

Ojo: Diciembre, mes preferido de los ciberdelincuentes

Por el Staff de El Inversionista

En diciembre todos los consumidores están expuestos a ser víctimas de un ciberataque. El año pasado, los fraudes por supuestas entregas de paquetes aumentaron en más de 200 por ciento y casi la mitad de las personas que cayeron perdieron más de 10 mil pesos, de acuerdo con información de Eset, firma especializada en ciberseguridad.

El incremento de las compras en diciembre (regalos, promociones y viajes, entre otros) hace de este mes el de mayor cantidad de fraudes en línea, según la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef).

Precisa que los delincuentes digitales publican en Internet cientos de sitios de páginas falsas, casi imposibles de detectar a simple vista, cuya finalidad es robar las claves bancarias y los recursos de las personas, por lo que la temporada de fiestas se puede convertir en una pesadilla.

“Los ciberdelincuentes saben que en diciembre la gente recibe aguinaldo, compra más en línea y revisa menos cuidadosamente los mensajes. La mezcla de todas las emociones, urgencia y sobrecarga de información es perfecta para los ataques digitales. Por eso vemos picos de fraudes en diciembre”, dijo David González, investigador de seguridad informática de Eset.

Información de la compañía, tomada del Consejo Ciudadano para la Seguridad y la Justicia, indica que los engaños relacionados con paquetería fantasma, uno de los fraudes más frecuentes en fin de año, aumentaron 222 por ciento el año pasado y afectaron “a miles de consumidores mediante la suplantación de empresas de mensajería.

Los ciberdelincuentes envían mensajes de texto SMS o por WhatsApp en los que aseguran que el paquete no pudo entregarse o

La mezcla de todas las emociones, urgencia y sobrecarga de información es perfecta para los ataques digitales

está retenido y solicitan un pago mínimo o datos bancarios para hacer la entrega. Usan logotipos y nombres de empresas reales para aparentar credibilidad. En estos casos, 44 por ciento de las víctimas transfirieron hasta 10 mil pesos, mientras 14 por ciento reportaron pérdidas superiores a 5 mil pesos.

La empresa de ciberseguridad informática refirió que el riesgo de esta temporada son los sitios fraudulentos que imitan tiendas oficiales y ofrecen grandes descuentos por Navidad. Una vez que el usuario paga, el producto nunca llega y sus datos quedan comprometidos.

Esta misma modalidad, planteó, es utilizada en fraudes de agencias falsas en línea que ofrecen paquetes de viajes a precios reducidos, y ante la demanda de vacaciones, los usuarios acceden a brindar sus datos o pagar, y una vez hecho esto, la agencia falsa desaparece.

“Durante diciembre también se incrementan los mensajes de cargos no reconocidos, bloqueo de cuentas, bonificaciones o actualizaciones obligatorias. La finalidad es obtener credenciales de banca electrónica. En 2024 las pérdidas por fraudes financieros en México ascendieron a cerca de 14 mil 500 millones de pesos”, añadió.

Otro fraude común es el hackeo de cuentas de WhatsApp, pues los atacantes toman el control de la usada por la víctima y envían mensajes a familiares y amigos solicitando dinero con urgencia. Este caso es frecuente durante las festividades decembrinas. Las estadísticas del Consejo Ciudadano para la Seguridad y Justicia revelan que los robos de cuentas de WhatsApp crecieron seis veces en 2024 respecto a 2023, y en 42 por ciento de los casos los estafadores piden menos de 3 mil pesos.

“Hoy vemos sitios falsos prácticamente idénticos a los originales, mensajes automatizados y

tácticas que mezclan ingeniería social con tecnología avanzada; diciembre es la temporada alta del ciberdelincrimen”, detalló el experto de Eset.

Muy bueno para ser real

Para protegerse, añadió, lo más recomendable es desconfiar de ofertas demasiado buenas y verificar siempre la URL antes de comprar, no abrir enlaces enviados por SMS, WhatsApp o correos no solicitados y tampoco hacer transferencias bancarias para compras en tiendas poco conocidas.

Al mismo tiempo, agregó, se debe habilitar la verificación bancaria en dos pasos en correos, WhatsApp y redes sociales, verificar directamente con el banco cualquier alerta o cargo no reconocido, comprar sólo en sitios oficiales o con reputación comprobada, preferentemente con métodos de pago protegidos, y revisar movimientos bancarios con regularidad, sobre todo después de compras de temporada.

