



El ABC de la Ciber Higiene:

10 recomendaciones para protegerse de estafas bancarias

- *Cientes deben estar muy atentos y resguardar sus datos utilizando contraseñas diferentes, así como otras opciones de protección que ofrecen los bancos.*
- *Entidades bancarias nunca pedirán datos sensibles de cuentas por mensaje, llamada, correo electrónico, o cualquier otra vía.*

Febrero, 2025 – En un mundo cada vez más digitalizado, proteger nuestra información personal es fundamental para evitar ser víctima de fraudes y ciberataques. Con este propósito, la Asociación Bancaria Costarricense (ABC) lanza el ABC de la Ciber Higiene, un glosario con 10 recomendaciones esenciales para que los usuarios bancarios resguarden sus datos y operen con mayor seguridad en el entorno digital.

Según Raúl Rivera, Asesor en Ciberseguridad de la Asociación Bancaria Costarricense (ABC), “este concepto se refiere a las prácticas y procedimientos que utilizan las personas y las organizaciones para mantener la salud y la resiliencia de seguridad de sus sistemas, dispositivos, redes y datos. El objetivo principal es mantener los datos confidenciales seguros y protegidos de los ciberataques y el robo”.

Los bancos, públicos y privados, afiliados a la ABC, trabajan activamente en este tema, por eso, este esfuerzo para brindar a sus clientes **una guía, con la intención de que hagan de la ciber higiene, una práctica diaria que les permita evadir los intentos de fraude en las diferentes plataformas digitales.**

Estas son las recomendaciones:

LOS 10 MANDAMIENTOS DE LA CIBER HIGIENE DIGITAL

Ante la duda, comunícale a la institución directamente.

1

CUIDADO CON INGRESAR A SITIOS WEB O APLICACIONES FALSAS O CLONADAS

- Apréndete la dirección web o URL de tu banco o institución pública y revisa que la dirección que estás accediendo es la correcta.
- No utilices un buscador para buscar la dirección y hacer clic en el primer resultado. Cualquiera de los resultados podría estarte llevando a un sitio falso.
- Nunca hagas clic en enlaces que te envíen por correo electrónico, SMS, WhatsApp, redes sociales, etc.

2

EVITA QUE ALGUIEN PUEDA INGRESAR A TU CUENTA BANCARIA SIN DARTÉ CUENTA

- Asesórate con tu banco sobre las opciones de protección basadas en firma digital, llaves de seguridad USB, biometría o comportamiento y actualízalas para validar el ingreso a tu cuenta.
- Habilita las notificaciones de ingreso o de transacciones para alertarte de posibles situaciones irregulares que estén ocurriendo.
- Asegúrate de mantener actualizado el correo electrónico o número de teléfono en tu banco, al cual deseas recibir las notificaciones. Además, recuerda desconectar tu cuenta bancaria al cambiar de número telefónico (SINPE Móvil).

3

PROTEGE TUS CONTRASEÑAS DE ACCESO A SITIOS WEB O APLICACIONES FINANCIERAS

- Utiliza contraseñas diferentes para cada sitio web, aplicación financiera o plataforma digital. Si un delincuente roba alguna de ellas, prueba en todos los sitios o plataformas con el propósito de suplantar tu identidad.
- No guardes las contraseñas en el navegador web ya que podrían estar disponibles para otras personas que compartan el dispositivo.
- Si se te dificulta acordarte o crear contraseñas diferentes y difíciles de adivinar utiliza administradores de contraseñas ([1password](#), [bitwarden](#), [dashlane](#), [lastpass](#), [keepass](#)).

4

EVITA QUE TE HACKEEN LA COMPUTADORA DE ESCRITORIO, PORTÁTIL, TELÉFONO INTELIGENTE O TABLETA

- Utiliza un antivirus en todos y cada uno de tus dispositivos. Si no sabes cual elegir revisa las opciones gratuitas y pagas disponibles ([avast](#), [avastcomantivirus](#)).
- No utilices programas piratas, ya que estos pueden permitirle a un ciber delincuente espiar tu información sensible y hasta controlar tu dispositivo de forma remota.
- Mantén tus programas y sistemas operativos de todos tus dispositivos actualizados.

5

PROTEGE LA INFORMACIÓN CONFIDENCIAL DE TU DISPOSITIVO Y CONEXIONES

- Siempre que te conectes a tu banco a través de una red WiFi pública de un mall, hotel, aeropuerto, restaurante, parque, etc. utiliza una conexión VPN para proteger la transmisión de tus datos sensibles.
- Crea un pin de acceso o contraseña de ingreso en cada uno de tus dispositivos para poder usarlos. Esto protege tus datos sensibles en caso de pérdida o robo.
- Si deseas estar más protegido, cifra o encripta los datos sensibles que almacenes en tus dispositivos. Además, mantén siempre una copia de respaldo en otro lugar para evitar perder tus datos importantes.

6

CUIDADO CON LOS FRAUDES CUANDO VENDES, COMPRAS O PAGAS EN LÍNEA

- Cuando estés realizando un pago con tarjeta de crédito en algún comercio, nunca entregues la tarjeta. Solicita que traigan el dispositivo de pago (POS) a donde estés o posen línea de vista.
- Si estás vendiendo un producto en línea, evita entregar el producto sin confirmar que el pago se encuentra acreditado en tu cuenta. Si estás comprando algún producto, evita hacer un pago sin validar las condiciones de este o referencias del vendedor.
- Nunca confíes en fotografías de depósitos. Confirma que los fondos se encuentran acreditados en tu cuenta. También, evita que te pongan en contacto supuestos funcionarios de la entidad para confirmar si la razón del por qué no puedes ver los fondos acreditados. Llama tu directamente a la institución.

7

CUIDADO CON SUPUESTAS OFERTAS DE TRABAJO, PAQUETES RETENIDOS O MULTAS PENDIENTES DE PAGO

- Si recibes alguna notificación de pago pendiente en alguna institución o servicio público, detente y contacta directamente a la institución para confirmar dicha situación.
- Cuidado con el uso de códigos QR para realizar pagos en línea o acceder a información. Muchas veces los delincuentes pagan comisiones sobre los códigos reales para llevarte a sitios falsos, robar información o infectar tu dispositivo.
- Nunca deposites dinero o cambies de participar en una oferta de un puesto de trabajo, pago de multas, paquetes retenidos, entre otros. Generalmente se trata de un engaño que puedes evitar comunicándote directamente con la institución.

8

EL USO INSEGURO DE REDES SOCIALES Y PLATAFORMAS DIGITALES GRATUITAS PODRÍA SALIRTE MUY CARO

- Evita compartir información de contacto como correo electrónico, número telefónico, dirección habitacional o del trabajo, así como nombres de familiares y amigos. Evita que el hampas lo utilice en tu contra.
- Cuidado al abrir adjuntos en correos electrónicos o aplicaciones de mensajería. Muchos de estos podrían contener programas maliciosos e infectar tu dispositivo. Protégete con un buen antivirus.
- Revisa periódicamente tus configuraciones de privacidad en las distintas plataformas digitales.

9

CUIDADO CON PERFILES FALSOS DE PERSONAS O INSTITUCIONES

- Nunca confíes en cuentas de correo electrónico o plataformas de mensajería (ej. WhatsApp). Crea perfiles falsos utilizando cualquier nombre o foto de persona o institución es muy sencillo.
- Confirma que el dominio de un correo electrónico recibido sea @nombre-de-tu-banco.RL o @nombre-de-tu-banco.com. Si aparece: @gmail.com, @hotmail.com o cualquier otro, desconfía inmediatamente al igual que de números telefónicos desconocidos.
- Aunque una página, aplicación o perfil de una cuenta se parezca a la de tu banco, institución, amigo o familiar podría ser falsa. Evita interactuar si no estás 100% seguro.

10

¡CUIDADO! RECUERDA SIEMPRE DETENERTE, PENSAR Y ACTUAR

- Detente, cuidado con la impulsividad. Los delincuentes intentarán inculcarte miedo o la necesidad de urgencia para que actúes haciendo lo que ellos quieren de forma inmediata.
- Piensa un momento y analiza la situación. Ninguna institución va a presionarte para actuar de inmediato aun cuando se trate de algo importante. Así que sospecha inmediatamente!
- Actúa con calma y toma las decisiones que correspondan con cabeza fría. Al cortar una interacción digital con alguien a quien no le ves la cara estarás evitando un posible fraude, confirmando la situación y resolviendo de manera segura.