ICBC MÉXICO

PROTÉGETE DEL FRAUDE

PROTÉGETE DEL FRAUDE

A continuación te brindamos algunos consejos para no ser víctima de fraude:

CONSEJOS PARA LA IDENTIFICACIÓN DE CORREOS ELECTRÓNICOS FALSOS:

Los correos electrónicos falsos, tambien son conocidos como Phishing. El Phishing es una técnica de fraude cibernético en la cual un delincuente se hace pasar por una entidad confiable (como un banco) para engañar a la víctima y obtener información sensible, como contraseñas, números de tarjetas de crédito o datos personales.

¿CÓMO FUNCIONA EL PHISHING?

1. Correo Electrónico Falso. Se recibe un correo electrónico que parece provenir de una fuente legítima (por ejemplo, tu banco) pidiéndote que hagas clic en un enlace.
2. Sitio Web Falso: El enlace del correo electrónico te lleva a un sitio web que se ve idéntico al sitio oficial de la entidad, pero es falso. Este sitio pedirá que se ingrese información personal.
3. Robo de Información. Cuando se ingresa la información en el sitio falso, esta es capturada por los delincuentes, quienes la usan para cometer fraudes o robos.

¿CÓMO RECONOCER EL PHISHING?

- Dirección de Correo Sospechosa: Verificar que el remitente sea realmente quien dice ser.
- Errores Ortográficos y Gramaticales: Muchos correos de phishing contienen errores que no se encontraría en comunicaciones oficiales.
- Solicitudes Urgentes: Correos que presionan para actuar rápidamente.
- Enlaces Sospechosos: Pasar el cursor sobre los enlaces sin hacer clic para ver la URL real (la dirección del sitio web). Si no coincide con la URL oficial, es probablemente una estafa.
- Solicitudes de Información Personal: Entidades legítimas nunca pedirán información personal sensible por correo electrónico.

¿QUÉ HACER SI SE SOSPECHA DE PHISHING?

- No hacer clic en enlaces ni abrir archivos adjuntos de correos sospechosos.
- Contactar a la institución a través de medios oficiales para confirmar/verificar la autenticidad del correo, e informar sobre el intento de phishing.

CONSEJOS PARA PROTEGER LA SEGURIDAD DEL ACCESO:

VERIFICA LA DIRECCIÓN DEL REMITENTE

Comprobar que la dirección de correo electrónico desde la cual se recibe el mensaje sea auténtica o legítima y esté asociada con la fuente oficial que afirma ser. Un correo del Banco debería tener un dominio como @icbc.com.mx.

REVISA EL CONTENIDO DEL CORREO ELECTRÓNICO

Ten cuidado con errores gramaticales y ortográficos, así como saludos genéricos como "Estimado Cliente".
Los estafadores frecuentemente crean direcciones de correo que parecen legítimas a primera vista, pero contienen errores menores o variaciones. Por ejemplo, una letra cambiada o un dominio con una ligera modificación.

NO COMPARTAS INFORMACIÓN PERSONAL.

Las instituciones legítimas no solicitan información personal o financiera a través de correos electrónicos no seguros, es decir que entidades confiables, como bancos o compañías de servicios, nunca te pedirán que envíes datos sensibles (como números de cuenta, contraseñas o información de tarjetas de crédito) por medio de correos electrónicos no seguros.

COLOCA EL CURSOR SOBRE EL REMITENTE:

Se puede pasar el cursor sobre el nombre del remitente para ver la dirección completa. Esto ayuda a detectar direcciones de correo que intentan parecerse a las legítimas, pero no lo son.

NO HACER CLIC EN ENLACES SOSPECHOSOS

Verifica a dónde realmente te llevará ese enlace.Esto se hace colocando el cursor del mouse sobre el enlace sin hacer clic. Al hacer esto, en muchos programas de correo electrónico y navegadores web, la URL real (la dirección web) a la que te llevará el enlace aparecerá en la parte inferior de la pantalla o en una pequeña ventana emergente cerca del cursor.
Esto es importante porque los enlaces en correos electrónicos fraudulentos pueden parecer legítimos a simple vista, pero en realidad llevan a sitios web maliciosos diseñados para robar tu información.

¿QUÉ HACER ANTE EL PHISHING?

- Si se recibe un correo que solicita información personal, verifica siempre contactando directamente a la institución a través de sus canales oficiales.
- Nunca compartas o envies datos sensibles por correo electrónico a menos que estés seguro de que es un canal seguro y legítimo.
- Usa canales seguros, esto significa utilizar las aplicaciones oficiales de las instituciones o sus sitios web cifrados (https://) para compartir información personal o realizar transacciones.
- Evita abrir archivos adjuntos sospechosos de remitentes desconocidos, ya que pueden contener malware, que puede dañar tu computadora, robar la información personal o permitir a los delincuentes acceder a tu sistema.
- Si se recibe un correo de alguien que no se conoce, se recomienda ser muy cauteloso con los archivos adjuntos. Si se necesita abrir un archivo adjunto, se debe verificar primero con el remitente si es legítimo. Usar métodos de comunicación distintos al correo recibido para confirmar.
- Usa software antivirus y antimalware actualizados que pueda escanear archivos adjuntos antes de abrirlos.
- Evita abrir archivos adjuntos de remitentes desconocidos para mantener la seguridad de tu información y tus dispositivos.

CONSEJOS PARA LA IDENTIFICACIÓN DE LLAMADAS O MENSAJES DE TEXTO FRAUDULENTOS.

- Las llamadas telefónicas fraudulentas también se les refiere como Voice Phishing o Vishing.
- Los mensajes de texto fraudulentos son conocidos tambén como SMS Phishing o Smishing.
- Son llamadas telefónicas o mensajes de texto que parecen legítimos que buscan engañar al destinatario con la finalidad de obtener información confidencial o realizar acciones financieras no autorizadas.

¿Cómo reconocer una llamada o mensaje de texto fraudulentos?

- Son llamadas o mensajes urgentes o amenazantes, para actuar rápidamente.
- Solicitan información confidencial.
- Corresponden a números de teléfono desconocidos.
- Los mensajes de texto incluyen enlaces o archivos adjuntos sospechosos y tienen ortografía y gramática deficientes.

A continuación se indican algunos consejos a tener en cuenta:

Llamadas fraudulentas.

- Verificar la identidad de la persona que lo contacta. Se sugiere preguntarle su nombre, el nombre de su organización o institución y cargo.
- Desconfíar de llamadas urgentes o amenazantes.
- No proporcionar información confidencial.
- No hacer transferencias o pagos bajo presión.

Mensajes de texto fraudulentos.

- Verificar la autenticidad del remitente, no responder a mensajes sospechosos.
- Desconfíar de mensajes con enlaces o archivos adjuntos sospechosos.
- No proporcionar información confidencial.
- No hacer clic en enlaces sospechosos.
- Revisar la ortografía y gramática del mensaje.
- Actualizar el software del sistema del dsipositivo móvil.

Se recomienda bloquear los números de teléfono sospechosos y reportar cualquier suplantación de identidad a ICBC México a través de los canales de comunicación establecidos.

Uso de canales de comunicación protegidos y cifrados para transmitir información.

Para proteger la información sensible, se sugieren las siguientes medidas:

- Utilizar conexiones HTTPS seguras para realizar transacciones en línea. Verificar que la dirección web del banco comience con "https://" y tenga un candado cerrado en la barra de direcciones.
- Utilizar un navegador actualizado que admita cifrado de 128 bits.
- Mantener actualizados los sistemas operativos y software para garantizar la compatibilidad con protocolos de seguridad avanzados.
- Utilizar contraseñas fuertes y únicas para acceder a las cuentas en línea, ya que protegen la identidad y seguridad en línea del usuario.

CONTRASEÑAS FUERTES

Una contraseña fuerte es una combinación de caracteres que es difícil de adivinar o descifrar, protegiendo de esta manera la seguridad de la cuenta de acceso o sistema.

Las características de una contraseña fuerte son:

- Longitud: Mínimo 12 caracteres.
- Complejidad: Combinar mayúsculas, minúsculas, números y símbolos especiales.
- No repetir contraseñas en diferentes cuentas de acceso.
- No utilizar información personal tal como nombres, fechas de nacimiento, etc.
- Para la creación de contraseñas fuertes se sugiere utilizar un generador de contraseñas, crear una frase u oración complicada, utilizar sustituciones por ejemplo la letra "e" por el número "3".
- No compartir información financiera sensible a través de correos electrónicos o mensajes no cifrados.
- Verificar la autenticidad de los mensajes y notificaciones del Banco antes de tomar acciones.

IMPLEMENTACIÓN DE SOLUCIONES EN LÍNEA COMO SOFTWARE ANTIVIRUS Y ANTIMALWARE

- Se recomienda utilizar herramientas de seguridad, tales como un software antivirus y antimalware para proteger la información y dispositivos que acceden a servicios en línea.
- Mantener estos programas actualizados es esencial porque las amenazas cibernéticas evolucionan constantemente, y las actualizaciones del software de seguridad incluyen nuevas definiciones de virus y mejoras en la detección y eliminación de malware.

A continuación, se recomiendan las siguientes acciones:

- Se debe prever que se realicen las actualizaciones regulares del software antivirus y malware del dispositivo para asegurar que siempre se esté protegido contra las últimas amenazas.
- Las actualizaciones pueden corregir vulnerabilidades en el software que los delincuentes cibernéticos podrían explotar.
- Se recomienda calendarizar escaneos regulares del sistema para detectar y eliminar posibles infecciones.