What to Verify Before Signing Into a Mirror Site

Why verifying a mirror matters

When you access a marketplace through a mirror or alternative address, you are putting your credentials and personal data in the hands of whoever controls that server. A legitimate mirror should be an exact copy of the real site, but attackers sometimes create fake mirrors to capture login details, session tokens, or two factor authentication codes. Before you type anything into a mirror, you need to confirm a few key points to avoid handing over your account to someone else.

Check the source of the mirror link

The first thing to verify is where you got the mirror address. A reliable mirror link should come from a trusted source, such as the official community forum, a verified announcement channel on a secure messaging platform, or a known directory that updates regularly. If you found the link in a random chat room, a social media post from an unknown account, or a search engine result that looks slightly off, treat it with suspicion. Attackers often post fake links in public spaces hoping that people will click without thinking.

One practical step is to cross-reference the mirror address against multiple trusted sources. If the same onion address appears on the official forum and in announcements from administrators, it is far more likely to be genuine. If only one source lists it, or if the source itself seems unreliable, do not use it.

Confirm the certificate and page integrity

When you load a mirror page, check that the site presents the same login page you expect. Look for visual inconsistencies, such as a different logo, altered wording, or missing elements. A fake mirror may look convincing but often has small errors, like a slightly different font, a misplaced button, or a missing security notice. Also, if the mirror uses HTTPS, check the certificate details. A legitimate marketplace should have a valid certificate that matches the domain. If your browser warns about an invalid certificate or if the certificate does not match the site you intend to visit, do not proceed.

Inspect the login form for extra fields or unusual behavior

Before you enter your username and password, look at the login form itself. A genuine login form asks only for your username and password, and possibly a one-time code if you have two factor authentication enabled. If the form asks for additional information, such as your

recovery code, your PIN, or a secondary password, that is a red flag. Attackers sometimes modify the form to harvest extra data that can help them bypass your security.

Also, pay attention to how the page behaves when you click the login button. A legitimate site should submit the form securely and then redirect you to your account dashboard. If the page seems to freeze, reloads without logging you in, or shows an error message that looks generic, it could be a phishing attempt. In such cases, close the page and do not use that mirror again.

Test with a wrong password first

A simple but effective technique is to enter a deliberately incorrect password on the first attempt. A genuine mirror will reject it with a standard "invalid credentials" message. A phishing site might accept it and then show a fake error, or it might silently capture the data and redirect you to a page that asks you to "try again". If the behavior seems odd, or if the error message is different from what you normally see, it is safer to assume the mirror is malicious. Do not use your real password on that site.

Verify that your two factor authentication works as expected

If you have two factor authentication enabled, the mirror should prompt you for a code after you enter your password. A legitimate site will ask for a time-based one-time password from your authenticator app or a code sent via SMS or email. A fake mirror may skip the two factor step entirely, or it may ask for your code but then redirect you to a page that says "two factor setup required" or asks you to "reconfigure" your authenticator. This is a common tactic to steal both your password and your current code, which the attacker can then use to log into the real site immediately.

If the mirror asks you to enter a recovery code or to set up two factor authentication again when you did not request it, stop. That is almost certainly a phishing attempt. The only time you should reconfigure two factor is if you have lost access to your authenticator device and are following a verified recovery process through the official site.

Look for signs of credential theft after login

Once you log into a mirror, monitor your account for unusual activity. Check your profile settings, your message inbox, and your recent login history. If you see changes you did not make, or if you receive messages that you did not send, the mirror may have compromised your session. In that case, change your password immediately, revoke any active sessions, and update your recovery codes. Also, contact the marketplace support team through a verified channel to report the incident.

Use a strong password and a password manager

Even when you verify a mirror thoroughly, using a strong, unique password for each site reduces the risk if your credentials are compromised. A password manager can generate and store complex passwords, so you do not have to remember them. It also helps you avoid reusing passwords across different services, which is a common way that credential theft spreads. If a mirror is compromised and your password is stolen, it should not give the attacker access to your other accounts.

Consider PGP encryption for additional verification

Some marketplaces, including WeTheNorth Market, provide PGP-signed messages or signed announcements that contain the official mirror addresses. If you have the marketplace's public PGP key, you can verify the signature on any announcement or link you receive. This is one of the most reliable ways to confirm that a mirror is legitimate, because a fake attacker cannot forge a valid signature without the private key. If you are unsure how to use PGP, look for guides on verifying signed messages; it is a skill worth learning for anyone who uses onion services regularly.

What to do if you suspect a mirror is fake

If you have already entered your credentials into a suspicious mirror, act quickly. Change your password on the real site as soon as possible. If you use two factor authentication, also rotate your recovery codes and check your session list for any unknown devices. If the fake mirror captured your session cookie, an attacker could hijack your session even after you change your password. Log out of all sessions and log in again from a trusted source.

Report the fake mirror to the marketplace administrators through a verified channel. They can add the address to a blocklist and warn other users. Do not share the link with anyone, even to warn them, because doing so may spread the phishing attempt further. Instead, direct people to the official source for mirror addresses.

Staying safe over time

Security is not a one-time check. Mirrors can change, and attackers are always finding new ways to trick users. Make it a habit to verify any mirror link every time you use it, even if it looks familiar. Bookmark the official mirror addresses you have verified, and only use those bookmarks to access the site. If you ever need a new mirror, go back to the trusted sources you used initially.

WeTheNorth Market provides guidance on accessing its services safely, and following that advice can help you avoid common pitfalls. The same principles apply to any marketplace or

service that uses mirrors: verify the source, check the page, test with a wrong password, and use two factor authentication properly. A little caution upfront can save you from losing your account or your personal data.