Publicado en Madrid el 31/10/2022

Swapping: protegerse del ciberdelito que devora las cuentas bancarias

Los móviles se han convertido en la principal puerta de entrada de fraudes, especialmente de los económicos. Para poder llevar a cabo las clonaciones de las tarjetas telefónicas el delincuente necesita obtener la identidad y datos personales de la víctima. Según PaynoPain, la autenticación de dos pasos es clave para garantizar la seguridad de los activos

El móvil se ha convertido en una herramienta que se usan para realizar muchas tareas de el día a día; hacer la compra, pedir comida, registrar un entrenamiento, llamar a los seres queridos, organizar el próximo viaje, etc. Convertir el smartphone en un almacén de datos de toda clase y es un hecho que ha llamado la atención de los ciberdelincuentes. PaynoPain, empresa tecnológica española especializada en el desarrollo de herramientas de pagos online, explica el swapping, la ciberestafa en tendencia, y cómo protegerse ante ella.

Cada vez existen más amenazas en la red y la mayoría de ellas tratan de abrirse paso a través de los teléfonos. Según la Asociación de Usuarios Financieros (Asefín), un 50 % de las estafas financieras se producen a partir de estos. Las tarjetas móviles suelen guardar datos confidenciales como contraseñas o direcciones por lo que se trata de una estafa con un alto riesgo de vulnerabilidad de la víctima.

Este es el caso del Swapping o SIM Swapping, una estrategia de fraude en la que los ciberdelincuentes hacen un duplicado de la tarjeta SIM de la víctima. Así, logran entrar en sus aplicaciones bancarias y acceder a su cuenta de activos para realizar movimientos de dinero.

Para poder clonar una tarjeta SIM el delincuente necesita los datos de la víctima, que en un 80% de las veces la consiguen a través de otro método delictivo como el phising, según Globatika Lab. Una manera por la que muchos se dan cuenta que están siendo víctimas de un ciberdelito, es gracias a que su móvil pierde señal durante un largo tiempo, porque en ese momento se está realizando la copia de la tarjeta. Para evitar ser víctima de estos ataques, PaynoPain ofrece cuatro estrategias que poner en práctica:

Contactar con la compañía telefónica: si se pierde señal por un tiempo prolongado es bueno llamar a la compañía de teléfonos y asegurarse de que nadie ha pedido una copia de la tarjeta haciéndose pasar por el dueño. Algunas de estas empresas ofrecen un servicio extra de seguridad en el que comprueban la identidad del solicitante de la nueva SIM a través de otro canal.

Doble o triple autentificación: tener un sistema de doble autenticación es clave. No solo en las cuentas bancarias, también en redes sociales, portales de compra, aplicaciones etc. Muchas de estas plataformas guardan datos del usuario, es importante que queden a buen recaudo, ya que si el ciberdelincuente puede acceder a cualquiera de estas cuentas, le será más fácil ir recolectando datos

de otras hasta conseguir su objetivo.

Autorización a dispositivos nuevos desde el original: mediante este sistema el usuario solo puede dar autorización de un inicio de sesión desde el dispositivo elegido como original, normalmente este es el teléfono móvil en sí. De esta manera aunque alguien haga un duplicado de la SIM o consiga las contraseñas del correo, el usuario se asegura de que la notificación llega únicamente a sus manos y solo él puede aprobar la solicitud.

Cuidado con el phishing: como se ha mencionado anteriormente, el phishing es una de las formas más usadas para robar datos de futuras víctimas. Es importante prestar atención a las direcciones de los correos y los mensajes de texto, asegurarse antes de hacer click que se trata de un enlace seguro y no dar datos a través de mensajes, llamadas o correos.

Tras la entrada en vigor de la normativa PSD2 es obligatorio solicitar dos de los tres factores de la Autenticación Reforzada de Clientes para la corrección inmediata de cualquier operación no autorizada y la reducción de la responsabilidad del consumidor ante posibles fraudes.

Por eso, es fundamental contar con herramientas que aseguren proteger los datos y cuentas del usuario. Como puede ser ChangeIt, el monedero electrónico de PaynoPain que garantiza la seguridad y el control de todos los gastos por parte del usuario. Gracias al sistema antifraude que tiene integrado y a la posibilidad de tokenizar las tarjetas del usuario, el cliente puede gozar de una tranquilidad absoluta sabiendo que tiene la mejor seguridad protegiendo sus activos. Sin embargo estas cualidades no hacen que su uso sea más complicado, con este wallet el consumidor puede sacar efectivo en cajeros usando la aplicación, pagar en tiendas físicas y online, hacer transferencias y recibir promociones, todo desde la aplicación.

"A la hora de comprar por un canal digital, la seguridad debe ser siempre lo primero. Las amenazas crecen al mismo ritmo que la digitalización y es una realidad contra la que toca luchar. Por eso, es importante ofrecer soluciones seguras y cómodas para los usuarios. Las empresas FinTech, las de procesos digitales y las consejeras financieras, entre otras, deben anteponer la seguridad de sus clientes, buscar las herramientas necesarias para cumplir con esta premisa y asegurar el poder garantizar una barrera de seguridad que si no es inquebrantable, siempre cuente con una solución como opción b", sostiene Jordi Nebot, CEO y Cofundador de PaynoPain.

Datos de contacto:
Everythink PR
91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Nacional Programación Emprendedores E-Commerce Software Ciberseguridad Dispositivos móviles