CUÍDATE
de los estafadores digitales

En este 2023 se prevén fraudes al por mayor

Todo comienza con una llamada. Al otro lado de la línea un supuesto asesor de Banco te dice que alguien intentó hacer una compra con tu tarjeta, te menciona el monto y el producto que quisieron comprar; tu reacción es de indignación y miedo, puedes perder tus ahorros. Para evitarlo proporcionas todos tus datos al "asesor" que te ofrece una solución. De esta manera nos convertimos en víctimas de fraude.

Tenable, empresa gestora de riesgos cibernéticos, prevé que para este 2023 los fraudes financieros digitales se incremen-

tarán a través de técnicas como el *phishing*. Por ello, en este artículo te diremos cuál es el método de operar de cada fraude digital y cómo prevenirlo, para que tus finanzas no sufran un ataque.

Radiografía de ataques por fraudes financieros en Latinoamérica

Según las cifras de "*Security Report*, Latinoamérica 2022", realizado por ESET, una compañía de *software* especializada en ciberseguridad, México es el segundo país de América Latina que sufre más ataques de *phishing* con la intención de llevar a cabo algún tipo de fraude.

Aunque la adopción y el uso de tecnologías ha facilitado las actividades diarias, también es cierto que nos expone a diversos fraudes. La investigación del ESET detectó vulnerabilidades en aplicaciones, redes sociales, plataformas de *streaming*, sistemas operativos o *hardwares* latinoamericanos, los cuales rompieron un récord en 2021, con un promedio de 4 mil 100 ataques diarios.

En resumen, el reporte *Security Report* reveló que Perú es el país con más ataques de *phishing* con el 33% de reportes, en segundo lugar se encuentra México con 14%, el tercer puesto lo tiene Ecuador con 9% y Argentina se encuentra con el cuarto lugar con el 8%.

Otro dato relevante son las reclamaciones ante la CONDUSEF por fraudes digitales, ya que entre enero y octubre de 2022 se registró un aumento de 9.5% en las denuncias, en contraste con los fraudes tradicionales y el robo de identidad que van a la baja.

El *phishing* se ha convertido en uno de los medios de infección más comunes; en promedio se detectan alrededor de 10 mil intentos diarios.

Además, de los 6 mil 172 millones de pesos que representan el monto total de reclamaciones requeridos a la banca múltiple, en dicho periodo, 3 mil 911 millones corresponde a posibles fraudes por transferencias electrónicas no reconocidas, compras no reconocidas o retiro móvil no solicitado.

Modo de operar de algunos fraudes digitales...

Debes saber que los fraudes digitales o cibernéticos tienen por objeto afectar tus finanzas y robar tu dinero. A continuación te explicamos cómo funcionan:

1. *Phishing:*

Esta modalidad de fraude cibernético tiene como finalidad conseguir información personal como contraseñas, NIP, números de cuentas bancarias o de tarjetas de crédito y demás datos de identidad para hacer mal uso de ellos.

¿Cómo funciona? Los *phishers*, como se les conoce a estos estafadores, buscan obtener tu información a través de correos electrónicos, haciéndose pasar por una empresa o persona legítima. Te solicitan actualizar alguna información de forma urgente, ofreciéndote un enlace de una página *web* falsa (con logos e imágenes propios de la institución oficial) o bien, que descargues archivos con virus (*malware*).

2. *Smishing:*

Este tipo de fraude, al igual que el anterior, busca hacerse de tu información confidencial, con la diferencia de que se origina desde un mensaje de texto (SMS); de hecho, esta amenaza ha evolucionado en los últimos años y ahora puede recibirse a través de un mensaje de WhatsApp.

¿Cómo funciona? Recibes un mensaje a través de un SMS o de alguna aplicación de mensajería,

en el cual te dan a conocer promociones, ofertas exclusivas o que necesitas realizar alguna actualización en tu cuenta, comúnmente los mensajes suelen estar acompañados de enlaces donde te solicitan completar un formulario con tus datos personales para luego robarlos o instalar algún virus en tu teléfono celular.

3. *Vishing:*

Esta es una variante de los fraudes anteriores, con la diferencia que ocurre a través de una llamada telefónica, por ello es importante estar preparados para identificarlas.

¿Cómo funciona? Los *vishers* (como se les denomina a los estafadores que realizan esta práctica), suplantan la identidad del personal de una institución bancaria (incluso de alguna empresa) y a través de una mentira y manipulación tratan de ganarse la confianza de las y los usuarios para obtener los datos de su número de tarjeta, código de seguridad (CVV), fecha de caducidad, entre otros.

En México, el 67% de los reportes por *phishing* corresponden a la suplantación de entidades financieras, el 14% a sitios de *e-commerce*, el 8% en aerolíneas e instituciones gubernamentales, de acuerdo con el Consejo Ciudadano para la Seguridad y Justicia de la CDMX.

Claves para no caer en fraudes financieros digitales

• Lo primero que debes recordar es que ninguna institución financiera te solicitará tus datos personales por correo, teléfono o mensajes. En caso de que te contacten por alguno de estos medios y te soliciten dicha información nunca reveles tus datos, cuelga inmediatamente y repórtalo al número oficial de tu institución o acude directamente a una sucursal.

• Los estafadores siempre intentarán llegar a ti llamando tu atención con promociones, ofertas laborales o de productos, incluso con sitios de tiendas en líneas falsas (*marketplaces* falsos). Recuerda nunca proporcionar datos o acceder a *links* sospechosos.

• Un hábito financiero saludable es revisar de forma constante los movimientos de tus cuentas bancarias, de esta forma podrás identificar a tiempo alguna transacción desconocida.

• Evita acceder a tu banca digital desde dispositivos o computadoras que no sean tuyas, al igual que realizar transacciones desde conexiones a internet poco seguras o redes de wifi abiertas.