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

LE GUIDE UTILI

GUIDA ALLE CARTE DI PAGAMENTO ED ALLA MONETA ELETTRONICA

Prevenzione delle frodi e delle truffe nei sistemi di pagamento e nell'utilizzo della moneta elettronica

La Valsabbina 1898
BANCA VALSABBINA

"....alcuni semplici comportamenti e regole...."

Le Carte di pagamento e la moneta elettronica (pagamenti on-line) ci consentono oggi una grande comodità: gestire il nostro denaro in modo semplice e pratico 24 ore su 24. Ma è importante non trovarsi impreparati sia di fronte a quei piccoli imprevisti: come ad esempio il furto o lo smarrimento sia anche ai tentativi di truffa come il furto di identità digitale, la clonazione ecc. Questa Guida illustra alcuni semplici comportamenti che rendono l'impiego della moneta elettronica oltre che vantaggioso, sicuro ed inoltre spiega cosa fare qualora ci accadesse di trovarci vittime di un tentativo di truffa o in una situazione di emergenza. Buona lettura.

Indice

Carte di Pagamento e Moneta elettronica: le regole di sicurezza 1

La moneta elettronica (Bancomat, Carta di Credito, Carta prepagate, transazioni on-line ecc.) ci fa risparmiare tempo, è comoda, semplice da utilizzare e ha migliorato la nostra vita quotidiana. **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 è ormai 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 garantiscono tranquillità e sicurezza.

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 e le truffe on-line. Le Forze dell'ordine hanno in questi anni dato vita ad una

sempre più stretta collaborazione con l'ABI (Associazione Bancaria Italiana) e con le Banche al fine di prevenire e circoscrivere tali fenomeni. Esiste anche il supporto di una **banca dati a livello europeo che raccoglie informazioni sulle Carte clonate** od illegali e un Nucleo di indagine Comunitario specializzato che permette in brevissimo tempo di attivare, in collaborazione con gli altri Paesi europei, indagini ricerche e 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 la busta sia integra e che provenga dalla vostra banca (o da chi emette la Carta). Inoltre verificate attentamente che **non vi siano rotture all'interno della busta ad esempio del cartoncino al quale è attaccata 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 raggiro si chiama "boxing"**.

Prelievi e pagamenti con le carte 2

Prelevare e pagare con il Bancomat

Quando prelevate denaro contante con la vostra Carta di Debito (Bancomat, Pagobancomat, ecc..) da uno sportello ATM (Automatic Teller Machine) meglio conosciuto come postazione Bancomat **vi suggeriamo di**:

- accertarvi che nelle immediate vicinanze non vi siano **persone ferme in atteggiamento sospetto** o con telecamere;
- osservare sempre attentamente la "postazione": tastiera al piano, lo spazio sopra al video, fessura ecc. che **non devono presentare anomalie o strane sporgenze** (se prelevate spesso nello stesso ATM vi sarà più facile notarlo). Soprattutto accertatevi che non vi siano "oggetti strani" **attaccati** alle pareti od intorno ad esempio sono state trovate **microtelecamere nascoste nel porta depliant** appeso di lato;
- verificare la bocca della fessura: la **fessura dove va inserita la Carta deve essere fissa** e non muoversi. La Carta deve poter essere inserita nella fessura senza alcuno sforzo. Se la **Carta fatica ad entrare e va spinta potrebbe essere stato inserita** in alto nella fessura una sottilissima **Card digitale che con-**

tiene uno "skimmer", piccolo *microchip* in grado di leggere i dati contenuti nella Carta memorizzandoli a propria volta o trasmettendoli subito tramite la tecnologia wireless ad un "Lettore" poco distante, ad esempio parcheggiato in auto. Se la fessura si muove potrebbe significare che essa sia stata manomessa o che ad esempio le sia stata applicata sopra una **finta fessura che contiene uno "skimmer"**;

⚠ 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 l**a tastiera non sarà a livello del piano**;

⚠ digitare il Pin, **coprendo la mano che digita con l'altra** in modo che nessuno o nessuna telecamera possa "leggere" le cifre del Pin. Soprattutto non dite **mai ad alta voce i numeri del Pin** perché spesso insieme allo skimmer può esservi **un microregistratore audio che può registrare ciò** che avete pronunciato;

⚠ ricordare che nel caso solo dopo 3 tentativi consecutivi di digitazione errata del Pin la Carta viene trattenuta automaticamente all'interno dell'apparecchio e poi spedita alla banca emittente. Per recuperarla bisogna rivolgersi alla filiale di competenza.

⚠ fare attenzione ai **pagamenti** nei negozi, supermercati, pompe di benzina...se vi dicono che il POS è in un'altra stanza, **non rivelate assolutamente il vostro Pin** e offritevi di accompagnare la persona;

! 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. 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 Carta. A volte è meglio affrontare un piccolo inconveniente come cambiare la Carta piuttosto che essere vittime di una truffa.**

Carte con il chip e "contactless"...oggi il futuro!

Le nuove Carte introdotte in anni recenti hanno anche la presenza di un **microchip**, grazie alla crittografia il "chip" è al riparo da accessi esterni non autorizzati e consente metodi di autenticazione del "titolare" che rendono la Carta estremamente sicura contro tentativi di contraffazione. E' possibile utilizzare normalmente la Carta con microchip in tutti gli esercizi commerciali in Italia (ed in area euro), lì dove sono presenti i terminali Pos di seconda generazione viene "letto" il microchip (e dovrete digitare il Pin della Carta di Credito) altrimenti continua ad essere "letta" la banda magnetica (e dovrete firmare lo scontrino). **Sono state recentemente immerse in commercio alcuni tipi di carte di pagamento dette "contactless"** ("senza contatto"), che a differenza delle Carte tradizionali, dotate di banda magnetica o microchip, non richiedono l'inserimento fisico della Carta nella fessura del lettore POS ma è sufficiente il suo posizionamento sopra. Questa funzione è possibile solo in presenza di apposito "lettore POS" abilitato. Il vantaggio è rendere la procedura di pagamento più rapida (la transazione viene effettuata senza digitare il Pin o firmare la ricevuta), questa funzione vale ad oggi solo per i piccoli importi e di solito fino ad un limite di 25 euro.

Pagare e prelevare con la Carta di Credito

Come sempre la sicurezza deriva prima di tutto **dall'attenzione e da un atteggiamento di prudenza**. Per ciò è bene avere presente che qualsiasi utilizzo della Carta di pagamento, sia in negozio che in internet comincia dal processo di "autenticazione" (identificazione) della Carta e del Titolare, ecco perché i dati personali e la loro attenta custodia (identità del Titolare, numero e dati della Carta, codice Pin...) sono importantissimi!

Si può ben comprendere allora come sia fondamentale prevenire, attraverso una attenta custodia dei propri dati, il "furto d'identità", un crimine perpetrato senza che i ladri entrino in casa vostra. Sono molti i modi attraverso i quali si può subire il furto dell'identità: questi vanno dal semplice furto del portafoglio, all'apertura dell'immondizia, fino alla ricerca di informazioni in internet (ad es. i *social network*). Di solito le vittime scoprono troppo tardi di essere state derubate della propria identità, ossia quando iniziano a ricevere richieste di pagamento per rate non rimborsate o addebiti per beni che non hanno acquistato.

In ragione di questo come afferma **il Garante della Privacy**: "la forma di **tutela più efficace** è comunque sempre l'autotutela, cioè la **gestione attenta dei propri dati personali**", ma esistono specifiche ed efficaci procedure di sicurezza nell'utilizzo della Carta di Credito che se impiegate rendono i pagamenti elettronici estremamente sicuri oltre che comodi. I pagamenti elettronici possono svolgere un ruolo nella ripresa economica: basta pensare alla questione dei flussi turistici. **A titolo di esempio** è bene sapere che: per quello che riguarda i pagamenti on-line per acquisti/spese **nel web oltre ai dati della Carta il sistema richiede l'inserimento del Codice di sicurezza CSC o CVV2** che è un codice di sicurezza di tre o quattro cifre presente nel retro o nel fronte della Carta di Credito. Potrà talora capitare anche il caso di una transazione che oltre al **Codice di sicurezza** richieda, come forma di maggior tutela l'utilizzo del **codice numerico generato dell'OTP** (One time Password) o **Token**, che è un piccolo generatore di codici di accesso (visualizzati sul display dello stesso "apparecchietto") e di solito consegnato in Banca per navigare con assoluta sicurezza nel proprio Internet Banking e che genera le cosiddette password "dispositive".

E' bene comunque al momento della transazione osservare alcune semplici regole:

non perdete mai di vista la Carta di Credito, se state facendo un acquisto **dovete pretendere** che al momento della transazione (cioè il passaggio/inserimento 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 il circuito che autentica la Carta si basa ancora esclusivamente sulla Banda magnetica (e quindi non vi richiederà di digitare il Pin, ma dovrete firmare la ricevuta) e 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;

⚠ **nel caso di addebiti di spesa impropri**: se vi arriva un estratto conto con addebiti per spese che non avete fatto, **avvisate l'emettitore della Carta, la Banca per conoscenza, e quindi denunciate alle Forze dell'ordine** la clonazione della Carta, disconoscendo con una lettera circostanziata e formale le spese addebitate;

⚠ un capitolo a parte sono gli acquisti fatti in internet. Nel caso di **acquisti sul web** dovete verificare che **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 della Carta;

⚠ molte Carte di Credito consentono di prelevare denaro contante dagli sportelli ATM, nel caso lo facciate seguite le indicazioni del paragrafo precedente e ricordate che solo dopo 3 tentativi consecutivi di digitazione errata del Pin la Carta viene trattenuta automaticamente all'interno dell'apparecchio e poi spedita alla banca emittente. Per recuperarla bisogna rivolgersi alla filiale di competenza;

⚠ dopo un acquisto con la Carta di Credito **non buttate mai la ricevuta consegnata dall'esercente** ma conservatela fino a che non abbiate **controllato l'estratto del mese**, quindi **strappatela in pezzi** e gettatela.

Che cosa si può rischiare? 3

Il principio è semplice: una volta entrati in possesso dei dati o dell'originale, è possibile, da parte dei malintenzionati, duplicare (clonare) una Carta di pagamento. È allora **importante conoscere quali possono essere le situazioni nelle quali si corre il rischio che ci vengano sottratti oltre alle carte anche i cosiddetti "dati sensibili"** (furto di identità: il numero della Carta di Credito, il Pin costituiscono una parte della nostra Identità digitale). Usando un po' di accortezza è possibile accorgersi rapidamente di quegli eventuali trucchi che un malintenzionato stia cercando di mettere in atto nei vostri confronti e agire prima che sia troppo tardi.

✓ La clonazione della Carta: cioè il duplicato illecito

Con l'introduzione delle Carte **con il microchip la clonazione integrale della Carta di pagamento è stata resa praticamente impossibile. "Le attuali Carte di credito e di debito usano una doppia tecnologia: hanno i dati registrati sia sulla banda magnetica sia sul chip. Il chip non si può clonare ma la banda magnetica...è possibile clonarla."** (Antonio Lioy, professore al Politecnico di Torino, esperto di Sicurezza Informatica, intervista a la Repubblica).

Quindi il problema non è tanto legato alle tecniche di raggiro e truffa od alla tecnologia quanto piuttosto legato alla nostra disattenzione o ad un basso livello di attenzione nell'impegno a proteggere i nostri "dati personali e sensibili" digitali e non, infatti senza il Pin (codice segreto) nessuno può utilizzare la nostra Carta di Credito o di Debito o la Ricaricabile anche se sottratta o clonata.

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

Fig.1 Riuscite a vedere lo skimmer? è nascosto all'interno della finta fessura!

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. **Quindi va introdotto nella fessura,** infatti lo "skimmer" è un **congegno di dimensioni ridotte (fig. 3) e non ha una forma standard,** solitamente è molto più piccolo di un pacchetto di sigarette, a volte **può essere sottile poco di più di un foglio di carta**. Lo "skimmer" è spesso alimentato con batteria e ricopia ("immagazzina") i dati presenti nella banda magnetica: nome, cognome e data

Fig.2 La microcamera nascosta nel portadepliant inquadra la tastiera .....

Fig.3 Lo skimmer è più piccolo un accendino. Un esempio di tastiera posticcia

di scadenza della Carta, nonché il codice di verifica trasmesso elettronicamente per confermare la validità della Carta stessa. Una volta che lo "skimmer" sarà collegato ad un computer 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 (una semplice Carta con Banda magnetica) 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. 2) 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 porre 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.

Trashing: consiste nella **ricerca degli scontrini delle Carte di pagamento (che riportano il numero della Carta e altri dati sensibili)** che erroneamente **gettia-**

Strappate le ricevute prima di buttarle. Un es. di "cordino" che blocca la Carta

mo 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 della Carta.

⚠ **Lebanese loop**: è una tecnica di manomissione dello sportello ATM (Postazione Bancomat). Con questa tecnica il truffatore entra in possesso del Bancomat e del relativo Pin. Viene **applicato un dispositivo che blocca la Carta (ad es. "un cordino") all'interno dello sportello**, il cliente **viene "soccorso" dal truffatore che lo invita a digitare il Codice Pin** (questo permette al ladro di memorizzare la sequenza segreta), quindi non **appena il titolare della Carta si allontana, il truffatore provvede a recuperare la Carta** per poi utilizzarla **con il Pin appena "memorizzato"**.

⚠ **Cash trapping**: è una tecnica molto semplice e consiste nell'inserimento di un "piccolo oggetto", **solitamente una piccola "forcella", nella fessura dell'ATM da cui escono le banconote**. In questo modo l'oggetto metallico **blocca la fuoriuscita delle banconote**, nonostante sul monitor venga visualizzata la regolarità dell'operazione di prelievo, correttamente riuscita. **Se il cliente, magari dopo aver riprovato l'operazione, si allontana, i malviventi ne approfitteranno per rimuovere l'oggetto metallico ed appropriarsi dei soldi** rimasti incastrati nella feritoia. In questo caso si consiglia di chiamare **l'assistenza della Banca e le Forse dell'Ordine e rimanere presso l'ATM**.

Internet e gli acquisti nel Web 4

In questa parte elencheremo le altre tipologie di truffe che riguardano le transazioni e gli acquisti effettuati on-line. Anche tali truffe possono essere neutralizzate da un acquirente attento e che protegge i propri dati.

✓ Contante, negozi on-line e pagamenti elettronici

Gli strumenti di pagamento alternativi al contante stanno progressivamente diventando sempre più uno strumento utilizzato dagli italiani anche per le recenti normative che prevedono limiti di utilizzo delle banconote ed obblighi da parte delle categorie economiche di utilizzo di Pos e strumenti della moneta elettronica. Da una recente ricerca Doxa per *Federconsumatori* emerge che il **61% degli Italiani intervistati ha usato la Carta di pagamento per acquisti on-line** e la metà per acquistare carburante. Solo il 30% per pagare bollette/utenze presso le tabaccherie, concentrati soprattutto nelle fasce di età più giovani. Insomma 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. Ormai

quasi tutte le aziende che vendono beni hanno un proprio sito internet che spesso consente di effettuare acquisti ("store"), con semplicità ed immediatezza. **Sono centinaia di migliaia ogni giorno gli acquisti on-line in tutto il Mondo**. Oggi è possibile **comprare in internet tutti i generi di prodotti: 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

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 (nelle sue varie formule), 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). 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** prima di effettuare un acquisto di prodotti o servizi on-line :

- effettuate acquisti presso siti conosciuti o t**enere sotto osservazione il sito per un po' di tempo prima di accingervi a comprare** (effettuando anche ricerche on-line per verificare se esistono note negative sul negozio/venditore). Il "popolo di internet" utilizza un sistema assai efficace di passaparola (**forum e blog**) per cui il truffatore o il negozio/venditore poco affidabile viene "identificato" con **feed-back negativi**;
- controllate 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;
- verificate che il sito presso il quale si intende acquistare un bene utilizzi **protocolli di sicurezza** informatica. 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://"**), e in basso a destra, comparirà un'icona con un **lucchetto chiuso**;

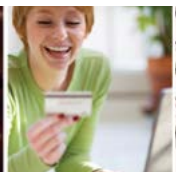
- **inserite i vostri dati** solamente quando sono rispettate le condizioni di sicurezza e comunque **non comunicate mai i dati della vostra Carta o altri dati riservati tramite e-mail;**
- i dati più importanti sono: numero Carta, data scadenza, numero CSC o CW2: proteggeteli!
- esistono **Carte di 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** 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, per poter contestare tempestivamente acquisti non effettuati;
- **conservate le ricevute dei pagamenti on-line**, indispensabili nel caso si debba contestare l'acquisto.

Le principali truffe negli acquisti on-line

Per chi intende acquistare on-line è bene tener presente che le frodi possono essere neutralizzate con facilità se si usa un po' di attenzione. I crimini informatici sono disciplinati principalmente dalla Legge 547/1993 e succ., che ha operato delle modifiche al Codice Penale prevedendo il **reato penale** per le più diffuse condotte criminose nel settore informatico. Ecco alcune:



- **Phishing e Pharming**: è una frode on-line di cui molto si parla. **Mira a sottrarre con l'inganno numeri di Carta di Credito, password, informazioni e dati personali (furto di identità)** e consiste nell'inviare **messaggi di posta elettronica, "mascherati" da messaggi "autentici"** (spesso delle ottime imitazioni) che **sembrano provenire ad esempio da parte di una Banca** o di un Ente conosciuto, dove **vi si chiede pretestuosamente un aggiornamento dei vostri dati** (ad es.: numero Carta di Credito) oppure di riregistrarvi 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 ad es. a quelle di una Banca**, chiedendo di aggiornare i propri dati. **Nessuna Banca mai vi chiederà** di effettuare on-line questa procedura!
- **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** on-line per poi poter fare acquisti all'insaputa del vero proprietario.
- **Hacking**: 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. Questa truffa solitamente non funziona se non vi è il "contributo" di un basista.

Spyware: lo spyware (software spia) **è un software illegale finalizzato a spiare (spy) le operazione compiute dell'utente del PC sottraendogli informazioni riservate** e talvolta riesce anche a far compiere al PC specifiche operazioni all'insaputa del proprietario. Spesso **si annida in alcuni programmi scaricabili gratuitamente ed è in grado di raccogliere informazioni specifiche riferite alla postazione (PC) nella quale si è installato**, tali dati vengono poi trasmessi ad insaputa ad un altro PC (Server remoto) quando ci si collega in rete. 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**.

La 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, a completamento il sito vi richiederà di creare ed inserire una password, di vostra invenzione, che vi permetterà di accedere direttamente all'area dell'"acquisto protetto". Queste password rappresentano un'ulteriore meccanismo di protezione 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. Nel creare una password è più efficace usare combinazioni alfanumeriche: cioè lettere e numeri (ad es. 1EAIZS0174). Memorizzate le password e comunque, se le scrivete non lasciatele in posti facilmente accessibili.

Un SMS avvisa quando fate un prelievo o un acquisto

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.

LE 10 REGOLE D'ORO... 5

Ecco alcune semplici regole che riassumono quanto è stato proposto nelle pagine precedenti. Se applicate, ci consentiranno di utilizzare la moneta elettronica con quella tranquillità e sicurezza che ci metterà nella condizione di poterne apprezzare la sua reale comodità, ed evitare così possibili spiacevoli e fastidiosi inconvenienti:

1. duplicate e conservate copia in luogo sicuro di tutti i documenti personali compresi gli estremi delle Carte di pagamento (Bancomat, 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 di pagamento e soprattutto tenetele lontano da fonti magnetiche e da elementi metallici per evitarne la smagnetizzazione; attenzione anche, per lo stesso motivo, a non graffiare il microchip e la banda magnetica;
3. non conservate mai il Pin (codice segreto) insieme alle Carte (Bancomat o Carta di Credito, ecc.); conservate a portata di mano i numeri telefonici (in genere 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 gli estremi delle Carte di pagamento soprattutto ad interlocutori telefonici o via internet;
6. se vi recate all'estero o in Paesi poco sicuri prima di partire verificate che la Carta di credito sia valida per tutta la durata del soggiorno, inoltre controllate il limite del fido della Carta (parlando con la Banca, si può adeguare alle esigenze del viaggio). Portate sempre con voi il numero del Call center estero della Banca, così da poter usufruire di assistenza se necessario (anticipo contanti in caso di emergenza o sostituzione della Carta);
7. 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;
8. controllate con regolarità gli estratti conto forniti dalla società di gestione della Carta non lasciate in giro o buttate le copie contabili di pagamenti e prelievi ancora leggibili nella spazzatura;
9. 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;
10. 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.

COME FARE QUANDO VADEMECUM PER LE EMERGENZE 6

E' importante nel momento dell'emergenza **agire subito**: per questo, qui riepiloghiamo per punti che cosa si deve fare **quando si perde o ci viene rubato il Bancomat e/o la Carta di Credito** ecc. o quando ci accade di subire un furto della nostra "identità digitale".

Furto o smarrimento del Bancomat

Se vi hanno rubato o avete smarrito la Carta di Debito (Bancomat) oppure scoprite che è stato oggetto di clonazione la procedura da seguire è la stessa:

1. **si deve procedere al "Blocco" della Carta chiamando il Numero Verde del Servizio Blocco** che è valido per l'Italia ed è **attivo 24 ore su 24** (riportato anche su tutti gli sportelli Bancomat). Per bloccare il Bancomat **se ci si trova all'estero sono disponibili specifici numeri**, (più avanti riportiamo un elenco dei numeri che potrebbe però essere suscettibile di modifica, se del caso chiedete il numero aggiornato in Banca). Il blocco si attiva con effetto immediato;
2. il Blocco **può essere fatto anche avvertendo subito la filiale della Banca** che ha emesso la Carta, telefonando o recandovi di persona;
3. 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;**
4. 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 che ha emesso la Carta;
5. 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; se necessario si dovrà allegare una copia **denuncia per truffa effettuata presso le Autorità di Pubblica Sicurezza**;
6. la **procedura** qui sopra descritta è stata prevista per **garantire innanzittutto la sicurezza del Titolare della Carta**, il quale potrà poi avvalersi del **supporto della Banca** per effettuare tutti quegli adempimenti necessari per consentirvi **una veloce risoluzione dell'inconveniente ed un rapido ritorno alla piena operatività.**

Furto o smarrimento della Carta di Credito ...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**, se in orario di sportello si potrà effettuare il Blocco anche rivolgendosi direttamente alla filiale della Banca;
2. **denunciare alle Autorità di Pubblica Sicurezza l'accaduto e farsi rilasciare copia della denuncia** da consegnare in Banca per completare il fascicolo e/o da inviare all'Assistenza 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. se si tratta di una **Carta prepagata vi è la sostituzione con una nuova Carta nella quale verranno trasferiti gli eventuali fondi residui**.

Smarrimento o furto del Codice PIN...

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



Numeri per blocco (furto o smarrimento) delle Carte

American Express	
Furto smarrimento Italia	06 72900347
	06 72282
Furto smarrimento estero	800 263 92 279
Servizio Card Protection CPP	
Furto smarrimento Italia	800 960 038
Furto smarrimento estero	+39 039 6578053
Cartasì	
Furto smarrimento Italia	800 151 616
Furto smarrimento estero	+39 02 34980020
Furto smarrimento USA	1 800 4736 896
Diners Club	
Furto smarrimento Italia	06 3575333
Furto smarrimento estero	+39 06 3213841
Carta Ciconto	
Furto smarrimento Italia	840 000 474
Furto smarrimento estero	+39 0521 1922110
Carta Chiara	
Furto smarrimento Italia	800 822 056
	800 301 020
Furto smarrimento estero	+39 02 60843768
CartaLibera, Bancomat e Maestro	
Furto smarrimento Italia	800 822 056
Furto smarrimento estero	+39 02 60843768

Credo nel mio territorio

Io resto qui. Investo nel mio futuro e scelgo il nuovo conto Socio & Cliente di Banca Valsabbina.

La Valsabbina
1898

BANCA VALSABBINA