Phishing y otras estafas

Producción:

cert.br nic.br cgi.br

NO CONFÍES EN TODO LO QUE VEAS EN INTERNET. ¡PODRÍA SER UNA ESTAFA!

Los delincuentes siempre inventan nuevos trucos para engañar y aprovecharse de las personas. No te dejes engañar.

Aquí te contamos cómo protegerte de las estafas en Internet.

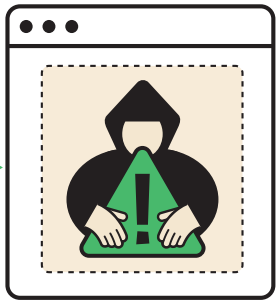
EL SENTIDO CRÍTICO ES FUNDAMENTAL

DESCONFÍA SIEMPRE

En Internet circula información de todo tipo y origen, incluso información falsa y maliciosa. Creer ciegamente en todo lo que recibes o en cualquier información a la que accedes les facilita el trabajo a los atacantes.

» Usa tu sentido crítico. ¡Puede ser una estafa!

- que esté en Internet o que te lo mande un conocido no significa que sea cierto o confiable

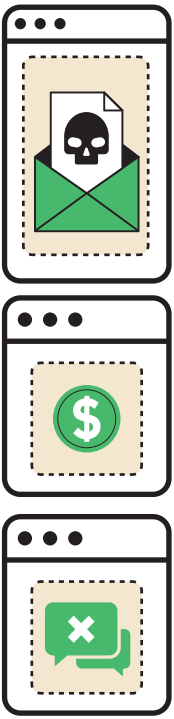


BUSCA MÁS INFORMACIÓN

Para no caer en las trampas de los estafadores hay que desconfiar, mantener la calma y verificar si el mensaje que recibimos o el contenido que vimos en Internet es confiable.

» Infórmate

- busca la información en la fuente
- busca historias de estafas similares
- conversa con amigos y familiares



PRESTA ATENCIÓN AL TONO DEL MENSAJE

Los estafadores se aprovechan de los sentimientos de las personas, como el miedo, la obediencia, la caridad, la falta de afecto y la codicia, para convencerlas de que actúen como ellos quieren y de forma rápida, sin pensar.

» Desconfía de los mensajes:

- que contengan amenazas
- que te ofrezcan la oportunidad de ganar dinero fácil
- con promociones o descuentos muy grandes
- que te pidan guardar un secreto
- que apelen a tus emociones
- que transmitan un sentido de urgencia

Ingeniería social es el término que se usa cuando una persona intenta convencer a otra para que ejecute acciones que la lleven a brindar información o a seguir pasos que faciliten las estafas.

PIENSA SI EL CONTENIDO TIENE SENTIDO

Los estafadores suelen enviar mensajes masivos con contenido genérico esperando que alguien "muerda el anzuelo". Analizar si el contenido tiene sentido te ayudará a no caer víctima de una estafa.

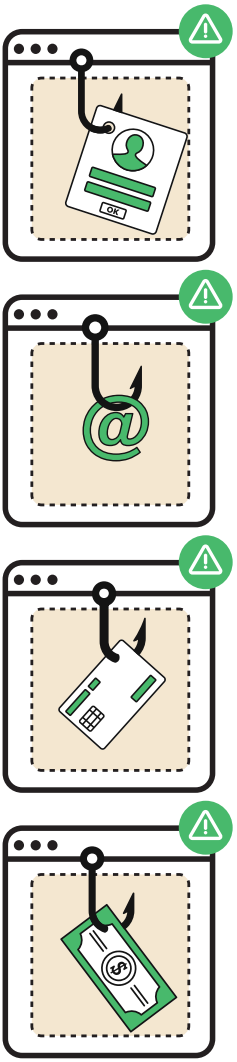
» Pregúntate, por ejemplo:

- ¿tengo cuenta en este banco?
- ¿esta es la forma de contacto que uso con esta institución?
- ¿el monto a pagar es correcto?
- ¿por qué anticipar el pago y no descontarlo al final?

» Observa si hay errores de ortografía

CUÍDATE DE LAS ESTAFAS DEL DÍA A DÍA

El *phishing* es un tipo de estafa común que busca capturar datos de los usuarios. Llega a través de mensajes electrónicos que llaman la atención de los usuarios para lograr que accedan a enlaces maliciosos o instalen *malware*.



» Desconfía de los mensajes con temas cotidianos, por ejemplo:
  - necesidad de volver a registrar una llave de seguridad física o *token*
  - cancelación de un documento
  - deudas pendientes
  - ofertas de empleo
  - cómo ganar puntos o premios

» No hagas lo que pide el mensaje
  - en caso de duda, ponte en contacto con la institución a través de un canal oficial

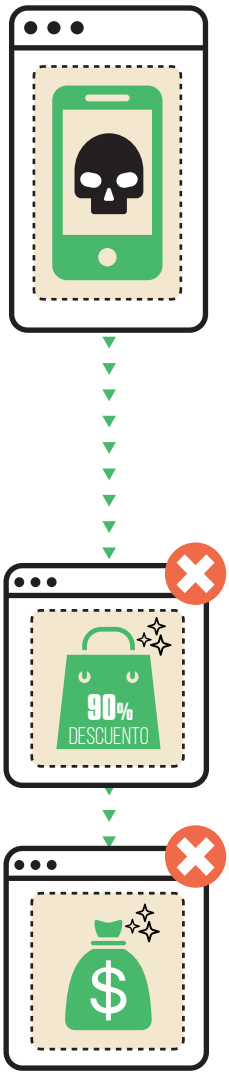
El *phishing* es un tipo de estafa donde el estafador intenta obtener información personal y financiera del usuario, combinando medios técnicos con ingeniería social.

La palabra *phishing* —del inglés "*fishing*"— es una analogía creada por los estafadores, en la que se utilizan "anzuelos" (mensajes electrónicos) para "pescar" información de los usuarios.

TAMBIÉN TEN CUIDADO CON LAS ESTAFAS DEL MOMENTO

Para atraer a sus víctimas, los oportunistas aprovechan los temas del momento, como los impuestos, las elecciones, la Copa del Mundo, las promociones (por ejemplo, *Black Friday*) y los acontecimientos que generan conmoción, como las catástrofes y las enfermedades graves.

- Desconfía de las ofertas demasiado buenas
  - recuerda: "cuando la limosna es grande, hasta el santo desconfía"
- Busca información solo en fuentes oficiales
  - verifica antes de hacer pagos o donaciones



NO RESPONDAS, DENUNCIA

Al responder un mensaje, estás confirmando que tu cuenta está activa. También puedes revelar información y preferencias que le ayudarán al estafador a ser más convincente.

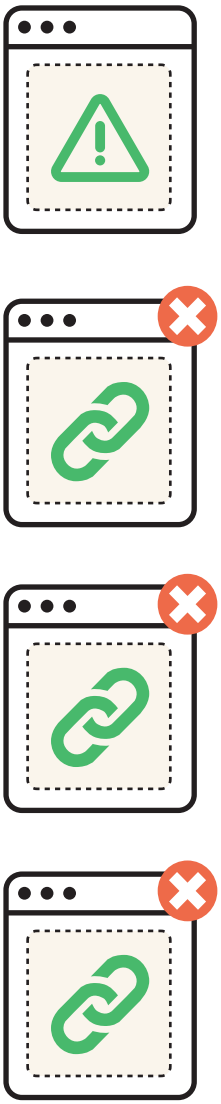
- Denuncia los mensajes, anuncios y perfiles maliciosos
  - usa las opciones que ponen a tu disposición las plataformas
- Bloquea los números de teléfono y las cuentas que envían mensajes maliciosos

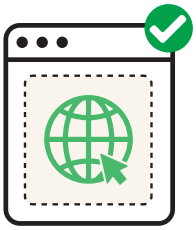
Denunciar ayuda a eliminar los anuncios, mensajes y perfiles falsos, lo que evita que otras personas se conviertan en víctimas.

NO HAGAS CLIC EN TODOS LOS ENLACES QUE RECIBES

Los enlaces y códigos QR maliciosos se usan para dirigir a los usuarios a páginas falsas o con *malware*, para así capturar datos y cometer estafas.

- Antes de hacer clic, analiza el contexto y los detalles
  - en caso de duda, ¡no hagas clic!
- Ten cuidado incluso con los mensajes que te envían personas "conocidas"
  - de ser necesario, comunícate con quien supuestamente te envió el mensaje usando otro medio de comunicación
- Solo lee los códigos QR si estás seguro de que la fuente es confiable

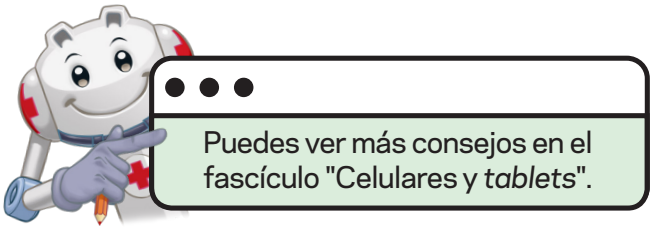




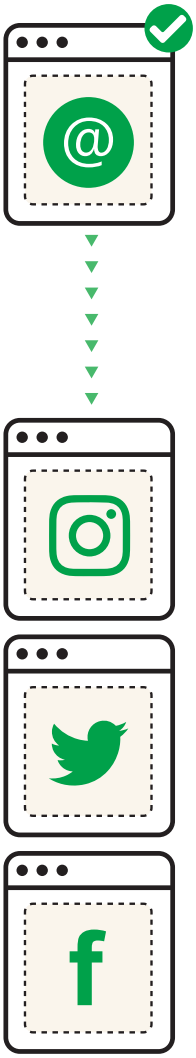
ACCEDE AL SITIO O A LA APLICACIÓN OFICIAL

Existen muchas páginas falsas y aplicaciones maliciosas que intentan hacerse pasar por organizaciones conocidas como bancos, sitios de comercio electrónico y redes sociales. Hay que tener cuidado de acceder solamente a sitios legítimos e instalar aplicaciones confiables.

- Accede al sitio digitando la dirección (URL) directamente en el navegador
  - si usas buscadores, confirma que la URL que aparece sea la correcta
  - usa siempre una conexión segura (https)
- Solo instala la aplicación oficial de la institución



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



BUSCA EL PERFIL OFICIAL DE LAS INSTITUCIONES EN LAS REDES SOCIALES

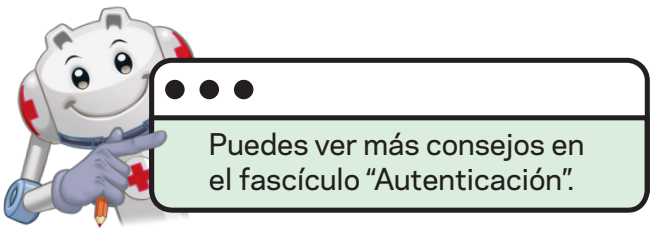
Al comunicarte con una institución a través de las redes sociales, por ejemplo, con atención al cliente, hay que verificar que el perfil sea legítimo. De lo contrario, podrías entregar tus datos a algún estafador, que los usará para crear perfiles falsos.

- Asegúrate de que sea el perfil oficial
- Siempre que esté disponible, busca el símbolo de "cuenta verificada"

PROTEGE TUS CUENTAS Y CONTRASEÑAS

Si obtiene tus contraseñas y códigos de verificación, un atacante puede ingresar a tus cuentas, robar tu identidad y estafar en tu nombre, perjudicándote a ti y a tus contactos.

- Nunca entregues tus contraseñas o códigos de verificación
  - tampoco imágenes de códigos QR
- Activa la verificación de dos pasos



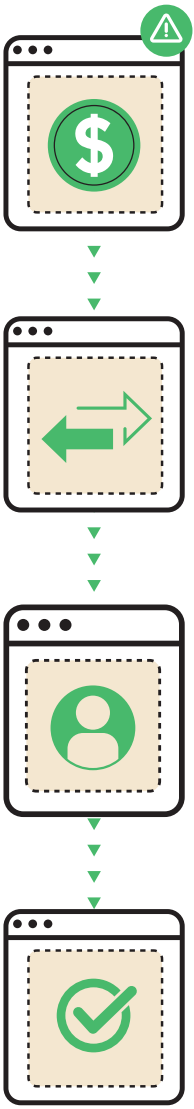
Puedes ver más consejos en el fascículo “Autenticación”.

REDUCE LA CANTIDAD DE INFORMACIÓN PERSONAL QUE COMPARTES

Cuanta más información publiques, más fácil será robar tu identidad y más convincente será el estafador en sus abordajes. La información también se puede utilizar para intentar adivinar tus contraseñas.

- Piensa bien antes de publicar algo
  - analiza lo que publicas y quién tendrá acceso
- Sé selectivo al aceptar nuevos contactos

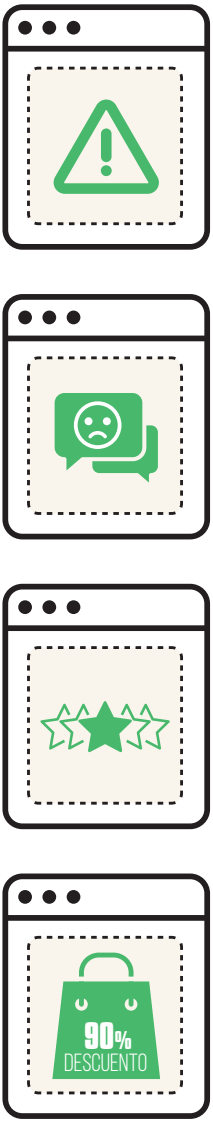
PRECAUCIONES CON LAS OPERACIONES BANCARIAS Y LAS COMPRAS EN LÍNEA



CONFIRMA LA IDENTIDAD ANTES DE REALIZAR TRANSACCIONES FINANCIERAS

Los estafadores se aprovechan de la confianza entre familiares y amigos y piden préstamos o ayuda para pagar sus cuentas, generalmente con urgencia. Para esto usan cuentas hackeadas o dicen haber cambiado sus datos de contacto, como su número de teléfono.

- Desconfía de los los mensajes que te pidan ayuda financiera
  - comunícate con la persona por algún otro medio
  - informa lo ocurrido al verdadero dueño de la cuenta, tus amigos y familiares
- Siempre verifica los datos del destinatario antes de realizar una transacción



VERIFICA QUE EL SITIO O LA TIENDA SEA CONFIABLE

Los estafadores crean sitios de comercio electrónico falsos con precios por debajo del mercado para engañar a los clientes, que después no reciben los productos. Los datos proporcionados también se pueden utilizar para cometer otras estafas.

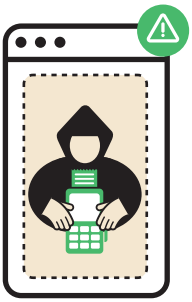
- Investiga la reputación de la empresa y las opiniones de los clientes
  - en las redes sociales y los sitios de quejas
  - prefiere los sitios y tiendas que conozcas o que tengan buenas referencias
- Haz una investigación de mercado y desconfía si el precio es muy bajo

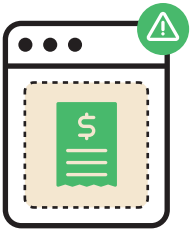
NO ACEPTES INTERMEDIARIOS EN LAS TRANSACCIONES DE COMPRAVENTA

Los estafadores crean anuncios falsos con precios más baratos para atraer compradores. Dicen ser intermediarios en la transacción para recibir el dinero del comprador. El verdadero vendedor no recibe el pago y no entrega el producto o servicio.

- Realiza toda la transacción a través de la plataforma del anuncio
  - sospecha de un intermediario que te pida que guardes en secreto los valores de la negociación

SOLO REALIZA LOS PAGOS EN LA PLATAFORMA DE COMPRAS ORIGINAL





Los estafadores dicen tener fallas en el sistema y les piden a las víctimas que realicen sus pagos por fuera de la plataforma de compras. Si pagas aparte, el estafador puede cambiar y ocultar el monto a pagar para cobrar más. También puede clonar la tarjeta.

» Cuando compres en un sitio o una aplicación:
  - si usas tarjeta de crédito, prefiere una tarjeta virtual
  - no hagas pagos por fuera de la plataforma

» Cuando hagas cualquier pago:
  - verifica el importe antes de autorizar el cargo
  - verifica el importe que se cobra de tu cuenta y/o tarjeta

QUÉ HACER SI ERES VÍCTIMA DE UNA ESTAFA

MONITOREA TU VIDA FINANCIERA Y TU IDENTIDAD

El robo de identidad puede causar muchos daños. Podrían quedar deudas a tu nombre, podrías perder tu reputación y tu crédito, e incluso podrías verte implicado en procesos judiciales.

- Activa las alertas y monitorea los resúmenes de tus tarjetas y cuentas bancarias
- Ponte en contacto con las instituciones involucradas
  - para aclarar tus dudas o disputar irregularidades
- Sigue tus registros financieros

Señales del robo de identidad:

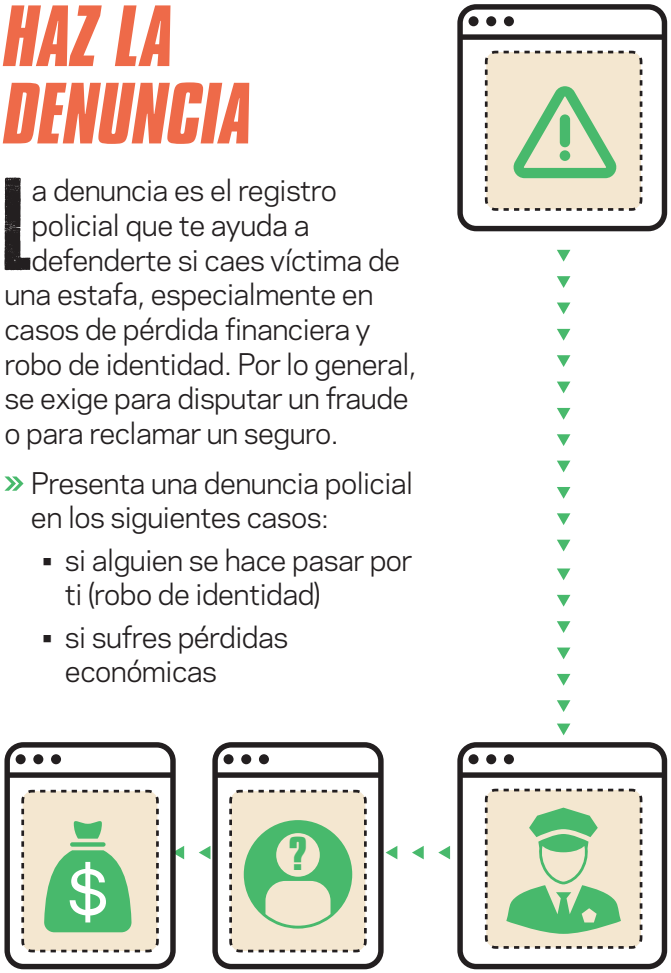
- notificaciones de instituciones de protección al crédito
- cuentas bancarias, préstamos, tarjetas o beneficios que no has solicitado

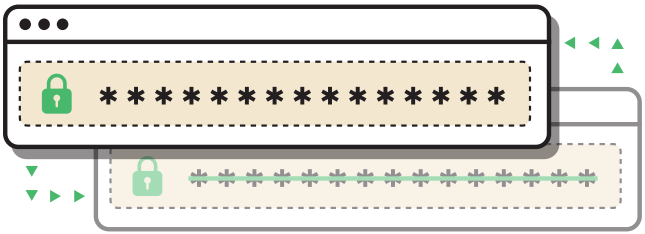
HAZ LA DENUNCIA

La denuncia es el registro policial que te ayuda a defenderte si caes víctima de una estafa, especialmente en casos de pérdida financiera y robo de identidad. Por lo general, se exige para disputar un fraude o para reclamar un seguro.

» Presenta una denuncia policial en los siguientes casos:

- si alguien se hace pasar por ti (robo de identidad)
- si sufres pérdidas económicas

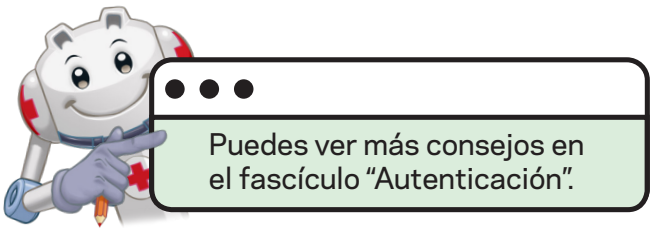


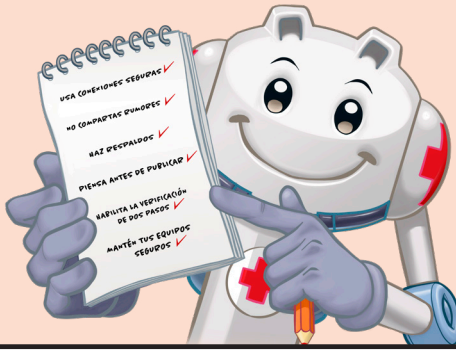


RECUPERA TUS CUENTAS Y CAMBIA TUS CONTRASEÑAS

Las cuentas hackeadas pueden ser la puerta de entrada para las estafas. Se pueden utilizar para cambiar las contraseñas de otras cuentas — incluso las de las entidades financieras— y para estafar a tus contactos.

- Si se ha producido un acceso no autorizado a alguna de tus cuentas:
  - intenta cambiar tu contraseña
  - de ser necesario, sigue los procedimientos para recuperar el acceso
- Si identificas un perfil falso a tu nombre, haz la denuncia en la plataforma
- Avisa a tus contactos





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.

diciembre de 2022