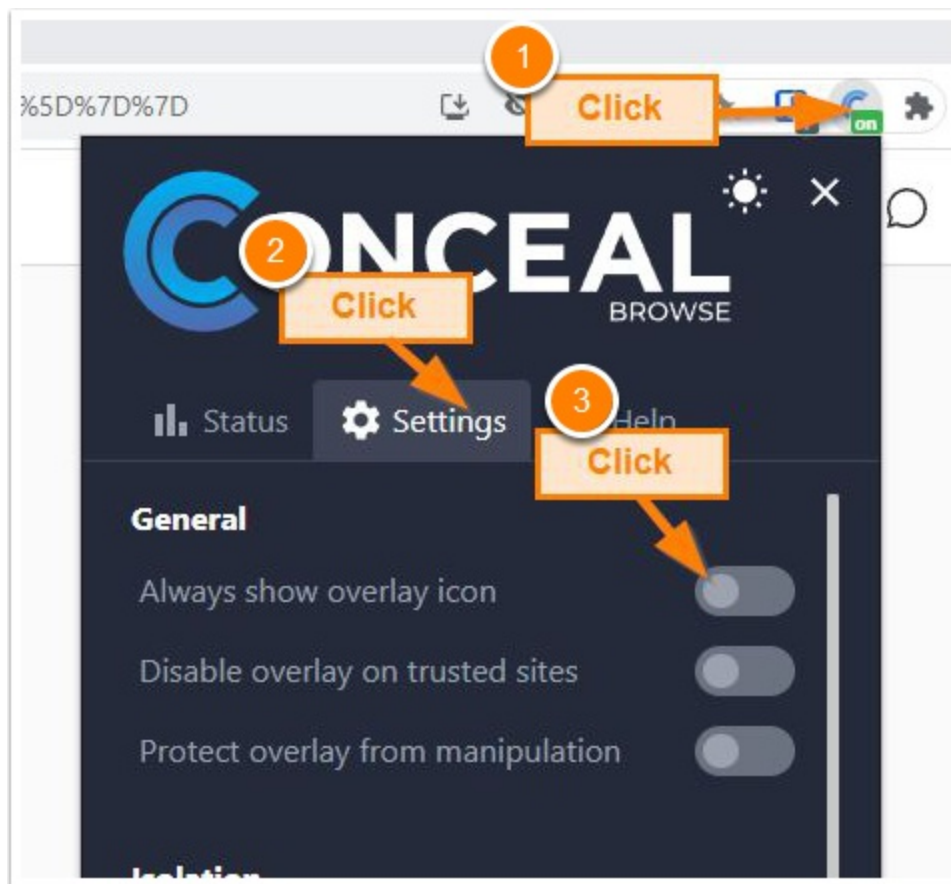
CrimeBlocker Icon and Overlay Icon

The CrimeBlocker Icon appears in the top bar of your browser as an unlocked padlock that is "on."

CrimeBlocker also displays an Overlay Icon, the letter "C", in the lower left area of your webpages.

To hide the Overlay Icon:

1. Click the CrimeBlocker icon in the top bar.
2. Click Settings.
3. Click the first toggle by "Always show overlay icon."



CrimeBlocker Warnings

If you click on a link to a suspicious webpage, CrimeBlocker gives you this Warning Page.

You may click on **Get a safe preview** to see a safe display of the suspicious webpage.

The screenshot displays the CrimeBlocker warning interface. At the top right, the text "Preparing website for safe access..." is shown above the URL "https://join55.com" with a red 'X' icon. Below this, a message states: "This website has been tagged as potentially malicious and might be dangerous. If you choose to continue, it will run in isolation so that your device is not put at risk". Two buttons are visible: "Return to previous page" and "Get a safe preview".

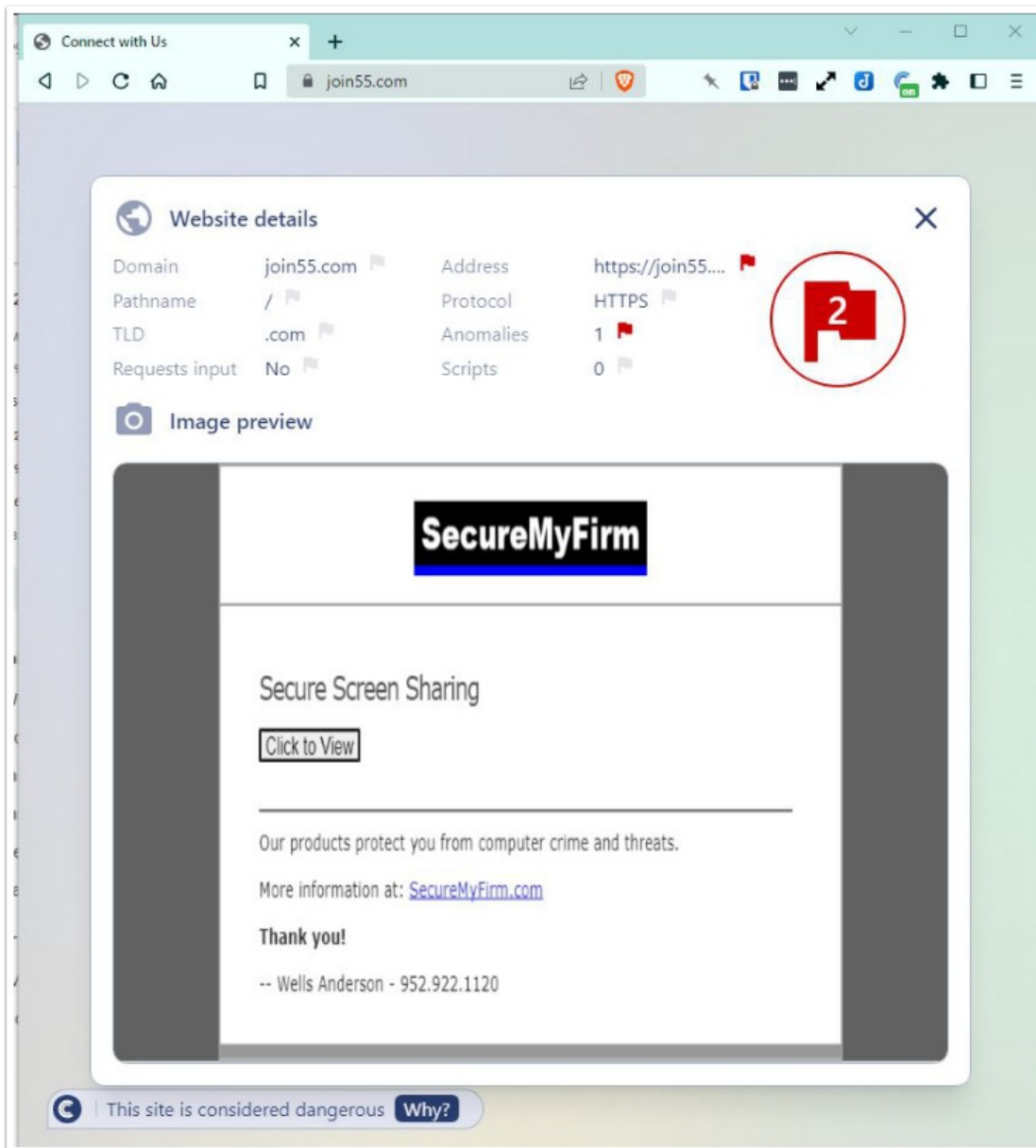
A "What we know.." panel on the left provides details: "The following information lists potential threats and provides an overall risk rating for this website". It lists threat types: Proximity, Profile, Phishing, and Malware. A risk meter shows a 36% risk level. Below the meter, it says "Engine Conceal Threat Types 4".

Callouts with orange arrows point to specific elements: "Click for Preview" points to the "Get a safe preview" button; "Risk Level" points to the 36% risk meter; "Warning" points to the "This site is considered dangerous" message at the bottom left.

Suspicious Webpage Preview

When you click **Get a safe preview**, you see a page display with details at the top.

In this example, we inserted a suspicious script into a demonstration webpage that includes our logo and a clickable button. CrimeBlocker blocked it, Safe web browsing extensions missed it.

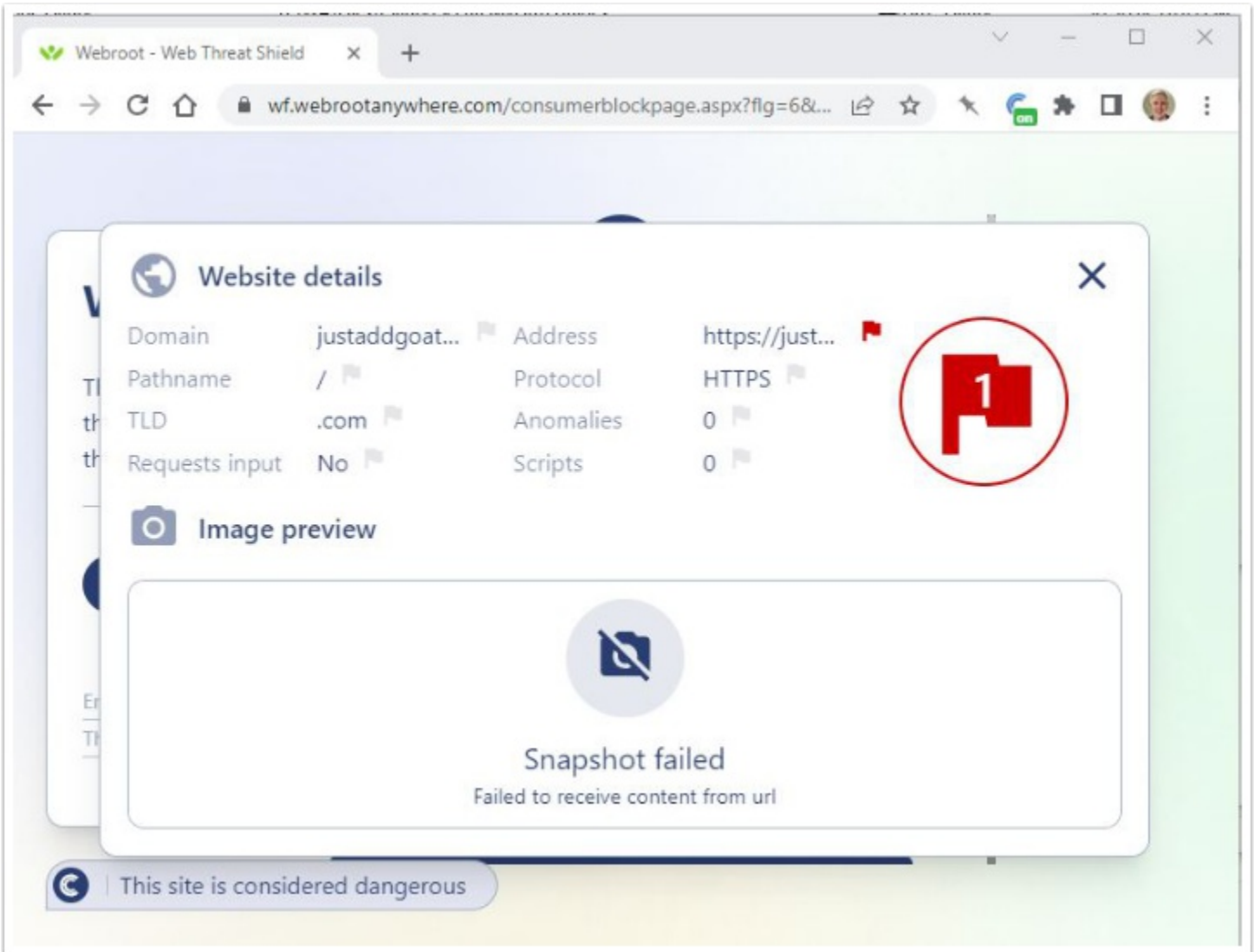


Interaction with Antivirus Software

Other antivirus products and browser extensions detect and block well-known, malicious web pages. In contrast, CrimeBlocker uses multiple techniques to analyze and block zero-day (never seen before) suspicious pages.

If your antivirus software blocks a page, it may warn you a fraction of a second before the CrimeBlocker warning. You may see only the antivirus warning. Or you may see the CrimeBlocker warning on top of the antivirus warning. Below is an example.

In this example, CrimeBlocker cannot display a **Safe Preview** because Webroot antivirus has blocked the page.



False Alarm

It is possible for CrimeBlocker to raise a false alarm and prevent you from accessing a good webpage. In most cases, the **Safe Preview** should allow you to view the page and even click on links to other pages. But it will stop you from filling in fields or downloading anything.

In the event of a false alarm, please report it to us as soon as possible, including the link to the webpage. We can add it to our **Allow List**.

If you cannot wait for us to add the page to CrimeBlocker's Allow List, you have these options:

- Visit the webpage on a smartphone or tablet.
- Download or switch to another web browser that does not have CrimeBlocker installed. Firefox is a good alternative: <https://www.mozilla.org/en-US/firefox/download/thanks>
- Use another computer where CrimeBlocker is not installed.

Note: Be very careful when using a web browser without CrimeBlocker.

Technical Information

Protection Beyond Antivirus

Antivirus services do their best to identify and stop known viruses and emerging new ones. Unfortunately, they have not been effective at stopping ransomware and theft of files. Essentially 100% of successful ransomware attacks are made against computers defended by antivirus services.

CrimeBlocker works differently. It does not scan your drives for evil files. That is still important so you need antivirus services, too. CrimeBlocker intervenes *before* something suspicious comes down from the internet onto your computer.

Security Awareness Training

Security Awareness Training is important, but nowhere near sufficient. Most security education is too brief and too infrequent to reduce your level of risk.

The rapidly growing number of successful ransomware attacks result from three simple errors:

1. Clicking a link in an email;
2. Opening an attachment in a “normal” email;
3. Landing on a counterfeit webpage found in a search.

While no technology can claim to be 100% effective, CrimeBlocker addresses these three most common threats specifically.

Author

Wells Anderson, CEO

SecureMyFirm Inc.

<https://securemyfirm.com>

952.922.1120

Version 1.1 - 2023-07-18