Can the router be infected with a virus?

A router is just as susceptible to a virus as a computer. A common reason why the router becomes infected with a virus is that the owner forgot to change the default admin password.

How can a router be infected with virus?

The router can get a virus if an attacker enters the initial login screen and modifies the router settings. In some cases, the virus can modify the firmware of the embedded router firmware.

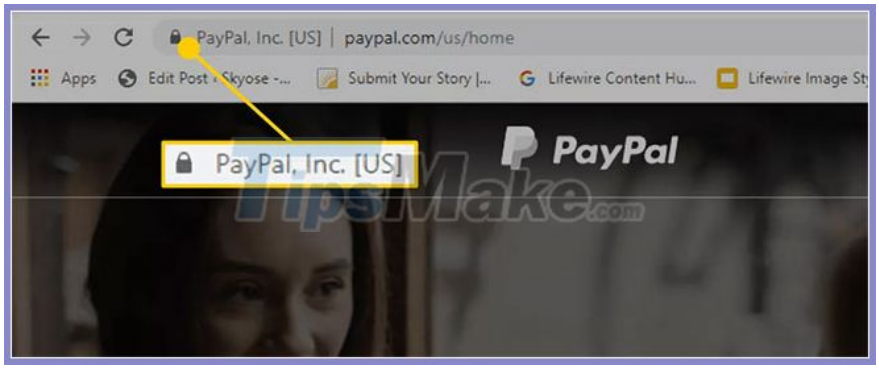
You do not need to throw away an infected router. Just repair and then protect the router from future virus infections.

Two common viruses that have infected thousands of routers in the past are **Trojan Switcher** and **VPNFilter** .

Is my router infected with a virus?

If the following behavior is happening on your network, chances are your router has been infected.

1. When you visit websites that need security (like Paypal or banks), but don't see a padlock in the URL field, you may have been infected. Every financial institution uses secure HTTPS protocol. If you don't see the lock icon, your activities on that website are not encrypted and can be viewed by hackers.



See if web pages that need security have a padlock icon in the URL
2. Over time, malware can consume computer CPUs and slow down performance. Malware running on your computer or router can cause this behavior. Combined with the other behaviors listed, it's possible that the router was infected with a virus.

3. If after scanning and cleaning malware, as well as viruses on your computer, you still see a pop-up ransomware window asking for payment, otherwise your files will be destroyed, then it is the Good signal indicates that the router is infected with a virus.

Ransomware pop-up window requires payment
4. When you visit normal websites but are redirected to strange websites without you realizing it, it could indicate that the router is infected. Sometimes those pages can be fake pages that look similar to the real one.

Note : If you are redirected to websites that don't appear to be doing well, never click any links or enter account login details.

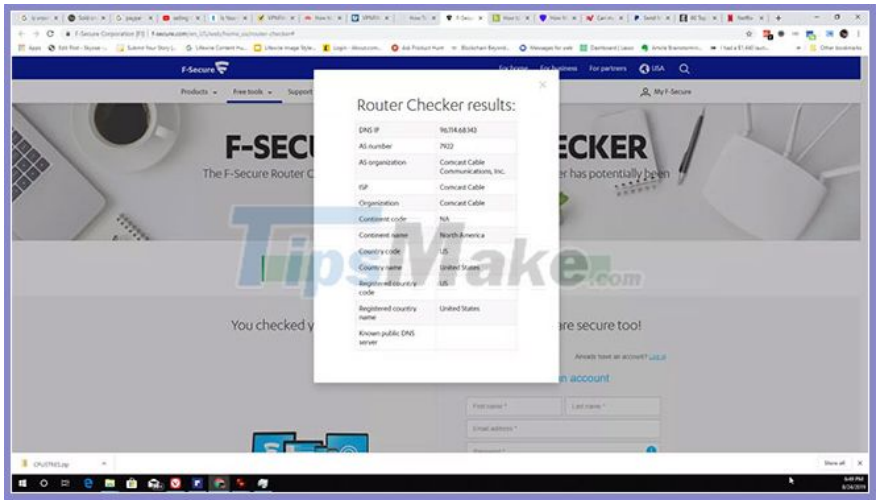
Instead, take steps to determine if the virus is causing the behavior.

5. If you click on a Google search link and go to an unwanted website (which doesn't look right), it could be another sign that the router is infected with malware.

How to fix a router infected with a virus

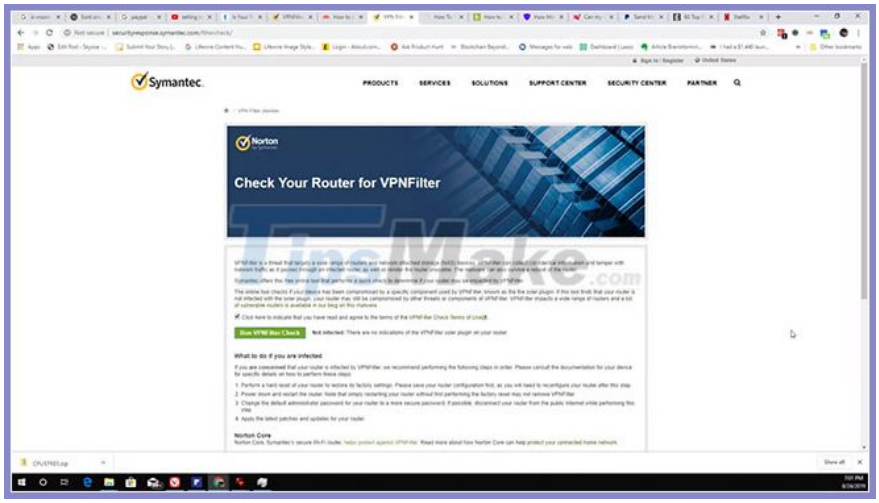
To check if your router is infected with a virus, scan it with available online tools. There are many of these tools available, but choose one that comes from a known and reliable source. One option worth considering is F-Secure, which will scan the router and determine if a virus has attacked the router's DNS settings.

If the router is 'clean', you will see a message with a green background indicating that the router is not infected.



F-Secure

Another option is to scan with Symantec to check specifically for the VPNFilter Trojan. To run the scan, select the check box indicating that you agree to the terms, and then select **Run VPNFilter Check** .



Select Run VPNFilter Check to scan the router

Important Note : Always read the Terms of Service and Privacy Agreement carefully. At times, a tool may be opaque about how it collects and uses users' personal data.

If any of the scans show that your router is infected with a virus, do the following:

1. Reset the router

In many cases, rebooting the router will not completely clean the infected device. Instead, perform a full router reset. Check the manufacturer's website for factory reset instructions.

1. How to reset the TP-Link WiFi router
2. How to reset Linksys router to factory default settings
3. How to reset WiFi VNPT router

A factory reset completely erases all settings from the router. You will have to reconfigure all settings again, so only perform a factory reset if you are sure that a virus or Trojan has infected the router.

2. Update the firmware

If the ISP provided the router, chances are it will automatically push firmware updates to the router. If you own such a router, visit the manufacturer's website to search for and download the latest firmware update for your router model. This process ensures the router has the latest patches to protect against new viruses.

3. Change the administrator password

To prevent any viruses or Trojans from re-entering the router, immediately change the admin password to a more complex one. Strong passwords are the best protection against a virus infection.

After removing the virus, run a full virus scan on all the devices connected to the infected router.