Saldi online, ma sicuri: come difendersi dalle truffe digitali durante le offerte di stagione

Offerte troppo allettanti, messaggi strani, email sospette. La nostra guida per evitare spiacevoli inconvenienti e poter così usufruire in sicurezza degli sconti online

(Fonte: https://www.corriere.it/ 7 luglio 2025)

Ogni estate, puntuali come il caldo torrido e le zanzare, arrivano i **saldi**. I negozi si riempiono di cartelloni con percentuali a tre cifre, le homepage degli e-commerce si colorano di rosso e giallo, e le caselle di posta elettronica iniziano a brulicare di newsletter, promozioni e «imperdibili occasioni». Fin qui, tutto regolare. Se non fosse che insieme agli sconti autentici, si infilano trappole digitali sempre più sofisticate, pensate per colpire proprio nei momenti di massima frenesia.

La tentazione è forte: con un clic si risparmia il 50%, il 70%, a volte anche il 90%. Ma la domanda è semplice: risparmiamo davvero? O rischiamo di perdere molto di più, come dati personali, soldi, tempo e fiducia nel commercio online? Secondo i dati della **Polizia Postale**, le truffe online sono cresciute del 15% solo nell'ultimo anno. E il periodo più critico è proprio quello estivo, quando i saldi attirano milioni di utenti sui siti e le app di shopping. I criminali informatici lo sanno bene: il consumatore distratto, che ha fretta di concludere l'affare, è la preda perfetta.

Il phishing si traveste da offerta

Una delle armi più usate dai truffatori è il **phishing**, ovvero l'invio di email o Sms che imitano comunicazioni ufficiali da parte di brand noti. Il messaggio è semplice e costruito per sembrare

legittimo: un pacco in arrivo, una promozione esclusiva, un problema con il pagamento. Basta cliccare sul link incluso per finire su un sito falso, identico all'originale, dove si inseriscono inconsapevolmente credenziali o dati bancari.
Un consiglio banale, ma sempre valido: se qualcosa sembra troppo bello per essere vero, probabilmente è una truffa. Diffidate da offerte-lampo che chiedono di agire subito. Prendetevi cinque secondi per controllare chi è il mittente, se il dominio è corretto, se ci sono errori grammaticali nel testo. Spesso basta poco per capire che qualcosa non torna.

Il sito è falso, ma sembra autentico

Un altro scenario frequente **è quello dei siti fake**, cloni perfetti di portali di shopping reali. L'utente arriva tramite una pubblicità su Facebook o Instagram, vede prodotti conosciuti a prezzi ridicoli, aggiunge al carrello e paga con carta. Ma l'ordine non arriverà mai, e quei soldi difficilmente saranno recuperabili.
Come evitarlo? Ci sono segnali precisi: indirizzi (gli «Url» del sito) sospetti, assenza di partita Iva o sede legale, metodi di pagamento poco trasparenti (come bonifici o ricariche Postepay), mancanza di recensioni reali. Se il sito è nuovo o sconosciuto, una ricerca veloce può salvare il portafoglio.
Spesso basta poco per capire che qualcosa non torna:

- Controllare che l'indirizzo inizi con «https://».
- Verificare la presenza del lucchetto accanto alla Url.
- Fare una ricerca sul dominio per vedere da quanto tempo esiste (servizi come Whois aiutano).
- Diffidare da offerte troppo allettanti: Nike a 29 euro? Probabilmente è un sito fake.

Occhio anche ai corrieri: la truffa viaggia via Sms

Negli ultimi mesi si è diffusa una tecnica ancora più insidiosa: **il finto Sms da parte di un corriere** (Dhl, Poste, Gls), che chiede di pagare una piccola somma per sbloccare una consegna. Cliccando sul link si viene dirottati su una pagina che ruba i dati della carta. E qui la regola è semplice: i corrieri non chiedono soldi via Sms. Mai. Se ricevete messaggi del genere, cancellateli subito. E se il dubbio resta, andate direttamente sul sito ufficiale del corriere e inserite il numero di tracking.

Social network: le nuove vetrine del crimine digitale

Instagram e **Facebook** sono diventati **il canale preferito per le truffe di massa**. Pagine con loghi rubati, foto professionali, recensioni inventate, promuovono scarpe, borse, occhiali a prezzi incredibili. Ma dietro non c'è alcuna azienda: solo una rete che raccoglie pagamenti e sparisce.
Il trucco è semplice: il profilo compare, fa promozioni per qualche giorno, incassa e scompare. Quando gli utenti iniziano a lamentarsi nei commenti, la pagina viene cancellata o cambia

nome. Prima di acquistare da un annuncio social, verificate se esiste un sito ufficiale, cercate recensioni vere su forum e blog, e soprattutto pagate solo con metodi tracciabili: PayPal, carte virtuali, e mai bonifici.

Attenti alle app: il rischio è anche nello smartphone

Anche il telefono può diventare una porta d'ingresso per i truffatori. Alcune app, scaricate da store non ufficiali o da link in rete, si spacciano per comparatori di prezzi o app ufficiali di brand famosi. Una volta installate, raccolgono dati, tracciano abitudini e possono perfino accedere ad altre app sensibili come **l'home banking.** La regola è una: **scaricare app solo da Google Play o App Store**. E leggere sempre le recensioni degli utenti. Un'app con valutazione bassa o con pochi download è già un primo campanello d'allarme.

Difese pratiche e tecnologiche

Non servono lauree in informatica per proteggersi. Bastano alcune buone abitudini:

- usare password complesse e uniche per ogni servizio;
- attivare l'autenticazione a due fattori, soprattutto per email e servizi bancari;
- evitare di connettersi a reti Wi-Fi pubbliche senza Vpn;
- controllare sempre la cronologia degli acquisti e i movimenti del conto;
- usare gestori di password per creare e memorizzare credenziali sicure.

Nel caso in cui la truffa fosse già avvenuta, la prima cosa da fare è bloccare immediatamente la carta usata, contattando la banca o l'emittente. Poi va presentata denuncia alla Polizia Postale. Conviene raccogliere tutte le prove: schermate del sito, email ricevute, ricevute di pagamento, **Url sospetti.** Infine, segnalare il sito truffaldino a portali come Google Safe Browsing o PhishTank, in modo da evitarne la diffusione.

I saldi online possono essere una grande occasione, ma solo se affrontati con attenzione e lucidità. Ogni clic va ponderato. Ogni offerta va verificata. E ogni dubbio, ascoltato. Internet ci ha abituati a pensare che tutto sia a portata di mano. Ma in mezzo alle offerte vere si nascondono esche, e pescatori abili. Proteggersi non significa rinunciare allo shopping, ma farlo con testa.