Truffe online, ecco tutti i modi per evitarle

È bene stare attenti a non divulgare informazioni sensibili se prima non si è accertata l'originalità e l'affidabilità del sito

Di Valentina Menassi 15 Maggio 2024

Le **truffe online** sono, purtroppo, all'ordine del giorno. Per questo motivo è bene prestare molta attenzione alle possibili frodi in cui si può cadere facendo shopping sul web. Sono infatti 12,7 milioni gli italiani, il 21,6% dei cittadini, che hanno subito almeno una truffa nel settore degli acquisti sul web, e addirittura un giovane su 3 (il 33,1%) è caduto nelle trappole dello shopping digitale. I dati di Consumerismo No Profit descrivono uno scenario critico. Ci sono però alcune **accortezze** che si possono mettere in pratica, a questo proposito Bankitalia ha dato dei consigli specifici per evitare di cadere nelle truffe online. **Attenzione ai siti ingannevoli** I cybercriminali creano **siti ingannevoli** che possono risultare molto simili rispetto a quelli autentici. Come capire se la pagina su cui siamo capitati è quella che effettivamente volevamo visitare? Tramite il **dominio** che indica la pagina web su cui ci si trova. Ogni sito Internet è raggiungibile tramite un URL ed è scritto nella barra degli indirizzi del browser. I siti web malevoli spesso presentano nomi di dominio e indirizzi creati proprio per trarre in inganno i visitatori. È bene evitare di navigare su siti con indirizzi in cui il nome di dominio del sito di destinazione non è evidente oppure ha caratteristiche che non tornano. Un esempio è un indirizzo IP, ossia una sequenza numerica come http://85.159.192.76:80 oppure un indirizzo mascherato tramite **servizi di url-shortening** come tinyurl.com o bit.ly, ad esempio http://bit.ly/1vwRM0A. Inoltre se dovessero presentarsi dei dubbi sull'attendibilità di un sito è possibile accertarsi che sia un sito "noto". Come fare? Recuperando l'indirizzo web ufficiale cercandolo su Google. Inoltre, per un'ulteriore verifica, è consigliabile digitare nella ricerca anche le parole chiave "truffa" o "phishing". **Prima di effettuare un pagamento** Quando ci viene richiesto di effettuare un pagamento è importante leggere attentamente le comunicazioni che arrivano. Inoltre è consigliabile fare attenzione a eventuali **errori di grammatica** (tipici dei siti che nascondono una truffa), alle richieste di pagamento, ai link e ai QR code. Se, invece, la richiesta viene inoltrata per telefono è bene interrompere la conversazione nel momento in cui vengono segnalate anomalie come l'accesso di estranei al conto, attacchi informatici, il blocco della carta o problemi con l'home banking. In questa situazione è consigliabile contattare la banca tramite i canali ufficiali. **Anomalie e password** È importante mantenere un costante controllo sulle attività finanziarie effettuate sul proprio conto. Qualora si dovessero riscontrare **transazioni anomale** o non autorizzate, è fondamentale contattare prontamente la banca per bloccare la carta e avviare le opportune verifiche. Inoltre, è assolutamente sconsigliato divulgare credenziali, password o codici a terzi, poiché ciò potrebbe compromettere la sicurezza del proprio conto. Per garantire una **maggiore sicurezza**, è meglio attivare notifiche che avvertano ogni volta che viene effettuato un pagamento elettronico, permettendo così di monitorare le transazioni in tempo reale e intervenire prontamente in caso di attività sospette. **Pagamenti online** Quando si inseriscono dettagli finanziari online o viene usata una carta di pagamento su internet è bene essere molto prudenti, come? Bisogna sempre controllare l'indirizzo del sito web nella barra del browser per assicurarsi che inizi con "https://" e che mostri un **lucchetto** o una chiave, indicando una connessione solida con un **certificato di sicurezza**. Questo aspetto aiuta a confermare l'autenticità del sito e la protezione dei dati durante i pagamenti online. Se dovessero esserci cambiamenti significativi nel sito rispetto alla visita precedente, potrebbe essere un segnale di autenticità dubbia. **Ilgiornale.it**