

Instructions on Recovering from an IP Address Theft on a Personal Computer



Secure your identity while using your computer online and staying protected after a cyber attack.

Computer Literacy Tutorial Mentor and Presenter: Steven C. Wong

Introduction



Definition of an IP address and why an IP address is important.

What is the definition of an IP address?

- A distinct identifier that enables a computer user's device to connect to the internet.

Why are IP addresses important?

- It connects the computer user's internet activities to the physical address of their device.

What happens if your IP address is stolen?

- Malicious network attacker can masquerade as your device, steal information, and get unauthorized access to accounts.

Signs Your IP Address is Stolen by your Hacker

How to spot an IP theft.

Odd or Suspicious Activity

- Unnecessary and unexplained logins or account modifications.

Slow Network Performance

- Relevant declines in internet speed or connecting to the internet has become a problem.

Security Warning Signs and Symptoms

- Notifications from antivirus applications or web browsers about unusual connections.



Step 1: Take your Hewlett Packard computer off it's internet connection



Why?

- Disconnecting your HP laptop from the internet prevents any continued unauthorized access to your exploited device.

How?

- Disable your Wifi temporarily or unplug your Ethernet Cable
- Turn off your mobile data if it is being used.

Tip: This assists in mitigating risks such as data theft of any further network exploits.

Step2: Get in Contact with your Internet Service Provider for them to issue you a new IP address.

Request a new IP address to replace the stolen one so you can connect to the internet without being vulnerable to cyber attacks.

Why?

- Modifying the IP address makes sure the network exploiter cannot use it to attack your device another time.

How?

- Get in reach of your Internet Service Provider and inquire about a new IP address.
- Reboot your router if your IP address is a dynamic one.
- If you have a static IP address, ask your Internet Service Provider about the manual modification.

Tip: Write down or record your new IP address given to you by your internet provider.

Step 3: Update the security settings of your network router.

Strengthen and harden your personal home network.

Why?

- Weakened router settings can enable network attackers to reconnect to your private network.

How?

- Modify or change the password of your network router to a strong, and hard to guess password.
- Keep your firmware up-to-date and allow a WPA3 encryption.
- Turn off remote management attributes.

Tip: Change and make your default credentials up-to-date as soon as possible.

Step 4: Conduct a cyber security scan of your HP laptop for malicious software like malware and viruses.

Make sure your laptop does not have any malware.

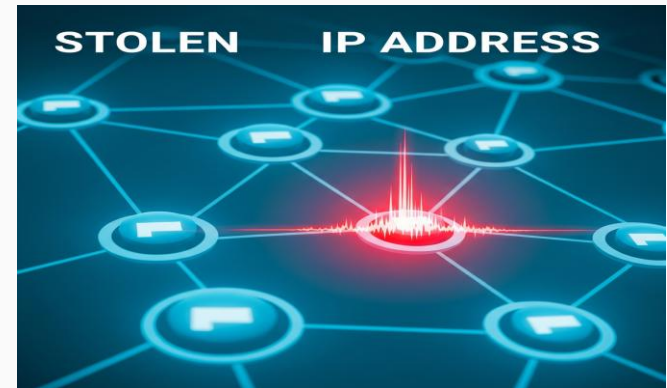
Why?

- Viruses and malware may have been utilized to steal your IP address.

How?

- Conduct a complete information system scan with cyber security software.
- A good software to use is malwarebytes.
- After the scan, delete and identify threats and restart your computer.

Tip: Conduct a routine security scan for additional protection.



Step 5: Modify your Internet passwords for your website accounts.

Secure accounts and stop any other attacks from occurring.

Why?

- Secure your internet website accounts from unwanted access that is in association with the IP address that was stolen.

How?

- Modify passwords for essential accounts (email, financial, and social network websites).
- Turn on two-factor authentication (2FA).
- Utilize a password management software for storage and more complicated passwords.

Tip: Turn on two-factor authentication as soon as possible.

Step 6: Keep surveillance of account and device activities.

Maintain focused monitoring of your devices and accounts.

Why?

- Surveillance helps identify unauthorized activity before the network attack actually happens.

How?

- View email and banking online accounts frequently or routinely for suspicious activity.
- Use surveillance software to stay on target with your accounts and devices.

Tip: Set up notifications for new account logins or exchanges within your account's activities.

Step7: Call law enforcement if deemed appropriate

Report stealing if it is a serious threat to your computer system.

Why?

- To be safe from a situation where there is a theft of your data, or critical incidents are occurring.

How?

- File an online crime report for cyber crime with local law enforcement or national cyber poice teams.
- Report fraud to your financial institution.

Tip: Maintain records of every communication attempt, and exchanges of information.

Utilize a Virtual Private Network to facilitate your computer's internet connection.

An additional level of security is given when you use a VPN

Why?

- A VPN covers your devices real IP address and secures your privacy on the internet.

How?

- Install a VPN service on your computer like ExpressVPN and NordVPN.
- The VPN provides encryption to your internet connection and route your data traffic through the secure server.

Tip: Use a VPN at all times, especially when using a public WiFi connection.

Conclusion

Keep an open eye and secure your internet protection.

Summary of primary objectives: Disconnect from internet, modify your IP address, improve network security, and conduct surveillance on online accounts.

Continuous Protection: Keep the software updated on your computer, use stronger passwords, and use a Virtual Private Network.

Keep a continued awareness: Be aware of phishing and illegal crimes online.

Q and A

Any Questions?

Thanks!

Your
ComputerLiteracy[Tutorials.com](https://www.computerliteracytutorials.com)

Mentor

