LITORALPRESS

Fecha: 07-04-2023
Medio: El Lector
Supl. : El Lector
Tipo: Actualidad
Título: Experto entrega recomendaciones para evitar delito de "media dropping"

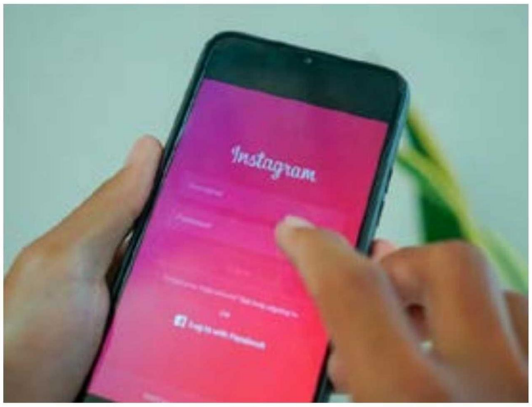
Pág. : 11
Cm2: 397,7
VPE: $ 194.872

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

Experto entrega recomendaciones para evitar delito de "media dropping"

El jefe de Seguridad Digital de la Universidad de Talca, Rodrigo Bustamante González, aconsejó tener un antivirus activo y siempre actualizado en el sistema operativo.

En caso de sufrir un ciberataque es vital cambiar la clave del servicio de almacenamiento virtual, indicó.



Las estafas a través de Internet han ido en aumento, en especial desde que la pandemia obligó a las personas y empresas a trabajar y realizar muchos de sus trámites mediante este sistema.

Si bien existen varios tipos de fraudes, uno de los que se destaca es el "media dropping", que es una técnica en la que el delincuente requiere conocer la rutina de la persona a la que va a atacar.

El jefe de seguridad digital de la Universidad de Talca, Rodrigo Bustamante González, se refiere a este método, denominado y las medidas para evitar o minimizar sus efectos. "Es una de las técnicas más trabajadas por los ciberdelincuentes, considerando que estos hacen un seguimiento previo con la finalidad de conocer los sitios que sus víctimas frecuentan para dejar un pendrive o un disco externo con un programa malicioso en el lugar", explicó.

El experto detalló que el ataque se produce cuando "la víctima recoge el dispositivo de almacenamiento externo, creyendo que se lo encontró, y posteriormente, lo conecta a su computador. De esta forma, automáticamente el programa malicioso se apodera de los datos".

Consejos de prevención

Por ello, el especialista precisó que, "una de las herramientas para prevenir este tipo de ataques es tener un antivirus actualizado, que puede ser pagado o gratuito, ya que la mayoría de los sistemas maliciosos están identificados por los programas de protección digital".

Por otra parte, Bustamante, comentó que, para resguardar los datos personales siempre es bueno definir una clave para iniciar los equipos y bloquearlos cuando no se esté presente. Junto con esto, "evitar mantener datos personales en los computadores. Una de las costumbres, que por facilidad se acepta, es guardar las contraseñas en el navegador. Lo ideal es no permitir esta práctica, pues facilita a los ciberdelincuentes los procesos de estafa", planteó.

A su vez, llamó a tener activo y actualizado el sistema operativo del computador, ya sea Windows, iOs, Linux o Ubuntu, así como "los programas instalados en éste, porque ayuda a mejorar la seguridad y evitar que los ciberdelincuentes accedan a información".

Por otra parte, Bustamante llamó a "mantener nuestra información respaldada en algún servicio de nube", ya que en caso de perder el computador o sufrir un ciberataque, se pueden salvar los archivos de una manera más simple, cambiando la contraseña de este sistema, lo que permite que se bloquee automáticamente el servicio en otro computador.