KIT GRATUITO · BLACK FRIDAY 2026

Kit anti-truffe Black Friday: 15 controlli prima di pagare

Tutto quello che ti ho spiegato nei video di novembre, in una sola pagina: lo sconto è vero? il sito esiste? come pago senza rischi? e se qualcosa va storto? Salvala e usala prima di ogni acquisto.

Lettura: **5 min** ✅ Con checklist finale

1 · Lo sconto è vero?

il prezzo barrato può essere gonfiato

1 **Il «prezzo di prima» è il più basso degli ultimi 30 giorni**

In Italia, per legge, lo sconto si calcola sul prezzo più basso applicato nei 30 giorni prima della promozione. Se il barrato è più alto di così, lo sconto non vale. Il «prezzo consigliato» non è il prezzo di prima e non conta.

2 **Guarda lo storico del prezzo**

Cerca il prodotto su un comparatore come **idealo** (tanti negozi) o su **Keepa** (Amazon): vedi quanto costava nei mesi scorsi. Se oggi costa come a settembre, non è un affare. Puoi anche impostare un avviso quando scende.

3 **«Fino al 70%» non vale per tutto**

Vuol dire che almeno qualcosa è scontato del 70%, magari pochi articoli. Conta lo sconto scritto sul prodotto che vuoi tu: confrontalo con altri negozi.

4

Le recensioni a 5 stelle possono essere finte

In un controllo europeo su 223 siti, più della metà non rispettava le regole sulle recensioni. Leggi prima quelle da 2 e 3 stelle e diffida di tante recensioni uguali, scritte negli stessi giorni.

5

Portatile in offerta? 3 controlli

Il nome esatto del **processore** (spesso in offerta finiscono modelli di 2-3 generazioni fa), almeno **16 GB di RAM** per farlo durare, schermo **Full HD IPS** (alcuni economici sono ancora HD).

2 · Il sito esiste davvero?

con l'IA un negozio finto si crea in pochi minuti

6

Leggi l'indirizzo lettera per lettera

I siti truffa copiano i nomi dei negozi veri cambiando poco: uno **zero al posto della «o»**, un **trattino in più**, un **finale strano** dopo il punto (.shop, .top…). Nel 2025, tra i nuovi siti a tema Black Friday analizzati da Check Point, **1 su 11 era pericoloso**.

7

Il lucchetto da solo non basta

Il lucchetto (https) dice solo che la connessione è cifrata: lo hanno anche i siti truffa. Per le offerte apri l'**app ufficiale** del negozio o scrivi tu l'indirizzo che conosci.

8

Cerca il nome del sito + «truffa»

Se il negozio è nuovo e nessuno ne parla, o trovi segnalazioni, lascia perdere. In fondo alla pagina devono esserci **partita IVA e indirizzo veri**.

9

Nessun famoso ti regala sconti in un video

Le pubblicità con volti e voci di personaggi famosi possono essere **deepfake** fatti con l'IA: è successo anche con il Governatore della Banca d'Italia. Non cliccare, cerca l'offerta sul sito ufficiale e segnala la pubblicità.

10

I marchi più imitati nelle email truffa

Tra ottobre e dicembre 2025, secondo Check Point: **Microsoft** (22%), **Google** (13%), **Amazon** (9%), **Apple** (8%). Un'email «da Amazon» sull'ordine? Controlla dall'app, non dal link.

3 · Come pagare senza rischi

se qualcosa va storto, devi poter riavere i soldi

11

Paga con metodi che ti rimborsano

PayPal (protezione acquisti) o **carta di credito**, che permette di contestare l'addebito. **Mai bonifico** o ricariche: una volta partiti, i soldi non tornano.

12

Usa una carta virtuale

Molte banche e prepagate ti fanno creare dall'app una carta virtuale, con un numero diverso dalla tua carta vera: ci carichi solo i soldi che ti servono. Se il sito è una truffa, rubano una carta vuota. Cercala nell'app della banca, alla voce **Carte**.

4 · Dopo l'acquisto

la truffa più comune arriva con la consegna

13 «Pacco in giacenza, paga 2 euro»: è una truffa

Nessun corriere chiede soldi con un link in un SMS: quei pochi euro servono a rubarti i dati della carta. Controlla dall'**app ufficiale** del corriere con il numero di spedizione della conferma d'ordine.

14 Hai 14 giorni per il reso

Se compri online da un negozio (non da un privato) hai 14 giorni dalla consegna per ripensarci, senza spiegare il perché. Di solito la spedizione del reso la paghi tu, se il negozio non la offre. Escluso, per esempio, ciò che è personalizzato.

5 · Se qualcosa è andato storto

conta la velocità

15 Blocca, avvisa, segnala

Blocca subito la carta dall'app della banca, poi chiama la banca o PayPal per contestare il pagamento. Segnala il sito o il messaggio alla Polizia Postale sul **Commissariato di PS online** (commissariatodips.it). Se hai usato la stessa password altrove, cambiala.

✅ Checklist veloce

stampala o fai uno screenshot

- [ ] Il barrato è il minimo degli ultimi 30 giorni
- [ ] Ho guardato lo storico del prezzo
- [ ] Lo sconto è scritto sul MIO prodotto
- [ ] Ho letto recensioni da 2-3 stelle
- [ ] L'indirizzo è giusto, lettera per lettera
- [ ] Sono entrato dall'app o scrivendo io l'indirizzo
- [ ] Ho cercato «nome del sito + truffa»
- [ ] Ci sono partita IVA e indirizzo veri

- [ ] Pago con PayPal, carta di credito o carta virtuale
- [ ] Niente bonifici, niente ricariche
- [ ] Gli SMS del corriere li controllo dall'app
- [ ] So che ho 14 giorni per il reso

> **Vuoi un parere prima di comprare?** Scrivimi su WhatsApp il link dell'offerta: se posso, ti dico se mi sembra affidabile.

Fonti

- La regola dei 30 giorni sul prezzo di prima · Lo storico dei prezzi · «Fino al 70%»
- Le recensioni false (controllo UE su 223 siti) · Portatile in offerta
- I siti finti del Black Friday (Check Point) · L'indirizzo del sito · Il negozio finto creato con l'IA
- Le offerte deepfake (avvisi Banca d'Italia) · Check Point: i marchi più imitati, Q4 2025
- La carta virtuale · Il pacco in giacenza · Il reso in 14 giorni

---