Linee guida per il corretto utilizzo della Carta ateneo+ e delle disposizioni online

Introduzione e modalità di ricarica

Carta ateneo+ è una carta di pagamento nominativa, prepagata, dotata di codice IBAN e ricaricabile identificata da:

- Un numero di 16 cifre
- Una data di scadenza
- Un codice di sicurezza posto sul retro
- Un codice PIN generato elettronicamente

La Carta è utilizzabile sul circuito MasterCard e non può essere ceduta in uso da parte del Cliente a terzi soggetti.

La ricarica della Carta (oltre che da sportello bancario, ATM e bonifico) può avvenire anche online attraverso SCRIGNO*Internet Banking* nel caso che il Cliente abbia un altro rapporto presso la Banca che consenta l'operazione di caricamento della Carta.

Informazioni preliminari e requisiti per l'utilizzo di SCRIGNOInternet Banking e per acquistare online

L'utilizzo dei servizi on line della Banca Popolare di Sondrio avviene tramite personal computer o altro dispositivo interattivo connesso alla rete Internet.
Per evitare potenziali problemi di sicurezza, si raccomanda di mantenere aggiornato:

- il browser
- il sistema operativo
- le eventuali app di accesso alla banca on line, ad esempio **SCRIGNO***IdentiTel*

Inoltre, si consiglia di sottoporre regolarmente i dispositivi a scansione di sicurezza con prodotti antivirus e anti-malware.

Nella sezione "Sicurezza" presente in **SCRIGNO***Internet Banking* sono raccolti alcuni suggerimenti e sono presenti servizi fruibili on line, che La invitiamo a consultare e a utilizzare, fra cui il servizio "navigosereno" per verificare lo stato di sicurezza di computer, smartphone e tablet nonché "Phil" e "Phillys", i giochi che insegnano a riconoscere gli attacchi di phishing.

È notorio che le tematiche relative alla sicurezza on line rivestono un'importanza crescente e richiedono di comportarsi con prudenza. Al proposito, si evidenzia che il canale email non può considerarsi sicuro per veicolare informazioni riservate o attinenti a esempio alla sicurezza dei servizi on line.

E' per questo, che le comunicazioni di Banca Popolare di Sondrio tramite newsletter afferenti alla sicurezza on line saranno accompagnate da una campagna informativa, visibile contestualmente all'accesso a **SCRIGNO***Internet Banking*, la quale riprenderà il tema della newsletter.
L'autenticità della newsletter e quindi dell'informativa potrà o meglio dovrà essere verificata all'interno di **SCRIGNO***Internet Banking*.

Si raccomanda pertanto di collegarsi a SCRIGNO – digitando l'indirizzo nel browser, senza seguire eventuali link presenti nella newsletter – ogni qualvolta viene ricevuta una comunicazione in tema di sicurezza da parte della banca, per verificarne l'autenticità e il contenuto.

Raccomandazioni per un utilizzo corretto delle credenziali di accesso

Credenziali SCRIGNO

L'accesso e l'utilizzo di SCRIGNO avviene tramite l'inserimento delle credenziali di accesso consegnate al Cliente. Le credenziali sono costituite dal codice utente (riportato sul contratto) e dal PIN SCRIGNO (scelta personalizzata dal Cliente).
Le credenziali devono essere mantenute riservate e non debbono essere fornite a terzi per nessuna ragione.
È altresì consigliabile modificare periodicamente i PIN suddetti, al fine di innalzare i profili di sicurezza e rafforzare i presidi a fronte di eventuali tentativi di utilizzi fraudolenti.
Si evidenzia che, trascorsi 6 mesi dall'ultimo accesso SCRIGNO, le credenziali vengono bloccate per inoperatività. In tali casi l'utente dovrà rivolgersi alla filiale che provvederà allo sblocco.

Credenziali 3D Secure (MasterCard SecureCode)

Al fine di garantire una migliore sicurezza ai pagamenti è necessario attivare "SecureCode", ossia il servizio di protezione anti frode gratuito di Mastercard, che garantisce una tutela ulteriore per la Carta: consiste in una password che viene richiesta al momento di autenticare un pagamento online. Seguendo l'apposita procedura, verrà richiesto al Titolare di definire una password per autorizzare il pagamento nonchè una frase identificativa che sarà proposta ogni volta che verrà richiesta la password della protezione anti frode SecureCode.

Procedura di autenticazione delle operazioni tramite SCRIGNOInternet Banking

Le operazioni effettuate tramite SCRIGNO devono essere autenticate dall'utente.
Il procedimento di autenticazione si svolge grazie a SCRIGNOIdentiTel SMS, basato sull'invio dell'OTP (One Time Password), ossia la password "usa & getta" richiesta e verificata dai servizi online della Banca.
Il funzionamento dell' autenticazione è molto semplice. Nel momento in cui l'Utente predispone un' operazione dispositiva, SCRIGNO ne richiede l'autenticazione tramite una specifica pagina che fornisce le istruzioni del caso. A quel punto occorre:

- attendere di ricevere via SMS l'OTP sul proprio telefono
- digitare il codice OTP nel campo collocato nella pagina di autenticazione

Procedura per gli acquisti online (e-commerce)

Per la corretta esecuzione degli acquisti online è necessario fornire il numero di Carta, la scadenza e il relativo codice di sicurezza (CVC2)

A maggior tutela, qualora fosse stato in precedenza attivato il servizio "SecureCode", nella fase di pagamento per un acquisto on line, viene richiesto - oltre agli estremi della carta di pagamento - di digitare SecureCode, ovvero la password definita dall'utente. Il sistema verificherà la veridicità delle informazioni relative al pagamento e l'operazione si concluderà.

Prontuario per smarrimento/utilizzo indebito di SCRIGNO

In caso di smarrimento e/o utilizzo indebito delle **credenziali di accesso,** il Cliente è tenuto a comunicare l'evento tempestivamente alla Banca, che provvederà al blocco del servizio. In caso di disconoscimento delle operazioni, occorrerà consegnare copia della denuncia avvenuta presso l'Autorità di Pubblica Sicurezza.
La comunicazione alla Banca può avvenire tramite:

1) **numero verde 800-23.98.89** (dall'Estero +39 06 55.24.11.23), servizio attivo 24 ore al giorno
2) **filiale**, negli orari di apertura al Pubblico

Prontuario per smarrimento/utilizzo indebito della Carta

In caso di smarrimento/utilizzo indebito della Carta, del PIN o del codice di sicurezza il cliente dovrà procedere all'immediata richiesta di blocco nelle seguenti modalità:

1) **numero Verde 800.822.056** (+39 02 60843768 dall'estero), servizio attivo 24 ore al giorno
2) attraverso **SCRIGNO***Internet Banking* (o attraverso la **SCRIGNOApp**)
3) informare la **filiale** negli orari di apertura al pubblico

A seguito della segnalazione il Cliente dovrà fornire alla Banca copia della denuncia presentata alle Autorità.

Responsabilità e oneri per la Banca

La banca, per motivi di sicurezza o per usi impropri da parte del Cliente, può:

- bloccare il servizio SCRIGNO o alcune operazioni (informative/dispositive);
- richiedere sistemi/procedure rafforzate per consentire l'esecuzione delle operazioni.

La Banca si impegna a bloccare il servizio SCRIGNO a seguito della ricezione di una richiesta in tal senso da parte del Cliente. Da quel momento, l'operatività verrà inibita.
In merito ad eventuali operazioni disconosciute dal Cliente, la Banca si riserva di effettuare le verifiche ritenute opportune al fine di escludere eventuali situazioni di dolo o colpa grave.
La limitazione della responsabilità del Cliente fino all'importo massimo di 150€, infatti opererà solo se il Cliente non ha agito con dolo o colpa grave.

A seguito del blocco del servizio SCRIGNO, la Banca fornirà le informazioni utili per ottenere le nuove credenziali e i nuovi dispositivi di sicurezza per accedere nuovamente al Servizio.

Al venir meno delle ragioni che hanno portato al blocco, la Banca provvede a riattivare la Carta o ad emetterne una nuova; anche a seguito di danneggiamento o smagnetizzazione, la Banca provvederà alla sua sostituzione.

La Banca ha l'obbligo, qualora il Cliente volesse recedere, di rimborsare la disponibilità presente sulla Carta a seguito della sua riconsegna e previa compilazione del modulo di rimborso.

Responsabilità e oneri in capo al Cliente

Il Cliente è tenuto a :

- custodire con attenzione la Carta, la quale non può essere ceduta a terzi soggetti
- non conservare il PIN insieme alla Carta
- non divulgare i codici segreti (credenziali SCRIGNO e PIN).

Al fine di garantire una migliore sicurezza ai pagamenti è necessario attivare il "SecureCode", ossia il servizio di protezione anti frode gratuito di MasterCard, che garantisce una tutela ulteriore per la Carta: consiste in una password che viene richiesta al momento di autenticare un pagamento on line.

In caso di smarrimento/uso improprio del Servizio, l'Utente dovrà darne immediata comunicazione alla Banca con le modalità indicate in precedenza.

Le operazioni registrate dalla Banca sono rese disponibili al Cliente attraverso richiesta presso gli sportelli bancari o nell'ambito del servizio di **SCRIGNO***Internet Banking,* trascorsi 60 giorni dalla fine del mese solare nel quale sono state registrate senza che il Titolare abbia sollevato contestazioni, si considerano approvate.

Fino al momento di ricezione da parte della Banca della comunicazione di smarrimento/ uso indebito il Cliente è responsabile di ogni perdita subita, la responsabilità si estende anche dopo la ricezione della comunicazione qualora abbia agito con dolo o colpa grave.

L'utilizzo di una Carta smarrita/rubata/scaduta rappresenta illecito, che la Banca si riserva di perseguire penalmente.