Raccomandazioni per un corretto utilizzo delle "carte di debito" emesse dalla Banca Popolare Sant'Angelo

Informazioni generali sulle "carte di debito"

Le Carte di debito sono carte di pagamento che impegnano i fondi sul conto corrente di regolamento contestualmente all'operazione di prelievo o di pagamento;
Le carte di debito emesse dalla Banca Popolare Sant'Angelo SCPA sono associate al solo circuito domestico **BANCOMAT®** (per il prelievo) **e PagoBANCOMAT®** (per il pagamento) oppure sono associate al circuito domestico ed anche al circuito internazionale **Cirrus** (per il prelievo) e **Maestro** (per il pagamento) per consentire il funzionamento anche all'estero.
Per verificare quali circuiti operano su una specifica carta è sufficiente per ciascun Titolare verificare i Marchi che sono apposti sul fronte e sul retro della stessa. Al momento del pagamento o del prelievo, ciascun Titolare ha la possibilità di scegliere il circuito con cui vuole operare: in caso di prelievo o di pagamento tramite ATM è sufficiente selezionare il Circuito dal display dell'ATM stesso; in caso di pagamento tramite POS è sufficiente comunicarlo all'esercente prima della transazione.

Utilizzando la carta per i prelievi presso gli sportelli automatici ATM o nei negozi per i pagamenti tramite POS, basterà prestare attenzione ai seguenti consigli per effettuare le operazioni in totale sicurezza:

Custodite gelosamente il codice PIN (Personal Identification Number)

Il PIN è un numero segreto con il quale il titolare della carta, previa digitazione, si autentica ed autorizza le operazioni di prelievo e pagamento. In linea di massima, il PIN non può essere decodificato e non vi si può risalire nemmeno dai dati contenuti nella banda magnetica e nel microchip, ma una volta scoperto, con altre modalità, i truffatori possono accedere al vostro conto. La cosa migliore da fare per prevenire eventuali frodi, quindi, è custodire gelosamente il proprio PIN.

Cosa fare

- Imparate il PIN a memoria, magari ricorrendo ad un espediente mnemonico
- Non annotate mai il PIN sulla carta e conservate le due cose separatamente
- Non rivelate il PIN a nessuno, nemmeno a persone fidate, poliziotti o impiegati di istituti finanziari. La banca non vi chiederà mai il vostro PIN per iscritto o per telefono
- Quando digitate il PIN, nascondete sempre i movimenti delle dita con la mano libera
- Non immettete mai il PIN per azionare il dispositivo apriporta. Se vi venisse chiesto di farlo, insospettitevi, perché nessuna banca vi chiederà mai di rivelare un'informazione così riservata.

Prelevamento ai distributori automatici "Atm" (*Automated Teller Machine*)

Quando prelevate denaro contante dai distributori automatici (ATM), i truffatori possono spiare il vostro PIN e, dopo avervi rubato la carta, accedere al vostro conto, pertanto, prendete le dovute precauzioni:

- per tutta la durata dell'operazione non permettete a nessuno di distrarvi o di spiarvi da dietro le spalle. Controllate sempre che chi è in coda dopo di voi resti a una distanza ragionevole rispetto a dove vi trovate. Siate prudenti se uno sconosciuto si offre di aiutarvi a uno sportello ATM, anche se la vostra carta resta bloccata o se incontrate difficoltà;
- se la vostra carta dovesse essere improvvisamente trattenuta dallo sportello automatico, disponetene immediatamente il blocco e contattate la vostra filiale di riferimento;
- osservate attentamente l'ATM, se notate qualcosa di strano (ad esempio, un elemento traballante), non utilizzatelo e andate a riferire i vostri sospetti alla banca gestore dell'ATM o, in orario di chiusura, alla polizia;
- non utilizzate gli ATM che non siano fissati e parte integrante di un edificio o comunque al riparo e al sicuro all'interno di una struttura chiusa. Utilizzate sempre ATM ben visibili e ben illuminati. Siate oltremodo prudenti con gli sportelli automatici collocati in aree buie o in luoghi che vi sembrano poco controllati e frequentati;
- osservate attentamente l'ATM, assicuratevi che su di esso non siano presenti eventuali oggetti sospetti o mobili oppure che la fessura della carta non sia stata coperta con un dispositivo di copiatura (Skimmer). Nel caso vi accorgiate di anomalie, non effettuate l'operazione di prelievo, ma segnalate immediatamente la vostra osservazione alla banca o all'occorrenza alla polizia.

Pagamento elettronico nei negozi tramite terminali POS *(Point of Sale*)

La carta di debito è accettata come mezzo di pagamento in quasi tutti i negozi, ristoranti ed esercizi commerciali in Italia e all'estero. Grazie alla tecnologia del CHIP, la carta è assolutamente sicura sotto il profilo tecnico.

Pertanto, quando dovete pagare state attenti a:

- non perdete d'occhio la vostra carta e non lasciate che il commesso o l'impiegato la porti con sé in un'altra stanza;
- digitate il PIN al riparo da occhi indiscreti e pretendete il rispetto della vostra privacy;
- prima di digitare il PIN, controllate sempre la somma da pagare indicata nel display del POS, per evitare che, per sbaglio, vi lasciate addebitare un importo maggiore del dovuto;
- controllate le ricevute e conservatele sempre;
- verificate regolarmente gli estratti conto e, in caso di anomalie, contattate subito la banca;
- un pagamento può considerarsi effettuato solo quando compare il messaggio "**transazione eseguita**".

Fare acquisti su Internet con la carta di debito internazionale abilitata al servizio di "E-Commerce" del circuito MAESTRO ® è facile e comodo e basterà prestare attenzione ai seguenti consigli per effettuare le operazioni in totale sicurezza

- acquistate online solo da aziende affidabili;
- prima di comprare qualcosa, leggete attentamente le condizioni di contratto;
- non rivelate mai il vostro numero di carta per scopi puramente informativi;
- non fidatevi di e-mail, instant message o siti web che vi chiedono di indicare dati riservati o personali. Potrebbe trattarsi di un tentativo di "phishing";
- proteggete sempre i vostri dispositivi personali.

Se hai un PC, uno Smartphone o un Tablet:

- installa e mantieni sempre aggiornato il software di protezione antivirus (i) e antispyware;
- installa sempre gli aggiornamenti del sistema operativo e dei principali programmi che usi appena vengono rilasciati;
- installa un firewall (ii) personale;
- effettua regolarmente scansioni complete con l'antivirus;
- non aprire messaggi di posta elettronica di cui non conosci il mittente o con allegati sospetti;
- non installare applicazioni scaricate da siti non certificati o della cui attendibilità non sei sicuro;
- se lo stesso PC/tablet/smartphone è usato anche da altre persone (familiari, amici, colleghi), fai in modo che adottino le stesse regole;
- proteggi i tuoi dispositivi con PIN, password o altri codici di protezione.

(i)Il software antivirus permette di tenere il proprio dispositivo al riparo da software indesiderati ("malware") che potrebbero essere installati senza il consenso dell'utente, e carpire i dati di pagamento e altri dati sensibili del cliente a scopo fraudolento.
(ii)Il firewall personale ha lo scopo di controllare e filtrare tutti i dati in entrata e in uscita del proprio dispositivo, aumentando il livello di sicurezza del dispositivo su cui è installato.

IMPORTANTE: La Banca Popolare Sant'Angelo Scpa non fornisce supporto tecnico su antivirus, firewall e altre soluzioni di sicurezza installati sui dispositivi personali del cliente, né può essere ritenuta responsabile per la configurazione degli stessi.

Tutela i tuoi acquisti in internet

Per una maggiore protezione degli acquisti "online" sui siti internet, è offerto "gratuitamente" al titolare della carta il servizio di sicurezza denominato "**3D Secure**".
Il servizio "3D Secure", che prende il nome di "**MasterCardSecureCode"** per il circuito MAESTRO, assicura una maggiore tutela sugli acquisti e-commerce poiché **prevede ulteriori elementi di autenticazione al momento del pagamento da parte del titolare della carta di pagamento**.
Il servizio consente quindi ai titolari aderenti di effettuare in sicurezza transazioni on-line sui siti internet di esercenti convenzionati con il medesimo servizio di sicurezza, utilizzando una procedura di identificazione che li garantisce in caso di utilizzi fraudolenti della propria carta di pagamento.
Attivare il servizio "3D Secure" garantisce una tutela per i tuoi acquisti online, permettendo di prevenire eventuali utilizzi illeciti della tua Carta sul web.

Con l'iscrizione al servizio "3D Secure" eviti che il tuo numero di Carta venga usato per pagamenti online a tua insaputa.
Per attivare il "3D Secure" è necessario accedere al servizio di "**Internet Banking dispositivo**" della Banca Popolare Sant'Angelo SCPA, selezionare la carta sulla quale attivare il servizio di sicurezza e seguire le istruzioni per la registrazione.
Puoi attivare il "3D Secure" su tutte le carte in tuo possesso, anche se ne hai più di una. In questo caso dovrai iscrivere al servizio ogni singola carta.

Controllare è importante

Conservate sempre le carte in un **luogo sicuro** e verificate regolarmente che siano al loro posto.
Controllate regolarmente le **spese** e i **prelievi** effettuati con le vostre carte sugli **estratti conto forniti dalla banca**.
Qualora rileviate un addebito ingiustificato, comunicatecelo al più presto possibile.
Mantenete il **controllo** dei vostri **pagamenti** e **prelievi attivando il servizio di SMS Alert**.
Scaricate sul Vs smarthphone l'APP. "BPSA mobile" per verificare rapidamente le operazioni contabilizzate sul conto corrente.

Come bloccare la carta di debito

Fate bloccare la vostra carta se:

- vi è stata rubata
- vi accorgete di averla smarrita
- sospettate un abuso
- notate transazioni anomale sul vostro conto corrente
- se il distributore automatico (ATM) non ve la restituisce senza un motivo valido

contattando immediatamente il NUMERO VERDE: 800 822 056 (dall'Italia), +39.02.60843768 (dall'estero) e presentate apposita denuncia alle forze dell'ordine (Carabinieri o Polizia);

Confermate l'avvenuta segnalazione di blocco alla banca (filiale di riferimento), personalmente ovvero mediante lettera raccomandata a.r., telegramma, fax o e-mail all'indirizzo: ***notifichesistemidipagamento@bancasantangelo.com***, fornendo copia della denuncia presentata alle Autorità competenti, indicando il numero di blocco.

Principali tipologie di frode

Skimming

Per "skimming" si intende la manomissione degli sportelli automatici (ATM) ma anche dei distributori di biglietti alla stazione ferroviaria o dei terminali di pagamento nelle stazioni di servizio, ai quali i truffatori applicano degli speciali congegni che consentono loro di copiare i dati contenuti nella banda magnetica delle carte bancarie, di credito e di debito. Il PIN viene acquisito mediante una microtelecamera nascosta o una finta tastiera mentre il cliente digita il codice. In Italia e in Europa non si può prelevare denaro contante senza il microchip, ma i truffatori aggirano l'ostacolo semplicemente prelevando contante, con una carta clonata, nei Paesi extraeuropei dove è ancora in uso la banda magnetica.

Card Trapping

Nel caso del “card trapping” i truffatori manomettono lo sportello automatico (ATM) facendo in modo che la carta vi resti incastrata. Poi si offrono di aiutare la vittima e le consigliano di digitare nuovamente il PIN, che viene così memorizzato. Quando la vittima alla fine si allontana, i truffatori recupereranno la carta e, poiché ormai sono a conoscenza del PIN, possono tranquillamente prelevare denaro dal conto della vittima.

Cash Trapping

Nel caso del “cash trapping”, i truffatori manomettono la fessura di erogazione delle banconote dell’ ATM in modo tale che il contante venga trattenuto all’interno della macchina. Pensando che lo sportello automatico non funzioni, la vittima si allontana. A quel punto, i truffatori recuperano indisturbati il loro bottino.

Phishing

Il phishing è una frode informatica con cui mediante un sito web contraffatto, un’e-mail o un instant message i truffatori cercano di ottenere dalla vittima informazioni riservate. Essi chiedono, infatti, di fornire oppure di confermare o modificare online il numero di carta, la password del “3D Secure” o il codice PIN. I truffatori contraffanno con grande maestria interi siti Internet o falsificano i mittenti di posta elettronica presentandosi come l’istituto finanziario della vittima per poterla poi ingannare.

Ecco alcuni preziosi consigli per capire se ti trovi su un sito phishing o hai ricevuto una mail di phishing:

Indirizzo internet contraffatto

La parte iniziale deve essere caratterizzata dalla presenza dell’**”https**”: significa che quel sito utilizza protocolli sicuri per la gestione dei dati personali. Inoltre, l’URL di un sito rimane nel tempo la stessa: il sito della banca ha l’indirizzo www.bancasantangelo.com, perciò devi considerare inaffidabile e pericoloso un sito identico a cui corrisponde un indirizzo diverso.

Analizza il testo della comunicazione

Fai attenzione alle comunicazioni con errori ortografici e grammaticali e con un utilizzo scorretto della lingua italiana, probabilmente sono mail di phishing.
Inoltre: un sito sicuro e certificato che adotta i protocolli di sicurezza per la gestione dei dati, riporta sempre nella finestra del browser in basso a destra o nella barra degli indirizzi, l’icona del lucchetto, che definisce il sito come sicuro. Devi quindi diffidare dei siti che richiedono l’inserimento di dati sensibili (Login o Password, dati della carta o personali) e che non riportano l’icona del lucchetto: i dati inseriti in quella pagina saranno facilmente trafugabili. Se poi vuoi essere sicuro dell’attendibilità del sito, fai doppio click sull’icona del lucchetto: una scheda ti aiuterà a verificare che le credenziali di sicurezza siano effettivamente quelle del sito che stai visitando.

Vishing

Il “vishing” è una forma di phishing basata sull’uso del telefono. Viene richiesto, tramite email o SMS, di chiamare un numero telefonico al quale comunicare i propri codici identificativi (Username/Email e Password, numero di carta, password si sicurezza del servizio “3D Secure”). In alternativa, viene effettuata una chiamata preregistrata, in cui viene chiesta l’immissione e conferma dei codici identificativi.

La banca non ti chiederà mai di comunicare o inserire telefonicamente i tuoi codici identificativi.

Responsabilità della banca e del titolare della carta per le operazioni di pagamento

Sia la Banca che il Cliente (Titolare della Carta) devono garantire, ciascuno per la propria parte, l'uso corretto e sicuro dei prelievi su ATM e dei pagamenti eseguiti su internet o su terminale POS. In particolare, come Cliente, sei responsabile della tua carta e devi custodire con cura, sia la carta che il PIN e gli eventuali altri i codici di sicurezza. In caso di anomalie o problemi riscontrati durante le operazioni di pagamento, o in caso di abuso o utilizzo sospetto della tua Carta, devi immediatamente contattare il Servizio Blocchi secondo le modalità indicate in precedenza. Inoltre, se controllando le spese in estratto conto ne trovi una che ritieni di non aver fatto o sulla quale vuoi maggiori informazioni, la banca avvierà le eventuali verifiche.

Ti ricordiamo infine che questa pubblicazione ha finalità esclusivamente informative. Nei siti della Polizia di Stato e dei Carabinieri (www.poliziadistato.it - www.carabinieri.it) sono riportate utilissime informazioni per il cittadino al fine di evitare truffe con le carte di pagamento.