A

Address Bar Spoofing: Fake URLs, Browser Tricks, and Protection

Address bar spoofing makes a malicious page appear to have a trusted browser location. Learn to distinguish actual browser UI attacks from fake URLs.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

Address bar spoofing is an attack that causes the browser's location display to show or appear to show a trusted address while attacker-controlled content is active. Its purpose is usually to make a phishing login, payment page, or permission request look authentic.

The term should not be applied to every deceptive URL. Several different tricks look similar but require different defenses.

Address bar spoofing vs. related tricks

- **Browser UI vulnerability:** a flaw creates a mismatch between displayed origin and active content. Mozilla has published security advisories for real examples, including MFSA 2016-28 .

- **Fake in-page address bar:** a full-screen page, popup, image, or mobile interface imitates browser controls. It cannot replace trusted browser UI but may hide it.
- **Look-alike domain:** typos, extra labels, Unicode characters, or a misleading subdomain make the real URL easy to misread.
- **Open redirect or rapid navigation:** a trusted address appears briefly before the browser moves elsewhere.

A valid padlock means the connection to the displayed hostname is encrypted. It does not prove that the hostname belongs to the brand shown on the page.

How to read the real URL

1. Exit full-screen or standalone-app mode and focus the browser's actual address field.
2. Reveal or copy the complete address without visiting it elsewhere. On mobile, use the browser menu's page information when available.
3. Identify the hostname between `https://` and the next slash, port, question mark, or fragment.
4. Read the registered domain from right to left. In `bank.example.attacker.test`, the controlling domain is `attacker.test`, not `example`.
5. Check for omitted letters, substitutions, unexpected country-code endings, and punycode beginning with `xn--`.

Warning signs

- the visible “bar” scrolls with the page or cannot receive normal focus;
- back, reload, share, or site-information controls behave differently from normal browser controls;
- opening the page in a new normal tab reveals another hostname;
- a sensitive sign-in appeared after an unsolicited message, popup, QR code, or redirect;

- the browser is outdated or displays a certificate or deceptive-site warning.

How to protect yourself

- Install browser and operating-system updates promptly; true address bar vulnerabilities require vendor fixes.
- Use saved bookmarks or a known official app for banking, email, and administration instead of message links.
- Use a password manager: it normally fills credentials only for the saved origin, so refusal to fill is an important warning.
- Prefer passkeys or phishing-resistant security keys. SMS and one-time codes can still be relayed by a live phishing site.
- Avoid installing unknown browsers, profiles, extensions, or “security certificate” packages.

If you entered credentials or payment data

1. Close the page and preserve the URL, message, and time for reporting.
2. From a known-clean device, change the affected password and every account that reused it.
3. Revoke sessions, review MFA and recovery settings, and remove unknown connected applications.
4. Contact the bank or card issuer through its official number if payment information was submitted.
5. Scan the original device if a download, extension, profile, or app was installed.

Address bar spoofing FAQ

Can a website normally edit the browser address bar?

A page can navigate the tab but should not control trusted browser chrome. A real mismatch is a security vulnerability; an in-page imitation is visual deception.

Does typing the domain always protect me?

It defeats many phishing links, but compromised DNS, a browser vulnerability, malware, or a typing mistake can still redirect or deceive.

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