Note per la corretta esecuzione in sicurezza dei pagamenti via Internet

Informazioni preliminari e requisiti per l'utilizzo di SCRIGNOInternet Banking

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***app* e **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

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), dal PIN SCRIGNO e dal PIN IdentiTel (entrambi i PIN vengono scelti e personalizzati 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.

Procedura di autenticazione delle operazioni on line

Le operazioni effettuate tramite SCRIGNO devono essere autenticate dall'utente.
Il procedimento di autenticazione si svolge grazie a **SCRIGNO***IdentiTel*, lo strumento di autenticazione basato sui cosiddetti "token".
I token, disponibili sia in versione "digitale" sotto forma di app, sia in formato "fisico", vengono utilizzati per generare i codici OTP (One Time Password), ossia le password "usa & getta" richieste e verificate dai servizi online della Banca in fase di autenticazione.
Il funzionamento di una autenticazione è molto semplice. Nel momento in cui l'Utente predispone una operazione dispositiva, SCRIGNO ne richiede l'autenticazione tramite una specifica pagina che fornisce le istruzioni del caso. A quel punto occorre:

- lanciare l'app (o accendere il token fisico) e avviare la generazione di un codice OTP, scegliendo l'opzione richiesta da SCRIGNO;
- autorizzare la generazione dell'OTP, digitando gli eventuali dati richiesti e il PIN IdentiTel;
- digitare il codice OTP così generato in un campo a tal fine collocato nella citata pagina di autenticazione.

A seguito di ciò viene visualizzato l'esito dell'operazione.

Il token è strettamente personale e deve essere conservato con cura e diligenza.
Le rammentiamo di custodire in un luogo non accessibile da terzi il "**Codice QR LICENZA**" (riferito al token in versione "app") riportato sul contratto **SCRIGNO***plus,* al fine di poter attivare il token su ulteriori dispositivi.

Prontuario per smarrimento/utilizzo indebito di SCRIGNO e degli strumenti di pagamento

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

In caso di smarrimento (ad esempio perdita dello smartphone sul quale il token è installato) e/o utilizzo indebito del token, il Cliente deve comunicarlo prontamente alla Banca.

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 riserva di sospendere/disattivare **SCRIGNO***IdentiTel* e di richiedere altri metodi di autenticazione in possesso del Cliente, come ad es. SMS IdentiTel.
Si evidenzia che la Banca non può garantire in quest'ultimo caso la continuità del servizio qualora il Cliente si fosse rifiutato di fornire il numero di recapito cellulare al momento (o successivamente) dell'adesione a **SCRIGNO***IdentiTel*.

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.

Responsabilità e oneri in capo al Cliente

Il Cliente è tenuto a custodire con attenzione lo strumento di pagamento (token fisico, smartphone sul quale è installata l'app del token software ecc.) e a non divulgare i relativi codici segreti (credenziali SCRIGNO e PIN IdentiTel).

In caso di smarrimento/uso improprio del Servizio, l'Utente dovrà darne immediata comunicazione alla Banca con le seguenti alternative modalità:

- comunicazione al numero verde 800-23.98.89 (dall'Estero +39 06 55.24.11.23), servizio attivo 24 ore al giorno
- recandosi direttamente in filiale, negli orari di apertura al pubblico

Qualora il Cliente avesse agito con dolo o colpa grave, sarà chiamato a rispondere per l'intero del danno e/o delle disposizioni fraudolente conseguenti; in caso contrario sopporterà la perdita solo fino all'importo massimo di 150 euro.