Il decalogo della sicurezza

Consigli e raccomandazioni per difendersi dalle truffe online

Banca Popolare di Sondrio
FONDATA NEL 1871

1 Non comunicare mai a nessuno i tuoi dati di accesso e non eseguire operazioni su richiesta via telefono, email o SMS

Non ti chiederemo mai - via telefono, email o SMS - di comunicarci i tuoi dati di accesso, ovvero di svolgere operazioni urgenti o di autorizzare delle operazioni con la tua utenza **SCRIGNO***bps*.
Tali eventualità configurano certamente un tentativo di frode.

2 Controlla sempre il dominio che stai usando per le tue operazioni

Controlla sempre il dominio: il nostro è solo popso.it. La posizione corretta della parola popso è sempre e solo prima di .it. I truffatori usano domini che rimandano a siti clonati e che hanno un nome diverso da popso.it, dove la parola popso non compare o non è inserita nella sua posizione corretta. Esempi di siti falsi sono per esempio: altrodominio.it/sicurezza, popso.altrodominio.it, scrigno.popso.altrodominio.it/ihb/run *(*)*

3 Non fidarti solo dei numeri di telefono, del mittente degli SMS o degli indirizzi email, ma presta sempre attenzione a quanto ti viene comunicato

La banca NON richiede e/o chiama i clienti chiedendo di fornire le credenziali di accesso (Codice utente, OTP IdentiTel)... non abbassare mai la guardia perché i truffatori sono abili e possono riuscire a simulare qualunque numero di telefono, anche quello della tua filiale, così come il mittente degli SMS che ricevi. Le email della nostra banca sono riconoscibili dal dominio @popso.it (per esempio: noreply@popso.it, scrigno@popso.it; la posizione corretta della parola popso è sempre e solo dopo il simbolo @ e prima di .it). Valuta quindi sempre attentamente il contenuto delle comunicazioni che ricevi. Per qualsiasi dubbio, contatta tu la banca ai riferimenti conosciuti.

4 Verifica sempre il contenuto delle email e degli SMS e non selezionare mai i link in comunicazioni sospette

Diffida dei messaggi che ti richiedono degli interventi urgenti, come selezionare un link o inserire dati personali: sono falsi! Non selezionare mai link nelle email che contengono questo tipo di comunicazione e non inserire mai i tuoi dati personali in pagine web che sembrano emulare il nostro internet banking. Non cliccare mai alcun tipo di link presente dentro un SMS e in questi casi semmai accedi ai nostri siti digitando direttamente il dominio e non tramite link.

5 Verifica sempre l'adeguatezza dei massimali operativi impostati in SCRIGNO*bps* e mantienili sempre coerenti con le tue reali esigenze

Se non hai esigenze specifiche riduci sempre i massimali operativi al minimo necessario, per limitare i rischi in caso di comportamenti errati che causano un utilizzo improprio del servizio.

6 Controlla sempre il riepilogo delle operazioni prima di autorizzarle

Controlla sempre, su **SCRIGNO***bps* e sull'app **SCRIGNO***IdentiTel*, la correttezza dei dati dell'operazione che stai autorizzando: l'IBAN del beneficiario, l'importo ecc.

7 Attiva le notifiche sull'operatività

Le notifiche di sicurezza che ricevi via SMS o Push – se hai attivato questo canale - sono inviate automaticamente e non puoi disabilitarle e ti invitiamo a controllarle con attenzione e a contattare tempestivamente la tua filiale in caso di eventuali anomalie. Inoltre, puoi ricevere anche aggiornamenti sull'operatività in **SCRIGNO***bps*, riferita ai conti correnti, ai depositi titoli e alle carte via email, SMS e notifiche Push. Se lo desideri, puoi riceverli su più canali contemporaneamente.

8 Tieni sempre aggiornato il tuo dispositivo con l'ultima versione del sistema operativo disponibile

Aggiornare il browser e il sistema operativo dei dispositivi da cui effettui le operazioni ti garantisce la migliore protezione. Ti consigliamo di utilizzare antivirus e antimalware, mantenendoli aggiornati costantemente, e di utilizzare sul tuo computer un'utenza senza le autorizzazioni di amministratore.

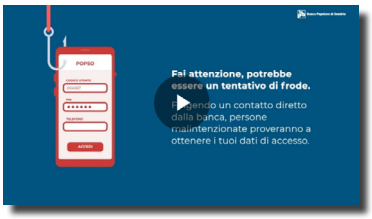
9 Scegli con cura le tue password e differenziale in funzione del rischio

Evita combinazioni semplici per la generazione dei tuoi PIN (per esempio 12345), le date di nascita e altre combinazioni facilmente riconducibili a te e ai tuoi cari. Utilizza password diverse sui vari servizi internet e fai particolare attenzione sui siti che ti espongono a maggior rischio (ecommerce, posta elettronica, ecc.), dove possibile, utilizza un sistema di One Time Password.

10 Informati sempre sui rischi che puoi correre online

Ce ne sono sempre di nuovi e aggiornarsi è fondamentale per navigare in sicurezza.
Visita la sezione Sicurezza in **SCRIGNO***bps* o la pagina popso.it/sicurezza.

Inquadra il QR code e guarda il nostro video: "**Guida alla protezione dei tuoi dati di accesso**".



(*) Nota: altrodominio.it è un nome di fantasia che usiamo a titolo di esempio per indicare qualsiasi dominio diverso da popso.it.

Il decalogo della sicurezza

Consigli e raccomandazioni per difendersi dalle truffe online

Banca Popolare di Sondrio
FONDATA NEL 1871