Secciones Sábado, 30 abril 2022 ISSN 2745-2794 Semana Suscribirse Crear cuenta Iniciar sesión

Últimas noticias Elecciones 2022 Semana TV Semana Play Economía Impresa Más Galerías Especiales

Tecnología

Ojo con el ‘Zoom snooping’, la técnica con la que descifran contraseñas por videollamada

Los expertos recomiendan a las personas vigilar muy bien con quién comparte videollamadas y evitar teclear información personal relevante mientras participa en una de ellas.

10/11/2020

Trabajo en Colombia: Ojo a las falsas ofertas laborales por redes sociales - Foto: Cortesía Icfes

Un equipo de la Universidad de Texas en Estados Unidos desarrolló un método que permite determinar lo que un usuario está tecleando, sin necesidad de enfocarlo, **solo partiendo del análisis del movimiento de sus hombros y brazos a través de una videollamada.** Se trata de una técnica llamada ‘Zoom snooping’.

De acuerdo con los investigadores, el ‘Zoom snooping’ se puede utilizar en cualquier aplicación para videollamadas **como Zoom, Google Meet, Skype,** por lo que esta técnica, de ser utilizada por una persona mal intencionada, **le permitiría saber qué está escribiendo un usuario en medio de una reunión virtual.**

Por lo tanto, lo anterior podría ser aprovechado para que, mientras la persona escribe en su teclado, otra le pueda **descifrar sus claves de acceso o número PIN, por poner un ejemplo.**

Mensajes que se autodestruyen en WhatsApp: la novedad confirmada del chat más usado del planeta

Para determinar el uso de esta técnica, los investigadores de la Universidad de Texas realizaron pruebas en un entorno controlado, donde sabían exactamente el modelo de la silla, el teclado, configuración y la webcam usada, **logrando un 75 % de acierto al determinar lo que se escribía**. No obstante, cuando implementaron la técnica ‘Zoom snooping’ en un ambiente no controlado, el porcentaje de precisión descendió en un 20 %.

Además, para llevar a cabo dicho proceso, el grupo de investigadores tomó imágenes en movimiento cuadro por cuadro de la persona, y de acuerdo a la posición de los pixeles, **lograron determinar por medio de un video en alta resolución la dirección tomaban las pulsaciones**, es decir, si iba hacia arriba o hacia abajo, de izquierda a derecha.

Posteriormente, mapearon las pulsaciones en un teclado QWERTY para inferir lo que se había redactado. Sin embargo, el estudio estableció que **si el usuario utiliza camisa manga larga o tiene el cabello largo y este cubre sus hombros**, el proceso se dificulta a la hora de acertar lo que teclea, teniendo en cuenta que al taparlos despista a los intrusos y garantiza la seguridad durante la videollamada.

Los investigadores también recomendaron **no redactar nada que ponga en evidencia datos privados o personales mientras la cámara del computador esté encendida**. Lo cierto es que el 'Zoom snooping' viene a sumarse a una larga técnica de métodos de espionaje, como utilizar el acelerómetro y el giroscopio de los smartphones como modo de deducir su PIN.

WhatsApp: ¿cómo saber si han hackeado, espiado o intervenido su cuenta?

La aplicación de mensajería más popular del mundo sigue sorprendiendo a diario a sus millones de usuarios con **actualizaciones para que sean probadas por ellos mismos; sin embargo, muchos aún desconfían de la seguridad de la plataforma** a la hora de intercambiar información personal como cuentas bancarias, documentos privados o imágenes personales.

Aunque la red viene trabajando para mejorar la experiencia de usuario, el hecho de ser tan popular pone en riesgo su información ante ataques cibernéticos. De hecho, junto a Facebook, es una de las aplicaciones con más intentos de 'phishing'.

Entre las razones por las cuales la plataforma no es segura –explicadas por el portal tecnológico ADSLZone– es que **WhatsApp le pertenece a Facebook. Y si bien la aplicación del logo verde ha tenido problemas con la seguridad de sus mensajes en casos muy escasos, Facebook ha tenido escándalos** por la filtración de datos, lo cual es un riesgo para los usuarios de las dos redes sociales.

WhatsApp Web: aprenda qué es y cómo activar la función “PIP”, la novedad en videos del chat

Según este portal, solo en 2019 la aplicación presentó 6 fallas de seguridad, de las cuales 3 fueron graves; la primera **hackeaba el teléfono al recibir una llamada de WhatsApp**, la segunda hace referencia a un atacante que podía ejecutar un código a través del envío de un GIF y la tercera falla de seguridad es que los hackers también podían realizar un ataque cibernético, pero con un archivo MP4.

¿Cómo saber si una cuenta de WhatsApp está intervenida o hackeada?

Según el diario *Metro Ecuador*, por el momento se conocen cuatro señales que alertan a los usuarios sobre una posible intervención a su cuenta:

1. El celular se descarga rápidamente.

2. El equipo vibra y suena con frecuencia.

3. El dispositivo se bloquea regularmente.

4. El teléfono móvil se calienta en numerosas ocasiones.

Cabe mencionar que **WhatsApp cuenta con la posibilidad de vincular una cuenta de correo electrónico al que llegará un enlace en el que se podrá cambiar la contraseña** en caso de que sea olvidada. Es importante que el correo inscrito sea el correcto, pues la aplicación no verifica su validez.

internet Fraude Contraseñas hackeadas

Convierta a Semana en su fuente de noticias aquí

Descarga la app de Semana noticias disponible en: Apple store Google play

Noticias relacionadas