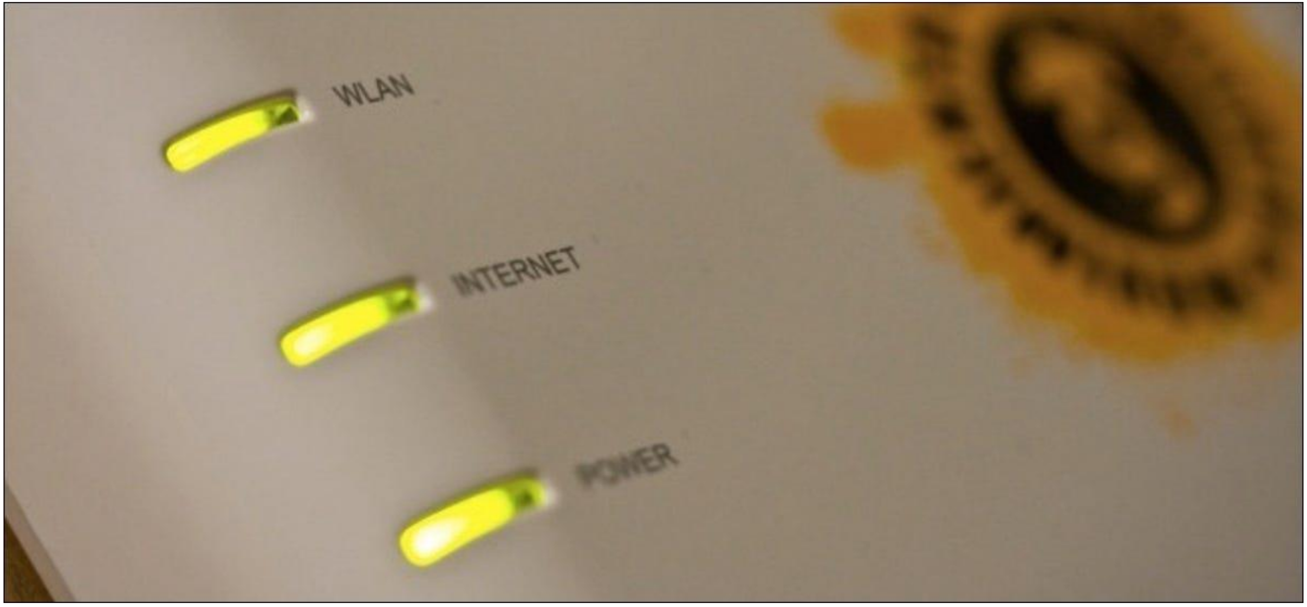
How to Check Your Router for Malware

CHRIS HOFFMAN

If you got your router from your ISP call them and tell them you think you have been hacked and have them check your DNS server setting. If you have your own router then type 192.168.1.1 into the browser bar and the user name and password for the browser.

@CHRISBHOFFMAN

UPDATED JUL 10, 2017, 3:44 PM EDT | 4 MIN READ



Consumer router security is pretty bad. Attackers are taking advantage of lackadaisical manufacturers and attacking large amounts of routers. Here’s how to check if your router’s been compromised.

The home router market is a lot like the Android smartphone market. Manufacturers are producing large numbers of different devices and not bothering updating them, leaving them open to attack.

0 seconds of 1 minute, 20 secondsVolume 0%

How Your Router Can Join the Dark Side

RELATED: ***What Is DNS, and Should I Use Another DNS Server?***

Attackers often seek to change the DNS server setting on your router, pointing it at a malicious DNS server. When you try to connect to a website — for example, your bank's website — the malicious DNS server tells you to go to a phishing site instead. It may still say bankofamerica.com in your address bar, but you'll be at a phishing site. The malicious DNS server doesn't necessarily respond to all queries. It may simply time out on most requests and then redirect queries to your ISP's default DNS server. Unusually slow DNS requests are a sign you may have an infection.

Advertisement

Sharp-eyed people may notice that such a phishing site won't have HTTPS encryption, but many people wouldn't notice. SSL-stripping attacks can even remove the encryption in transit.

Attackers may also just inject advertisements, redirect search results, or attempt to install drive-by downloads. They can capture requests for Google Analytics or other scripts almost every website use and redirect them to a server providing a script that instead injects ads. If you see pornographic advertisements on a legitimate website like How-To Geek or the New York Times, you're almost certainly infected with something — either on your router or your computer itself.

Many attacks make use of cross-site request forgery (CSRF) attacks. An attacker embeds malicious JavaScript onto a web page, and that JavaScript attempts to load the router's web-based administration page and change settings. As the JavaScript is running on a device inside your local network, the code can access the web interface that's only available inside your network.

Some routers may have their remote administration interfaces activated along with default usernames and passwords — bots can scan for such routers on the Internet and gain access. Other exploits can take advantage of other router problems. UPnP seems to be vulnerable on many routers, for example.

How to Check

RELATED: ***10 Useful Options You Can Configure In Your Router's Web Interface***

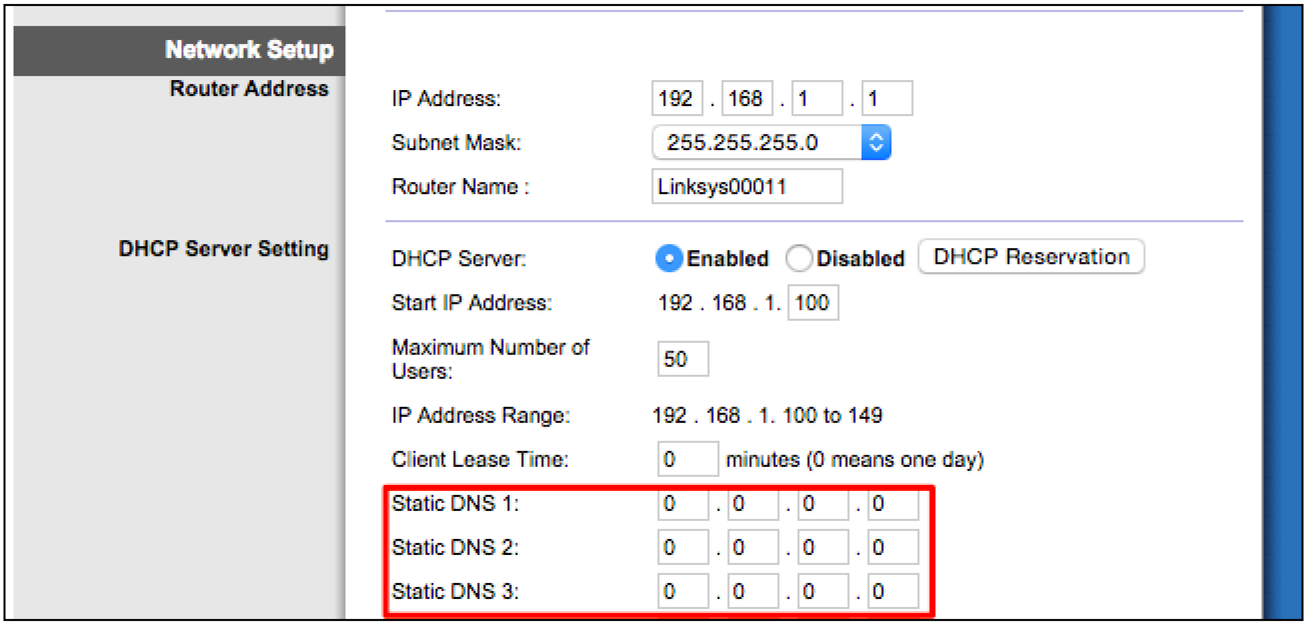
The one telltale sign that a router has been compromised is that its DNS server has been changed. You'll want to visit your router's web-based interface and check its DNS server setting.

First, you'll need to access your router's web-based setup page. Check your network connection's gateway address or consult your router's documentation to find out how.

Sign in with your router's username and password, if necessary. Look for a "DNS" setting somewhere, often in the WAN or Internet connection settings screen. If it's set to "Automatic," that's fine — it's getting it from your ISP. If it's set to "Manual" and there are custom DNS servers entered there, that could very well be a problem.

It's no problem if you've configured your router to use good alternative DNS servers — for example, 8.8.8.8 and 8.8.4.4 for Google DNS or 208.67.222.222 and 208.67.220.220 for OpenDNS. But, if there are DNS servers there you don't recognize, that's a sign malware has changed your router to use DNS servers. If in doubt, perform a web search for the DNS server addresses and see whether they're legitimate or not. Something like "0.0.0.0" is fine and often just means the field is empty and the router is automatically getting a DNS server instead.

Experts advise checking this setting occasionally to see whether your router has been compromised or not.



Network Setup

Router Address

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

Router Name : Linksys00011

DHCP Server Setting

DHCP Server: ● Enabled ○ Disabled DHCP Reservation

Start IP Address: 192 . 168 . 1. 100

Maximum Number of Users: 50

IP Address Range: 192 . 168 . 1. 100 to 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0 . 0 . 0 . 0

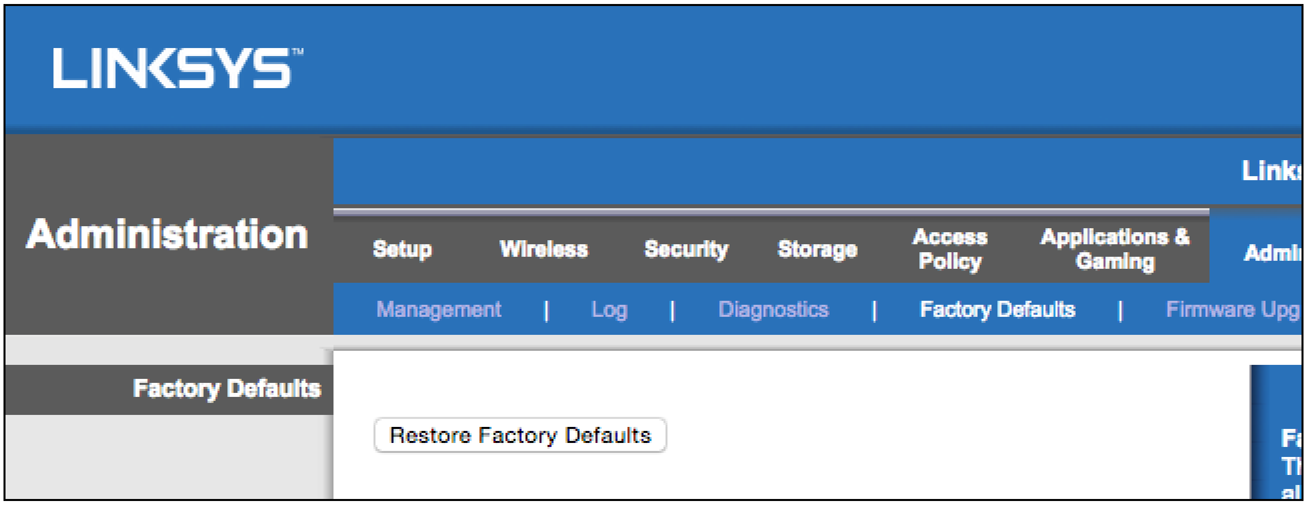
Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

Help, There' a Malicious DNS Server!

If there is a malicious DNS server configured here, you can disable it and tell your router to use the automatic DNS server from your ISP or enter the addresses of legitimate DNS servers like Google DNS or OpenDNS here.

If there is a malicious DNS server entered here, you may want to wipe all your router's settings and factory-reset it before setting it back up again — just to be safe. Then, use the tricks below to help secure the router against further attacks.

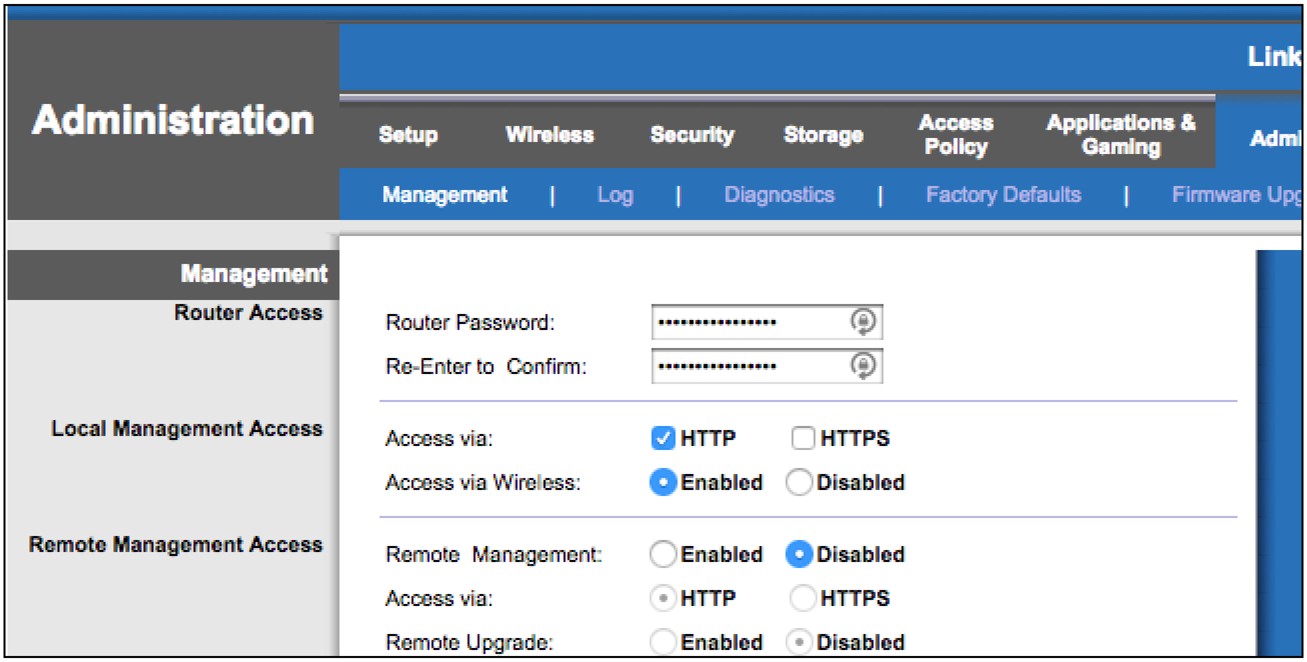


Hardening Your Router Against Attacks

RELATED: ***Secure Your Wireless Router: 8 Things You Can Do Right Now***

You can certainly harden your router against these attacks — somewhat. If the router has security holes the manufacturer hasn't patched, you can't completely secure it.

- **Install Firmware Updates**: Ensure the latest firmware for your router is installed. Enable automatic firmware updates if the router offers it — unfortunately, most routers don't. This at least ensures you're protected from any flaws that have been patched.
- **Disable Remote Access**: Disable remote access to the router's web-based administration pages.
- **Change the Password**: Change the password to the router's web-based administration interface so attackers can't just get in with the default one.
- **Turn Off UPnP**: UPnP has been particularly vulnerable. Even if UPnP isn't vulnerable on your router, a piece of malware running somewhere inside your local network can use UPnP to change your DNS server. That's just how UPnP works — it trusts all requests coming from within your local network.



Management

Router Access

Router Password: ••••••••••••••••

Re-Enter to Confirm: ••••••••••••••••

Local Management Access

Access via: ☑ HTTP ☐ HTTPS

Access via Wireless: ● Enabled ○ Disabled

Remote Management Access

Remote Management: ○ Enabled ● Disabled

Access via: ○ HTTP ○ HTTPS

Remote Upgrade: ○ Enabled ○ Disabled

DNSSEC is supposed to provide additional security, but it's no panacea here. In the real world, every client operating system just trusts the configured DNS server. The malicious DNS server could claim a DNS record has no DNSSEC information, or that it does have DNSSEC information and the IP address being passed along is the real one.