How dangerous is IP address exposure?

You may not know that there is always some danger if someone knows your IP address. Hackers can use your IP address to conduct cyber attacks or scam yourself or others.

TipsMake.com will discuss with you the problem of exposing IP addresses and what hackers can do with an IP address.

In what ways can your IP be exposed?

First we will find out how hackers get your IP address.

1. Borrow your device. If someone borrows and uses your device they can get your IP address in seconds.
2. From an email. If you email someone they can get your IP in the header.
3. Click a link. When you click on a link you need to give your IP address to the server on the other end for it to deliver the content of the link to you. So the owner of the server will know your IP address.
4. Hack your router. Hackers can hack into the router to see your IP.
5. Retrieved from web server. Every time you visit a website your IP address is collected and stored on a web server. Anyone who owns that server can access and view your IP.
6. Click the ad. When you click on the ad you give your IP to the provider. Some online ads are created by hackers and can get you in trouble.
7. Join an online forum. If you participate in a discussion on an online forum, the admin of that forum can see your IP address.
8. Connect to a rogue network access point. Hackers can create fake network access points to deceive users and collect IPs and other information.
9. Activity on social networks. Social networking service providers may also collect your information including your IP address.

What can hackers do with your IP?

Although your IP address does not reveal sensitive information such as phone numbers, home addresses, hackers can still use IP addresses to do some damage to you. If hackers, cybercriminals know your IP, they can do the following things:

1. Figure out your location and invasion of privacy in real life: Your IP address reveals which city you live in. Therefore, bad guys can use it to cause trouble for you. Let's say you share that you are going to travel in the near future on social networks. Bad guys just need to invest, learn a little more to be able to identify your home to break in and steal while you are away.
2. Use IP to hack your device: To connect to the Internet, the system needs to use your ports and IP address. Each IP address will connect through thousands of ports and the hacker who has your IP address can try brute-force attack on all ports to hack the connection. From there, they can take control of your device and

steal other sensitive information from you.

3. Someone can impersonate to obtain, use your IP address: Your network provider (ISP) can expose your IP address to others. Using information collected from social networks, cybercriminals can contact your ISP to impersonate you and then steal personal information.
4. Hackers can do a DDoS attack on your IP address: If a hacker knows your IP, a hacker can annoy you with a DDoS attack. During a DDoS attack, your computer or network may have difficulty accessing the internet or even lose connection to the internet altogether.
5. Hackers can use your IP to perform illegal activities.

How to not expose your IP

To avoid exposing your IP and being exploited by hackers, you can do the following solutions:

1. Change privacy settings

You should change the settings of messaging apps and other apps to private and don't receive texts or calls from people you don't know. By now, almost every hacker knows how to get your IP address from messaging apps like Skype.

2. Update firewall (firewall) and router (network device)

Cybercriminals can hack into your network devices, routers easily if you use default settings or use outdated firmware. Therefore, you need to change the password of the router, network device as well as regularly update the firmware to the latest version.

3. Use VPN

A VPN service can protect your IP address and private information. By directing your data online through a VPN server with a private IP address, you can block websites from accessing your device and location information. However, the downside of this method is that the VPN provider will know your information, so you should use reputable VPN services.

Hope you all stay safe on the internet!

You finished reading the article "**How dangerous is IP address exposure?**" 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.
