MILLORA

Navegando Seguro

Guía para reconocer y evitar los fraudes más comunes en internet. Un servicio a la comunidad de Millora.

Ante la duda, detente y consulta a alguien de confianza antes de dar clic o dar datos. No hay prisa que valga tu dinero ni tu tranquilidad.

01. Correos y mensajes que fingen ser de tu banco

Te escriben con urgencia para que des clic o entregues tus claves. No lo son.

Recibes un correo o mensaje que parece de tu banco, una tienda o una paquetería. Tiene el logotipo, los colores y un tono urgente: “tu cuenta será bloqueada”, “verifica tus datos ahora”, “tienes un paquete retenido”. Te piden dar clic en un enlace y escribir tus claves, tu tarjeta o un código.

SEÑALES DE ALERTA

- Te apuran. La urgencia es la herramienta favorita del fraude.
- El correo del remitente tiene letras raras o no coincide con el oficial.
- Te piden contraseñas, NIP o el código que llega por SMS.
- El enlace se ve extraño si lo dejas presionado sin abrirlo.
- Hay faltas de ortografía o saludos genéricos (“Estimado cliente”).

QUÉ HACER

- No des clic. Cierra el mensaje.
- Ningún banco real pide tus claves por correo, mensaje o llamada.
- Si dudas, entra tú mismo a la página o app oficial, escribiéndola a mano.
- Antes de actuar, muéstraselo a alguien de confianza.

02. El robo de tu WhatsApp

Te piden un código de 6 dígitos. Si lo das, pierdes tu cuenta.

Alguien intenta entrar a tu WhatsApp. Para lograrlo necesita un código de 6 dígitos que llega a tu teléfono por SMS. Entonces te escribe —a veces haciéndose pasar por un familiar o por “soporte”— y te dice: “te envié un código por error, ¿me lo reenvías?”. Si se lo das, toman tu cuenta y luego escriben a tus contactos pidiéndoles dinero en tu nombre.

SEÑALES DE ALERTA

- Te llega un código que tú no pediste.
- Alguien te pide ese código “por error” o “para verificar”.
- Un contacto conocido pide dinero con prisa y de forma rara.

QUÉ HACER

- Nunca compartas el código de 6 dígitos. Con nadie. Por ningún motivo.
- Activa la verificación en dos pasos en los ajustes de WhatsApp.
- Si un familiar te pide dinero por mensaje, llámalo por teléfono para confirmar.
- Si pierdes tu cuenta, avisa a tus contactos por otro medio.

03. Cargos en tu tarjeta que tú no hiciste

Compras pequeñas y repetidas que se acumulan sin que te des cuenta.

Después de entregar tu número de tarjeta en una página falsa, o tras un descuido, empiezan a aparecer cargos. A veces son grandes; a veces son pequeños y seguidos, justamente para que pasen desapercibidos en el estado de cuenta.

SEÑALES DE ALERTA

- Cobros que no reconoces, aunque sean de montos bajos.
- Suscripciones que nunca contrataste.
- Mensajes de tu banco sobre compras que no hiciste.

QUÉ HACER

- Revisa tus movimientos con calma cada semana.
- Activa las alertas por mensaje de cada compra con tu banco.
- Si ves algo raro, llama al número que está al reverso de tu tarjeta.
- Pide ayuda a alguien de confianza para revisar juntos el estado de cuenta.

04. Amenazas y chantajes

Te escriben para asustarte y que pagues. Casi siempre es mentira.

Recibes un mensaje que busca asustarte: dicen tener fotos tuyas, información privada, o que un familiar está en problemas. Exigen dinero rápido y te presionan para que no le cuentes a nadie. El miedo y el secreto son sus armas.

SEÑALES DE ALERTA

- Te exigen dinero con amenazas y mucha prisa.
- Te insisten en que no le digas a nadie.
- Usan miedo: “le pasará algo a tu familia”, “publicaré esto”.

QUÉ HACER

- No pagues y no respondas con miedo. Respira.
- El secreto es justo lo que ellos quieren. Cuéntale a alguien de confianza de inmediato.
- Si mencionan a un familiar, llámalo directamente para verificar.
- Guarda los mensajes y considera denunciar ante las autoridades.

05. Cuando entran a tus cuentas

Una contraseña débil o repetida es una puerta abierta.

Si usas la misma contraseña en todos lados, o una muy fácil de adivinar, basta con que se filtre una para que entren a varias: tu correo, tus redes, tu banca. Desde ahí pueden hacerse pasar por ti o cambiar tus claves.

SEÑALES DE ALERTA

- No puedes entrar a una cuenta que sí usabas.
- Te avisan de un inicio de sesión desde un lugar desconocido.
- Tus contactos reciben mensajes raros de tu parte.

QUÉ HACER

- Usa una contraseña distinta para tu correo y tu banco.

- Activa la verificación en dos pasos donde se pueda.
- Una frase larga y fácil de recordar es más segura que una palabra corta.
- Si sospechas que entraron, cambia la clave y avisa a alguien de confianza.

06. Tus redes sociales abiertas a todos

Lo que publicas en público le da pistas a quien quiere engañarte.

Cuando tu perfil es público, cualquiera ve tus fotos, tu familia, dónde vives, cuándo sales de viaje y los nombres de tus seres queridos. Con esa información construyen engaños creíbles, hechos a tu medida.

SEÑALES DE ALERTA

- Tu perfil se puede ver sin ser tu amigo o contacto.
- Publicas en tiempo real cuándo no estás en casa.
- Aceptas solicitudes de personas que no conoces.

QUÉ HACER

- Pon tus perfiles en privado: que solo te vean tus contactos.
- No aceptes a desconocidos.
- Evita publicar viajes mientras ocurren; cuéntalos al volver.
- Pide ayuda a alguien de confianza para revisar tu configuración de privacidad.

07. Llamadas con la voz de un familiar (hecha con inteligencia artificial)

Suena igual que tu hijo o nieto pidiendo dinero urgente. Pero no es él.

Con unos pocos segundos de audio —tomados de una nota de voz o de un video en redes sociales— hoy se puede imitar la voz de cualquier persona usando inteligencia artificial. El estafador te llama y escuchas una voz idéntica a la de tu hijo, nieto o un familiar: llora, dice que tuvo un accidente o que está en problemas y necesita dinero de inmediato. La voz suena real, y por eso engaña.

SEÑALES DE ALERTA

- Una llamada con mucha urgencia y pidiendo dinero ya.
- La voz suena conocida, pero la situación es extraña o repentina.
- Te piden que no cuelgues y que no llames a nadie más.
- Insisten en transferencias, depósitos o tarjetas de regalo.

QUÉ HACER

- Cuelga y llama tú mismo al familiar a su número de siempre para confirmar.
- Acuerda con tu familia una palabra secreta para verificar emergencias reales.
- Haz una pregunta que solo el familiar verdadero sabría responder.
- Que la voz suene igual no prueba nada: hoy la voz se puede imitar.

08. El falso soporte técnico

Te dicen que tu equipo tiene un virus y se ofrecen a “arreglarlo”.

Recibes una llamada, un correo o una ventana emergente que dice que tu computadora o teléfono tiene un virus o un problema grave. Se hacen pasar por una empresa conocida y te ofrecen ayuda. Para “arreglarlo”, te piden instalar un programa o darles acceso remoto a tu equipo. Con eso toman el control, ven tus claves y pueden vaciar tus cuentas.

SEÑALES DE ALERTA

- Una alerta que aparece de la nada diciendo que tienes un virus.
- Te piden instalar un programa o darles control de tu equipo.
- Te presionan para que actúes rápido y pagues una “reparación”.
- Piden el pago en tarjetas de regalo o transferencias.

QUÉ HACER

- Las empresas reales no te llaman para avisarte de un virus. Cuelga.
- Nunca instales programas que te pida un desconocido.
- No des acceso remoto a tu equipo a nadie que no conozcas.
- Si te preocupa tu equipo, acude con alguien de confianza o un técnico conocido.

09. Códigos QR falsos

Un código pegado encima del verdadero te lleva a una página de fraude.

Los códigos QR son prácticos, pero también se usan para engañar. Los estafadores pegan un código falso encima de uno real —en un parquímetro, un restaurante, un recibo o un cartel— o lo mandan por mensaje. Al escanearlo, te llevan a una página falsa que pide tus datos o tu tarjeta, o instala algo dañino en tu teléfono.

SEÑALES DE ALERTA

- Un código QR pegado encima de otro, o que se ve manipulado.
- Te lleva a pedir datos o pagos de forma inesperada.
- Llega por mensaje de un remitente que no reconoces.
- La dirección de la página se ve rara después de escanear.

QUÉ HACER

- Antes de dar datos, revisa que la dirección sea la oficial.
- Desconfía de códigos pegados o sueltos en lugares públicos.
- No escanees códigos que llegan por mensaje de desconocidos.
- Si dudas, mejor entra a la página oficial escribiéndola tú mismo.
