04/08/2024

“Te rompí el retrovisor, llámame”: la nueva estafa que deja la cuenta del banco vacía

Es muy fácil caer en este nuevo fraude en el que los ’hackers’ se hacen pasar por la compañía de seguros de otro coche o conductor.



Hoy día hay un par de**fraudes y estafas** dando vueltas que involucran los vehículos particulares. Por ejemplo, el que suplanta la identidad de la Dirección General de Tráfico con la intención de robar los**datos personales**.

El **robo de datos personales** o*phishing* es una técnica que utilizan los*hackers* para**suplantar identidades** o, incluso, vender esa información a empresas o a entidades interesadas, casi siempre a través de la*dark web*. No obstante, hay otra serie de estafas que están más enfocadas en la comisión de delitos económicos.

Ahora hay un**nuevo fraude** que involucra el coche y en el que es muy**fácil caer**. Cuando la víctima de esta estafa va a recoger su coche, se encuentra **un golpe, una abolladura** o un desperfecto provocado, previsiblemente, por otro vehículo. En el parabrisas, se encuentra una nota pidiendo disculpas e**indicando un número de teléfono** con el que contactar para proceder a la reparación de los daños.

La**víctima**, contenta incluso de que el otro conductor haya sido responsable,**llama** al número de teléfono facilitado. Una persona responde y afirma que**su compañía de seguros** se pondrá en contacto para cubrir los gastos de la reparación. Aquí es donde empieza el proceso **para robarle los datos** y sustraer su identidad.

Un enlace del seguro: así empieza el fraude

El**conductor damnificado**, ignorante de que está cayendo en una estafa, recibe un mensaje de esa supuesta compañía de seguros del coche culpable. En él,**hay un enlace** para hacer una videollamada y proceder con la reparación de los daños. Este enlace es**la clave** de todo el engaño.

Y es que, en realidad, **al hacer clic en ese link**, la víctima está permitiendo que los estafadores entren a su teléfono gracias a una**aplicación de tipo espejo**, que permite ver en remoto todo lo que el usuario hace con su*smartphone*. Entre otras cosas, escribir la clave para**entrar a la aplicación del banco** y a la propia cuenta bancaria.

En el momento en el que la víctima accede a **su app del banco**, los *hackers* se hacen con la clave de acceso y proceden a vaciar la cuenta corriente. También pueden apropiarse, con el mismo método, de otros **datos personales** importantes.

Para **evitar estafas de este tipo**, hay que evitar clicar en enlaces sospechosos que lleguen a través de mensajería o redes sociales. Igualmente, en caso de encontrarse una situación parecida, siempre es mejor **llamar directamente a la compañía de seguros**, para evitar caer en fraudes.

Fuente: https://motor.elpais.com

LINK DE LA NOTICIA