Banca Mediolanum S.p.A.- Capitale Sociale euro 600.064.563,10 i.v. - Codice Fiscale Iscr. Registro Imprese di Milano n. 02124090164 - Partita IVA 10698820155
Capogruppo del Gruppo Bancario Mediolanum iscritto all'Albo dei Gruppi Bancari
Banca iscritta all'Albo delle Banche - Aderente al Fondo Nazionale di Garanzia ed al Fondo Interbancario di Tutela dei Depositi - Sede Legale e Direzione: 20080 Basiglio (MI) - Via Francesco Sforza - Palazzo Meucci - Tel. +39 02 9049.1 - bancamediolanum@pec.mediolanum.it - bancamediolanum.it

INFORMAZIONI PRELIMINARI RELATIVE AI SERVIZI DI PAGAMENTO VIA INTERNET

1. Requisiti tecnici (apparecchiature, software e altri strumenti necessari) e raccomandazioni pratiche sulla sicurezza
Per navigare sul sito bancamediolanum.it 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 le 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 pubbliche.
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;
- *utilizzare:*
• un personal firewall;
• un software antimalware e di mantenerlo aggiornato.

E' possibile conoscere la cronologia degli accessi al sito dell'Home Banking seguendo le seguenti istruzioni.
Dopo aver inserito il codice cliente e il primo codice segreto, è sufficiente accedere alla "timeline". Sotto la voce Calendario, è presente la sezione "I tuoi accessi": qui è possibile visualizzare il giorno e gli orari degli ultimi cinque ingressi.
Al termine dell'utilizzo dei nostri servizi Internet, si consiglia di chiudere la sessione di lavoro, cliccando sull'icona Esci, presente in ogni pagina del sito, in alto a destra.
In caso di un periodo di inattività superiore a 20 minuti, il collegamento al nostro sito sarà automaticamente interrotto, ciò al fine di prevenire il rischio di eventuali accessi non autorizzati.

2. Accesso al Servizio di Home Banking: strumenti, modalità e istruzioni d'uso
Per accedere al Servizio di Home Banking la Banca fornisce al Cliente i seguenti strumenti:
• il Codice Cliente numerico che il Cliente può personalizzare scegliendo un nickname da utilizzare in luogo del Codice Cliente numerico;
• il Primo Codice Segreto numerico di 5 cifre;
• il Secondo Codice Segreto numerico di 5 cifre;
• il terzo codice segreto "Codice B.Med"; trattasi di un codice numerico o alfanumerico che viene generato di volta in volta in tempo reale ("one time password" o codice "OTP"). E' valido solo per una singola operazione/transazione o, quando consentito, per un complesso di operazioni/transazioni. E' da utilizzarsi insieme alle due cifre del codice segreto richieste al momento di conferma dell'operazione.
Il Codice B.Med può essere ricevuto tramite queste modalità:
SMS: il Codice B.Med è inviato direttamente al numero di cellulare ad ogni accesso alla pagina di riepilogo dell'operazione che si desidera effettuare o entrando nella sezione "La mia Area Personale".
Per tutte le disposizioni effettuate tramite app mobile, il Codice B.Med è generato automaticamente.
TOKEN APP: è la funzione che consente di generare il Codice B.Med da app Mediolanum e app Mediolanum Wallet per smartphone e tablet. Dopo aver effettuato l'autorizzazione del device da app, sarà possibile richiedere il servizio Token App tramite Home Banking (all'interno della sezione la mia Area Personale/Sicurezza/Richiedi Token App), oppure contattando il Banking Center. Al momento di effettuare una disposizione tramite sito internet, oltre a due cifre del secondo codice segreto, sarà richiesto di inserire anche il Codice B.Med, che dovrà essere generato attraverso la funzione "Codice B.Med per Internet Banking", disponibile all'interno delle app. Diversamente, per tutte le disposizioni effettuate tramite app mobile, il Codice B.Med sarà generato automaticamente e non sarà richiesto l'inserimento manuale.
TOKEN: in alternativa al servizio SMS è possibile richiedere il Token, un dispositivo portatile che il Cliente riceve al proprio indirizzo. Il Token genera automaticamente il Codice B.Med facendolo visualizzare sul display. Dopo averlo attivato, il Cliente dovrà utilizzarlo ogni volta che sarà richiesto dalle procedure di internet banking, tramite PC, smartphone e tablet. Sarà richiesto di generare/utlizzare un codice per ogni singola disposizione.

3. Orientamenti per l'uso corretto e sicuro delle credenziali di sicurezza personalizzate
Di seguito le principali regole per salvaguardare la riservatezza dei Codici Segreti:
• Custodire i Codici con cura, in modo da evitare che altri ne vengano a conoscenza;
• Non trascriverli in modo evidente su documenti che possano essere smarriti o sottratti;
• Non memorizzarli sul pc, smartphone o tablet, su file non crittografati;
• Nell'operatività telefonica con Banca Mediolanum, oltre al codice cliente, comunicare solo 2 cifre per ogni codice segreto;
• Non comunicare mai i propri codici per intero, anche a seguito di eventuali richieste telefoniche;
• Nessun dipendente, collaboratore o consulente finanziario della Banca richiederà mai i codici segreti completi;
• Inserire i propri codici segreti in modo completo solo sul sito www.bmedonline.it;

Il Cliente può decidere di cambiare i propri Codici Segreti, in qualsiasi momento, in modo autonomo, riservato e gratuito:
• attraverso l'Home Banking, all'interno dell'Area Personale, sezione Sicurezza.
• contattando un operatore del Banking Center al numero 800.107.107 dall'Italia e al numero 0039.02.9045.1625 dall'estero;
• utilizzando il servizio di Risponditore Automatico, sempre ai numeri 800.107.107 dall'Italia e 0039.02.9045.1625 dall'estero;
Si consiglia di modificare i Codici di Sicurezza periodicamente, almeno ogni 6 mesi e ogni volta che si ha il minimo dubbio che qualcuno, in modo fraudolento, ne sia venuto a conoscenza.

4. 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 Banking Center al Numero Verde 800.107.107 dall'Italia e al numero 0039.02.9045.1625 dall'estero.
Come difendersi dal phishing
Digitare sempre manualmente l'indirizzo della nostra banca e verifica di trovarti effettivamente sul nostro sito.
La Banca non effettua mai la richiesta al Cliente di inserire i propri dati via email e che ogni cambiamento relativo alla gestione dei Codici è eventualmente comunicato al Cliente con anticipo.
Come difendersi dal crimeware
Ecco alcuni consigli per prevenire la presenza di virus:
- mantenere sempre aggiornato un programma di protezione del tuo PC (antivirus ad abbonamento);
- aggiornare costantemente il sistema operativo e gli applicativi in uso;
- effettuare spesso la pulizia dei file temporanei (cache e cookies);
- digitare manualmente l'indirizzo della banca e verificare, una volta collegato, di trovarsi effettivamente sul sito di Banca Mediolanum. Controllare che nella barra degli indirizzi sia rimasto l'indirizzo corretto e che i dati richiesti nella pagina non siano diversi dal solito;
- evitare il salvataggio automatico delle password sul browser tramite la funzione di "completamento automatico";

5. Procedure per inoltrare e autorizzare un'operazione di pagamento e/o ottenere informazioni, inclusi gli esiti di ogni azione
Si prenda visione dello specifico documento pubblicato sul sito internet della Banca alla sezione Sicurezza.

6. Responsabilità e oneri della Banca e del Cliente per quanto riguarda l'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. Il tutto come disciplinato nell'accordo quadro sui Servizi di Pagamento nonché nelle Condizioni per l'erogazione dei servizi di pagamento di cui alle Sezioni C5 e C6 del Fascicolo Contrattuale, 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 delle 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 (Primo Codice Segreto, Secondo Codice Segreto, Codice B.Med) sia degli hardware o software atti a generare o ricevere tali codici (per es. token fisici o virtuali, Device, Mediolanum Wallet, Medilanum App).
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 POP, 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 nel Contratto in particolare per quanto attiene l'art. 24 della Sezione A del Fascicolo Contrattuale – Norme di Banca Mediolanum.