

# VADEMECUM

per la **Sicurezza** nell'utilizzo  
della **Moneta elettronica**

**in collaborazione con la Polizia di Stato**  
Reparto Polizia Postale e delle Comunicazioni

che cosa sapere per effettuare prelievi,  
pagamenti o acquisti con bancomat  
e carta di credito in sicurezza



**BANCA POPOLARE di MAROSTICA**

**VERSIONE PER I COMMERCianti  
ED ESERCENTI**

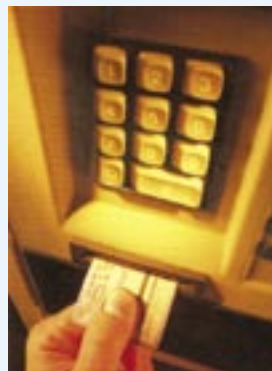
che cosa sapere per  
effettuare prelievi,  
pagamenti o acquisti  
con bancomat  
e carta di credito

La "moneta elettronica" ha oggi segnato un fondamentale passo avanti nella gestione delle transazioni economiche, raggiungendo un livello di diffusione che ne ha fatto lo strumento preferito di pagamento da parte degli italiani che lo considerano anche il più sicuro. Il mondo sta cambiando e cambia, ma ciò che non deve cambiare è la soglia di attenzione e prudenza che chiunque svolga una attività (commerciale o meno) deve avere, e allora l'uomo resta la prima ed indispensabile risorsa in termini di sicurezza, anche per ciò che riguarda l'utilizzo della moneta elettronica (Carte e POS).

### Il terminale (POS)

Il POS è un terminale elettronico che consente di effettuare in modo semplice e sicuro il pagamento delle vostre vendite usando le carte più diffuse. I vantaggi di questa tecnologia per il commerciante ed il cliente sono molteplici:

- i pagamenti sono sicuri perché tutti autorizzati e, per le carte di debito, protetti da un codice segreto (Pin);
- non si corrono rischi per via di assegni scoperti o di denaro falso, ed inoltre diminuisce la presenza del contante in cassa;
- diminuisce la gestione cartacea a carico del commerciante utilizzando la via elettronica garantendo la sicurezza dell'operazione;
- tutte le operazioni sono documentate dallo scontrino, stampato dal POS in automatico, che fa fede in caso di contestazioni.



### Le frodi con le carte di pagamento

#### Le carte clonate o false



Le tecniche per produrre Carte di credito clonate o per falsificarle sono molte e di diverso tipo, ma tutte hanno il medesimo scopo: impossessarsi illegalmente dei dati contenuti nella banda magnetica della carta. L'acquisizione illecita di tali dati può avvenire con differenti modalità: all'atto dell'esecuzione di operazioni presso gli sportelli bancomat, nel corso delle transazioni commerciali via internet, sottraendo in fase di spedizione l'estratto conto o la carta stessa inviata al titolare, utilizzando carte di credito rubate o smarrite, recuperando dati tramite gli scontrini di carte di credito gettati via incautamente dopo un acquisto, ecc.. una volta entrati in possesso dei dati o dell'originale, è possibile, da parte dei malintenzionati, duplicare (clonare) una Carta di credito od un Bancomat. È allora importante conoscere quali sono gli elementi fondamentali da verificare in caso di Carta clonata. Innanzitutto cercate sempre (anche se non avete sospetti) di verificare l'identità dell'acquirente, attraverso la richiesta di esibizione di un documento. Quando la Carta viene clonata significa che ne viene fatta una copia per cui il malfattore sa di avere poco tempo per utilizzare la Carta illecita, e che solitamente può effettuare un solo acquisto prima che il sistema rilevi la presenza di un duplicato, quindi non ha il tempo di "produrre" una Carta di Identità falsa che sia in grado di avvalorare la sua "nuova identità". La richiesta di un documento è il deterrente più efficace per scoraggiare il malintenzionato che a questo punto lascerà "di corsa" o con una scusa il vostro negozio.

#### La manomissione del POS

A volte accade che vengano manomessi i POS presenti in negozi, supermercati, ecc... E' già successo infatti che dei malintenzionati avessero simulato un furto, in realtà con l'obiettivo di manomettere il POS, inserendovi uno skimmer, in grado di memorizzare i dati della Carta. La tecnica dello skimming, un processo nel quale i dati contenuti nella banda magnetica di una Carta originale sono copiati in quella falsa, senza che il legittimo proprietario ne venga a conoscenza, avviene per mezzo di uno skimmer ovvero un "lettore" che, all'atto di un pagamento effettuato tramite terminale POS, è in grado di catturare i dati della banda magnetica con la semplice "strisciata" della Carta, nonché il Pin del Bancomat digitato, ed inviare questi dati anche in radio frequenza nelle prossimità del negozio dove magari vi è un complice. I dati copiati vengono in un secondo tempo trasferiti su un supporto plastico idoneo, che riproduce l'aspetto di una Carta di credito che poi verrà utilizzata per effettuare transazioni fraudolente.

#### La custodia: il controllo dei locali e l'infedeltà

Ogni esercente per l'installazione del POS sottoscrive con la propria Banca una specifica convenzione, con la quale si impegna a conservare e custodire con diligenza i terminali (apparecchiature e software) installati. La ragione di ciò è semplice: la sicurezza comincia prima di tutto da un comportamento di attenzione e prudenza. Per questo è opportuno verificare i locali e la presenza di apparecchiature "strane" magari vicino ai contatori od alla scatola dell'allarme. Inoltre è fondamentale consentire l'accesso alla cassa ed al terminale POS solo al personale di cui si ha fiducia e di cui si sono verificati i requisiti di onorabilità. Se il cliente dimentica lo scontrino della transazione custoditelo qualche giorno se pensate che ritornerà, se no distruggetelo in modo che non sia leggibile. Tale scontrino potrebbe diventare preda di malintenzionati che praticano la truffa cosiddetta trashing: consiste nella ricerca degli scontrini delle Carte che erroneamente vengono gettati via e che riportano il numero della tessera e altri dati sensibili, utilizzabili quindi magari per acquisti via internet!

### Il phishing

È una tecnica che consiste nell'inviare messaggi di posta elettronica o via fax, "mascherati" da messaggi ufficiali inviati da parte di una Banca o di un gestore di Carte di credito, dove vi si chiede l'invio di dati relativi a transazioni effettuate nel vostro punto vendita, come ad esempio: fotocopia delle Carte di credito, dati anagrafici dei titolari, copie dei documenti di vendita. Banche e gestori delle Carte o gli enti potrebbero richiedere l'invio di documenti di vendita agli esercenti convenzionati ma non richiedere certo l'invio dei dati dei relativi ai titolari delle Carte, né le fotocopie delle Carte stesse. A questi messaggi non bisogna assolutamente rispondere. Piuttosto verificate l'indirizzo da cui provengono le richieste quindi chiamate l'assistenza (Banca od il gestore delle Carte) o chiamate le Forze dell'ordine, avendo l'accortezza di non cancellare l'e-mail ricevuta e di conservare il fax di richiesta.



### La prevenzione delle frodi: cosa fare

#### La verifica dell'identità

Il commerciante non deve avere timore di chiedere in fase di perfezionamento dell'acquisto ed in presenza di un cliente che non conosce, un documento di identità. Poter verificare la corrispondenza del nome e dei dati tra la carta di pagamento e il documento esibito, oltre ad essere un efficacissimo deterrente nei confronti di malintenzionati, consente di prevenire spiacevoli conseguenze. In caso di dubbi sull'identità (ad es. la firma si discosta da quella della Carta) l'esercente dovrà annotare gli estremi del documento sul retro dello scontrino dal POS.

#### La verifica del POS: quali controlli

Nel caso in cui venga manomesso il lettore POS (inserimento di una "memoria"), i malviventi sono costretti ad entrare due volte nell'esercizio commerciale, prima per inserire e in seguito per "scaricare" i dati. Anche se ultimamente esistono "circuiti" provvisti di un modulo GSM, in grado di trasmettere quanto catturato (in tempo reale, tramite SMS) all'esterno o nelle vicinanze del punto vendita. Quindi quando si entra in negozio la prima cosa è verificare la posizione del terminale POS, si trova dove l'avete lasciato? Può essere utile stabilire un posto fisso ed una posizione sul piano dove riporlo a fine giornata, ci aiuterà a capire se è stato mosso. Se avete dei dubbi, verificate subito il sigillo di sicurezza se è intatto o se magari è stato sostituito. È possibile utilizzare una ulteriore tecnica di protezione come quella di apporre in un punto del bordo di congiunzione fra il coperchio ed il fondo un ulteriore vostro sigillo (magari un adesivo con il vostro logo): una volta rotto i malfattori si troveranno in difficoltà nel sostituirlo e voi potrete facilmente capire se il terminale è stato aperto. Nel caso riscontriate anomalie o avete dubbi avvisate subito la Banca e le Forze dell'ordine.

#### *Una visita ingannevole per la manutenzione del POS*

*Sono capitati casi in cui o senza preavviso o con una falsa telefonata di preavviso un certo giorno si è presentato nel punto vendita un tecnico della manutenzione per effettuare presunti interventi di manutenzione. In questi casi è sempre bene verificare presso l'assistenza con una telefonata di controllo. In caso di dubbi sull'identità del presunto tecnico avvertire anche le Forze dell'ordine.*

#### La verifica della carta di pagamento

Il commerciante dovrebbe sempre prestare attenzione ad un eventuale comportamento sospetto del titolare della Carta ed effettuare dei controlli nel momento in cui gli viene consegnata una Carta per il pagamento di un acquisto. In particolare l'esercente deve assicurarsi della genuinità della Carta attraverso l'esame degli elementi di sicurezza presenti sulla Carta, quali ad esempio:

- specifiche sul logo e sul design,
- data di scadenza,
- presenza della firma sul retro.

Qui sotto descriviamo alcuni tipi di controllo effettuabili direttamente dal negoziante sulla Carta di pagamento e che lo rendono in grado di capire se la Carta è originale o falsificata.



#### I controlli visivi

Alcuni controlli possono essere eseguiti maneggiando la Carta e prestando attenzione ai segni distintivi e caratteristici. Controllate la presenza dei caratteri speciali in rilievo. I caratteri speciali "MC" nel caso di Mastercard, e "V" in Visa sono difficili da copiare in quanto stampati in rilievo con caratteri particolari. Nel caso delle Carte Visa o Mastercard le prime quattro cifre in rilievo devono coincidere con quelle stampate in piccolo sotto. Qualora non sia presente questa forma di microscrittura la Carta può essere considerata falsificata. È poi importante verificare che nello spazio riservato alla firma

sia presente una microscrittura diagonale in colori diversi, inclinata di 45° da sinistra a destra, che riproduce la dicitura del circuito d'appartenenza (Visa e Mastercard). Devono essere riportati, inoltre, incisi, il codice completo della Carta di credito o solo le ultime quattro cifre. Ad una certa distanza dal codice Carta dovrà essere riportato un codice numerico di tre cifre, detto CVV2 (per Visa) o CVC2 (per Mastercard).



### I controlli dell'ologramma e della fluorescenza

Le Carte di pagamento Visa e Mastercard presentano un importante elemento anticontraffazione e di sicurezza: l'ologramma. Questo tipo di stampa, così particolare, non può essere imitata pena un risultato scadente facilmente riconoscibile come una imitazione. Se siete in possesso di una Lampada di Wood ad ultravioletti, magari acquistata per la verifica delle banconote, potrete ulteriormente controllare che sulla Carta vi siano scritte o simboli fluorescenti. Sulla Carta Visa è una colomba, sulla Mastercard compaiono le lettere M e C, sulla Carta American Express compare la scritta AMEX e sulla Carta Diners l'immagine del logo posto sulla sinistra. L'assenza di questi elementi deve generare sospetti sull'originalità della Carta.

### Ulteriori controlli

E' fondamentale anche controllare che il numero della Carta corrisponda al numero che compare sullo scontrino emesso dal POS. I truffatori spesso utilizzano Carte rubate, emesse regolarmente, alterando solo i dati presenti nella banda magnetica. Se i numeri non corrispondono, la Carta di pagamento non è regolare.

### Sicurezza dei locali: sistemi di allarme e assicurazioni

Dotarsi di adeguate misure di sicurezza preventive è oggi indispensabile. Porte blindate, sistemi di allarme, videosorveglianza, cassaforte (in cui riporre il POS a fine giornata) ecc. sono efficaci deterrenti per i malintenzionati che intendono manomettere il POS. E' utile anche disporre di una assicurazione.

### Vendite on-line e sicurezza nell'e-commerce

#### La sicurezza del negozio on-line

La Carta di credito è lo strumento più utilizzato nelle transazioni on-line. Quando "si apre" un negozio on-line bisogna innanzitutto accertarsi che: il provider presso i cui server è posizionato il "negozio" ci garantisca la massima affidabilità in termini di sicurezza software, e di scegliere un applicativo di gestione a prova di "hacker". Molte Banche e molti Gestori di Carte dispongono di soluzioni applicative funzionali e altamente sicure che utilizzano codifiche di sicurezza praticamente inespugnabili. In questo caso le truffe che possono accadere rappresentano una eventualità remota, se ci si comporta con la indispensabile attenzione.

Di seguito alcuni accorgimenti che possono essere utili nel caso in cui si pratichi il "commercio elettronico", cioè la vendita on-line via internet.

#### Attenzione all'hacking

Attività praticata da pirati informatici che cercano di violare i database di chi vende servizi o prodotti via internet, per accedere ai numeri delle Carte di credito memorizzati durante la transazione o la registrazione (accreditamento) presso il negozio. Questo tipo di truffa solitamente non funziona a fronte di protezioni informatiche efficaci (firewall ed antivirus) e se non vi è il "contributo" di un basista all'interno.

#### Le password

La gestione di un negozio on-line presuppone l'utilizzo di password (parole chiave segrete). È importante che teniate segrete le vostre password e che le cambiate periodicamente. Una password costituita da frasi o parole facilmente intuibili è una password a rischio, quindi create la password componendola con le iniziali di una frase che vi possa facilmente richiamare alla memoria una situazione familiare nota soltanto a voi, soprattutto non utilizzate i vostri dati anagrafici! Memorizzate le password e comunque, se le scrivete, non lasciatele in posti facilmente accessibili.



#### Il Database ed il file clienti

Conservate copia cartacea di tutti i documenti generati dalla procedura di pagamento e custoditeli sotto chiave insieme ai dati dei vostri clienti e delle loro Carte di pagamento. Se ricevete richieste via e-mail sospette chiamate l'assistenza del Gestore: si tratta di "phishing".