

Domande frequenti - Sicurezza

Sommario

| | |
|---|---|
| Quando navigo sul sito di Intesa Sanpaolo Private Banking, la mia sicurezza è garantita? ... | 1 |
| Anche quando accedo alla mia nuova esperienza digitale la mia sicurezza è garantita? .. | 2 |
| I miei dati e le mie informazioni sono protette da un servizio di sicurezza? | 2 |
| Cos'è il Phishing? | 2 |
| Come posso riconoscere ed evitare il Phishing? | 2 |
| Sono stato vittima di Phishing: ho ricevuto un'email con la richiesta dei dati personali, cosa devo fare? | 2 |
| Sono stato vittima di Phishing: ho ricevuto una comunicazione sospetta apparentemente proveniente dalla banca, cosa devo fare? | 2 |
| Sono stato vittima di Phishing: ho riscontrato delle anomalie nei servizi, cosa devo fare? | 3 |
| Sono stato vittima di Phishing: ho erroneamente comunicato i codici della mia nuova esperienza digitale a seguito di un messaggio sospetto, cosa devo fare? | 3 |
| Esistono delle "buone regole" per garantire la mia sicurezza online? | 3 |
| Ho smarrito la mia carta. Cosa devo fare? | 3 |

Quando navigo sul sito di Intesa Sanpaolo Private Banking, la mia sicurezza è garantita?

Certamente, perché con noi le tue informazioni sono al sicuro. L'internet banking è stato progettato con i migliori sistemi di sicurezza e crittografia. Offriamo le più avanzate tecnologie sulle nostre carte di pagamento e strumenti di prevenzione frodi come GeoControl, il servizio per scegliere l'area geografica dove utilizzare la carta. I nostri sistemi di controllo per prevenire frodi ed email di Phishing contribuiscono a mantenere elevati gli standard di protezione.

Anche quando accedo alla mia nuova esperienza digitale la mia sicurezza è garantita?

Sì, perché per accedere alla nuova esperienza digitale di Intesa Sanpaolo Private Banking ti chiediamo di inserire tre codici: il codice titolare che è indicato nel tuo contratto, il codice PIN scelto da te la prima volta che accedi e il codice O-Key che crei ogni volta e che è comunicato al sito direttamente dall'app, se hai attivato il servizio O-Key Smart, o che ricevi tramite messaggio sul tuo smartphone, se hai attivato O-Key SMS.

I miei dati e le mie informazioni sono protette da un servizio di sicurezza?

Tutti i dati e le informazioni, su internet banking e app di Intesa Sanpaolo Private banking, sono protetti con il sistema più avanzato di crittografia SSL a 128 bit (compatibile AES 256 bit). Per maggiore sicurezza, Quando entri nel tuo internet banking verifica sempre la presenza del lucchetto chiuso sulla finestra del browser che indica la protezione della trasmissione dati, del prefisso <https://> e della "colorazione rame" che mostra il certificato di attendibilità del sito ufficiale della banca.

Cos'è il Phishing?

Il Phishing può essere un messaggio SMS o un'email. Queste comunicazioni sono molto simili a quelle della banca, sia nella grafica sia nel contenuto. Il messaggio di solito invita a cliccare su un link che indirizza verso una copia fittizia del sito ufficiale, anche questo molto fedele a quello originale. L'obiettivo è ottenere da te le informazioni personali, come i codici di accesso ai servizi online o delle carte di credito.

Come posso riconoscere ed evitare il Phishing?

Per evitare il Phishing verifica sempre il mittente e certifica i tuoi contatti. Inoltre, cancella le comunicazioni sospette. Se non sei sicuro della provenienza, non cliccare sui link che ricevi e non aprire allegati all'interno delle email o degli SMS. Inoltre, digita la url del sito www.intesasanpaoloprivatebanking.com sempre direttamente nel browser.

Sono stato vittima di Phishing: ho ricevuto un'email con la richiesta dei dati personali, cosa devo fare?

Ti consigliamo di inoltrare una copia dell'email alle autorità competenti e avvisare la banca o altri soggetti interessati, in modo che possano prendere ulteriori disposizioni contro il sito falso e informare gli altri clienti.

Sono stato vittima di Phishing: ho ricevuto una comunicazione sospetta apparentemente proveniente dalla banca, cosa devo fare?

Informa la Filiale Digitale telefonando al Numero Verde 800.99.55.33 (dall'estero +39 011.8019.111).

Ci aiuterai così a ridurre i rischi di frodi online.

Sono stato vittima di Phishing: ho riscontrato delle anomalie nei servizi, cosa devo fare?

Rivolgiti immediatamente alla tuo private banker o alla Filiale Digitale al Numero Verde 800.99.55.33 (dall'estero +39 011.8019.111).

Sono stato vittima di Phishing: ho erroneamente comunicato i codici della mia nuova esperienza digitale a seguito di un messaggio sospetto, cosa devo fare?

Ti suggeriamo di cambiare subito il Codice PIN e contattare la Filiale Digitale per verificare se ci sono tentativi di accesso fraudolenti e provvedere al blocco del contratto. Non entrare nel tuo internet banking fino a che non sei sicuro che il computer sia privo di virus. Se puoi, fai anche una scansione antivirus.

Esistono delle “buone regole” per garantire la mia sicurezza online?

Sì, esistono degli accorgimenti che puoi osservare. Ad esempio:

- controlla spesso la tua situazione per verificare i movimenti del tuo conto e delle tue carte
- assicurati di proteggere il tuo pc aggiornando il tuo programma antivirus e il tuo sistema operativo
- se possibile, non memorizzare le tue password sul browser e custodisci con cura i tuoi codici
- non affidare mai la tua carta a un'altra persona, neanche un familiare, per eseguire le operazioni
- annota sempre i numeri di emergenza e portali con te

Per offrirti una sicurezza in più, tutte le carte di pagamento sono protette dal sistema del circuito. Dopo aver trasmesso le informazioni della tua carta, quindi, ti sarà richiesto di inserire il codice O-Key. Ovunque tu sia, puoi gestire la sicurezza della tua carta scegliendo di ridurre il limite di spesa e al tempo stesso limitare l'ambito geografico di utilizzo con il servizio GeoControl.

Ho smarrito la mia carta. Cosa devo fare?

Puoi bloccare immediatamente la tua carta di pagamento contattando la Filiale Digitale al numero 800.99.55.33 (dall'estero +39 011.8019.111) disponibile, per la funzionalità di blocco, clonazione e smarrimento carta, 24 ore su 24, 7 giorni su 7.

In caso di emergenza sulle tue carte puoi contattare anche il numero verde sempre attivo 800.444.223 (dall'estero o da telefono cellulare +39.02.8710.9001).

Dovrai poi anche sporgere una denuncia alla polizia e richiedere una copia del verbale.