SEGURIDAD EN TU APP

Pág. 3

EVITALOS FRAUDES CIBERNÉTICOS

Pág. 4

SUPLANTACIÓN DE IDENTIDAD BANCARIA

Pág. 8

CUIDA TU LLAVERO DIGITAL***

Pág. 6

AMENAZAS FANTASMA:

NUEVOS FRAUDES SILENCIOSOS

Pág. 9

DETECTACORREOS FALSOS

Pág. 7

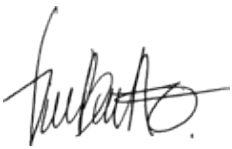
CARTA EDITORIAL

Nos emociona encontrarte de nuevo en estas páginas porque este 2023 iniciamos con un propósito claro: queremos que entres de lleno al mundo digital y domines la banca en línea, móvil y las apps financieras. Por eso, te preparamos con los mejores consejos para disfrutar de estas herramientas de manera segura.

En esta edición la banca digital es protagonista y por eso hacemos un repaso breve de su historia y de cómo usarla adecuadamente. Te enseñamos cómo cuidar tus contraseñas y a estar alerta para detectar correos falsos en tu bandeja electrónica.

También queremos que estés actualizado en temas de fraudes cibernéticos, porque siguen surgiendo nuevas variantes que atentan contra la salud de tus finanzas. Por esta razón te damos consejos de seguridad para protegerte en todo momento.

¡Que este 2023 tus finanzas crezcan de manera segura!



Viviana Bueso
Gerente General Banco Azteca Honduras

CONTACTO

aprendeycrece@bancoazteca.com

SEGURIDAD EN TU APP

La banca móvil es una gran aliada para facilitar las operaciones del día a día. Por eso es importante tomar ciertas medidas de seguridad al usar tu App.

1. Úsala cuando estés conectado a una red WiFi doméstica o confiable. Evita las redes públicas.

2. No instales aplicaciones que no estén disponibles en las tiendas de Android o Apple.

3. No permitas que alguien más manipule tu App sin tu consentimiento.

4. Al acudir a una sucursal, los ejecutivos sólo podrán guiarte, pero no están autorizados para operar tu App ni para ingresar información.

5. Si extravías o te roban el celular, solicita el bloqueo de tu App a tu institución financiera.

Toma en cuenta estos consejos y protege tus finanzas.

EVITALOS FRAUDES CIBERNÉTICOS

La banca digital ofrece muchas ventajas, pero también se ha vuelto un entorno vulnerable a los ciberataques. Aquí te decimos cómo protegerte.

ESTAFAS DIGITALES

PHISHING

Robo de información a través de correos electrónicos fraudulentos.

SMISHING

El robo se comete por medio de mensajes de texto o chats.

VISHING

Son estafas por teléfono en las que un delincuente se hace pasar por empleado de algún banco.

ANGLER PHISHING

A través de perfiles falsos en redes sociales, los delincuentes pueden robar tu información.

5 CONSEJOS DE SEGURIDAD

1. Al acceder a tu banca en línea, asegúrate de usar una red doméstica.

2. Usa contraseñas complejas para tener mayor seguridad.

3. No compartas datos confidenciales por teléfono o por redes sociales.

4. Monitorea tus estados de cuenta periódicamente.

5. No permitas que alguien más manipule tus *apps* financieras.

Si detectas alguna anomalía, repórtalo a tu institución financiera

CUIDA TU LLAVERO DIGITAL***

Para usar los servicios de la banca en línea, debes contar con un usuario, contraseña y clave de seguridad. Aquí te decimos cómo cuidarlos.

CONTRASEÑAS SEGURAS

Memoriza tu usuario, contraseña y clave de seguridad. No los compartas.

Utiliza una clave que no tenga datos personales.

Usa contraseñas únicas en tu banca en línea y en tu App. No recicles las de otras cuentas.

Renueva tus contraseñas cada 3 meses.

CAMBIA O RECUPERA TUS CONTRASEÑAS

Banca en línea

En "Administración y Seguridad", selecciona "Cambio de contraseñas" y ahí elige la que desees cambiar.
Si la olvidaste, hay una opción que te permitirá recuperarla.

App

Da clic en "Ajustes", luego en "Perfil" y después en "Seguridad y privacidad". Ahí puedes actualizar tu contraseña y tu clave de seguridad.
Si no la recuerdas, puedes recuperarla en la opción "Olvidé mi contraseña".

Protege tu llavero digital con estas medidas.

DETECTA CORREOS FALSOS

El robo de información mediante correos electrónicos es una de las técnicas más recurrentes en el bajo mundo del ciberespacio. Se conoce como *phishing* y aquí te decimos cómo identificarlo.

Características de un correo falso

- Utilizan la imagen de alguna institución, pero el correo es diferente al oficial.
- Solicitan aclaraciones o información de manera urgente.
- Contienen links a sitios falsos.
- Tienen un tono alarmista.
- Te piden que descargues archivos adjuntos.

¿Cómo protegerte?

A. No descargues los archivos adjuntos de correos sospechosos.

B. Actualiza el antivirus de tu equipo personal.

C. No envíes datos personales por correo electrónico.

D. No accedas a tu banca en línea en redes públicas.

E. No des clic en links desconocidos.

Recuerda que ninguna institución financiera te solicitará por ningún medio datos personales ni de tus cuentas.

SUPLANTACIÓN DE IDENTIDAD BANCARIA

Los delincuentes también pueden hacerse pasar por algún banco y contactarte para robar tu información. Por eso te damos recomendaciones para estar alerta.

Maestros del disfraz

Parece que los delincuentes se han preparado en las artes del engaño porque pueden utilizar el nombre y la imagen corporativa de algún banco para cometer un fraude financiero.

1. Primero, te **contactan por teléfono** o por redes sociales.
2. Te ofrecen **créditos** de inmediato que suenan muy atractivos.
3. Piden algún **anticipo como garantía** o gastos de apertura.
4. Reciben el dinero y simplemente **desaparecen.**

¿Cómo protegerte?

Si no consiguen el depósito, al menos buscarán tu información personal para actos ilícitos. Mantente prevenido con estos consejos:

- **Verifica que la entidad financiera esté registrada** en la Comisión Nacional de Bancos y Seguros.
- **Nunca des un anticipo** para obtener un crédito.
- **No entregues información** personal por ningún medio.
- **No uses WhatsApp** para contratar un servicio financiero.

Recuerda que ninguna institución financiera te solicitará por ningún medio datos personales ni de tus cuentas.

AMENAZAS FANTASMA:

NUEVOS FRAUDES SILENCIOSOS

Hay peligros que se desplazan entre las sombras y acechan de manera sigilosa, pero sus consecuencias son tan reales que debemos estar alerta. Aquí te explicamos las nuevas modalidades de fraudes cibernéticos

SIM swapping
El delincuente reporta el robo o extravío de la tarjeta SIM y solicita una reposición con el mismo número. Después recoge el chip con una identificación falsa y así obtiene acceso a tus datos.

Doxing
Hay aplicaciones que te ofrecen préstamos exprés, pero al descargarlas solicitan acceso a tus contactos y a tu galería. Con esta documentación o "docs", los delincuentes te amenazan con exponerte en sitios para adultos o en cualquier red.

Protégete
De acuerdo con la firma de seguridad Kaspersky, la extorsión a través de las aplicaciones de mensajería instantánea creció en un 120% durante el año pasado, por lo que aquí te damos las medidas básicas para protegerte.

- No busques ni aceptes préstamos financieros en redes sociales.
- Activa la verificación en dos pasos de tus plataformas de mensajería instantánea.
- Descarga y usa sólo la aplicación oficial de tu banco.
- Activa las notificaciones de pago vía correo electrónico.
- Si tu chip dejó de funcionar, repórtalo de inmediato con tu proveedor de servicios.

Ilumina todos los rincones de tus finanzas y protégete.