

VADEMECUM

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

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



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

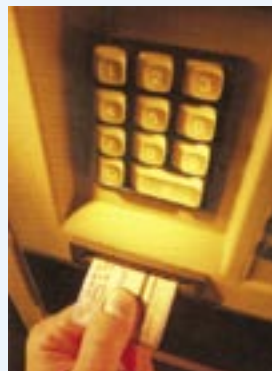
che cosa sapere per effettuare prelievi,
pagamenti o acquisti con bancomat
e carta di credito in sicurezza



BANCA POPOLARE di MAROSTICA

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

La moneta elettronica (Bancomat, Carte di Credito, transazioni on-line.... ecc.) ci fa risparmiare tempo, è comoda, semplice da utilizzare ed ha migliorato la nostra vita quotidiana. Ecco alcune semplici regole che rendono il suo utilizzo oltre che pratico, sicuro. Negli ultimi anni lo sviluppo della tecnologia e soprattutto della tecnologia informatica ha portato una vera e propria rivoluzione nella nostra vita, basti pensare all'avvento del telefonino, che ha permesso di annullare le distanze, e ha dato un impulso senza precedenti alla vita di relazione. Come per ogni cosa anche per la moneta elettronica ciò che fa la differenza è il nostro modo di "viverla" ed usarla. Certo nessuno potrebbe oggi immaginare la propria vita senza Bancomat, Carta di Credito ed anche Internet, che per molti è oggi uno strumento indispensabile di lavoro, ma non dobbiamo sottovalutare che la comodità non ci dispensa dall'applicare quelle minime regole di attenzione e prudenza, che ci garantiscono sicurezza. Nell'utilizzo della moneta elettronica se non ci comporteremo con la necessaria avvedutezza potremo più facilmente essere oggetto delle possibili truffe di malintenzionati. La casistica delle situazioni di rischio è comunque estremamente limitata e facilmente prevedibile: la clonazione delle tessere magnetiche (la duplicazione illegale del nostro Bancomat e/o Carta di Credito), l'alterazione del Pos (lo strumento che trovate nei punti vendita e negozi e che legge i dati presenti nella banda magnetica delle carte di pagamento), la manomissione (spesso ben camuffata) degli Atm (postazioni di prelievo dei contanti mediante tessera Bancomat), i raggiri. Le Forze dell'ordine hanno in questi anni dato vita ad una sempre più stretta collaborazione con l'ABI (Associazione Bancaria Italiana) e con gli Istituti di credito al fine di prevenire e circoscrivere tali fenomeni. Esiste anche il supporto di una banca dati a livello europeo che raccoglie informazioni sulle Carte di Credito clonate o comunque illegali, ed un nucleo di indagine comunitario specializzato che permette, in brevissimo tempo, di attivare una collaborazione con gli altri Paesi europei per effettuare ricerche ed azioni coordinate di intervento.



Bancomat e Carta di Credito



Se la Carta viene recapitata a casa per posta, controllate che le buste siano integre e che provengano dalla vostra Banca (o da chi emette la Carta di Credito). Analoga attenzione va riservata alla busta contenente il codice segreto Pin (personal identification number). Verificate attentamente che non vi siano manomissioni anche all'interno della busta. Diffidate di buste bianche inviate con posta prioritaria o con francobolli perché solitamente l'invio avviene con buste con tassa prepagata. Va posta attenzione anche alla regolarità di arrivo dell'estratto conto. Se arriva tardi insospettitevi perché potrebbe essere stato sottratto "temporaneamente" per impadronirsi dei dati che in esso sono contenuti (ad es. il numero della Carta di Credito). In questo caso controllate i movimenti del conto. Questo tipo di raggio si chiama "boxing".



Le 10 regole d'oro

Prima di affrontare nel dettaglio come e cosa fare per prelevare e pagare in sicurezza con la moneta elettronica e quali sono i rischi ai quali potenzialmente siamo esposti se non utilizziamo attenzione e prudenza, riassumiamo qui sotto le 10 regole d'oro che ci consentiranno di usare Bancomat e Carta di credito senza rischi ed in sicurezza:

- 1 Duplicare e conservare copia, in luogo sicuro, di tutti i documenti personali (compresi gli estremi del Bancomat e delle Carte di Credito ecc., dati che andranno indicati nella denuncia in caso di furto o smarrimento) e quelli delle proprietà, sarete quindi facilitati nel dover disporre delle informazioni in caso di necessità e di emergenza.
- 2 Conservare con cura le tessere, soprattutto tenetele lontano da fonti magnetiche ma anche da altre tessere o elementi metallici: eviterete così il rischio della smagnetizzazione ed i rischi di graffiare la banda magnetica, e la conseguente necessità di sostituzione della stessa.
- 3 Non conservare mai il Pin (codice segreto) insieme alla tessera (Bancomat o Carta di Credito abilitata al prelievo).
- 4 Conservare i numeri telefonici (in genere numeri verdi attivi 24 ore su 24) forniti dall/i gestore/i della/e tessera/e indispensabili per attivare la procedura di blocco a seguito di furti e smarrimenti; se la Carta di Credito prevede la funzione Bancomat la segnalazione andrà fatta anche al relativo numero verde.
- 5 Chiedete sempre l'identità del vostro interlocutore; sappiate che i mistificatori si possono nascondere ovunque.
- 6 Controllate sempre gli estratti conto forniti dalla società di gestione delle card (tessere). Non lasciate in giro o abbandonate le copie contabili di pagamenti e prelievi ancora leggibili, strappatele accuratamente se le gettate nella spazzatura.
- 7 Evitate di fornire il numero delle tessere Bancomat o Carta di Credito, soprattutto ad interlocutori telefonici.
- 8 Imparate l'ubicazione degli uffici delle Forze dell'ordine.
- 9 Denunciate immediatamente il furto o lo smarrimento delle Carte di Credito, dei libretti degli assegni e del libretto della pensione e di tutti quei documenti che possono essere oggetto di contraffazione e di illecita e immediata utilizzazione.
- 10 Avvaletevi di forme assicurative, depositi di sicurezza e ogni altro mezzo atto alla diminuzione del pericolo e del danno derivante dalle iniziative di malintenzionati.

Se vi accingete a prelevare del contante presso un Atm (postazione Bancomat) vi suggeriamo di:

Prelevare e pagare con il Bancomat



- ⚠ • accertare che nelle immediate vicinanze non vi siano persone ferme in atteggiamento sospetto, magari con telecamere;
- ⚠ • osservare sempre attentamente l'apparecchiatura che non deve presentare anomalie o modifiche o sporgenze (se prelevate spesso o sempre nello stesso Atm, sarà più facile notare la difformità). Scrutate che non vi siano micro telecamere ad altezza della tastiera o "oggetti strani" attaccati nei pressi (ad es. sulle pareti, se la postazione è al chiuso);
- ⚠ • verificare la bocca della fessura: la fessura dove va inserita la carta Bancomat deve essere ben salda e non muoversi. La tessera deve poter essere inserita nell'apposita fessura dello sportello senza alcuno sforzo. Se si muove o si stacca potrebbe significare che è stata "coperta" con uno "skimmer" (vedi più avanti). All'atto della restituzione, la tessera deve poter essere facilmente afferrata con le dita senza particolare difficoltà;
- ⚠ • controllare che la tastiera dell'Atm sia ben fissata perché vi potrebbe essere una tastiera falsa posizionata proprio sopra quella dell'Atm, con lo scopo di catturare il codice Pin. In tale evenienza ci si accorgerà perché la tastiera non è a livello del piano e presenta un piccolo gradino di circa un paio di millimetri;
- ⚠ • quando digitate il Pin, nascondere la mano che digita con l'altra in modo che nessuno possa leggere il vostro Pin;
- ⚠ • se avete anche il minimo dubbio, non introdurre la tessera e tanto meno digitare il Pin. Se la banca è aperta avvisate il personale, altrimenti chiamare le Forze dell'ordine;
- ⚠ • fare attenzione ai pagamenti con il Bancomat tramite Pos (lettore della tessera presente nei negozi e nei supermercati, pompe di benzina ecc..) se vi dicono che il Pos è in un'altra stanza, non lasciate che facciano l'operazione senza che voi siate presenti, offritevi di accompagnare la persona a cui avete data la tessera;
- ⚠ • se avete il dubbio di essere osservati, fermarvi e riflettere o parlarne con chi vi accompagna o con chi effettua il servizio di vigilanza;
- ⚠ • se avete sospetti, contattare il personale della banca. In orari di chiusura degli sportelli contattate le Forze dell'ordine, o se la tessera è bloccata in maniera irregolare nella fessura o ritenete che ciò che vi sta capitando non sia normale chiamate il Servizio Blocco della tessera. A volte è meglio affrontare qualche piccolo inconveniente come cambiare la tessera Bancomat piuttosto che essere vittima di una truffa.

Pagare o prelevare con la Carta di Credito

Come sempre la sicurezza deriva prima di tutto da uno stato di attenzione, ed anche nel caso dei pagamenti con la Carta di Credito, è bene osservare alcune semplici regole:



- ⚠ • non perdetela mai di vista. Dovete pretendere che al momento della transazione (cioè il passaggio della tessera nella famosa "macchinetta" che registra il pagamento, Pos) il negoziante, l'albergatore, il benzinaio, ecc. effettui lo "striscio" alla vostra presenza ed "a vista". Questo vale soprattutto nei paesi esteri dove sono stati segnalati casi in cui il negoziante porta la tessera nel retrobottega per effettuare la transazione e così può provvedere alla copia dei dati utili ai fini della clonazione;
- ⚠ • tutte le Carte di Credito sono dotate di un codice CSC o CVV2, che è un codice di sicurezza di tre o quattro cifre presente sul retro o sul fronte della Carta di Credito, senza questo codice la Carta di Credito è sicuramente una copia falsa. Questo dato è una forma di ulteriore controllo. Purtroppo questo codice di sicurezza, seppur presente su tutte le carte italiane, non è stato ancora completamente implementato dai gateway di pagamento del nostro Paese;
- ⚠ • controllate l'estratto conto: verificatelo puntualmente ogni mese, è l'unico modo per accorgersi di eventuali spese mai effettuate (soprattutto quando ci si reca all'estero);
- ⚠ • nel caso di addebiti impropri: se vi arriva un estratto conto con addebiti per spese che non avete fatto avvisate l'emittitore della tessera, la banca per conoscenza, e quindi denunciare alle Forze dell'ordine la clonazione della tessera, disconoscendo le spese addebitate;
- ⚠ • un capitolo a parte sono gli acquisti effettuati con Carta di Credito in internet. Nel caso di acquisti sul web dovete verificare che l'area del sito in cui state effettuando il pagamento sia sicura cioè sia visibile un "lucchetto" (simbolo che caratterizza la transazione protetta da un sistema di sicurezza) posto sulla parte inferiore dello schermo. In caso contrario non effettuate il pagamento perché si corre il rischio di vedersi rubare i dati personali e quelli della tessera;
- ⚠ • molte Carte di Credito consentono di prelevare contante dagli sportelli Atm, nel caso seguite quanto riportato al paragrafo precedente;
- ⚠ • se avete effettuato un acquisto od un pagamento con la Carta di Credito non gettate mai la ricevuta consegnatavi dall' esercente, ma conservatela con cura fino a che non abbiate controllato l'estratto conto del mese per verificarne l'esattezza.

Prelevare e pagare con la moneta elettronica sono ormai azioni che tutti compiono quotidianamente. Si calcola che ogni giorno siano decine di milioni le transazioni effettuate con la moneta elettronica, e solo una piccolissima percentuale è esposta a rischi. Il principio è molto semplice, 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 od effettuare altri tipi di truffe. È allora importante conoscere quali possono essere le situazioni nelle quali si corre il rischio che ci vengano sottratti i cosiddetti "dati sensibili" (il Pin ecc.) e le carte Bancomat, di Credito, ecc.. Infatti usando un po' di accortezza è possibile accorgersi rapidamente degli eventuali trucchi che un malintenzionato sta cercando di mettere in atto nei vostri confronti, ed agire prima che sia troppo tardi.



La clonazione: cioè il duplicato illecito (le fasi di una truffa)



Fig.1 Riuscite a vedere lo skimmer?

Clonare una Carta di Credito od un Bancomat significa in sostanza riuscire a "duplicare" la banda magnetica presente sulla tessera, ma se chi la duplica non conosce il Pin (codice segreto) non può utilizzarla. Il problema quindi non è di carattere tecnologico quanto piuttosto legato alla nostra disattenzione o ad un basso livello di protezione dei nostri dati personali e sensibili. Uno degli strumenti più utilizzati per clonare le carte è il cosiddetto "skimmer" (fig. 1), una specie di "lettore", dotato di memoria "eprom" (la memoria eprom è



Fig.2 Ecco!

un tipo di memoria veloce, inventata nel 1971 dalla Intel per immagazzinare programmi -firmware- per microprocessori), che cattura i dati della banda magnetica con la semplice "strisciata" della Carta di Credito/Bancomat su di esso. Lo skimmer è un congegno di dimensioni ridotte (fig. 2) e non ha una forma standard, solitamente è grande quanto un pacchetto di sigarette ed auto-alimentato con batteria e "immagazzina" i dati presenti nella banda magnetica: nome, cognome e data di scadenza



Fig.3 La microcamera è nel portadepliant

za della tessera, nonché l'invisibile codice di verifica trasmesso elettronicamente per confermare la validità della tessera stessa. Una volta che si collegherà lo skimmer ad un computer, munito di un programma specifico per bande magnetiche, potranno essere trascritti i dati, presi illecitamente, su un supporto plastico con le caratteristiche di una Carta di Credito/Bancomat.

invece del codice di identificazione della tessera, alcuni modi ricavabili dalla banda magnetica, la camera nascosta (fig. 3 e fig. 4) che filma la e che solitamente trasmette (fig. 5) il Pin in radio Ci si rende conto, quindi, che quando ci si accoppo' di attenzione controllando che non ci siano



Fig.5 La microcamera e trasmettente



Fig.4 Ecco la microcamera

Per impossessarsi del Pin, che non è in un solo colpo, i truffatori utilizzano generalmente una microte digitazione dei numeri del Pin (codice segreto) frequenza ad un ricevitore posto nelle vicinanze. cinge a prelevare presso un Atm basta fare un alterazioni o manomissioni

Le altre truffe

Vi sono altri tipi di frodi che è bene tener presente, ma anche queste possono essere neutralizzate con un po' di accortezza.

Trashing: consiste nella ricerca degli scontrini delle Carte di Credito (che riportano il numero della tessera e altri dati sensibili) che erroneamente gettiamo via dopo un acquisto! Bisogna sempre conservare la propria copia per verificare la regolarità dell'estratto conto e, appunto, per non fornire l'occasione ad altri di impossessarsi dei dati di identificazione della tessera.



Il **lebanese loop:** è una tecnica di manomissione dello sportello Atm (postazione Bancomat), infatti allo sportello di prelievo automatico viene applicato un dispositivo che, una volta inserita la tessera la trattiene in modo che il distributore non riesca più a restituirla. In tale situazione si resta solitamente perplessi, perché la tessera rimane "incastrata" e non si può completare la transazione né riavere indietro la tessera. In questo clima di sconcerto di solito "spunta" il truffatore che, fingendo di prestarvi soccorso, vi invita a digitare nuovamente il Pin, manovra che gli consente di spiare e memorizzare il codice segreto. Poi quando il proprietario della tessera Bancomat si allontana il truffatore stacca il dispositivo e recupera la tessera per poi utilizzarla con il Pin appena memorizzato.

