LITORALPRESS

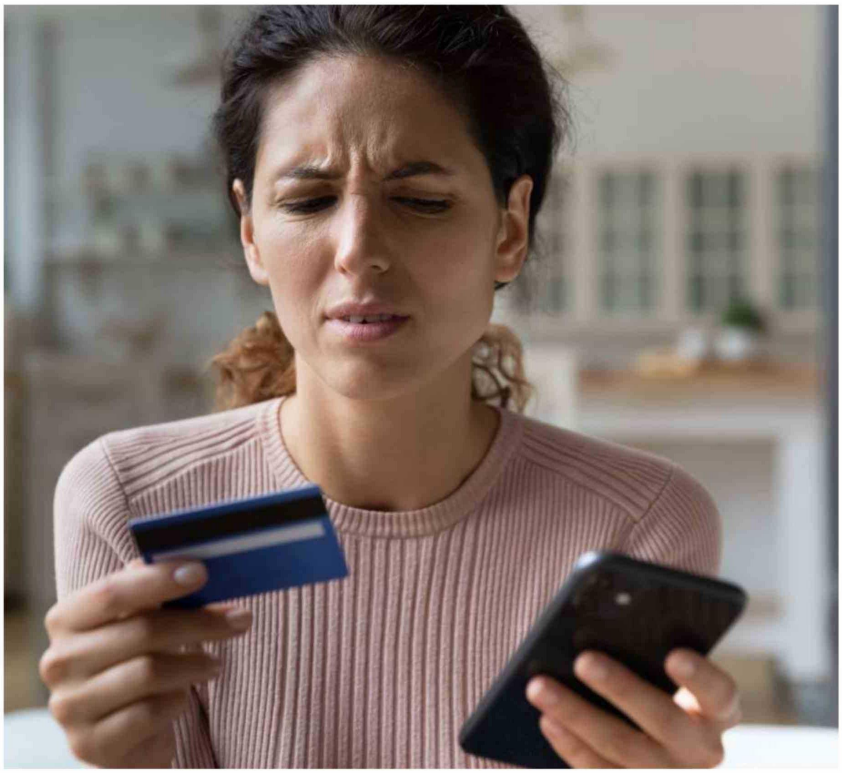
Fecha: 12-02-2026
Medio: El Divisadero
Supl. : El Divisadero
Tipo: Noticia general
Título: Experto entrega claves para evitar estafas impulsadas por Inteligencia Artificial ante el aumento de ciberataques

Pág. : 14
Cm2: 609,8

Tiraje: 2.600
Lectoría: 7.800
Favorabilidad: No Definida

Experto entrega claves para evitar estafas impulsadas por Inteligencia Artificial ante el aumento de ciberataques

Frente al incremento del 60% en ataques de phishing potenciados por IA durante el último año, Edgardo Fuentes, director de Ingeniería en Ciberseguridad de la Universidad Andrés Bello, ofrece recomendaciones prácticas para que los usuarios de la región protejan su información y eviten ser víctimas de fraudes digitales.



La inteligencia artificial ha revolucionado la forma en que interactuamos con la tecnología, pero esta herramienta también ha sido aprovechada por ciberdelincuentes para sofisticar sus métodos de engaño. Según reportes recientes, los fraudes en línea han crecido significativamente; un informe de Zscaler reveló que los ataques de phishing impulsados por IA aumentaron casi un 60% en 2023, incluyendo la aparición de deepfakes de voz y vishing. A esto se suma que, tras el lanzamiento de ChatGPT, los ataques de phishing, smishing y vishing crecieron un 1.265%, caracterizándose por mensajes mucho más personalizados y difíciles de detectar.

Ante este escenario, Edgardo Fuentes, director de Ingeniería en Ciberseguridad de la Universidad Andrés Bello, llama a la calma y a la acción informada. "Estas cifras pueden parecer inquietantes, pero no son motivo de pánico. Al contrario, son una invitación a actuar con inteligencia y calma", asegura el académico, quien enfatiza que la mayoría de los fraudes se pueden evitar mediante hábitos digitales responsables. Según el experto, "la prevención no requiere conocimientos técnicos avanzados, sino atención y sentido común".

Para protegerse, el primer paso es siempre verificar la fuente de la información. Antes de hacer clic en un enlace o responder un correo, es fundamental revisar la dirección del remitente y la legitimidad de la URL. Fuentes explica que "si algo parece sospechoso, lo mejor es confirmar por otro canal, como llamar directamente al número oficial de la empresa". A esto se debe sumar el fortalecimiento de las claves de acceso, optando por contraseñas únicas, largas y complejas, además de activar la autenticación en dos pasos (2FA). El especialista afirma que "esta simple medida bloquea la mayoría de los intentos de acceso no autorizado".

La seguridad de los equipos también juega un rol crucial. "Mantener los dispositivos actualizados es otro escudo poderoso", subraya el profesor de la UNAB, explicando que dichas actualizaciones corrigen vulnerabilidades que los delincuentes suelen aprovechar. Asimismo, advierte sobre la necesidad de desconfiar de mensajes que generan presión emocional o urgencia, especialmente ante la capacidad de la IA para clonar voces. "Si recibes una llamada que suena demasiado real para ser falsa, recuerda que la IA puede imitar voces; siempre verifica por otro medio antes de actuar", recomienda.

En el ámbito de las compras por internet, donde también abundan los riesgos, el experto sugiere utilizar siempre sitios oficiales y evitar enlaces recibidos por redes sociales. "Antes de pagar, revisa que la dirección web comience con "https://" y que aparezca el candado de seguridad. Evita usar redes WiFi públicas para realizar pagos y, si es posible, utiliza métodos seguros como tarjetas virtuales o plataformas reconocidas (PayPal, MercadoPago)", detalla Fuentes.

Finalmente, el llamado es a confiar en la capacidad de prevención y a educar al entorno cercano. "La realidad es que los fraudes existen y evolucionan, pero también lo hace nuestra capacidad para prevenirlos. Saber que muchas personas ya confían en su habilidad para detectar estafas inspira esperanza; y esa confianza se fortalece con educación y práctica. Compartir consejos con familiares y amigos multiplica la protección colectiva", declara el experto. Fuentes concluye con una reflexión sobre el uso de la tecnología: "la tranquilidad en la era digital no se logra evitando la tecnología, sino usándola con criterio. La inteligencia artificial puede potenciar el fraude, pero también puede ayudarte a protegerte. Adoptar hábitos simples como verificar, proteger y actualizar te permite disfrutar de los beneficios de la conectividad sin miedo. La prevención está en nuestras manos, y con ella, la confianza para navegar seguros".