LA SICUREZZA DEL TUO HOME BANKING

Banca Progetto ti garantisce un servizio di Home Banking sicuro, anche grazie ai seguenti strumenti

Protezione della trasmissione dei dati

La trasmissione dei dati con il nostro Home Banking è protetta attraverso il sistema di **crittografia SSL a 128 bit** (compatibile AES 256 bit), il protocollo standard che consente di stabilire un canale di comunicazione sicuro per impedire l'intercettazione di informazioni riservate che viaggiano sulla rete Internet.

Per assicurarti che la protezione sia attiva, è necessario verificare che nella parte superiore della finestra del browser Internet Explorer/Chrome/Firefox (barra degli indirizzi) sia sempre presente l'icona del "**lucchetto chiuso**", che rappresenta una garanzia di autenticità del sito e di protezione delle informazioni trasmesse.

Codici di accesso

Il servizio utilizza un sistema combinato di password statiche (**Codice Utente** e **Password**) scelti in "fase di primo accesso" e, per aumentare il livello di sicurezza, in "fase di apertura" del conto viene richiesto un **Codice Pin** di sicurezza, da te impostato, da utilizzare per accedere al servizio e confermare le operazioni dispositive.

Al fine di creare e gestire la tua **Password** in modo corretto e sicuro ed evitare l'accesso a persone non autorizzate, di seguito alcune semplici regole:

- **scegli una password che abbia una lunghezza di 8 caratteri,** di cui almeno un numero e una lettera maiuscola. Il sistema Internet Home Banking è *case-sensitive*, quindi riconosce i caratteri minuscoli e maiuscoli;
- **non includere al suo interno codici/parole facilmente intuibili**, quali ad. es. il tuo codice utente, il tuo nome o cognome, la tua data di nascita, etc.;
- **modifica la password frequentemente** (almeno ogni 60 giorni), e comunque ogniqualvolta si abbia il minimo dubbio che qualcuno, in modo fraudolento, ne sia venuto a conoscenza, accertandoti di scegliere una password che sia diversa dalle ultime 10 inserite **(**il sistema dell'Home Banking le memorizza e non ti permette di riutilizzarle);
- **scegli una password diversa** anche da quelle che normalmente utilizzi per altri servizi su Internet (e-mail, social network…).

Il Cliente può decidere di cambiare i propri Codici di accesso, in qualsiasi momento, in modo autonomo, riservato e gratuito, all'interno dell'Area Personale.

Più in generale, per garantirti una maggiore sicurezza delle tue **credenziali** (Codice Utente e Password), ricordati di:

- non diffonderle attraverso strumenti di comunicazione (social network, e-mail, telefono, ….);
- non comunicarle ad amici, conoscenti o ad operatori di Servizio Clienti;
- prima di effettuare il "Log In" al sito Home Banking, verifica ed eventualmente disattiva la funzione di "salvataggio automatico";
- custodisci i codici con cura, in modo da evitare che altri ne vengano a conoscenza, evitando, per quanto possibile, di annotarle su carta o su tuoi dispositivi (pc, tablet, smartphone, etc.), oppure assicurandoti di conservarle in posti diversi e comunque non accessibili da persone da te non autorizzate:

Se smarrisci o ti vengono sottratti i tuoi codici di accesso, contatta subito il Servizio Clienti di Banca Progetto al **Numero Verde 800.06.09.09**. Per ulteriori modalità di comunicazione con il Servizio Clienti, consulta le Condizioni Contrattuali relative allo specifico Servizio sottoscritto.

Avvisi via SMS/E-mail

La Banca ha predisposto un servizio di sicurezza "Alert SMS/E-mail". Un SMS o una e-mail ti avviseranno inviandoti un messaggio in caso di accesso al conto o di transazioni.

Durata massima della sessione

Per tutelare maggiormente la tua sicurezza, il nostro Home Banking prevede un tempo massimo di inattività di circa 20 minuti, passato il quale, il sistema interrompe automaticamente la connessione.

Monitoraggio degli accessi e delle operazioni effettuate tramite Home Banking

Il servizio Home Banking prevede che gli accessi (o i tentativi di accesso) e le operazioni effettuate siano costantemente monitorati, per permettere alla Banca di intervenire tempestivamente nel caso in cui si verifichino situazioni anomale o tentativi di frode. In caso di anomalie o di incidenti sospetti durante le tue sessioni di pagamento, contatta subito il Sevizio Clienti al Numero Verde 800.06.09.09. Per ulteriori modalità di comunicazione con il Servizio Clienti, consulta le Condizioni Contrattuali relative allo specifico Servizio sottoscritto.

Per una maggiore sicurezza, prima di accedere ai servizi Home Banking ed effettuare pagamenti digita l'indirizzo della Banca direttamente nella barra di navigazione del browser.

Il nostro servizio di Home Banking è sicuro ma occorre anche la tua collaborazione per mantenere le tue informazioni al sicuro.

Alcune regole per proteggerti dalle frodi online:

1) Fai sempre attenzione alle e-mail false

Il **Phishing** è un tentativo di truffa che "non viola" i sistemi di Home Banking (che garantiscono comunque la massima sicurezza), ma tenta di acquisire le tue credenziali e/o i tuoi dati riservati.

Come si verifica:

L'utente riceve una e-mail, simile a quella della Banca, in cui viene invitato a collegarsi ad un link; cliccando si accede ad un sito simile a quello della Banca. Nel "falso sito" viene richiesto l'inserimento dei propri codici

segreti. Seguendo le istruzioni riportate, il cliente si collega al sito e trasmette lui stesso ai "truffatori" le proprie informazioni personali.

Come tutelarti:

Non inserire mai i tuoi dati personali o le tue credenziali all'interno di e-mail: Banca Progetto non richiederà mai i tuoi dati o le tue credenziali tramite e-mail.

Cerca di identificare le e-mail false: solitamente non sono personalizzate, dichiarano motivazioni di invio non precise, come ad esempio la scadenza o lo smarrimento dei codici, fantomatici problemi tecnici o di sicurezza. Spesso minacciano la sospensione del servizio in caso di mancata risposta.

Non cliccare su link e non aprire file allegati alle e-mail, soprattutto se di dubbia provenienza: i siti web "truffa" non vanno mai visitati ed i file allegati non devono mai essere scaricati sul proprio PC.

Segnala di aver ricevuto una e-mail sospetta: nel caso in cui ricevi una e-mail e non sei completamente sicuro della sua autenticità, puoi chiamare il Numero Verde 800.06.09.09 per saperne di più. Per ulteriori modalità di comunicazione con il Servizio Clienti, consulta le Condizioni Contrattuali relative allo specifico Servizio sottoscritto.

2) Controlla la sicurezza di ogni sito prima di fornire dati riservati

Prima di inserire in un sito web i tuoi codici/password o numeri di carte di credito/debito, ti consigliamo di verificare sempre che la trasmissione dei dati del sito web che stai utilizzando sia "sicura" e che il sito web sia autentico. In particolare, ricordati di verificare sempre la presenza del prefisso "**https://**" nell'indirizzo web.

Per aumentare il livello di sicurezza, è molto importante che anche il tuo PC e i tuoi dispositivi siano sempre protetti dalle minacce online.

3) Non effettuare il salvataggio automatico delle password sul PC o sul browser

I codici segreti di identificazione del tuo Home Banking e, più in generale, le tue credenziali di accesso ai servizi in Internet non dovrebbero mai essere "salvati" nella memoria del tuo PC o in quella del browser.

Puoi comunque disabilitare e cancellare le password già salvate per altri servizi dalle impostazioni del browser.

4) Proteggi il computer con AntiVirus e dispositivi di filtraggio

L'Antivirus è un ottimo strumento per stare al sicuro da tentativi di intrusione e virus, alcuni dei quali mirano a sottrarti le tue credenziali di accesso e dati personali. Ricordati di effettuare, nel tempo, i vari aggiornamenti generalmente segnalati online dal produttore anche nel proprio sito. Inoltre, può essere utile utilizzare programmi per la gestione della posta elettronica perché sono in grado di attenuare i rischi filtrando molte e-mail sospette attraverso la funzione di anti-spam.

Un'ulteriore protezione contro gli hacker, facilmente scaricabile da Internet o acquistabile, è rappresentata dai dispositivi Firewall, che tengono sotto controllo ciò che entra e ciò che esce dal PC, proprio come dei "buttafuori" digitali.

5) Seleziona la condivisione dei file su Internet

Condividere file su Internet (con i software per scaricare mp3, video, etc.) significa lasciare una "porta aperta" e quindi permettere l'accesso a "ospiti" indesiderati. Particolari software denominati *spyware*, possono avere facile accesso e "catturare" via Internet le tue informazioni personali a tua insaputa. Evita quindi di condividere file se vuoi aumentare la sicurezza, o installa un dispositivo anti-*spyware*.

6) Aggiorna spesso il Sistema Operativo

Le aziende produttrici dei Sistemi Operativi rendono disponibili gli aggiornamenti, scaricabili gratuitamente online. Si tratta delle cosiddette Patch, che incrementano, tra l'altro, la sicurezza dei programmi. Assicurati di scaricare e installare solo gli aggiornamenti ufficiali.

Decaloghi Comportamentali

In allegato il decalogo comportamentale di Abi-Lab che fornisce una serie di raccomandazioni per un utilizzo sicuro dell'home banking:

ABI Lab - Decalogo antiphishing per i clienti

Requisiti tecnici e raccomandazioni pratiche sulla sicurezza

Per navigare sul sito della Banca in tutta sicurezza è necessario che il Cliente disponga di quanto segue:

- **Accesso alla rete** tramite Internet Service Provider e modem (min. 56,6 Kbps);
- **Browser**: Chrome, Safari, Firefox, e versioni aggiornate di Internet Explorer 8, 9, 10, 11; in caso di browser con versione precedente a quella consigliata si raccomanda di scaricare la versione aggiornata dal sito del produttore (Google,Apple, Mozilla e Microsoft);
- **Applicativi e plug-in**: Acrobat Reader 4.0 (o versioni superiori), Flash Player, Media Player;
- **Risoluzione**: sito ottimizzato per la risoluzione 1024x768.

Si raccomanda di utilizzare sempre un pc sicuro per collegarsi al sito della Banca, evitando per esempio di operare da postazioni/internet point pubblici.

È' importante che il pc utilizzato per la connessione sia adeguatamente protetto.

Con riferimento alla propria postazione di lavoro si consiglia di mantenere aggiornato:

- il sistema operativo (ad esempio Windows);
- il browser e i plugin (Adobe Flash Player, Adobe Acrobat Reader, Java);
- il sistema antivirus.

Si consiglia inoltre di utilizzare:

- un personal firewall;
- un software antimalware, mantenendolo aggiornato.

Le procedure da seguire in caso di abuso riscontrato o sospetto

In caso di abuso riscontrato o sospetto, non inserire i codici e chiamare subito il Servizio Clienti al Numero Verde 800.060.909.

Uso dei Servizi di Pagamento via Internet

La Banca è responsabile della corretta esecuzione delle operazioni di pagamento impartite dal Cliente e dell'adozione di tutte le opportune precauzioni per garantire la riservatezza delle informazioni trattate nella prestazione dei Servizi (come disciplinato nell'accordo quadro sui Servizi di Pagamento e più in generale, nel Contratto).

La Banca non è responsabile nelle ipotesi di mancata prestazione, anche in misura parziale, dei Servizi di Pagamento, qualora ciò dipendesse da caso fortuito o forza maggiore compreso lo sciopero del personale della Banca così come nelle ipotesi di mancato adempimento dei propri obblighi per l'applicazione di norme o di leggi nazionali o comunitarie o per l'assolvimento di obblighi impostigli da ordini emanati dalla Pubblica Autorità.

La Banca non è responsabile nei casi di colpa grave e di dolo del Cliente.

Il Cliente è tenuto ad osservare da parte sua, con la dovuta diligenza, tutti gli obblighi previsti dalla Banca avendo riguardo al contenuto delle singole norme che disciplinano i diversi Servizi di Pagamento nonché il Servizio di Banca Diretta. Ciò in particolare per quanto attiene la riservatezza e il corretto utilizzo sia dei Codici Segreti (codice cliente, password, pin) sia degli hardware o software atti a generare o ricevere tali codici (per es. token fisici o virtuali).

Il Cliente è tenuto ad adottare tutte le possibili precauzioni finalizzate a garantire un utilizzo sicuro degli hardware di cui si avvale per impartire le istruzioni alla Banca ovvero per fruire dei Servizi messi a disposizione della Banca medesima. A titolo esemplificativo, il Cliente deve installare e aggiornare a propria cura e spese software con funzionalità antivirus, antimalware oltre che di protezione della propria identità, dati e informazioni personali.

La Banca non si assume alcuna responsabilità per la mancata o tardiva ricezione delle istruzioni dovute a qualsiasi problema di trasmissione ed informatico - quali virus, bugs, trojans, indisponibilità del servizio mail, attacchi di hackers, indisponibilità delle linee telefoniche per lavori di manutenzione od attacchi vandalici e terroristici, ecc. - od a scioperi degli operatori telefonici e dei fornitori di servizi di posta elettronica ed Internet.

Restano comunque ferme le esclusioni di responsabilità già previste dal Contratto.