P

Pharming Attack: Meaning, Examples, Detection, and Prevention

Pharming manipulates name resolution so a correctly typed domain can lead to a fake site. Learn how to identify the affected layer and recover safely.

PUBLISHER
Gridinsoft Support

UPDATED
Aug 28, 2026

READ TIME
4 min

Pharming is a cyberattack that redirects traffic from an intended website to a fraudulent destination by manipulating how a domain name is resolved. A victim may type the correct address or use a trusted bookmark and still reach an attacker-controlled page.

The fake site usually imitates a bank, email provider, store, or company portal to steal credentials and payment details or deliver malware. MITRE CAPEC tracks pharming as CAPEC-89.

Pharming vs. phishing and DNS hijacking

- **Phishing** persuades a person to follow a deceptive link, attachment, QR code, or message.
- **Pharming** changes the route to a destination, so no deceptive link may be required.
- **DNS hijacking** is a broader technical category in which DNS configuration or control is changed. Pharming is one malicious outcome of that manipulation.

- **Typosquatting** uses a look-alike domain. It can imitate the same site but does not require compromised name resolution.

A padlock does not settle the question. HTTPS confirms an encrypted connection to the hostname shown by the browser; it does not prove that the hostname is the one you intended.

How a pharming attack works

- **Device-level change:** malware alters a hosts file, DNS setting, proxy, or browser configuration.
- **Router compromise:** an attacker changes the DNS servers distributed to every device on a home or office network.
- **Resolver or cache manipulation:** a recursive DNS service returns a fraudulent address.
- **Authoritative DNS or domain-account compromise:** an attacker changes real zone records or nameserver delegation, affecting users across networks.

Possible signs of pharming

- a familiar site suddenly looks different or asks for unusual information;
- certificate warnings appear for a correctly typed domain;
- the same redirect occurs on several devices using one router;
- router DNS or administrator settings changed unexpectedly;
- the domain resolves to different addresses on the affected network and a trusted comparison network.

None of these signs alone proves pharming. Websites use CDNs and legitimately return different IP addresses. Compare the complete hostname, certificate, DNS provider information, and results from more than one trusted resolver.

How to find the affected layer

1. **Stop entering information.** Save the full URL, time, screenshot, and certificate warning without interacting further.
2. **Compare another device and network.** If only one device redirects, inspect that device. If all devices behind one router redirect, inspect the router and DHCP-provided DNS. If independent networks see the result, the domain owner should investigate authoritative DNS and registrar access.
3. **Check configuration.** Review DNS servers, proxy settings, the hosts file, browser extensions, installed apps, and router administration logs.
4. **Scan for malware.** Use an updated security tool. A DNS change may be only one action performed by the infection.

Fix and recover

- Remove confirmed malware before restoring DNS and proxy settings.
- Update router firmware, replace the administrator password, disable internet-facing administration, and factory-reset the router if control cannot be trusted.
- Domain owners should secure registrar and DNS-provider accounts, revoke sessions and API keys, enable strong MFA and registry lock where supported, then correct records.
- After the route is trustworthy, change credentials entered on the fake site from a clean device, revoke sessions, and contact the bank if payment data was exposed.

How to reduce pharming risk

Keep endpoints and routers updated, protect router and registrar accounts with unique credentials and MFA, and monitor DNS changes. DNSSEC helps validate signed DNS data but does not fix malware or a maliciously configured endpoint. Encrypted DNS can reduce tampering in transit but cannot make an untrusted resolver trustworthy.

Pharming FAQ

Does pharming require clicking a link?

No. That is the defining danger: correct typing or a bookmark may still be redirected.

Will clearing the DNS cache fix it?

Only if a stale poisoned cache is the cause. It will not repair malware, router settings, or authoritative DNS records.

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