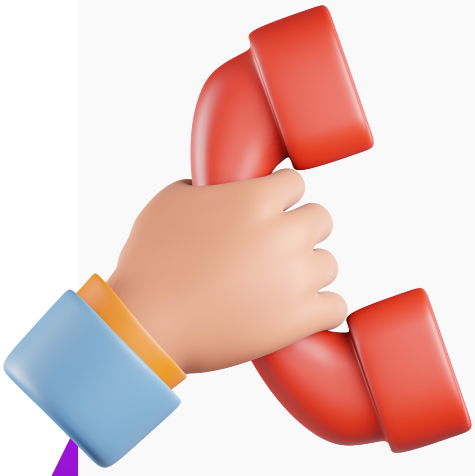
SEGURIDAD BANCARIA Y DIGITAL

¡Aprende a identificar posibles estafas y a protegerte de cada una de ellas!

Ante el incremento exponencial de las transacciones en plataformas digitales por efectos de la digitalización de las compañías y por las nuevas estrategias de consumo, Créditos Diport S.A.S - Kuikash, da a conocer las modalidades de fraude más utilizadas por los ciberdelincuentes.



Vishing

(llamadas telefónicas para extraer información confidencial)

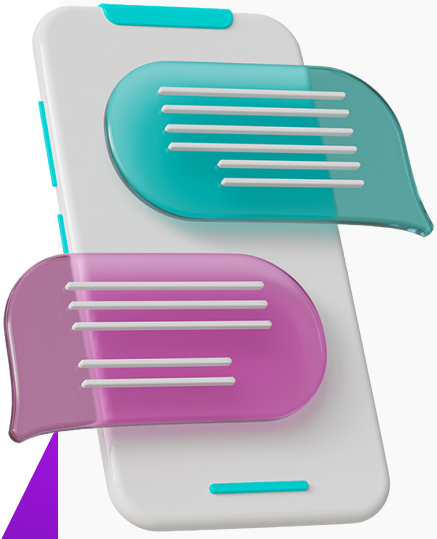
Los delincuentes intentan ganar la confianza de la víctima llamándola y haciéndose pasar por funcionarios de una entidad financiera. Para lograrlo, dan información parcial de los productos financieros o datos personales que obtuvieron usando programas maliciosos de ingeniería social; cautivan a la víctima ofreciéndole promociones y ofertas exclusivas.

Incluso, pueden decir que detectaron movimientos sospechosos en los productos financieros y que necesitan información confidencial para supuestamente proteger a la víctima.

Phishing

(correo electrónico con enlace a sitios fraudulentos)

El Phishing es una táctica en la que los criminales suplantan entidades confiables como empresas de pagos en línea, agencias gubernamentales o entidades financieras. A través de un correo electrónico falso, los delincuentes solicitan a su víctima que actualice sus datos confidenciales en un sitio web fraudulento. Usualmente aseguran que existe un problema con sus cuentas bancarias, una transacción o un envío; una vez la víctima ha entregado sus datos, los delincuentes pueden adueñarse de su dinero y productos financieros.



Smishing

(mensajes de texto maliciosos)

El Smishing es una práctica fraudulenta en donde los criminales buscan tener toda la información confidencial de su víctima y el medio para lograrlo es a través de mensajes de texto. Aprovechan las nuevas tecnologías para enviar SMS (mensajes de texto) que contienen links que redireccionan a páginas falsas, enlaces para descargar programas maliciosos y solicitudes con preguntas personales para así robar la información y el dinero.

Web Scraping

(robo de datos en sitios web)

Es una sofisticada técnica que utilizan los ladrones cibernéticos en la que, a través de un programa informático, extraen contenido y datos de un sitio web, logrando almacenar de manera automatizada grandes cantidades de bases de datos encontradas en los diversos motores de navegación para posteriormente usar dicha información en contra de los incautos. La recolección de información se hace sin contar con el permiso de los propietarios de sitios web.

SIM Swapping

(hurto tarjeta SIM de celular)

Esta es una novedosa técnica en la que, a través de llamadas telefónicas, o por medio de ingeniería social, los delincuentes engañan a sus víctimas recabando su información personal y poniéndose en contacto posteriormente con las compañías de telefonía celular solicitando reposición de la tarjeta SIM.

Ante esta modalidad, se recomienda: cuidar la información personal en páginas públicas y redes sociales; también ante una posible pérdida o robo del celular, informar inmediatamente al operador de telefonía móvil solicitando el bloqueo del IMEI, anulando la tarjeta SIM y solicitando un duplicado, cambiando todas las contraseñas.

Tips que debes tener en cuenta para evitar caer en posibles fraudes

- Cuida la información compartida a través de redes sociales o que puede ser buscada en motores o navegadores de internet.
- Nunca reveles las contraseñas y mantén actualizados los antivirus de los computadores de uso frecuente o equipos móviles y no proporciones información confidencial por medios no autorizados.
- No almacenes toda la información en tu celular y evita vincular las contraseñas de los productos bancarios con el mismo número de teléfono.
- Si el celular ha sido robado, pide al operador que bloquee el IMEI (código de identificación del teléfono) de inmediato.
- No expongas información de productos financieros en sitios no seguros o en llamadas sospechosas.
- Cuando recibas correos electrónicos de los bancos o entidades de comercio, verifica que la dirección del remitente sea la correcta.
- Nunca hagas clic en enlaces de correos electrónicos de los cuales se sospecha su procedencia.

Todas las recomendaciones son importantes y te permitirán protegerte de los delincuentes, por esto, si conoces algún indicio de posible fraude en el cual estén utilizando el buen nombre de ***Créditos Diport S.A.S. – Kuikash*** *en estos eventos, por favor reportarlo a nuestro correo electrónico autorizado* ***servicioalcliente@creditosdiport.com***.

¡Estamos comprometidos con tu seguridad!