Nueva estafa en los cajeros automáticos: de qué se trata el hackeo que pone en riesgo nuestros datos

27/09/2024

Nadie está exento de sufrir una estafa virtual, más aún si se trata de algún tipo de hackeo, en donde la víctima ni siquiera se puede dar cuenta de que está siendo robada hasta cuando es ya demasiado tarde. Un nuevo caso se da alrededor de los cajeros automáticos, donde nuestro dinero puede quedar expuesto.

Pero existe una manera de **poder evitar una forma de hackeo en los cajeros automáticos.** Para esto, será necesario tener el celular actualizado y corroborar la fuente de los mensajes que se reciban.

Los hackers buscan siempre alternativas para realizar estafas virtuales. Foto: Freepik.

El crecimiento de las estafas virtuales va de la mano con la mayor utilización de la tecnología, la cual cubre casi todos los aspectos sociales y económicos de las personas. Es que **los delincuentes o hackers cada vez buscan métodos más rebuscados para llevar a cabo sus estafas virtuales**.

De qué se trata la nueva estafa virtual con cajeros automáticos

Esta estafa involucra a la función NFC, una tecnología presente en los **chips de las tarjetas bancarias y de la SUBE**, que es inalámbrica de alta frecuencia y que funciona en la banda de los 13.56 MHz.

Además, se la puede encontrar en algunos celulares. Este método nuevo de hackeo lo que haces es **introducirse en esta comunicación e invade el dispositivo.** A partir de allí puede sustraer datos sensibles, como lo son las **claves bancarias.**

El ataque empieza con un **mensaje de pishing**, donde las víctimas reciben un **SMS que pareciera provenir del banco** con el que operan. Allí, se les piden que **descarguen una aplicación oficial** o resuelvan un problema con su cuenta.


Los delincuentes tienen acceso a las claves de los damnificados y pueden retirar dinero de los cajeros automáticos. Foto: Archivo.

Al hacer clic en el enlace y descargar la app, **los usuarios sin saberlo infectan su dispositivo con malware**, un software malicioso escrito intencionadamente para dañar los sistemas informáticos. De inmediato, este virus malicioso intercepta el tráfico NFC, lo que **habilita a los atacantes a poder capturar datos sensibles, como son los de las tarjetas de pago.**

Luego, los delincuentes utilizan un dispositivo Android conectado para clonar la tarjeta y pueden **hacer retiros o**

compras fraudulentas. La víctima nunca se entera hasta tanto revise su cuenta bancaria.

La mejor manera de protegerse de la nueva estafa en los cajeros automáticos

El primer paso y el más seguro es **no descargar ninguna aplicación en el celular que provenga de enlaces sospechosos.** Esto incluye a SMS o correos electrónicos o mensajes de WhatsApp u otras apps.

Lo ideal, si se quiere descargar una aplicación, es ir a la versión oficial de la misma presente en el Play Store.

Cómo evitar caer en una estafa virtual a través de los celulares. Fuente: Pexels.

Además, otra forma útil de prevenir este tipo de estafas es **verificando la autenticidad de los mensajes bancarios.** Cualquier mensaje proveniente de una supuesta entidad de este estilo no incluye contenido que diga «urgente». A su vez, los bancos pocas veces envían enlaces a través de SMS.

También se puede **instalar software de seguridad en los teléfonos.** Se puede usar antivirus que detecta software malicioso. **Mantener actualizado el móvil también ayudará** a incrementar parches de seguridad en el sistema operativos y en las apps.

Fuente: Canal 26