



Duda con método

03

¿Me quieren estafar? Revísalo en 30 segundos

*¿Cuántos mensajes te llegaron esta semana
pidiéndote que hicieras algo ya?*

Las 4 señales

Casi todos los fraudes usan al menos una:



1. **Prisa.** “Tu cuenta se bloquea hoy”, “solo quedan dos horas”.
2. **Secreto.** “No le digas a nadie”, “no cuélgues”.
3. **Un pago raro.** Un depósito en tienda, una transferencia a una persona, “un pago para liberar tu premio”.
4. **Una liga o un código.** Te mandan a una página o te piden un código que te acaba de llegar.

Si ves una, frena. Si ves dos, casi seguro es fraude.

La prueba de los 30 segundos

Antes de pagar, dar un dato o abrir una liga:

- **Cuelga o cierra el chat.** La prisa es suya, no tuya.
- **Busca tú el contacto oficial:** el teléfono atrás de tu tarjeta, la app del banco o una página que termine en **.gob.mx**. Y pregunta ahí.
- **Cuéntaselo a alguien.** Si te pidieron secreto, con más razón.

Ningún banco, gobierno o empresa seria se enoja porque verifiques.



“Le escribimos de su banco”

De enero a marzo de 2026, tres de cada cuatro reclamos a los bancos fueron por posible fraude, y el mensaje de texto falso es el anzuelo más usado. Suele decir que hay un cargo raro o que tu cuenta se va a bloquear, y trae una liga.



- No abras la liga: entra tú a la app de tu banco.
- Tu banco no te pide por mensaje tu NIP, tu contraseña ni los códigos que te llegán.

El registro de tu celular

Las líneas de prepago se tienen que vincular a tu CURP, con fechas que van de agosto al 31 de diciembre de 2026 según el último dígito del número. Es real, y por eso mismo ya hay ligas falsas.



- El trámite es **gratis**.
- Hazlo solo en **registratuline.crt.gob.mx**, que te manda al portal de tu compañía, o en un centro de atención de tu compañía.
- No mandes fotos de tu INE ni tu CURP por ligas que te lleguen en mensajes.

Becas, pensiones y apoyos

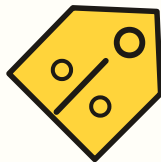
Cada vez que abre un registro grande del gobierno, aparecen páginas falsas. Pasó con la Beca Rita Cetina y con la credencial del INAPAM: piden datos bancarios o un depósito “para activar el apoyo”.



- Esos trámites no cuestan.
- Las páginas oficiales terminan en **.gob.mx**. Por ejemplo, la de la beca es becaritacetina.gob.mx.
- Si te cobran por inscribirte o por “agilizar”, es fraude.

Buen Fin y compras en línea

El Buen Fin 2026 va del 13 al 17 de noviembre. Las ofertas falsas llegan antes.



- **Escribe tú la dirección** de la tienda; no entres desde anuncios ni mensajes.
- **Desconfía de precios demasiado buenos** y de vendedores que solo aceptan transferencia o depósito.
- **Paga con tarjeta**, de preferencia la digital. Con tarjeta puedes pedirle una aclaración al banco; el dinero que le transfieres a un desconocido es mucho más difícil de recuperar.

Famosos que te venden inversiones

Videos de famosos o empresarios que “recomiendan” una plataforma para multiplicar tu dinero. Muchos están hechos con IA: la cara y la voz son falsas. Impunidad Cero documenta uno que usaba la imagen de Carlos Slim.



- Nadie serio te promete ganancias seguras y rápidas.
- Antes de invertir, busca a la empresa en el **SIPRES** de Condusef. Si no aparece, no le deposites.

Préstamos que luego te persiguen

Apps que prometen dinero en minutos y sin revisar tu historial.

Después cobran intereses imposibles y amenazan a tus contactos. Condusef les dice “montadeudas”. Señales:



- Te piden dinero por adelantado para “liberar” el préstamo.
- Quieren acceso a tus contactos, tus fotos o tu micrófono.
- No aparecen en el **SIPRES** de Condusef.

¿Y a quién le conviene?

Modo deconstruir

¿Por qué los fraudes se sienten cada vez más reales? Porque saben más de ti. En enero de 2026, un grupo aseguró haberse llevado información de instituciones como el SAT, el IMSS-Bienestar y la SEP. La consultora Grant Thornton calculó que ahí venían datos de unos 36 millones de personas.



Con tu nombre, tu CURP y tu dirección, una llamada falsa suena oficial. Cuidarte ayuda, pero cuidar tus datos también es chamba de quien los guarda.

La otra mitad

La misma inteligencia artificial que hace más creíbles los fraudes también se usa para detectarlos: hay empresas dedicadas a frenar en tiempo real los intentos hechos con IA.



Y tú tienes la herramienta más vieja y más efectiva: preguntar antes de actuar. Haz la prueba de los 30 segundos hasta que te salga sola, y mándale esta guía a quien más quieres.

y te dejo con esta pregunta

Si cada filtración de datos hace más creíbles los fraudes, ¿a quién le vas a exigir que cuide los tuyos?

¿Te pasó algo así? Cuéntamelo en deconstruir.me/envianos-tu-historia

Léela en línea y compártela: deconstruir.me/guias/me-quieren-estafar

El porqué, en una nota: Hackear ya no es cosa de genios

Fuentes

1. El Informador: reclamos por fraude bancario y el SMS falso como canal principal (datos de Condusef) (informador.mx)
2. Por Esto: cómo registrar tu línea celular paso a paso (portal oficial de la CRT) (poresto.com)
3. El Imparcial: qué líneas deben vincularse con la CURP y fechas límite (elimparcial.com)
4. Excélsior: sitios falsos para el registro de la Beca Rita Cetina (excelsior.com.mx)
5. ADN40: la credencial del INAPAM es gratis; cuidado con páginas falsas (adn40.mx)
6. Expansión: fechas del Buen Fin 2026 (expansion.mx)
7. Impunidad Cero: Guía para denunciar fraudes cibernéticos (impunidadcero.org)
8. El Imparcial: Condusef alerta sobre apps de préstamos fraudulentas y cómo verificarlas (elimparcial.com)
9. El Universal: el hackeo al SAT, al IMSS y a otras instituciones (enero 2026) (eluniversal.com.mx)
10. Expansión: la IA en el fraude bancario (datos de Incode) (expansion.mx)

Las ligas completas están en deconstruir.me/guias/me-quieren-estafar

Información general, no asesoría legal ni financiera. Si tu caso es complicado, busca a una persona experta.

Hecha con ayuda de inteligencia artificial y revisada contra las fuentes.

Licencia CC BY-NC 4.0: puedes imprimirla y compartirla sin fines de lucro, dando crédito a deconstruir.me.