Banca electrónica

Producción:

cert.br nic.br cgi.br

PROTEGE TU VIDA FINANCIERA

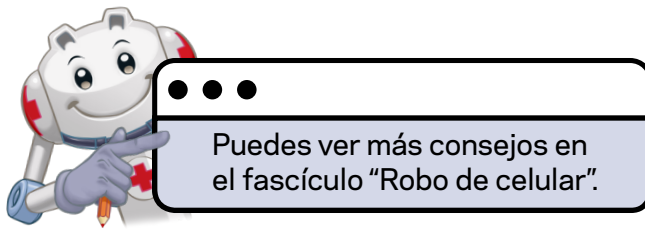
Gracias a Internet, las transacciones financieras se han vuelto más fáciles y rápidas. Pero sin un mínimo de cuidados, los estafadores pueden aprovecharse de esta practicidad.

Aquí te contamos cómo protegerte y evitar pérdidas.

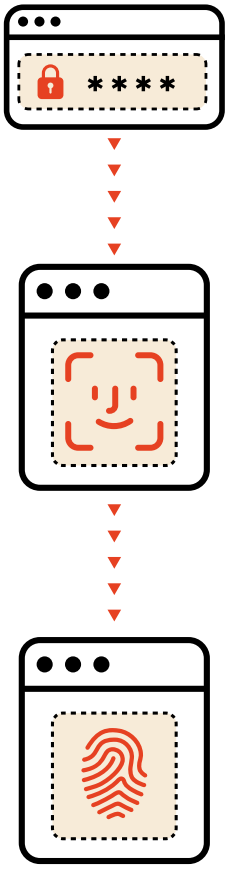
USA UNA CONTRASEÑA FUERTE PARA BLOQUEAR TU CELULAR, INCLUSO CON AUTENTICACIÓN BIOMÉTRICA

El celular siempre tiene una contraseña o patrón que permite desbloquearlo, incluso cuando se usa biometría. Si esta contraseña es débil, un ladrón la podría adivinar, desbloquear y cambiar la configuración del celular y acceder a otras aplicaciones, datos y cuentas.

- Define una contraseña larga, preferentemente alfanumérica
- Si usas un patrón de desbloqueo, evita los diseños demasiado sencillos
- Activa el bloqueo de pantalla automático en el menor tiempo disponible



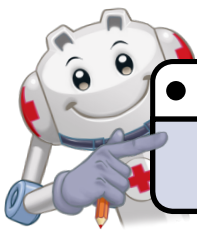
Puedes ver más consejos en el fascículo “Robo de celular”.



EN LAS APLICACIONES FINANCIERAS COMBINA UNA CONTRASEÑA FUERTE CON AUTENTICACIÓN BIOMÉTRICA

Las aplicaciones financieras generalmente controlan el acceso por medio de una contraseña y biometría. Incluso con la autenticación biométrica activada, si la contraseña es fácil de adivinar, un ladrón podría descubrirla e ingresar a tu cuenta.

- Crea una contraseña fuerte para acceder mediante una aplicación (Internet)
- Habilita la biometría para facilitar el acceso y no tener que recordar tantas contraseñas
- No repitas las contraseñas

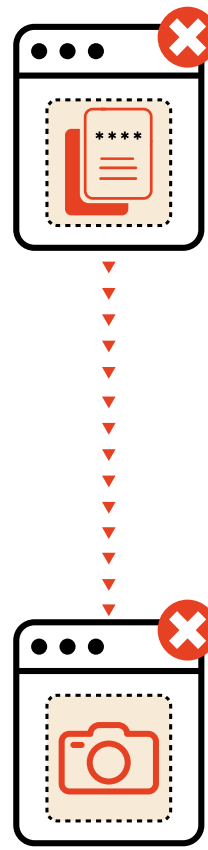


Puedes ver más consejos en el fascículo “Autenticación”.

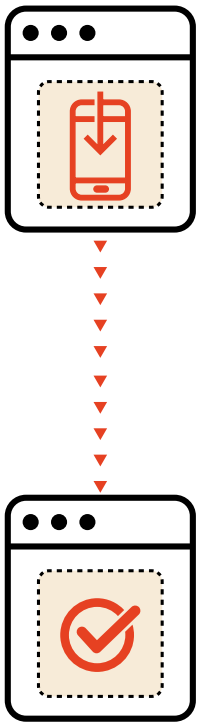
NO GRABES LAS CONTRASEÑAS DE LOS SERVICIOS FINANCIEROS EN TU CELULAR

Los ladrones podrían encontrar las contraseñas grabadas en el celular usando los mecanismos de búsqueda disponibles en el propio celular y las aplicaciones.

- No guardes las contraseñas en un bloc de notas, junto con tus contactos o en un navegador
- No envíes contraseñas por mensaje ni por correo electrónico
- No tomes fotos de las contraseñas



Busca en tu celular la palabra “contraseña”. ¡Los resultados podrían sorprenderte! Se pueden encontrar contraseñas en distintas aplicaciones e incluso en fotos.



SOLO INSTALA APLICACIONES OFICIALES

Hay aplicaciones falsas que intentan hacerse pasar por oficiales. Si se instalan, pueden dar acceso remoto al dispositivo, cambiar el funcionamiento de otras aplicaciones y engañar al usuario para que haga transferencias a desconocidos.

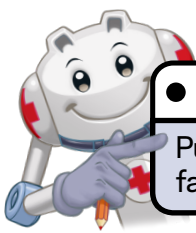
- Usa solo la tienda oficial del sistema o del fabricante del dispositivo
- Antes de instalarla, confirma si el nombre de la aplicación y del desarrollador son correctos

Puedes ver más consejos en el fascículo “Celulares y *tablets*”.

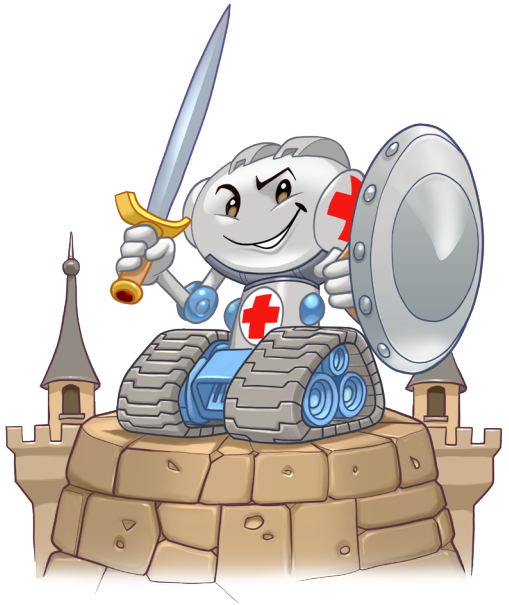
CONOCE LOS CANALES OFICIALES DE LA INSTITUCIÓN FINANCIERA

Los estafadores crean páginas y perfiles falsos, y los promocionan a través de anuncios en los buscadores, las redes sociales y las aplicaciones de mensajería. Si sigues los enlaces de esos anuncios podrías terminar siendo víctima de una estafa.

- Accede al sitio oficial digitando la dirección (URL) directamente en el navegador
  - usa siempre una conexión segura (https)
- Guarda la página en tus "Favoritos" para facilitar futuros accesos
- Verifica en el sitio de la institución cuáles son los otros canales oficiales



Puedes ver más consejos en el fascículo "*Phishing* y otras estafas".



MANTÉN LAS APLICACIONES Y LOS SISTEMAS ACTUALIZADOS

Las fallas (vulnerabilidades) de las aplicaciones y los sistemas pueden ser explotadas, por ejemplo, para instalar *malware*, modificar el funcionamiento, robar datos y cometer fraudes financieros.

» Instala actualizaciones de forma regular
- habilita la actualización automática siempre que sea posible

AJUSTA LOS LÍMITES PARA REDUCIR LAS PÉRDIDAS FINANCIERAS

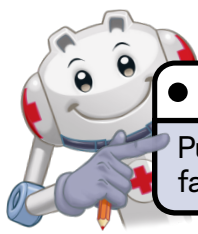
Los estafadores aprovechan la velocidad de las transferencias electrónicas para robar dinero, que no siempre se puede recuperar. Limitar los montos de las operaciones ayuda a reducir las pérdidas.

- Reduce los límites de las transferencias entre cuentas
- Revisa los límites de crédito preaprobados

NO ENTREGUES INFORMACIÓN A PERSONAS QUE TE CONTACTEN

Las instituciones financieras no contactan a la gente para pedirles sus contraseñas, códigos de verificación, *tokens*, códigos QR, datos de sus tarjetas de crédito u otros datos personales. Solo solicitan datos para confirmar la identidad del cliente cuando accede a los canales oficiales.

» Termina la comunicación y, en caso de duda, ponte en contacto con la institución a través de los canales oficiales



Puedes ver más consejos en el fascículo "*Phishing* y otras estafas".

MONITOREA TUS TRANSACCIONES FINANCIERAS Y ACTÚA RÁPIDAMENTE

Monitorear las alertas y notificaciones de las transacciones financieras permite descubrir cualquier movimiento irregular y actuar rápidamente para contener los fraudes y las pérdidas.

- Activa las alertas y notificaciones de los movimientos en tus cuentas y tarjetas de crédito
- Revisa periódicamente las notificaciones y los estados de cuenta
  - comunícate con la institución financiera y desconoce rápidamente cualquier transacción irregular

USA TARJETAS DE CRÉDITO VIRTUALES PARA LOS PAGOS NO PRESENCIALES

Las tarjetas de crédito virtuales normalmente son generadas por medio de una aplicación, tienen datos diferentes a los de las tarjetas físicas y se pueden modificar con frecuencia. Esto evita que una tarjeta se use en fraudes, incluso si los datos se filtran o alguien los roba.

- Usa los datos de la tarjeta virtual cuando hagas compras y contrates servicios a través de una aplicación, un sitio o por teléfono
- De ser posible, reduce el límite de la tarjeta virtual

EXIGE AUTENTICACIÓN PARA LOS PAGOS CON BILLETERAS DIGITALES

Las billeteras digitales, como Apple Wallet y Google Wallet, ofrecen opciones de pagos en línea y por aproximación. Si la billetera no exige autenticación antes de realizar las transacciones, podrías convertirte en víctima de una estafa o realizar compras por accidente.

- Escoge un mecanismo de autenticación para realizar los pagos
- En el caso de los pagos por aproximación, verifica los datos en la pantalla del lector de tarjetas antes de acercar el celular

NO COMPARTAS INFORMACIÓN FINANCIERA

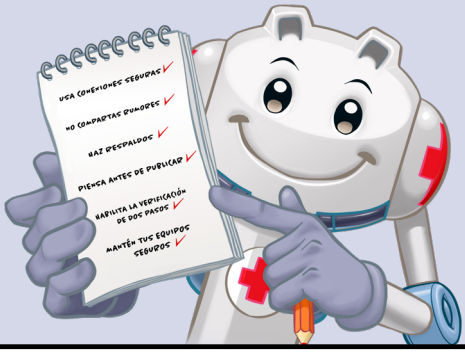
Compartir información financiera, especialmente en las redes sociales, le facilita el trabajo a los estafadores.

» No publiques fotos de tarjetas de crédito o débito, contraseñas, etc.

UTILIZA UN CORREO ELECTRÓNICO INDEPENDIENTE PARA LAS INSTITUCIONES FINANCIERAS

Para entrar a las cuentas financieras, los estafadores aprovechan los mecanismos de recuperación de contraseñas que envían un enlace o código a la dirección de correo electrónico registrada. Si la cuenta de correo está logueada en un celular robado, el estafador podrá acceder a tu cuenta en la institución financiera.

- Crea un correo electrónico exclusivo para usar en las instituciones financieras
- No dejes este correo logueado en ninguna aplicación o navegador del celular
- Accede a este correo regularmente para verificar las notificaciones de inicio de sesión y los comunicados enviados por las instituciones financieras



MÁS INFORMACIÓN

» Para obtener más información sobre este y otros asuntos relacionados con los cuidados que debes tener en Internet, consulta los demás Fascículos de la Cartilla de Seguridad para Internet, disponibles en: **https://cartilla.cert.br/**

cert.br

CERT.br **(https://cert.br/)** es un Grupo de Respuesta a Incidentes de Seguridad (CSIRT) con jurisdicción nacional y de último recurso, mantenido por NIC.br. Además de la gestión de incidentes, también trabaja en la sensibilización en temas de seguridad, conciencia situacional y transferencia de conocimiento, siempre respaldado por una fuerte integración con las comunidades de los CSIRT nacionales e internacionales.

nic.br

El Núcleo de Información y Coordinación del Punto BR - NIC.br **(https://nic.br/)** es una entidad civil de derecho privado y sin fines de lucro, encargada de la operación del dominio .br, así como de la asignación de números IP y del registro de Sistemas Autónomos en Brasil. Lleva adelante acciones y proyectos que benefician la infraestructura de Internet en Brasil.

cgi.br

El Comité Gestor de Internet en Brasil **(https://cgi.br/)** es responsable por el establecimiento de directrices estratégicas relacionadas con el uso y el desarrollo de Internet en Brasil. Coordina e integra todas las iniciativas de servicios de Internet en Brasil, promoviendo la calidad técnica, la innovación y la difusión de los servicios ofrecidos.

abril de 2023