CUADERNO DE IDEAS

Cómo comprar en línea sin caer en estafas en temp

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

Black Friday y Cyber Monday traen buenas ofertas… y también tiendas falsas, enlaces trampa y pagos que no se pueden recuperar. Estas son las señales para detectarlas, cómo pagar más seguro y qué hacer si ya te estafaron en Colombia.

Llega el Black Friday —este año cae el viernes 27 de noviembre— y con él una avalancha de correos, mensajes de WhatsApp y anuncios con descuentos del 50, 60 y hasta 80 %. Muchos son reales. Otros son trampas muy bien hechas. La buena noticia es que la mayoría de las estafas en línea dejan pistas, y aprender a verlas toma menos tiempo que llenar un carrito.

El tamaño del problema es real: según el Ministerio TIC y ColCERT, en 2024 Colombia registró más de 36.000 millones de intentos de ciberataques, y el 74 % empezó con un correo electrónico fraudulento. En temporada de descuentos los delincuentes simplemente se disfrazan de oferta.

Las 5 señales de una tienda o una oferta falsa

1. Un precio que no tiene sentido

Un celular de gama alta a un tercio de su precio, unas zapatillas de marca a $60.000. Los descuentos grandes existen, pero cuando el precio es imposible, casi siempre lo es. Compara el mismo producto en dos o tres tiendas conocidas antes de emocionarte.

2. Una dirección web rara

Fíjate bien en la barra del navegador. Las páginas falsas copian el diseño de tiendas famosas, pero la dirección las delata: letras cambiadas, palabras de más («-ofertas», «-black», «-oficial») o terminaciones extrañas. Verifica también que empiece por https:// y tenga el candado. Ojo: el candado solo significa que la conexión está cifrada, no que la tienda sea honesta; es un requisito mínimo, no una garantía.

3. No sabes quién te está vendiendo

Una tienda seria muestra razón social, NIT, dirección, teléfono y políticas de cambios y devoluciones. Si no encuentras a quién reclamarle, no le compres. Busca el nombre de la tienda junto a la palabra «estafa» o «opiniones» antes de pagar.

4. Te llegó por un enlace que no pediste

Mensajes de texto, correos o chats de WhatsApp con «última oportunidad» y un enlace corto son la puerta de entrada favorita. MinTIC recomienda no abrir esos enlaces y escribir tú mismo la dirección de la tienda en el navegador.

5. Solo aceptan transferencia directa

Si la «tienda» solo recibe consignaciones o transferencias a la cuenta de una persona —por Nequi, Daviplata o un banco—, desconfía. Ese dinero es mucho más difícil de recuperar que un pago con tarjeta o por una pasarela reconocida.

Antes de pagar: la lista de 1 minuto

Escribe tú la dirección de la tienda, no entres desde el anuncio.

Revisa quién vende: NIT, contacto y política de devoluciones.

Paga con un medio que se pueda reclamar: tarjeta de crédito, tarjeta virtual o una pasarela de pagos reconocida, como recomienda MinTIC.

Activa el doble factor (2FA) en tu banco, tu correo y las tiendas donde compras.

Activa las alertas de consumo de tu banco para enterarte al instante de cualquier cobro.

Guarda todo: capturas del producto, del precio, la factura y el comprobante de pago.

Un truco extra para pagar en línea: muchas apps de bancos y billeteras permiten crear una tarjeta virtual. Si le pones solo el saldo de la compra, aunque alguien robe los datos no hay más plata para sacar.

Tus derechos como comprador en Colombia

El Estatuto del Consumidor (Ley 1480 de 2011) te protege cuando compras a distancia, y hay dos herramientas que vale la pena conocer:

Derecho de retracto (artículo 47): en las compras a distancia, como las de internet, puedes arrepentirte dentro de los 5 días hábiles siguientes a la entrega del producto y pedir la devolución del dinero. El envío de la devolución corre por tu cuenta, y hay excepciones, por ejemplo productos perecederos o hechos a la medida.

Reversión del pago (artículo 51): si pagaste en una compra por comercio electrónico con tarjeta de crédito, débito u otro instrumento de pago electrónico (la ley menciona expresamente PSE) y fuiste víctima de fraude, la operación no fue solicitada, el producto no llegó o no corresponde a lo que pediste, puedes pedir que te devuelvan el pago. Tienes 5 días hábiles desde que te enteraste del problema; el reclamo se hace al vendedor y a la entidad que emitió tu medio de pago.

Por eso importa tanto cómo pagas: la reversión funciona con medios de pago electrónicos, no con plata entregada en efectivo o consignada a la cuenta de un desconocido.

Si ya te estafaron: qué hacer hoy mismo

Llama a tu banco o a tu billetera digital de inmediato: bloquea la tarjeta, cambia claves y pide la reversión del pago si aplica.

Junta las pruebas: capturas de pantalla, dirección de la página, chats, comprobantes y correos.

Denuncia en el CAI Virtual de la Policía Nacional. Tu denuncia ayuda a que otras personas no caigan.

Si el problema es con una tienda real que no te entregó o no te responde, presenta tu queja

ante la Superintendencia de Industria y Comercio.

Cambia tus contraseñas si las escribiste en la página sospechosa, empezando por el correo y el banco.

La mejor protección: no comprar con afán

Casi todas las estafas en línea tienen algo en común: te apuran. El contador que no para, las «últimas 2 unidades», el «solo por hoy». Cuando sientas esa presión, detente un momento. Una oferta real resiste que la revises cinco minutos; una estafa, no.

Y si quieres un filtro más, prueba la regla de las 48 horas (te la explico en un video de un minuto): si algo no estaba en tu lista, déjalo dos días en el carrito antes de pagarlo. Te protege de las compras por impulso… y también de las ofertas demasiado buenas para ser verdad.

Fuentes

Ministerio TIC y ColCERT — 10 recomendaciones para sacarle provecho digital al Black Friday de manera segura.

Policía Nacional — En este Black Friday, #CompraConSeguridad y CAI Virtual.

Congreso de Colombia — Ley 1480 de 2011, Estatuto del Consumidor (artículos 47 y 51).

Superintendencia de Industria y Comercio.

Este artículo es informativo y no reemplaza la asesoría de tu banco ni de un abogado.