LA SICUREZZA DEL TUO HOME BANKING

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

La 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.

Puoi assicurarti che la protezione sia attiva verificando che nella parte inferiore della finestra del browser Internet Explorer/Chrome sia sempre presente il "lucchetto chiuso"; se usi Firefox, verifica la presenza dell'icona colorata nella parte sinistra della barra indirizzo.

I codici di accesso

Per aumentare il livello di sicurezza, il servizio Home Banking utilizza un sistema di "autenticazione forte" combinando due Codici statici (il Codice Utente e la Password scelti da te durante il primo accesso) ed una password dinamica prodotta dal dispositivo OTP. Il dispositivo OTP genera infatti una password "usa e getta" temporanea per accedere al servizio e confermare le operazioni dispositive: dovrai generarne una per ogni operazione dispositiva che intendi effettuare, anche durante la stessa sessione.

Al fine di creare e gestire la tua password in modo corretto e sicuro, segui alcune semplici regole:

- Scegli una password che abbia una lunghezza minima 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;
- Cambiala frequentemente, almeno ogni 60 giorni;
- Non includere, al suo interno, la tua "username", il tuo nome o cognome né la tua data di nascita, o qualsiasi altro riferimento personale facilmente intuibile o codici facilmente decifrabili;
- Accertati 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 che sia diversa anche da quelle che normalmente utilizzi per altri servizi (e-mail, social network...).

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

- Non diffonderle attraverso strumenti di comunicazione (social network, e-mail, telefono);
- Prima di effettuare il "Log In" al sito Home Banking, verifica ed eventualmente disattiva la funzione di "completamento automatico" del browser, per evitarne il salvataggio automatico;
- Non annotarle, né su carta né sui tuoi dispositivi, oppure assicurati di conservarle in posti diversi.

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.

Gli avvisi via SMS/E-mail

La Banca ha predisposto il servizio di sicurezza "Alert SMS/E-mail". Un SMS o una e-mail ti avviseranno inviandoti un messaggio circa le principali operazioni che hai effettuato.

La 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.

Il monitoraggio degli accessi e delle operazioni effettuate tramite Home Banking

Il servizio Home Banking prevede che gli accessi (e 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. Se noti anomalie o si verificano 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.

IMPARA A RICONOSCERE LE FRODI ONLINE

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

Ecco alcune regole che possono aiutarti a proteggerti dalle frodi online:

1. Fai sempre attenzione alle e-mail false

Stiamo parlando di PHISHING, 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 presso cui è cliente in cui viene invitato a collegarsi ad un link; cliccando si accede ad un sito simile solo nella grafica 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 ha mai richiesto i tuoi dati tramite e-mail, né lo farà mai.

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;

Accertarti che sia presente l'icona "**lucchetto chiuso**" nella barra di stato del browser (Internet Explorer/Chrome), l'icona colorata nella parte sinistra della barra indirizzo (Mozilla Firefox): rappresentano una garanzia di autenticità del sito e di protezione delle informazioni trasmesse.

Controllare che sia attivo il **protocollo SSL 128bit** che protegge la trasmissioni dei dati, facendo doppio click sull'icona del "lucchetto chiuso".

PROTEGGI IL TUO PC DALLE MINACCE ONLINE

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

1. **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:

su Internet Explorer:

- Clicca sulla funzione Opzioni Internet nel menù Strumenti;
- Nella cartella Contenuto, clicca sul tasto Completamento Automatico;
- Elimina la selezione da Nome Utente e Password sui moduli;
- Cancella i dati precedentemente memorizzati cliccando sui tasti Cancella Moduli e Cancella Password;
- Completa l'operazione cliccando il tasto OK su tutte le finestre precedentemente aperte.

su Firefox:

- Clicca sul menù Strumenti ed attiva Opzioni;
- clicca quindi sulle voci Privacy, Impostazioni e seleziona Password Salvate;
- premi OK per chiudere la finestra di opzioni.

su Chrome:

- In alto a destra, clicca su Altro e poi Impostazioni;
- Clicca quindi su Mostra impostazioni avanzate;
- In "Password e moduli", deseleziona la casella accanto a "Richiedi di salvare le tue password web" o a "Chiedi di salvare le password con Google Smart Lock per password".

2. Proteggere 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.

3. Selezionare 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.

4. 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

ABI Lab e il CASPUR, in collaborazione con il dipartimento di informatica dell'Università "La Sapienza" di Roma, hanno realizzato un percorso formativo rivolto al cittadino per un utilizzo sicuro dell'home banking.

Puoi consultare le seguenti raccomandazioni:

ABI Lab - Decalogo antiphishing per i clienti