Recomendaciones de seguridad

En Banco Activo, Banco Universal C.A. trabajamos para incorporar sistemas tecnológicos y mecanismos de seguridad que permitan resguardar y proteger tu información.

Por tratarse de tu seguridad, hemos creado esta sección para brindarle algunas recomendaciones y así evitar ser víctima de fraudes.

Importante: Banco Activo, Banco Universal C.A. enviará mensajes de texto (SMS) a tu número de teléfono celular sobre transacciones realizadas. Reporta inmediatamente cualquier discrepancia a través de nuestro Centro de atención 0501 ACTIVO-1 (2284861).

Recuerda: Banco Activo, Banco Universal C.A. nunca solicitará por correo electrónico o por teléfono, datos confidenciales tales como contraseñas de tu cuenta personal. Mantén actualizados tus números telefónicos dirigiéndote a cualquiera de nuestras oficinas.

Te invitamos a tomar en cuenta las siguientes recomendaciones para aumentar tu seguridad en: uso clave personal, uso de Internet, tarjetas de crédito y débito, emisiones de cheque, cajeros automáticos y uso de las oficinas comerciales.

Uso de clave personal

- Debes utilizar alguna técnica propia para la construcción de las contraseñas, de forma tal que sean lo suficientemente complejas, y que un tercero no pueda deducirlo, pero tú la puedas recordar fácilmente.

- Es importante que combines letras en Mayúscula y Minúscula, junto con números.

- Nunca reveles tu clave de operaciones electrónicas (ATM, POS), así como la de Banca por Internet a terceras personas.

- No recomendamos utilizar como clave personal:
    - Número de identificación
    - Número telefónico
    - Fechas de nacimiento

Uso de Internet

- Accede siempre a tu cuenta con clave personal desde computadoras seguras, y evita hacer consultas y/o transacciones bancarias en equipos de uso público.
- Si deseas ingresar a la banca por Internet, introduce la dirección web: www.bancoactivo.com.
- Nunca utilices un enlace desde un correo electrónico para acceder al sitio web de Banco Activo, porque podría ser falso. Para evitarlo introduce la dirección www.bancoactivo.com.
- Nunca contestes ningún correo electrónico que pida información financiera o tus datos personales, incluso si tiene apariencia oficial. Evita ser víctima de correos maliciosos.
- Banco Activo nunca te enviará correos electrónicos solicitando tu usuario, claves de acceso, números de tarjeta, número de cuenta o cualquier otra información confidencial. No contestes este tipo de correos electrónicos.

Uso de tarjetas de crédito y débito

- Cuando recibas tu tarjeta de crédito asegúrate de que el sobre de seguridad no haya sido abierto y que cumpla con las medidas de protección señaladas en el mismo.
- Evita perder de vista tu tarjeta de crédito al pagar en establecimientos comerciales, y verifica que sea la tuya cuando te la devuelvan.
- No suministres a extraños el número de tu cédula de identidad, el de tutarjeta de crédito ni la fecha de vencimiento, con el fin de participar en supuestos sorteos o promociones.
- Al realizar compras por Internet, hazlo en comercios que garanticen la confidencialidad de tus datos personales y de tu tarjeta.
- Evita dejar la documentación personal dentro del automóvil, especialmenteen los valet parking. En caso de salir de viaje, jamás dejes tus tarjetas en la habitación, ni guardadas en la maleta.
- En caso de que te hayan sido robadas, debes reportar al banco el plagio; exige nuevos números de tarjetas.
- Cuando retires efectivo de cajeros automáticos, observa a tu alrededor pues quizá alguien te observe con el objetivo de conocer tu clave y clonar tu tarjeta.

- Cuando tengas en tus manos las facturas correspondientes por el uso de tu tarjeta, revisa cuidadosamente para percatarte si no se han realizado compras no autorizadas con éstas.
- Es recomendable verificar los estados de cuenta de cada una de tus tarjetas y compararlos con las copias correspondientes de tus compras.
- En caso de que la tarjeta haya vencido, esté deteriorada o haya sido cancelada, se recomienda raspar la firma y cortar el plástico en fragmentos.
- Nunca proporciones tu contraseña de tarjeta a ningún extraño.
- Se recomienda portar las tarjetas de crédito que se utilizarán, no más de dos tarjetas bancarias, en caso de ser necesario, se deben cargar en un lugar distinto a la billetera.
- Al realizar el pago por una compra, procura que la transacción se realice siempre en tu presencia y cuando la tarjeta sea devuelta, corrobora que sea la tuya.
- No prestes tu tarjeta ni permitas que otras personas la usen a tu nombre.
- En caso de pérdida o extravío debe comunicarse a través del Centro de atención 0501 ACTIVO-1 (2284861).

Emisión de cheque

- Cuida tus cheques en blanco como si se tratara de dinero en efectivo. Evita que alguien más tenga acceso a estos cheques y a la información de sus cuentas.
- Verifica siempre tu chequera, ya que en ocasiones los cheques sustraídos por extraños suelen estar entre los últimos o en la mitad del talonario, para evitar sospechas.

Uso de cajeros automáticos

- No retires altas sumas de dinero en cajeros automáticos en sitios inhóspitos, a horas nocturnas.
- Procura que personas extrañas que permanezcan a tu alrededor mientras realizas alguna operación mantengan una distancia prudencial mientras ingresas tu clave secreta.

Tipos de fraudes

- Smishing

Se denomina smishing a todo ataque de phishing que se perpetra mediante el envío de un SMS, habitualmente simulando que el remitente es un banco o cualquier otro organismo que despierte confianza en el receptor.

- Whishing

El whishing es igual que el smishing, pero en este caso recurre a WhatsApp para enviar mensajes instantáneos con, por ejemplo, ofertas o promociones de marcas populares.

- Pharming

El término pharming hace referencia a la inclusión de un enlace en el mensaje enviado para que el usuario haga clic y crea que está navegando en un sitio web determinado. En realidad, lo que está haciendo es adentrarse en una página web falsa creada por los ciberdelincuentes para obtener sus datos personales.

- SIM swapping

Una de las últimas variantes de phishing, no por ello menos peligrosas. El SIM swapping consiste en el duplicado de la tarjeta SIM de alguien para suplantar su identidad y acceder así a sus credenciales del banco.

- Spear phishing

El hacker que comete un ataque de spear phishing pretende engañar a un individuo en particular y, para ello, elabora un mensaje 100% personalizado tras estudiarlo detenidamente a través de sus redes sociales.

- Vishing

La técnica del vishing se diferencia del resto en que se desarrolla mediante una llamada de voz, en la que el phisher se hace pasar por otra persona (por ejemplo, un miembro del equipo de Microsoft) para convencer a la víctima de que realice un acto concreto, como facilitarle su tarjeta de crédito para adquirir la nueva actualización de su antivirus.

- Qrshing

Como el resto de las formas de phishing, el qrshing busca adaptarse a las tendencias actuales, en este caso simulando un código QR de una supuesta marca o comercio pero que enlaza a un sitio web fraudulento. Lo que se suele hacer es

crear y pegar adhesivos con estos códigos en las mesas de los bares o en los escaparates de las tiendas.

- Skimming

Es la captura y transferencia no autorizadas de datos de pago a otra fuente. Su finalidad es cometer fraude, la amenaza es grave y puede golpear el entorno de cualquier comerciante. Los ladrones pueden robar datos de pago directamente de la tarjeta de pago del consumidor o de la infraestructura de pago en una ubicación del comerciante. Ambas técnicas suelen requerir el uso de un dispositivo físico deshonesto instalado en el sitio.

Medidas de protección

- No te conviertas en víctima, cuando ingreses a Internet recuerda que existen muchos programas espías que se auto instalan durante tu conexión, introduciéndose en tu PC y obteniendo toda la información.

- Para evitarlo instala en tu computadora de uso frecuente un firewall, ya que es la mejor manera de evitar controlar todo lo que entra y sale de tu computador.

Recomendaciones en oficinas comerciales

- Realice sus operaciones únicamente en las taquillas expresamente señaladas.

Centro de atención

- 0501 ACTIVO-1 (2284861)
- atcliente@bancoactivo.com