EL MERCURIO

Fecha: 31/12/2024 Audiencia: 320.543 Sección: CIENCIA Y TECNOLOGIA
Vpe: $10.338.790 Tirada: 126.654 Frecuencia: SEMANAL
Vpe pág: $20.570.976 Difusión: 126.654
Vpe portada: $20.570.976 Ocupación: 50,26%

Las personas, en su vida diaria, serán posibles víctimas:

Engaños con IA y el robo de datos a relojes están entre los peligros digitales de 2025

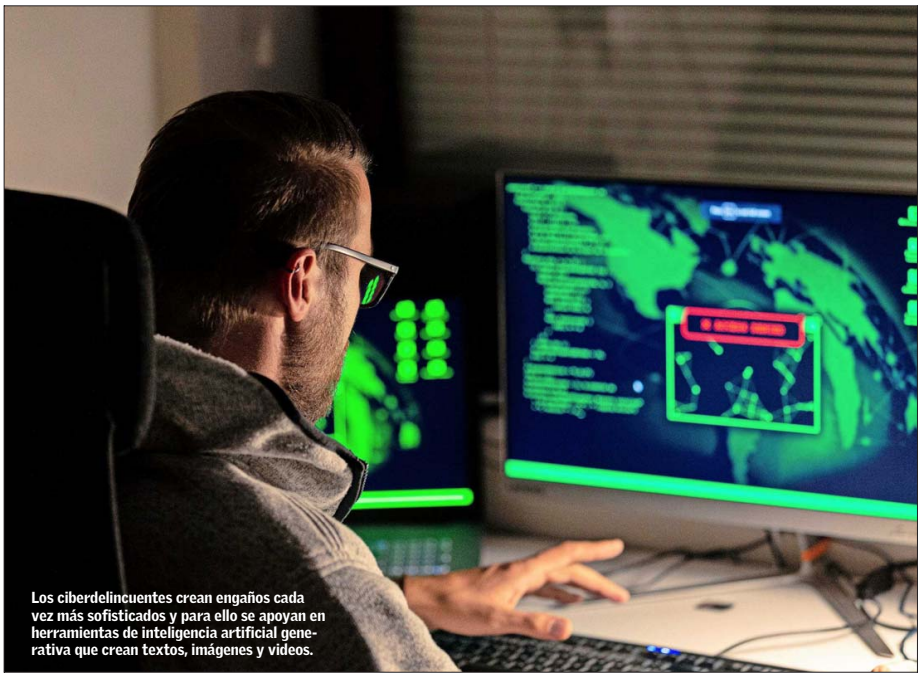
ALEXIS IBARRA O.

Algunas amenazas aparecieron este año, pero se consolidarán el siguiente, dicen diversos expertos. La clonación de la voz para timos telefónicos, hasta supuestos famosos promoviendo ofertas falsas son algunos temas a los que habrá que estar alertas.

"El 2025 se vaticina como un año de amenazas más complejas de las que hemos estado viendo, precisamente por la evolución de estas y la incorporación masiva de la inteligencia artificial", dice Walter Montenegro, gerente regional de ciberseguridad en Cisco.

La IA rápidamente fue adoptada por cibercriminales para cometer delitos cada vez más sofisticados. Su uso, de distintas formas, marca una de las principales tendencias este 2025.

Preguntamos a especialistas en ciberseguridad sobre cuáles serían las principales amenazas y peligros digitales a los que nos veremos expuestos en 2025 y estas fueron sus predicciones:



Los ciberdelincuentes crean engaños cada vez más sofisticados y para ello se apoyan en herramientas de inteligencia artificial generativa que crean textos, imágenes y videos.

FORTINET

Videos falsos de famosos

Una tendencia que comenzó en 2024 y que se acrecentará en 2025 será el uso de videos de personas famosas (artistas, deportistas o políticos) ofreciendo o divulgando algo y que se distribuyen en redes sociales. "Pero ese video es falso, fue creado con herramientas de la IA para engañar a la gente", dice Fabio Assolini, director de Análisis e Investigación de Kaspersky para América Latina.

El especialista dice que es común encontrar en Instagram supuestos videos de Messi promocionando una criptomoneda que puede generar muchas ganancias o de Shakira anunciando una promoción de perfumes gratis. "Todo es falso, los usuarios deben estar bien informados para no caer en trampas", aclara.

"Las falsificaciones complejas basadas en IA serán cada vez más convincentes", complementa Cristian Vásquez, *country manager* de Check Point Software en Chile.

Phishing perfeccionado

La IA se usará ampliamente para cometer ciberdelitos. El tradicional *phishing*, en que se engaña mediante un correo falso, que usa un gancho para atraer a usuarios incautos, ahora se sofistica con la ayuda de la IA.

"La IA puede analizar el lenguaje de los correos para crear mensajes que imitan perfectamente un estilo", dice Mario Micucci, investigador de seguridad informática de ESET Latinoamérica.

Clonación de voz

Relacionado con lo anterior está el uso del *Deepfake – Deepvoice*, "técnicas que clonan el rostro, timbre y forma de hablar de una persona casi a la perfección", dice Francisco Fernández, gerente general de Avantic Chile. Y agrega: "Esta clase de fraudes se asocia con llamadas a familiares, amigos, colegas y jefaturas, solicitando en forma urgente dinero o alguna aprobación de transacción de dinero".

El engaño "también usará herramientas como el *lipsync* y los *deepfakes*, capaces de crear videos y audios extremadamente realistas que simulan voces y gestos de personas", añade Miguel Cisterna, gerente de Seguridad e Inteligencia de Movistar Chile.

El peligro de contar todo en las redes

"Los ciberdelincuentes se centrarán cada vez más en las plataformas de redes sociales al usar datos personales para estafas y suplantaciones específicas", dice Vásquez.

"En 2025, la práctica habitual del *sharenting* —padres que comparten en exceso información sobre sus hijos en línea— hará que las preguntas de seguridad basadas en conocimientos tradicionales, como '¿Cuál es el nombre de tu primera mascota?, sean completamente inútiles", dice. Con personas divulgando fácilmente estos detalles personales en redes sociales, los estafadores tendrán vía libre para explotar esta información y burlar medidas de seguridad, comprometiendo cuentas", señala Daniel Molina, vicepresidente de iProov para América Latina.

Acechan los *stealers*

"Los *stealers* son una familia de código malicioso programados para robar cualquier cosa (desde datos hasta *passwords*) y creemos que será de las amenazas más importantes para este 2025, ya que la forma en que se distribuye afecta directamente al usuario final", dice Assolini.

Se les suele encontrar como enlaces en canales de YouTube, como activadores, por ejemplo, de un WhatsApp Gold o de un *crack* (pequeño programa para activar una aplicación pirata) de algún *software* comercial popular. "Una vez instalados roban todo: contraseñas, números de tarjetas, cualquier dato. Al final, los cibercriminales van a crear bases de datos y venderlas en la *Deep Web*".

Relojes bajo ataque

Los *wearables*, como los relojes inteligentes, también serán blancos de ataque, afirma Walter Montenegro. "Manejan la ubicación, movimientos e información sobre la salud de los usuarios. Al vulnerarlos, los atacantes obtienen el conocimiento necesario para poder realizar un ataque mucho más dirigido, robar información personal que está almacenada y hacer mal uso de ella (como las ubicaciones en las que se estuvo en el día). Hay que tener especial precaución y conciencia, ya que son dispositivos que usamos a diario", explica el especialista.

Rapto de equipos con foco al consumidor

El *ransomware* (secuestro del computador a cambio de dinero) ya no está limitado a empresas. "En 2025, se prevé que los atacantes cifren (encripten) dispositivos personales, exigiendo pagos en criptomonedas a cambio de liberar fotos, documentos y otros datos personales críticos. Casos recientes han mostrado un aumento en ataques a pequeños dispositivos NAS (para almacenar datos) personales", dice Mario Micucci.

Cómo protegerse

"Estas amenazas hacen imprescindible que los usuarios extremen precauciones", dice Miguel Cisterna. Entre ellas menciona verificar siempre la fuente de cualquier solicitud de datos, evitar acceder a enlaces sospechosos y utilizar medidas de seguridad adicionales, como la autentificación en dos pasos, para proteger la información personal. "Hay que sospechar de la veracidad de mensajes que parecen demasiado buenos para ser reales: ¿Es lógico que esta promoción me haya llegado solo a mí? ¿Es razonable el valor ofrecido? Antes de entregar cualquier dato personal o financiero, realizar un doble chequeo, consultar fuentes confiables y asegurarse de que el remitente sea legítimo", agrega el especialista de Movistar. Mario Micucci, en tanto, recomienda lo que él llama "higiene de contraseñas": no usar siempre las mismas y cambiarlas constantemente.