

## Carte elettroniche: l'attenzione non è mai troppa per scongiurare i danni

**Achab ha raggruppato in dieci semplici, quanto spesso dimenticate, regole tutto quello che chiunque posseda una carta elettronica dovrebbe mettere in pratica per evitare clonazioni e furti e continuare a utilizzarla in serenità**

Distruggere la vecchia tessera in caso di sostituzione, firmare sempre la carta di credito anche se può sembrare banale, verificare le transazioni anche di importo minimo perchè i truffatori sfruttano proprio le carte per transazioni di basso importo tali da non indurre il malcapitato nel dubbio.

Sono queste alcune delle dieci regole che il team di **Achab**, distributore italiano specializzato nello scouting e nell'introduzione in Italia di soluzioni It innovative, ha realizzato per proteggere la propria carta di credito. **Secondo i dati di Confcommercio**, il 2015 sembra essere in ripresa con un più 5% rispetto al 2014 e, in particolare tra novembre e dicembre scatta la corsa agli acquisti natalizi.



E con loro cresce il numero di frodi sulle carte di credito. **Le truffe sono compiute attraverso l'uso del numero della carta di credito** che è riprodotto illegalmente su carte "clonate" che vengono utilizzate sia per lo shopping tradizionale sia per il commercio elettronico. Secondo le stime della **Bce** relative allo stesso periodo dello scorso anno, circa un euro viene frodato ogni 2.635 spesi con carta di credito. A volte però queste iniziative sono più audaci e portano via all'ignaro compratore somme molto più alte.

Spesso le competenze informatiche aiutano a prevenire le frodi su carta di credito, specialmente per

quanto riguarda gli acquisti online, ma sia nel caso in cui gli acquisti avvengano attraverso e-commerce sia nel caso che si decida di comprare in store fisici, è bene ricorrere a una serie di buone pratiche per evitare di agevolare i malintenzionati.

A questo proposito la sicurezza fisica è importante:

1. Si deve tenere la carta di credito in un luogo sicuro e non accessibile a tutti (tenerla nel cassetto della macchina non è una buona idea).
2. Non scrivere mai il PIN da nessuna parte e accertarsi che non contenga dei numeri semplici come il prefisso o la data di nascita.
3. Ricordarsi di firmare la carta di credito: sembra una banalità, ma in alcune circostanze la firma è verificata e controllata



4. Si verifichi regolarmente l'elenco delle transazioni: anche quelle di pochi centesimi o pochi euro. Spesso i cybercriminali fanno delle piccole transazioni per vedere se si sta controllando gli estratti conti, se non si controllano, e le transazioni restano non "contestate", si dedicano a somme ben più ingenti.
5. Prima di utilizzare la carta a uno sportello bancomat assicurarsi che il bancomat sia integro, non ci siano segni di effrazione, strane telecamere o oggetti insoliti.
6. Dopo aver fatto un prelievo assicurarsi che la ricevuta riporti lo stesso importo dei soldi effettivamente prelevati.
7. Quando si riceve la nuova carta di credito o un nuovo bancomat si distrugga il vecchio e non riporlo semplicemente nel cassetto.
8. Se si fanno acquisti online, assicurarsi che il sito web utilizzi i protocolli sicuri come HTTPS; non mettere mai informazioni personali o finanziarie su un sito che non usa transazioni cifrate.
9. Quando si finisce di utilizzare un sito web o un'applicazione effettuare il logout, ossia scollegarsi completamente: alcuni servizi e applicazione dopo un certo tempo di inattività ti scollegano automaticamente, ma non fare affidamento su questo. Se non ci si scollega, chi userà il computer o l'applicazione agirà con le credenziali dell'ultimo utilizzatore.
10. Non usare computer pubblici per effettuare transazioni o acquisti e non fare mai transazioni di denaro da reti che non si conoscono a priori.