



Beware of spoof websites

Spoof websites can lure unsuspecting people into giving away their information without knowing that they're doing it. A spoof website will try to make itself look almost exactly like the website it is trying to spoof, hoping a person will enter their personal information or username and password.

Once a scammer's fake, but legitimate-looking website gets indexed by search engines, it will appear in search results based on the search words you type.

Even if you are a seasoned internet user, it is easy to fall prey to the sophisticated techniques that are used in website spoofing. With the wool pulled over your eyes, you could inadvertently give phishers extremely damaging information. The best way to handle spoofed websites is by exercising caution at all times.

Finding your way onto a spoofed website usually happens by using vague or incorrect search engine terms. It also can happen if you type a web address too quickly and accidentally transpose two letters or misspell the web address.

How to spot spoof websites

There are several ways to spot a fake website:

- **Misspellings and grammar mistakes:** While most fraudulent websites try to make it look as close to the actual website they're trying to spoof as possible, misspellings or

improper capitalization of words sometimes creep in. Also look for missing periods or commas

- **Take a close look at the URL:** If the URL isn't what you expect it to be, it's probably a spoof website. Close that website as soon as possible.
- **Blurry logos or images:** Because spoof websites don't have access to original company logos and images, the ones they'll use are lower resolution and likely will appear to be blurry on the spoof website.

If you see any of these red flags, don't click on any links.

How to prevent visiting a spoof website

If it is a website you visit often, such as your bank website, bookmarking the website and accessing it directly via the bookmark will prevent you from accidentally typing in the website address incorrectly.

Also, be extra careful when using a search engine. Ensure the words are spelled correctly.

Before clicking on a link, hover over it and read the true website address at the bottom left of the browser. If it isn't familiar, don't click on the link.

By taking your time and being careful, you should be able to avoid most problems.

What to do if you suspect a spoof website

If you happen across a spoofed website, you can report the fake website to the federal government here <https://reportfraud.ftc.gov/> and you can report it to Google as well here https://safebrowsing.google.com/safebrowsing/report_phish/?hl=en

Opinions expressed above are the personal opinions of the author and meant for generic illustration purposes only.
RCB Bank, Member FDIC.

Sources:

<https://www.phishing.org/phishing-and-spoofing>