Skimming: la clonazione fraudolenta di carte di credito e bancomat, in aumento a causa di gruppi cri

Data: 1 febbraio 2012 | Autore: Redazione

LECCE 2 GEN. 2012 - Skimming: la clonazione fraudolenta di carte di credito e bancomat, in aumento a causa di gruppi criminali organizzati. Probabile un’impennata del fenomeno con le nuove norme sulla tracciabilità e sul divieto di pagamento in contanti delle pensioni, introdotte dalla Manovra finanziaria “Salva Italia”. Come difendersi[MORE]

Con la dichiarata volontà del governo di ridurre al minimo i pagamenti in contatti, con la riduzione della soglia a 1.000 euro per l’acquisto di qualsiasi bene o servizio a fine di garantirne la tracciabilità e la norma che non consentirà il pagamento in contanti per le pensioni superiori a mille euro, una delle assai probabili conseguenze sarà, senz’alcun dubbio l’aumento del ricorso a bancomat e carte di credito.

Tali forme di pagamento elettronico, anche se assicurano la certezza della tracciabilità e la comodità di ridurre o non portare contante nel portafogli, si scontrano con un fenomeno che nel Nostro Paese, come nel resto dell’UE è in forte aumento: lo skimming, ossia la fraudolenta clonazione di carte bancarie.

La crescita di questa tendenza criminale non sarebbe dovuta solo a singoli ed isolati hackers ma, secondo quanto è dato appurare da numerose inchieste anche di livello europeo a rubare i contenuti delle bande magnetiche e i codici di accesso sarebbero soprattutto gruppi criminali organizzati.

E se la tendenza dello skimming è in crescita da anni, secondo Giovanni D'Agata componente del Dipartimento Tematico Nazionale "Tutela del Consumatore" di Italia dei Valori e fondatore dello "Sportello dei Diritti", con le misure dell'ultima manovra "Salva Italia", potrebbe subire un'impennata a causa del coinvolgimento di milioni di nuovi soggetti, e tra questi la maggior parte anziani e quindi più vulnerabili, che potrebbero essere costretti all'utilizzo di carte di pagamento elettroniche.

Il termine "skimming" deriva dal verbo inglese to skim, che vuol dire "sfiorare, strisciare". Da questa parola discende la parola skimmer che è il congegno elettronico utilizzato per memorizzare i contenuti delle bande magnetiche delle carte di pagamento. Negli sportelli automatici ATM (Automated Teller Machine), meglio noti come sportelli bancomat sono i dispositivi usati per leggere le relative carte elettroniche di pagamento e, quindi, abilitare l'utente alle operazioni richieste dopo aver effettuato l'ulteriore verifica del PIN (Personal Identification Number) che, pur presente in modalità cifrata all'interno della banda magnetica della carta, viene digitato direttamente dall'utente dopo aver inserito la Card nello Skimmer.

L'uso improprio di questi dispositivi, la loro manomissione, fino ad arrivare addirittura alla sostituzione dello skimmer originale con uno appositamente installato per leggere e registrare i contenuti delle carte magnetiche che vengono fatte "strisciare" al suo interno, ha determinato lo sviluppo di una nuova tecnica criminale chiamata, come detto, skimming, termine poi utilizzato anche per descrivere in generale le truffe compiute ai danni di possessori di carte di credito, bancomat, carte prepagate etc. attraverso un utilizzo illecito di dispositivi di lettura delle stesse (skimmer e P.O.S.).

Si tratta di un fenomeno organizzato, sia in termini tecnici che logistici. Ad essere coinvolti sono bande di criminali che si muovono in tutta Europa, non solo rumeni e bulgari, anche se questi pare siano i più avanzati e strutturati.

Ad essere colpiti sono bancomat, terminali per il pagamento con carta di credito posti in ogni luogo possibile, dai supermercati ai distributori di biglietti nelle stazioni. Ad aver contribuito all'aumento dei casi di sottrazione di dati in Europa, è la semplicità con la quale si possono ottenere dispositivi per skimming anche attraverso la rete.

Per la diffusione globale di questi strumenti di pagamento, il problema riguarda inevitabilmente tutti i paesi industrializzati, e secondo le statistiche quelli più colpiti sarebbero proprio l'Italia e la Francia. I dati in possesso sono notevoli e dimostrano la tendenza in aumento del fenomeno: nel 2009 sarebbero stati manomessi, 82 bancomat, 191 nel 2010 fino ad arrivare a ben 265 nei soli primi

quattro mesi di quest’anno!
Anche a causa dei costi annuali stimati che sfiorerebbero il mezzo miliardo di euro per i reati finanziari commessi in Europa tramite gli sportelli automatici, ENISA (European Network and Information Security Agency - agenzia europea per la sicurezza delle reti e dell'informazione) raccomanda agli utenti di essere maggiormente consapevoli dei rischi e di adottare le necessarie precauzioni per evitare di rimanere vittime di tali reati. Ma vediamo quali sono i consigli utili per difendersi, se proprio non si può fare a meno di un bancomat o di una carta di credito.

Per quanto riguarda le carte di credito al fine di saperne in tempo reale l’utilizzo, i gestori hanno previsto la possibilità di attivare un’opzione d’invio di un sms ogni volta che si effettua un’operazione con la carta o almeno se si supera una determinata soglia di pagamento. È superfluo, affermarlo, ma è uno dei migliori sistemi di monitoraggio e controllo unitamente alla verifica costante dei propri estratti conto anche on line.

In caso di furto o smarrimento, o comunque quando si abbia il sospetto che la carta sia stata utilizzata impropriamente la prima cosa da fare, è di procedere immediatamente al blocco della stessa recandosi presso la propria banca, oppure contattando direttamente i numeri verdi del circuito bancomat o del circuito carta. Se la carta è multi servizi ossia è abilitata anche alle funzioni bancomat e pagobancomat è necessario, in caso di furto o smarrimento, procedere alla chiamata di entrambi i numeri verdi.

Successivamente, è necessario effettuare una apposita denuncia penale presso l’Autorità di Pubblica Sicurezza (Polizia, carabineri, Finanza, ecc) e quindi inoltrare una conferma della richiesta di blocco (già effettuata al numero verde), tramite lettera raccomandata alla propria banca, allegando copia della suddetta denuncia.
Sino a che non si effettua il blocco, si corre il rischio che tutti i prelevamenti e gli addebiti restino a carico del titolare. Effettuato il blocco rimane a carico del titolare una franchigia che di solito corrisponde a 150 euro, ma in molti casi i gestori di carte non fanno pagare neanche quella.

In ogni caso, se ci si accorge soltanto nel momento della lettura dell’estratto conto di utilizzazioni illecite o non autorizzate della propria carta, entro 60 giorni dalla data di ricevimento dell’estratto occorrerà inviare un reclamo scritto, con allegata denuncia effettuata alla polizia.

Come previsto dal Testo Unico in materia bancaria e creditizia, D.Lgs. n. 385/93, come modificato dal D.Lg.s 342/99 che recepiva la Racc. n. 489/97 CE, in mancanza di opposizione scritta da parte del cliente, gli estratti conto e le altre comunicazioni periodiche alla clientela si intendono approvati trascorsi sessanta giorni dal ricevimento.

In caso di esclusione di qualsiasi responsabilità del titolare nell’uso fraudolento della carta, gli importi relativi vengono in genere riaccreditati dalla società emittente.

L’ultima difesa per i malcapitati truffati nel caso in cui venga scoperto il responsabile - essendo lo skimming un’attività idonea ad integrare gli estremi della figura di reato prevista dall’art. 12 del D.L. 143/91, convertito nella Legge 197/91 - è quella di perseguirlo in sede penale costituendosi parte civile nel relativo giudizio sperando di poter essere risarciti in quella sede.

(notizia segnalata da giovanni d'agata)