3. PHARMING / DNS HIJACK

Pharming redirects users to a malicious website even when they type the correct URL into their browser.

Instead of relying on fake links, attackers tamper with the systems that guide your device to the right website.

Attackers can corrupt:

* DNS servers so the domain lookup points to the attacker’s site

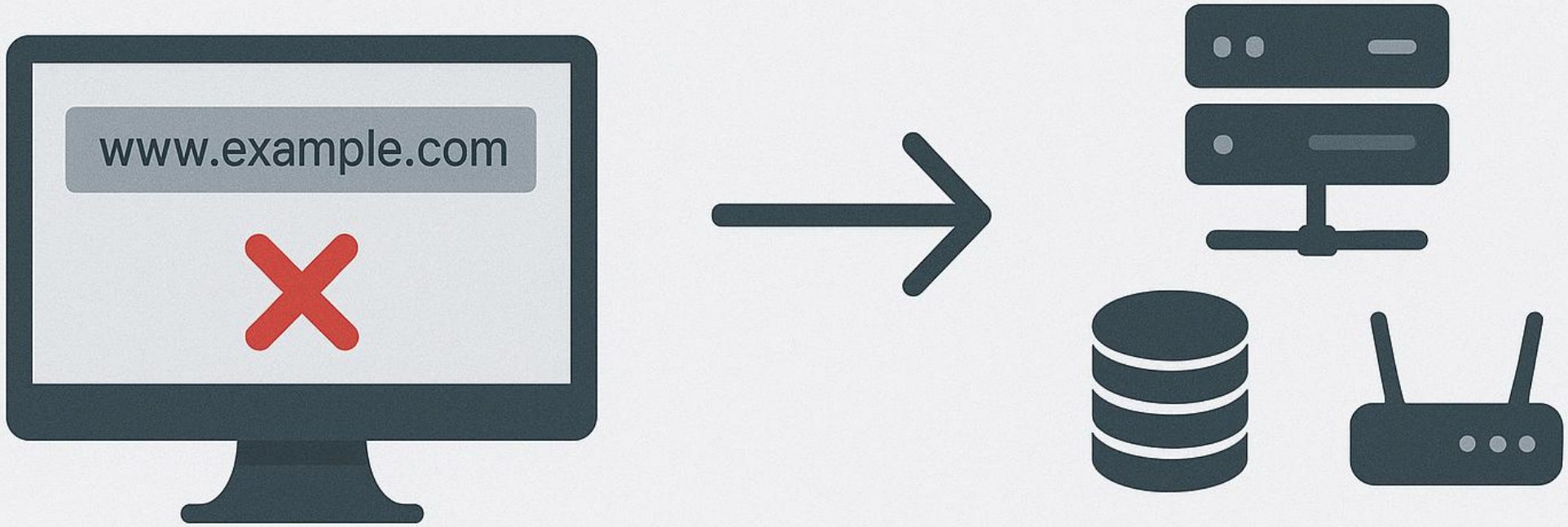
* Home or office routers by changing their DNS settings

* The local DNS cache on a user’s computer, forcing it to load the wrong site

Because the user enters the correct address but still lands on a fake page, pharming can be very difficult to detect.

What Is Pharming?

Pharming redirects users to a malicious site
even if the URL typed is correct



Attackers corrupt:

- DNS server
- Router

Scenario: Hassan Visits “facebook.com” But Lands on a Fake Page

Hassan types facebook.com manually, expecting the real site.

But because his router’s DNS settings were compromised, he is silently redirected to a lookalike phishing page.

Believing it’s genuine, he enters his login details, which the attacker captures instantly.

Lesson: If trusted sites behave strangely or load unexpected pages, check your router’s DNS settings and avoid entering any credentials until the issue is verified.


facebook
facebook.com
Log in
Email or phone
Password
Log In

How Pharming Happens?

- Malware changes DNS settings
- ISP DNS hacked
- Home router compromised
- Host file modified in system

Detecting DNS Hijacking

- Website layout looks slightly off
- SSL certificate missing
- Random redirects
- Multiple sites behaving strangely

Prevention Tips

- Keep router firmware updated
- Use secure DNS (1.1.1.1 / 8.8.8.8)
- Use DNS-over-HTTPS
- Report unusual redirects immediately