

■ IA OFENSIVA · ALERTA 2026

Cómo usan ChatGPT para atacarte

01 — IA AL SERVICIO DEL ENGAÑO

Los atacantes ya usan ChatGPT y otros modelos de lenguaje para hacer sus ataques más convincentes, masivos y difíciles de detectar. Lo que antes tardaba horas ahora tarda segundos.

■ Phishing sin errores

Antes los correos fraudulentos se detectaban por mala redacción. Ahora la IA los escribe perfectamente en cualquier idioma.

■ Personalización masiva

Con datos de redes sociales, la IA genera mensajes personalizados con tu nombre, empresa y contexto real.

■ Scripts de vishing

Guiones completos para llamadas fraudulentas, adaptados al perfil de la víctima en tiempo real.

■ Código malicioso

Modelos sin filtros (jailbreak) generan código para exploits y malware funcional.

02 — ATAQUES REALES CON IA EN MÉXICO 2026

Estos no son escenarios futuros — están ocurriendo ahora mismo.

■ Correos de SAT falsos perfectos

IA genera notificaciones de auditoría del SAT sin errores de ortografía, con formato oficial.

■ WhatsApp de 'tu banco'

Mensajes personalizados con tu nombre y los últimos 4 dígitos de tu tarjeta (datos filtrados + IA).

■ Facturas CFDI falsas

IA genera facturas con XML válido para fraudes a empresas.

■ Perfiles falsos de reclutadores

Ofertas de trabajo convincentes para robar datos personales o instalar malware.

03 — CÓMO IDENTIFICAR CONTENIDO GENERADO CON IA

■ Urgencia artificial

Mensajes que crean presión extrema de tiempo son señal de manipulación, con o sin IA.

■ Verifica por otro canal

Si recibes un mensaje urgente de tu banco o jefe, llama directo por un número conocido — no respondas al mismo mensaje.

■ Desconfía de lo perfecto

Un correo demasiado bien escrito de una fuente inesperada puede ser IA. La perfección en contexto sospechoso es señal de alerta.

■ Protocolo de verificación

Establece en tu empresa una palabra clave o proceso de doble confirmación para transferencias y accesos urgentes.

¿Tu equipo sabe identificar ataques con IA?

Capacitación empresarial — wa.me/527771631152

// REGLA DE ORO

La ciberseguridad no es tecnología — es conocimiento. Comparte esta infografía.