How to keep your Android device secure

Making over 75% of all mobile devices, Android phones are the favorite target of cybercriminals. Learn how not to become the next victim now.

According to estimates, Android devices made up almost three-quarters of all mobile phones in 2019. Despite that, attacks on those devices constitute nearly half of all attacks, meaning PCs, IoT and iPhones are included in the report. Due to its open-source nature, it's much easier for cybercriminals to take advantage of your mobile device if you have Google's OS on it, compared to Apple devices, for example.

Its popularity is another clear reason for so many attacks. After all, open-source or not, almost 75% of people use those devices, so it's a smart choice on the criminals' side to attack the majority and maximize their chances of success. That doesn't mean, however, that you should get scared and throw your phone away or switch it for an iPhone. Just because there are threads doesn't mean you can't protect yourself against them.

Picture 1 of How to keep your Android device secure

Networks are your enemy

Well, not all networks, obviously, but some of them. Your home or work network, for example, are most likely very secure. At your workplace, multiple IT people are ensuring its safety and home networks are usually safe by nature unless you're a high-profile target in which case someone might want to target you specifically, but that's rarely the case.

They don't care who you are

Most of the time, cybercriminals don't target anybody in particular, especially when it comes to network attacks. After all, we all possess valuable data such as passwords to our bank accounts which those with malicious intentions can easily exploit. In addition to that, if they decide to infect your phone, once you connect to another network, the malware can spread to other devices connected to it, giving the hackers even more access and information.

We take our phones everywhere

We are especially prone to network attacks on our mobile devices as we keep them on us most of the time. If you don't have a mobile data plan, or even if you do have it but don't want to use it or there's a problem with your provider, you might end up connecting to a public network. That's perfectly OK, and it can happen to anybody,

but it's where the problems begin as far as staying secure goes.

Man-in-the-middle attacks

If you want to connect to the Internet through a network, you will end up connecting to a router, and it's that device that then connects you to the world wide web. One of the most popular ways criminals exploit it is by placing themselves in the middle of that connection where they effectively can intercept everything you send or receive from the Internet including, but not limited to, your passwords and other sensitive data.

Not only passwords

Having access to the information you not only send from the Internet but also receive, the hacker can add something to it, therefore infecting your device with malware and compromising it. In this case, even after you disconnect from the network, they will still have access to your device without the need to be in close proximity.

How to protect yourself

As mentioned before, just because hackers prefer Android phones doesn't mean you should switch. It could be a very costly solution which can also disrupt your lifestyle, depending on how much you're used to the friendly green robot. You also don't have to stop using public networks, and while you certainly can do that, there's a very high chance you will need to connect to one sooner or later. To protect yourself from such scenarios, we recommend you have totally free VPN on your device.

What a virtual private network?

It's a way you can prevent man-in-the-middle attacks and so much more. The way it works is as follows: when you connect to a network, you first connect to a server that can be located anywhere in the world and it's through that server that you ultimately connect to the Internet. That means that what you do on the Internet is not visible to other people, including your Internet provider or the government.

Why should I care?

Having your phone infected through a network will affect not only you but also others. Once there's malware on your device, it can spread through the networks you connect to later, ultimately spreading to other devices and similarly compromising them. In addition to that, virtual networks increase privacy which we're slowly losing every day.

The bottom line

As you can see, network attacks are no joke and are extremely common in today's world. Luckily, there's a simple way to protect yourself. Having free VPN software on your device will ensure safety should you need it because otherwise, when you find yourself having to connect to a network you don't fully trust, it might be too late to get it.