



¿Recibiste una llamada o un mensaje inesperado?
Aprende a verificar antes de actuar

ABC para verificar antes de actuar

Aprende a reconocer intentos de fraude por llamadas y mensajes, a proteger tus datos y a saber qué hacer si algo no te parece seguro.



Alerta

Reconoce las señales de alerta.



Busca

Busca la presión y protege tus datos.



Confirma

Confirma por tu cuenta.

Una alerta, una etiqueta o un nombre visible pueden dar pistas.
Ninguno garantiza que la comunicación sea segura.

Reconoce las señales

Los intentos de fraude llegan por llamadas o mensajes y pueden parecer comunicaciones reales. Usan nombres conocidos, números parecidos, premios, amenazas o urgencia para que actúes sin pensar, con miedo y sin consultar a nadie.

Detente si...

- Te exigen actuar de inmediato para evitar un bloqueo, una multa o la pérdida de dinero.
- Te solicitan abrir un enlace, instalar una aplicación o compartir pantalla.
- Te piden claves, códigos, datos de tarjeta o transferir dinero para “proteger” una cuenta.
- El remitente, el número o el mensaje parecen oficiales, pero el contacto no era esperado.

Una señal no prueba por sí sola que sea un fraude,
pero sí es razón suficiente para detenerse y verificar



Conoce las formas de contacto fraudulento

1. Smishing por mensaje de texto



Es un engaño que llega por mensaje de texto (SMS). El mensaje simula venir de un banco, una empresa de mensajería, una entidad pública o un operador, y busca que usted abra un enlace, entregue datos o haga un pago.

¿Cómo reconocerlo?

El mensaje combina urgencia con un enlace o con una solicitud de datos que usted no esperaba.



“Tu cuenta será bloqueada hoy. Ingresa aquí para confirmar tus datos eej.af/ySkTFhFIN”.



¿Qué hacer?

- No respondas ni abras el enlace.
- Si el mensaje dice ser de una entidad, contacta a la entidad por medio de sus canales oficiales.
- Entra por tu cuenta a la aplicación o página oficial de la entidad y verifica si hay un aviso real.

Ten en cuenta

Que el mensaje incluya tu nombre, número de documento o el nombre de un producto no confirma que sea auténtico. Esa información puede haberse obtenido o reutilizado para hacer más creíble el engaño.



2. Vishing

por llamada de voz

Es un engaño por llamada telefónica. Quien llama puede inventar una emergencia, fingir que pertenece a un banco, operador, entidad pública o autoridad, y pedir datos, códigos o dinero.

¿Cómo reconocerlo?

Le piden información confidencial, mover dinero o instalar una aplicación, y le insisten en que no cuelgue.



"Te hablamos del área de seguridad del banco. Detectamos un movimiento extraño. Para protegerlo, compártenos el código que acaba de llegar a tu celular"



¿Qué hacer?

- No compartas claves ni códigos que recibas en tu celular.
- No sigas instrucciones para mover dinero, instalar aplicaciones o cambiar configuraciones.
- Cuelga si te presionan o te impiden verificar. Y contáctalos tú por medio de sus canales oficiales.

Ten en cuenta

El número que aparece en pantalla puede ser alterado. Una llamada que parece provenir de un contacto conocido no es prueba suficiente de identidad.



3. Spoofting o suplantación del número

Es una técnica que altera el número o el nombre que aparece en una llamada o mensaje para que parezca venir de una persona o entidad conocida.

¿Cómo reconocerlo?

El número o el nombre parece confiable, pero la conversación te exige datos, pagos o acciones inusuales con rapidez.



En la pantalla aparece el número o el nombre de tu banco, pero quien llama no trabaja en el banco.



¿Qué hacer?

- No confíes solo en el número o el nombre que ves en la pantalla.
- Busca el contacto oficial y confirma si la solicitud es real.
- No uses el número que te contactó para devolver la llamada o continuar por otro chat.

Ten en cuenta

El identificador de llamada, el nombre del remitente o una apariencia institucional no bastan para confirmar quién está al otro lado.



Es una llamada muy breve que cuelga antes de que contestes. La intención puede ser que devuelvas la llamada, a veces a un número internacional o de alto costo.

¿Cómo reconocerlo?

Número desconocido, uno o dos timbres y ningún motivo aparente para que lo llamen.

Tienes una llamada perdida de un número con indicativo de otro país, y no esperas ninguna llamada de ese lugar.



¿Qué hacer?

- No devuelvas la llamada a números desconocidos solo por curiosidad o por presión.
- Si podría ser una entidad o un servicio que necesitas, busca el teléfono oficial y llama directamente.
- Revisa si reconoces el número y si esperabas un contacto.

Ten en cuenta

La urgencia y la curiosidad también pueden ser usadas para que actúes sin comprobar.

Busca la presión y protege tus datos personales

Quien intenta un fraude busca provocar presionarte por medio del miedo, la urgencia, la confianza o la ilusión para que entregues información o sigas instrucciones sin verificar. Esta forma de manipulación se conoce como ingeniería social

Antes de actuar pregúntate

- ¿Me están apurando o asustando?
- ¿Me piden guardar datos personales, entregar un código, enviar dinero o instalar algo?
- ¿Puedo terminar el contacto y comprobarlo por otro canal?
- ¿Me piden guardar el secreto o no colgar?

Protege tus datos y nunca entregues por llamada o mensaje:

- Contraseñas o claves
- Códigos que llegan a su celular (códigos de verificación o de un solo uso).
- Número, fecha de vencimiento o código de seguridad de sus tarjetas.
- Dinero o pagos para «proteger» una cuenta, recibir un premio o evitar una sanción.
- El control de tu celular: no instales aplicaciones ni compartas la pantalla a petición de quien te contactó.

Recuerda

En Colombia, la Ley 1581 de 2012 reconoce tu derecho a conocer, actualizar y rectificar tus datos personales; solicitar información sobre su uso y prueba de la autorización; acceder gratuitamente a los datos que hayan sido objeto de tratamiento; y, cuando corresponda, revocar la autorización o solicitar su supresión.



Confirma por tu cuenta

No uses el enlace, teléfono o chat incluido en el contacto inesperado para comprobar si ese mismo contacto es real. Busca los canales de contacto oficial e inicia una comunicación nueva y confirma según el contacto recibido:

★ Si recibiste un mensaje

No respondas. Abre por tu cuenta la aplicación oficial o inicia una conversación desde el canal que aparece en documentos o páginas oficiales.

★ Si recibiste un enlace

No lo abras desde el mensaje. Escribe tú mismo la dirección oficial o entra desde la aplicación. Revisa cuidadosamente el dominio: el candado del navegador, por sí solo, no demuestra que el sitio sea legítimo.

★ Si recibiste una llamada

Cuelga y busca el número en una fuente oficial. El identificador que aparece en pantalla puede ser alterado.

★ Si te piden un código o una clave

No los dictes ni los envíes por chat. Úsalos solo en una aplicación o sitio oficial cuando tú hayas iniciado la operación.

★ Si ves una alerta o una etiqueta

Tómala como una señal para revisar con cuidado. No la trates como una prueba definitiva de que la comunicación es segura o fraudulenta.

★ Si instalaste una aplicación o compartiste pantalla

Desconecta el equipo de internet si sospechas que otra persona tiene acceso. Desde un dispositivo confiable, cambia tus claves y busca asistencia técnica confiable. Comunícate con tu operador si crees que tu línea o tarjeta SIM fue afectada.

SI YA HICISTE CLIC O COMPARTISTE INFORMACIÓN

Actúa pronto para reducir el riesgo

No te culpes ni sigas conversando con quien te contactó. Prioriza detener el contacto y proteger tus cuentas y productos.

- ★ **1. DETÉNTE:** Cuelga, cierra el chat y no sigas instrucciones. No descargues ni instales nada más.
- ★ **2. AVISA:** Contacta cuanto antes al banco, entidad u operador por un canal oficial. Solicita bloqueo o medidas de protección si corresponde.
- ★ **3. PROTEGE:** Desde un dispositivo confiable, cambia las contraseñas afectadas. Si reutilizaste una clave, cámbiala también en otros servicios.
- ★ **4. REVISAS:** Verifica movimientos, sesiones abiertas, cambios de datos y operaciones que no reconozcas. Sigue las indicaciones de la entidad.
- ★ **5. GUARDA:** Conserva capturas, número, enlace, fecha, hora y comprobantes. No borres la conversación antes de guardar la evidencia.
- ★ **6. REPORTA:** Usa los canales oficiales de la entidad y de las autoridades competentes según el caso. Para asuntos relacionados con datos personales, consulta los canales de la SIC.



RECUERDA EL ABC: Reconoce las señales de **Alerta**, **Busca** la presión, protege tus datos y **Confirma** por tu cuenta. **#LaClaveEsVerificar**

Consulta materiales y recomendaciones en el micrositio de la CRC en www.crcom.gov.co/es/micrositios/la-clave-es-verificar.

Esta guía es pedagógica: no reemplaza la atención de tu entidad financiera, operador ni la orientación de las autoridades competentes.

 **#LaClave
EsVerificar**