



LE GUIDE UTILI

GUIDA ALLA SICUREZZA DELLA MONETA ELETTRONICA

cosa sapere per
effettuare prelievi, pagamenti o
acquisti con bancomat,
carta di credito ed on-line
in sicurezza

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



2009 © Tutti i diritti riservati MTK srl www.metakomedizioni.it - Ufficio Studi e Ricerche - Vietata la riproduzione - Tutti i marchi riportati appartengono ai legittimi proprietari



GENTILE CLIENTE,



tutti, oggi, abbiamo in tasca, oltre al tradizionale libretto degli assegni, carte magnetiche o con microchip e strumenti che ci permettono di gestire il nostro denaro in modo semplice ed immediato e con facilità 24 ore su 24. Bancomat, Carte di Credito, transazioni on-line.... ecc., insomma la cosiddetta "moneta elettronica" ci fa risparmiare tempo, è comoda, semplice da utilizzare e ha migliorato la qualità della nostra vita quotidiana. Nata per ridurre

tempi e semplificare i trasferimenti di fondi fra soggetti diversi, la moneta elettronica ha 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. Sono sempre di più le persone che usano regolarmente le carte di pagamento per comperare e fare spese. Per questo è importante non trovarsi impreparati di fronte a quei piccoli imprevisti che possono capitare: come ad esempio il furto, lo smarrimento od in alcuni casi la truffa. Abbiamo quindi realizzato questa breve Guida che illustra alcune semplici regole che rendono l'impiego della moneta elettronica oltre che pratico, sicuro. La Guida è divisa in tre parti: la prima parte illustra gli accorgimenti da utilizzare quando si effettuano prelievi e pagamenti per evitare che qualcuno possa impossessarsi del numero della carta e del codice segreto Pin (Personal Identification Number o codice segreto) ed inoltre spiega come non diventare vittime di possibili truffe e raggiri (anche per chi utilizza internet per fare acquisti). La seconda parte contiene, invece, un vero e proprio Vademecum, che contiene tutte quelle informazioni necessarie per sapere come comportarsi in tali spiacevoli circostanze. La terza infine illustra i vantaggi e come funzionano le carte di nuova generazione cioè quelle con il microchip.



La sua Banca

INDICE

PARTE PRIMA

I La moneta Elettronica: regole di sicurezza	pag	5
Ricevere a casa Bancomat e Carta di Credito... ecc.	pag	6
II Prelievi e pagamenti con le Carte	pag	6
Prelevare e pagare con il Bancomat	pag	6
Prelevare e pagare con la Carta di Credito	pag	8
III Che cosa si rischia?	pag	10
La clonazione: cioè il duplicato illecito	pag	10
Le altre truffe	pag	11
IV Internet e il commercio elettronico	pag	12
I sistemi di sicurezza on-line	pag	12
La sicurezza di acquistare in internet	pag	12
Che cosa si rischia	pag	15
Sicurezza: l'utilizzo delle password	pag	16
V Le 10 regole d'oro...	pag	17

PARTE SECONDA

VI Come fare quando: vademecum per le emergenze	pag	19
Furto o smarrimento del Bancomat	pag	19
Furto o smarrimento della Carta di Credito....	pag	21

PARTE TERZA

VII Le nuove Carte con il microchip	pag	22
Numeri Utili per il furto o smarrimento delle Carte	pag	26

1

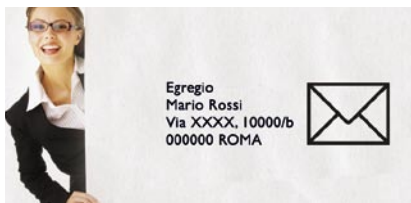
LA MONETA ELETTRONICA: REGOLE DI SICUREZZA



La moneta elettronica (Bancomat, Carte di Credito, Carte prepagate, transazioni on-line.... ecc.) ci fa risparmiare tempo, è comoda, semplice da utilizzare e ha migliorato la nostra vita quotidiana. Ecco alcune semplici regole che rendono il suo impiego semplice e 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 oggi è difficile immaginare la propria vita senza Bancomat, Carta di Credito ed anche internet, che per molti è oggi uno strumento insostituibile di lavoro, ma non dobbiamo dimenticare che la comodità non ci dispensa dall'applicazione di quelle minime regole di attenzione e prudenza,



che ci garantiscono tranquillità e 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 Carte (duplicazione illegale del nostro Bancomat e/o Carta di Credito ecc.), la manomissione del Pos (la "macchinetta" che legge i dati presenti nella Carta quando effettuiamo un acquisto nei punti vendita e negozi), la manomissione (spesso ben camuffata) degli ATM o sportello Bancomat (Automatic Teller Machine, postazioni di prelievo dei contanti), 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 e un nucleo di indagine Comunitario specializzato che permette in brevissimo



tempo di attivare una collaborazione con gli altri Paesi europei per ricerche, verifiche ed azioni coordinate.

Ricevere a casa Bancomat e Carta di Credito ...ecc.

Vi sono alcune Banche che consegnano direttamente allo sportello il Bancomat o le altre Carte, se così non fosse e le Carte vi venissero recapitate direttamente a casa per posta e così pure il relativo codice Pin, controllate che le buste siano integre e che provengano dalla vostra banca (o da chi emette la Carta). Verificate attentamente che non vi siano rotture anche all'interno della busta ad esempio del cartoncino che contiene la Carta. Diffidate di buste bianche inviate con francobolli perché solitamente l'invio avviene con buste con tassa pagata. Va posta attenzione anche alla regolarità di arrivo dell'estratto conto delle Carte, se arriva tardi insospettitevi perché potrebbe essere stato sottratto ed aperto "temporaneamente" per impadronirsi dei dati che in esso sono contenuti (ad es. proprio il numero della Carta). Questo tipo di raggio si chiama "boxing".

2 PRELIEVI E PAGAMENTI CON LE CARTE

Prelevare e pagare con il Bancomat

Se vi accingete a prelevare del denaro contante con la vostra Carta di Debito (Bancomat, Pagobancomat, Cirrus, Maestro ecc..) presso un sportello ATM (Automatic Teller Machine) meglio conosciuto come postazione/sportello Bancomat vi suggeriamo di:

- ⚠ accertarvi che nelle immediate vicinanze non vi siano persone ferme in atteggiamento sospetto magari con telecamere;
- ⚠ osservare sempre attentamente la "postazione" e la sua apparecchiatura (tastiera al piano o di lato al video, fessura ecc..) che non devono presentare anomalie o strane sporgenze (se prelevate spesso o sempre nello stesso ATM vi sarà più facile notare eventuali "difformità"). Soprattutto scrutate che non vi siano "oggetti strani" attaccati ad esempio negli angoli o nei pressi come





ad esempio micro telecamere nascoste nel porta depliant od a altezza della tastiera (se la postazione è al chiuso, fare attenzione ad eventuali oggetti appesi alle pareti);

- ⚠ verificare la bocca della fessura: la fessura dove va inserita la Carta deve essere ben salda e non muoversi. La Carta deve poter essere inserita nell'apposita fessura senza alcuno sforzo. Se la fessura si muove o si stacca potrebbe significare che essa sia stata manomessa o che ad esempio sia stato applicato sopra (quindi "coperta") uno "skimmer" camuffato da "fessura originale" (vedi più avanti). All'atto della restituzione la tessera deve poter essere facilmente afferrata senza difficoltà;
- ⚠ controllare che la tastiera sia ben fissata perché vi potrebbe essere una tastiera falsa posizionata sopra quella dell'ATM, con lo scopo di "catturare" il codice Pin durante la digitazione. In tale evenienza ci si accorgerà perché la tastiera non sarà a livello del piano e sarà presente un piccolo "gradino" di circa un paio di millimetri;
- ⚠ digitare il Pin, nascondendo la mano che digita con l'altra in modo che nessuno o nessuna telecamera nascosta possa

"leggere" le cifre del vostro Pin;

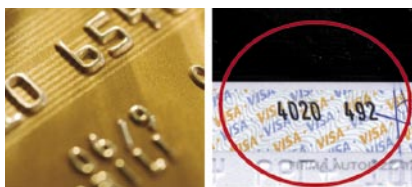
- ⚠ in presenza anche di un minimo dubbio, non introdurre la Carta e tanto meno digitare il Pin. Se la Banca è aperta avvisate il personale, altrimenti è bene chiamare le Forze dell'ordine;
- ⚠ fare attenzione ai pagamenti tramite Pos (lettore della Carta presente nei negozi e nei supermercati, pompe di benzina ecc..) se vi dicono che il Pos è in un'altra stanza, non rivelate assolutamente il vostro Pin e non lasciate che facciano l'operazione senza che voi siate presenti, offritevi di accompagnare la persona;
- ⚠ se avete il dubbio di essere osservati, parlatene con chi vi accompagna o con chi effettua il servizio di vigilanza;
- ⚠ in caso di sospetti, contattare il personale della Banca. In orari di chiusura degli sportelli contattate le Forze dell'ordine, o se la Carta è bloccata in maniera irregolare nella fessura o ritenete che ciò che vi stia capitando non sia normale chiamate il *Servizio Blocco* della Carta. A volte è meglio affrontare qualche piccolo inconveniente come cambiare la Carta piuttosto che essere vittime di una truffa.



Prelevare e pagare con la Carta di Credito

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

- ⚠ non perdetela mai di vista, se state facendo un acquisto dovete pretendere che al momento della transazione (cioè il passaggio della Carta nel Pos) il negoziante, l'albergatore, il benzinaio, ecc. effettuino lo "striscio" alla vostra presenza ed "a vista". Questo vale soprattutto in alcuni Paesi esteri dove sono stati segnalati casi in cui il negoziante portava la Carta nel retrobottega per effettuare la transazione e poi provvedeva alla copia dei dati utili a fini di truffa o di 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 nel retro o nel 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: verificarlo 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 Carta, la Banca per conoscenza, e quindi denunciare alle Forze dell'ordine la clonazione della Carta, disconoscendo le spese addebitate (vedi più avanti);
- ⚠ un capitolo a parte sono gli acquisti fatti 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 nella parte inferiore dello schermo. In caso contrario non effettuate il pagamento: si corre il rischio di vedersi rubare i dati personali e quelli della Carta;

⚠ molte Carte di Credito consentono di prelevare denaro contante dagli sportelli

ATM, nel caso lo facciate seguite le indicazioni del paragrafo precedente;

⚠ se avete effettuato un acquisto od un pagamento con la Carta di Credito non buttate mai la ricevuta consegnata dall'esercente ma conservatela fino a che non abbiate controllato l'estratto conto del mese, quindi strappatela e gettatela.

Carte con il microchip...aumenta la sicurezza !



Il motto è sicurezza e tecnologia in tasca! Sono sempre più diffuse le Carte con la presenza di un microchip, studiate per consentire da un lato una maggiore sicurezza, rispetto alla tradizionale Carta con la banda magnetica e dall'altro per permettere di memorizzare e gestire dati in

maniera interattiva. Infatti per via di una maggiore capacità di memoria e grazie al microprocessore interno, le smart card (così sono dette in gergo le Carte con il chip) potranno essere utilizzate per accedere a più servizi: memorizzare dati identificativi, concorsi a punti, ecc. In una prima fase le Carte emesse con microchip continueranno a riportare anche la banda magnetica, per consentire il normale svolgimento delle transazioni anche in presenza di terminali Pos e sportelli Bancomat non ancora sostituiti con i nuovi terminali abilitati alla lettura del microchip (Pos). Il passaggio a questa tecnologia (già in corso) sarà ultimato da parte di tutte le Banche dando comunque il tempo agli utenti di abituarsi a questa nuova tecnologia. Grazie alla crittografia la "memoria della Carta" (appunto il chip) è al riparo da accessi esterni non autorizzati e consente metodi di autenticazione del "titolare" che la rendono estremamente sicura contro tentativi di duplicazione e contraffazione. Il microchip consente di autenticare in qualunque momento la Carta: mentre le carte a banda magnetica contengono un valore di verifica (CVV,CSC...) che può essere verificato solo tramite il collegamento con la banca emittente, la genuinità delle Carte dotate di microchip può essere verificata direttamente tramite il chip. Nel periodo di cosiddetta "doppia circolazione" cioè quello in cui sono utilizzate contestualmente sia le Carte con la banda magnetica che quelle con il microchip lì dove sono presenti i Pos di seconda generazione verrà letto il microchip altrimenti la banda magnetica. Quindi per i prossimi anni sarà possibile utilizzare la Carta con microchip in tutti gli esercizi commerciali in Italia, normalmente, in una modalità o nell'altra a seconda del tipo Pos mentre all'estero per la Carta di Credito semplicemente si segnerà a firmare lo scontrino. (Vedi la Parte terza)

3

CHE COSA SI RISCHIA ?

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. È allora importante conoscere quali possono essere le situazioni nelle quali si corre il rischio che ci vengano sottratti sia i cosiddetti "dati sensibili" (ad esempio il numero della Carta di Credito, il Pin ecc.) sia le Carte (Bancomat, Carta 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

Clonare una Carta di Credito o di Debito (Bancomat) significa in sostanza riuscire a "duplicare" la banda magnetica presente



Fig.1 Riuscite a vedere lo skimmer? eccolo !

nel retro della Carta, ma se chi la duplica non conosce il Pin (codice segreto) non può utilizzarla. Il problema quindi non è tanto legato alla tecnologia quanto piut-



Fig.2 La microcamera è nel porta depliant....

tosto 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" (un tipo di memoria che immagazzina programmi - firmware- per microprocessori), che cattura i dati presenti nella banda magnetica con la semplice "strisciata" della Carta (Carta di Credito, Bancomat ecc..) su di esso. Lo skimmer è un congegno di dimensioni ridotte (fig. 3) e non ha una forma standard, solitamente è grande quanto un pacchetto di sigarette. Lo skimmer è spesso alimentato con batteria e ricopia ("immagazzina") i dati presenti nella banda magnetica: nome, cognome e data di scadenza della tessera, nonché l'invisibile codice di verifica trasmesso elettronicamente per confermare la validità della Carta stessa. Una volta che lo Skimmer sarà collegato ad un computer

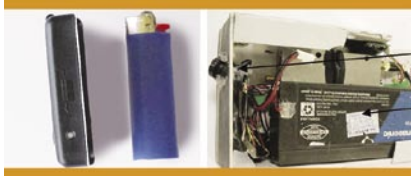


Fig.3 Dimensioni skimmer, microcamera e trasmettente....

munito di un programma apposito per la gestione e creazione di bande magnetiche, i dati "catturati" illecitamente potranno essere trascritti in un nuovo supporto plastico con le caratteristiche di una Carta di Credito/Bancomat, generando di fatto un "clone" di una Carta. Per impossessarsi invece del codice Pin, che non è in alcun modo ricavabile dalla banda magnetica, i truffatori utilizzano generalmente una micro telecamera nascosta che filma la digitazione dei numeri del Pin (codice segreto) e che poi solitamente trasmette (fig. 3) il Pin "catturato" in radio frequenza ad un "ricevitore" posto nelle vicinanze che visualizza i numeri del codice segreto. Ci si rende conto, quindi, che quando ci si accinge a prelevare presso uno sportello ATM basta fare attenzione a ciò che stiamo facendo, controllando che le apparecchiature non siano alterate o manomesse.

Le altre truffe

Vi sono altri tipi di frodi che è bene tener presente ma anche queste possono essere neutralizzate con semplici verifiche e ponendo attenzione a ciò che si sta facendo.



Non gettate mai la ricevuta del pagamento senza strapparla....

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 Carta.

Il lebanese loop: è una tecnica di manomissione dello sportello ATM (postazione Bancomat), infatti sullo sportello di prelievo automatico viene applicato un dispositivo che, una volta inserita la Carta la "trattiene" in modo che il distributore non riesca più a restituirla. In tale situazione si resta solitamente perplessi, perché la Carta rimane "incastrata" e non si può completare la transazione ne riavere indietro la Carta. In questo clima di sconcerto di solito "spunta" il truffatore che, fingendo di prestarvi



Ecco la "falsa" fessura e il "nastro" che bloccano la Carta....

soccorso, vi invita a digitare nuovamente il Pin, manovra che gli consente di spiare e memorizzare il codice segreto della Carta. Poi quando il proprietario della Carta si allontana il truffatore stacca il dispositivo e recupera la Carta per poi utilizzarla con il Pin appena "memorizzato".

4

INTERNET E IL COMMERCIO ELETTRONICO

In questa parte della guida elencheremo le altre tipologie di truffe che riguardano le transazioni e gli acquisti effettuati on-line via internet. Anche tali tecniche sono inefficaci di fronte ad un acquirente attento e prudente e che protegge i propri dati.

I sistemi di sicurezza on-line

Negli ultimi anni si è diffuso sempre di più il cosiddetto "commercio elettronico", cioè la possibilità di acquistare beni e servizi on-line ed in particolare via internet. Recentemente l'ABI ha dichiarato che sono ben



oltre un milione gli italiani che acquistano regolarmente on-line. Quasi tutte le aziende che vendono beni hanno un proprio sito internet che spesso consente di effettuare acquisti, con semplicità ed immediatezza. Stiamo parlando di veri e propri "negozi on-line", in cui è possibile vedere la foto dei prodotti e leggere tutte le loro caratteristiche. Sono centinaia di migliaia ogni giorno gli acquisti on-line in tutto il mondo. Oggi è possibile comprare on-line tutti i generi di prodotti (ed alcuni è possibile acquistarli solo tramite internet): moto, auto, elettrodomestici, mobili, telefonini, profumi, orologi, generi alimentari ecc., nonché beni di privati di qualsiasi tipo, nuovi od usati, come ad esempio oggetti da collezione. È uno scenario che solo qualche anno fa sembrava solo verosimile ma oggi è realtà.

La sicurezza di acquistare in internet

Anche nel caso di internet le transazioni con la moneta elettronica o meglio "virtuale" (e-cash) vanno effettuate con qualche semplice precauzione ed una normale

dose di prudenza, potremo dire la stessa che usiamo per traversare la strada. Per gli acquisti on-line i pagamenti possono essere realizzati con differenti strumenti ed in diverse modalità, si va dal bonifico bancario, al vaglia postale, al contrassegno, all'utilizzo di circuiti o sistemi proprietari di pagamento, alla Carta di Credito, alle Carte prepagate, ecc. Nella maggioranza dei casi comunque viene utilizzata la Carta di Credito sia per la facilità di impiego sia per l'elevato tasso di diffusione e sia per l'affidabilità del circuito a livello internazionale. Anche la transazione on-line compiuta con Carta di Credito prevede che vengano comunicati i propri dati anagrafici ed i dati specifici della Carta. La procedura prevede che avvenga una prima registrazione (accreditamento) da effettuarsi



presso il sito del venditore, che può essere permanente (si resta registrati fino alla propria richiesta di cancellazione) oppure "temporanea" (si comunicano i dati solo durante il perfezionamento dell'acquisto). In questo caso le truffe che possono accadere rappresentano una eventualità remo-



ta, se ci si comporta con la indispensabile dose di attenzione. Nei negozi on-line che possiamo trovare in internet, solitamente è attivato un sistema di protezioni di carattere informatico finalizzate a garantire la sicurezza del cliente. Come sempre molto dipende da noi: se disponiamo di un allarme a prova di ladro che protegge la nostra casa e usciamo senza attivarlo, nel caso di intrusione di un malfattore, niente potremo imputare all'efficacia dell'allarme stesso. Acquistare in internet e pagare con la "moneta elettronica" è semplice, comodo, e sicuro, i negozi del web accreditati utilizzano codifiche di sicurezza praticamente inespugnabili perché basate su generazioni di numeri casuali e validi per una sola transazione. Comunque qui riportiamo alcuni accorgimenti che possono essere utili nel caso in cui ci si accinga ad effettuare un acquisto di prodotti o servizi on-line :

🔒 effettuare acquisti presso siti conosciuti o tenere sotto osservazione il sito per un po' di tempo prima di accingersi a comprare

(effettuando anche ricerche on-line per verificare se esistono note negative circa il sito o lo specifico negozio/venditore ad esempio nei *blog*). Il "popolo di internet" utilizza un sistema assai efficace di *passaparola* per cui il truffatore o il negozio/venditore poco affidabile viene "identificato" e viene emesso nei suoi riguardi una sorta di punteggio negativo (feed-back negativi);

🔒 controllare sempre se nel sito web è indicato un indirizzo fisico e telefonico dove contattare il negozio/venditore in caso di necessità, nei casi dubbi inviate un messaggio e-mail all'azienda intestataria del sito per ottenere maggiori garanzie;

🔒 verificare che il sito presso il quale si intende acquistare un bene utilizzi protocolli di sicurezza informatica che permettano di identificare l'utente. I più diffusi sono il 3D Secure, il Secure Socket Layer (SSL) e il SET...ecc.. Infatti generalmente durante la transazione si viene reindirizzati ad un'area protetta (si potrà allora vedere come sulla barra dell'indirizzo compaia "https://" anziché "http://"), ed in basso a destra della finestra, comparirà un'icona con un lucchetto chiuso che sta a significare che in quel momento la connessione è protetta;

🔒 inserite i vostri dati economici solamente quando sono rispettate le condizioni di sicurezza e comunque non comunicate mai i dati della vostra Carta o altri dati riservati tramite e-mail;



🔒 fornite solo le informazioni indispensabili, altre informazioni ad esempio quelle relative al proprio conto corrente possono mettervi a rischio; per effettuare una transazione con Carta di Credito i dati più importanti sono: numero Carta, data scadenza, numero CSC o CW2: proteggereteli!

🔒 esistono nel mercato Carte di Credito "virtuali" che utilizzano un codice differente per ogni acquisto come se si utilizzasse una Carta di Credito differente per ogni singola transazione. Anche le Carte prepagate e i borsellini elettronici svolgono la stessa funzione della Carta di Credito e presentano il vantaggio di "contenere" solo una somma di denaro limitata;

🔒 nel caso in cui si effettui il pagamento con un programma di internet banking, controllate saldo e movimenti dopo aver effettuato il bonifico on-line, in modo da agire tempestivamente qualora vengano addebitati acquisti non effettuati;

🔒 è necessario stampare e conservare le ricevute dei pagamenti on-line, nonché le clausole dei contratti, potrebbero risultare utili in caso si voglia contestare l'acquisto.



Che cosa si rischia

Vi sono alcuni tipi possibili di frodi, che per chi intende acquistare on-line è bene tener presente, ma che sicuramente possono essere neutralizzate con facilità se si usa un po' di attenzione. I crimini informatici sono disciplinati principalmente dalla Legge 547/1993 che ha operato delle modifiche al Codice Penale prevedendo il reato penale per le più diffuse condotte criminose nel settore informatico come ad esempio l'accesso abusivo, il danneggiamento, la frode informatica, il falso informatico, lo spionaggio, l'attentato ad impianti di pubblica utilità, la detenzione e la diffusione abusiva di codici d'accesso, la violenza sui beni informatici ecc.. Ecco alcuni dei crimini informatici più frequenti.

Phishing: è una frode on-line di cui molto si parla e che sembra non passare di moda. Mira a sottrarre con l'inganno numeri di Carta di Credito, password, informazioni su account personali...ecc. e consiste nell'inviare messaggi di posta elettronica, "mascherati" da messaggi "autentici" (spesso delle ottime imitazioni) che sembrano pro-

venire ad esempio da parte di una Banca o di un Ente conosciuto o altro, dove vi si chiede pretestuosamente un aggiornamento dei vostri dati sensibili (ad es.: numero Carta di Credito) oppure di registrarvi per avere dei "benefici" (ad es.: un concorso a premi). A questi messaggi non bisogna assolutamente rispondere. È necessario avvertire subito la Banca o le Forze dell'ordine avendo l'accortezza di non cancellare l'e-mail ricevuta. Un tipo di phishing più evoluto viene detto **Pharming** e consiste nel realizzare pagine web identiche a siti già esistenti in modo che l'utente sia convinto di trovarsi ad esempio nel sito della propria Banca e vi cominci ad operare. Una volta digitate le credenziali (password ecc..) il danno è fatto. Anche in questo caso avvisare subito la Banca o le Forze dell'ordine. **Sniffing:** è una tecnica informatica che, nel caso di siti che consentono l'acquisto, ma



non offrono sistemi aggiornati di protezione, permette di intercettare le coordinate dei pagamenti fatti con le Carte di Credito, utilizzando poi le stesse per fare ulteriori acquisti all'insaputa del vero proprietario.

Hacking: quest'attività è 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 immagazzinati, anche questo tipo di truffa solitamente non funziona se non vi è il "contributo" di un basista all'interno.

Spyware: lo spyware (software spia), come è noto a chi "gira in internet" è un software illegale finalizzato a spiare (spy) le operazioni dell'utente del PC (personal Computer) sottraendogli informazioni riservate e talvolta riesce anche a far compiere al PC specifiche operazioni all'insaputa del proprietario e contro la sua volontà. Spesso si annida in alcuni programmi scaricabili gratuitamente o a pagamento ed è in grado di raccogliere informazioni specifiche riferite alla postazione (PC) nella quale si è installato, tali dati vengono poi trasmessi ad insaputa dell'utilizzatore del PC ad un altro PC (Server remoto) quando ci si collega in rete. Quindi prima di scaricare un programma bisogna fare attenzione a quello che si sta facendo e se si ha anche il minimo dubbio: informarsi. Se il dubbio permane evitare tassativamente di scaricare (download). In Italia non è consentito



appropriarsi di tali informazioni soprattutto senza il consenso dell'interessato. Se si vuole beneficiare di maggiore sicurezza e se si opera con l'estero dove la legislazione è in alcuni casi differente, è sufficiente installare nel proprio PC dei programmi (anche gratuiti) che fungono da barriera, le cosiddette "firewall" (letteralmente: pareti di fuoco) che impediscono tali fuoriuscite di dati, vi sono anche software specifici anti-spyware. Tutti gli utilizzatori di internet sanno che per navigare senza rischi o quasi è necessario installare anche un antivirus e spesso tali antivirus effettuano anche attività di firewall od anche anti-spyware. È buona norma quindi non navigare in internet se non provvisti di antivirus e firewall, il che impedirà che si verifichino le situazioni di cui sopra.

Sicurezza: l'utilizzo delle password

Solitamente prima di effettuare un acquisto on-line il sito web del negozio richiede



una registrazione che consente poi di identificare l'acquirente anche per gli acquisti successivi, attraverso un semplice codice identificativo (User Id, Pseudo..ecc.), in questo modo ad un acquisto futuro il sito web "ci riconoscerà" e non sarà più necessario fornire i dati. Vi sono alcuni negozi on-line che fra i dati richiesti in fase di registrazione oltre ai nostri dati anagrafici, il codice fiscale, l'indirizzo al quale solitamente vogliamo che la merce arrivi ecc. prevedono i dati relativi alla Carta di Credito, viceversa in altri casi inserirete tali dati solo nel momento in cui state perfezionando l'acquisto. In entrambi i casi il sito vi richiederà di creare ed inserire delle password, di vostra invenzione, che vi permetteranno di accedere con più facilità all'area dell'"acquisto protetto". Queste password rappresentano un'ulteriore meccanismo di protezione e



sicurezza in quanto generate da voi e di sola vostra conoscenza. La procedura delle password riguarda anche l'utilizzo dei programmi di internet banking che consentono di effettuare pagamenti comodamente on-line dal proprio PC senza recarsi in Banca. È quindi importante tenere segrete e custodire le vostre password e se del caso che vengano cambiate periodicamente. Una password costituita da frasi o parole facilmente intuibili è una password a rischio, quindi create la vostra 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! È meglio utilizzare combinazioni di caratteri alfanumerici: cioè lettere e numeri (ad es.: 1EAIZS0174). Memorizzate le password e comunque, se le scrivete non lasciatele in posti facilmente accessibili.

5

LE 10 REGOLE D'ORO

Riportiamo qui in forma sintetica alcune regole di comportamento, che riassumono quanto è stato proposto nelle pagine pre-

cedenti sia in termini di possibilità che di casistica. Queste semplici regole, se applicate, ci consentiranno di utilizzare la moneta elettronica con quella tranquillità e sicurezza e poterne apprezzare la sua reale comodità, mettendoci nella condizione di evitare spiacevoli e fastidiosi inconvenienti:

- 1 duplicare e conservatene copia in luogo sicuro di tutti i documenti personali compresi gli estremi delle Carte (Bancomat e Carte di Credito ecc.), le password ed i documenti che attestano eventuali proprietà (scontrini, fatture, foto di oggetti... ecc.) sarete così facilitati in caso di necessità e di emergenza, ad esempio per la denuncia di furto o smarrimento;
- 2 conservate con cura le Carte e soprattutto tenetele lontano da fonti magnetiche e da elementi metallici per evitarne la smagnetizzazione; attenzione anche, per lo stesso



motivo, a non graffiare la banda magnetica;

- 3 non conservate mai il Pin (codice segreto) insieme alle Carte (Bancomat o Carta di Credito abilitata al prelievo); conservate a portata di mano i numeri telefonici (in gene-

re numeri verdi) forniti dal/i gestore/i della/e Carta/e per effettuare il blocco della Carta a seguito di furto e smarrimento;

- 4 conservate fatture, ricevute fiscali e contratti di tutto quello che avete acquistato on-line, potrete essere precisi e documentati in caso di contestazione od in qualsiasi altra spiacevole evenienza;
- 5 chiedete sempre l'identità del vostro interlocutore: sappiate che i mistificatori si possono nascondere ovunque; evitate di fornire il numero della Carta soprattutto ad interlocutori telefonici o via internet;
- 6 controllate sempre gli estratti conto forniti dalla società di gestione della Carta;
- 7 non lasciate in giro o buttate le copie contabili di pagamenti e prelievi ancora leggibili nella spazzatura;
- 8 denunciate immediatamente il furto o lo smarrimento delle Carte, dei libretti degli assegni e della pensione e di tutti quei documenti che possono essere oggetto di contraffazione e di illecita e immediata utilizzazione;
- 9 avvaletevi di forme assicurative, depositi di sicurezza e ogni altro mezzo atto per diminuire il rischio e gli effetti del danno derivante dalle iniziative di malintenzionati;
- 10 se vi recate all'estero o in Paesi poco sicuri o se non vi fidate di un sito web effettuate pagamenti con le cosiddette Carte prepagate che consentono di spendere solo il denaro presente nella Carta in quel momento.

6

COMEFAREQUANDO VADEMECUM PER LE EMERGENZE

Come abbiamo già detto oggi nessuno di noi potrebbe immaginare la propria vita senza Bancomat, Carta di Credito ed anche internet. Questa familiarità con la moneta elettronica non ci deve dispensare dall'applicare quelle minime regole di prudenza ed attenzione che ci garantiscono sicurezza. Ma è altrettanto importante nel momento dell'emergenza agire subito: per questo qui sotto abbiamo riepilogato per punti salienti che cosa si deve fare quando si perde o ci viene rubato il Bancomat e/o la Carta di Credito ecc. o quando a nostra insaputa ci accade di trovarci vittime di un tentativo di furto della nostra identità digitale. In questa parte della Guida è possibile trovare tutte quelle informazioni di utilità e necessarie per far fronte ai casi di emergenza come furto o smarrimento delle Carte. Insomma un breve vademecum per sapere come comportarsi in queste eventualità, in modo che si possa agire con la necessaria determinazione al fine di evitare spiacevoli ed onerosi inconvenienti. Troverete nelle prossime pagine la descrizione in forma sintetica delle procedure previste e da seguire, memoriz-



zatele, perché quanto più saremo pronti nel reagire tanto più saremo in grado di limitare il danno alle nostre proprietà derivante da comportamenti criminosi e tanto più potremo ridurre il lasso di tempo per ripristinare la "normalità".

Furto o smarrimento del Bancomat

Se vi hanno rubato o avete smarrito la Carta di Debito (Bancomat) oppure scoprite che il Bancomat è stato oggetto di clonazione (quindi è stato utilizzato da malintenzionati per prelievi od acquisti fraudolenti), la prima cosa da fare è agire tempestivamente. Sia per il furto che per lo smarrimento e la clonazione la procedura da seguire è la stessa:

- 1 si deve procedere al "Blocco" della Carta chiamando l'apposito Numero Verde del Servizio Blocco che è valido per l'Italia ed è attivo 24 ore su 24 (peraltro riportato anche su tutti gli sportelli Bancomat); nel caso in cui si debba procedere al blocco della Carta Bancomat e ci si trovi all'este-



ro in molti Paesi sono disponibili specifici numeri verdi, che quindi potranno essere utilizzati gratuitamente (nelle pagine successive riportiamo un elenco riassuntivo che potrebbe però essere suscettibile di modifica, se del caso basterà consultare l'elenco telefonico del Paese dove ci si trova per reperire il numero aggiornato);

- 2 il Blocco può essere fatto anche avvertendo subito la filiale della Banca che ha emesso la Carta, telefonando o recandovi di persona.
- 3 Quando si chiama il numero apposito per il Blocco, è bene appuntarsi: la data, l'ora ed il nominativo della persona del "Servizio Blocco" con la quale si è parlato ed eventualmente, se rilasciato dall'operatore telefonico, anche il "codice di operazione" con la quale si identifica il Blocco della vostra Carta.
- 4 Dopo aver provveduto ad effettuare il Blocco della Carta si dovrà denunciare l'accaduto alle Autorità di Pubblica Sicurezza e farsi rilasciare copia della denuncia.

5 Quindi si dovrà consegnare una copia della denuncia alla filiale della Banca ad integrazione della documentazione ed entro 2 giorni lavorativi dall'accaduto si dovrà confermare la richiesta di Blocco inviando una Raccomandata a. r., allegando anche una copia della denuncia, alla Società S.I.A. che gestisce il circuito (oppure alla Società che ha emesso la Carta).

6 Nel caso in cui verificando l'estratto conto si riscontri la presenza di addebiti per acquisti o prelievi non effettuati dal titolare (fraudolenti) è bene telefonare al numero di Assistenza Clienti della Banca o della Società che ha emesso la Carta, segnalando l'inconveniente; quindi andrà inviata, entro 60 giorni dalla data di emissione dell'estratto conto, una contestazione scritta e firmata dall'intestatario della Carta, allegando copia dell'estratto conto contestato e copia fronte/retro della Carta; si dovrà allegare inoltre una copia denuncia effettuata presso le Autorità competenti.

7 La procedura qui sopra descritta è stata prevista per garantire innanzitutto la

Smarrimento o furto del PIN...

Anche nel caso di smarrimento o sottrazione solo del PIN del Bancomat, cioè del Codice personale segreto, ci si dovrà comportare come sopra, in questo caso si deve restituire anche la Carta Bancomat.

sicurezza del titolare della Carta, il quale potrà poi avvalersi anche dell'aiuto e del supporto della Banca che rimane a disposizione per qualsiasi chiarimento e per effettuare insieme a voi quegli adempimenti necessari per consentirvi una veloce risoluzione dell'inconveniente ed un rapido ritorno alla piena operatività.

Furto o smarrimento della Carta di Credito, delle Carte Prepagate ...ecc.

Nel caso di furto, smarrimento e/o clonazione della Carta di Credito o della Carta Prepagata la procedura è la stessa prevista per la Carta Bancomat:

- 1 blocco della Carta chiamando i numeri di telefono dedicati e che potete consultare (elencati carta per carta nella pagina successiva), in molti casi si potrà effettuare il Blocco anche rivolgendosi direttamente alla filiale della Banca dove si intrattiene il rapporto di conto corrente;
- 2 denunciare alle Autorità di Pubblica Sicurezza quanto successo e farsi rilasciare copia della denuncia da consegnare in Banca per completare il fascicolo e/o da inviare all'As-

Carta di Credito con funzione Bancomat

Se la Carta di Credito è abilitata alla funzione Bancomat e Pagobancomat in alcuni casi sarà necessario effettuare entrambe i Blocchi: sia quello della Carta di Credito (si veda il paragrafo dedicato) sia quello del Bancomat.

sistenza Clienti di chi ha emesso la Carta;

- 3 nel caso di contestazione di addebiti illeciti, il titolare dovrà inoltrare all'Ufficio Titolari (in alcuni casi: Assistenza Clienti o Ufficio dispute o Servizio Marketing... ecc.) una lettera di contestazione firmata con la copia della denuncia e dell'estratto conto riportante la spesa contestata.
- 4 Il duplicato viene emesso per tutte le Carte, salvo quelle con funzione Bancomat e PagoBancomat, che devono essere richieste nella filiale di appoggio.
- 5 Se si tratta di una Carta prepagata di solito non vi è l'emissione di un duplicato, ma la sostituzione con una nuova Carta nella quale verranno trasferiti gli eventuali fondi residui in alternativa al rimborso che viceversa è previsto per le Carte prepagate monouso, cioè non ricaricabili.

Clonazione della Carta ...

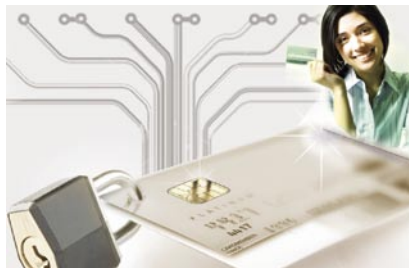
Nel caso in cui qualcuno sia riuscito ad impadronirsi dei dati di una delle vostre Carte e ne effettui un utilizzo fraudolento o anche nel caso in cui si scopra o si venga avvisati dalla Banca che la propria Carta sia stata clonata, la procedura che si deve seguire è quella prevista per i casi di furto e smarrimento. Andrà inoltre verificato con attenzione l'estratto conto per disconoscere e contestare utilizzi e prelievi fraudolenti, inviando un reclamo scritto alla Società che ha emesso la carta (allegando la denuncia effettuata all'Autorità di Pubblica Sicurezza).

7

LE NUOVE
CARTE CON IL
MICROCHIP

innovazione, Sicurezza e vantaggi..

Le nuove carte di pagamento sono sviluppate con la tecnologia del microchip, una novità che vuol dire non solo più sicurezza ma anche maggiori vantaggi. Dopo il passaggio alla moneta unica nel 2002, l'Europa ha proseguito nell'attuazione del Progetto SEPA (Single Euro Payments Area, cioè: area unica dei pagamenti in euro) in una logica di integrazione dei vari sistemi di pagamento nazionali che vedrà di qui a pochissimi anni i Paesi dell'U.E. dotarsi di un unico standard anche per i pagamenti con la moneta elettronica (carte, bonifici e addebiti su conto corrente..). In



questa direzione entro il 2010 avverrà per la cosiddetta moneta elettronica quello che è già avvenuto con l'adozione della moneta unica (l'euro) cioè ogni cittadino o impresa dell'U.E. potrà effettuare, con un unico conto corrente e con strumenti omogenei, pagamenti con la moneta elettronica in tutta l'area euro. Un esempio recente di questa vera e propria "rivoluzione" è l'introduzione dell'Iban (il codice unico europeo del conto corrente). Nella scia di questo cambiamento la prossima tappa, che è già cominciata, è rappresentata appunto dalle carte di pagamento (Carta di Credito, Bancomat ecc...) con il microchip (microprocessore). In questo modo si riducono i tempi, vengono semplificate le procedure e vi è più sicurezza. Una rivoluzione...che non modifica nulla ed offre sempre più vantaggi !

La nuova tecnologia del microprocessore

Le nuove carte di pagamento con il microchip (sul fronte della Carta) con-

sentono già oggi un'operatività in tutta l'area euro migliorando sensibilmente la sicurezza nelle transazioni. Insomma più sicurezza e più tecnologia comodamente in tasca!.... Il microchip racchiude al proprio interno tutte le caratteristiche e le funzioni di un vero e proprio computer, quali ad esempio la capacità di memorizzare informazioni, effettuare funzioni di calcolo, nonché la capacità di interagire attivamente scambiando dati. Quindi la presenza del microchip sulla Carta di pagamento trasforma di fatto la tradizionale Carta (con la sola banda magnetica) in una smart card (così sono chiamate in gergo bancario le Carte con il microchip) che può anche essere utilizzata per accedere a nuovi servizi come ad esempio la memorizzazione dei dati identificativi per la partecipazione a concorsi a premio e raccolte punti...ecc.

Ecco che cosa cambia...

Le Carte emesse con microchip continuano a riportare anche la banda magnetica,



per consentire il normale svolgimento delle transazioni anche in presenza di terminali Pos e sportelli ATM non ancora sostituiti con i nuovi terminali abilitati alla lettura del microchip. La banda magnetica consente inoltre di utilizzare, come già avviene, la carta in Paesi non area euro ad esempio gli Stati Uniti. Per i titolari non cambia nulla, infatti lì dove sono presenti i terminali Pos o gli sportelli ATM (postazione Bancomat) di seconda generazione viene "letto" il microchip altrimenti continua ad essere "letta" la banda magnetica. Quindi per i prossimi anni è possibile utilizzare normalmente la Carta con microchip in tutti gli esercizi commerciali in Italia, mentre all'estero semplicemente si seguirà a firmare lo scontrino. Anche nel caso di prelievi presso gli sportelli automatici sia in Italia che all'estero non cambia nulla: si deve digitare il PIN come si è sempre fatto.

Microchip= maggiore sicurezza...

Grazie alla possibilità data dai nuovi lin-

guaggi crittografici la "memoria della carta", che risiede appunto nel microchip, non permette accessi esterni non autorizzati e consente un metodo di autenticazione del Titolare della carta che la pone al riparo da tentativi di duplicazione e contraffazione. Inoltre il microchip consente di autenticare in qualunque momento la Carta (per così dire off-line), diversamente dalla banda magnetica che permette l'autenticazione solamente in presenza del collegamento con la Banca emittente (on-line), infatti solo se il collegamento è attivo è possibile la verifica della corrispondenza del codice (CVV,CSC...) iscritto nella banda magnetica da parte del circuito e della Banca emittente.

Microchip= più durata!

La banda magnetica è spesso soggetta ad usura e graffi o smagnetizzazione, mentre il microchip presenta una durata molto



maggiore proprio per via dei materiali impiegati e dei criteri di realizzazione. Un esempio: il microchip presente nella sim del telefonino che molti di noi hanno in tasca da molti molti anni...

Una rivoluzione che non cambia niente..... ma migliora tutto!

Il modo di prelevare o di pagare è lo stesso di una carta tradizionale: puoi infatti utilizzare la tua Carta con microchip in tutti gli sportelli ATM, seguendo a digitare il tuo codice PIN (personal identification

N.B.firma dello scontrino o PIN?

A seguito del processo di adeguamento dei terminali Pos e degli ATM può capitare che anziché richiedervi la firma dello scontrino, l'esercente vi richieda la digitazione del PIN, come oggi già accade per la Carta Bancomat, in questo caso basta inserire il PIN della Carta di credito e non occorre firmare lo scontrino. Il PIN è un codice segreto, in genere di 4 cifre, personale recapitato al Titolare della Carta tramite apposita comunicazione, inviata per posta o consegnata in Banca e che solo il Titolare deve conoscere (è importante tenerlo sempre separato dalla Carta, poiché in caso di furto o smarrimento, chiunque potrebbe "comodamente" utilizzare la vostra Carta, senza bisogno di contraffazioni).



number), come hai sempre fatto, e in tutti gli esercizi commerciali in Italia e all'estero semplicemente firmando lo scontrino o se richiesto digitando il PIN.

Come avere la carta con Microchip?

Il passaggio alle Carte con il microchip avviene progressivamente e in modo automatico, e senza costi aggiuntivi per il Titolare. Infatti le nuove Carte sono emesse con microchip. Quindi nel caso di attivazione di una nuova Carta (ad esempio all'apertura del Conto corrente) ci viene consegnata la Carta con anche la presenza del microchip (Carta di Credito o Bancomat). Questo vale anche per tutti i rinnovi a scadenza e tutte le riemissioni (duplicati, sostituzioni...). Per il Titolare della Carta il passaggio è gratuito.



Un SMS di "notifica autorizzazione"...



Attivando il servizio SMS di "notifica autorizzazione" si può ricevere,

a seguito di una spesa effettuata con la Carta, un messaggio SMS contenente i dati riepilogativi della transazione. Questo è un servizio che permette di tenere sotto controllo la attività effettuata con la Carta comodamente e ovunque ci si trovi. Se si riceve, ad esempio, un SMS per una transazione che si sa di non aver effettuato, si deve contattare immediatamente il Servizio Clienti della Carta che avvierà gli accertamenti e le necessarie verifiche del caso al termine delle quali verranno valutate le misure da prendere per tutelare la sicurezza del Titolare della Carta. Attivare il servizio è molto semplice: basta recarsi allo sportello della Banca, effettuare la richiesta tramite l'apposito modulo ed entro breve sarà inviato un messaggio SMS di benvenuto che informerà dell'avvenuta attivazione del servizio SMS "notifica autorizzazione". Questo servizio via SMS è disponibile per i clienti Vodafone, Tim, Wind e H3G e può essere attivato per i telefoni cellulari abilitati all'invio e alla ricezione dei messaggi SMS. Per ogni informazione e tutti i dettagli basta chiedere allo sportello della propria Banca.

Numeri Utili per il furto o smarrimento delle Carte

American Express

Furto smarrimento Italia	06 72900347
Furto smarrimento estero	+800 263 92279 +39 06 72900347

Carta di Credito BCC

Furto smarrimento Italia	800 086531
Furto smarrimento estero	+39 06 87419901

Carta BCC Tasca

Furto smarrimento Italia	800 086530
Furto smarrimento estero	+39 06 47825280

Carta Aura Findomestic

Furto smarrimento Italia	800 866 116
Furto smarrimento estero	+39 055 3374830

Cartasi

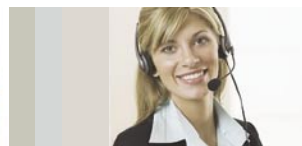
Furto smarrimento Italia	800 151616
Furto smarrimento estero	+39 02 34980020
Furto smarrimento USA	1 800 4736896

Carta Bancomat BCC Cash

Furto smarrimento Italia	800 822056
Furto smarrimento estero	+39 02 45403768
Furto smarrimento estero	

numeri verdi:

Argentina	0039 800 3027742
Australia	1 800 140714
Austria	0 800 295695
Belgio	0 800 72585
Brasile	00 083 977255
Canada	1 800 3706780
Cipro	08 095605
Danimarca	800 10101
Finlandia	0 800 113970
Francia	0 800 906772
Germania	0 800 1815154
Gran Bretagna	0 800 969760
Grecia	00 800 391278620
Irlanda	1 800 553914
Lussemburgo	0 800 2387
Norvegia	800 11616
Olanda	0 800 0224493
Portogallo	800 839908
Spagna	900 993954
Svezia	02 0794393
Svizzera	0 800 553405
Turchia	00 800 399078918
Ungheria	06 800 11259
USA - AT&T	1 800 3489906
USA - MCI	1 800 3738584





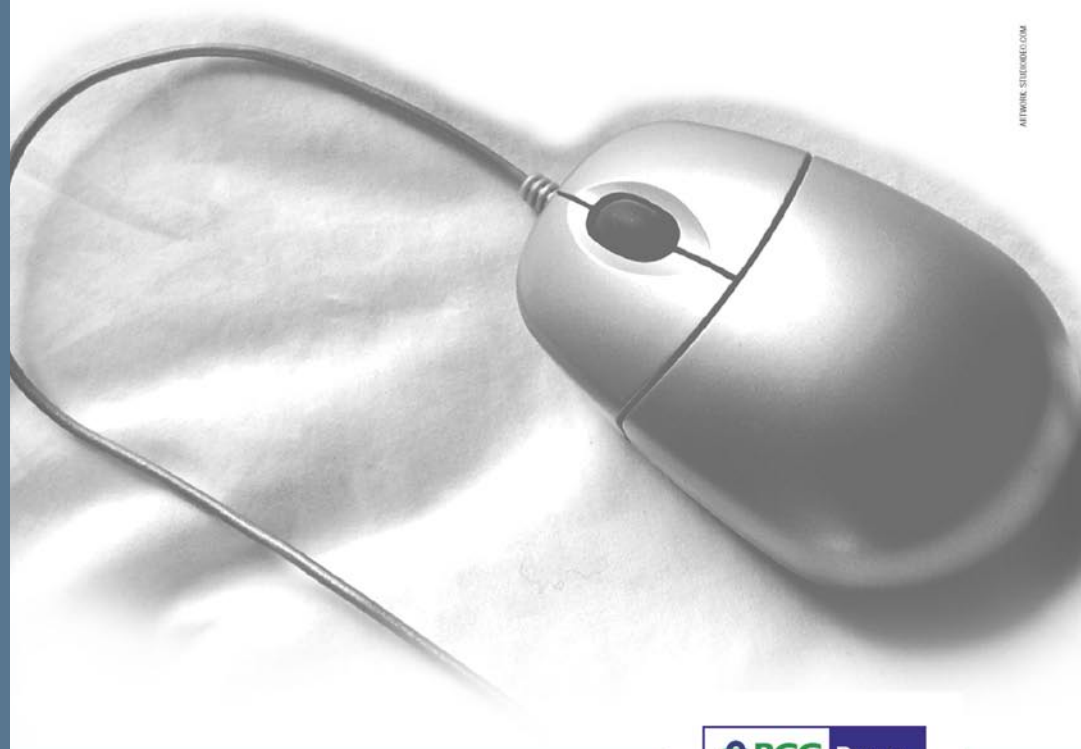
RELAX BANKING

QUANDO LA TECNOLOGIA
TI SEMPLIFICA LA VITA



Rilassati, la tua banca é aperta giorno e notte, senza orari. Mettiti comodo. Grazie a Relax Banking **puoi accedere** a tutte le informazioni relative ai tuoi conti correnti direttamente da casa, **ovunque** tu abbia a portata di mano una connessione internet o un telefono cellulare GSM.

PER LA FAMIGLIA E L'IMPRESA



Message pubblicitario con finalità promozionale. Le condizioni economiche e le principali clausole contrattuali sono riportate sui fogli informativi disponibili presso ogni sportello - D.Lgs. 17/1/1999 n. 286.

ATTORINE STEREO.COM

Banca di Credito Cooperativo di Roma
Via Sardegna, 129 - 00187 Roma
Tel. 06.52861 - Fax 06.52863305
www.bccroma.it



DIFFERENTE PER FORZA.