LITORALPRESS

Fecha: 15-02-2026
Medio: La Estrella de Chiloé
Supl. : La Estrella de Chiloé
Tipo: Noticia general
Título: Estafas con IA: tenga el software actualizado y no les siga el "chamullo"

Pág. : 13
Cm2: 423,6

Tiraje: 2.800
Lectoría: 8.400
Favorabilidad: No Definida

Estafas con IA: tenga el *software* actualizado y no les siga el "chamullo"

Los sistemas pueden imitar su voz y grabar mensajes de "emergencia", así como enviar correos con enlaces falsos.

V.B.V.

El teléfono suena y al contestar hay solo silencio del otro lado: esta podría ser una estafa realizada con inteligencia artificial (IA), debido a que los maleantes buscan provocar que la persona hable para tomar los tonos de su voz y con ellos construir mensajes para solicitar dinero a sus cercanos. En vista de lo real que puede parecer este método, sumado a otros que incluyen imágenes, el académico de la Universidad Andrés Bello (UNAB), Edgardo Fuentes, entregó una serie de consejos para evitar engaños.

El sostenido aumento de estos fraudes "son una invitación a actuar con inteligencia y calma", señaló el director de Ingeniería en Ciberseguridad de la casa de estudios, porque "la prevención no requiere conocimientos técnicos avanzados, sino atención y sentido común".

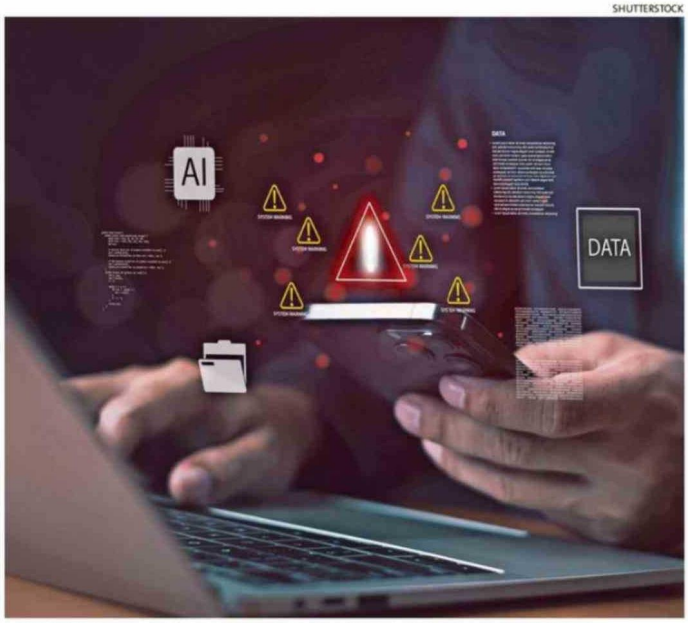
Todo comienza por verificar la fuente de la información, indicó el docente, por lo que aconsejó antes de responder a un correo o hacer clic en un enlace, revisar la dirección del remitente y asegurarse de que la URL (página web) sea legítima. "Si algo parece sospechoso, lo mejor es confirmar por otro canal, como llamar al número oficial de la empresa".

Otra estrategia para evitar robos mediante la aplicación de nuevas tecnologías es reforzar las contraseñas, que no sean predecibles, como la fecha de cumpleaños, sino que únicas, largas y complejas, junto con siempre activar la opción de autenticación en dos pasos (2FA).

Este sistema, además de solicitar la contraseña, pide verificar identidad mediante un código enviado al teléfono o correo electrónico personal. "Esta simple medida bloquea la mayoría de los intentos de acceso no autorizado", afirmó Fuentes.

"Mantener los dispositivos actualizados es otro escudo poderoso", subrayó el académico, porque estas nuevas versiones del *software* corrigen las vulnerabilidades "que los delincuentes aprovechan, y un buen antivirus añade una capa extra de protección".

SHUTTERSTOCK



ACADÉMICO RECOMENDÓ NO USAR REDES DE INTERNET PÚBLICAS PARA REALIZAR PAGOS.

Otra medida clave es desconfiar de los mensajes que se presentan como una urgencia, del tipo "su hija tuvo un accidente, soy su amigo y necesito plata para pagar la clínica, porque está inconsciente...", guión que conlleva una presión emocional.

"Si recibe una llamada que suena demasiado real para ser falsa, recuerde que la IA puede imitar voces", dijo Fuentes, razón por la que "siempre verifique por otro medio antes de actuar", por ejemplo, llame a la mejor amiga de su hija.

> "Si algo parece sospechoso, lo mejor es confirmar por otro canal, como llamar a la empresa".
>
> **Edgardo Fuentes**
> ingeniero en informática

Las compras por internet también pueden derivar en fraudes. Para evitarlo, el docente señaló que se deben realizar en sitios oficiales y conocidos, nunca por enlaces que llegan al correo o redes sociales.

"Antes de pagar, revise que la dirección web comience con 'https://' y que aparezca el candado de seguridad. Evite usar redes WiFi públicas para realizar pagos y, si es posible, utilice métodos seguros como tarjetas virtuales o plataformas reconocidas" de transferencia de dinero, como PayPal o MercadoPago, guardando siempre el comprobante.