Billeteras virtuales: consejos para evitar estafas

20/01/2024

Las **billeteras virtuales** se encuentran en pleno auge y, con ellas, las **estafas**. En las últimas horas, usuarios de **Payoneer** fueron víctimas de un ataque que se cobró miles de dólares de las cuentas. Esta aplicación es utilizada por aquellas personas que venden sus servicios al exterior.

Según el consultor en seguridad informática y CEO de BTR Consulting, Gabriel Zurdo, se trató de un caso de **smishing**, una modalidad que utiliza mensajes de texto para obtener información privada.

Crecieron las estafas en las billeteras virtuales. Foto: Unsplash.

Las billeteras virtuales en jaque

De acuerdo con el informe **“Números que hablan” de Fiserv** (un proveedor líder de pagos y tecnología financiera), un 20% de las personas usuarias de estas herramientas sufrieron un hackeo en su billetera virtual alguna vez y al 18% de los comerciantes les pasó lo mismo.

Además, reveló que:

- El 60% de las personas fueron víctimas el **robo sus tarjetas o los datos** de las mismas.
- El 15% enfrentó el **hurto de sus datos del homebanking.**
- El 5%, fue engañado de otras formas.

El 60% de las personas sufrió el robo de su tarjeta. Foto: Unsplash

Ante lo ocurrido, el 43% de los afectados indicó que le devolvieron el dinero que perdió, un 35% resolvió parte del problema y, finalmente, el 22% no pudo encontrar una resolución.

Cómo prevenir estafas

El **Banco Central de Argentina** advirtió que «se perfeccionan cada vez más rápido las modalidades de estafas y fraudes: perfiles falsos en redes sociales que envían mensajes directos, llamadas telefónicas, mensajes de texto o de WhatsApp y otras aplicaciones de mensajería, además de correos electrónicos engañosos para obtener datos personales y bancarios”.

Por este motivo, es necesario tener en cuenta una serie de **recomendaciones** para proteger al máximo los datos personales.

- Activá la **autenticidad de dos factores** en cuentas de redes sociales y WhatsApp o las plataformas digitales que utilices: esta herramienta hace que solo la persona usuaria de la cuenta pueda acceder a sus redes sociales y plataformas digitales.
- No brindes ningún **dato personal** (usuarios, claves, contraseñas, pin, Clave de la Seguridad Social, Clave Token, DNI original o fotocopia, foto, ni ningún tipo de dato), por teléfono, correo electrónico, red social, WhatsApp o mensaje de texto.
- No ingreses **datos personales** en sitios por medio de enlaces que llegan por correo electrónico.

Hay que tener en cuenta ciertas recomendaciones para evitar estafas. Foto: Unsplash.

- **Usá contraseñas fuertes** mezclando mayúsculas, minúsculas y números.
- **Leé cada correo electrónico** recibido con cuidado y verificá que los sitios remitentes sean legítimos.
- Tené cuidado con los **enlaces sospechosos** y asegurate siempre de estar en la página legítima antes de ingresar información de inicio de sesión.
- No uses **equipos públicos o de terceras personas** para acceder a aplicaciones, redes sociales o cuentas personales.
- No uses **redes de wi-fi públicas** para acceder a sitios que requieran contraseñas.
- Mantené **actualizado** el navegador, el sistema operativo de tus equipos y las aplicaciones (borrá las que no uses).

Otras modalidades de engaño

Además del mencionado **smishing**, el cual utiliza los mensajes

de texto como medio para obtener información privada, hay otros métodos de los que se valen los estafadores.

Muchos estafadores utilizan correos electrónicos. Foto: Unsplash.

El phishing usa como intermediario el correo electrónico. Los estafadores esperan que la persona destinataria abra un enlace, complete formularios con información personal o descargue archivos que contienen malware o programas maliciosos para obtener datos.

Por último, podemos mencionar el **spoofing**. Hay diferentes tipos, entre ellos el envío de correos electrónicos o páginas fraudulentas, falsificación de dispositivos o de direcciones IP. Quienes realizan este tipo de fraude buscan hacerse pasar por otras **personas, organizaciones o empresas** para acceder a los datos personales y distribuir malware.

Fuente: Canal 26