

1P_jess
1Password Employee • 1 year ago

Typosquatting

Cybercriminals will often use slightly misspelled URLs to add legitimacy to their fake websites. If the URL and page design looks familiar at first glance, it's easy to go into autopilot and either enter your login credentials or initiate a download.

This is where typosquatting comes in – a form of cybercrime that can be surprisingly difficult to notice. Malicious actors impersonate credible software and trick unsuspecting users by preying on how hard spelling mistakes are to spot in website URLs and extension names. This can lead to identity theft and other harmful consequences. It can also cause reputational damage and revenue loss for targeted companies.

As sneaky as typosquatting can be, understanding how it happens can help you catch it early or avoid it altogether.

What is typosquatting?

“Typosquatting” refers to a cybercriminal registering domain names that are similar but slightly different to legitimate domains. The technique can include subtle misspellings, adding a hyphen to a phrase, making a singular word plural, or using a different top-level domain (TLD), like .co instead of .com. For example, 1Password.com could be written as IPassword.com, using a capital i instead of a 1 (one) in the domain name to try to imitate 1Password. (Thankfully, we already own it!)

Typosquatting differs from cybersquatting, which refers to someone buying the actual, correctly-spelled domain with the intention of selling it back to an interested buyer or others from owning it.

Chat

Over time, typosquatting has expanded beyond just website domains and into other services, like developer IDE extensions and package manager libraries. The same idea applies: the user thinks they're installing a credible resource and accidentally installs a harmful one instead. (Read our blog post on how a phony IDE extension led to a developer's cryptocurrency wallet being infiltrated.)

The intention of typosquatting is to lead the user into believing the imposter site belongs to the legitimate company, even though it doesn't. The user visits a website that has an error in its domain and thinks they're on the intended site, which puts them at risk of sharing sensitive information (like financial details or login credentials) or downloading harmful files, such as malware or viruses.

It's worth noting that typosquatting isn't only done by cybercriminals. Some companies will typosquat versions of their own domain to avoid someone else trying to do this maliciously.

How typosquatting can affect you and your customers

Typosquatting is dangerous because it can happen without a person even realizing, especially if the imposter site is styled to resemble the intended site – a form of phishing.

Some common repercussions of falling victim to typosquatting include:

- Data theft as a result of sharing login credentials can give the malicious actor access to private data.
- Financial loss, which can result from identity theft or a company trying to buy the domain with the typo.
- Damage to your personal devices that results from malware or viruses being installed.
- Broken trust with customers who no longer feel comfortable engaging with the company.

Typosquatting poses real threats. Thankfully, there are several ways you can protect yourself online and make it easier to spot fake domains and other typo-based tricks.

How to stay protected from typosquatting

Given how common and relatable typos are, it's important to find ways to make sure you only engage with the intended website.

Apply these tips to ensure you're visiting the correct website or installing legitimate extensions/software:

1. **Bookmark the websites you visit often** and navigate to them via the bookmark. You can also leave websites open or pin them in your browser to avoid having to reopen them each time. Just remember to log out of any accounts you signed into at the end of each session, even if you're leaving the tabs open!
2. **Confirm the website you're visiting is the intended one** before entering login credentials or downloading anything – even if the website looks credible.
3. **Hover over links before clicking on them.** This lets you view the URL text and check it's the intended website.
4. **Search for a company's website in your preferred search engine** instead of manually typing in the URL. This will help you avoid misremembering or misspelling the credible website's domain. However, typosquatting pages can still show up in search results, so remember to check the spelling of any pages you click.
5. **Use serif fonts when possible**, which tend to make similar characters look noticeably different. For example, a zero and capital O, or a lowercase L and uppercase i are easier to distinguish in a serif font.
6. **Use passkeys when possible**, which tie your authentication to a specific website. (Learn more about passkeys in a previous blog post.)
7. **Use a password manager like 1Password**, which will only fill login credentials for the intended website.

Using 1Password is the easiest way to avoid this issue altogether. Any passwords or passkeys you save in 1Password are associated with the website they were saved on. This means the login credentials for your email will only load when you visit the specific domain associated with those credentials. If you go to a website with a similar URL, 1Password will notice it doesn't match and won't suggest the login information as an autofill option.

If you don't see 1Password suggesting the item information, it's a good hint that the website might not be credible. This gives you the opportunity to double-check which page you're on and close the page immediately if it's in any way suspicious.

As is the case with most cybersecurity precautions, it's always good to trust your gut if something feels off. If you stay alert and use a password manager, you're well placed to catch

typosquatting attempts, no matter how convincing they are, and stick to legitimate websites and extensions.

Like Reply Follow Share

Leave a reply...

Was this helpful?



Passwordless

Device Security

Compliance and Cyber Insurance

What's new

Community blog

Events

Developers

Discussions

Documentation

Integrations

Slack

Bug bounty

Resources

Guides and toolkits

Help and documentation

1Password blog

1Password Marketplace

Random but Memorable

Community guidelines

Company

About

We're hiring!

Terms of Service

Your Privacy Choices

Cookie Policy

Privacy Policy

Accessibility

©2026 1Password. All rights reserved.
4711 Yonge St, 10th Floor, Toronto Ontario, M2N 6K8, Canada