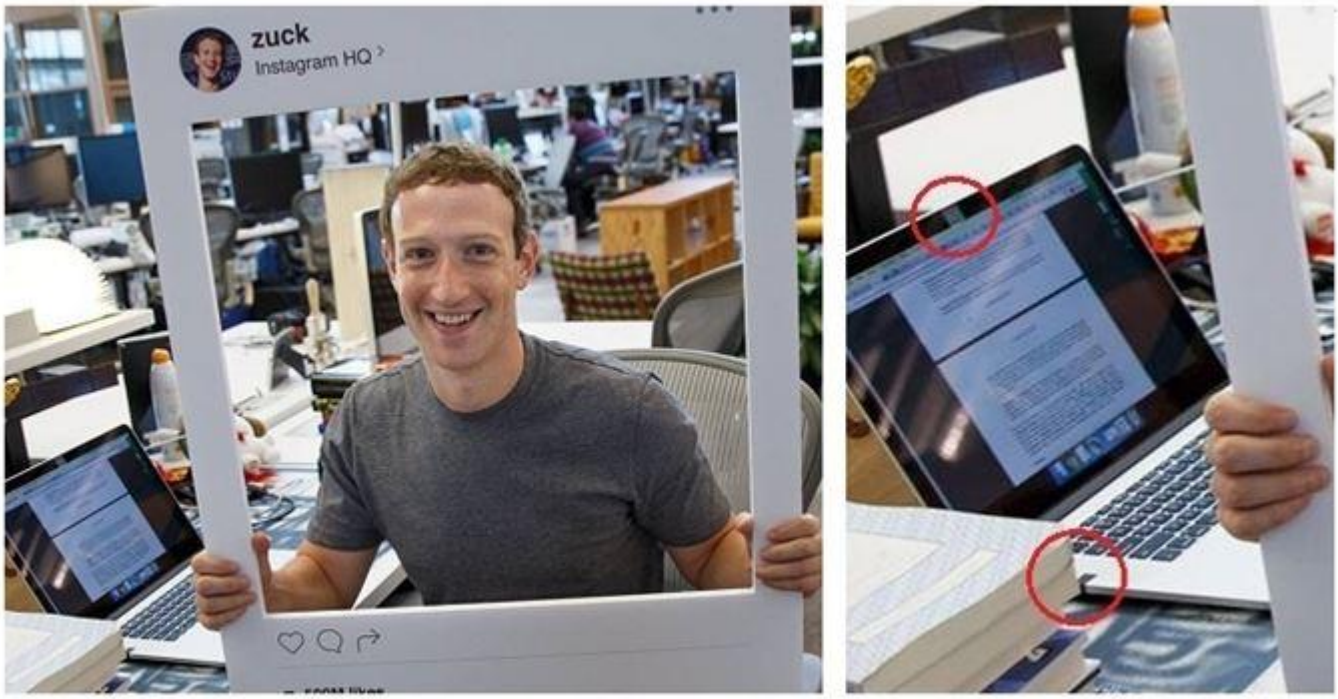
¿Por qué deberías tapar tu webcam? según el FBI y el dueño de Facebook

Expertos en tecnología han admitido usar cinta como medida de seguridad tapando la cámara en computadores y celulares.

EL TIEMPO/GDA
Martes, 19 Diciembre 2017



La computadora de Mark Zuckerberg tiene la webcam tapada. Foto: Facebook Mark Zuckerberg

El temor a la violación de la privacidad es uno de los miedos que más sienten quienes se han sumergido en el mundo de la tecnología y de las redes sociales. Este sentimiento aqueja tanto a novatos como a los más expertos del mundo digital.

Episodios como el sucedido el 21 de junio de 2016, cuando Mark Zuckerberg publicó en su perfil oficial una fotografía para conmemorar que más 5000 millones de personas usaban Instagram, dejaron en evidencia la particular práctica del creador de Facebook **de tapar con cinta adhesiva la cámara y el micrófono de su computador personal**.

Meses después James Comey, antiguo director del FBI, reiteró que los ataques cibernéticos son inevitables y por eso no se debe olvidar la importancia de cubrir estos tipos de dispositivos asegurando que todas las personas deben ser "cuidadosas con su propia seguridad y no asumir que alguien lo será por ellas".

"Hay algunas cosas sensatas que debería estar haciendo, y esa es una de ellas", dijo Comey durante una conferencia en el Centro de Estudios Estratégicos e Internacionales, sobre la curiosa técnica.

Paranoia o no, más de uno en algún momento se ha sentido observado a través de la cámara web de su computador y por eso muchos repitieron la particular medida que reveló la fotografía de Zuckerberg.

¿Pueden estarlo observando o escuchando?
Para Jhon Saavedra, director de tecnología del Politécnico Grancolombiano —a través de investigaciones en la deep web o viendo el software que está disponible— terceros ya pueden tomar desde remoto el control no solamente de un aparato tecnológico sino también de la cámara y el micrófono de ese dispositivo.

Por ende, el especialista señala que es mejor proteger este tipo de aditamentos de los equipos portátiles o móviles para aumentar los niveles de seguridad. "Cualquier país es susceptible de hackeo. Esto lo vimos con el tema de Ransomware que afectó empresas a nivel mundial y también lo podemos ver a nivel de Colombia (…) Si el programador o el hacker tiene habilidad lo puede hacer sin necesidad de la autorización del dueño del equipo o de la persona que lo esté utilizando en ese momento", añadió.

Por eso, si usted es de las personas que maneja datos privados o equipos que son de uso ejecutivo, según Saavedra, debe estar muy atento a mantener medidas que lo protejan de métodos usados por delincuentes para robar su información.

Si el programador o el hacker tiene habilidad lo puede hacer
"Muchas veces hay personas que comparten videos o enlaces a través de WhatsApp y es ahí donde se puede dar el robo. Por otro lado, se pueden tomar equipos de forma remota y los hackers son especialistas en tomar equipos con mensajes engañosos como links que llevan a otro tipo de páginas donde le pueden capturar la información", mencionó.

Frederick Ferro, especialista de la Universidad Central, señala que cualquier equipo es susceptible a ser intervenido o manipulado para tener acceso a sus periféricos, a su memoria y a cualquier dispositivo que esté conectado al mismo.

"Entre más importante sea la persona, más importantes e interesantes son los datos e información almacenada en su equipo. La mayoría debe 'blindarse' y utilizar equipos 'señuelo'. Las acciones de Mark Zuckerberg son un sarcasmo a la realidad tecnológica en la que vivimos, si él no puede protegerse, ¿Entonces quién?", afirmó.

Resaltó que siempre que se utilice tecnología las personas deben pensar en las consecuencias, es decir anticiparse a los eventos positivos o negativos que puede dejar su uso.

"En general todos achacan el problema de la inseguridad a los entes del estado, pero ¿nosotros mismos con educación y formación en tecnología no podríamos hacer mejor la tarea?", concluyó.