CUADERNO DE IDEAS

How to Shop Online Without Falling for Scams Dur

Tecnología e IA · 25/11/2026 · Por Camilo Calderón

Black Friday and Cyber Monday bring great deals… and also fake stores, trap links and payments you can't get back. Here are the warning signs, how to pay more safely and what to do if you've already been scammed in Colombia.

Black Friday is here —this year it falls on Friday, November 27— and with it comes a flood of emails, WhatsApp messages and ads with discounts of 50, 60 and even 80 %. Many are real. Others are very well-made traps. The good news is that most online scams leave clues, and learning to spot them takes less time than filling a cart.

The problem is real: according to Colombia's Ministry of ICT and ColCERT, the country recorded more than 36 billion attempted cyberattacks in 2024, and 74 % started with a fraudulent email. During sale season, criminals simply dress up as a deal.

5 signs of a fake store or offer

1. A price that makes no sense

A high-end phone at a third of its price, brand-name sneakers for 60,000 pesos. Big discounts exist, but when a price looks impossible, it usually is. Compare the same product in two or three well-known stores before getting excited.

2. A strange web address

Look closely at the browser bar. Fake pages copy the design of famous stores, but the address gives them away: swapped letters, extra words («-deals», «-black», «-official») or odd endings. Also check that it starts with https:// and shows the padlock. Careful: the padlock only means the connection is encrypted, not that the store is honest; it's a minimum requirement, not a guarantee.

3. You don't know who's selling

A serious store shows its legal name, tax ID (NIT), address, phone number and return policy. If you can't find who to complain to, don't buy. Search the store's name together with the word «scam» or «reviews» before paying.

4. It came through a link you didn't ask for

Text messages, emails or WhatsApp chats with «last chance» and a short link are the favorite way in. The Ministry of ICT recommends not opening those links and typing the store's address into the browser yourself.

5. They only accept direct transfers

If the «store» only takes deposits or transfers to a person's account —via Nequi, Daviplata

or a bank—, be suspicious. That money is much harder to recover than a card payment or one made through a recognized payment gateway.

Before you pay: the 1-minute checklist

Type the store's address yourself; don't go in from the ad.

Check who's selling: tax ID, contact details and return policy.

Pay with a method you can dispute: credit card, virtual card or a recognized payment gateway, as the Ministry of ICT recommends.

Turn on two-factor authentication (2FA) for your bank, email and the stores you use.

Turn on spending alerts from your bank so you hear about any charge instantly.

Keep everything: screenshots of the product, the price, the invoice and the payment receipt.

One extra trick for paying online: many banking and wallet apps let you create a virtual card. If you load only the amount of the purchase, even if someone steals the details there's no more money to take.

Your rights as a buyer in Colombia

Colombia's Consumer Statute (Law 1480 of 2011) protects you when you buy remotely, and there are two tools worth knowing:

Right of withdrawal (article 47): for remote purchases, such as online ones, you can change your mind within 5 business days after the product is delivered and ask for your money back. You cover the return shipping, and there are exceptions, such as perishable or custom-made products.

Payment reversal (article 51): if you paid for an e-commerce purchase with a credit card, debit card or another electronic payment method (the law expressly includes PSE) and you were a victim of fraud, the transaction wasn't requested, the product never arrived or it isn't what you ordered, you can ask for the payment to be reversed. You have 5 business days from when you learned of the problem; the claim goes to the seller and to the entity that issued your payment method.

That's why how you pay matters so much: reversal works with electronic payment methods, not with cash or money deposited into a stranger's account.

If you've already been scammed: what to do today

Call your bank or digital wallet right away: block the card, change passwords and request a payment reversal if it applies.

Gather evidence: screenshots, the page's address, chats, receipts and emails.

Report it to the National Police's CAI Virtual. Your report helps keep others from falling for it.

If the problem is with a real store that didn't deliver or doesn't answer, file a complaint with the Superintendence of Industry and Commerce (SIC).

Change your passwords if you typed them on the suspicious page, starting with your email and

bank.

The best protection: don't shop in a rush

Almost every online scam has one thing in common: it rushes you. The countdown that never stops, the «last 2 units», the «today only». When you feel that pressure, stop for a moment. A real deal can survive five minutes of checking; a scam can't.

And if you want one more filter, try the 48-hour rule (I explain it in a one-minute video): if something wasn't on your list, leave it in the cart for two days before paying. It protects you from impulse buys… and from deals that are too good to be true.

Sources

Colombia's Ministry of ICT and ColCERT — 10 recommendations for a safe digital Black Friday (in Spanish).

Colombian National Police — #CompraConSeguridad this Black Friday and CAI Virtual (in Spanish).

Congress of Colombia — Law 1480 of 2011, Consumer Statute (articles 47 and 51, in Spanish).

Superintendence of Industry and Commerce (in Spanish).

This article is for information only and does not replace advice from your bank or a lawyer.