2025

CLONAN VOCES CON IA PARA ESTAFAR: QUÉ ESTÁ PASANDO Y CÓMO PROTEGERSE

Confederación Colombiana de Consumidores
Informa, Educa y Protege

En las últimas semanas ha surgido un nuevo tipo de fraude que utiliza inteligencia artificial para suplantar la voz de familiares, amigos o incluso empleados de entidades financieras. Aunque el fenómeno se ha reportado en varios países, recientemente las autoridades colombianas han alertado sobre un incremento de este método en el país.

¿CÓMO FUNCIONA LA ESTAFA?

Los delincuentes emplean herramientas de IA para recrear la voz de una persona conocida por la víctima. Con ese audio falso, plantean situaciones de urgencia, por ejemplo, un supuesto problema financiero o una emergencia familiar para presionar a la persona y conseguir datos sensibles, contraseñas o transferencias de dinero. En algunas variantes más sofisticadas, combinan la imitación de voz con la suplantación por videollamada (deepfake) o con el secuestro de llamadas reales para que la comunicación parezca totalmente creíble.

SEÑALES DE RIESGO

Es importante desconfiar de comunicaciones inesperadas que exijan información confidencial o transferencias inmediatas. Algunos indicadores de alerta son:

- Peticiones urgentes de claves, códigos o datos bancarios.
- Llamadas o mensajes fuera de lo habitual que generan presión emocional.
- Solicitudes para descargar enlaces o aplicaciones que permitan el acceso remoto.

En el caso de mensajes y llamadas que se hacen pasar por plataformas como WhatsApp, también deben encenderse las alarmas si el mensaje contiene errores ortográficos o solicita abrir enlaces externos, compartir contraseñas o hacer pagos por el uso del servicio.

RECOMENDACIONES PRÁCTICAS

Para reducir el riesgo de ser víctima de estas estafas, las autoridades y expertos recomiendan:

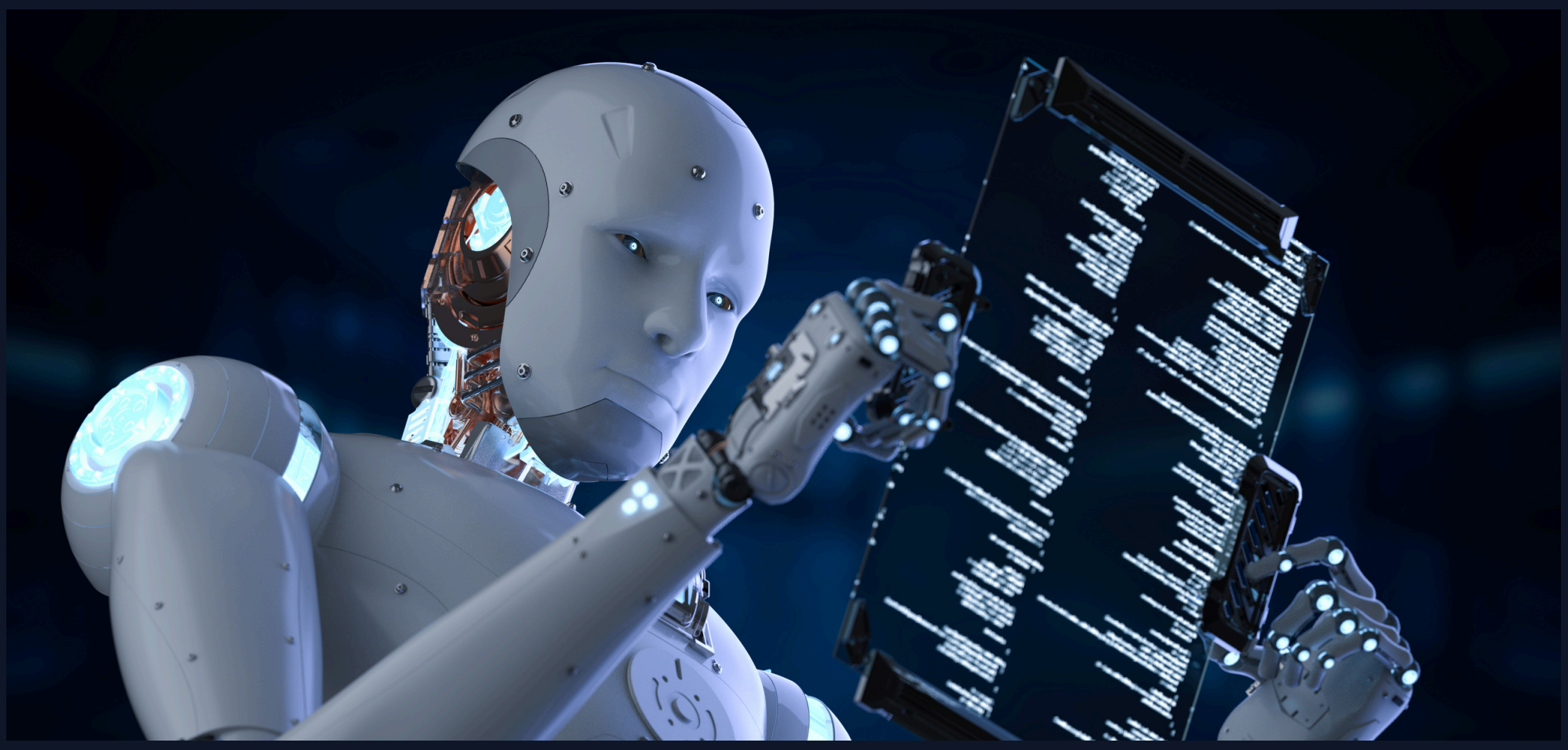
- No facilitar nunca claves ni datos bancarios por teléfono o mensajería instantánea.
- Colgar y comunicarse por otro canal (por ejemplo, marcar directamente el número conocido de la persona supuestamente contactante) para verificar la solicitud.
- Activar la verificación en dos pasos (2FA) en correo, redes sociales y servicios bancarios.
- Mantener contraseñas robustas y renovarlas periódicamente.
- Evitar compartir en redes sociales información, audios o videos íntimos o excesivamente personales que puedan utilizarse para recrear voces o rostros.
- Reportar y bloquear números o cuentas sospechosas desde la propia aplicación.

Confederación Colombiana de Consumidores
Informa, Educa y Protege

ccconsumidores.org.co @consumidoresccc

Confederación Colombiana de Consumidores
Informa, Educa y Protege

EL RIESGO DEL "DEEPFAKE" Y EL SECUESTRO DE LLAMADAS



Los especialistas advierten que la disponibilidad de herramientas de IA ha facilitado la creación de deepfakes —tanto de voz como de imagen— con un nivel de realismo cada vez mayor. Además, existen técnicas que permiten interceptar llamadas y simular que una conversación proviene de un contacto legítimo. Por eso, la exposición pública de audios, fotos y otros datos personales aumenta la probabilidad de que delincuentes puedan recrear la identidad digital de alguien.

CASO RECIENTE EN BOGOTÁ: SUPLANTACIÓN POR SUPUESTOS FUNCIONARIOS DE WHATSAPP

En Bogotá se han detectado intentos de fraude donde los atacantes se hacen pasar por empleados de WhatsApp para "verificar" cuentas o "activar funciones", con la intención de obtener acceso o información financiera. Señales que indican que se trata de un fraude incluyen solicitudes de abrir enlaces sospechosos, pedir datos personales o pedir reenviar mensajes o realizar pagos por servicios que la plataforma no cobra.

WhatsApp recuerda que no solicita dinero por el uso del servicio y recomienda comprobar la autenticidad de un remitente observando si hay contactos en común, si el número pertenece a otro país o si ya está registrado en su libreta de direcciones.

Qué hacer si recibe un intento de estafa:

Si sospecha de una llamada o mensaje:

1. No entregue información ni realice transferencias.
2. Verifique la identidad del remitente por otros medios.
3. Bloquee y reporte el número o la cuenta.
4. Denuncie el intento ante las autoridades competentes o los canales de atención oficial de su ciudad.

En Bogotá, por ejemplo, la Secretaría Distrital de Seguridad insta a reportar cualquier intento de fraude al CAI Virtual, disponible las 24 horas por WhatsApp.