Detecta deepfakes y fraudes con voz clonada

Señales para reconocer llamadas y videos falsos hechos con IA, cómo acordar una palabra clave familiar y qué hacer si te piden dinero urgente.

Léelo con tu familia y con quien maneja pagos en tu negocio. Hoy una voz o un rostro se pueden imitar con muy poco material; tu defensa es verificar por otro canal antes de actuar.

Señales de alerta

En la llamada o el audio	En el video o la foto
Urgencia: «es ahorita o pasa algo grave»	Labios que no coinciden con la voz
Secreto: «no le digas a nadie»	Parpadeo, dientes o manos extraños
Dinero por transferencia o depósito	Bordes de la cara borrosos al moverse
«Cambié de número»	Luz que no corresponde al fondo
Evade preguntas personales	Video muy corto o de mala calidad

Las imitaciones mejoran cada año, así que no te fíes solo de lo que ves u oyes. La señal más confiable es la combinación de urgencia, secreto y dinero.

Palabra clave familiar

1. Elijan en persona una palabra o frase que no aparezca en redes (nada de mascotas ni fechas).
2. Acuerden la regla: quien pida dinero o ayuda urgente debe decirla.
3. No la escriban en chats ni la compartan fuera del círculo.
4. Practíquenla con niñas, niños y personas mayores.
5. Cámbienla si alguien la dijo por error.

En el negocio aplica lo mismo: ningún pago ni cambio de cuenta bancaria se autoriza solo por llamada, audio o mensaje. Se confirma por un segundo canal.

Si recibes la llamada

1. **No des datos.** No digas nombres («¿eres tú, Dany?»); deja que quien llama se identifique.
2. **Pide la palabra clave** o pregunta algo que solo esa persona sabría.
3. **Cuelga y marca tú** al número que ya tenías guardado, o a alguien que esté con esa persona.
4. **No transfieras ni compartas códigos.** Ninguna urgencia real impide verificar cinco minutos.
5. **Guarda evidencia:** número, hora, capturas y audios.

Si ya caíste o lo intentaron

- ☐ Llama de inmediato a tu banco para reportar la operación y bloquear lo necesario. Si no te da solución, pide orientación a la CONDUSEF.
- ☐ Reporta al 088 de la Guardia Nacional, que orienta sobre delitos cibernéticos. Si hay riesgo inmediato, marca al 911.
- ☐ Avisa a tu familia y contactos para que no caigan con tu nombre o tu voz.
- ☐ Cambia contraseñas y activa la verificación en dos pasos.

Errores comunes

- Confiar porque «sonaba igualito»: la voz ya no es prueba de identidad.
- Verificar por el mismo canal por el que llegó el mensaje.
- Actuar por pena o por miedo en lugar de colgar y confirmar.
- Reenviar el video dudoso «por si acaso»: así se propaga el engaño.

¿Quieres dominar el tema? El curso «Seguridad, privacidad y ética de la IA» lo enseña paso a paso, con ejercicios y certificado: https://klaroia.com/cursos/seguridad-etica-ia