Manual de Educación Financiera

para prevenir ser objeto de fraudes y/o estafas cibernéticas

Banco Promerica


Banco Promerica
República Dominicana
Banpro
Grupo Promerica
Nicaragua
St. Georges Bank
Grupo Promerica
Islas Caimán
Panamá
Banco Promerica
Guatemala
El Salvador
Honduras
Costa Rica
Produbanco
Grupo Promerica
Ecuador

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.

Recomendaciones sobre los riesgos asociados con el uso de sus 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, 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 solicitara 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.

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 URLs falsos, SMS, 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.
- **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 desde 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.

- Estas 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 debe realizar una denuncia ante las autoridades competentes.

- Su labor es estar atento y hacer todo lo que esté a su alcance para detener los intentos de fraude cibernético, pues cualquier persona puede ser víctima de una estafa por internet. mantenga su dinero seguro, y tome en cuenta las medidas de seguridad necesarias para protegerse ante cualquier fraude cibernético.

- Monitoree sus cuentas: Verifique la actividad de su cuenta con frecuencia para detectar actividad inusual. Si percibe algo que no está dentro de lo normal, comuníquese con el Banco de inmediato.

Consejos para prevenir ataques de Phishing

1. Aprenda 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 perdida de su cuenta.

2. Verifique la fuente de información de sus correos entrantes

- El banco nunca le pedirá él envió de información sensible relacionada con sus productos bancarios por correo (usuario, claves, pines, tokens.) Nunca responda a este tipo de preguntas y si tiene una mínima duda, llame directamente a su banco para aclararlo.

3. Nunca entre en la web de su banco pulsando en links

- No haga clic en los hipervínculos o enlaces que le adjunten en el correo, ya que de forma oculta podrían dirigir a una web fraudulenta, mejor teclee directamente la dirección web en su navegador.

4. Introduzca sus datos confidenciales únicamente en webs seguras

- Las webs 'seguras' han de empezar por 'https://' y debe aparecer en su navegador el icono de un pequeño candado cerrado.

5. Ante la mínima duda sea prudente y no se arriesgue

Otras recomendaciones

- Proteja 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 sus credenciales, y, por tanto, el objetivo principal de los ciberdelincuentes.
- No abra 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. La aplicación oficial se deberá descargar solamente desde las tiendas oficiales de aplicaciones móviles y no desde fuentes no autorizadas.
- Debe ser capaz de reconocer una URL oficial contra una fraudulenta. Ejemplo: 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.
- Detecte un ataque de secuestro de número telefónico (SIM Swap), de manera que logre identificar la suplantación de su tarjeta SIM y comunicarse con servicio al cliente de la Institución para el congelamiento de sus cuentas.
- Proteja sus contraseñas de un ataque, pues si son complejas se olvidan y si son fáciles se vulneran. ¿Como lograr el balance? Sigue estos 3 pasos:
  - o Utilice las iniciales de una frase fácil de recordar
  - o Esconda el resultado transformando caracteres
  - o Personalice la clave para cada aplicación

De esta manera conseguimos una contraseña fuerte, difícil de descifrar y fácil de recordar para nosotros.

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

Signos para detectar un fraude cibernético

Actividad inusual en tu cuenta

Alertas de movimientos desconocidos.

Llamadas o mensajes sospechosos

Correos electrónicos que solicitan información

Una oferta demasiado buena para ser verdad

Una solicitud de dinero urgente

Vendedores o compradores sospechosos

No consideres correos en que te piden actualizar tu tarjeta y te solicitan datos.

Ningún Banco te pedirá información por mail.

Desconfía y no respondas ese tipo de correos.

Banco Promerica