RECOMENDACIONES DE SEGURIDAD

koa

Entérate de como protegerte de los **ataques informáticos.**

Por eso, te invitamos a leer este documento y seguir algunas recomendaciones para protegerte de estos fraudes.

¿Conoces quiénes son los cibercriminales?

Son individuos que se dedican a cometer diversos tipos de delitos, como:

- ✔ Cibernéticos
- ✔ Electrónicos
- ✔ Informáticos

Su objetivo suele ser dañar sistemas para obtener algún tipo de beneficio.

MODALIDAD DE FRAUDE:

1 Ingeniería social

La ingeniería social es una técnica que utilizan los delincuentes y cibercriminales para engañar y manipular a sus víctimas, con el fin de persuadirlas a realizar alguna acción y obtener información confidencial, como números de cuenta, usuarios, contraseñas, datos personales y financieros. Con esa información, pueden cometer otros fraudes. A continuación, te compartimos algunas de las técnicas más comunes de ingeniería social en las que cualquiera podría caer:

Cambiazo: Es un tipo de fraude dirigido a tarjetas débito o crédito. Los delincuentes distraen a la víctima de diferentes maneras para intercambiar la tarjeta real por otra que se parezca.

Clonación: En esta modalidad, los delincuentes copian la información de las tarjetas débito o crédito mediante dispositivos instalados en datáfonos y cajeros automáticos. Posteriormente, clonan las tarjetas para hacer uso de ellas.

Fleteo: Este fraude ocurre generalmente en oficinas bancarias. El delincuente identifica a la víctima cuando retira grandes sumas de dinero, con la intención de abordarla y robarle más adelante.

Paquete chileno: Esta modalidad se basa en el engaño y suele ocurrir en oficinas bancarias. El delincuente simula dejar caer un paquete “con dinero”. Un cómplice recoge el paquete y le pregunta a la víctima si le pertenece. Luego, logran convencerla para ir a otro lugar fuera de la oficina a dividir el supuesto dinero. Una vez en el lugar acordado, el cómplice persuade a la víctima para entregarle su dinero a cambio del paquete.

Phishing: Esta técnica comienza con un correo electrónico falso que aparenta ser legítimo. El mensaje contiene un enlace que solicita información confidencial, como usuarios, contraseñas, datos personales o financieros. La víctima cree que está entrando en una página real y entregando sus datos a una entidad de confianza, pero en realidad, está entregándolos a un delincuente.

Vishing: Es una técnica utilizada por los delincuentes en la que se hacen pasar por funcionarios de entidades confiables, como del sector salud, financiero, educativo o gubernamental, a través de llamadas telefónicas. El objetivo es robar información confidencial, como contraseñas, números de cuenta o datos personales.

Smishing: Similar al vishing, esta modalidad se basa en mensajes de texto (SMS) en los que los delincuentes suplantan a entidades de confianza. El mensaje suele pedirte que llames a un número de teléfono o que ingreses a un enlace, con la intención de obtener información confidencial como contraseñas, cuentas bancarias y datos personales.

Pharming: Los cibercriminales utilizan esta técnica para instalar malware en tu computadora o dispositivo móvil. El malware altera las direcciones web de tus sitios favoritos, redirigiéndote a páginas falsas diseñadas por ellos, haciéndote creer que estás en un sitio legítimo.

Malware: Es un software malicioso que se instala en computadoras o dispositivos móviles y puede causar distintos daños. Aquí tienes algunos de los tipos más comunes:

- ✔ **Keylogger:** Una vez instalado en tu equipo, registra todas las pulsaciones del teclado, capturando usuarios, contraseñas, datos personales y financieros. Normalmente, el equipo se infecta al conectar una USB desconocida o, en el caso de dispositivos móviles, al descargar aplicaciones sospechosas.
- ✔ **Ransomware:** Conocido como secuestro de datos, este tipo de malware cifra toda la información de tu disco duro, dejándote sin acceso. A cambio de liberar la información, los delincuentes piden un pago, generalmente en criptomonedas. El ransomware suele instalarse al descargar archivos adjuntos maliciosos en correos electrónicos.
- ✔ **Criptojacking:** Los cibercriminales usan esta técnica para tomar el control de un dispositivo y utilizarlo para minar criptomonedas sin tu consentimiento.
- ✔ **Troyanos:** Son programas maliciosos que se instalan en tu computadora, dañando la información almacenada y, en algunos casos, permitiendo que los delincuentes tomen control total del equipo.

Whaling: Es una combinación de varias técnicas de ingeniería social, en la que la víctima es atacada repetidamente con correos electrónicos, llamadas y mensajes de texto falsos, todo con el propósito de robar información confidencial.

CONSEJOS DE SEGURIDAD PARA TI AL ADQUIRIR NUESTROS PRODUCTOS:

Para nosotros es muy importante proteger tu información y seguridad a través de nuestros canales de atención. Por tanto, sigue estas recomendaciones para protegerte de actividades maliciosas a las que podrías estar expuesto.

1 Crédito de Libranza Koa

Solicita tu crédito a través de nuestros canales oficiales: Antes de ingresar cualquier información para solicitar tu Crédito de Libranza, asegúrate de hacerlo a través nuestra página web **www.koa.co/libre-inversion/**
Fíjate que la página web tenga el candado de seguridad y que la URL comience con "https://". **Solicita tu crédito con nuestros asesores comerciales oficiales**

No realizamos cobros anticipados por la solicitud de tu crédito: En KOA no realizamos cobros por ningún concepto antes o después de la aprobación, aceptación y desembolso del crédito. Abstente de entregar dinero o realizar pagos a terceros aunque así te lo exijan. Si este es tu caso escríbenos a nuestro **WhatsApp: 3157706670**

Verifica los términos del crédito: Antes de aceptar cualquier oferta, revisa con detalle las condiciones del crédito de libranza, como tasas de interés, plazos y cargos adicionales. Asegúrate de entender bien los términos y que no haya cargos ocultos. Puedes consultar nuestras tasas y tarifas aquí: **www.koa.co/tasas-y-tarifas/**

Desconfía de ofertas demasiado buenas: Si ves una oferta de crédito con tasas de interés excesivamente bajas o condiciones poco realistas, probablemente sea una señal de advertencia de fraude. Siempre verifica la información en nuestro sitio web oficial: **www.koa.co**
Consulta con el área de atención al cliente: Si tienes alguna duda sobre el proceso de solicitud de tu crédito, comunícate directamente con nosotros a través de los canales de contacto habilitados aquí: **www.koa.co/puntos-de-contacto/**

2 CDT Digital Koa

Si estás listo para abrir tu CDT 100% Digital KOA, aquí tienes algunos consejos para que tu información esté siempre segura:

1. **Accede a través de canales oficiales:** Antes de aperturar tu CDT Digital KOA e ingresar cualquier información, asegúrate de que nuestra página web **(https:// koa.co/cdt/)** tenga el candado de seguridad y que la URL comience con "https://". Esto garantiza que tu conexión sea segura. Para Simular tu CDT Digital KOA asegúrate siempre de ingresar a la web correcta: **https://koa.co/simulacion**

2. **Crea una contraseña segura:** Elige una contraseña difícil de adivinar. No uses fechas especiales personales como tu cumpleaños, tu número de documento, o números asociados a ti. Recuerda cambiarla regularmente.

3. **Mantén tu dispositivo seguro:** Si vas a aperturar tu CDT Digital KOA desde tu móvil, asegúrate de no conectarlo a redes públicas o desconocidas. También asegúrate de tener una contraseña, pin o huella para desbloquear tu móvil. Lo anterior aplica también para tu computador, solo que en este dispositivo debes asegúrate de tener un antivirus activo para evitar riesgos de fraude.

4. **Monitorea tu CDT Digital KOA desde tu portal de cliente:** Revisa periódicamente el estado de tu CDT Digital KOA aquí: **https:// koa.co/cdt/portal** y asegúrate de que no haya movimientos extraños. Si notas algo fuera de lo común, contacta inmediatamente a nuestros canales de contacto KOA. Conócelos aquí: **https://koa.co/puntos-de-contacto/**

5. **No compartas tus claves:** En KOA jamás te pediremos tus claves de acceso por correo electrónico o mensajes de texto. Si algún tercero te pide esta información, es probable que sea un intento de fraude. Por tanto debes reportarlo inmediatamente a nuestros canales de contacto en: **https://koa.co/puntos-de-contacto/**

Siguiendo estos simples pasos, podrás disfrutar de la comodidad y seguridad de abrir tu CDT digital KOA sin preocupaciones. **¡Cuida tu información y haz tus transacciones de forma segura!**

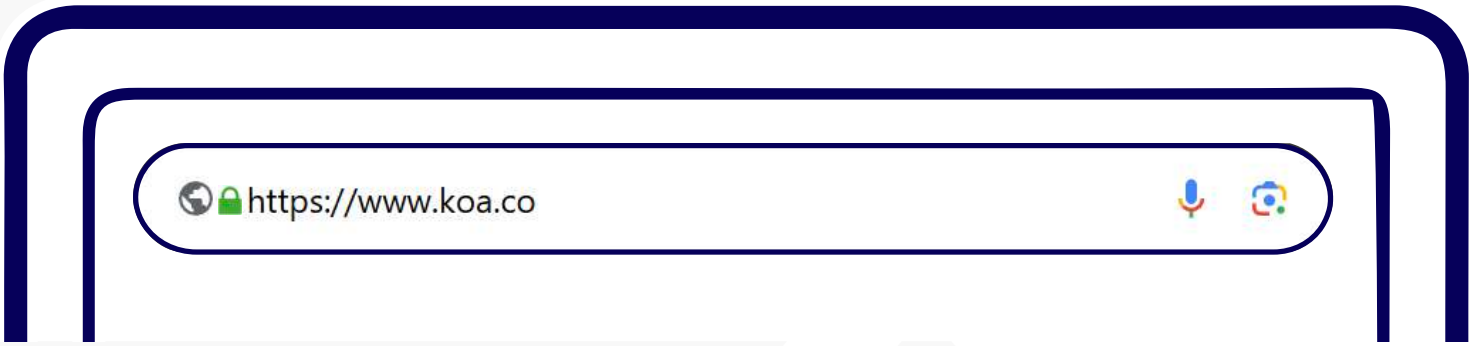
3 Portal clientes Koa

✔ No uses claves fáciles de adivinar para acceder a tu portal de clientes KOA
✔ Recuerda que nunca te pediremos tus claves de acceso a través de correos electrónicos o mensajes de texto.
✔ No hagas modificaciones de seguridad en tu celular, como el "root" o "rootear".
✔ Asegúrate de cerrar correctamente tu sesión al finalizar.

Siguiendo estos simples pasos, podrás disfrutar de la comodidad y seguridad de abrir tu CDT digital KOA sin preocupaciones. **¡Cuida tu información y haz tus transacciones de forma segura!**

4 Seguridad en transacciones por internet:

✔ No abras archivos adjuntos que vengan en correos en cadena, ya que podrían contener virus.
✔ Mantén siempre actualizado y activo un antivirus en tu computadora.
✔ Usa solo computadoras de confianza para hacer transacciones y evita hacerlo desde redes públicas o dispositivos compartidos, ya que podrían guardar tu información y poner en riesgo tus cuentas.
✔ Escribe directamente la dirección de la entidad en el navegador: **www.koa.co** No uses enlaces que lleguen por correo electrónico.
✔ Antes de realizar cualquier transacción, asegúrate de que haya un símbolo de candado en la barra de dirección, lo que indica que la conexión es segura. Además, revisa que la dirección comience con “https”. Ejemplo:



✔ Al hacer compras en línea, verifica que la página sea segura antes de ingresar números de tarjetas de crédito o cualquier dato confidencial.
✔ Al finalizar tus operaciones en la banca virtual, recuerda siempre cerrar tu sesión.
✔ No guardes tus credenciales en el navegador; memorízalas e ingrésalas manualmente cada vez.
✔ Mantén tu dispositivo de seguridad (token) en un lugar seguro y privado, sin compartirlo con nadie ni dejarlo a la vista.

5 Seguridad en oficinas o sucursales

- ✔ Realiza tus transacciones y entregas de dinero solo con el personal autorizado en las cajas de la entidad.
- ✔ Evita retirar grandes sumas de dinero; opta mejor por cheques de gerencia o transferencias electrónicas.
- ✔ Si necesitas retirar mucho efectivo, cuenta el dinero en la caja y solicita el acompañamiento de la policía.
- ✔ Mantente alerta ante personas con comportamientos sospechosos dentro o fuera de la entidad.
- ✔ Si ves algo fuera de lo normal, avisa de inmediato a los colaboradores de KOA C.F.

6 Seguridad de la información en tarjetas Crédito / Débito

Sigue estas recomendaciones de seguridad para que tus transacciones estén siempre protegidas:

✔ Personaliza tu tarjeta en el espacio en blanco que se encuentra en la parte trasera, con tu nombre o alguna marca que te permita identificarla fácilmente.
✔ **NO** pierdas de vista tu tarjeta cuando hagas compras.
✔ **NO** olvides verificar si hay personas sospechosas a tu alrededor.
✔ Al ingresar tu clave, cubre el teclado con la mano para evitar que cámaras ocultas o personas cercanas puedan ver lo que estás digitando.
✔ **NO** aceptes ayuda de desconocidos en los cajeros automáticos.
✔ Antes de retirar dinero en un cajero automático, revisa que no haya dispositivos extraños en la ranura donde insertas tu tarjeta o un teclado sobrepuesto.
✔ Evita retirar dinero en lugares inseguros o a horas poco recomendables.
✔ Si por alguna razón tu tarjeta es retenida en el cajero, no te retires hasta finalizar o anular la transacción.
✔ Memoriza tu clave, no la lleves escrita ni la apuntes en ningún lugar, y recuerda cambiarla de manera periódica.
✔ En caso de cancelar tu tarjeta, destrúyela raspando la firma, cortando el plástico en pedazos y asegurándote de que el chip quede inutilizable.

7 Seguridad con Tarjetas Contactless (Sin contacto)

✔ **Revisa tu estado de cuenta regularmente:** Las tarjetas contactless permiten hacer pagos pequeños sin PIN, lo que puede hacer que algunos cargos pasen desapercibidos. Por eso, revisa tu estado de cuenta y reporta cualquier transacción sospechosa.

✔ **Activa notificaciones en tu celular:** Configura tu teléfono para recibir alertas del banco cada vez que uses tu tarjeta contactless. De esta manera, si alguien más la utiliza, recibirás una notificación de inmediato.

8 Seguridad en tu celular

✔ Siempre que puedas, instala un antivirus en tu celular.
✔ Evita conectarte a redes Wi-Fi públicas.
✔ Activa el Bluetooth y Wi-Fi solo cuando los necesites.
✔ Configura tu celular con medidas de seguridad como huella digital, contraseña, pin o patrón de desbloqueo.
✔ No abras enlaces sospechosos que lleguen por mensajes de texto.
✔ No conectes tu celular a dispositivos desconocidos o sin protección.
✔ No guardes en las notas del celular información confidencial como usuarios, contraseñas o datos financieros.
✔ Si pierdes tu teléfono, cambia tus contraseñas de inmediato e informa a tu banco.
✔ Evita usar teléfonos de otras personas para hacer transacciones.
✔ No descargues contenido a través de enlaces recibidos en mensajes de texto que no hayas solicitado.

9 Seguridad con las contraseñas

✔ Crea contraseñas que combinen mayúsculas, minúsculas, números y símbolos.
✔ No uses nombres, fechas de nacimiento, hobbies o información fácil de adivinar.
✔ Cambia tus contraseñas regularmente y memorizarlas.
✔ Evita reutilizar las últimas dos contraseñas que hayas tenido.
✔ Nunca compartas tus contraseñas con nadie.
✔ No entregues tus claves a ninguna persona, aunque digan ser de la entidad.
✔ Ten cuidado con personas que fingen ser empleados de la entidad para ofrecer premios o promociones y te pidan tus claves.
✔ Recuerda que tus contraseñas son privadas y deben cumplir con ciertas medidas de seguridad.
✔ Si tienes alguna duda o preocupación sobre seguridad, contacta la **línea de atención al cliente KOA 018000184095** o al **WhatsApp: 3157706670**

10 Seguridad al usar datáfonos

✔ Al hacer pagos, asegúrate de que solo usen tu tarjeta en datáfonos o dispositivos autorizados y nunca la pierdas de vista.
✔ Si tu tarjeta tiene chip, no permitas que la pasen por la banda magnética del datáfono.
✔ Si notas algo extraño en la manipulación de la tarjeta, avisa de inmediato a tu banco.
✔ Guarda siempre el número de contacto de tu banco para emergencias.
✔ Si pierdes tu tarjeta o te la roban, repórtalo de inmediato a tu entidad financiera y presenta la denuncia correspondiente.
✔ Firma siempre tus tarjetas y los comprobantes de compra.
✔ Ten cuidado con las aplicaciones que descargas en tu celular.