How to check if the DNS has been changed by malware

This article helps you find out if your Windows DNS settings have been changed by malware and how to undo those unwanted changes. By default, a user should have the IP and the DNS server addresses assigned automatically. However, some forms of malware can modify these settings, and the user will see random IP and DNS server addresses.

In such cases, it is necessary to change the TCP/IP settings, by following the steps detailed below:

1. Access Network Connections.

For Windows 10 and Windows 11 users:

- Click on the Windows logo in the lower-left corner of the screen.
- Type **View network connections**, and then select **View network connections**.

For Windows 8/8.1 users:

- Click on the Windows logo in the lower-left corner of the screen.
- Type **View network connections**, and then select **View network connections**.

For Windows 7 users:

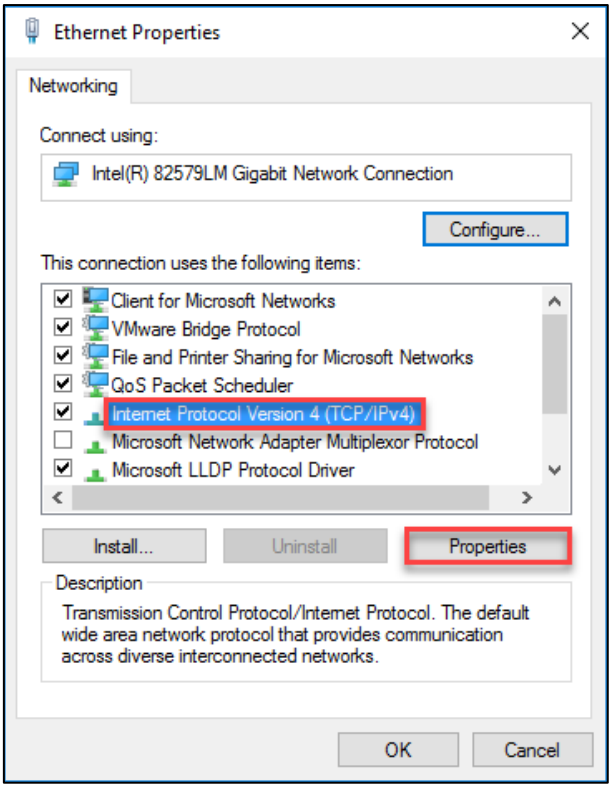
- Click on the Start button and select **Control Panel**.
- In the search box situated in the upper right corner of the windows, type **adapter**.
- After that, select **View network connections**, situated under Network **and Sharing Center**.

2. Right-click on the connection that you wish to modify and select **Properties**.

ⓘ **Note**: In some cases, it is necessary to provide an administrator password or confirmation. If so, simply type the password or provide confirmation.

3. In the Networking tab, under **This connection uses the following items**, click on **Internet Protocol Version 4 (TCP/IPv4)**.
4. Click the **Properties** button.

ⓘ **Note**: Do not uncheck the box next to Internet Protocol Version 4 (TCP/IPv4).



5. Remove any unknown IP addresses, subnet masks, default gateways and DNS servers.
6. Click on **Obtain an IP address automatically**.
7. Click on **Obtain DNS server address automatically**.
8. Click on **OK**.