T

Typosquatting: Look-Alike Domains, Detection, and Response

Typosquatting uses misspelled or look-alike domain names to misdirect users. Learn the main variants, warning signs, defenses, and incident response steps.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 How typosquatting works
02 Common look-alike techniques
03 How users can spot and avoid it
04 Protection for organizations
05 If you used a look-alike site
06 Sources

Quick answer: Typosquatting is the registration or use of a domain name that resembles a legitimate one, often by adding, removing, swapping, or replacing characters. Attackers use the confusion for phishing, malware delivery, advertising, counterfeit sales, or credential theft. Inspect the registrable domain, not just the logo or first words in a URL.

01 How typosquatting works

A person mistypes a familiar address, clicks a deceptive link, or overlooks a small difference on a mobile screen. The look-alike site may copy branding, redirect to another page, show ads, or present a false sign-in. Email can use the same domain for convincing sender addresses and reply destinations.

The important part of a web address is the registered domain immediately before the public suffix. In `company.example-login.com`, the registered domain is `example-login.com`, not `company.com`. HTTPS and a padlock only mean the connection to that domain is encrypted; they do not prove the operator is trustworthy.

02 Common look-alike techniques

- **Missing, added, or repeated characters:** a dropped letter, doubled letter, or extra hyphen.
- **Adjacent-key and transposition errors:** two characters are swapped or a nearby keyboard key is substituted.
- **Homographs:** visually similar Unicode characters from different scripts imitate Latin letters.
- **Wrong suffix:** the familiar name appears under another top-level or country-code domain.
- **Combosquatting:** a trusted name is combined with words such as login, support, secure, invoice, or update.
- **Misleading subdomains:** the real brand is placed far to the left of an attacker-controlled registered domain.

Typosquatting overlaps with phishing but is not identical to it. A parked typo domain may display ads without stealing a password, while phishing can occur on a completely unrelated or compromised domain.

03 How users can spot and avoid it

1. Use a saved bookmark or password manager for important banking, email, cloud, and payment sites.
2. Before signing in, expand the full address and read the registered domain from right to left. Be cautious with shortened links and QR codes.
3. Let the password manager fill only on the exact saved domain. An unexpected failure to fill is a useful warning.
4. Do not rely on page design, search-ad placement, a padlock, or a familiar favicon as proof.
5. Use phishing-resistant MFA. It can stop credential replay when passwords are captured, though users should still report the site.

04 Protection for organizations

Register the most plausible high-risk variants where justified, but do not try to buy every possible spelling. Monitor certificate transparency, new domain registrations, DNS, brand mentions, and email telemetry. Configure SPF, DKIM, and DMARC for owned domains; these controls reduce spoofing of your domain but do not stop mail sent from a look-alike domain. Secure registrar accounts with strong MFA and registry lock where appropriate.

For takedown, preserve the full URL, screenshots, message headers, timestamps, DNS information, and the harm observed. Report the content to the hosting provider and the domain to its registrar through published abuse channels. ICANN contractual complaints can address a registrar’s failure to investigate applicable abuse reports, but ICANN is not a universal content takedown service and does not control country-code registries.

05 If you used a look-alike site

Close the page. If you entered credentials, change them from the legitimate site on a clean device, revoke sessions, review MFA methods, and check account activity. If you downloaded or ran a file, disconnect the device and scan or investigate it. Contact the bank or payment provider

immediately for financial information, and notify the impersonated organization using contact details obtained independently.

06 Sources

Definitions and response context are supported by the ICANN DNS Security Facilitation Initiative report and ICANN DNS Abuse Mitigation Program.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com