

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
Reparto Polizia Postale e delle Comunicazioni

MTK METAKOM2005©



**Casse Rurali
Trentine**

Indice

Parte Prima

- I La moneta Elettronica: regole di sicurezza** pag 4
 - Ricevere a casa Bancomat e Carta di Credito pag 5
- II Prelievi e pagamenti con le carte** pag 6
 - Bancomat pag 6
 - Carta di Credito pag 7
- III Che cosa si rischia?** pag 9
 - 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 13
 - La sicurezza di acquistare in internet pag 13
 - Che cosa si rischia pag 16
 - Sicurezza: l'utilizzo delle password pag 19
- V Le regole d'oro** pag 20

Parte Seconda

- VI Vademecum per le emergenze** pag 22
 - Memorandum dei dati pag 23
 - Bancomat pag 24
 - Assegni pag 25
 - American Express pag 26
 - Cartasi pag 27
 - BankAmericard pag 28
 - Diners Club International pag 29
 - Libretto deposito a risparmio, Certificato di deposito pag 30
 - Tessera Viacard pag 31

Gentile Cliente,



tutti, oggi, abbiamo in tasca, oltre al tradizionale libretto degli assegni, carte magnetiche e strumenti che ci permettono di gestire il nostro denaro in modo semplice ed immediato con facilità, 24 ore su 24. Sono sempre di più le persone che usano regolarmente le carte di pagamento per comperare e fare spese: dal conto del ristorante alla benzina, dal profumo al pedaggio in autostrada...ecc., Bancomat, Carte di credito e debito, Viacard ecc., la cosiddetta moneta elettronica ci semplifica la vita ma è importante non trovarsi impreparati di fronte a quei piccoli imprevisti che possono capitare: come ad esempio il furto o lo smarrimento. Abbiamo realizzato una breve Guida suddivisa in due parti. La prima parte riguarda gli accorgimenti da utilizzare quando si effettuano prelievi e pagamenti con la moneta elettronica per evitare che qualcuno possa impossessarsi del numero della Carta e del codice segreto Pin (Personal Identification Number), e inoltre spiega come non diventare vittime di possibili truffe e raggiri, anche per chi utilizza internet per fare acquisti. La seconda parte contiene un vero e proprio Vademecum, per fornirLe in dettaglio quelle informazioni necessarie per sapere che cosa fare e come comportarsi in tali spiacevoli circostanze.



La moneta elettronica: regole di sicurezza

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), la alterazione del Pos (lo strumento che legge i dati sulla banda magnetica, presente nei punti vendita e negozi), la manomissione (spesso ben camuffata) degli Atm (postazioni di prelievo dei contanti con il 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 in-

formazioni 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 effettuare ricerche ed azioni coordinate di intervento.

Ricevere a casa 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 Pin. Verificate attentamente che non vi siano rotture anche all'interno della busta e del cartoncino che contiene la tessera. Diffidate di buste bianche inviate con posta prioritaria o con francobolli perché solitamente l'invio avviene con buste con la tassa già pagata. 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 esempio il numero della Carta di Credito). In questo caso controllate con più attenzione l'estratto conto. Questo tipo di raggio si chiama "boxing".

Prelievi e pagamenti con le carte







Bancomat

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

- ⚠️ • 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 strane sporgenze (se prelevate spesso o sempre nello stesso Atm, vi sarà più facile notare la difformità). Soprattutto scrutate che non vi siano micro telecamere ad altezza della tastiera o "oggetti strani" attaccati nei pressi (magari 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 sia ben fissata perché vi potrebbe essere una tastiera falsa posizionata 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 è bene allontanarsi e 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, fermarsi 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.

Carta di Credito

Come sempre la sicurezza deriva prima di tutto da uno stato di atten-

zione, 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 in alcuni paesi esteri dove sono stati segnalati casi in cui il negoziante portava la tessera 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 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: 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 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 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 con cura fino a che non abbiate controllato l'estratto conto del mese.

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 i cosiddetti "dati sensibili" (ad esempio il numero della Carta di Credito, 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.



Fig.1 Riuscite a vedere lo skimmer?

La clonazione: cioè il duplicato illecito

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 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 o del 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 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 di gestione



Fig.2 Ecco!

per bande magnetiche, potranno essere trascritti i dati, presi illecitamente, su un supporto plastico con le caratteristiche di una Carta di Credito/Bancomat. Per impossessarsi invece del codice Pin, che non è in alcun modo ricavabile dalla banda magnetica, i truffatori utilizzano generalmente una microtelecamera nascosta (fig. 3 e fig.



Fig.3 La microcamera è nel porta depliant

4) che filma la digitazione dei numeri del Pin (codice segreto) e che solitamente trasmette (fig. 5) il Pin 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**



Fig.4 Ecco la microcamera

uno sportello Atm basta fare un po' di 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 un po' di attenzione.

Trashing: consiste nella ricerca degli scontrini delle Carte di Credito (che riportano il numero della tes-

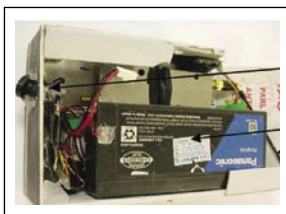


Fig.5 La microcamera e trasmittente

sera 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 sullo 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.



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.

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 le transazioni 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 inverosimile ed 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 seguendo qualche semplice precauzione. Per gli acquisti on-line i pagamenti possono essere realizzati con differenti modalità, si va dal bonifico bancario, al vaglia postale, al contrassegno, all'utilizzo di sistemi proprietari di pagamento, alla Carta di Credito, alle carte prepagate, ecc.



Spesso comunque viene utilizzata la Carta di Credito, sia per la facilità di impiego, sia per l'elevato tasso di diffusione e affidabilità 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 tessera. 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 remota, se ci si comporta con la indispensabile 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 moneta virtuale è semplice, comodo, e sicuro, i negozi internet 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 si pratichi il "commercio elettronico", cioè l'acquisto on-line via internet:

- 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 od il venditore). 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 sul 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 circa l'affidabilità della stessa;
- verificare che il sito presso il quale si intende acquistare un bene utilizzi protocolli di sicurezza che permettano di identificare l'utente. Il più diffuso è il Secure Socket Layer (SSL). 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 che sta a significare che in quel momento la connessione è protetta da intrusioni ed è sicura;
- inserite i vostri dati economici solamente quando sono rispettate le condizioni di sicurezza e comunque non comunicate mai i dati della vostra tessera o altri dati riservati tramite e-mail;
- fornite solo le informazioni indispensabili, informazioni troppo personali in particolare quelle relative al proprio conto corrente possono mettervi a rischio;



per effettuare una transazione con Carta di Credito i dati più importanti sono: numero della Carta di Credito e relativa scadenza: proteggeteli!



- esistono nel mercato Carte di Credito "virtuali" che utilizzano un codice differente per ogni acquisto



come se ogni volta 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 richiedere la trasmissione dei dati relativi solo ad una piccola somma, piuttosto che quelli di un intero conto corrente;



- nel caso in cui si utilizzi il programma di internet banking, controllate il vostro estratto conto dopo aver effettuato pagamenti on-line, in modo da agire tempestivamente qualora si disconoscessero delle spese addebitate;



- è necessario, sempre, 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 di frodi, che per chi intende acquistare on-line è bene tener presente, ma che sicuramente possono essere neutralizzate con facilità se si fa un po' di attenzione. I criminali informatici sono disciplinati dalla legge 547 del 1993 che ha operato delle modifiche al Codice penale, punendo penalmente le più diffuse condotte criminose nel settore informatico come 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 e la violenza sui beni informatici. Ecco alcuni dei crimini informatici più frequenti:

Phishing: è una tecnica che consiste nell'inviare messaggi di posta elettronica, "mascherati" da messaggi ufficiali inviati da parte di una banca o di un ente 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 la banca o le Forze dell'ordine avendo l'accortezza di non cancellare l'e-mail ricevuta.

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 tracce 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 nascosto tra i file di sistema di alcuni programmi scaricabili (gratuitamente o a pagamento) da internet, in grado di raccogliere

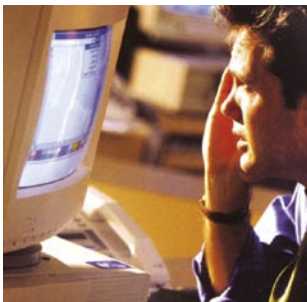


informazioni specifiche riferite alla postazione (computer) nella quale si è installato, tali dati vengono poi trasmessi ad insaputa dell'utilizzatore del PC ad un altro PC (server remoto) quando ci si collega in rete. Quindi prima di scaricare un programma bisogna fare attenzione a quello che si sta facendo, e se si ha anche il minimo dubbio: informarsi ed 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. 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. 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. Infatti, anche se è una eventualità assai remota, può accadere che un utilizzatore inesperto, che stia utilizzando una postazione senza antivirus né firewall, possa inavvertitamente "scaricare" dei programmi speciali cosiddetti "spyware", che di nascosto dall'utente, riescono a "leggere" le parole che vengono digitate sulla tastiera, riuscendo, in qualche modo, a "catturare" eventuali dati sensibili come password, numero di Carta di Credito, ecc., quando questi vengono digitati.



Sicurezza: l'utilizzo delle password

Solitamente prima di effettuare un acquisto on-line il sito web del venditore richiede una registrazione che consente di identificare il cliente attraverso un semplice codice identificativo, in questo modo ad un acquisto futuro il sito web "ci riconoscerà" e non sarà più necessario fornire i nostri dati. I dati della registrazione possono contenere i nostri dati anagrafici, il codice fiscale, l'indirizzo al quale solitamente vogliamo che la merce arrivi ecc. In alcuni casi il sito web richiederà già dalla fase di registrazione i dati relativi alla vostra Carta di Credito, viceversa in altri casi inserirete tali dati solo nel momento in cui state perfezionando l'acquisto on-line. 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 protetta. 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, da proprio PC senza recarsi in banca. È quindi 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 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 vostre password e comunque, se le scrivete, non lasciatele in posti facilmente accessibili.

V Le regole d'oro

- 1** Duplicare e conservare copia, in luogo sicuro, di tutti i documenti personali (compresi gli estremi del Bancomat e delle Carte di Credito e le password, 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 la tessera, lontano da fonti magnetiche ma anche da altre tessere o elementi metallici (per evitare la sua smagnetizzazione e la conseguente richiesta di sostituzione); attenzione anche, per lo stesso motivo, a non graffiare la banda magnetica.
- 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 dal/i gestore/i della/e tessera/e per eventuali blocchi 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 Conservate fatture, ricevute fiscali e contratti di tutto quello che avete acquistato on-line, in modo da essere precisi e documentati per qualsiasi evenienza.

6 Chiedete sempre l'identità del vostro interlocutore; sappiate che i mistificatori si possono nascondere ovunque.

7 Controllate sempre gli estratti conto forniti dalla società di gestione della tessera. Non lasciate in giro o buttate le copie contabili di pagamenti e prelievi ancora leggibili, nella spazzatura.

8 Evitate di fornire il numero di tessera, soprattutto ad interlocutori telefonici.

9 Imparate l'ubicazione degli uffici delle Forze dell'ordine.

10 Denunciate immediatamente il furto o lo smarrimento delle Carte di Credito, dei libretti degli assegni e della pensione e di tutti quei documenti che possono essere oggetto di contraffazione e di illecita e immediata utilizzazione.

11 Avvaletevi di forme assicurative, depositi di sicurezza e ogni altro mezzo atto alla diminuzione del pericolo e del danno derivante dalla iniziativa di malintenzionati.

12 Se vi recate all'estero od in Paesi poco sicuri o se non vi fidate di un sito web effettuate pagamenti con le cosiddette carte o tessere pre-pagate che consentono di spendere solo la cifra per la quale sono abilitate in quel momento.



VI **Vademecum** per le emergenze

In questa parte della Guida è possibile trovare tutte quelle informazioni necessarie per far fronte ai casi di emergenza come furto

o smarrimento delle tessere Bancomat, Carta di Credito, Viacard ed inoltre del libretto degli assegni, dei certificati di deposito..ecc.. Insomma un breve vademecum per sapere come comportarsi in queste eventualità, in modo che si possa agire con la necessaria prontezza e determinazione, al fine di evitare spiacevoli ed onerosi inconvenienti. Troverete qui riportate le norme di comportamento da attuare qualora vi doveste trovare nella condizione sgradevole di aver smarrito o che vi abbiano sottratto illegalmente il Bancomat e gli altri gli strumenti per effettuare pagamenti o prelievi od i documenti che attestano le vostre proprietà detenute presso la banca. In questi casi è necessario agire con prontezza ed avvisare immediatamente la banca, per evitare che malintenzionati possano porre in essere comportamenti lesivi delle vostre proprietà. Nella pagina qui a fianco abbiamo riportato un memorandum riassuntivo compilando il quale potrete "memorizzare" i dati relativi alle vostre tessere, in modo da poter disporre in maniera immediata, in caso di occorrenza, di quelle informazioni necessarie per poter affrontare una situazione di emergenza.



Memorandum dei dati



In caso di perdita o furto del Bancomat o della Carta di Credito ecc., è importante averne immediatamente disponibili gli estremi. Qui accanto si potranno trascrivere quelle informazioni utili in una situazione di emergenza:

Carta di Credito

n. _____ Scadenza _____

n. _____ Scadenza _____

n. _____ Scadenza _____

Bancomat

n. _____ Scadenza _____

n. _____ Scadenza _____

Viacard

n. _____ Scadenza _____

n. _____ Scadenza _____

Libretto assegni

n. _____

n. _____

Conto corrente

n. _____

n. _____

N.B. Conservare questi dati con attenzione e custodirli in un luogo sicuro.

*Se smarrite o vi
rubano...*

Bancomat



Se vi rubano o smarrite il Bancomat, la tempestività di denuncia è importante per evitare che qualcuno senza scrupoli possa abusare di ciò che è vostro, prelevando a vostra insaputa del denaro o tentando una truffa.

1 Si deve avvertire subito la filiale della banca che ha emesso la tessera telefonando o recandosi personalmente. In alternativa si potrà chiamare l'apposito **Numero Verde**

800-82.20.56 anche nei giorni festivi e in orari non lavorativi. Se vi trovate all'estero il numero da chiamare per il blocco del Bancomat è **+39 02.45.40.37.68**

2 Si dovrà quindi denunciare l'accaduto alle Autorità di Pubblica Sicurezza, e consegnare una copia della denuncia alla filiale per integrare la documentazione. Quindi si potrà richiedere l'emissione di un nuovo Bancomat avendo cura di ricevere (e memorizzare) il nuovo codice personale segreto (Pin).

Perdita del Pin. Anche nel caso di smarrimento o sottrazione solo del codice personale segreto (Pin) ci si dovrà comportare come sopra, in questo caso si deve restituire anche la carta Bancomat.



*Se smarrite o vi
rubano...*

Assegni



Sia per il furto o lo smarrimento di:

- Assegni di Conto Corrente
- Assegno bancario emesso
- Assegno Circolare emesso

dovrete denunciare l'accaduto alla banca e contemporaneamente depositare circostanziata denuncia alle Autorità di P.S. (Carabinieri o Polizia).

1 La denuncia dovrà contenere la data e le modalità di sottrazione o smarrimento, i dati

identificativi del titolo (data emissione, numero assegno, c/c di traenza, beneficiario, ecc.), e dovrà essere consegnata in copia alla banca che istruirà per vostro conto la "procedura di ammortamento" del titolo (tempi dai 3 ai 6 mesi).

2 Nel caso invece di Assegno bancario o Circolare emesso con la clausola della "non trasferibilità" non si fa luogo alla "procedura di ammortamento", ma il presentatore o il beneficiario potrà ottenere un duplicato: decorsi 20 gg (dalla denuncia alle Autorità di Pubblica Sicurezza), se si tratta di assegno circolare; immediato se si tratta di assegno bancario.

N.B. Nel caso di un assegno bancario o circolare di un'altra banca diversa dalla vostra, bisogna contattare subito la banca sulla quale l'assegno bancario è stato tratto o che ha emesso l'assegno circolare disperso o rubato per attivare la procedura necessaria.



Se smarrite o vi rubano...

American Express



In caso di perdita o furto della Carta American Express la prima cosa da fare è telefonare al Servizio Clienti al numero telefonico 06.72.282.

1 Presentare denuncia all'Autorità di Pubblica Sicurezza e conservarne una copia per eventuale richiesta da parte della società emittente. È opportuno informare la filiale della banca presso la quale si intrattiene il rapporto di conto corrente di appoggio.

2 Confermare quanto preannunciato nella telefonata e richiedere una nuova tessera per iscritto, a mezzo raccomandata A.R., allegando copia conforme della denuncia presentata alle Autorità di Pubblica Sicurezza, a:
American Express Services Europe Limited - Largo Caduti di El Alamein, 9 00173 ROMA

N.B. Particolare attenzione deve essere prestata dal titolare agli estratti conto che arriveranno, per verificare che non ci siano operazioni che egli disconosce. Nel caso in cui ciò avvenisse, dette operazioni dovranno essere segnalate entro un termine prefissato, con raccomandata A.R. all'Ufficio Servizio Clienti.



Se smarrite o vi rubano...

Cartasi



Per prima cosa si deve avvisare telefonicamente chiamando immediatamente il Servizio Clienti di CartaSi:

Numero Verde in Italia **800-15.16.16**

Numero Verde in USA **1.800.4736.896**

Numero dall'estero +39 02.3498.0020

(Si accettano chiamate a carico del destinatario).

1 Presentare la denuncia alle Autorità di Pubblica Sicurezza competenti

(da conservare per almeno 12 mesi).

2 Solo nel caso di contestazione di un eventuale utilizzo illecito della tessera, il titolare dovrà inoltrare a Servizi Interbancari - Ufficio Dispute Titolari - una lettera di contestazione firmata con la copia della denuncia e dell'estratto conto riportante la spesa contestata. Il duplicato viene emesso automaticamente per tutte le carte, salvo quelle con funzione Bancomat e PagoBancomat, che devono essere richieste nella filiale. Il duplicato è solitamente gratuito.

N.B. Se la tessera è abilitata alla funzione Bancomat e PagoBancomat, il titolare deve provvedere anche a chiamare l'Ufficio Blocchi della S.I.A. (che gestisce il servizio) al **Numero Verde 800-82.20.56**

N.B. Il blocco della tessera ne inibisce immediatamente l'utilizzo in tutto il mondo. Anche in caso di smarrimento o sottrazione del solo codice personale segreto contattare Servizi Interbancari.



Se smarrite o vi rubano...

BankAmericard



In caso di furto o smarrimento della carta BankAmericard, per prima cosa, si deve avvisare immediatamente il Servizio Clienti chiamando il **Numero Verde 800-20.71.67**. Se ci si trova all'estero telefonare al: +39 0432 744 106.

1 Effettuare la denuncia all'Autorità di Pubblica Sicurezza (Carabinieri o Polizia) e consegnare una copia della denuncia alla propria filiale di riferimento, la quale provvederà ad espletare le formalità del caso. Il duplicato della tessera va richiesto alla filiale stessa.

2 Se la tessera è abilitata alla funzione Bancomat e Pagobancomat, il titolare deve provvedere anche a chiamare l'Ufficio Blocchi della S.I.A. al **Numero Verde 800-82.20.56**

N.B. Particolare attenzione deve essere prestata dal titolare agli estratti conto che arriveranno, per verificare che non ci siano operazioni che egli disconosce. Nel caso avvenga, dette operazioni dovranno essere segnalate entro il termine prefissato.



Se smarrite o vi rubano...

Diners Club International



Pin (personal identification number) telefonare allo 06.35.75.333.

In caso di perdita o furto della Carta Diners Club telefonare al Numero Verde Servizio Sicurezza smarrimento e furto: **800-86.40.64** (operativo 24 ore su 24, 365 giorni all'anno). Per lo smarrimento del

1 Sporgere denuncia all'Autorità di Pubblica Sicurezza (Carabinieri o Polizia) e conservarne una copia per eventuale richiesta da parte della società emittente. È consigliabile comunque avvisare la filiale della banca che ha richiesto la tessera consegnando copia della denuncia.

2 Confermare quanto preannunciato nella telefonata e richiedere una nuova tessera per iscritto, a mezzo raccomandata A.R., allegando copia conforme della denuncia presentata alla Pubblica Sicurezza, a: Diners Club Europe S.p.a - Ufficio Sicurezza Lungotevere Flaminio n. 18 - 00196 Roma.

N.B. In caso di furto o smarrimento della Tessera all'estero è necessario contattare il Servizio Sicurezza al numero telefonico: +39063213841 in funzione 24 ore su 24. Sarà inviata una Tessera d'emergenza entro le 48 ore circa.



Se smarrite o vi rubano...

Libretto Deposito a risparmio

Certificato di Deposito



In caso di perdita o furto di Libretti sia del "Deposito a Risparmio" e "Certificati di Deposito al portatore", e sia di "Deposito a Risparmio nominativo", è necessario, rivolgersi alla filiale di riferimento per denunciare l'accaduto.

1 Nello stesso tempo si deve presentare circostanziata denuncia di furto o smarrimento alle Autorità di Pubblica Sicurezza (Carabinieri o Polizia). Tale denuncia dovrà inoltre essere depositata in copia presso la banca, la quale potrà così istruire

la "procedura di ammortamento" del libretto.

2 Per i Libretti nominativi invece è sufficiente consegnare la denuncia effettuata alla banca, la quale decorsi 90 giorni senza opposizioni provvederà all'emissione del duplicato.



Se smarrite o vi rubano...

Tessera Viacard

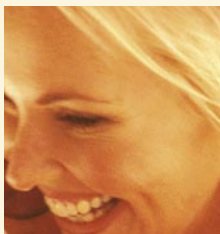


In caso di smarrimento o furto, il titolare della Viacard, deve darne immediata comunicazione alla Società Autostrade inviando un fax ad uno dei seguenti numeri: 06/4363.4050 - 055/4202.373 - 055/4202.370.

1 Sporgere denuncia all'Autorità di Pubblica Sicurezza (Carabinieri o Polizia) e conservarne una copia da allegare alla comunicazione che dovrà essere inoltrata entro 30 giorni alla Società Autostrade. È consigliabile avvisare la filiale della banca che ha richiesto la tessera consegnando copia della denuncia.

2 Confermare quanto preannunciato nella telefonata e descrivere l'accaduto in una lettera indirizzata, a mezzo raccomandata A.R., allegando copia conforme della denuncia presentata alla Pubblica Sicurezza, a: Società Autostrade - Direzione Generale Uffici di Firenze Casella Postale 2310 - 50100 Firenze Ferrovia.

N.B. Se una Viacard C/C (o Plus) risulta deteriorata il cliente deve spedirla in busta chiusa a: Ufficio Gestione Operativa Clienti CP 2310 Ferrovia - 50100 Firenze, oppure consegnarla direttamente presso un qualsiasi Punto Blu o Ufficio commerciale della Società Autostrade. Verrà restituita appena risanata o sostituita.





Casse Rurali
Trentine

WWW.CR-SURFING.NET

SICUREZZA

attiva il servizio di Alert, riceverai un SMS ad ogni prelievo o pagamento, superiore alla soglia prescelta, effettuato con la tua Carta Bancomat.

Potrai anche sospendere e poi riattivare l'operatività all'estero della Carta Globo o Universicard, inviando un SMS o chiamando la tua Cassa Rurale.

RICARICA CELLULARE

con un semplice SMS puoi ricaricare il cellulare.

INFOSMS

Controllo totale



le Banche delle nostre comunità