La carta di credito

Le truffe con le carte di credito sono particolarmente frequenti e ogni anno presentano un trend in aumento.

Le statistiche di analisi di questo tipo di reati segnalano che le transazioni più pericolose sono quelle effettuate via Internet o per telefono quando non è necessario esibire fisicamente la carta. [d]

Le truffe vengono compiute attraverso l'utilizzazione del numero della carta di credito che viene riprodotto illegalmente su carte "**clonate**" che vengono utilizzate sia per lo *shopping* tradizionale sia per il commercio elettronico.

Per impedire ciò le società che gestiscono le *credit card* stanno adottando dei sofisticati sistemi **anticontraffazione** per le carte di ultima generazione. Nel frattempo, però, bisogna non perdere mai di vista la propria carta (per evitare che i dati possano essere memorizzati e successivamente trasferiti su carte clonate) quando si pagano i propri acquisti e seguire precauzioni particolari per il commercio via Internet.

Alcuni accorgimenti per gli **acquisti tradizionali**:

- controllate sempre l'estratto conto della carta di credito badando in modo particolare alle spese di piccolo importo, dove spesso si nasconde la truffa;
- non perdete mai di vista la persona alla quale consegnate la carta per l'acquisto durante la transazione. E' sempre preferibile recarsi di persona alla cassa, anche se la cosa (specie in alcuni esercizi pubblici quali ristoranti e pizzerie) può farci perdere cinque minuti di tempo in più e può sembrare meno "chic";
- verificate sempre, in ogni negozio, che la carta venga regolarmente passata una sola volta e, comunque, mai in apparecchi diversi nel caso vi venga detto che l'operazione non è andata a buon fine. In questi casi chiamate subito i carabinieri;
- non distraetevi e non fatevi distrarre durante il passaggio della carta;
- tenete da parte le ricevute fino all'arrivo dell'estratto conto;
- **stracciate** le ricevute prima di cestinarle;
- non conservate mai il PIN (numero segreto) insieme alla carta;
- ricordate che molte banche offrono bancomat che possono essere usate anche come carte di credito. In caso di smarrimento o furto telefonate immediatamente al numero verde specifico per bloccare la carta.

In caso di **commercio elettronico**:

- effettuate acquisti *online* solo sui siti ad alto standard di **sicurezza**, protetti dai sistemi di sicurezza internazionali: **SSL** (*Secure Socket Layer*) e **SET** (*Secure Electronic Transaction*) riconoscibili dalla certificazione e dal lucchetto che appaiono sulla schermata. Questi siti garantiscono la trasmissione sicura dei dati, che vengono "crittografati" e non possono essere decifrati dagli "hackers";[d]
- trasmettete i vostri **dati economici** solamente quando sono rispettate le condizioni di sicurezza e comunque non comunicate mai i dati della vostra carta, o altri dati riservati, tramite e-mail;
- verificate che il **venditore** sia un esercizio reale e non solo virtuale e che siano indicati tutti i dati significativi dello stesso compreso l'indirizzo. In particolare prendete nota dei dati del venditore e cioè il nome dell'azienda e l'indirizzo geografico della sede sociale, delle condizioni generali di vendita, delle modalità per esercitare il diritto di recesso e della descrizione dei singoli beni o servizi venduti;
- nei **casi dubbi** inviate un messaggio e-mail all'azienda intestataria del sito per ottenere maggiori garanzie circa l'affidabilità della stessa;
- prendete sempre nota dell'indirizzo del sito presso il quale si è effettuato l'acquisto di servizi;
- ponete particolare attenzione alle **condizioni di pagamento** del servizio per non cadere in una sottoscrizione inconsapevole di un abbonamento con ripetuti addebiti mensili;
- diffidate di **offerte** incredibilmente vantaggiose che spesso celano spiacevoli sorprese;
- in caso di **acquisti frequenti** in Rete, dotatevi di un lettore esterno della carta: in questo modo i dati non viaggiano su Internet. Alcuni istituti bancari mettono a disposizione una **carta di credito virtuale** che utilizza un codice differente per ogni acquisto come se ogni volta si utilizzasse una carta di credito differente in merito ad ogni specifica transazione. Un altro metodo alternativo di pagamento è il **denaro elettronico** tramite i pagamenti cosiddetti E-cash che possono essere adottati scaricando direttamente dalla Rete il software necessario ed aprendo un conto virtuale presso le banche abilitate on line. Anche le **carte prepagate** e i borsellini elettronici svolgono la stessa funzione della carta di credito e presentano il vantaggio di richiedere la trasmissione dei dati relativi solo ad una piccola somma, piuttosto che quelli di un intero conto corrente.

Se l'estratto conto riporta la registrazione di **spese non riconosciute**, inviate ai Servizi Interbancari, entro 60 giorni dalla data di emissione dell'estratto conto, una contestazione scritta e firmata dell'intestatario della carta di credito, allegando copia dell'estratto conto contestato e copia fronte-retro della carta. Nel caso in cui si è certi che si tratta di un utilizzo fraudolento della carta di credito, allegate anche una denuncia contro ignoti effettuata presso le Autorità competenti.

Qualche altro suggerimento utile per evitare spiacevoli sorprese

In caso di **furto / smarrimento** della carta o del bancomat è necessario:

- bloccare la carta rubata o smarrita telefonando subito ad uno dei numeri verdi messi a disposizione dalle società che gestiscono i circuiti telematici, in modo da prevenire ogni tentativo di utilizzo fraudolento della stessa;
- immediatamente dopo, sporgere denuncia dell'accaduto presso la più vicina Stazione Carabinieri;
- inviare copia della denuncia, anche via fax, alla società che ha bloccato la carta, in modo da consentire l'avvio della procedura per l'eventuale risarcimento del danno.

Presso gli **sportelli bancomat**, prima di qualsiasi prelievo:

- verificate che nelle immediate vicinanze non vi siano persone ferme in atteggiamento sospetto;
- accertatevi che sullo sportello non siano state applicate apparecchiature posticce, controllando, ad esempio, la fessura ove viene inserita la carta (per l'eventuale presenza di skimmer, fili o nastro adesivo sospetto) oppure l'aderenza della tastiera al corpo dello sportello (verificando che non vi siano due tastiere sovrapposte) - queste applicazioni, è bene ricordarlo, non inficiano l'operazione da svolgere, per cui al termine della stessa non potremo neppure accorgerci della duplicazione del nostro codice-;
- controllate che non vi siano fori anomali all'interno dello sportello (specialmente sul lato superiore), ove potrebbero trovare eventuale alloggiamento microtelecamere (queste non superano il mezzo centimetro di diametro);
- qualora abbiate il sospetto che lo sportello sia stato manomesso chiamate il "112".

Durante l'operazione di digitazione del vostro codice, utilizzate una protezione "visiva" (anche l'altra mano, ben collocata, o il portafogli stesso possono essere sufficienti) che renda effettivamente difficoltoso, per potenziali "spioni", prendere conoscenza del codice attraverso microtelecamere in precedenza installate.
Qualora al termine dell'operazione non vi venga restituita la carta, è buona norma chiamare subito il numero verde per bloccarla.