Recomendaciones de Seguridad

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

Por tratarse de su 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 su número de teléfono celular sobre transacciones realizadas. Reporte inmediatamente cualquier discrepancia a través de nuestro Centro de Atención Activa 0500 ACTIVAT (2284828)

Recuerde: Banco Activo, Banco Universal C.A. nunca solicitará, por correo electrónico o por teléfono, datos confidenciales tales como contraseñas de su cuenta personal. Mantenga actualizado sus números telefónicos dirigiéndose a cualquiera de nuestras oficinas.

Le invitamos a tomar en cuenta las siguientes recomendaciones para aumentar su 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

- Debe 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 usted siempre lo pueda recordar fácilmente.

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

- Nunca revele a terceras personas su clave de Operaciones Electrónica (ATM, POS) así como la de Banca por Internet.

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

Uso de Internet

- Acceda siempre a su cuenta con clave personal desde computadoras seguras, y evite hacer consultas y/o transacciones bancarias en equipos de uso público.
- Si desea ingresar a la banca por Internet, introduzca usted mismo la dirección web: www.bancoactivo.com
- Nunca utilice un enlace desde un correo electrónico para acceder al sitio Web de Banco Activo, porque podría ser falso. Para evitarlo introduzca usted mismo la dirección www.bancoactivo.com
- Nunca conteste ningún correo electrónico que le pida información financiera o sus datos personales, incluso si tiene apariencia oficial. Evite ser víctima de correos maliciosos
- Banco Activo nunca le enviará correos electrónicos solicitando su usuario, claves de acceso, números de tarjeta, número de cuenta o cualquier otra información confidencial. No conteste este tipo de correos electrónicos

Uso de Tarjetas de Crédito y Débito

- Cuando reciba su tarjeta de crédito asegúrese de que el sobre de seguridad no haya sido abierto y que cumpla con las medidas de protección señaladas en el mismo.
- Evite perder de vista su tarjeta de crédito al pagar en establecimientos comerciales, y verifique que sea la suya cuando se la devuelvan.
- No suministre a extraños el número de su cédula de identidad, el de su tarjeta de crédito ni la fecha de vencimiento, con el fin de participar en supuestos sorteos o promociones
- Al realizar compras por Internet, hágalo en comercios que garanticen la confidencialidad de sus datos personales y de su tarjeta.
- Evita dejar la documentación personal dentro del automóvil, especialmente en los valet parking. En caso de salir de viaje, jamás dejes en la habitación, ni guardadas en la maleta tus tarjetas.
- En caso de que te hayan sido robadas se debe 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 que la tarjeta haya vencido, este 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 Activa 0500 ACTIVAT (2284828)

Emisión de Cheque

- Cuide sus cheques en blanco como si se tratara de dinero en efectivo. Evite que alguien más tenga acceso a estos cheques y a la información de sus cuentas.
- Verifique siempre su 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 retire altas sumas de dinero en cajeros automáticos en sitios inhóspitos a horas nocturnas
- Procure que personas extrañas que permanezcan a su alrededor mientras realizas alguna operación mantengan una distancia prudencial mientras realiza el ingreso de su clave secreta.

Tipos de Fraudes

- El “Pharming” consiste en direccionar al usuario a una página Web falsa con un entorno semejante a la página web solicitada.
- El keylogger captura todo lo que escribe la víctima y lo envía a una dirección de correo electrónico configurado por su administrador recibiendo contraseñas, números de tarjetas, cuentas, y demás datos financieros que al ser utilizados por personas malintencionadas, el titular puede ser víctima de una estafa sin darse cuenta. Para evitarlo, debe ingresar a equipos seguros como la PC del hogar.
- El Phishing, consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario. Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas.

Medidas de Protección

- No se convierta en víctima, cuando ingrese a Internet recuerde que existen muchos programas espías que se auto instalan durante su conexión introduciéndose en su PC y obteniendo toda la información.

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

Recomendaciones en Oficinas Comerciales

- Realice sus operaciones únicamente en las taquillas expresamente señaladas.

Centro de Atención Activa 0500 ACTIVAT (2284828)

- Correo Contacto: atcliente@bancoactivo.com