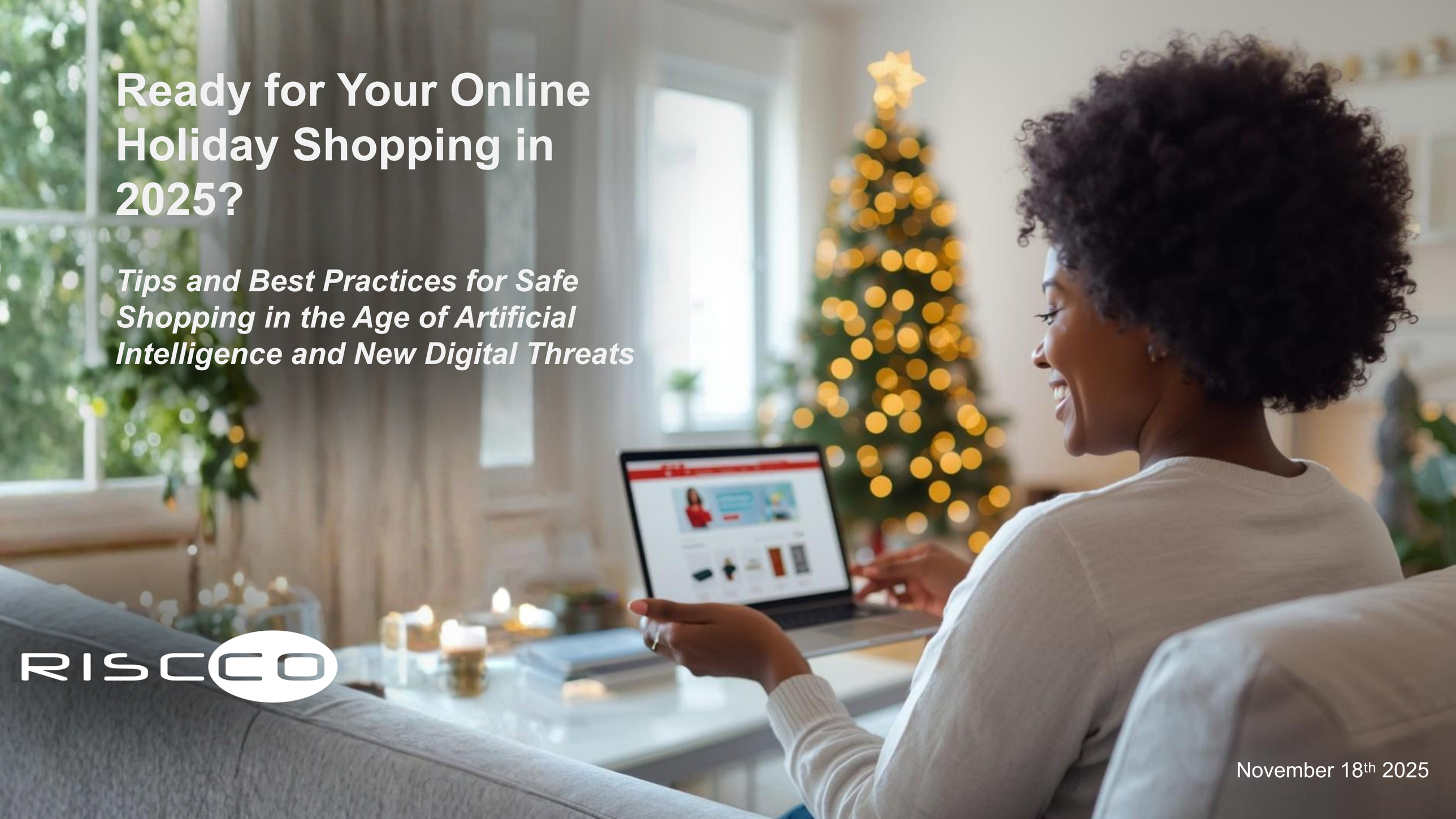
Ready for Your Online Holiday Shopping in 2025?

Tips and Best Practices for Safe Shopping in the Age of Artificial Intelligence and New Digital Threats



November 18th 2025

Contents

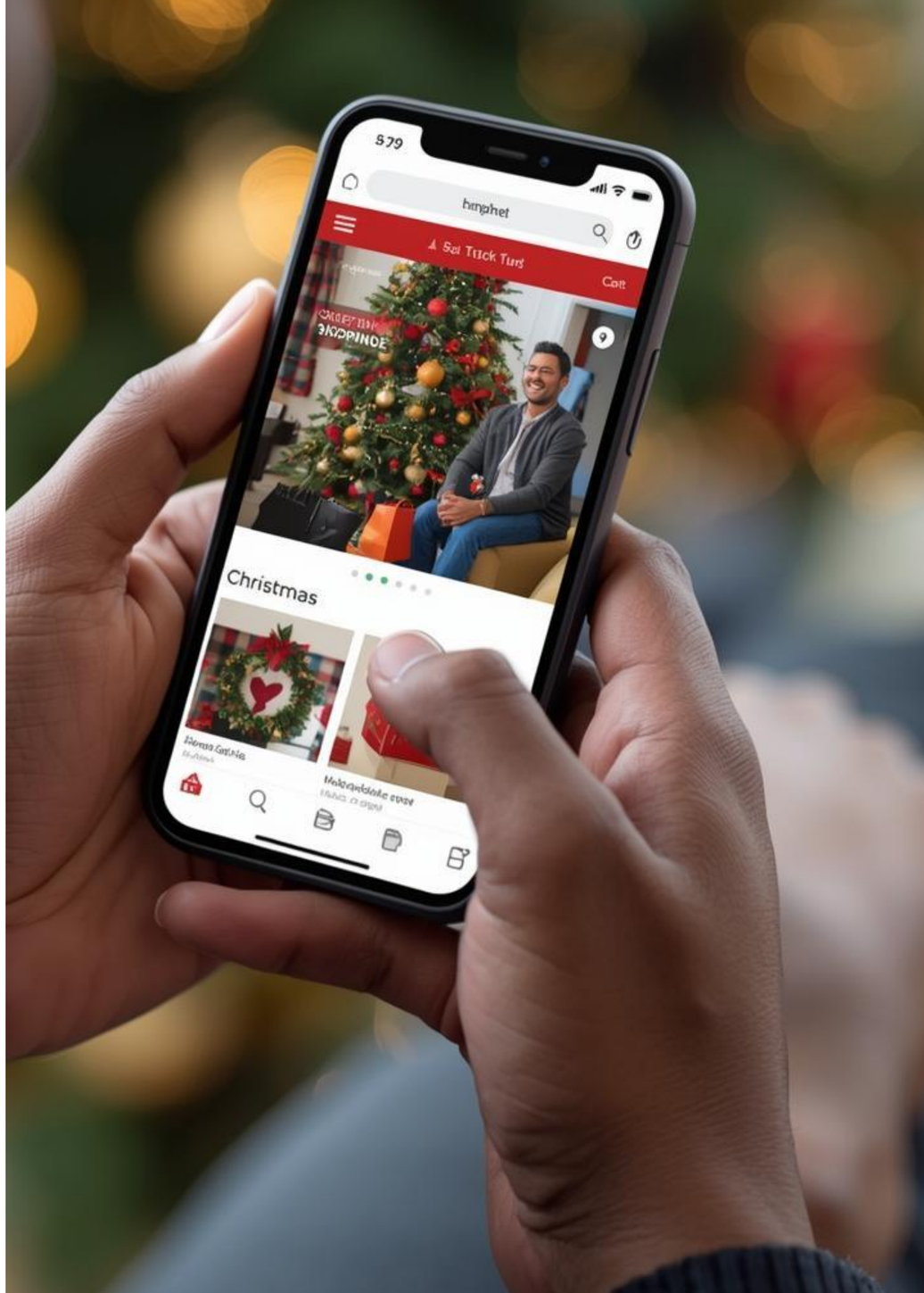
1.Introduction
2.Risks and threats
3.Security tips
4.What to do in case you become a victim of an online fraud

1. Introduction

The 2025 online holiday shopping season brings amazing deals… but also new and more sophisticated digital threats. With global e-commerce surpassing USD6.3 trillion, and cybercriminals increasingly leveraging Artificial Intelligence (AI), staying safe is more important than ever.

This guide will help you understand:

- The main online fraud risks and emerging threats in 2025
- Practical and actionable tips for safe online shopping
- What to do if you become a victim of online fraud



2. Risks and threats

These are the scams regular people face most often when shopping online.

1. **Fake Online Stores**
   Scammers create websites that look real but are designed to steal your money.

2. **Social Media Scams**
   Fake shops, sellers and influencers promoting ads, and posts.

3. **Fake Delivery or Bank Messages**
   Texts or emails pretending to be Amazon, FedEx, UPS, or your bank asking you to click a link.

4. **Dangerous QR Codes**
   Fake QR codes that send you to harmful websites when scanned.

5. **AI-Generated Fake Audio Messages or Videos**
   Scammers use AI to imitate real people to gain your trust.

6. **Unsafe Payment Requests**
   Sellers who demand payment by cryptocurrencies, bank transfer, or strange apps—the money is usually gone forever.

3. Security tips

Protect Your Passwords

- Use long, strong passwords
- Use a safe password manager so you don’t have to remember everything
- Never reuse the same password for important accounts

Use Safe Internet Connections

- Avoid using public Wi-Fi (e.g., at cafes or airports)
- Use your home Wi-Fi or mobile data when buying online
- If needed, use a VPN for extra safety

3. Security tips

Turn On Two-Step Verification (MFA)

- This adds a second layer of protection. Even if someone steals your password, they still cannot enter your account.

Use Safe Payment Methods

- Credit cards (prepaid credit cards)
- Virtual cards
- Trusted payment apps like Apple Pay or Google Pay. These methods offer buyer protection.

3. Security tips

Check the Website Before You Buy

- Make sure the web address starts with https://
- Check for spelling errors in the address in your browser
- Type the store’s website yourself instead of clicking on ads

Watch for Fake Videos or Messages

- AI can now create videos and voices messages that look real. Be careful if:
- Something feels unnatural
- The person sounds robotic
- The message feels urgently pressured

3. Security tips

Keep Your Devices Updated

- Updates fix security problems. Always update your phone, tablets, computer, apps and antivirus.

4. What to do in case you become a victim of an online fraud

a. Immediately contact your bank/credit card issuer: Report fraudulent charge; Request card blocking/cancellation; Request new card issuance.

b. Change compromised passwords: Accounts where you purchased; associated email accounts; any account with same password.

c. Report to Platform: Amazon, eBay, Mercado Libre have reporting processes; social media allow reporting fraudulent sellers; PayPal and similar sites have resolution centers.

d. Report to local authorities in your country.

CONTACTS

CARICOM

Antonio Ayala I.
CEO
aayala@riscco.com

Rubén Fernández
Consulting Manager
rfernandez@riscco.com

Roberto Delgado
Commercial Manager
rdelgado@riscco.com

Dixie Rampersad
Business Development
drampersad@riscco.com

riscco.com

It is an independent international company dedicated exclusively to helping organizations meet their challenges in GRC (Governance, Risk & Compliance) and Artificial Intelligence; composed of professionals with the knowledge and credibility necessary to translate very technical aspects into a simple language with business sense. With sixteen (16) years of having started operations, RISCCO has in its client portfolio private companies and Government Institutions in the region leaders in their field