D

DNS Hijacking: Types, Detection, Fixes, and Prevention

DNS hijacking redirects name lookups by changing a device, router, resolver, or domain configuration. Diagnose the affected layer before changing settings.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

DNS hijacking is unauthorized manipulation of Domain Name System resolution or control so that a domain returns an attacker-chosen destination. A victim can type the correct domain and still reach a fake login page, advertising redirect, or malware site.

Do not confuse this with DNS rebinding. In a rebinding attack, an attacker-controlled name changes its answer so a browser or application may reach an internal service; recovery and prevention depend on identifying which DNS-related mechanism is involved.

The term is often used loosely. Finding the affected layer is essential because flushing one computer's cache will not repair a compromised router or domain account.

Four common types of DNS hijacking

- **Local device hijacking:** malware or unwanted software changes DNS, proxy, VPN, hosts-file, or browser settings.

- **Router hijacking:** an attacker changes router DNS or DHCP configuration, affecting devices that obtain settings from it.
- **Resolver or cache manipulation:** a recursive DNS service returns or caches a fraudulent answer. DNS cache poisoning is one technique in this category.
- **Domain or authoritative DNS hijacking:** an attacker takes over a registrar, DNS-provider, nameserver, API key, or administrator account and changes real records or delegation.

DNS spoofing commonly means forging DNS responses, while DNS hijacking emphasizes unauthorized control or redirection. Pharming describes the resulting redirection of users to fraudulent sites.

Possible warning signs

- certificate errors or an unexpected site for a correctly typed domain;
- search, advertising, or login redirects across several browsers;
- unknown DNS server addresses in a device or router;
- multiple devices fail only on one network;
- unapproved nameserver, DNS-record, registrar, or administrator changes;
- DNS monitoring shows a sudden address, delegation, or DNSSEC change.

Different IP addresses are not automatically malicious: CDNs, load balancing, location, and IPv4/IPv6 can legitimately change answers.

How to diagnose the affected layer

1. **Record evidence.** Save the complete hostname, time, network, returned address, certificate warning, and security alerts.
2. **Compare devices.** One affected device points toward local configuration; every device on one LAN points toward the router or supplied resolver.

3. **Compare a trusted network and resolver.** If independent networks receive the same bad authoritative data, notify the domain owner and investigate registrar and DNS-provider access.

4. **Inspect configuration.** Check DNS and DHCP values, proxy and VPN profiles, hosts files, browser policies and extensions, router remote management, and recent firmware or account changes.

The UK government's DNS hijacking guidance similarly separates local, router, and server-side cases.

How to fix DNS hijacking

- **Device:** isolate it, remove malicious software, restore approved DNS, proxy and hosts-file settings, then update and rescan.
- **Router:** update firmware, change the administrator password from a clean device, disable internet management, review DHCP/DNS and forwarding, and factory-reset if integrity is uncertain.
- **Resolver:** switch to an approved trusted resolver while the provider investigates. Flush caches only after the underlying source is corrected.
- **Domain:** secure registrar and DNS accounts, revoke sessions and API tokens, correct delegation and records, restore DNSSEC carefully, and monitor propagation.

After redirection is fixed, reset credentials entered at the fraudulent destination from a clean device and revoke sessions. Contact financial providers if payment details were submitted.

Prevention

Use unique administrator credentials and strong MFA, patch routers and DNS software, restrict management interfaces, protect registrar and DNS APIs, log record changes, and segment network infrastructure. DNSSEC validates signed DNS data and is recommended by the Canadian Centre for Cyber Security, but it does not repair a compromised endpoint or registrar account. DoH or DoT encrypts DNS transport; it does not make a malicious resolver honest.

DNS hijacking FAQ

Will changing to public DNS fix everything?

No. It may bypass a bad resolver, but malware, router compromise, or authoritative record changes still require remediation.

Does HTTPS prevent DNS hijacking?

It can expose a mismatch through a certificate warning, but users can still be redirected and look-alike domains can have valid certificates.

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