If I don't use the Internet, do I need anti-virus software?

Today, most people use their devices to connect to the Internet. But if you happen to not be using the Internet on a certain device, such as a tablet or laptop, do you still need anti-virus software or is this a waste of money?

Online cyber attack

Picture 1 of If I don't use the Internet, do I need anti-virus software?

It is undeniable that online cyberattacks are more common than offline attacks. The Internet age has opened the door for threat actors looking to exploit unknown victims, be it for data theft, remote access, espionage or other acts.

The most common types of online cybercrime are phishing, malware attacks, denial of service (DoS) attacks, and Man-in-the-Middle (MitM) attacks.

All these cybercriminal methods can be incredibly damaging. There are many types of malware out there, many of which get more sophisticated over time. Phishing attacks are also becoming harder to detect. As anti-virus software improves and people's knowledge of cybercrime grows, criminals need more advanced ways of accessing devices and data.

But things don't stop at online attacks. Offline attacks can be extremely dangerous.

What is an offline network attack?

Picture 2 of If I don't use the Internet, do I need anti-virus software?

A common method for offline malware infection is to use a flash drive. Flash drives can contain malware that will then infect any device it's plugged into. If you are using your device in public or at work, it is much easier for an attacker to infect your device with a flash drive if you leave it unattended for a few minutes.

Threat actors use flash drives to infect devices for a variety of reasons, such as for remote access and data theft. An infected USB can also trigger a charging process that severely damages the hardware on your device, often beyond repair. Attackers will often disguise malicious programs as seemingly infinite files for victims to click on without thinking twice. After this is done, malware can become active.

Flash drives can also be used to spoof HID (Human Interface Device). In such an attack, the flash drive installs a program that tricks the computer into thinking it's attached to an external keyboard (but is actually an HID). The

keystrokes are then used to infect the device with malware. HID spoofing is often used to execute commands without the consent of the device owner.

Take StuxNet as an example. Discovered in 2010, this computer worm can penetrate and infect offline networks, mainly focusing on targeting Iran's nuclear program. StuxNet can infect devices via a simple USB stick and can even be targeted by security tools with a rootkit.

This is why you should never plug any random flash drive into your device. Even if you think it's trustworthy, the USB can still be infected with malicious programs.

Devices can also be infected through the Juice Jacking attack, an attack that involves infecting ports and cables at public charging stations through the data pins of a USB connection. If you are a frequent user of public charging stations, you can be attacked by malware regardless of whether your device is connected to the Internet or not.

Through Juice Jacking, your device can be stolen and subjected to malware-based attacks. Your device may also be completely disabled, preventing you from taking any action.

Why do you need antivirus software all the time?

Picture 3 of If I don't use the Internet, do I need anti-virus software?

Even if you only use your device to draw, write, or do another offline activity, you're still at risk of malware infection.

An anti-virus program will not only warn you about malicious programs; it will usually isolate or eradicate them. While this cannot be done with all malware programs, it certainly serves as a strong first line of defense. Many antivirus programs can work without an Internet connection, so this won't be a problem if your device is never online.

On top of that, most antivirus programs give you security recommendations to protect your device as much as possible. Even if you think your security level is pretty high, there may still be certain areas that you haven't thought about that are currently being security holes. For example, you may not be able to password protect your device at startup.

Antivirus software is paramount

No one really wants to pay for antivirus software. Most of the time, it works in the background and users rarely interact with this software. But this kind of tool can prove to be invaluable for your device, both online and offline. So be careful - equip your device with a reliable antivirus service.