How to Spot a Fraudulent Website

MARSHALL GUNNELL @bacon_gritz, howtogeek,com, JAN 23, 2022

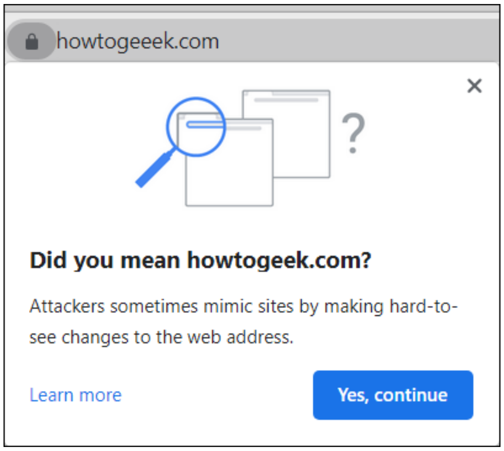
The internet is home to roughly 1.7 billion websites. Unfortunately, many of these websites live only to scam you out of your personal data or money. Here are a few signs to look out for to spot a fraudulent website.

Double-Check the URL Name

The first thing you should do before visiting a site is ensure that the domain name is the one you intend to visit. Fraudsters create fake sites masquerading as an official entity, usually in the form of an organization you would likely recognize, such as Amazon, PayPal, or Wal-Mart. Sometimes the difference between the real site's name and the fraudulent site's name is almost unnoticeable. For example, the cybercriminal may build a site using rnicrosoft.com, but you think you're visiting microsoft.com.

There are two basic ways the cybercriminal, or "threat actor," gets you to visit the fraudulent site. The first way is by a method known as "phishing." Phishing is a form of cyberattack that is delivered mainly by email. The threat actor tries to entice you to click a link in the email that will then redirect you to a fraudulent copy of the real website.

Another way the threat actor may get you to visit the fraudulent site is by a method known as "typosquatting." Typosquatting uses common misspellings of domain names (for example, amazom.com) to trick users into visiting fraudulent websites. You think you entered the domain name correctly, but you're actually visiting a fraudulent copy of the genuine site. If you're lucky, your web browser will warn you.



Did you mean howtogeek.com?

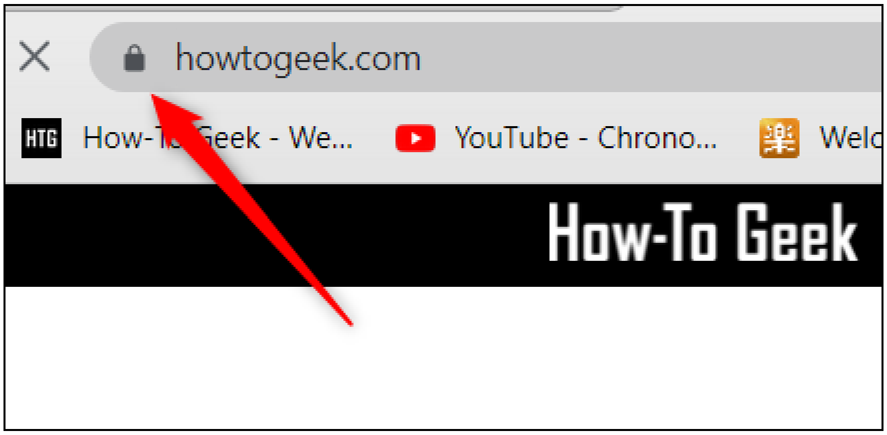
Attackers sometimes mimic sites by making hard-to-see changes to the web address.

Regardless of how you get to the site, once you log in to this fraudulent website, the threat actor will harvest your login credentials and other personal data, such as your credit card information, and then use those credentials themselves on the actual website or any other website where you're using the same login credentials.

The first and most basic method of spotting a fraudulent website is to make sure the domain name is the one you truly intend to visit.

Look For the Padlock, Then Look Harder

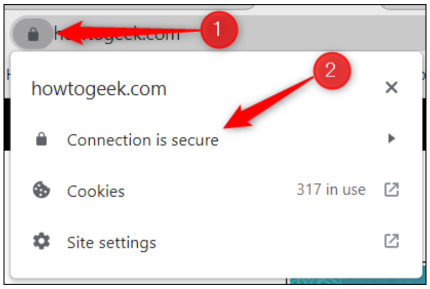
When you visit a website, look for the padlock to the left of the URL in the address bar. This padlock indicates that the site is secured with a TLS/SSL certificate, which encrypts data sent between the user and the website.



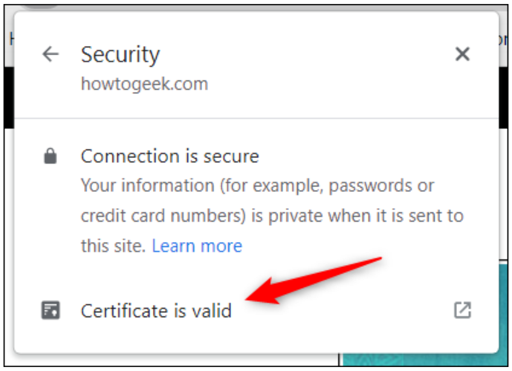
If the website hasn't been issued a TLS/SSL certificate, an exclamation mark (!) will appear to the left of the domain name in the address bar. If a site isn't TLS/SSL certified, any data you send is at risk of being intercepted.

The downside to this is that not all SSL certificates are authentic. These sites are usually caught pretty quickly, but it's still best to look a little harder at the padlock just to be sure. Unfortunately, you can only dig deeper if you're browsing the web using a desktop.

First, click the padlock and then click "Connection is Secure" from the context menu.

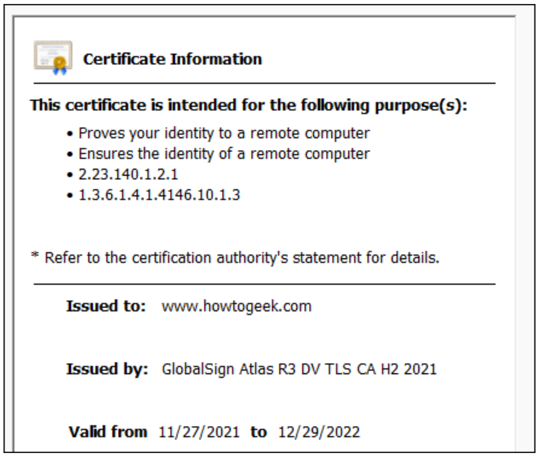


If the certificate is valid, then you'll see the "Certificate is Valid" text on the next menu. Go ahead and click that for more details.



Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

A new window displaying the information about the certificate will appear. You can check which site the certificate was issued to, who it was issued by, and its expiration date.



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.1
- 1.3.6.1.4.1.4146.10.1.3

* Refer to the certification authority's statement for details.

Issued to: www.howtogeek.com

Issued by: GlobalSign Atlas R3 DV TLS CA H2 2021

Valid from 11/27/2021 **to** 12/29/2022

While this won't always protect you from fraudsters, the padlock (and the certificate information) is a good indicator that you're visiting a legitimate site.

Check the Site's Privacy and Return Policies

Fraudulent websites generally don't go to the extent that genuine websites go to concerning privacy and return policies, if at all. For example, Amazon has a pretty thorough return policy and privacy policy that details everything the customer needs to know about each respective policy.

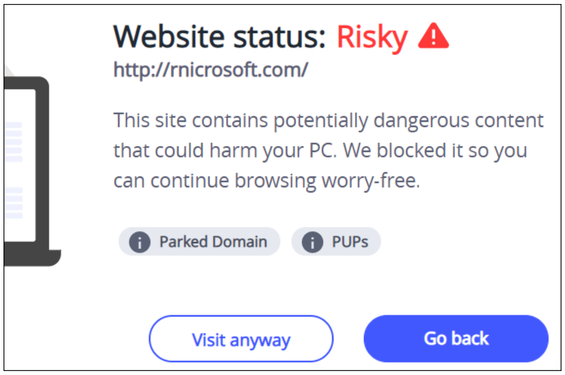
If a site has a poorly written return or privacy policy, that should raise some red flags. If a site doesn't have these policies stated on their website at all, avoid them at all costs, as the site is likely a scam site.

Check For Poor Spelling, Grammar, and UI

A spelling or grammar mistake is likely to happen now and again, even on the most authoritative of websites. However, most websites have teams of professionals creating these websites. If a website looks like it was created in a day by one person, is riddled with spelling and grammar errors, and has a questionable user interface (UI), there's a chance that you're visiting a dangerous website.

Use a Site Scanner

If you'd like to add another layer of protection between you and fraudulent websites (and also give you a heads up if you may be visiting one), then use a site scanner such as McAfee SiteAdvisor.
These tools crawl the web and test sites for spam and malware. If you visit a dangerous (or potentially dangerous) site that the program determines may contain dangerous content that could harm your PC, you'll be notified and asked to confirm you still want to proceed to the site when you try to visit.



Website status: Risky ⚠

http://rnicrosoft.com/

This site contains potentially dangerous content that could harm your PC. We blocked it so you can continue browsing worry-free.

While site scanners are helpful in spotting a potentially fraudulent website, not all fraudulent websites will be flagged. While you use them as an extra layer of protection, still be conscious of the sites you visit.

What to Do If You've Been Scammed

If you're a victim of an online scam, there are a few measures you can take to protect yourself (and potentially protect others). What you need to do next depends on what type of information you believe the scammer may have on you.

If you purchased something using your credit or debit card from the fraudulent site, the first thing you should do is call your bank immediately and report to them what happened. They'll freeze your accounts and cards so that the threat actor can no longer purchase anything with your details.

If you believe the threat actor may also have your personal information, such as your Social Security Number, date of birth, address, and so on, you'll want to freeze your credit so that the fraudster can't take out any loans or open any accounts in your name.

Once that's taken care of, file a report with your local police, notify the Internet Crime Complaint Center (IC3), and report the site to Google.