15/05/2023

¿Qué hacer en caso de ser víctima de suplantación de identidad por internet?

Explicamos en qué consiste, las consecuencias y cómo evitar este tipo de fraude, cada vez más habitual en las redes



En 2022, se registró un fuerte incremento en los fraudes virtuales en España. Según los últimos datos del Sistema Estadístico de Criminalidad (SEC), se denunciaron 266.531 delitos informáticos. Se estima que, para 2025, estos delitos le costarán al mundo más de USD 10.500 millones. Existen muchos tipos de crímenes virtuales. Sin embargo, la**suplantaciónde identidad** genera **gran preocupación** ya que cualquier persona puede ser víctima de estos engaños.

¿En qué consiste?

La suplantación de identidad por internet se da cuando una persona se hace pasar por otra, con el objetivo de perjudicarla o cometer un delito. Existen varios tipos de robo de identidad. Uno de ellos es, por ejemplo, cuando alguien crea un**perfil falso** en una red social utilizando el nombre y la imagen de otra persona sin su consentimiento.

Otra forma común de**suplantación de identidad** por internet se produce cuando un cibercriminal accede a los datos bancarios de una víctima con el fin de**hacer transferencias** o**pedir un crédito** a su nombre.

¿Cuáles son sus consecuencias?

Aquellos cuya identidad ha sido suplantada en el internet pueden sufrir repercusiones negativas y, en ciertos casos, severas. A través de la**clonación de tarjetas bancarias, compras online no autorizadas**, contratación de servicios a su nombre y solicitud de préstamos, los cibercriminales pueden causar**grandes problemas económicos a las víctimas.**

Esto puede resultar en**daños a la reputación** e imagen de la persona o empresa afectada, así como también en **problemas legales** derivados de las estafas o delitos que quedan a nombre de la víctima. A parte de las consecuencias financieras y legales, las víctimas pueden sufrir bullying y acoso en las redes sociales.

¿Cómo denunciarla?

Hacerse pasar por otra persona, sea en línea u “offline” es un delito. Aquellos que son víctimas de fraude o acoso virtual pueden ponerse en contacto con laBrigada de Investigación Tecnológica (BIT) de la Policía Nacional y elGrupo de Delitos Telemáticos (GDT) de la Guardia Civil.

Redes sociales como Instagram, Twitter, Facebook y TikTok ofrecen la opción de reportar el hackeo de una cuenta o la suplantación de identidad en una cuenta fraudulenta. De ser víctima de delitos financieros, es importante **bloquear tarjetas de crédito y reportar el incidente al banco** lo antes posible.

Medidas para prevenirla o evitarla

Es posible tomar una serie de medidas para evitar la suplantación de identidad por internet. Se recomienda, por ejemplo, no publicar datos personales (como nombre completo, teléfono, correo electrónico, o dirección, entre otros) de manera abierta y**configurar la privacidad de los perfiles** en las redes sociales lo máximo posible. Las**contraseñas** de estas cuentas, así como las de los correos electrónicos, deben ser**fuertes**,**únicas** y han de**modificarse regularmente**.

Es importante **reportar y bloquear correos falsos** que aparentan ser de bancos, entidades gubernamentales y otras páginas web de confianza. Dichos correos normalmente alertan de un falso problema en la cuenta bancaria del usuario o una deuda que no se ha pagado y solicitan información personal para remediar la situación.

Finalmente, se puede**hacer uso de una VPN** para proteger la conexión a internet y conectarse de manera segura a redes de Wi-Fi públicas. Aunque este es normalmente un servicio pago, se puededescargar VPN de manera**gratuita** y utilizar por un periodo de prueba.

Fuente:elespanol.com

Link: https://cronicaglobal.elespanol.com/vida/que-hacer-victima-suplantacion-identidad-internet-bc-nprs_785102_102.html