**CARTE DI PAGAMENTO: DIFFUSIONE E OPERATIVITÀ**

| DATI (in migliaia) | 2008 | Var. % 08/07 |
|---|---|---|
| Carte di credito attive | 16.089 | -0,7% |
| Numero operazioni | 522.607 | +3,71% |
| Carte di debito abilitate Pos | 37.064 | +11,98% |
| Numero operazioni | 522.607 | +3,71% |
| Carte prepagate | 8.208 | +41,4% |
| Numero operazioni | 72.557 | +46,37% |

Fonte: Banca d'Italia e Poste Spa.


Foto Francesco Bianchi

L'esercente può essere pagato con carte di credito clonate, rubate o contraffatte e può subire la manomissione del Pos, ma può mettere in pratica una serie di accorgimenti per evitare gli illeciti. Primo fra tutti: essere sempre vigile ed effettuare tutti i controlli necessari

*di Sergio Redaelli*

# Occhio alle frodi con la moneta elettronica

Attenti al rischio di truffe attraverso carte di credito e bancomat. Il problema riguarda tutti gli operatori commerciali ed è fortemente sentito dai consumatori, dal sistema bancario, dalle aziende che emettono le carte di credito e dalle forze di Polizia che sono tenute a contrastarlo. «Naturalmente non è tanto coinvolto il bar dove si beve il caffè e si paga con gli spiccioli - spiega il vicequestore aggiunto Sabrina Castelluzzo, responsabile della sezione crimini informatici della Polizia Postale e delle Comunicazioni a Roma -. Se parliamo di carte di credito clonate, dobbiamo pensare a pubblici esercizi misti, bar tabaccherie dove si possono fare anche gli acquisti, ricevitorie e bar ristoranti o pizzerie dove c'è un conto da pagare. È bene fare attenzione. È importante aggiornare e controllare gli strumenti in dotazione e apportare gli accorgimenti necessari a limitare il fenomeno delle clonazioni e delle truffe via etere e via telefono».


*Per verificare che il Pos non sia stato manomesso controllate l'integrità del sigillo di sicurezza (nella foto a sinistra).*

**SFIORATI 800 MILIONI DI PAGAMENTI CON I BANCOMAT**

| DATI | 2008 | 2007 |
|---|---|---|
| Operazioni di pagamento su Pos con PagoBancomat (milioni) | 768 | 750 |
| Numero Pos attivi PagoBancomat (migliaia) | 1.180 | 1.000 |
| Numero carte Bancomat / PagoBancomat (milioni) | 28,5 | 28 |

Fonte: Abi.

## La piaga della clonazione

Di solito, per clonare le carte di credito si utilizza la tecnica dello skimming, cioè si copiano i dati contenuti nella banda magnetica, senza che il legittimo proprietario ne venga a conoscenza. Ciò avviene per mezzo di un lettore che all'atto di pagare con il Pos, strisciando la card nell'apposita fessura, cattura i dati della banda magnetica. Basta un registratore e il gioco è fatto: carpisce e immagazzina centinaia di dati che, in un secondo momento, vengono trasferiti su una carta di credito falsa con cui il truffatore mette a segno i suoi colpi. Come ci si può

## Quali controlli è bene effettuare

### sul Pos

Fate attenzione. Il terminale Pos potrebbe essere stato manomesso nel corso di un furto, reale o simulato, presso il vostro punto vendita. Controllate sempre che non sia stato violato il sigillo di sicurezza sul retro. Lo skimmer è diverso dal normale lettore Pos fornito dalle società emittenti. Per eseguire questo genere di frodi è necessario che il malintenzionato entri in possesso della carta di credito del cliente.

### sulla carta

Controllate sempre gli elementi di sicurezza della carta: le specifiche sul logo e sul design, la data di scadenza, la presenza della firma sul retro. Per esempio, la carta Visa senza microchip è autentica se compare una colomba uguale all'ologramma. La Mastercard ha in evidenza una M e una C. Sull'American Express deve comparire la scritta Amex. La Diners Club si riconosce dall'immagine del logo sulla sinistra.

### sullo scontrino

È utile controllare che il numero in rilievo sulla carta coincida con quello stampato sullo scontrino del Pos. I truffatori spesso utilizzano carte emesse regolarmente, alterando solo il contenuto della banda magnetica.

Fonte: "Dispensa informativa sugli standard di sicurezza presso gli operatori del commercio".

*in evidenza*

**TRUFFE**
Tra le frodi più diffuse, si segnala la clonazione delle carte di credito per mezzo di uno skimmer, ovvero un lettore che, all'atto di un pagamento, cattura i dati della banda magnetica con la "strisciata" della carta nel Pos.

**VERIFICHE**
Oltre a garantire l'inviolabilità del terminale Pos, il gestore dovrebbe prestare attenzione a comportamenti sospetti del titolare ed effettuare dei controlli nel momento in cui gli viene consegnata una carta di credito.

difendere? Ci sono Pos più o meno difficili da manomettere e carte di credito con codici di riconoscimento. Ma è sempre bene stare attenti a chi si da il compito di strisciare le carte.
Secondo un'indagine dell'Istituto per gli studi sulla pubblica opinione (Ispo), il 52% degli esercenti italiani vede di buon occhio l'uso del denaro elettronico per le transazioni sopra i 20 euro. Il 68% è convinto che in futuro i pagamenti saranno fatti quasi esclusivamente con le carte (l'81% tra quanti possiedono il Pos). Ma il pagamento elettronico ha determinato un calo delle rapine? «Difficile dirlo - risponde il vicequestore -. Probabilmente sono cambiate le modalità degli scippi, delle rapine e dei furti presso gli uffici postali e gli sportelli bancari».

## La prevenzione, la miglior cura

Per Luca Squeri, presidente della Commissione per la sicurezza e la legalità di Confcommercio, la riduzione del contante in cassa è in ogni caso il primo fattore di prevenzione. Non a caso Confcommercio ha ottenuto anche per il 2010 che i Pos rientrino fra gli "strumenti" finanziabili con il credito d'imposta. Ma ci sono dei ma. «Le commissioni d'esercizio possono arrivare al 2 o 3% - spiega -. Questo non facilita la diffusione del sistema per i piccoli importi (in altri Paesi si paga anche il caffè con la moneta elettronica) e per chi ha un margine di guadagno molto ridotto. Proprio nelle categorie più a rischio di rapine come le tabaccherie, i benzinai e i bar, l'utilizzo del denaro virtuale va incentivato e gli esercenti e clienti devono essere tutelati anche da possibili truffe. Ben vengano l'invio di sms al cliente ogni volta che viene eseguita una transazione e lo snellimento delle procedure "conciliative" fra le banche in caso di utilizzo improprio delle carte da parte di terzi». ■