

5 Tips To Avoid Cybersecurity Risks While Streaming On New Platforms

TechRounder PDF Edition

Live article:

<https://www.techrounder.com/tips/few-tips-to-avoid-cybersecurity-risks-while-streaming-on-new-platforms/>

By Vipin PG | Published December 9, 2022 | Updated December 9, 2022 | Format: Article | 4 min read

In brief

To stay safe while streaming on new platforms, avoid clicking unknown links, stick to trustworthy services, and never share your account credentials.

With the current popularity of streaming, hackers and cyberattackers have found an entirely new field to play with. There are thousands of streaming websites and apps that hackers are targeting and trying their hacking skills out on. Even well-established global streaming giants like Netflix, Disney+, and more have been targeted.

But the streaming industry continues on an upwards trajectory and doesn't show any signs of slowing down. Even geo-restrictions aren't stopping people, as people install VPNs to stream Paramount+ outside USA and other streaming platforms.

So, if streaming is becoming more prevalent, but hackers are not going away, what can one do to protect themselves from cybersecurity risks? Especially with new platforms popping up all the time. Here are five tips you can keep in mind to avoid cybersecurity risks when streaming.

5 Tips For To Avoid Cybersecurity Risks

1. Don't Open Unknown Links From Untrustworthy Sources

Phishing attacks are a tale as old as time, and they simply work by stealing your data by getting you to click on fake or malicious links which take you to websites that look real but are fake.

They get you to enter your real credentials to steal your data and access your accounts.

It may be a very old trick, but it is still going quite strong, and even today, thousands of people fall prey to phishing attacks worldwide. For example, hackers have targeted Netflix users with phishing attacks to get access to their Netflix accounts and steal their payment information.

So, how do you prevent this from happening? The first step is to avoid all emails or texts from unknown sources that contain odd links you don't recognize. If the hacker gets access to your account, they may access all information, including billing details, social security numbers, and addresses.

There are also tools available online that you can use, such as an anti-phishing plugin that you can download and install on your browser that will detect phishing scams for you.

2. Avoid Untrustworthy Streaming Platforms

Everyone loves a website or app that allows you to stream content for free, but most people don't know that these apps are the target of platform hacks. Such streaming apps or websites aren't safe, and many of these platforms are used to hack your device and download malware/viruses onto your device.

So, how do you prevent this? Well, some apps or services offer to stream content for free, but only a few are trustworthy. So, before accessing such a service, verify that the app or website is trustworthy.

You should also install an antivirus and a VPN like ExpressVPN, which hides your IP address and encrypts your traffic. This way, if someone does try to launch a hack, they will encounter your antivirus firewall, and your VPN will be able to terminate the connection through a kill switch.

3. Avoid Sharing Streaming Accounts

Identity Theft has become much easier in the digital age. With even a basic understanding of how photo editing software works, people can make passable copies of IDs and more. Unfortunately, it is also easier to steal identities once a hacker has gained access to your streaming account.

Sharing your account is fine, but we do not recommend sharing the password with people, as they might easily share it with others, which can become a huge issue for you later on.

4. Watch Where You Click

Even using the best and most trusted apps isn't completely safe. Kaspersky detected over 93,000 intrusions and injections of malware onto users' systems. Hackers picked the most popular shows of the time (ex: Money Heist) and used them as fronts to lure people into clicking on them to inject malware onto people's devices.

Even gamers found themselves targeted, with apps promising people that they could play paid games for free and, in reality, infect their PCs with malware once they downloaded and installed said apps.

How do you prevent this? First, keep an eye out for fake software and keep your antivirus updated.

5. Use Different Credentials For Different Platforms

Many people use the same or similar usernames and passwords for most, if not all, of their accounts. This allows hackers to use a technique known as credential stuffing. This is also referred to as a brute force attack, where hackers use already-known credentials on multiple platforms to get access to the rest of your accounts.

This is why it is recommended that you change all your accounts' passwords if even one of your accounts is compromised/hacked. We also recommend using Multi-factor authentication so that even if they have the right username-password combination, they still come up against an added layer of security.

Conclusion

These 5 tips are just the tip of the iceberg, but they should give you a basic understanding of protecting your data and accounts from hackers. Of course, the best cure is prevention, as they say. And as long as you adhere to these 5 tips, your chances of avoiding hackers are very high.

References

1. crazystreamers.com - paramount-plus / countries - <https://www.crazystreamers.com/paramount-plus/countries/paramount-plus-outside-usa/>
2. netflix.com - <https://www.netflix.com/>