Revelación de la seguridad

Last Updated: *May 2017*

En Denizen somos conscientes de la necesidad de asegurar la transmisión de información a las personas interesadas en nuestras actividades. Por ese motivo, Denizen pone especial énfasis en la seguridad y confidencialidad de todas las comunicaciones. Las operaciones se realizan utilizando un servidor seguro mediante el protocolo SSL (Secure Socket Layer), que se activa al acceder al servicio. El servidor seguro establece una conexión segura que transmite información cifrada mediante algoritmos, garantizando de este modo que solo pueda leerla el ordenador del cliente y el servidor del banco. Así que el uso del protocolo SSL permite:

- Que los usuarios comuniquen sus datos al servidor de Denizen y no a cualquier otro servidor que afirme ser de Denizen.
- Que los datos de compra se transmitan en formato cifrado entre el usuario y el centro de servidores de Denizen.

Seguridad de sus contraseñas

Denizen usa un sistema de Contraseñas seguras.

El número PIN de su tarjeta de Denizen y su código de acceso a la app de Denizen es información privada que se debe proteger de forma segura. Se almacena en nuestros sistemas internos y está cifrada de modo que nadie en Denizen la conoce.
Denizen nunca le preguntará sus credenciales de Denizen por correo electrónico, teléfono o mensajes SMS. Si recibe este tipo de mensaje, no facilite dicha información. Las contraseñas son secretas y solo debe conocerlas su propietario para su exclusivo uso en la app de Denizen.

Los navegadores ofrecen la opción de guardar los nombres de usuario y contraseñas para los sitios web que las solicitan y, a continuación, se almacenan en la memoria de su ordenador. Esta práctica, aunque acelera el acceso a los sitios que solicitan un nombre de usuario y contraseña, es totalmente desaconsejable en el caso de las contraseñas de bancos u otros servicios, cuya pérdida o robo podría causar graves perjuicios a los usuarios. Denizen recomienda que no guarde nunca sus códigos de acceso a nuestra aplicación en un ordenador o tableta. Estos dispositivos pueden sufrir ataques informáticos y podrían revelar sus códigos.

Consejos

- Use contraseñas complejas que resulten difíciles de adivinar y contengan una mezcla de caracteres en mayúsculas y minúsculas y números.
- No comparta sus contraseñas con nadie. Las contraseñas son secretas y solo debe conocerlas su propietario.
- No apunte su contraseña en notas adhesivas o libretas; memorícela o use gestores de contraseñas especializados.
- Desactive la opción “guardar contraseña” en su navegador. Es más seguro escribirla cada vez que inicia una sesión.
- Cambie sus contraseñas periódicamente.

- El PIN y el código de acceso deben ser diferentes. Esto dificultará que un tercero los descubra o adivine.
- Si sospecha que alguien ha sido capaz de adivinar su código de acceso, deberá cambiarlo lo antes posible.

Si recibe un SMS confirmando una operación que no ha realizado, póngase en contacto con Denizen en la dirección *support@denizen.io*

Detección de ataques y virus

Los virus informáticos son programas cuya finalidad es instalarse en un ordenador sin permiso o conocimiento del usuario. Existen varios tipos de virus, pero todos ellos suelen compartir la capacidad de propagarse y extenderse por el ordenador a través de Internet. Es fácil contribuir involuntariamente a propagar los virus reenviando correos electrónicos que contienen archivos adjuntos infectados. La colaboración de todos los usuarios de Internet es esencial para evitar la propagación de virus informáticos.
Existen diferentes tipos de virus, de los cuales los más notorios son:

- **Phishing o suplantación de identidad**: consiste en enviar un mensaje de correo electrónico fingiendo que procede de una organización conocida y solicitando datos del usuario (dirección, datos bancarios, contraseñas, etc.). Para facilitar estos datos, en la mayoría de los casos, al usuario le piden que siga un vínculo que aparece en el mensaje de correo electrónico y a continuación que escriba la información solicitada una vez dentro de la página falsa.
- **Ransomware o secuestro informático**: es un lucrativo método de delincuencia tecnológica. Normalmente escondido como "servicios de entrega de paquetes" o cualquier otra excusa creíble, se propaga a través del correo electrónico mediante vínculos que permiten la instalación de programas o la descarga de archivos infectados. Este virus bloquea el acceso a la información del ordenador y exige un rescate que presuntamente facilitará la clave para descifrar la información.
- **Troyanos**: se introducen en ordenadores personales escondidos dentro de un programa. Transforman el comportamiento del ordenador para que todo lo que se hace en él se pueda ver en el ordenador del delincuente.
- **Bulos**: son mensajes de correo electrónico que contienen ciertos rumores falsos con la única intención de transmitir y aumentar la cantidad de información poco fiable que circula por Internet. En general no son muy dañinos y resultan fáciles de eliminar.

A continuación se enumera una lista de los síntomas que se pueden observar en un ordenador infectado por un virus informático:

- Las operaciones se realizan con mayor lentitud.
- Los programas tardan más en cargarse y ejecutarse.
- Se produce una reducción ocasional o permanente e inexplicable del espacio libre en el disco duro y la memoria RAM disponible.
- Pueden aparecer programas desconocidos en la memoria.

Consejos

A continuación se enumera una lista de las precauciones que debe tomar para aumentar la seguridad frente a los virus:

- Si tiene que escribir sus credenciales, compruebe que la dirección (URL) del servidor comienza por https, lo cual significa que está accediendo a un servidor seguro.
- Otra indicación de que el servidor es seguro es la presencia de un candado cerrado (al contrario que uno abierto en el caso de un servidor no seguro) a la izquierda o derecha de la dirección (URL).
- Compruebe los certificados de seguridad de la página en la que se encuentra haciendo clic en el icono del candado que aparece al acceder a un área segura, o en el certificado en la barra del navegador, y verifique que la fecha de caducidad y el dominio del certificado están actualizados. La información detallada incluye el emisor, el periodo de validez y para quien se emitió el certificado.
- Antes de hacer clic en un vínculo, mueva el cursor sobre él para ver la dirección a la que accede al hacer clic en él. Compruebe que la dirección es correcta y está relacionada con la actividad que desea realizar.
- Siempre que finalice una operación o consulta, no olvide usar el botón de desconexión. Así cerrará la sesión con seguridad en la app de Denizen, y la próxima vez que inicie sesión, le solicitarán de nuevo su número de usuario y código de acceso.
- Su sistema operativo, su navegador y programas de uso frecuente siempre deben estar actualizados.
- Debe instalar un cortafuegos y un antivirus y mantenerlos siempre actualizados y en ejecución.
- Es conveniente realizar copias de seguridad regulares de sus archivos.
- No conecte ningún dispositivo externo a sus dispositivos si no sabe su procedencia, por ejemplo, unidades flash, discos duros y teléfonos móviles desconocidos.
- Descargue programas y apps exclusivamente de sitios web oficiales.
- Establezca un patrón de desbloqueo en sus dispositivos para que puedan acceder a ellos terceras personas.

A continuación se enumera una lista de las precauciones que debe tomar para aumentar la seguridad frente a los virus:

- Si tiene que escribir sus credenciales, compruebe que la dirección (URL) del servidor comienza por https, lo cual significa que está accediendo a un servidor seguro.
- Otra indicación de que el servidor es seguro es la presencia de un candado cerrado (al contrario que uno abierto en el caso de un servidor no seguro) a la izquierda o derecha de la dirección (URL).
- Compruebe los certificados de seguridad de la página en la que se encuentra haciendo clic en el icono del candado que aparece al acceder a un área segura, o en el certificado en la barra del navegador, y verifique que la fecha de caducidad y el dominio del certificado están actualizados. La información detallada incluye el emisor, el periodo de validez y para quien se emitió el certificado.
- Antes de hacer clic en un vínculo, mueva el cursor sobre él para ver la dirección a la que accede al hacer clic en él. Compruebe que la dirección es correcta y está relacionada con la actividad que desea realizar.
- Siempre que finalice una operación o consulta, no olvide usar el botón de desconexión. Así cerrará la sesión con seguridad en la app de Denizen, y la próxima vez que inicie sesión, le solicitarán de nuevo su número de usuario y código de acceso.
- Su sistema operativo, su navegador y programas de uso frecuente siempre deben estar actualizados.
- Debe instalar un cortafuegos y un antivirus y mantenerlos siempre actualizados y en ejecución.

- Es conveniente realizar copias de seguridad regulares de sus archivos.
- No conecte ningún dispositivo externo a sus dispositivos si no sabe su procedencia, por ejemplo, unidades flash, discos duros y teléfonos móviles desconocidos.
- Descargue programas y apps exclusivamente de sitios web oficiales.
- Establezca un patrón de desbloqueo en sus dispositivos para que puedan acceder a ellos terceras personas.

Tarjetas y comercio electrónico

Denizen se toma la seguridad de las tarjetas muy en serio.

La seguridad de las consultas y operaciones a través de la app de Denizen se basa en un sistema de códigos seguros. Estos se guardan en nuestros sistemas y se cifran mediante un algoritmo de modo que nadie en Denizen sabe dichos códigos.
La app de Denizen le permite activar y desactivar sus tarjetas con facilidad.

Consejos

Denizen recomienda seguir estos consejos para aumentar la seguridad del uso de sus tarjetas:

- La tarjeta se debe firmar y es absolutamente personal y no transferible.
- Memorice su número secreto. No lo anote nunca ni se lo diga a nadie bajo ninguna circunstancia.
- No use datos personales en su número secreto que se puedan deducir fácilmente, por ejemplo, su fecha de nacimiento o la matrícula de su coche
- Destruya las tarjetas caducadas con unas tijeras; no las tire sin destruirlas primero.
- Esté atento a la fecha de caducidad de su tarjeta de Denizen. Si no recibe una tarjeta nueva, notifíquelo inmediatamente a Denizen en la dirección support@denizen.io
- Cuando realice una compra, no pierda de vista su tarjeta
  y asegúrese de que se la devuelven. Guarde una copia del recibo de la transacción y compare los cargos que se muestran en el extracto.
- Informe inmediatamente de la desaparición de la tarjeta llamando al número +1-844-207-7702 o a través de la app en el menú de administración de la tarjeta tocando el botón “Report card as lost or stolen” (Denunciar la pérdida o robo de la tarjeta). Es crucial la inmediatez con que lo haga.
- Antes de emprender un viaje, compruebe la fecha de caducidad y el límite de crédito de la tarjeta.

Anote el número +1-844-207-7702 para que pueda ponerse en contacto con nosotros en caso de cualquier problema con la tarjeta.