INFO-TYPERS · GUÍA SIN COSTO

¿este mensaje de mi paquete es falso?

Mensajes falsos de bancos y envíos: cómo reconocerlos

Las 3 señales de un mensaje falso, lo que tu banco nunca te pide, qué hacer si ya caíste y cómo reportarlo. En 5 minutos.

VERSIÓN INTERACTIVA

typersagency.com/blog/mensajes-falsos-bancos-envios

TYPERS

LA IDEA EN UNA FRASE

Para, mira y entra tú



Si no lo esperabas, te apura y el enlace no es el oficial, es falso: no lo abras, entra tú por la app o la página que ya conoces y repórtalo.

- Las 3 señales de un mensaje falso.
- Lo que tu banco nunca te pide.
- La tarea: reporta el próximo en 5 pasos.

Datos de la Superintendencia Financiera, la DIAN, la Policía Nacional y la FTC de Estados Unidos, consultados el 6 de noviembre de 2026. Envíos Rayo y TU BANCO son nombres inventados para los ejemplos.

PARTE 1 DE 4

01
Las 3 señales



- No lo esperabas: no pediste nada, el número es raro y aun así sabe tu nombre.
- Te apura: «hoy vence», «tu cuenta será bloqueada». La prisa es para que no pienses.
- El enlace no es el oficial: tiene guiones, letras de más o un final raro.
- Te pide pagar o dar datos para liberar un paquete. La DIAN advierte este engaño: piden datos de la tarjeta para el «envío retenido».

EJEMPLO · EMPRESA INVENTADA

«Envíos Rayo te escribe que tu paquete está retenido y que pagues 2.000 pesos en enviosrayo-co.top/pago. Su página oficial es enviosrayo.co: el guion y el .top la delatan.»

ERROR COMÚN

Creerle porque trae tu nombre o un número de guía. Esos datos también se filtran.

02

Lo que tu banco nunca te pide



NUNCA POR MENSAJE, LLAMADA O CORREO · EJEMPLO

- Tus claves: ni la de la app ni la de la tarjeta.
- Los códigos que te llegan por mensaje, ni el número de tu token.
- Ni por mensaje de texto, llamada o correo. Lo recuerda la Superintendencia Financiera. Trata igual un WhatsApp.
- Si dudas, cuelga y entra tú por la app o llama al número que está detrás de tu tarjeta.

EJEMPLO · BANCO INVENTADO

«Te llega un SMS de TU BANCO: hubo un movimiento raro y debes confirmar tu clave en un enlace. Ningún banco te la pide así.»

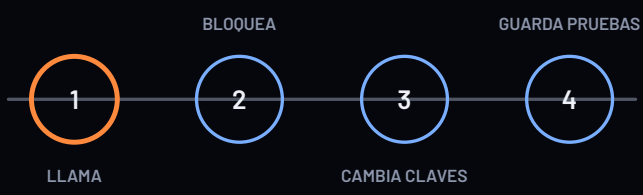
ERROR COMÚN

Dictar el código que te acaba de llegar porque «es para cancelar la compra». Ese código es solo tuyo.

PARTE 3 DE 4

03

Si ya hiciste clic o diste datos



- Llama ya a tu banco por el número de tu tarjeta o de su app, no por el del mensaje.
- Bloquea la tarjeta o la cuenta desde la app, si te deja.
- Cambia tus claves, primero la del banco y la del correo.
- Guarda pruebas: captura del mensaje, el número que lo envió y la hora.
- Si solo abriste el enlace, cierra la página y no descargues nada.

EJEMPLO · CASO DE MUESTRA

«Pagaste los 2.000 pesos en la página falsa de Envíos Rayo: llamas al número de tu tarjeta, la bloquean y guardas la captura.»

No borres el mensaje todavía: lo necesitas para el reporte.

ERROR COMÚN

Responderle al mensaje para reclamar. Solo confirmas que tu número está activo.

PARTE 4 DE 4

04

Tarea: repórtalo en 5 pasos



1. No abras el enlace ni respondas.
2. Toma captura de pantalla del mensaje y del número que lo envió.
3. Repórtalo en tu celular: en Android (Mensajes de Google), mantén pulsada la conversación y toca Bloquear y Marcar como spam; en iPhone, toca Reportar como no deseado y Eliminar y reportar.
4. Avísale a la empresa o al banco por su canal oficial y, si diste datos o perdiste plata, repórtalo en el CAI Virtual de la Policía (caivirtual.policia.gov.co) o denuncia en ADenunciar.
5. Bórralo, si tu celular no lo borró al reportarlo.

EJEMPLO · CASO DE MUESTRA

«Te llegó otro «paquete retenido» de Envíos Rayo: captura, Marcar como spam, aviso por enviosrayo.co y a la papelera.»

Reportar no tiene costo. En iPhone no puedes reportar un mensaje después de responderlo.

ERROR COMÚN

Reenviar el mensaje a tus grupos «para avisar» con el enlace vivo. Manda la captura, no el enlace.

PREGUNTAS FRECUENTES

Preguntas rápidas

¿Y si el paquete sí es real?

Mira el estado en la app o la página que ya conoces, no en el enlace del mensaje. Así lo aconseja también la FTC.

¿Leer el mensaje ya es peligroso?

Leerlo no es lo grave. Lo riesgoso es tocar el enlace, descargar algo o escribir tus datos.

¿Mi banco me puede escribir de verdad?

Sí, para avisos. Pero no te pide claves ni códigos. Si dudas, entra tú por la app.

GLOSARIO

Las palabras que vas a encontrar

Smishing: Engaño por mensaje de texto con un enlace a una página falsa.

Suplantación: Cuando alguien se hace pasar por tu banco o por una empresa.

Dominio: El nombre de la página, como enviosrayo.co. Una letra o un guion de más ya es otra página.

Token: El código que cambia cada tanto y aprueba tus operaciones. Es solo tuyo.

Lo que esta guía no promete

- No detecta todos los engaños: cambian rápido. Ante la duda, entra tú por el canal oficial.
- No reemplaza lo que te diga tu banco ni la Policía.

FUENTES

De dónde sale cada dato

Páginas oficiales consultadas el 6 de noviembre de 2026.

Superintendencia Financiera · No se deje engañar: suplantación con correo falso
https://www.superfinanciera.gov.co/publicaciones/10112102/

DIAN · Fraudes de tráfico postal y envíos urgentes
https://www.dian.gov.co/aduanas/Documents/Fraudes-de-trafico-postal-y-envios-urgentes.pdf

Policía Nacional · Ciberseguridad y CAI Virtual
https://www.policia.gov.co/ciberseguridad

FTC · Cómo reconocer y reportar mensajes de texto no deseados (en inglés)
https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages

Google · Cómo denunciar spam en Mensajes de Google
https://support.google.com/messages/answer/9061432?hl=es

Apple · Reportar mensajes no deseados y bloquear remitentes en el iPhone
https://support.apple.com/es-lamr/guide/iphone/iph3f94d910d/ios

CÓMO LO HACEMOS EN TYPERS

En Typers ayudamos a negocios a contarles a sus clientes por qué canales oficiales les escriben.

¿POR DÓNDE LES ESCRIBES?

Revisamos contigo tus canales oficiales. Pide tu diagnóstico sin costo.

DIAGNÓSTICO SIN COSTO · TYPERSAGENCY.COM/BRIEF

Más guías en typersagency.com/blog. Síguenos como Info-Typers para aprender más.