3 ways hackers can attack home routers

A router is an important source of data transmission in the home. Computers, laptops, tablets and phones all use routers to transfer data to websites worldwide.

A router is an important source of data transmission in the home. Computers, laptops, tablets and phones all use routers to transfer data to websites worldwide. This, naturally, makes the router a lucrative prey for hackers, always wanting to find ways to steal information.

Here are some ways hackers can attack home routers for bad purposes.

How can hackers attack home routers?

1. 1. Put the router into the botnet
    1. How to avoid routers being put into botnets?
2. 2. Perform unauthorized access and use of routers
    1. How to avoid router access and unauthorized use?
3. 3. Change the data going through the router
    1. How to avoid data through the router being changed?

1. Put the router into the botnet

ZDNet.com has reported that hackers will infect the botnet into a home router, which will then be used in DDoS attacks against web servers. Users infected with malware may not even realize that their routers are being used in such digital attacks.

The botnet case is very special, because the fix is ??very simple: Just restart the router. However, most people never touch the router unless there is a connection problem, meaning that the malware has not been removed for

a long time.

How to avoid routers being put into botnets?

If you are worried about your router being taken into the botnet, be sure to regularly update the router's firmware. You may need to see the router user guide to learn how to do this. Besides, regularly restart the router to make sure nothing is hidden inside.

2. Perform unauthorized access and use of routers

Because routers are data centers for homes, they become the main target of hackers. Thus, if hackers have access to the router, they can track or steal when data passes. If you have IoT devices or network drives connected, hackers can access them if you don't set the appropriate password.

This may sound scary, but less likely to happen. Ideally, hackers will be in the WiFi range of the router, which means they must be quite close together.

This will not be a major concern if you live in a rural area. However, if you live in a city or apartment complex, you can see that the home computer captures many different WiFi networks.

How to avoid router access and unauthorized use?

If you live in a densely populated area, protect your device properly. Many modern routers have abandoned the old standard, using both the default username and password **'admin',** but should also check to see if the router's password is compromised.

Also check to see if the firmware is up to date. Otherwise, hackers can hack into the router without any username or password!

3. Change the data going through the router

If hackers do not want to access the router or use it for their own needs, they can redirect users to fake websites. This phenomenon is called poisoning or DNS spoofing and involves changing the router's DNS cache, then bringing users to the site incorrectly.

DNS cache is like a phone book for the Internet. It stores the names and IP addresses of all the websites you have previously visited. DNS poisoning works by sneaking into this directory and changing the real IP address with a fake address. For example, a hacker can change the **Amazon.com** entry in a DNS cache to redirect it from the real Amazon site and to a fake, designed website that looks like the real thing.

How to avoid data through the router being changed?

When using the Internet, keep a close eye on where you enter detailed information. Typically, websites require login details using an HTTPS certificate to encrypt your login details. A fake site does not have this protection. It is an important sign of awareness if you pay close attention. If you see a router redirecting you to a bad site, try changing the router's DNS.

Router has become a data center for homes in the modern world. This makes them the top target for hackers who are always stalking the opportunity to steal information from victims. Thankfully, there are many ways to stay safe before router-based attacks take place.

When was the last time you restarted the router? What measures have you taken to ensure the safety of your router? Please share your comments in the comment section below!

You finished reading the article "**3 ways hackers can attack home routers**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.