



ESET da consejos
para evitar caer
en estafas

FRAUDES

EN EL BUEN FIN 2025:

LO QUE DEBES SABER ANTES

DE COMPRAR EN LÍNEA

› **FIRMAS EXPERTAS** alertan que en este tipo de temporadas se observa un incremento en el número de ilícitos; sistema financiero mexicano registra pérdidas de hasta 11 mil mdp por engaños cibernéticos

› Redacción

La campaña de descuentos conocida como El Buen Fin 2025 se caracteriza por ser una de las que más impulsa el comercio electrónico, con un repunte estimado de alrededor de 40 por ciento. Este crecimiento, sin duda prende las alarmas ya que tanto en México como en América Latina, las pérdidas económicas derivadas de fraudes digitales están alcanzando niveles sin precedentes, mientras los ciberdelincuentes aprovechan el auge del *e-commerce*, como esta temporada para perfeccionar sus técnicas.

De acuerdo con Kuvasz Solutions, el sistema financiero mexicano registró en el último año pérdidas por aproximadamente 11 mil millones de pesos derivadas de fraudes cibernéticos. El incremento está directamente relacionado con el crecimiento de las transacciones digitales y la complejidad de los métodos de pago.

Aunque 80 por ciento de las instituciones financieras del país ya utiliza Inteligencia Artificial (IA) o herramientas relacionadas, la compañía advierte que la adopción estratégica —donde la IA funciona como eje central de prevención— sigue siendo limitada, lo cual deja brechas en un ecosistema donde “la Inteligencia Artificial ya no espera a que el fraude ocurra; lo detecta en patrones antes de que el usuario siquiera apriete el botón de pago”, explica Lucas Souza, gerente de Innovación en Kuvasz Solutions.

El informe “Ciberseguridad, habilitador de confianza y competitividad”, publicado por Endeavor Data Unit e In-

code, muestra que América Latina sufre 40 por ciento más ciberataques semanales que el promedio global, registrando 2 mil 803 incidentes por semana, frente a los mil 984 que se registran en el resto del mundo.

Asimismo, se estima un crecimiento regional de 25 por ciento en incidentes entre 2014 y 2023, y un costo promedio de 3.81 millones de dólares por brecha. Las amenazas predominantes son el *phishing* y la ingeniería social (68 por ciento), seguidas del *ransomware* (54 por ciento).

VENTANA PARA ESTAFADORES.

En este contexto, durante El Buen Fin 2025, ESET prevé un aumento significativo de fraudes digitales debido al incremento de compradores, la urgencia por aprovechar descuentos y la confianza que los consumidores depositan en tiendas y plataformas.

“El Buen Fin es un periodo de alta vulnerabilidad. Los estafadores crean sitios casi idénticos a los reales, sofisticados correos de *phishing* y campañas que explotan la prisa del usuario”, señala David González, investigador de ESET.

TIPOS DE FRAUDES MÁS COMUNES DURANTE EL BUEN FIN.

1. Phishing o suplantación de identidad. Mensajes por correo, SMS o redes sociales que aparentan ser de tiendas, bancos o paqueterías. Buscan que el usuario “verifique” una compra o envío para robar datos

bancarios o instalar *malware*.

2. Sitios de comercio electrónico falsos. Páginas con URL alteradas o diseño idéntico al original donde el usuario paga, pero no recibe el producto y entrega sus datos financieros.

3. Ofertas engañosas en redes sociales. Publicaciones con descuentos irreales, meses sin intereses falsos o entregas “gratis” que piden depósitos anticipados.

4. Fraudes de paquetería. Notificaciones falsas de envío o aduana que llevan a formularios fraudulentos para solicitar depósitos o datos bancarios.

5. Robo de datos en redes WiFi públicas. Usuarios que compran desde redes abiertas pueden ser víctimas del robo de contraseñas o tarjetas.

El Buen Fin 2025 se perfila para alcanzar cifras récord en ventas digitales, pero también en intentos de fraude.

Las pérdidas multimillonarias en México y el crecimiento acelerado de ataques en la región de América Latina demuestran que la ciberseguridad ya no es un complemento, sino un requisito básico para consumidores, bancos y comercios.

La combinación de información, la verificación y el uso de herramientas tecnológicas —incluida la Inteligencia Artificial— será clave para que los compradores y consumidores disfruten los descuentos sin poner en riesgo su dinero o sus datos personales.

el dato

EL MERCADO de detección y prevención de fraudes en México está valuado en 513 mdd en 2024, podría crecer hasta 3 mil 699 millones para 2033.

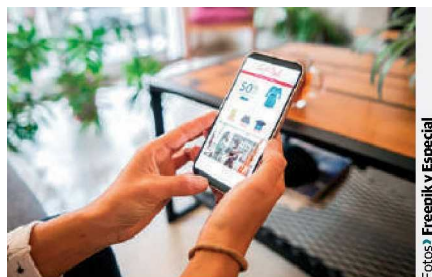
¿QUÉ RECOMIENDA ESET PARA COMPRAS SEGURAS EN EL BUEN FIN 2025?

- **1. VERIFICA** siempre la URL antes de comprar. Debe iniciar con "https://" y tener candado. Revisa que el nombre de la tienda esté escrito correctamente.
- **2. USA MÉTODOS** de pago seguros. Opta por tarjetas virtuales, temporales o plataformas de pago reconocidas. Evita transferencias directas a cuentas desconocidas.
- **3. EVITA COMPRAR** desde redes Wi-Fi públicas. Si es necesario usarlas, utiliza una VPN para proteger tus datos.
- **4. NO HAGAS CLIC** en enlaces sospechosos. Si un mensaje pide "verificar" o "confirmar" algo, entra directamente a la página oficial.
- **5. REvisa** políticas de devolución y datos del vendedor. Desconfía si los precios son demasiado bajos o si no hay información de contacto.
- **6. MANTÉN** tus dispositivos actualizados y con 2FA. Actualizaciones y autenticación en dos pasos reducen las posibilidades de intrusión.
- **7. MONITOREA** tus movimientos bancarios. Particularmente durante y después del Buen Fin.
- **8. PLANEA** tus compras y evita actuar por urgencia. Los estafadores se aprovechan del impulso y de la percepción de "oferta imperdible".

el tip

AUNQUE 65% de las organizaciones se consideran bien preparadas, sólo 17% realiza evaluaciones de ciberseguridad de manera continua.

EN ASCENSO. En el segundo trimestre de este año, los ciberataques crecieron 21% a nivel global, alcanzando una media de mil 984 ataques semanales, según Check Point.



Fotos: Freepik y Especial

UN CONSUMIDOR revisa las ofertas de este Buen Fin 2025.



LAS COMPRAS en línea deben realizarse con mayor cuidado para evitar exponer datos sensibles.