LITORALPRESS

Fecha: 02-06-2026
Medio: El Heraldo
Supl. : El Heraldo
Tipo: Columnas de Opinión
Título: Columnas de Opinión: Cyber, fraudes e IA: la oferta perfecta puede ser una trampa

Pág. : 4
Cm2: 444,1
VPE: $ 888.149

Tiraje: 3.000
Lectoría: 6.000
Favorabilidad: No Definida

Cyber, fraudes e IA: la oferta perfecta puede ser una trampa

Si queremos entender por qué el fraude digital se volvió más sofisticado, basta hacer una prueba controlada como pedirle a una herramienta de inteligencia artificial que genere una página web similar a una tienda online, con una oferta atractiva y un botón de compra. En segundos, la herramienta puede producir una maqueta convincente. Ese ejercicio, usado con fines educativos, muestra que clonar la apariencia de un sitio ya no es una tarea reservada a expertos.

Por eso, el Cyber requiere ser cuidadosos, ya no está solo el riesgo en la existencia de páginas falsas, sino en que esas páginas pueden parecer cada vez más legítimas. Se trata de un evento masivo de compra online, donde convergen urgencia, alto volumen de transacciones y múltiples canales. Así los ciberdelincuentes encuentran condiciones favorables para operar. El usuario recibe correos, mensajes, notificaciones bancarias, avisos en redes sociales y alertas de despacho. En ese escenario, la capacidad de verificar disminuye y aumenta la probabilidad de actuar por impulso.

Durante años, una recomendación frecuente para identificar estafas fue observar errores ortográficos, diseños poco profesionales o mensajes incoherentes. Hoy esa señal pierde efectividad. Las herramientas de inteligencia artificial generativa permiten producir textos consistentes, anuncios creíbles, respuestas automáticas y sitios fraudulentos similares a los originales. Desde una perspectiva técnica, la IA no crea una nueva categoría de delito, pero sí modifica su escala, velocidad y verosimilitud.

Esto obliga a comprender la ciberseguridad desde una mirada más amplia. Ya no basta con recomendar que no se haga clic en enlaces sospechosos, porque aquello que antes parecía sospechoso hoy puede estar bien redactado, usar una identidad visual convincente y estar contextualizado con precisión. Un correo falso puede simular a una tienda reconocida; un mensaje de WhatsApp puede aparentar provenir de una empresa de despacho; un aviso en redes sociales puede redirigir a una página casi idéntica a una marca legítima. La IA permite generar y distribuir estos contenidos con costos menores.

Aparecen también los agentes de inteligencia artificial, que son sistemas capaces de ejecutar tareas con cierto grado de autonomía. Utilizados de forma responsable, podrían apoyar a consumidores y empresas revisando la confiabilidad de una URL, detectando inconsistencias o advirtiendo patrones de riesgo. Sin embargo, la misma lógica puede ser explotada con fines maliciosos para automatizar phishing, personalizar mensajes, simular atención al cliente o guiar a una persona hasta entregar datos personales o códigos bancarios.

La paradoja es evidente. La misma tecnología que puede ayudarnos a comprar mejor también puede utilizarse para engañarnos con mayor precisión. El debate no debiera presentar la inteligencia artificial como una amenaza en sí misma, sino comprender que amplifica las capacidades de quien la utiliza. En manos responsables, puede mejorar procesos y seguridad. En manos de bandas dedicadas al fraude digital, puede aumentar la escala, rapidez y credibilidad del engaño.

Nicolás Caselli Benavente
Director Ingeniería Civil Informática
Universidad Andrés Bello

Los usuarios enfrentan una brecha entre uso y comprensión. Muchas personas utilizan plataformas digitales a diario, pero no necesariamente cuentan con hábitos sistemáticos de verificación. Comprar bajo presión, confiar en el primer enlace recibido, reutilizar contraseñas o entregar códigos de seguridad siguen siendo prácticas riesgosas.

Las recomendaciones siguen siendo simples, pero hoy adquieren mayor importancia: ingresar a tiendas desde sitios oficiales, revisar la dirección web, desconfiar de ofertas desproporcionadas, evitar enlaces recibidos por SMS o WhatsApp, activar doble autenticación y nunca entregar claves ni códigos de verificación. En tiempos de IA, la prevención no puede depender solo de la intuición del usuario; también requiere sistemas de alerta, plataformas responsables y educación digital continua.

Desde la carrera de Ingeniería Civil Informática de la Universidad Andrés Bello, sede Concepción, observamos este fenómeno como un desafío técnico, formativo y social. Por ello, mantenemos un trabajo constante de vinculación con la comunidad mediante charlas, talleres e instancias de divulgación orientadas a promover el uso responsable de la inteligencia artificial y una cultura digital más crítica. Al mismo tiempo, formamos profesionales capaces de desarrollar soluciones tecnológicas y comprender sus impactos éticos, sociales y de seguridad.

El Cyber no debe entenderse únicamente como una fiesta de descuentos. También es una prueba de madurez digital. En un entorno donde las ofertas pueden ser reales, falsas o generadas mediante sistemas automatizados, la mejor compra no será necesariamente la más rápida, sino la más informada. Porque en tiempos de inteligencia artificial, la oferta perfecta también puede ser una trampa técnicamente bien diseñada.