

Cómo reconocer un correo, un mensaje o un QR falso

Tres cosas que se miran antes de pulsar: qué te pide, quién lo envía y a dónde lleva. También para los códigos QR pegados y las llamadas con una voz clonada.



Un mensaje falso se hace pasar por alguien en quien confías —tu banco, una tienda, un familiar, tu jefe— para que pulses un enlace, entregues un dato o hagas un pago sin comprobar quién lo pide. No hace falta ser experto para descubrirlo: hace falta un método y una pausa.

Las tres piezas que se miran siempre

Antes de responder, pulsar o pagar, revisa tres cosas:

- **Qué te pide.** ¿Te asusta, te apura o te promete un premio? ¿Te pide una contraseña, un código o un pago?
- **Quién lo envía.** Mira la dirección o el número completos, no solo el nombre que aparece. Una letra de más o una terminación rara cambian por completo quién está detrás.
- **A dónde lleva.** El enlace puede decir una cosa y llevar a otra. Lo que cuenta es la dirección real, no el texto azul.

Un mensaje puede traer el logotipo verdadero, tu nombre y hasta datos ciertos de una compra tuya, y aun así ser falso. La apariencia no demuestra quién lo escribió.

La prisa es parte de la trampa

«Último aviso», «tu cuenta se bloquea en una hora», «necesito que me transfieras ya»: la urgencia está ahí para que actúes antes de pensar. La respuesta nunca sale del propio mensaje:

1. Detente.
2. No uses el enlace, el botón ni el número que trae el mensaje.
3. Entra tú por la app oficial o escribiendo la dirección que ya conoces, y comprueba ahí si el problema existe.

Si el mensaje parece de una persona conocida, confírmalo por el canal que siempre usas con ella, nunca respondiendo al mismo mensaje.

Las direcciones que engañan al ojo

Hay direcciones hechas para pasar a simple vista: un número «0» en lugar de la letra «o», una «rn» que parece una «m», o el nombre real seguido de otra terminación, como `mibanco-seguro.net` en lugar de `mibanco.com`. Léelas despacio, letra por letra, y mejor en la barra del navegador que en el texto del correo.

Archivos que no esperabas

Un adjunto que no esperabas no se abre, aunque venga de alguien conocido: su cuenta puede estar en manos de otra persona. Pregunta primero por otro medio si de verdad lo envió. Desconfía todavía más si viene comprimido o te pide «activar contenido» para verse.

Los QR también mienten

Un código QR es solo una dirección de internet en forma de dibujo, y el ojo no puede leerla. Por eso hay quien pega su propio QR **encima** del verdadero: en un parquímetro, en la mesa de un restaurante, en un cartel. Quien lo escanea para pagar termina en una página falsa que se queda con su tarjeta.

- Antes de abrirlo, mira la vista previa de la dirección que muestra la cámara.
- Si no es la dirección del sitio que esperabas, no metas ningún dato.
- Si tienes la menor duda, paga por la app o la web oficial que ya conoces: un QR nunca es la única forma de pagar.

La voz de un familiar pidiendo dinero

Hoy bastan unos segundos de audio de un video público para imitar la voz de una persona. La llamada siempre se parece: un hijo, una nieta o un hermano, asustado o llorando, pide una transferencia **ya** a una cuenta que no conoces.

- **Cuelga y llama tú** al número de siempre de esa persona. Si no contesta, llama a alguien que pueda estar con ella.
- **Acuerden una palabra clave familiar**, en persona y nunca por chat: algo que solo ustedes sepan. Si alguien llama con una emergencia y pide dinero, se le pide la palabra. Sin palabra, no hay transferencia.

Tu lista para hoy

1. Ante cualquier aviso urgente, entro por la app o la web oficial, no por el enlace.
2. Leo la dirección completa de quien me escribe y la del enlace, letra por letra.
3. No abro adjuntos que no esperaba sin confirmarlo por otro medio.
4. Miro la vista previa de un QR antes de pagar con él.
5. Acordé una palabra clave con mi familia para emergencias con dinero.

Practícalo · Módulo 3 de Tu primer escudo: Mensajes que mienten

En el módulo revisas catorce correos simulados uno por uno, sigues a alguien que va a pagar un parquímetro con un QR y recibe una llamada con la voz de su hija, y practicas con una herramienta que analiza enlaces. Puedes leer las salas sin cuenta; responder los casos y guardar tu avance pide iniciar sesión.

Empieza aquí: pro.whoami-labs.com/rutas/tu-primer-escudo/mensajes-que-mienten

Esta guía en la web: pro.whoami-labs.com/guias/como-reconocer-un-mensaje-falso