PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 9 - numero 1725 di martedì 05 giugno 2007

I 5 sensi per acquisti sicuri sul web

Alcune regole per acquistare on line senza rischi. Dalla scelta delle password alla serietà dei venditori: come non cadere nelle truffe.

Vista, tatto, olfatto, udito, gusto: utilizzare i cinque sensi "reali" per fare acquisti sicuri nel mondo virtuale. E' quanto propone la Polizia di Stato nella campagna informativa "Buonsenso in tutti i sensi", realizzata in collaborazione con E-Bay.

"Gli accorgimenti che si usano per fare acquisti in negozi, mercati e supermercati ? affermano gli esperti della Polizia - devono essere utilizzati anche per comprare online. [...]Con l'aumento degli acquisti aumentano anche i reati, tanto che in poco più di 2 mesi al commissariato di polizia online sono arrivate 4.654 denuncie di cui 2.538 riguardavano proprio il commercio elettronico."

Valutare l'attendibilità del venditore, controllare la merce, effettuare pagamenti in modo sicuro: sono operazioni che bisogna saper fare sul web come...al mercato.

La campagna educativa è promossa tramite il sito www.compraconbuonsenso.it che, oltre a fornire indicazioni per acquisti on line sicuri, invita l'utente a mettersi alla prova, proponendo un test sulla sicurezza nel commercio elettronico.

Ecco alcune delle regole suggerite:
Vista. Guarda di scegliere bene la password. Le tue password sono le chiavi della tua vita su internet. Ogni password deve essere almeno di 8 caratteri; deve contenere lettere (maiuscole e minuscole), numeri e simboli e non essere comunicata a nessuno. La password deve essere cambiata periodicamente. Non comunicare mai la tua password via mail: nessuna azienda affidabile te lo chiederà mai.

Udito. Ascolta i feedback sulla serietà dei venditori. Reperisci il maggior numero di informazioni sul venditore prima di fare un acquisto. In caso di venditori professionali assicurati che informazioni come ragione sociale, indirizzo, condizioni per l'esercizio della garanzia, diritto di recesso e di ripensamento siano chiare e facilmente reperibili. Per una maggiore valutazione del venditore potrebbero essere utili anche i profili utenti (feedback), che si trovano ad esempio su siti come eBay, e i marchi di qualità.

Gusto. Assaggia prima i tuoi acquisti. Fare attenzione ai dettagli controllando per esempio la descrizione, le condizioni di spedizione e di consegna.
E' meglio fare qualche domanda al venditore se non si è certi della qualità della merce, delle condizioni di recesso, delle modalità di pagamento accettate o della tipologia di spedizione che verrà utilizzata.
A tale proposito è meglio scegliere sempre un metodo di spedizione tracciabile (raccomandata con ricevuta di ritorno, pacco celere, corriere, spedizione assicurata.). "Una spedizione in posta prioritaria, ad esempio, è più economica, ma non permette di rintracciare l'oggetto in caso di smarrimento."

Tatto. Tocca con mano il pagamento on line. I metodi di pagamento sicuri sono rintracciabili.
Metodi di pagamento sicuri. Il bonifico bancario, il conto corrente postale e il contrassegno sono metodi di pagamento sicuri. Un elevato livello di protezione viene garantito anche dai servizi di pagamento online come PayPal, Bankpass o da quelli di deposito a garanzia.
Metodi di pagamento NON SICURI. La ricarica di carte prepagate (Postepay, Kalibra, etc.) e i servizi di trasferimento contanti

come Western Union o Moneygram, invece, non sono i metodi di pagamento adatti se non conosci di persona il venditore. Non fare mai acquisti online se il venditore intende utilizzare a tutti i costi un servizio di trasferimento contanti o una ricarica di carta prepagata come metodo di pagamento.

Olfatto. Fiuta le false e-mail: È importante sapersi difendere da email e siti web contraffatti (spoof o phishing). Diffida delle e-mail che chiedono dati riservati, password o informazioni sulla carta di credito attraverso un link inviato via e-mail. Le aziende serie non lo fanno mai. Diffida da queste email anche se sembrano inviate da un'azienda affidabile, in quanto potrebbe trattarsi di copie contraffatte con lo scopo illecito di carpire dati personali, come il numero della carta di credito o l'ID utente e la password.