¿Listo para hacer sus compras online de fin de año 2025?

Consejos y Mejores Prácticas para Compras Seguras en la Era de la Inteligencia Artificial y las Nuevas Amenazas Digitales

RISCO

18 de noviembre de 2025

Contenido

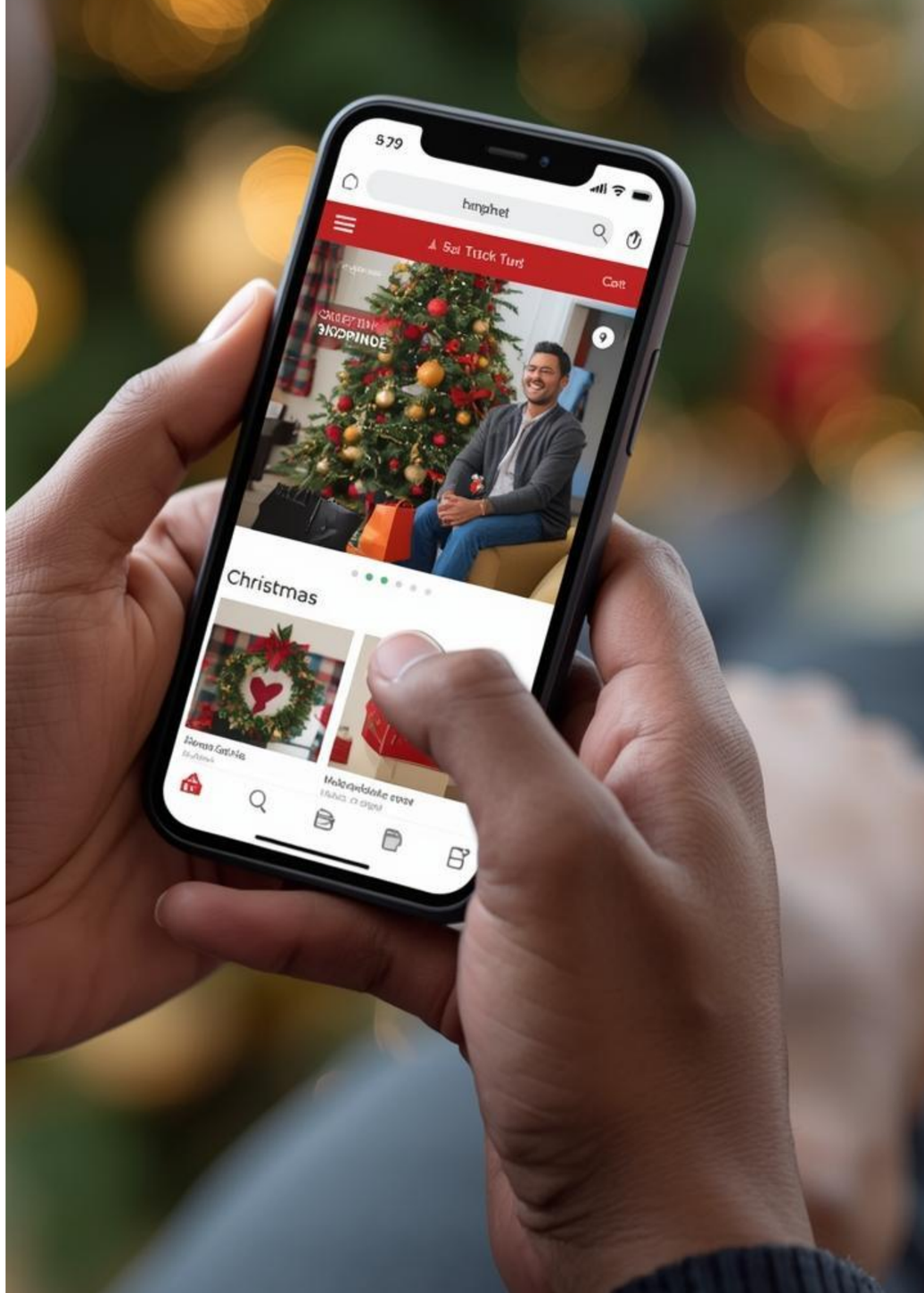
1. Introducción
2. Riesgos y amenazas
3. Consejos de seguridad
4. Qué hacer en caso de ser una víctima de un fraude en línea

1. Introducción

La temporada de compras navideñas en línea de 2025 trae ofertas increíbles... pero también amenazas digitales nuevas y más sofisticadas. Dado que el comercio electrónico global supera los $6.3 billones de dólares estadounidenses, y los ciberdelincuentes aprovechan cada vez más la Inteligencia Artificial (IA), mantenerse seguro es más importante que nunca.

Esta guía le ayudará a comprender:

- Los principales riesgos de fraude en línea y amenazas emergentes en 2025.
- Consejos prácticos y aplicables para compras seguras en línea.
- Qué hacer si se convierte en víctima de fraude en línea.



2. Riesgos y amenazas

Estas son las estafas que la gente enfrenta con mayor frecuencia al comprar en línea.

1. **Tiendas Falsas en Línea**
   Estafadores crean sitios web que parecen legítimos, pero están diseñados para robar su dinero.

2. **Estafas en Redes Sociales**
   Tiendas, vendedores e influencers falsos que promocionan anuncios y publicaciones.

3. **Mensajes Falsos de Entrega o de Bancos**
   Mensajes o correos electrónicos que pretenden ser de Amazon, FedEx, UPS o su banco, pidiéndole que haga clic en un enlace.

4. **Códigos QR Peligrosos**
   Códigos QR falsos que lo envían a sitios dañinos al ser escaneados.

5. **Videos o mensajes de audio Falsos Generados por IA**
   Estafadores usan la IA para imitar a personas reales y ganarse su confianza.

6. **Solicitudes de Pago Inseguras**
   Vendedores que exigen pagos mediante criptomonedas, transferencias bancarias o aplicaciones extrañas; el dinero generalmente se pierde para siempre.

3. Consejos de seguridad

Proteja Sus Contraseñas

- Use contraseñas largas y fuertes
- Use un gestor de contraseñas seguro para que no tenga que recordar todo
- Nunca reutilice la misma contraseña para cuentas importantes

Use Conexiones a Internet Seguras

- Evite usar Wi-Fi público (por ejemplo, en cafeterías o aeropuertos)
- Use el Wi-Fi de su casa o datos móviles cuando compre en línea
- Si es necesario, use una VPN para seguridad adicional

3. Consejos de seguridad

Active la Verificación en Dos Pasos (MFA)

- Esto añade una segunda capa de protección. Incluso si alguien roba su contraseña, aún así no podrá ingresar a su cuenta

Utilice Métodos de Pago Seguros

- Tarjetas de crédito (tarjetas de crédito prepagadas)
- Tarjetas virtuales
- Aplicaciones de pago confiables como Apple Pay o Google Pay. Estos métodos ofrecen protección al comprador

3. Consejos de seguridad

Verifique el Sitio Web Antes de Comprar

- Asegúrese de que la dirección web comience con https://
- Verifique si hay errores ortográficos en la dirección del navegador
- Escriba usted mismo el sitio web de la tienda en lugar de hacer clic en los anuncios

Esté Atento a Videos o Mensajes Falsos

- La IA ahora puede crear videos y mensajes de voz que parecen reales. Tenga cuidado si:
  - Algo se siente antinatural
  - La persona suena robótica
  - El mensaje se transmite una sensación de urgencia

3. Consejos de seguridad

Mantenga Sus Dispositivos Actualizados

- Las actualizaciones solucionan problemas de seguridad. Siempre actualice su teléfono, tabletas, computadora, aplicaciones y antivirus

4. Qué hacer en caso de ser víctima de un fraude en línea

a. Comuníquese inmediatamente con su banco/emisor de su tarjeta de crédito: Reporte el cargo fraudulento; Solicite el bloqueo/cancelación de la tarjeta; Solicite una nueva tarjeta.

b. Cambie las contraseñas comprometidas: Cuentas donde compró; cuentas de correo electrónico asociadas; cualquier cuenta con la misma contraseña.

c. Reporte a la Plataforma: Amazon, eBay, Mercado Libre tienen procesos de denuncia; las redes sociales permiten denunciar a vendedores fraudulentos; PayPal y sitios similares tienen centros de resolución.

d. Reporte a las autoridades locales en su país.

CONTACTOS

CARICOM

Antonio Ayala I.
CEO
aayala@riscco.com

Rubén Fernández
Gerente de Consultoría
rfernandez@riscco.com

Roberto Delgado
Gerente Comercial
rdelgado@riscco.com

Dixie Rampersad
Desarrollo de Negocios
drampersad@riscco.com

riscco.com

Es una empresa internacional independiente dedicada exclusivamente a ayudar a las organizaciones a enfrentar sus desafíos en GRC (Gobernanza, Riesgo y Cumplimiento) e inteligencia artificial, compuesta por profesionales con el conocimiento y la credibilidad necesarios para traducir aspectos muy técnicos a un lenguaje simple con sentido empresarial. Con dieciséis (16) años desde el inicio de sus operaciones, RISCCO tiene en su cartera de clientes a empresas privadas e instituciones gubernamentales líderes en su campo en la región.