Cinco alertas que determinan si la cámara del computador fue hackeada

23/11/2022

Los ataques cibernéticos a las cámaras de los computadores son una realidad hace varios años, por lo que diferentes marcas de tecnología han desarrollado alternativas para notificar a los usuarios que la cámara fue vulnerada y que por lo tanto, existen opciones para bloquearla.

De esta manera, existen los siguientes tips para identificar estos abusos por parte de los ciberdelincuentes:

La cámara se mueve

Para quienes compraron un dispositivo externo y lo conectaron al computador de escritorio o al portátil, se debe conocer si

tiene esa cámara un sensor que reconoce el seguimiento de una persona, entonces, si se identifica un movimiento extraño cuando no se está usando, se debe poner atención.

De igual forma si el dispositivo no hace caso a las ordenes del usuario, se puede tener certeza que el dispositivo fue vulnerado y será necesario desconectarlo para revisar que no haya ningún malware atacando.

Otras señales similares es que el micrófono del computador se encienda solo o que los parlantes reproduzcan sonidos extraños.

Hay varias alertas que permiten saber si un computador ha sido hackeado y están espiando desde la cámara.

La luz se enciende

Una de las herramientas que utilizan las marcas para indicar que la cámara está encendida es con una luz junto al lado del dispositivo, pero solo debe prenderse cuando el usuario

realmente la active.

Si se está realizando cualquier otra actividad y de un momento a otro la luz empieza a parpadear o se enciende por completo, será una señal clara de que alguien está intentando controlarla o ya la tiene bajo su mando.

También, puede suceder todo lo contrario, que el usuario quiera acceder a la cámara pero la luz no se prenda. Un indicativo de que algo no está bien, porque es una función de seguridad que debe estar operando de buena forma.

La cámara se abre con aplicaciones

Es normal que se instalen extensiones o aplicaciones en los computadores para diferentes funciones, pero si alguna de ellas ejecuta la cámara sin el permiso adecuado o su función final no tiene nada que ver con encender este dispositivo hay que verificar.

Todos los navegadores tienen la opción de controlar los permisos a los que accede una app o una página web, por lo que habrá que ir a los ajustes y revisar que no haya un acceso peligroso. En caso de no poder quitarlo será mejor desinstalar la extensión o dejar de entrar a esa página.

Hay varias alertas que permiten saber si un computador ha sido hackeado y están espiando desde la cámara.

Archivos de audio y video desconocido

Cuando se utiliza la cámara y se hace alguna **grabación** es normal que esta deje algún registro en la carpeta de documentos. Pero si aparecen audios o grabaciones que nunca se hicieron se debe generar una alerta de inmediato porque pueden estar controlando la cámara y tal vez el computador al tener acceso a los archivos y creación de carpetas.

Una forma de averiguarlo es revisar la ubicación en la que la cámara está guardando los archivos, si no es la predeterminada o una que se haya creado personalmente, es bueno verificar si el computador está siendo expuesto a un tercero.

Tapar la cámara

Cuando se conocieron los documentos filtrados por Edward Snowden, exempleado de la Agencia Central de Inteligencia y de la Agencia de Seguridad Nacional de Estados Unidos, hace más de una década, una de las informaciones aseguraba que las organizaciones espiaban a las personas a través de la cámara y muchos optaron por taparlas.

Esta no es una decisión errónea, porque quizás el hacker logra saltar todas las señales anteriores y espiar sin dar muestras al usuario. Así que cubrir la cámara con una cinta adhesiva es una buena opción, aunque algunos computadores traen la opción de taparla con una pestaña o un botón que la deshabilita momentáneamente.

Fuente: Infobae