P

Pharming: How traffic is redirected to fake websites

What it is Pharming is an attack that redirects a user from an intended website to a fraudulent one, often to steal credentials or payment information. Unlike ordinary phishing, it may not require the victim to click a deceptive link...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 19, 2026

READ TIME
2 min

What it is

Pharming is an attack that redirects a user from an intended website to a fraudulent one, often to steal credentials or payment information. Unlike ordinary phishing, it may not require the victim to click a deceptive link. The address can be typed correctly while compromised name resolution sends the browser elsewhere.

How it works

Attackers may change a device's hosts file or DNS settings, compromise a router, poison DNS data, or attack a DNS provider. The fake site imitates the expected service and captures information entered by the victim. HTTPS warnings may appear, but a sophisticated attacker can also use a valid certificate for a lookalike domain.

Key points

- Phishing manipulates the user into choosing a fake destination; pharming manipulates how the destination is resolved.
- Several devices showing the same redirect can point to a router or DNS-level problem.
- A padlock confirms encryption to the displayed domain, not that the domain itself is the intended one.

What to do

- Stop entering credentials and compare the full hostname and certificate details.
- Check DNS, proxy, hosts-file, and router settings from a trusted device.
- Update router firmware, replace default admin credentials, and use a trusted DNS resolver.
- Reset exposed passwords and revoke sessions after the redirection path is fixed.

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