# ¿Real o *deepfake*?

## Guía para detectar suplantaciones digitales

Los rostros ya no dicen toda la verdad. En un contexto mundial donde la inteligencia artificial puede hacer que cualquiera diga o haga lo que nunca dijo ni hizo, distinguir entre una persona real y una suplantación digital se vuelve crucial. **¿Estamos viendo a tu jefe o a un robot que se parece mucho a él?.**

Esta guía te ayudará a identificar los *deepfakes* y proteger tu identidad y tu empresa del engaño digital.

### ¿Qué es un *deepfake* y por qué debería importarte?

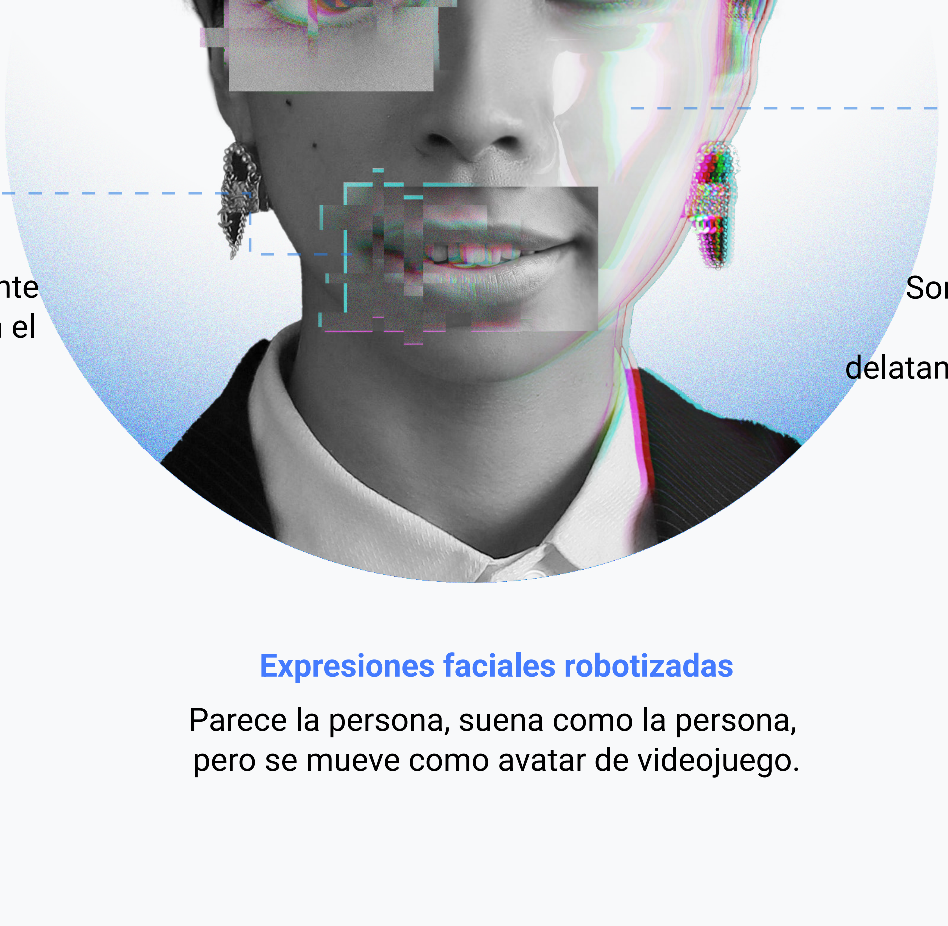
El término *deepfake* se popularizó en 2017 en Reddit (plataforma diseñada para compartir contenido con el fin de crear comunidades de discusiones temáticas conocidas como subreddits) cuando un usuario comenzó a compartir videos de carácter sexual manipulados con tecnología de código abierto para intercambiar los rostros de los actores de dicho contenido por los de celebridades.

**Un *deepfake* es un contenido falso —video, audio o imagen— generado con inteligencia artificial para imitar a una persona real.**

Se usa para todo, desde bromas hasta fraudes millonarios. Y sí, ya ha pasado que un CEO ficticio “autorizó” transferencias millonarias con su voz clonada.

Tu identidad vale más de lo que crees.
Y alguien más podría estar usándola ahora mismo.

## Top 5 | Señales de alerta para detectar un *deepfake*



**Ojos que no parpadean o parpadean raro**
La mayoría de los *deepfakes* fallan en simular movimientos oculares naturales.

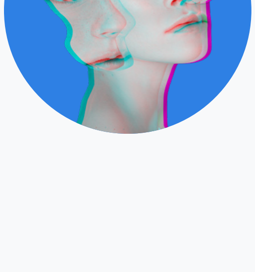
**Textura de piel plástica o demasiado perfecta**
Los *deepfakes* muchas veces suavizan de más o tienen fallas en la piel.

***Lipsync* fallido**
Si los labios no están perfectamente sincronizados con el audio, desconfía.

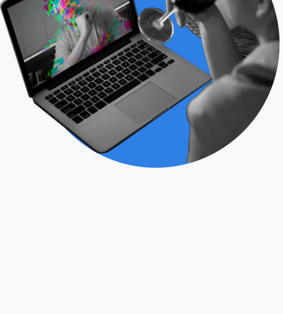
**Iluminación inconsistente**
Sombras fuera de lugaro luces pocorealistas delatan una edición artificial.

**Expresiones faciales robotizadas**
Parece la persona, suena como la persona, pero se mueve como avatar de videojuego.

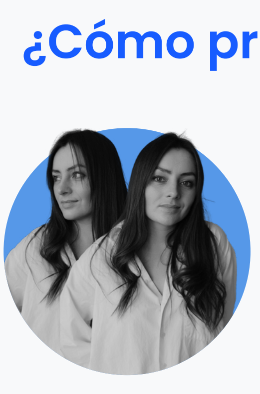
## Modos en que los usan para fraudes



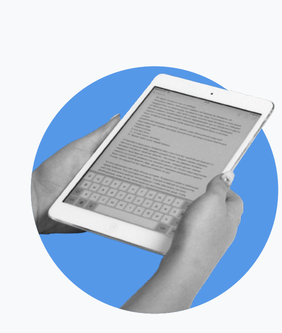
**Autorizaciones falsas**
*Deepfakes* de directivos para pedir transferencias urgentes o liberar acceso a sistemas.



**Campañas de desinformación**
Videos falsos de políticos o figuras públicas diciendo cosas que nunca dijeron.



**Suplantación de identidad en entrevistas laborales remotas**
Candidatos que no son quienes dicen ser.

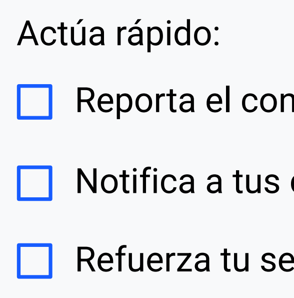


**Estafas románticas con videochats alterados**
También se liga con *deepfakes*.

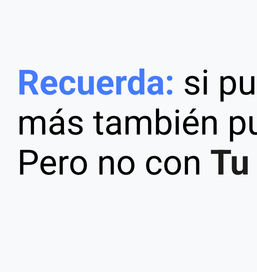
## ¿Cómo protegerte?

**Usa autenticación biométrica real y en vivo**
Las pruebas de vida, como parpadear o girar la cabeza, no pueden ser imitadas fácilmente por *deepfakes*.

**Verifica documentos y rostros con soluciones KYC certificadas**
En **Tu Identidad** contamos con herramientas de validación facial con detección de *deepfakes* y pruebas antifraude.



**Capacita a tu equipo**
Una empresa entrenada es una empresa protegida.
No basta con ver para creer.



**Nunca tomes decisiones importantes solo por video o videollamada**
Valida siempre por otro canal o con una solución tecnológica confiable.

## ¿Y si ya fuiste víctima?

Actúa rápido:

- ☐ Reporta el contenido falso.
- ☐ Notifica a tus contactos o clientes.
- ☐ Refuerza tu seguridad digital.
- ☐ Acércate a especialistas en protección de identidad como **Tu Identidad**.

**Recuerda:** si puedes ser tú en internet, alguien más también puede hacerse pasar por ti.
Pero no con **Tu Identidad** de tu lado.

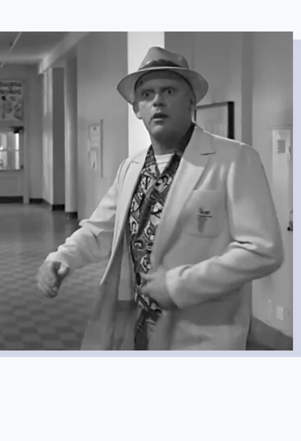
## Mini test:
## ¿Real o *deepfake*?

¿Te animas a jugar?
Prueba tu ojo con ejemplos de videos reales y falsos.

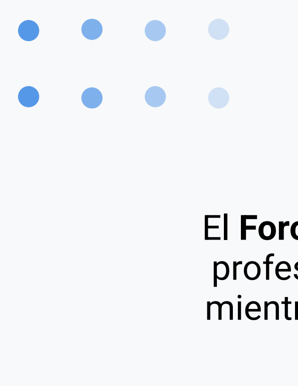
Desafía a tu equipo o comunidad:
¿Quién detecta el engaño mejor?.

**Verifica tus respuestas al final**

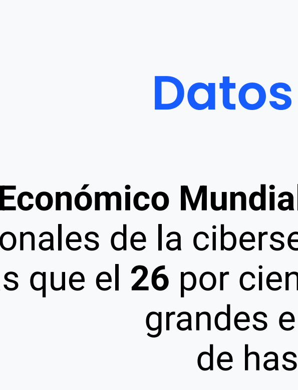
1



2

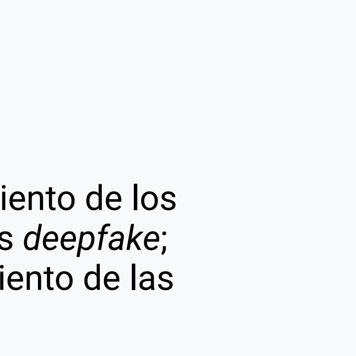


3



4

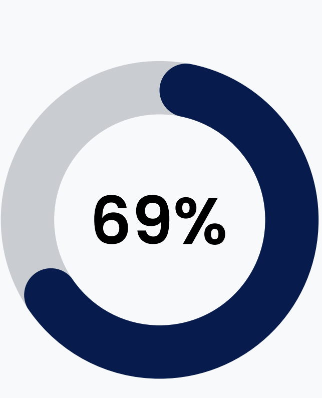
5



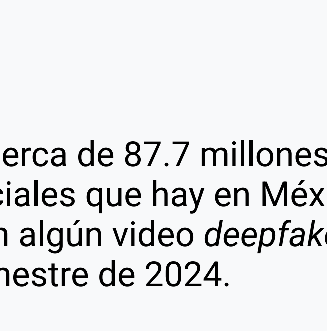
6

## Datos sobre *deepfakes*.

El **Foro Económico Mundial**, señala que en 2022 el **66** por ciento de los profesionales de la ciberseguridad experimentaron ataques *deepfake*; mientras que el **26** por ciento de las pequeñas y el **38** por ciento de las grandes empresas tuvieron pérdidas de hasta 9 millones de pesos.

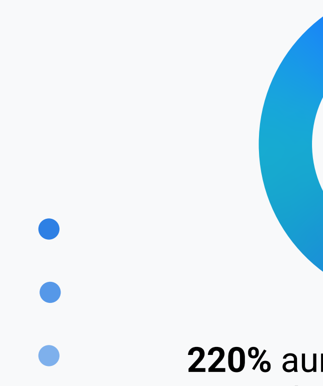


Profesionales de la ciberseguridad que experimentaron ataques *deepfake*.

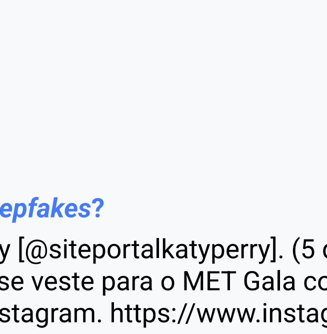


Pequeñas empresas.

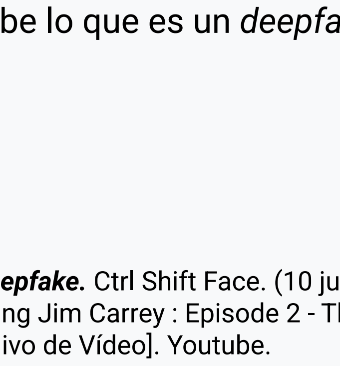
Grandes empresas.



**69%** de los cerca de 87.7 millones de usuarios de redes sociales que hay en México tuvieron contacto con algún video *deepfake* en el segundo trimestre de 2024.



**220%** aumentaron los fraudes cometidos con videos *deepfake* en México durante 2024.



**72%** de los usuarios de Internet en nuestro país no sabe lo que es un *deepfake*.

### Respuestas de: ¿real o *deepfakes*?

**1. Real.** siteportalkatyperry [@siteportalkatyperry]. (5 de mayo de 2025). Ninguém se veste para o MET Gala como Katy Perry! [Fotografía]. Instagram. https://www.instagram.com/p/DJSJ0KEyV5B/?utm_source=ig_web_copy_link&igsh=ZTR4d245aXo0YmFo
**2. *Deepfake*.** Katy Perry [@katyperry]. (6 de mayo de 2025). ouldn’t make it to the MET, I’m on The Lifetimes Tour (see you in Houston tomorrow IRL) [Fotografía]. Instagram. https://www.instagram.com/p/DJTlSmeR9Kg/?utm_source=ig_web_copy_link&igsh=MW55enA3eGRhNzF0eQ==
**3. Real.** Kubrick S. (Director). (1980). El resplandor [Película].
**4. *Deepfake*.** Ctrl Shift Face. (10 julio de 2019). The Shining starring Jim Carrey : Episode 2 - The Bat [DeepFake] [Archivo de Vídeo]. Youtube. https://www.youtube.com/watch?v=-ZRUZzZPGto
**5. *Deepfake*.** EZRyderX47. (14 de febrero de 2020). Robert Downey Jr and Tom Holland in Back to the future - This is heavy! [ deepfake ] [Archivo de Vídeo]. Youtube. https://www.youtube.com/watch?v=8OJnkJqkyio&t=3s
**6. Real.** Zemeckis R. (Director). (1985). Volver al futuro [Película].

**Para entrevistas o más información, contáctanos en:**
**prensa@tuidentidad.com**

**tuidentidad.com**

tuidentidad