How to Verify Links Before Entering Account Details

Every time you type a password or a recovery phrase into a login page, you are trusting that the page is genuine. On the darknet, where onion addresses change, services go down, and copycat sites appear within hours, that trust can be hard to place. A single wrong link can send your credentials to someone who does not run the marketplace at all. This article walks through the checks that help you confirm a link is real before you hand over anything sensitive.

Start with a Trusted Source for the Link

The safest way to reach any login portal is to get the address from a source you have verified beforehand. Bookmarking a known-good link inside Tor Browser is one reliable method, because bookmarks are stored locally and cannot be changed by a DNS hijack or a compromised search result. If you do not have a bookmark yet, the next best option is a mirror directory that has been maintained over time and cross-checked by multiple people.

An official mirror directory does not just list addresses. It also shows the status of each mirror, often with a timestamp or a green indicator, so you know which ones are reachable at that moment. The directory itself is only useful if you have reached it through a path you trust. That means typing the directory's own onion address from memory, or from a source you have already confirmed, rather than clicking a link in a forum post or a chat message.

Check the Onion Address Character by Character

Onion addresses are long strings of random characters followed by .onion. Phishing sites often use an address that looks almost identical to the real one, substituting a single character or using a homoglyph, a letter from another alphabet that looks the same on screen. Tor Browser does not warn you about these lookalikes because the address is technically valid.

Read the address aloud to yourself, character by character, or paste it into a text file and compare it side by side with a known-correct version. If the directory you use lists the full address, copy it from there rather than retyping it. Even a single wrong character sends you to a different hidden service.

Check for HTTPS and the Right Padlock Icon

Onion sites served through Tor's own protocol already have end-to-end encryption, but many also support HTTPS. When you visit a login page, look for the padlock icon in the address bar and confirm that the connection says "Onion" or "Secure". A phishing site can still get a TLS

certificate if the phisher sets up HTTPS on their own domain, so the padlock alone is not proof of legitimacy. But its absence is a strong warning. If a mirror site that should use HTTPS presents a plain HTTP connection, treat it with suspicion.

Verify the Page Content, Not Just the Address

A convincing phishing page copies the design of the real login portal down to the logo, the font, and the layout. The difference is often in the behaviour. Try submitting an intentionally wrong password. A real marketplace typically shows a generic error such as "Invalid credentials" and does not reveal whether the username exists. A phishing page might redirect you, show a different error message, or accept the wrong password without complaint.

Another tell is the page source. Look at the HTML for any form action that points to an external domain or an IP address. Onion services do not normally submit form data to clearnet addresses. If the form action is an IP or a regular web domain, the data is going somewhere outside Tor. That is a clear sign of a phishing attempt.

Good guidance for avoiding phishing reminds you to treat the login page itself as part of the attack surface. The page you see is not necessarily the page that processes your input.

Use Two-Factor Authentication When Available

Even if you have confirmed the link is correct, a compromised account can still happen if your password is reused or guessed. Two-factor authentication (2FA) adds a second check that a phisher cannot bypass with just your password. On the darknet, 2FA often means a time-based one-time password generated by an app on your phone, or a PGP challenge that you must decrypt. If the marketplace supports it, enable it. It will not stop a phishing page that asks for your 2FA code and forwards it in real time, but it does protect against credential theft from database breaches on other sites.

Keep a Short List of Bookmarks

Bookmarking the login page inside Tor Browser means you never have to search for the address again. Tor Browser stores bookmarks locally and does not phone home to check them. Make sure you only bookmark the page after you have verified it through the checks above. Once bookmarked, use that bookmark every time. Do not click links in emails, forum threads, or private messages that claim to be a mirror. Those are common delivery methods for phishing links.

If a bookmark stops working because the service changed its address, return to the official mirror directory to find the current link. Update your bookmark immediately so you are not tempted to use a search engine or a third-party list next time.

Beware of Urgent or Threatening Language

Phishing pages often create a sense of urgency: "Your account will be disabled in 24 hours if you do not log in now." Or "A security issue requires you to re-enter your password." The real marketplace rarely asks for credentials outside the normal login flow. If a page pressures you to act fast, slow down. Open the official mirror directory separately, confirm the address, and only then enter your details.

Another common trick is a fake "maintenance mode" page that asks for your password to "verify your identity before the site comes back." Legitimate maintenance pages do not collect credentials. If you see a login form on what looks like a maintenance screen, close the tab and go back to the directory.

What to Do If You Suspect a Phishing Page

If a page feels off, do not enter anything. Close the tab and clear your Tor Browser identity. Then visit the official mirror directory from a known-safe bookmarked source and check whether the suspect address is listed. If it is not listed, report it to the marketplace administrators if they have a contact method. Many marketplaces have a PGP-signed message on their official page that lists known phishing addresses. Compare the suspect address against that list.

Beyond the specific checks above, consistent **guidance for avoiding phishing** is the single most effective habit. Each time you log in, run through the same small routine: confirm the source of the link, read the onion address, check the padlock, and test the page behaviour. Over time the routine becomes automatic, and the mental cost of verifying a link becomes very low.

Remember That No Single Check Is Enough

A valid onion address does not guarantee a safe page. A padlock does not guarantee the site is the one you want. A convincing design does not mean the form goes to the right place. The strength of the verification comes from combining several checks: a trusted source, a correct address, a matching page, and sensible behaviour from the login form. Skip any one of them and you increase the risk of handing your credentials to a phisher.

The official mirror directory exists to give you a reliable starting point. Use it, but verify the link it gives you before you trust it. And once you have verified a working mirror, bookmark it so you can bypass the directory next time. That reduces the number of times you need to repeat the full verification, while still keeping you safe each time you log in.