Can a VPN Protect You From Ransomware?

Ransomware is a worrisome online threat. If it's installed on your computer, you not only risk paying a ransom to get your files back, but you also potentially won't get them back even after paying.

VPNs are a popular tool to protect you online. As a result, you may be wondering if they can protect you from ransomware. Unfortunately, VPNs are not designed for this purpose.

Why doesn't a VPN protect you from ransomware and what should you do instead?

VPNs protect Internet users by hiding their IP addresses and encrypting all their traffic. While both VPNs and ransomware use encryption, VPNs offer no protection against ransomware.

Ransomware usually spreads by tricking people into downloading it. This can be achieved by using spam emails or giving away something people want for free. VPNs do not restrict what you download and therefore do not prevent this from happening.

How does a VPN protect you?

VPNs are worth using, but not for ransomware prevention purposes. VPN protects you in the following ways.

VPN hides your IP address

This prevents websites from knowing your location when you visit them. This is useful to avoid being tracked and stay anonymous when you post something.

VPN hides your Internet activity

VPN encrypts all your Internet traffic. This prevents your Internet service provider from knowing what websites you visit. This is useful for security purposes and prevents your Internet provider from throttling the connection when you're doing something they don't like.

VPN prevents packet sniffing

If you use an unencrypted WiFi connection, bad guys can see your Internet activity using the Packet Sniffing feature. VPN prevents this from happening and makes unencrypted WiFi safe to use.

What does a VPN not protect you from?

VPN offers anonymity but does nothing to protect your files.

Lets you download anything

A VPN allows you to download anything and therefore does not prevent you from downloading ransomware. If you downloaded the ransomware yourself, it doesn't matter whether you're using a VPN or not.

Lets you install anything

VPN does not prevent you from installing ransomware. If you have anti-virus software installed on your computer, it will issue a warning and may prevent the program from running. But VPNs are not designed to do this.

VPN does not encrypt your files

VPN encrypts your Internet traffic. This means that data is protected from packet sniffing as it is transferred to and from your computer. The VPN doesn't do anything to the files on your computer. And those are the files targeted by the ransomware.

How to protect against ransomware?

While a VPN doesn't offer protection against ransomware, you can protect yourself in other ways.

Only download software from official sources

Software should only be downloaded directly from the publisher. If you download software from anywhere else, it runs the risk of including malware like ransomware.

Do not download email attachments

Junk email is often used to advertise ransomware. Spam emails provide various reasons for you to download attachments, but this should be avoided.

Don't click on suspicious links

Never click on suspicious links! It's possible that clicking the link will start downloading the ransomware or take you to a malicious website. If you are tempted and want to make sure that the URL is safe, try a site that checks the authenticity of the links.

Use an anti-virus program

If you want software to protect you from ransomware, you should buy an antivirus, not just a VPN. Antivirus software is specially designed for this purpose. It will warn you if there is a ransomware program on your computer and prevent you from running it.

Be careful when using USB

USBs are often set up to spread ransomware. They can automatically run ransomware when you plug it into your computer. These USBs are often left in public places in the hope that someone will pick them up and use them.

Back up your files

As long as your files are backed up, even if ransomware interferes by reformatting your computer, the consequences will not be too serious. It is important to note that this does not provide complete protection, as some ransomware also steal a copy of the file and use it to blackmail you.

How VPNs Can Cause Ransomware Attacks

VPN is a reputable product but can cause ransomware attacks if configured incorrectly. This does not apply to VPNs used to browse the Internet. But if a VPN is used to provide remote access to the network, any vulnerability in that VPN could be used as a way to carry out a cyber attack.

VPNs need to be updated regularly to prevent this from happening. But this doesn't always happen, and unpatched VPNs are now a common cause of ransomware attacks against large organizations.

If a VPN user has weak passwords or has their passwords exposed through a phishing attack, this can also provide an access point to another secure network.

VPNs don't protect you from ransomware

VPNs are popular because they keep you anonymous online and provide protection against a number of cyberattacks. However, they do not prevent ransomware and should not be considered a form of protection against attacks like these.

Instead, if you want to be protected from ransomware, you need to modify your online behavior. Do not click on suspicious links and do not download software from unofficial sources. You should also install anti-virus software that can sometimes stop ransomware from running.