Recomendaciones de seguridad para E-banking

1- ¿Cómo configuro una contraseña segura para iniciar sesión en Banca personal?

Elegir una contraseña que no se adivine fácilmente es muy importante para mantener a salvo su dinero y sus datos personales. Al configurar la contraseña, no use números consecutivos de su número de tarjeta bancaria, número de A / C, número de tarjeta de identificación, número de teléfono o número de teléfono móvil, o un número de 6 dígitos que incluya la fecha, el mes y el año de tu cumpleaños. No use su número de teléfono, número de placa del automóvil, que se adivinan fácilmente.

Utilice únicamente números, letras alfabéticas en minúsculas, letras en mayúscula y otros caracteres visibles para su contraseña de inicio de sesión de Banca personal. Cuando inicie sesión, se le pedirá que utilice otra en los siguientes casos:

- Si cada número de su contraseña es el mismo,
- Si es una simple contraseña con números
- Si la contraseña incluye números o alfabetos en secuencia normal o inversa.

En estos casos se le sugerimos que cambie la contraseña cuando inicie sesión.

2- ¿Cómo me aseguro de que mi cuenta esté segura cuando uso la banca en línea?

Para asegurar nuestra cuenta al momento de usar la banca en línea es necesario tomar en cuenta los siguientes puntos:

1) Primero, no revele su contraseña a nadie. ICBC México nunca le pide su contraseña por teléfono, correo electrónico o por escrito. Además, mantenga su contraseña en un lugar seguro, no la escriba en su computadora o en algún otro lugar público..

2) No pase su tarjeta de inicio de sesión de Banca por Internet a nadie, no escuche a alguien que no conoce para que le diga cómo usar la tarjeta.

3) Asegúrese de que su navegador use encriptación de 128 bits.

4) Verifique los detalles de sus transacciones.

5) Cuando termine, salga de la banca en línea con los pasos correctos, haga clic en "Cerrar sesión" en la página web. No abandone la computadora antes de cerrar sesión en Internet Banking.

6) Establezca la contraseña como una cadena de 8 caracteres, números más caracteres (mayúsculas y minúsculas). No establezca la contraseña con números consecutivos de su número de tarjeta bancaria, número de A / C, número de tarjeta de identificación, número de teléfono o número de teléfono móvil, o su fecha de nacimiento.

3- Trucos de estafador

(I) Usar virus para transmitir sitios web falsos

Los estafadores clonan una página web que se ve casi idéntica a la página web de un banco real y eligen la dirección de inicio de sesión similar a la dirección del sitio web del banco. Luego, envían la URL del sitio web falso a su computadora utilizando un software de virus o spam y colocan la URL en los sitios web de búsqueda para engañarlo al iniciar sesión y revelar su número de tarjeta, contraseña. Hemos encontrado sitios web falsos como “http://www.1cbc.com.mx”, “http://corpebank2.iclc.com.cn/”, “http://www.icbc.dizhen.com” muy

similar a la URL del sitio web de ICBC México: http://www.icbc.com.mx, https://corpebank2.icbc.com.cn.

(II) Enviar SMS fraudulentos que parecen ser de un banco
Los estafadores envían SMS fraudulentos a su teléfono móvil supuestamente desde su banco, diciéndole que ganó el sorteo o que su cuenta ha sido robada. Luego se le pide que confirme la información de su cuenta iniciando sesión en el sitio web especificado en el SMS. El sitio web es en realidad un sitio falso creado por los phishers para robar su información. Si inicia sesión en el sitio web falso, sus datos personales (número de tarjeta, contraseña, número de identificación) serán capturados por ellos.

(III) Envían correos electrónicos fraudulentos que afirman ser de un banco con la finalidad de engañar y accesar a su sitio web falso. Los estafadores envían mensajes de correo electrónico fraudulentos pidiéndole que haga clic en el enlace del correo electrónico e inicie sesión en una interfaz muy similar a la página web de un banco. Las razones pueden ser: ganar un sorteo, darle consejos, conciliar sus cuentas, su número de cuenta ha sido bloqueado o actualizar el sistema bancario. Una vez que haga clic en el enlace, el número de su tarjeta (A / C) se capturará al ingresar.

(IV) Crear sitios web de comercio electrónico falsos, usar páginas web de pagos falsos para robar la información bancaria en línea de los clientes.
En primer lugar, los ciberdelincuentes eligen un sitio web falso de comercio electrónico y luego publican productos falsificados, como por ejemplo; alibaba.com, mercadolibre.com.mx u otros sitios web de comercio electrónico. Los precios de las mercancías falsificadas suelen ser mucho más baratos que productos similares en el mercado. Los ciberdelincuentes también dejan su celularu otro número de mensajería instantánea y URL de los sitios web falsos de comercio electrónico. Cuando decide comprar la atractiva mercancía de bajo precio y pagar en línea a través del sitio web, se le redirige a una página web de pago aparentemente legítima de un banco. Los ciberdelincuentes capturan su número de tarjeta, contraseña, una vez que ingresa a la página web de pagos falsos.

4- Consejos para evitar estafas en falsos sitios web

Ingrese la URL correcta
Escriba la dirección correcta del sitio web de ICBC México y agréguelo a la carpeta “Favoritos” de su navegador (IE) para un inicio de sesión fácil en ocasiones posteriores. No haga clic en ningún hipervínculo para acceder al sitio web de ICBC México.
El URL del portal web de ICBC México es:
https://corpebank2..com.cn//corporbank/index.jsp?areaCode=6012&dse_locale=es-ES;

Verificar dirección del sitio web
Cuando inicie sesión en la Banca por Internet de ICBC México, verifique si la URL es la misma que la anunciada por ICBC México. Tenga cuidado con las estafas para robar su información confidencial en sitios web falsos que se parecen al sitio web de ICBC México. Las URL de la página de inicio de sesión de Banca Corporativa por Internet ICBC México comienzan con corpebank2.icbc.com.cn.

Compruebe el candado y la seguridad web
El cifrado SSL de 128 bits se utiliza para la página de inicio de ICBC México Personal Internet Banking y la página web de pago en línea. Después de abrir las páginas web anteriores, verifique si se muestran un "candado" en la barra de estado en la esquina inferior derecha del navegador. Haga clic en el candado y deberá ver lo siguiente:
En la página web de inicio de sesión de Banca por Internet, el certificado que coincida con el icono del candado que se muestra en la barra de estado en la esquina inferior derecha del navegador debe ser:
Emitido a: corpebank2.icbc.com.cn
Emitido por: DigiCert Baltimore Root

Actualizar tu software

Instale un firewall en su computadora. Al mantener el software actualizado, hace que sea más difícil para los piratas informáticos robar la información de su cuenta. Además, para evitar que otros utilicen las vulnerabilidades de su software para acceder a la información en su computadora, debe descargar los últimos parches del sistema operativo Windows y asegurarse de que se apliquen.

Manténgase alerta todo el tiempo
ICBC México ha asignado un departamento especial para administrar el sitio web de ICBC México y garantizar que el sitio web funcione sin problemas, sin "mantenimiento del sistema" en general. El sistema ICBC México suspenderá los servicios en caso de una actualización importante. Se dará aviso previo a todos los clientes en el portal web. ICBC México nunca usa correo electrónico, SMS, llamadas telefónicas para pedir a los clientes que cambien la contraseña en una página web específica. Además, un banco nunca informa a los clientes por correo electrónico, SMS o llamadas telefónicas que han ganado un sorteo, y les pide a los clientes que paguen impuestos o franqueo antes de recoger el premio. Si recibe este tipo de correo electrónico, SMS o llamadas telefónicas, llame directamente a la línea directa de atención al cliente de ICBC México (+52) 800-759-5588.

5 - Tenga cuidado con los pagos en línea

Al realizar el pago a través de la Banca por Internet, no abra "Asistencia remota" en el sistema operativo o las herramientas de mensajería instantánea. Verifique la información como el beneficiario, el monto del pago y luego realice el pago solo si no hay error.

Al realizar el pago de compras en línea, verifique el icono de candado que se muestra en su navegador (IE). Haga clic en el icono, debería ver que el certificado se emite a corpebank2.icbc.com.cn, lo que significa que su pago está encriptado;

No caiga en la trampa de alguien que utiliza herramientas de mensajería instantánea para publicar mercancías falsas o de bajo precio, o inicie sesión en las plataformas de pago fraudulentas de alguien y pague una pequeña cantidad para hacer una "prueba de compra", ya que el riesgo es menor. Tenga en cuenta, protejer su número de tarjeta, contraseña o numerales de tarjeta de código para que no sean robados.

6 - ¿Qué es la estafa de sitio web falso?

La página web de sitios falsos es una forma de "phishing". Los Phishers, pretendiendo ser un banco legítimo, crean un sitio web que parece un sitio web de un banco o página web de banca en línea y le envía mensajes fraudulentos para robar su número de tarjeta de registro de banca en línea (ID de inicio de sesión), contraseña, tarjeta de código y luego su dinero.

7- Tipos de sitios web falsos

Página web y contenido similar. Los sitios web falsos incluyen LOGO, imágenes, noticias y enlaces de los sitios web reales para hacer que los sitios web parezcan legítimos, utilizando un diseño y contenido similar.

8- ICBC México garantiza que su banca en línea esté protegida

ICBC México garantiza que su banca en línea esté protegida: ICBC México ofrece una variedad de herramientas de seguridad para garantizar que siempre esté protegido cuando realice operaciones bancarias en línea. Elija la herramienta adecuada para sus transacciones en línea

9 - Dispositivo de contraseña electrónica ICBC México

I. Introducción
El dispositivo de contraseña electrónica ICBC México, es un nuevo producto de seguridad de hardware de banca electrónica ICBC México que viene con una fuente de alimentación y un chip para la generación de contraseña en el interior, una pantalla externa y un teclado digital. El dispositivo de contraseña electrónica ICBC México se puede utilizar en diferentes canales de banca electrónica sin la necesidad de instalar ningún controlador.

II.Clientes de destino
El dispositivo de contraseña electrónica de ICBC México está diseñado para clientes de ICBC México que realizan operaciones bancarias en línea, ya sea en banca personal por Internet, banca móvil o banca telefónica, especialmente aquellos que usan iPhone o iPad para realizar grandes pagos.

III.Características
1. Fácil de usar. El dispositivo de contraseña electrónica ICBC México, no necesita estar conectado a ninguna computadora. No es necesario instalar ningún controlador.
.
2. Seguro y confiable. El uso del dispositivo de contraseña electrónica ICBC México para sus actividades bancarias en línea puede protegerlo de los estafadores que roban su contraseña mediante sitios web falsos, virus troyanos o ataques de piratas informáticos, una contraseña única para sus transacciones bancarias.

3. Amplio uso. Puede usar el dispositivo de contraseña electrónica ICBC México en Banca personal por Internet, Banca móvil o Banca telefónica.

IV. Pautas de operación
Una vez que haya solicitado un dispositivo de contraseña electrónica ICBC México, úselo para recuperar una contraseña dinámica e ingrese la contraseña para sus pagos externos (transferencia, compras B2C, pago de facturas) a través de Banca por Internet personal, Banca móvil o Banca telefónica.

V. Consideración
Cuando se registra en diferentes canales, debe usar el mismo dispositivo de contraseña electrónica ICBC México, es decir, un dispositivo de contraseña electrónica ICBC México para un cliente.

Declaración de responsabilidad: El contenido de esta página es solo de referencia. El máximo poder de interpretación está bajo el Industrial and Commercial Bank of China Limited. Para parte del contenido, prevalecerán los avisos y las regulaciones específicas de las sucursales locales.

10- Protégete cuando estés en línea

Para evitar ser engañado por sitios web falsos o virus troyanos, debe tener cuidado con las estafas de phishing, mantener una buena práctica para mantenerse seguro en línea.

11- Mantenga su computadora y teléfono móvil a salvo

Su computadora y software pueden verse amenazados por virus o piratería.

11.1 - Evite que otros usen su computadora, teléfono móvil

Restrinja el uso de su computadora sin su autorización.

12 - Otras medidas

- Establezca una contraseña para su computadora
- Mantenga segura su información bancaria, verifique cuidadosamente que se encuentre en un lugar seguro
- No cierre el navegador cada vez que cierre la sesión de Banca por Internet
- No divulgue sus datos personales a nadie

Para aprender más de seguridad de la información, visitar cualquiera de los siguientes sitios web:

https://www.gob.mx/condusef/acciones-y-programas/comercio-electronico
https://www.condusef.gob.mx/gbmx/?p=medidas-de-seguridad
https://www.condusef.gob.mx/gbmx/?p=lo-que-debes-saber