U

URL Hijacking: Redirects, Look-Alike Links, Diagnosis, and Prevention

URL hijacking is an ambiguous term for techniques that send a user to an unintended destination. Finding where the URL changed is essential to fixing the correct layer.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

URL hijacking is an informal, ambiguous term for techniques that cause a user, browser, application, or search visitor to reach an unintended destination. It can describe a deceptive link, abused redirect, changed browser setting, compromised site, DNS manipulation, or look-alike domain. These are different problems and should not be diagnosed from the final page alone.

Different ways a destination changes

- **Look-alike domain or typosquatting:** a separate domain resembles the intended spelling. No technical redirect is required.
- **Open redirect:** a trusted site accepts an unvalidated destination parameter and forwards the browser to an attacker-chosen URL.

- **Compromised website or advertising chain:** injected code, a plugin, tag, or ad redirects selected visitors.
- **Browser hijacking:** an extension, policy, application, or sync account changes search, startup, new-tab, proxy, or notification behavior.
- **DNS, hosts-file, router, or proxy manipulation:** name resolution or traffic routing sends multiple browsers or devices elsewhere.
- **Search or canonical abuse:** deceptive advertising or site configuration causes users or crawlers to choose the wrong page; this is distinct from browser malware.

Warning signs

- the registered domain differs by a character, word, public suffix, or internationalized character;
- a trusted domain appears at the start of a long link but the final hostname is unrelated;
- redirects occur only from one search result, ad, device, browser profile, account, network, region, or referrer;
- search, new-tab, proxy, DNS, hosts, extension, policy, or router settings changed unexpectedly;
- the destination requests credentials, payment, notifications, software, or remote access with urgency.

HTTPS does not prove that the domain belongs to the brand it resembles. A certificate secures the connection to the hostname shown.

Find where the destination changed

1. **Record without signing in.** Preserve the original link, visible text, referrer, timestamp, redirect chain, final hostname, screenshots, and affected network.

2. **Compare scope.** Test an approved clean browser profile, another device, and another network without repeatedly visiting a dangerous destination.
3. **Inspect the browser layer.** Review extensions, notification permissions, search provider, startup pages, managed policies, proxy, service workers, and sync.
4. **Inspect the system and network.** Check applications, startup items, hosts file, DNS, VPN, certificates, router settings, and management profiles.
5. **For a website you operate:** review redirects, application and web-server code, CMS plugins, tags, advertising, DNS, CDN, deployment history, access logs, and administrator accounts.

User response

Close the destination and open the intended service from a saved bookmark or independently typed official address. If credentials were entered, change them on the real service from a clean device, revoke sessions, and review MFA and recovery settings. Contact the financial provider if payment data was submitted. Scan the device if a file, app, profile, certificate, or extension was installed.

Remove the specific cause rather than adding a broad security exception. If browser sync or organizational policy restores a setting, correct it at the source.

Developer and site-owner defenses

- avoid user-controlled redirect destinations; use server-side identifiers mapped to known internal paths;
- when external redirects are required, parse and allowlist exact schemes and destinations and reject userinfo, protocol-relative, encoded, and nested bypasses;
- do not rely on string prefixes such as `startsWith` for URL trust decisions;
- protect DNS, registrar, CDN, CMS, advertising, analytics, and deployment accounts with phishing-resistant MFA and change monitoring;

- monitor new look-alike domains and report phishing with evidence to providers and protection services.

OWASP defines an open redirect as forwarding users to a URL supplied through an unvalidated parameter and documents common validation bypasses.

URL hijacking FAQ

Is URL hijacking the same as typosquatting?

No. Typosquatting uses a separate look-alike domain. “URL hijacking” may refer to it, but also to redirects, browser changes, DNS attacks, or search issues.

Why does the redirect affect only some users?

Malicious code and ad chains may target referrer, device, region, cookies, or time to evade review. Compare preserved evidence across conditions.

> **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**