LUN

Fecha: 05/08/2025 Audiencia: 271.020 Sección: ACTUALIDAD
Vpe: $2.961.284 Tirada: 91.144 Frecuencia: DIARIO
Vpe pág: $4.399.200 Difusión: 91.144
Vpe portada: $4.399.200 Ocupación: 67,31%

Expertos en ciberseguridad entregan claves para identificar páginas fraudulentas

Zapatero generado con IA estafa a compradores con descuentos falsos

"Las páginas 'Velto Santiago' y 'Novo Santiago' operan con características claras de estafa", dice subcomisario de la PDI.

IGNACIO MOLINA

"Mis amigos, estoy aquí haciendo mi último par de zapatos. Me jubilo, así que todo está al 70% de descuento".

La frase aparece en un video que circula por redes sociales. Un hombre mayor, de bigote y delantal, habla a cámara desde un supuesto taller artesanal. Tiene voz suave, una historia de retiro y una promesa: zapatos finos a precio de liquidación. No es cierto. El rostro, la voz y el guion fueron generados con inteligencia artificial. El personaje no existe. La tienda, tampoco.

"La Brigada del Cibercrimen de la PDI ha identificado que existen páginas fraudulentas que utilizan los nombres de 'Velto Santiago' y 'Novo Santiago', operando con características claras de estafa", dice el subcomisario Julio Vargas. "Venden productos que no existen o que son de muy mala calidad, sin entregar lo prometido".

El artificio no se agota en un solo rostro. En sus versiones más sentimentales, las tiendas incluyen una despedida firmada por "Andrés y María", supuestos dueños que escriben en el sitio web: "Aunque cerraremos nuestras puertas, queremos agradecer de corazón a cada uno de ustedes por el amor y el apoyo que nos han brindado durante estos 28 maravillosos años".

Los productos ofrecidos son igual de cuidadosamente ficticios: botas Chelsea de cuero, rebajadas de $155.000 a $69.990. El método es simple: capturar atención con estética profesional y construir confianza con una historia emocional.

Pareja de artesanos ficticios usados en la estafa digital de Velto Chile.

"Usan perfiles falsos junto a promociones engañosas como liquidación por cierre", señala el subcomisario Vargas.

La investigación parte con reclamos en redes sociales y ante el Sernac. A medida que se multiplican los casos, se repite el patrón: pagos adelantados, productos que nunca llegan o que llegan sin relación con lo ofrecido.

Sebastián Rebolledo -ingeniero en redes, experto en ciberseguridad y director de países de la 8.8 Computer Security Conference- describe el proceso. "Estas estafas funcionan como una operación digital altamente coordinada que combina ingeniería social, inteligencia artificial y suplantación digital", explica.

Los estafadores -detalla Rebolledo- montan tiendas online falsas que imitan plataformas reales como Temu o Shein. "Se apoyan en herramientas de inteligencia artificial generativa para crear imágenes hiperrealistas de productos, rostros y personajes ficticios -como el supuesto maestro zapatero- que humanizan la historia y generan empatía con el público".

Luego, compran publicidad segmentada y amplifican la campaña en redes. "Los pagos son canalizados a través de pasarelas que muchas veces no permiten identificar fácilmente al destinatario final, dificultando el seguimiento por parte de las autoridades".

Nicolás Silva, máster en tecnologías de la información y director de tecnología de Asimov Consultores, explica que hoy no se necesita más de una jornada para montar una operación de este tipo. El sitio -explica- se construye con plantillas prefabricadas, se cargan imágenes y textos artificiales, y se lanza la campaña. Cuando la tienda alcanza el volumen deseado de pagos, desaparece. "Una vez que juntan suficiente plata, bajan la página", dice Silva.

Para no caer

¿Cómo detectar una tienda falsa? Rebolledo entrega señales clave: "Imágenes excesivamente perfectas con fallas anatómicas -tres brazos, dedos extra-. Historias demasiado emocionales, como jubilaciones repentinas o descuentos absurdos. Errores gramaticales. Dominios recién creados. Falta de razón social, RUT o medios de pago protegidos como Webpay o PayPal".

Silva añade síntomas comunes: "Tiendas que solo existen en redes sociales, con comentarios de supuestos compradores que parecen bots. Sin dirección física ni teléfono. Solo aceptan pagos por transferencia o tarjeta prepago". Frente a cualquiera de esas señales, la recomendación es tajante: no confiar. No comprar. Denunciar.