

Canales físicos

Evita fraudes en espacios físicos como fleteo, clonación de tarjetas, suplantación de personal y cambiazo.

Fleteo

Es una modalidad de hurto que ocurre después de retirar grandes sumas de dinero, donde los delincuentes suelen actuar en grupo.

Recomendaciones

- Evita retirar altas sumas de dinero en efectivo. Utiliza transferencias electrónicas o cheques.
- Si vas a retirar altas sumas de dinero, pide el acompañamiento que ofrece la Policía Nacional llamando al 911.
- Si observas la presencia de personas sospechosas en tu entorno, avisa a nuestros funcionarios o a las autoridades.

En cajeros automáticos

Consiste en la instalación de dispositivos no autorizados en los cajeros automáticos y puntos de venta POS en comercios y corresponsales bancarios.

Recomendaciones:

- Verifica que el cajero automático no contenga objetos extraños visibles en el teclado, en el dispositivo de lectura de la tarjeta y en el dispensador del dinero.
- Sólo debes ingresar la tarjeta en puntos de venta, PIN pads o cajeros automáticos autorizados.
- Si por algún motivo debes salir del cajero automático antes de terminar la transacción, anula la operación oprimiendo la tecla "Cancelar".

Suplantación de personal

Los delincuentes se hacen pasar por colaboradores del Banco para engañar a los usuarios y obtener su dinero.

Recomendaciones:

- Nuestros colaboradores siempre portan su credencial de identificación del Banco VisionFund Ecuador.
- Los únicos lugares habilitados en nuestras oficinas para realizar pagos o recibir dinero en efectivo son las cajas/ventanillas.
- Evita dar información sobre las transacciones que vas a realizar en las oficinas bancarias, tales como: monto, tipo, lugar, fecha y hora de transacción.

Seguridad en canales digitales

Aprende a reconocer las amenazas digitales más comunes.

Por correo (phishing)

Los delincuentes intentarán engañarte ofreciéndote premios, descuentos en impuestos o cuotas para obtener tu información personal y la de tus productos financieros como números de tarjeta, códigos de seguridad, cuentas, saldos, etc.

Por llamada (vishing)

Se le conoce como vishing a las llamadas telefónicas falsas que realizan los delincuentes suplantando las comunicaciones oficiales del banco.

Durante la llamada escucharás grabaciones bastante parecidas a las de cualquier servicio telefónico de atención al cliente. Además, te solicitarán información personal y de tus productos financieros con la que podrán ejecutar el fraude.

Por SMS (smishing)

Es el término para los mensajes de texto (SMS) falsos con los que los delincuentes te redirigen a sitios web o números de contacto fraudulentos

Recomendaciones:

- Verifica que el mensaje esté bien escrito, sin errores de ortografía ni digitación y nunca entregues datos personales.
- No contactes a números referenciados en mensajes de texto que te informan sobre posibles bloqueos de tus productos, transacciones inusuales, premios, ofertas, entre otros.

Protección de accesos, protege tus credenciales de acceso

Sigue estas recomendaciones para cuidar tu información personal y financiera.

Por tu seguridad nunca compartas tu usuario y clave ya que estos son tu responsabilidad.

- El usuario y la contraseña son personales e intransferibles. No los dejes escritos o expuestos.
- No utilices claves fáciles de deducir, como fechas de cumpleaños, nombres de tus hijos, nombre de tu empresa, etc.
- Mantén siempre actualizado el sistema de seguridad de los dispositivos que utilices para ingresar a las páginas web del Banco VisionFund Ecuador.
- Te recomendamos que cuando ingreses a nuestra página web, no lo hagas a través de buscadores. Es más seguro digitar directamente en tu navegador. En el caso de las páginas web del Banco te recomendamos digitar directamente <https://visionfund.ec> o <https://bvfenlinea.visionfund.ec>

Si crees que tus claves de acceso han sido comprometidas, cámbialas inmediatamente en todos los sistemas.

SEGURIDAD EN COMUNICACIONES

Desde Banco VisionFund Ecuador nunca te pediremos que compartas claves, códigos, números de tarjetas, ni datos personales por llamadas o mensajes.

Ten presente que te comunicaremos únicamente por medio de correo electrónico y SMS, información referente a:

- Contenido multimedia educativo, demos, videos e infografías que se encuentren en la página web del banco.
- Encuestas de satisfacción de servicio.
- Páginas web de promociones y alianzas especiales que tenemos en el banco.
- Enlaces para suscribirse a las redes sociales del banco.

Correos electrónicos autorizados

En Banco VisionFund Ecuador utilizamos únicamente los siguientes buzones autorizados para el envío de comunicaciones con fines comerciales:

comunicaciones@visionfund.org

Los anteriores correos electrónicos no están habilitados para recibir información. Por eso, si envías cualquier mensaje, no podremos leerlo y se tomará como no recibido.

Redes sociales autorizadas

Facebook: VisionFund Ecuador

Instagram: @visionfundecuador

X: BancoVisionFund

LinkedIn: Banco VisionFund Ecuador

TikTok: @bancovisionfund



Sitios Web autorizados

<https://visionfund.ec>

<https://bvfenlinea.visionfund.ec>

<https://aprendiendoconbvfe.com>