Manual de Educación Financiera

Para prevenir ser objeto de **fraudes y/o estafas cibernéticas**

Banco Promerica

Conceptos que **debes conocer**

Fraude Cibernético:

Actividad encaminada a obtener de forma engañosa, datos sensibles como información bancaria, credenciales de acceso, información personal para cometer delitos, provocando pérdidas financieras a las víctimas.

Ciberseguridad:

Preservación de la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas de información a través del ciberespacio.

Ciberdelincuente:

Un ciberdelincuente es una persona que utiliza tecnología, como computadoras, dispositivos móviles y redes de Internet entre otros, para cometer delitos y actividades ilícitas.

Ingeniería Social:

Es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información o el acceso a un sistema.

Sim Swap (también conocido como cambio de SIM)

Es una técnica de fraude en la que un ciberdelincuente se apodera del número de teléfono de la víctima mediante la activación de una nueva tarjeta SIM en un dispositivo móvil bajo su control.

Phishing:

Es una técnica de fraude digital y de ingeniería social mediante la cual los ciberdelincuentes suplantan la identidad de entidades legítimas (como bancos, empresas, instituciones públicas o redes sociales) para engañar a las personas y lograr que revelen información confidencial (usuarios, contraseñas, datos bancarios etc.). Este tipo de técnica se ejecuta por medio de correo electrónico.

Vishing

Es una técnica de ingeniería social en la que los delincuentes intentan obtener datos confidenciales mediante llamadas telefónicas.

Canales Digitales

Canales dispuestos por las instituciones supervisadas a los usuarios financieros para la realización de gestiones y transacciones utilizando medios tecnológicos. Pueden ser páginas web, aplicaciones móviles, integraciones con redes sociales, entre otras.

URL (Uniform Resource Locator):

Es la dirección única que identifica la ubicación de un recurso en internet, como una página web, una aplicación o un servicio digital. La URL indica dónde se encuentra y cómo acceder a dicho recurso a través de la red.
Ejemplo: https://www.bancopromerica.com

Billetera Digital (Wallet Digital):

Es una plataforma electrónica que permite almacenar de forma segura tarjetas de crédito o débito en un dispositivo celular para realizar pagos, transferencias y otras transacciones sin necesidad de usar efectivo o tarjetas físicas.

Recomendaciones sobre
los riesgos asociados con el uso de tus productos y servicios por medio de canales digitales

- La apertura de productos y/o servicios digitales son personales, se recomienda no ceder total o parcialmente a un tercero el uso o el control de su producto y/o servicio digital, ya que todos los derechos y obligaciones contractuales que respectan al producto vinculado son intransferibles.
- Se recomienda no permitir el uso de sus productos y/o servicios digitales para transacciones de terceros de las que desconoce su origen, motivo o destino, ya que en cualquier momento el banco puede requerir el soporte de estas.
- Se recomienda no ceder total o parcialmente el uso de los accesos/medios físicos o digitales a su producto financiero digital, entendiéndose por accesos/medios a: Usuario y contraseña de banca en línea, tarjeta de débito y crédito, PIN de seguridad y libreta de ahorros, ya que las transacciones realizadas por estos accesos/medios serán enteramente de su responsabilidad.
- Se recomienda no brindar información sensible a terceros que puedan hacer uso indebido de la misma para acceder a los fondos de sus depósitos. EL BANCO nunca le solicitará datos como usuario, contraseñas, códigos de verificación, tokens o PIN de seguridad, por ende, usted está en autorización de nunca entregarlas.
- Se recomienda reportar a EL BANCO cualquier operación inusual o no reconocida identificada en su cuenta de ahorros y/o tarjeta de crédito.
- Se recomienda utilizar únicamente dispositivos propios y de confianza para acceder a sus productos y/o servicios digitales, evitando el uso de equipos públicos, conexiones a redes WIFI públicas que puedan comprometer la seguridad de su información.
- Se recomienda verificar siempre que los sitios web y aplicaciones utilizadas correspondan a canales oficiales de EL BANCO, evitando acceder mediante enlaces recibidos por mensajes, correos electrónicos o redes sociales de procedencia desconocida.
- Se recomienda cerrar correctamente la sesión de sus productos y/o servicios digitales una vez finalizadas sus operaciones, especialmente cuando se accede desde dispositivos móviles o compartidos.

Algunas tipologías existentes de fraudes

Prácticas de ingeniería social que utilizan los estafadores para obtener información confidencial: Llamadas telefónicas suplantando al personal del banco, mensajes a aplicaciones de comunicación, correos electrónicos invitando a hacer clic en URL falsos, SMS (mensajes de texto), entre otros. Un ejemplo es la típica llamada del "empleado bancario" que nos alerta de un cargo a nuestra tarjeta de débito o crédito en realidad se trata de un engaño conocido como vishing en el que los estafadores se hacen pasar por representantes de una institución y convencen a los usuarios de que existe un problema con su cuenta.

Solicitud de dinero: Existe un tipo de fraude cibernético en el que le solicitan que transfiera dinero, ya sea a través de un amigo que le envía un aviso urgente por correo electrónico o a través de redes sociales. Otro escenario también común es aquel en el que recibe una notificación de que tiene derecho a la herencia de un familiar perdido desde hace mucho tiempo, pero debe enviar dinero para reclamar por esa parte.

Vendedores o compradores sospechosos: Al comprar o vender en línea, siempre asegúrese de que cualquier transacción haya sido liquidada antes de entregar artículos a un comprador, así como tener los comprobantes de la operación. Nunca confíe en un comprador o vendedor que se niegue a hablar por teléfono o reunirse en persona con usted.

Algunas tipologías existentes de fraudes

Ataques de Phishing: Los ciberdelincuentes mediante correos que aparentan ser de sitios que utilizamos frecuentemente, solicitarán que realice acciones que podrán comprometer la seguridad de sus accesos. Por ejemplo: solicitando que por medio de un código QR y/o través de un link acceda a cambiar sus credenciales de acceso, haciendo énfasis en que si no actualiza en determinada fecha su cuenta será bloqueada.

Smishing: Es el envío de mensajes de texto con un vínculo para que entre a esa página fraudulenta y le roben sus datos.

SIM SWAPPING o intercambio de SIM: Ocurre cuando un delincuente engaña a un proveedor de servicios de telefonía móvil para que transfiera el número de teléfono de un cliente hacia la tarjeta SIM del delincuente. Luego, puede suplantar la identidad del propietario ante servicios bancarios y redes sociales para robar dinero.

Derechos y obligaciones **de los usuarios sobre este particular**

• Tienes derecho a recibir educación financiera de parte de la institución financiera para prevenir ser objeto de fraudes y/o estafas cibernéticas.

• Tienes derecho a conocer cuáles son los riesgos al contratar un producto y/o servicio de manera digital y/o física.

• Estás en la obligación como usuario financiero de examinar a detalle cualquier situación que se salga de lo ordinario y en caso de que se dé cuenta de un ataque en progreso, avisar al banco lo antes posible para mitigar los riesgos de fraude.

• En caso de ser víctima de un fraude cibernético debes realizar una denuncia ante las autoridades competentes.

• Tu labor es estar atento y hacer todo lo que esté a tu alcance para detener los intentos de fraude cibernético, pues cualquier persona puede ser víctima de una estafa por internet. Manten tu dinero seguro, y toma en cuenta las medidas de seguridad necesarias para protegerte ante cualquier fraude cibernético.

• Monitorea tus cuentas: verifica la actividad de tu cuenta con frecuencia para detectar actividad inusual. Si percibes algo que no está dentro de lo normal, comunícate con El BANCO de inmediato.

Consejos para prevenir ataques de Phishing

1. Aprende a identificar los correos electrónicos sospechosos

- Utilizan nombres y adoptan la imagen de empresas reales.
- Incluyen webs que visualmente son iguales a las de empresas reales.
- Como señuelo utilizan regalos o el bloqueo y pérdida de tu cuenta.

2. Verifica la fuente de información de tus correos entrantes

- EL BANCO nunca te pedirá el envío de información sensible relacionada con tus productos bancarios por correo (usuario, claves, pines, tokens.) Nunca respondas a este tipo de preguntas y si tienes una mínima duda, llama directamente a tu banco para aclararlo.

3. . Nunca ingreses al sitio web de tu banco haciendo clic en enlaces

- No hagas clic en los hipervínculos o enlaces que te adjunten en el correo, ya que de forma oculta podrían dirigir a una web fraudulenta, mejor teclea directamente la dirección web en tu navegador.

4.Introduce tus datos confidenciales únicamente en webs seguras, validando el URL/dominio completo.

5. Ante la mínima duda sé prudente y no te arriesgues.

Otras recomendaciones

Protege el correo electrónico personal registrado para hacer uso de los canales digitales, con doble factor de autenticación y el uso de contraseñas robustas, ya que este es el principal canal para recuperar tus credenciales y, por tanto, el objetivo principal de los ciberdelincuentes.

- No abras enlaces de fuentes dudosas, el phishing es una de las principales técnicas para realizar ataques de Doxing y robar información.
- Hacer uso de la aplicación oficial para tu seguridad, descarga aplicaciones solo desde las tiendas autorizadas: Google Play Store, Apple App Store y no desde fuentes no autorizadas.
- Debes ser capaz de reconocer una URL oficial contra una fraudulenta. Ejemplo de URL maliciosa: al colocar el mouse sobre el link “actualiza aquí”, se puede visualizar el nombre real del sitio utilizado, en este caso el sitio apunta a una dirección fuera de los recursos tecnológicos del banco.
- Detecta un ataque de secuestro de número telefónico (SIM Swap) identificando señales como la pérdida repentina de señal, la imposibilidad de realizar o recibir llamadas y mensajes, o notificaciones de cambios no solicitados en tus cuentas. Ante cualquiera de estas señales, contacta de inmediato al servicio al cliente de la institución para reportar la posible suplantación de tu tarjeta SIM y solicitar el congelamiento preventivo de tus cuentas.
- Protege tus contraseñas creando claves fuertes, difíciles de descifrar y fáciles de recordar para ti.

¿Cómo lograr el balance? Sigue estos 3 pasos:

- Utiliza las iniciales de una frase fácil de recordar
- Esconde el resultado transformando caracteres
- Personaliza la clave para cada aplicación

Recuerda: Las contraseñas deben ser mayor a 12 caracteres, contener mayúsculas, minúsculas, números y caracteres especiales.

Signos para detectar un fraude cibernético

- *Ningún banco te pedirá información por mail*
- *Actividad inusual en tu cuenta*
- *Una solicitud de dinero urgente*
- *Alertas de movimientos desconocidos*
- *Llamadas o mensajes sospechosos*
- *Vendedores o compradores sospechosos*
- *Correos electrónicos que solicitan información*
- *Una oferta demasiado buena para ser verdad*
- *No consideres correos en que te piden actualizar tu tarjeta y te soliciten datos*

Manual de
Educación Financiera

Banco Promerica