INFORMATIVA SULLA SICUREZZA CARTE DI DEBITO

Credenziali di Sicurezza Personalizzate previste per le Carte di Debito

La carta di debito - conosciuta in Italia anche come carta Bancomat dal nome del circuito nazionale - è uno strumento di pagamento dotato di tecnologia contactless, microchip e/o banda magnetica per il riconoscimento dei dati identificativi del titolare della stessa e degli elementi di sicurezza.
L'utilizzo del servizio presuppone l'utilizzo della carta:

- congiuntamente al codice segreto personale detto P.I.N. (Personal Identification Number). Elevati protocolli di sicurezza abbinano il P.I.N. alla relativa carta. In presenza anomale digitazioni del P.I.N. la carta viene resa inutilizzabile;
- senza digitazione del P.I.N. sui terminali P.O.S. dotati di tecnologia Contactless al verificarsi di condizioni specifiche correlate all'importo della/e operazione/i ed alla frequenza con il solo avvicinamento della carta al lettore;
- senza digitazione del P.I.N. presso i caselli appositamente abilitati che espongono il marchio FASTpay ubicati sul territorio nazionale con il solo inserimento della carta nel lettore.

Consigli sulla corretta conservazione delle Credenziali di Sicurezza Personalizzate

La carta plastica deve essere conservata con cura, evitando che si graffi o si spezzi ed al riparo da fonti di calore o campi magnetici, tutti elementi che possono impedire il corretto funzionamento.
Il P.I.N. deve essere conservato in luogo separato dalla carta plastica evitando di trascriverlo su agende, fogli, rubriche anche elettroniche.

Procedura in caso di abuso riscontrato o sospetto

Lo smarrimento, furto o clonazione delle Credenziali di Sicurezza Personalizzate impone all'Utente l'attivazione di immediate azioni volte a impedirne o contenerne l'utilizzo.
Appena venuto a conoscenza dell'evento l'Utente deve:

- bloccare subito la carta telefonando al numero verde (il cui operatore rilascia un numero che va inserito nella denuncia alle forze dell'ordine e comunicato alla Banca) oppure alla Banca
- presentare quanto prima la denuncia alle Autorità Giudiziaria o di Polizia di cui una copia, su richiesta, dovrà essere consegnata alla Banca

Responsabilità dell'Utente e della Banca

Nell'uso del servizio di pagamento con carte di debito, l'Utente assume responsabilità:

- in mancanza di rispetto dei termini e delle condizioni contrattuali;
- in mancanza dell'immediata adozione di tutte le misure idonee a garantire la sicurezza del servizio e delle Credenziali di Sicurezza Personalizzate;
- sulla perdita derivante dall'utilizzo indebito del servizio conseguente al furto o smarrimento o uso non autorizzato delle Credenziali di Sicurezza Personalizzate per un importo comunque non superiore complessivamente a 50 euro, salvo il caso in cui abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la sicurezza delle Credenziali di Sicurezza Personalizzate;

Nell'uso del servizio di pagamento con carte di debito, la Banca assume responsabilità:

- affinchè l'Utente abbia sempre a disposizione strumenti adeguati per il blocco o lo sblocco del servizio;
- sull'impedimento di qualsiasi uso del servizio dopo il blocco del servizio;
- sui rischi derivanti dalla spedizione delle Credenziali di Sicurezza Personalizzate;
- sui rischi connessi alla continuità operativa del servizio;
- sui rischi connessi alla sicurezza informatica del servizio.

Difesa dai Rischi

CONSERVAZIONE
La carta plastica ed il P.I.N. debbono essere conservati in luogo separato in modo tale da impedire che il furto o lo smarrimento di uno dei due, impedisca al malvivente l'utilizzo.
Per quanto ovvio, deve essere evitato di comunicare o consegnare a terzi la carta plastica ed il P.I.N..

ATTENZIONE NELL'UTILIZZO
Nell'utilizzo del servizio per qualunque operazione, è necessario digitare il P.I.N. - quando richiesto - in maniera riservata senza essere osservati, evitando che terzi ne vengano a conoscenza.
E' altrettanto importante accertarsi che l'apparecchiatura su cui si sta eseguendo l'operazione non presenti manomissioni o alterazioni; i più comuni sistemi messi in atto dai malviventi sono:

- Skimmer: dispositivo elettronico capace di leggere e in certi casi immagazzinare i dati della banda magnetica delle carte alloggiato – spesso – sopra il lettore carte della terminaleria
- Microcamere: dispositivo elettronico utilizzato per visualizzare il PIN digitato dall'Utente nascosti – spesso – in involucri (pacchetti, cestini, dispositivi elettronici …) o fori del neon dell'ATM o in prossimità del terminale POS.
- Frontalini e Tastiere: dispositivi posizionati sopra quelli originali per copiare i dati delle carte inseriti nel lettore ed i codici PIN digitati.

ATTENZIONE NELL'APRIRE O RISPONDERE AD EMAIL SOSPETTE
Trattasi di sistemi che ricorrendo ad email sospette (raramente telefonate) cercano di carpire le Credenziali di Sicurezza Personalizzate.

- Phishing: tecnica utilizzata mediante l'utilizzo delle comunicazioni elettroniche, quali messaggi di posta elettronica, finestre a comparsa, messaggi su cellulari ed anche contatti telefonici che, replicando generalmente in modo similare l'aspetto grafico ed il logo dei siti istituzionali, inducono l'Utente ad indicare le Credenziali di Sicurezza Personalizzate in un sito clone di quello ufficiale.

CLONAZIONI
Trattasi di sistemi che, con la manomissione dei lettori sulla terminaleria e con la lettura del P.I.N., possono riuscire a "clonare" la banda magnetica delle carte da poter utilizzare in alcuni paesi del mondo dove la tecnologia contactless o a microchip (tecnologie indenni da tale attacco) non è ancora completamente diffusa.

SMS Alert
Il Servizio SMS permette di ricevere sul proprio cellulare immediata evidenza dei movimenti effettuati con la carta permettendo di agire prontamente in presenza di frodi e furto o smarrimento della Carta.
Il Cliente sceglie il limite di importo oltre il quale ricevere tali messaggi.

CONTROLLO DELLA SITUAZIONE CONTABILE
E' necessario che l'Utente verifichi spesso i movimenti del conto corrente per accorgersi di eventuali operazioni non conformi.

COMUNICAZIONI PERIODICHE SULL'USO CORRETTO E SICURO DEL SERVIZIO
L'Utente sarà informato dalla Banca sulle novità in materia di sicurezza del servizio.