29 giugno 2007 0:00

FRODI CON CARTE DI CREDITO: MISURE DI SICUREZZA E CONSIGLI

di Rita Sabelli

Ultimo aggiornamento: 19/10/2012

Abbiamo gia' visto cosa sono le carte di credito, quanti tipi ne esistono e come funzionano (clicca qui (http://sosonline.aduc.it/scheda/carte+credito+bancomat_12137.php)).
In questa scheda ci proponiamo di stilare una guida sulle misure di sicurezza per l'utilizzo delle stesse, con i consigli nel caso si sia incappati in un uso indebito od una truffa.

Indice scheda
CONSIGLI PREVENTIVI
FURTO E SMARRIMENTO: COSA FARE
UN CASO PARTICOLARE: LA CLONAZIONE DELLA CARTA
L'ARCHIVIO ANTIFRODE "SIPAF"
LINK UTILI

CONSIGLI PREVENTIVI

La regola numero uno, valida per ogni modalita' di utilizzo della carta, e' quella di **controllare regolarmente l'estratto conto della carta di credito,** spuntando ogni addebito con gli scontrini e le ricevute.
In alternativa e' possibile usufruire dei servizi che sempre piu' spesso le banche -soprattutto quelle on-line- propongono ai propri clienti. Quello piu' utile al riguardo e' la comunicazione via SMS -quindi praticamente in tempo reale- di ogni utilizzo della propria carta.
Il vantaggio e' notevole, visto che cio' permette di bloccare immediatamente la carta in caso di uso non riconosciuto impedendo ulteriori addebiti illegittimi.

Altro consiglio da tenere in considerazione sempre e' **non fornire mai il numero di carta di credito** in risposta a richieste o sollecitazioni sconosciute o sospette, sia che esse avvengano tramite telefonata od invio di posta cartacea ed elettronica (tipicamente il PHISHING, ovvero i messaggi email che, copiando esattamente le pagine internet della propria banca o della posta, chiedono l'inserimento dei dati della propria carta, o del conto corrente on-line, con l'unico scopo di carpirli per usi illeciti).

Un ultimo consiglio e' **stracciare bene la corrispondenza bancaria e le ricevute di pagamento del bancomat e della carta di credito prima di buttarli via,** od addirittura bruciarli: non si tratta di un fenomeno diffuso, per ora, pero' i dati vengono carpiti anche rovistando tra i rifiuti e carpendo in tal modo dati personali associati con coordinate bancarie o dati delle carte di pagamento, tramite il cosiddetto TRASHING.

Per quanto riguarda i prelievi agli sportelli ATM, sia che avvengano con bancomat che con carta di credito, e' bene sempre fare la massima attenzione a non essere spiati, coprire bene la mano che digita il codice in modo da vanificare eventuali riprese di microtelecamere presenti (normalmente abbinate ad un lettore applicato per "clonare" le carte) , ritirare la carta e la ricevuta eventualmente stampata.

In particolare, per gli acquisti in negozio:
- non perdere mai di vista la persona (il commesso) alla quale si consegna la carta;
- non conservare mai il PIN (numero segreto) insieme alla carta;
- molte banche offrono bancomat che possono essere usati anche come carta di credito. In caso di smarrimento o furto, occorre telefonare immediatamente al numero verde specifico -che e' bene sempre avere con se'- per bloccare la carta;
- conservare le ricevute del pagamento fino all'arrivo, al proprio domicilio, dell'estratto conto;

Per gli acquisti su internet:
Rappresentano il piu' diffuso e tipico utilizzo delle carte di credito, e sono indubbiamente vantaggiosi, rispetto ai canali di acquisto tradizionali, sia in termini di comodita' che di varieta' di scelta e di velocita'.
Benche' diano la sensazione di essere sempre e comunque molto rischiosi, in realta' sono relativamente sicuri a

patto di rispettare determinate "regole":

- e' bene acquistare on line solo su siti ad alto standard di sicurezza, protetti dai sistemi di sicurezza internazionali: SSL (Secure Socket Layer) e SET (Secure Electronic Transaction). Simboli riconoscibili dalla certificazione e dal lucchetto che appare sulla schermata del computer. Questi siti garantiscono la trasmissione sicura dei dati, che sono crittografati e non possono essere decifrati dagli "hackers";
- trasmettere i dati economici solo quando sono rispettate le condizioni di sicurezza e non comunicare mai i riferimenti della carta o altre informazioni personali via e-mail;
- verificare che il "negozio on line" sia un esercizio reale e non solo virtuale, che indichi tutti i dati utili per l'identificazione, compreso l'indirizzo.
- stampare (o memorizzare) una copia dell'ordine con i dati del venditore, il nome dell'azienda e l'indirizzo geografico della sua sede sociale, le condizioni generali di vendita, le modalita' per esercitare il diritto di recesso e la descrizione dei singoli beni o servizi venduti;
- nell'incertezza, e' meglio inviare una mail all'indirizzo del sito per ottenere maggiori informazioni e garanzie di affidabilita' del servizio;
- prendere sempre nota dell'indirizzo del sito;
- porre particolare attenzione alle condizioni di pagamento, per non incorrere in una sottoscrizione inconsapevole di un abbonamento con ripetuti addebiti mensili;
- diffidare o, per lo meno, porre molta attenzione alle offerte incredibilmente vantaggiose rispetto al prodotto venduto;

Se gli acquisti sono frequenti
In caso di acquisti in rete frequenti, e' bene dotarsi 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 per ogni transazione si utilizzasse una carta di credito differente. Un altro metodo alternativo di pagamento e' il denaro elettronico, tramite i pagamenti 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 hanno il vantaggio di richiedere la trasmissione dei dati relativi solo ad una piccola somma.

FURTO O SMARRIMENTO: COSA FARE
E' innanzitutto opportuno, e obbligatorio, **presentare denuncia all'autorita'** (polizia, carabinieri, etc.). Dell'accaduto va anche avvisata la societa' emittente (la banca, il circuito interbancario, etc.), chiamando il numero verde fornito con la carta o comunque seguendo le istruzioni che la stessa prevede in questi casi, **chiedendo il blocco immediato della carta.** Se il furto o la perdita riguarda una carta di credito di solito e' richiesta la ripetizione della comunicazione entro 48 ore tramite raccomandata a/r, allegando copia della denuncia (che va comunque conservata per almeno un anno).

Fatta la comunicazione la responsabilita' di ogni eventuale utilizzo e' della banca (o posta/finanziaria/circuito interbancario), e il possessore danneggiato deve essere rimborsato per intero.

Per gli utilizzi e prelievi effettuati PRIMA della comunicazione il discorso e' piu' complesso. Si fa riferimento al D.lgs.11/2010 (art.12) che ha, conformemente alla raccomandazione della comunita' europea n. 97/489/CE, fissato una franchigia di 150 euro che rappresenta la massima perdita addebitabile al cliente fino al momento in cui inoltra la comunicazione di perdita o furto alla societa' emittente. La condizione e' che lo stesso si sia comportato in buona fede, abbia custodito con diligenza la carta e l'abbia utilizzata prendendo tutte le precauzioni possibili, rispettando le norme di sicurezza previste dal contratto. Se c'e' stato da parte del titolare della carta un comportamento fraudolento, doloso o una colpa grave, il rimborso puo' essere rifiutato.

E' interessante in merito una pronuncia dell'ABF (Arbitro Bancario Finanziario) n.4085 del 26/7/2013, secondo la quale la colpa grave di verifica quando la condotta e' consapevolmente contraria alle regole di correttezza e buona fede, oppure totalmente irrispettosa delle regole di normale prudenza correttezza e buona fede. Non vi rientra il caso in cui la truffa sia stata subita per comportamento approssimativo, poco attento o poco scaltro, come quello di merito, dove una signora e' stata derubata della carta alla cassa di un supermercato dalla cassiera, e dato che le era stata ri-consegnata una finta carta simile alla propria, sul momento non vi aveva fatto caso e si era accorta del

furto dopo qualche giorno.

Se si notano utilizzazioni dubbie o non riconosciute soltanto nel momento della lettura dell'estratto conto, occorrera' comunque muoversi come gia' detto contestando lo stesso entro 60gg dal suo ricevimento, tramite reclamo da presentare a mano o da inviare per raccomandata a/r , sempre allegando la denuncia presentata alle autorita'.

UN CASO PARTICOLARE: LA CLONAZIONE DELLA CARTA
La clonazione, ovvero la duplicazione della carta (di credito o bancomat), e' meno frequente dello smarrimento e del furto, ma negli ultimi anni si sta evolvendo ed espandendo, diventando sempre piu' insidiosa.

La tecnica piu' diffusa di clonazione e' l'applicazione di un lettore magnetico a quello presente sugli sportelli ATM di prelievo contanti, abbinato ad una microtelecamera che riprende il codice segreto digitato o ad una finta tastiera applicata su quella dello sportello. Per carpire il codice viene anche utilizzata la tecnica del "finto aiuto" offerto -per esempio- dalla zelante persona che era in attesa dietro di noi dopo che la carta e' stata trattenuta dall'apparecchio. Non di rado gli apparecchi clonatori, detti "skimmer", vengono invece utilizzati manualmente dai negozianti, che tenendoli nascosti nella mano riescono a carpire i dati della carta senza che noi ce ne accorgiamo, mentre stiamo pagando. L'ultima "novita'" e' l'installazione degli skimmer direttamente dentro i POS dei negozi (gli apparecchi utilizzati per leggere le carte) da parte di truffatori che si introducono di notte nei locali senza lasciare traccia del loro passaggio. Di giorno, poi, durante le transazioni, i dati delle carte via via utilizzate vengono carpiti tramite un computer collegato attraverso sistemi di comunicazione senza fili, i Bluetooth.

La procedura da seguire nel caso si sospetti una clonazione e' la stessa del furto e smarrimento, ovvero va presentata denuncia e inoltrata richiesta di blocco al gestore della carta, attenendosi alle disposizioni dello stesso.

La caratteristica fortemente negativa della clonazione e' che il titolare si accorge spesso molto in ritardo di esserne rimasto vittima, perche' la carta rimane nelle sue mani e -a meno che non sia attivo il servizio di comunicazione via SMS degli utilizzi- tutti gli addebiti fraudolenti vengono rilevati solo al momento in cui arriva l'estratto conto a casa. In questo caso il consiglio e' comunque di inviare tempestivamente, dopo aver fatto denuncia, un reclamo alla banca.

Anche in questo caso, se viene esclusa la responsabilita' del titolare della carta relativamente alla sua custodia e al suo utilizzo, vengono normalmente rimborsate tutte le cifre indebitamente prelevate da terzi. Cio' anche perche' la clonazione, tipicamente, e' un problema che ricade soprattutto sui gestori (la banca, tipicamente) e sulle "falle" dei loro sistemi di sicurezza. Le banche, tra l'altro, sottoscrivono a tal scopo delle coperture assicurative che rendono l'ottenimento del risarcimento generalmente "agevole".

Tuttavia, e' bene provvedere, al primo rifiuto, a contestare i prelievi indebiti in modo formale, con raccomandata a/r, chiedendo esplicitamente il risarcimento dei danni subiti.

Il contenuto della lettera varia caso per caso, ovviamente, ma il presupposto generale su cui poggiare la richiesta e' la dimostrazione di aver agito sempre con la massima diligenza nel custodire ed utilizzare la carta.
Per rafforzare l'ipotesi della clonazione, inoltre, sarebbe bene poter evidenziare l'improbabilita' che gli utilizzi siano riferiti agli utilizzatori abituali della carta, per esempio esibendo estratti conto dove, a distanza di poco tempo, vengono riportati utilizzi fatti in luoghi molto lontani l'uno dall'altro. Come "prova", inoltre, si rivelano utili anche gli esiti delle indagini delle autorita' a cui si e' presentata denuncia. Non di rado, infatti, vengono rilevati sistemi di clonazione presso gli sportelli o scoperte truffe organizzate.
Per redigere la lettera come messa in mora clicca qui (http://sosonline.aduc.it/scheda/messa+mora_8675.php)

L'ARCHIVIO ANTIFRODE "SIPAF"
Il SIPAF (SIstema di Prevenzione Anti Frodi) e' l'archivio antifrode istituito dalla legge 166/2005 tenuto presso il Ministero delle finanze dove confluiscono tutte le segnalazioni riguardanti carte di credito clonate, utilizzi di carte non riconosciuti e denunciati, negozi dove si sono verificate frodi e/o ai quali sono state revocate le concessioni per l'utilizzo delle carte, sportelli bancomat manomessi, etc.

Le segnalazioni sono effettuate dalle banche e dagli intermediari finanziari che emettono le carte e gestiscono le

reti commerciali, con lo scopo di prevenire frodi. Gli stessi soggetti, infatti, possono consultare l'archivio. I dati possono inoltre essere scambiati anche con la Banca d'Italia.

Recentemente il Garante della privacy (con parere del 12/7/2012) ha approvato l'accesso a questo archivio da parte delle forze di polizia nell'ambito di indagini su reati connessi in qualche modo all'utilizzo di carte di credito o altri mezzi di pagamento.

LINK UTILI
- Consigli e suggerimenti della polizia: clicca qui (http://www.poliziadistato.it/articolo/241/)
- Sito utile per la sicurezza delle transazioni via Internet creato dalla Polizia in collaborazione con E-bay: clicca qui (http://www.compraconbuonsenso.it)
- Sito di consigli di sicurezza utile anche per presentare segnalazioni on-line: clicca qui (http://www.commissariatodips.it)

Ha collaborato Katia Moscano