Techno-Tips: Somebody could be spying on me[1]

By Antonio Hernández

This is neither the title of the next thriller nor an urban legend going around. This is a real-life threat resulting from the use of smart devices with cameras, mainly computers, tablets, and phones. While I am working on the computer, a hacker or cybercriminal has the potential to watch and hear me, even though I might not be using the camera or microphone. This is true for the more common operating systems in both Android and Windows.

How do they do it? First, they try to find a way to insert malicious "malware" software into your device. Malware is a type of trojan[2] program from the family of Remote Administration Trojan (RAT) computer virus programs. Once installed, the cybercriminal can take control of the device and activate the camera and the microphone, unbeknownst to you. This phenomenon is prevalent in devices and programs that are designed more for functionality than for security. It is the price we pay for having access to user-friendly technologies at an acceptable cost.

How can I lower the risk of an intrusion? There are several recommendations to be followed in other to avoid intrusions:

- Cover the camera in your device. Use an adhesive tape or, better yet, get a specially designed window or shade to blind the camera. It costs no more than a couple of dollars. I have added this to all my devices and a "good practice" is to keep it closed when the camera is not in use. In video conferences and face-time communications, I open it only when I am sure I am with a trusted person or group at the other end. This also protects your privacy and lets you avoid uncomfortable situations.

[1] This article was written based on an article published in the Colombian newspaper El Tiempo, on June 18th 2020

[2] Called trojan for the mythological Trojan Horse

- Be aware of the programs and Apps that you download into your devices, especially the FREE ones. Try to verify the source or company of the program or check comments and reviews for the product, written by the public. Always download programs from the official company site.

- In the programs and Apps you download, especially the FREE ones, always read the “Fine Print” before installing. You will be surprised by all authorizations you are giving for the use of your information. One quite common feature used with mobile platforms like cellular phones and tablets is authorization to track your location. They could essentially follow you around all time!

- Avoid all messages and survey offers that promise more than makes sense for them to offer. Those are always unrealistic, and they serve as a mechanism to harvest your information and infect your device. I always keep in mind “This is too good to be true.”

- Never insert USB drives in your devices if you don’t know where they were used before.

Remember, always apply your common sense and safe practices when you are using your devices. N