Cuando el juego deja de ser un juego: lo que le estás diciendo a la IA sobre ti sin darte cuenta

“Create a caricature of me and my job based on everything you know about me”

En los últimos días se ha viralizado una invitación aparentemente inocente:

“Everyone play along 🤣😅!! Go to ChatGPT and use this prompt…”

La propuesta es sencilla, incluso divertida. Pedirle a una inteligencia artificial que cree una caricatura tuya y de tu trabajo basándose en todo lo que “sabe” de ti. Una mezcla de curiosidad, humor y ego digital. ¿Qué puede salir mal?

La respuesta corta: **mucho más de lo que parece**.

La trampa perfecta: cuando algo es divertido, bajamos la guardia

Este tipo de tendencias funcionan precisamente porque no parecen peligrosas. No hay enlaces raros, no hay peticiones explícitas de datos, no hay amenazas. Solo una pregunta creativa que apela a la curiosidad personal.

Pero hay una pregunta mucho más importante que casi nadie se hace antes de participar:

👉 **¿Qué crees que "sabe" realmente una IA sobre ti?**

Y, aún más relevante:

👉 **¿de dónde crees que sale esa información?**

La falsa sensación de intimidad con la IA

Cuando una IA responde con detalles que encajan —tu profesión, tu tono, tus intereses— se produce un efecto psicológico muy claro: **sentimos que nos "conoce"**. Que hay una relación. Que es casi personal.

Pero no es conocimiento íntimo. Es **correlación de datos**.

La IA no te conoce como persona, pero:

- Analiza patrones públicos
- Interpreta cómo te describes
- Cruza información que tú mismo has expuesto
- Rellena huecos con probabilidad estadística

Y muchas veces acierta lo suficiente como para generar confianza.

El verdadero problema no es la caricatura

Que una IA genere una imagen simpática sobre ti no es el riesgo principal. El problema es **el mensaje cultural que normaliza este tipo de dinámicas**:

“Usa todo lo que sabes de mí.”

Esa frase, aplicada al contexto adecuado, es exactamente lo que necesitan:

- Los atacantes que usan IA para estafas personalizadas
- Los sistemas que entrenan modelos con comportamiento humano
- Las campañas de ingeniería social basadas en identidad

Hoy es una caricatura.

Mañana puede ser un mensaje, una llamada o un vídeo que **parezca escrito por ti o para ti**.

De la broma al perfil digital explotable

Cada vez que participamos en este tipo de juegos estamos reforzando una idea peligrosa:

que nuestra identidad digital es **material creativo**, no **superficie de ataque**.

Pero la realidad es que:

- Tu profesión define cómo pueden atacarte
- Tu tono define cómo escribirte
- Tu exposición define qué partes de ti pueden imitar
- Tu huella digital define qué es creíble y qué no

La IA no inventa desde cero. **Imita lo que ya existe**.

Y lo que existe… lo has publicado tú.

El paralelismo incómodo: así funcionan los ataques modernos

Los ciberataques actuales basados en IA funcionan exactamente igual que este "juego":

1. Recopilan información pública
2. Construyen un perfil creíble
3. Generan contenido personalizado
4. Eliminan señales clásicas de alerta
5. Atacan cuando menos lo esperas

La única diferencia es la intención.

Por eso este tipo de tendencias son tan valiosas para concienciar: **muestran el problema sin necesidad de explicarlo técnicamente**.

Cuando el humor tapa el riesgo

El emoji de risa 😬 no está ahí por casualidad. Representa esa incomodidad ligera que sentimos, pero que decidimos ignorar porque “no pasa nada”.

El problema es que en ciberseguridad:

- Lo cómodo suele ser inseguro
- Lo viral suele ser explotable
- Lo divertido suele ser reutilizable

Y la IA no distingue entre juego y ataque. Solo procesa datos.

La pregunta clave que deberíamos hacernos

No es:

“¿Qué caricatura haría la IA de mí?”

La pregunta real es:

“¿Qué podría hacer alguien malintencionado con esta misma información?”

Ahí cambia todo.

No se trata de dejar de usar IA (ni redes sociales)

Este artículo no va de demonizar la inteligencia artificial ni de vivir con miedo. Va de **usar la tecnología con criterio**.

La IA es una herramienta brutalmente potente.

Pero cuanto más humana parece, **más responsabilidad exige por nuestra parte**.

La conciencia digital hoy ya no va de contraseñas.

Va de **identidad, contexto y exposición**.

Isaac Ruiz Romero.