A

Address Bar: How to Read URLs and Spot Fake Websites

The address bar shows the current page's URL and security context. Learn how to identify the real domain, understand URL parts, and spot phishing tricks.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 What the address bar tells you

02 How to read a domain safely

03 Address bar warning signs

04 HTTPS is not proof that a site is trustworthy

05 Five checks before entering sensitive information

06 Address bar versus search box

07 What if the address bar is missing or looks fake?

08 Frequently asked questions

09 References

The address bar (also called the URL bar, location bar, or omnibox) is the field at the top of a web browser that shows the address of the current page. You can use it to open a web address, search the web, and check which site is actually asking for your password or payment details.

Modern browsers often combine navigation and search in one field. A complete web address opens a page; ordinary words are sent to the default search engine.

01 What the address bar tells you

Consider `https://accounts.example.com/security/reset?source=email#help`.

Part	Example	Meaning
Scheme	`https`	How the browser connects. HTTPS encrypts traffic to this host.
Hostname	`accounts.example.com`	The server name, including subdomain and registrable domain.
Registrable domain	`example.com`	The key part for deciding who controls the address.
Path	`/security/reset`	A page or resource on that site.
Query	`?source=email`	Parameters sent to the site.
Fragment	`#help`	A location or state within the page.

For a trust decision, focus on the hostname and especially the registrable domain. Text after the first single slash belongs to the path, query, or fragment; a malicious site can place a familiar brand there without owning that brand's domain.

02 How to read a domain safely

Start after `https://` and stop at the next `/`, `?`, or `#`. Within the hostname, read from right to left. In `login.bank.example.com`, `example.com` is the registrable domain and `login.bank` consists of subdomains controlled by its owner.

A name at the far left does not prove ownership. `paypal.com.signin-example.net` is controlled through `signin-example.net`, not `paypal.com`. Likewise, `signin-example.net/paypal.com` remains a page on `signin-example.net`.

03 Address bar warning signs

- **Lookalike spelling:** an extra letter, missing hyphen, substituted digit, or different top-level domain.
- **Misleading subdomains:** a trusted name appears before the attacker's real domain.
- **A familiar name in the path:** everything after the hostname can be written by that site's owner.
- **Unusual characters:** internationalized domains are legitimate, but visually similar characters can support impersonation.
- **A shortened link:** the destination is hidden until it redirects. Open the known official site for sensitive accounts.
- **An IP address or unexpected port:** not automatically malicious, but unusual for a public login or payment page.
- **Browser warnings:** do not bypass certificate, deceptive-site, or download warnings.

04 HTTPS is not proof that a site is trustworthy

HTTPS protects the connection to the hostname shown in the address bar. It helps prevent someone on the network from reading or modifying that traffic. It does not prove that the organization behind the hostname is honest. A phishing site can also use HTTPS and show a normal connection indicator.

Check both conditions: the connection should not show a security warning, and the domain must be the exact domain you intended to visit.

05 Five checks before entering sensitive information

1. **Expose the address bar.** Exit full-screen mode or reveal hidden browser controls.
2. **Expand the URL.** Click or tap the field so the browser shows more of the address.
3. **Identify the real domain.** Verify the hostname in browser chrome, not an address printed inside the page.
4. **Use a known route.** For banking, email, cloud storage, or account recovery, type the saved address, use a trusted bookmark, or open the official app.
5. **Stop on a mismatch.** Do not enter a password, card, recovery code, or MFA code. Contact the organization through a separately verified channel.

06 Address bar versus search box

In Chrome and many other browsers, one field performs both jobs. A search result page is not the address bar. Ads and result titles can point to a different domain than their visible text suggests. After opening a result, verify the final destination in the address bar.

07 What if the address bar is missing or looks fake?

A web page can draw an image resembling a browser window, but that drawing is not the trusted browser interface. Leave full-screen mode, switch tabs, or open the browser menu to reveal the real controls. On mobile, scrolling upward usually restores them. If a popup prevents you from leaving, close the tab or browser without interacting with the page.

08 Frequently asked questions

Can a website change the address bar?

A site can update its path, query, or fragment under browser rules and can redirect elsewhere. It cannot silently become the owner of a different domain. Recheck the hostname after a redirect or login handoff.

Does a padlock mean the website is safe?

No. It indicates an encrypted connection to the displayed hostname without a certificate error. You still need to confirm that the hostname belongs to the intended service.

Why does the browser hide part of the URL?

Browsers simplify long addresses to emphasize useful information. Click or tap the field to reveal more. On a small screen, inspect the hostname before entering sensitive data.

09 References

- MDN: What is a URL?
- Chromium: Guidelines for URL Display
- Google Chrome Help: Search the web in Chrome
- Caltech: How to read a website address

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