BancoEstado
desde 1855

Manual de bolsillo

para tu bolsillo

Guía práctica para aprender
a usar y cuidar tu plata.

Portada sitio web
“Educación Financiera BancoEstado”

Introducción

En BancoEstado, creemos que **la educación financiera es clave para construir un futuro sólido**. Por eso, este manual es parte de nuestro compromiso de apoyarte en tu camino hacia la estabilidad y el orden financiero.

Aquí encontrarás **consejos prácticos para aprender a usar y cuidar tu plata con responsabilidad y de manera informada**. Encontrarás formas de organizar tus finanzas y establecer metas claras, descubrirás estrategias para aumentar tus ahorros y conocerás opciones de inversión seguras para hacer crecer tu dinero. Además, te enseñaremos a gestionar tus deudas de manera responsable y a proteger tu información financiera en el mundo digital.

Nuestro principal objetivo es proporcionarte las herramientas necesarias para mejorar tu bienestar financiero y alcanzar tus metas con tranquilidad.

¡Avancemos juntos hacia el bienestar financiero!

BancoEstado, un banco para todos **y para cada uno.**

Índice

Pág.

¿Qué es la ciberseguridad?

En un mundo donde las transacciones financieras y el comercio electrónico se han vuelto cada día más frecuentes y masivos, es muy importante conocer las acciones que debemos tomar y los cuidados que debemos tener para evitar ser víctimas de estafas y fraudes que en una gran proporción se realizan a través de Internet.

Así, **la ciberseguridad es el conjunto de acciones, medidas y cuidados orientados a la protección de sistemas y dispositivos informáticos** del contagio de softwares y virus maliciosos, cuyo fin es impedir el robo de información a las personas y/o la toma de control de sus equipos.

A continuación, te contamos de algunos de los ataques informáticos, fraudes y estafas más comunes en la actualidad. Teniendo presente que las técnicas y engaños de los delincuentes van cambiando en el tiempo, siempre es importante mantenerse informado y al tanto de nuevas amenazas.

Virus informático

Es un **programa para modificar, estropear o tomar control de computadoras y móviles**. Se propaga de un equipo a otro, en general estos virus pueden robar contraseñas, registrar pulsaciones de teclado, dañar archivos, enviar spam a los contactos de mail de la víctima e incluso tomar el control del equipo.

Cómo evitarlo

Mantener actualizados los antivirus y el sistema operativo. Hay que ser cuidadoso al navegar por Internet, **no abrir enlaces**, bajar archivos en mail ni mensajes de textos en SMS y WhatsApp, que sean de remitentes no confiables. En las páginas web, no hacer clic en botones que ofrecen sexo, dinero o premios. En el móvil, **no bajar App sospechosas**.

Phishing (suplantación de identidad)

Es un correo electrónico en que el remitente simula un mensaje de un banco, una empresa u otra organización real, ofreciendo rebajas increíbles de algún producto, un mensaje de alerta de un banco, una institución judicial, señalando que se debe hacer clic en un enlace para tomar conocimiento de la situación, así extraen datos como RUT, contraseñas y otros.
Con esta información extraen el dinero del banco o realizan compras online. Una modalidad de fraude similar se realiza a través de mensajes de texto (SMS), llamada, por lo mismo, "Smishing".

Cómo evitarlo

No hacer clic en los enlaces de los correos electrónicos (ni mensajes de SMS), revisar bien la dirección de correo electrónico, leer bien el contenido del mensaje y detectar faltas de ortografía o de gramática y de diseño gráfico (no necesariamente replican las páginas reales con total fidelidad). Si se dirigió a una página sustituta, revisar la URL (dirección web) para ver si coincide con el nombre de la tienda o banco.

Hacking (piratería)

El Hacking es como el Phishing, **se trata de mails de personas conocidas, con las cuales ya hemos intercambiado mails anteriormente**. El remitente, que puede ser un pariente o un amigo, nos invita a hacer clic en un enlace, recomendándonos un sitio web. Esto ocurre porque el ciberdelincuente ingresa a un dispositivo y roba las direcciones de correos y contraseñas y así envía un spam a todas las direcciones de la libreta de direcciones de la víctima.

Cómo evitarlo

Desconfiar de todo mail que porta un enlace en su contenido, incluidos los correos electrónicos de tus parientes y conocidos. Si tienes dudas, comunícate con el remitente del mail para confirmar si el correo es válido o se trata de un ciberataque.

Secuestro de WhatsApp

El "secuestro de WhatsApp" **tiene como finalidad que los estafadores se apoderen de tu cuenta y soliciten dinero en tu nombre a tu lista de contactos, o bien te exijan una suma de dinero para devolverte la cuenta**.
Pero ¿cómo logran robar tu cuenta? El ciberdelincuente solicita reactivar la cuenta que busca robar generando un código de verificación que le llega al usuario por SMS. En ese momento, el estafador llama o escribe por WhatsApp, haciéndose pasar por un ejecutivo que envió el código por error y, en un tono de amabilidad y de urgencia, pide que le entregue el número secreto recibido. Una vez que das los dígitos, ya has perdido el control de tu cuenta de WhatsApp.

Cómo evitarlo

No compartir tu código de verificación, contraseñas u otros datos personales, así como tampoco hacer clic en enlaces dudosos que recibas por mensajería de texto o por la misma aplicación de WhatsApp. Además, resguarda la seguridad de WhatsApp activando la verificación de dos pasos en los ajustes de la aplicación.

Llamada de falso ejecutivo bancario

No es directamente un fraude informático, pero sí una de las estafas más comunes. La víctima recibe una **llamada de teléfono de una persona que se hace pasar por un ejecutivo de su banco**. Para generar confianza, el delincuente se expresa de manera formal como lo haría un verdadero ejecutivo bancario. En la mayor parte de los casos, ya maneja alguna información personal de la víctima. Por medio de una historia como, por ejemplo, que el banco ha detectado un intento de violar su cuenta bancaria o que debe "sincronizar" sus claves, conducirá a la víctima a que le proporcione los datos para robarle dinero o le pedirá que introduzca ella misma una clave de transferencias, con lo cual abonará sus fondos a la cuenta del delincuente.

Cómo evitarlo

Para no ser víctima de esta modalidad de estafa **no debes entregar información privada, números de tu tarjeta de coordenadas o contraseñas**. La regla de oro para evitar fraudes es tener presente que tu banco jamás te solicitará tus claves ni te pedirá hacer clic en un enlace o link. **Desconfía de los números desconocidos y también de promociones o premios**. Simplemente, corta la llamada o, si tienes dudas, comunícate directamente con un ejecutivo de tu banco.

La regla de oro para evitar fraudes es tener presente que tu banco jamás te solicitará tus claves ni te pedirá hacer clic en un enlace o link.

Consejos de prevención

- Mantener actualizado el sistema operativo de tu dispositivo web.
- Tener antivirus y mantenerlo actualizado.
- No abrir ningún enlace, ni descargar archivos sospechosos de los correos electrónicos.
- No ingresar a sitios web falsos, copias de los originales, ya que están contaminados con Malware.
- No actuar de forma impulsiva al recibir un mail que informa que has ganado un premio o descuento.
- Al ingresar a un sitio online para realizar alguna transacción comercial, revisar que la dirección web sea la correcta y que no se trata de una imitación.

Otros consejos de prevención

- Navegar con precaución por sitios web de dudosa procedencia.
- Informarse antes de bajar una App, porque puede contener algún tipo de programa maligno.
- Revisar que una App tenga bastantes números de comentarios respecto de su importancia y que tenga una cantidad y calidad de especificaciones técnicas adecuadas a la App real.
- No realizar transacciones comerciales o de modificación de información personal desde una red pública, como un café, aeropuerto o plaza libre de wifi.
- No instalar antivirus desconocidos de dudosa procedencia.
- Tener cuidado con publicar detalles con información personal en las redes sociales.

Notas:

Notas:


BancoEstado
desde 1855

Un banco para todos y para cada uno.