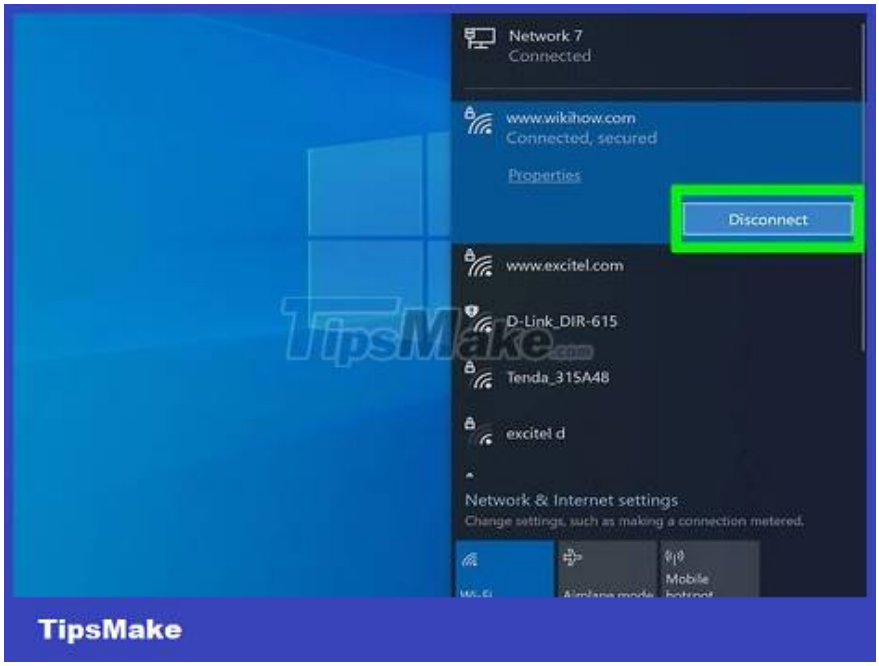
How to Detect Remotely Accessed Computers

Surely there are few things that make you feel as scared as having your personal computer hacked. If you think your computer is being controlled by a hacker, the first thing you should do is disconnect from the network. Once you're offline, you can find and remove the gateway the hacker used to access your system. Once your system is secure, there are several steps you can take to keep your computer from being hacked.

Check for signs of intrusion



Disconnect your computer's network connection. If you believe someone is accessing your computer remotely, disconnect from the network immediately. That means you'll unplug the Ethernet cable and turn off the Wi-Fi network connection.

Some sure signs that your computer is compromised are the mouse moving when you're not using it, applications opening in front of you, or files accidentally being deleted. However, you don't need to worry too much about pop-up ads - many apps with automatic updates can generate pop-ups during the update process.

Slow internet speeds or strange programs are not necessarily signs that your computer is compromised.

Check the list of recently accessed files and applications. Windows and Mac computers both allow you to view a list of recently accessed files and applications. If you see something unusual in these lists, someone has probably hacked your computer. Please check the information in the following way:

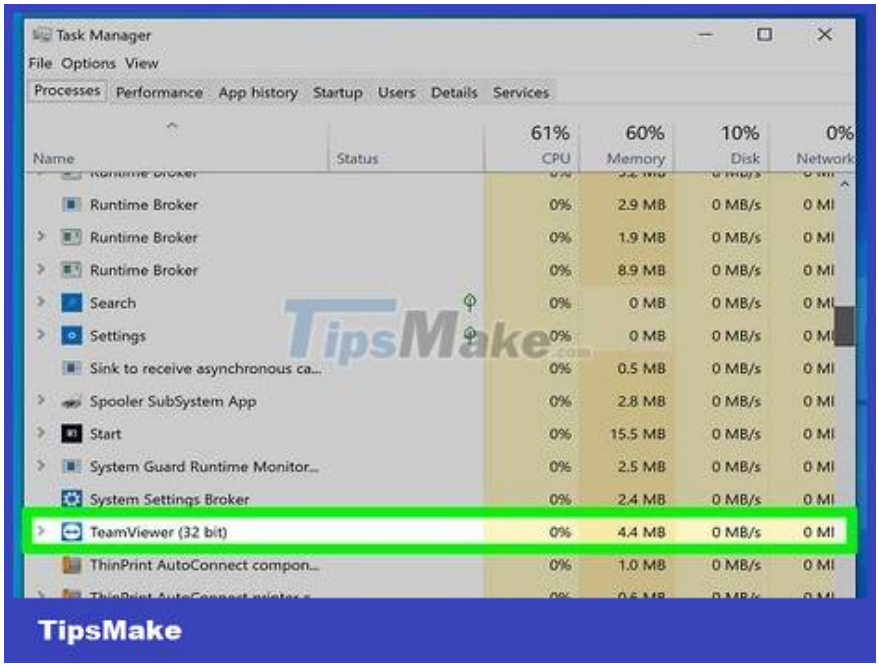
Windows: To view recently opened files, you will press **Windows** key + **E** to open File Explorer. Look at the "Recent files" section at the bottom of the main control panel for any unusual signs. You can also see recently opened apps at the top of the Start menu.

Mac: Click the Apple menu in the top left corner of the screen and choose **Recent Items** . You can click **Applications** to see recently used applications, **Documents** to see files, and **Servers** to see a list of 'out of the box' connections.

Open Task Manager or Activity Monitor. These utilities can tell you what's going on on your computer.

Windows – Press **Ctrl** + **Shift** + **Esc** .

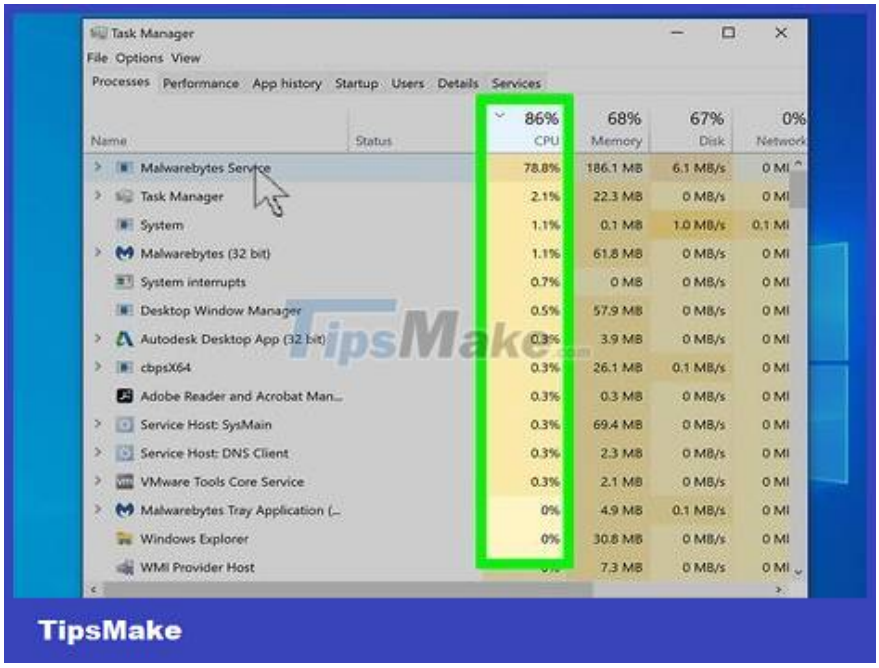
Mac - Open the Applications folder in Finder, double-click the **Utilities** folder , and double-click **Activity Monitor** .



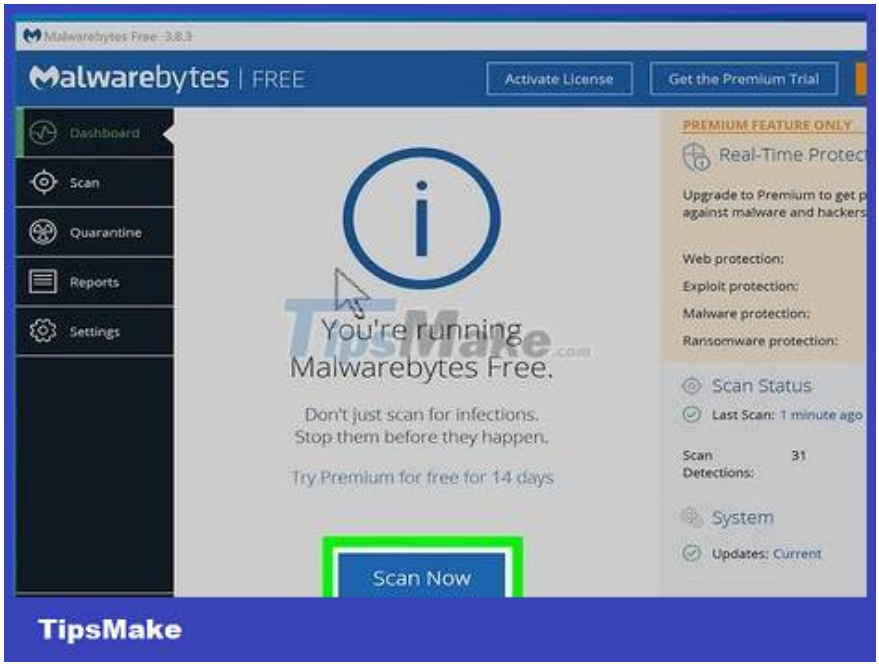
Find the remote access program in the list of active programs. Now that Task Manager or Activity Monitor is open, you will look at the list of active programs to look for strange or suspicious programs. Here are some common remote access programs that may be installed on your computer without your permission:

VNC, RealVNC, TightVNC, UltraVNC, LogMeIn, GoToMyPC and TeamViewer.

Look for programs that seem suspicious or that you've never heard of. You can look up information online if you don't know what program it is.



Watch out for unusually high levels of CPU activity. You will see this information in Task Manager or Activity Monitor. While a high level of CPU activity is not necessarily an unusual sign of an intrusion, if you are not using the computer it indicates that there are many background activities that are beyond your control running. . However, CPU activity also increases when a program is updating or there is a torrent being downloaded that you forgot about.

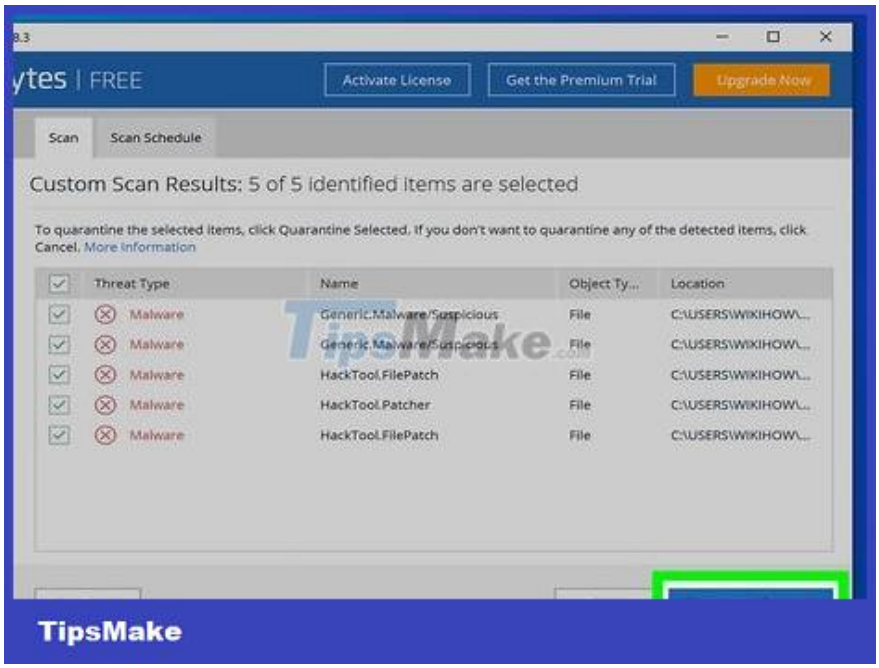


Scan your computer for viruses and malware. If you use Windows 10, you can use the built-in scanning tool in **Settings** > **Update & Security** > **Windows Security** to detect fake applications. If you use a Mac, see instructions for using Mac-specific scanning tools.

Malware is often the easiest way for hackers to get into your personal computer.

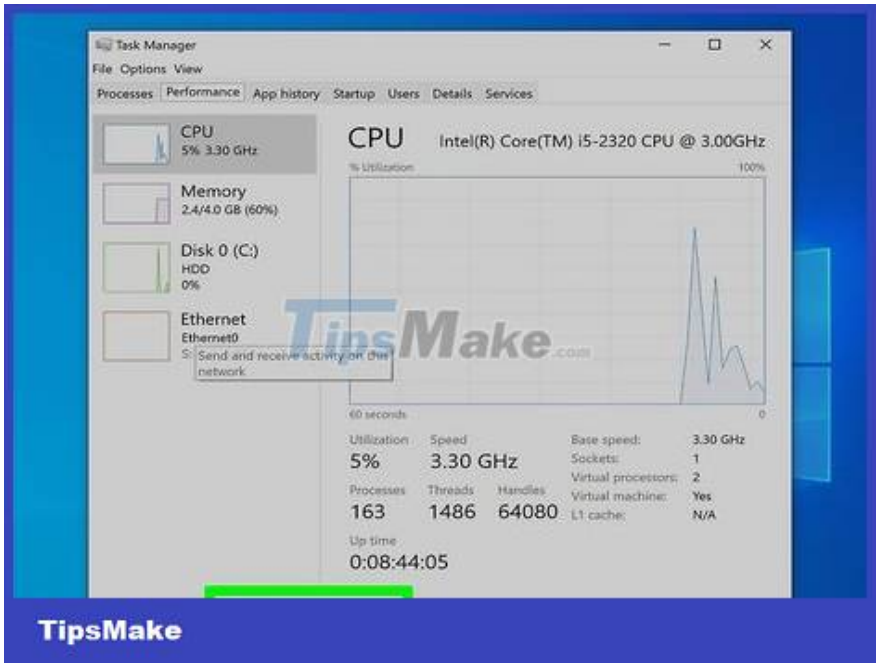
If you don't have anti-virus software, you can download the program using another computer and save it to a USB to transfer to your computer. Install an anti-virus program and scan your computer.

Malwarebytes Anti-Malware is a free third-party anti-malware program that can be used on both Windows and Mac computers. You can download this program for free at https://www.malwarebytes.com.

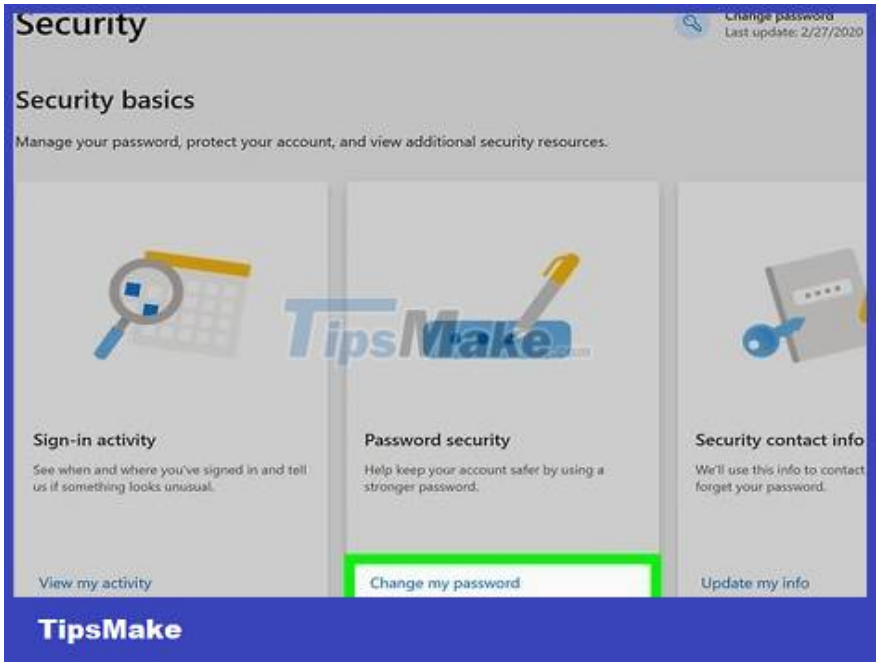


Quarantine found files. If your anti-virus or anti-malware program detects any files during the scan, quarantining them will stop them from affecting the system.

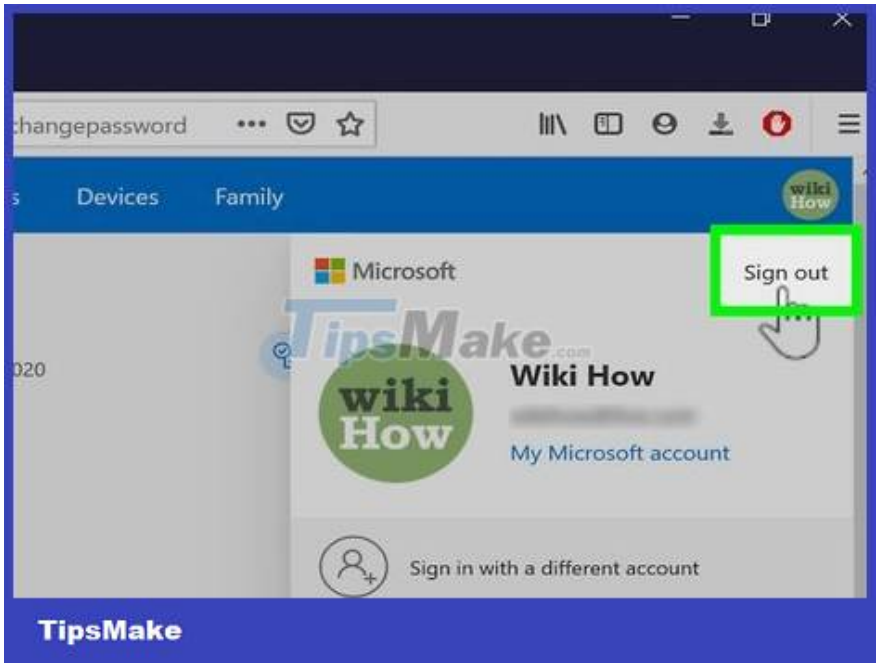
Download and launch the Malwarebytes Anti-Rootkit Beta program. You can download this program for free at https://www.malwarebytes.com/antirootkit. Thus, the program will help you find and remove "rootkits" - harmful programs 'hiding' in your system files. Your computer will be scanned by the program, which may take some time.



Monitor your computer after removing malicious code. If your anti-virus and/or anti-malware program finds malicious programs, you have successfully removed the harmful agent, but you still need to monitor your computer closely to make sure the harmful agent is removed. That damage has been completely erased.



Change all your passwords. If your computer has been compromised, it's possible that all your passwords have been saved by a keylogger. If you're sure the malware is gone, change your passwords for all your accounts. Avoid using the same password for multiple services.



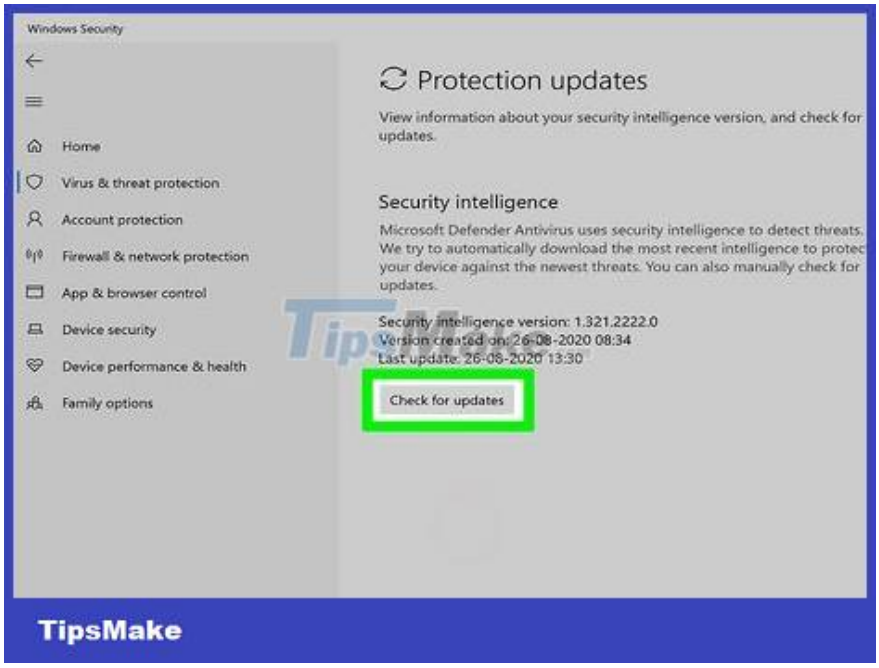
Sign out of all accounts. After changing your password, you'll check each account and log out completely. Remember to log out of that account on all devices. This is to ensure that the new password will be valid and that someone else cannot use the old password.

Delete the entire system if you cannot remove the intrusion. If your computer is still compromised or you think there are still harmful elements, the only way to be sure is to wipe the system and reinstall the operating system. However, you need to back up important data first because everything will be wiped and reset.

When backing up data on an infected computer, remember to scan each file before backing up. Re-importing old files can always cause your computer to be infected again.

See instructions on how to format your Windows or Mac computer and reinstall the operating system.

Prevent future intrusions



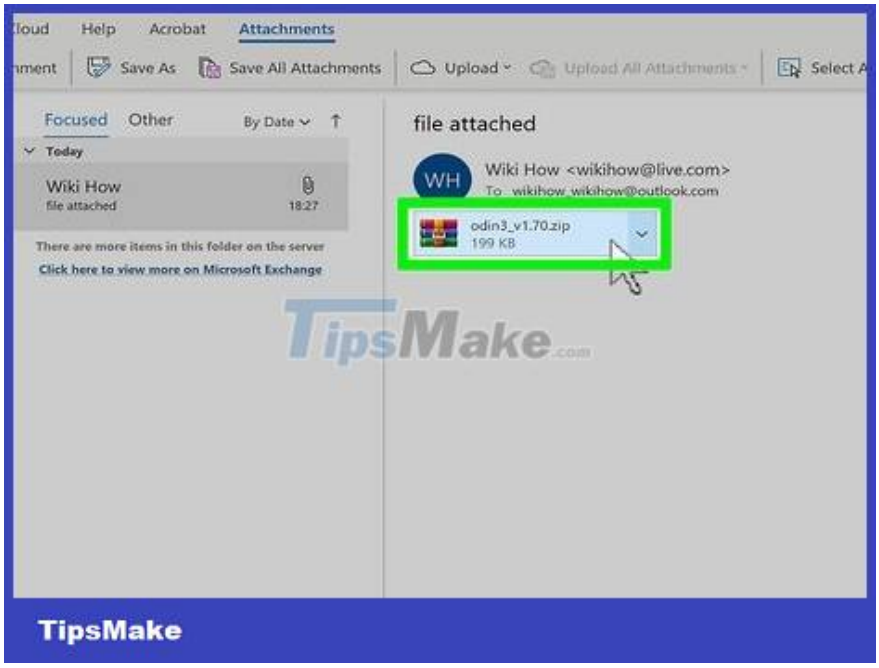
Always keep your anti-virus and anti-malware programs up to date. Updated anti-virus programs will identify most potential attacks. The Windows operating system has a built-in Windows Defender anti-virus program that can automatically update and execute in the background. In addition, you can also find many other free programs such as BitDefender, avast! and AVG. Simply installing an anti-virus program is enough.

See instructions for turning on Windows Defender on a Windows computer.

You can also refer to the instructions for installing another antivirus program if you do not want to use Defender. The Windows Defender program will be automatically disabled if you install another antivirus program.

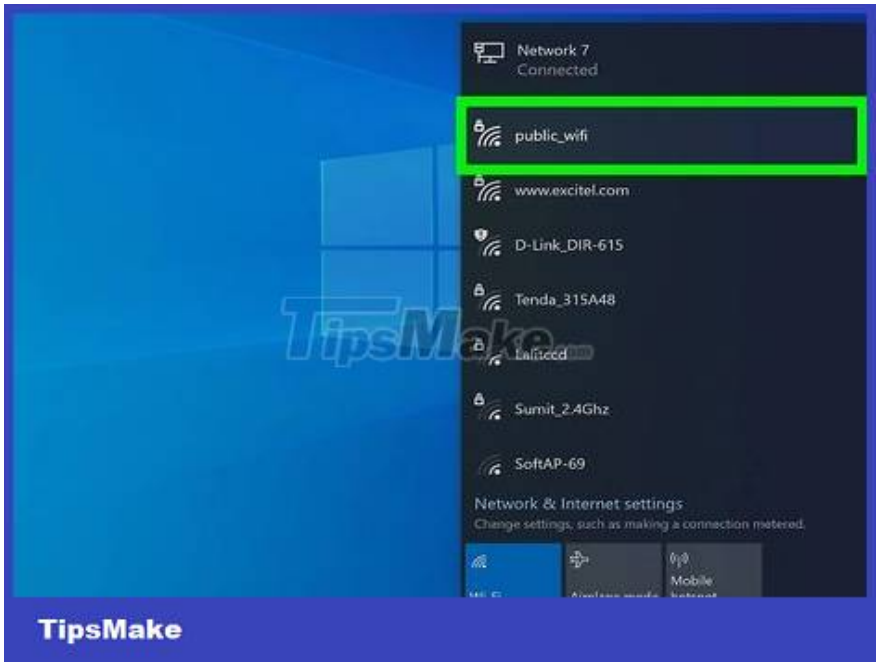
Make sure your firewall has the correct configuration. If you are not using a web server or other program that requires remote access to your computer, you do not need to open connection ports. Most programs that need a connection port use UPnP - it will open the connection port when needed and close it when the program is not in use. Leaving connection ports open indefinitely will make your network vulnerable to intrusion.

Let's look at how to set up port forwarding on your router and make sure no ports are open unless necessary for the server you're using.



Be careful with email attachments. Attaching files in emails is one of the most common ways your system can be infected with viruses and malware. You should only open attachments sent from people you trust, and you're sure they sent the file themselves. If someone in your contacts has a computer infected with a virus, they may send an attachment containing the virus without even realizing it.

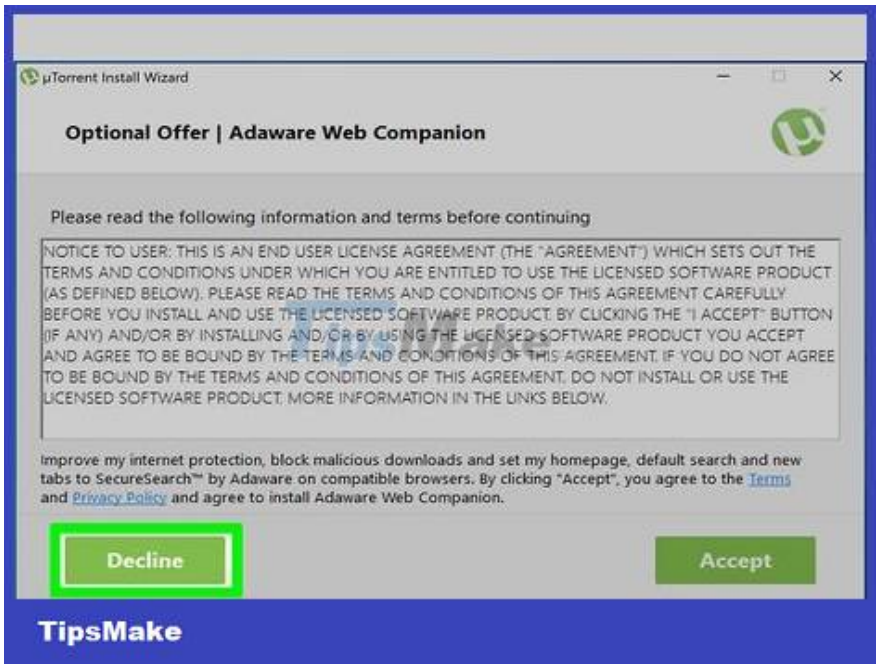
Make sure the passwords you use are highly secure and difficult to guess. Each password-protected service or program you use must have a unique and difficult-to-guess password. This is a way to ensure hackers cannot use the hijacked service's password to access other accounts. Check out the instructions for using the password manager to make it easier for you.



Avoid using public Wi-Fi spots. Public Wi-Fi spots are risky because you have no control over the network. You don't know if the same Wi-Fi user is controlling access from your computer. Through public Wi-Fi systems,

other people can access open web browsers or more information. You can limit the risk by using a VPN every time you connect to Wi-Fi to encrypt your connection.

See how to configure a VPN to establish a connection to a VPN service.



Always be cautious with programs downloaded online. Many "free" programs available online contain other software that you don't need. Pay attention during the installation process to ensure you decline any further 'invitations'. Avoid downloading illegal software, as this is a common way for your operating system to be infected.

You finished reading the article "**How to Detect Remotely Accessed Computers**" 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.
