BANCA POPOLARE DI MILANO

GUIDA ALLA SICUREZZA DELL'UTILIZZO DEI SERVIZI BANCARI ONLINE

In questa guida ti forniamo alcune indicazioni operative sull'utilizzo degli strumenti di sicurezza del tuo conto, seguite da informazioni utili alla sicurezza online e alla protezione della tua identità digitale.

INDICE

1. COME ACCEDERE A BPMBANKING.IT

2. ATTIVAZIONE APP BPM MOBILE

3. COME UTILIZZARE L'APP CERTIFICATA

4. ATTIVAZIONE DEL TOKEN FISICO

5. COME SI UTILIZZA IL TOKEN

6. CONSIGLI UTILI PER LA TUA SICUREZZA

7. PROTEGGI LA TUA IDENTITÀ DIGITALE!

8. UTILIZZARE IN SICUREZZA L'INTERNET BANKING

9. IN GENERALE QUANDO SEI ONLINE RICORDATI DI...

1. COME ACCEDERE A BPMBANKING.IT

1.1 PER ACCEDERE ALL'AREA PRIVATA DI WWW.BPMBANKING.IT

Inserisci USERID e la tua Password Personale, successivamente dovrai utilizzare uno strumento di Strong Authentication a scelta fra token digitale, integrato nell'App BPM Mobile oppure token fisico.

Se accedi da una postazione autorizzata:
Per ogni computer da cui ti connetti al sito bpmbanking.it, potrai scegliere se renderlo una **postazione autorizzata**: in questo modo ad ogni nuova login ti verrà richiesta solo la USERID e Password Personale. Assicurati di effettuare questa scelta soltanto su computer adeguatamente protetti e strettamente personali. Eventuali operazioni dispositive dovranno comunque essere autorizzate tramite il token digitale oppure attraverso il codice generato dal token fisico.
La postazione autorizzata collega la tua utenza al computer ed al browser che stai utilizzando. Tale collegamento resta attivo fino a quando non vengono cancellati i cookie.

1.2 PER ACCEDERE DA APP

Dopo aver certificato l'App, che verrà associata in maniera univoca al tuo smartphone e alla tua USERID, per entrare nell'App e consultare la tua posizione sarà sufficiente inserire la Password Personale.

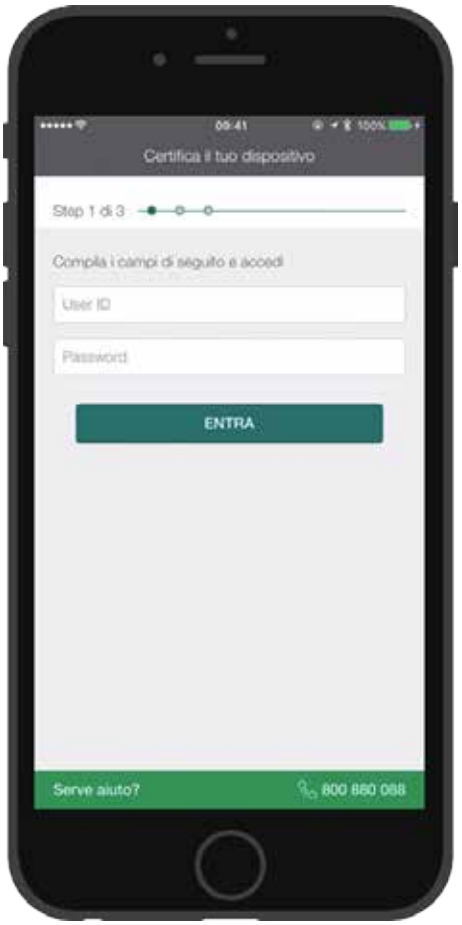
Per mantenere elevati livelli di sicurezza del tuo conto bpmbanking.it, hai a disposizione due strumenti alternativi di **Strong Authentication** che ti serviranno per autorizzare gli accessi al conto e le operazioni dispositive: l'App BPM Mobile con token digitale oppure il token fisico.

Di seguito trovi le informazioni operative in base allo strumento che hai scelto.

2. ATTIVAZIONE APP BPM MOBILE

Le **funzioni di sicurezza sono integrate nell'App di BPM Mobile**: questo ti permette di avere la tua Banca sempre a portata di mano e con un unico strumento consultare il conto corrente, effettuare e autorizzare operazioni in qualsiasi momento, sia dall'App stessa che dal sito bpmbanking.it
Ti ricordiamo che l'App BPM Mobile è disponibile gratuitamente su Google Play, App Store e Windows Store.

2.1 COME CERTIFICARE L'APP
Per utilizzare l'App di BPM Mobile sarà necessario procedere con la **certificazione**: ogni installazione dell'App viene così associata ad un unico cliente.



1. Se non l'hai ancora fatto, certifica il tuo numero di cellulare ed indirizzo email dalla tua area privata del sito bpmbanking.it;
2. apri l'App BPM Mobile sul tuo smartphone ed inserisci USERID e Password;
3. inserisci il codice OTP (One Time Password) che riceverai sul numero di cellulare certificato e conferma;
4. se hai scelto l'App come tuo strumento di Strong Authentication, crea ora il tuo PIN di sicurezza che può variare da 4 a 8 cifre. Per alcuni modelli di smartphone sarà possibile associare al PIN di sicurezza la tua impronta digitale che potrai utilizzare in alternativa al PIN.

Attenzione: scegli bene il tuo PIN, ti verrà richiesto ogni volta per disporre le operazioni e dopo cinque tentativi errati, per motivi di sicurezza, verrà bloccato; per sbloccarlo sarà necessario chiamare il numero verde come descritto nella schermata di blocco che compare. Al contempo l'App verrà bloccata e per sbloccarla sarà necessario ripetere il processo di certificazione;

5. la tua App è ora certificata e puoi procedere con la configurazione delle funzioni veloci e con la normale operatività.

3. COME UTILIZZARE L'APP CERTIFICATA

3.1 SUL SITO BPMBANKING.IT

Hai scelto come strumento di Strong Authentication l'App? Anche quando accedi da web tieni a portata di mano il tuo smartphone. Le operazioni di login o dispositive, per essere autorizzate, generano automaticamente una notifica push che riceverai sul tuo smartphone:

per completare l'operazione di login dovrai fare un tap sulla notifica ricevuta;

per completare le operazioni dispositive dovrai fare un tap sulla push notification e inserire il PIN di sicurezza oppure la tua impronta digitale;

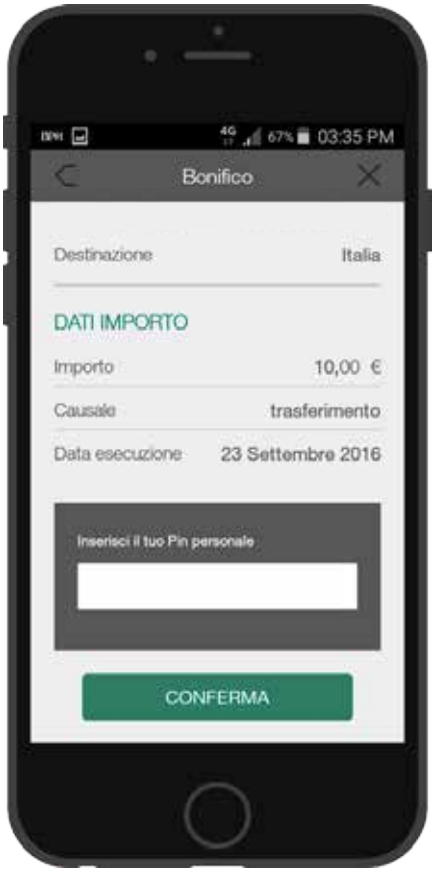
una pagina di conferma sul sito ti avviserà del buon esito dell'operazione.

Se il tuo telefono non dovesse ricevere le notifiche push potrai comunque generare il codice di sicurezza, questa funzione è disponibile anche quando il tuo smartphone è offline:

- clicca sul bottone presente nella pagina web «usa Genera codice token»;
- apri l'App sul tuo smartphone e vai alla funzione veloce «Genera codice token» e inserisci nella pagina web il codice generato dall'App.

3.2 SULL'APP BPM Banking

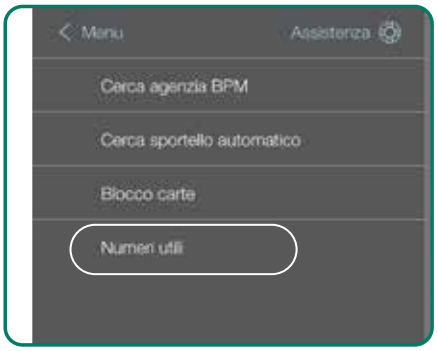
- Il login verrà effettuato con il solo inserimento della Password Personale.
- Utilizzerai il PIN che hai scelto per autorizzare sull'App le operazioni dispositive. Se hai abilitato la modalità fingerprint, in alternativa al PIN, utilizzerai la tua impronta digitale.



Con il token digitale il tuo cellulare diventa uno strumento molto importante per la tua sicurezza: trattalo con la dovuta attenzione come fai per le tue carte di pagamento.

3.3 UTILIZZO DELL'APP PER CONTATTARE IL SERVIZIO CLIENTI

Per contattare il Servizio Clienti accedi all'App con la tua password e chiama il Numero Verde che trovi cliccando sull'icona ☰, segui il percorso Assistenza > Numeri utili e scorri orizzontalmente la barra relativa alle categorie dei Numeri utili finché non raggiungi la voce Help Center.



Sarai automaticamente identificato e potremo offrirti un supporto ancora più immediato!

FAQ

1. E SE PERDO O MI RUBANO IL TELEFONO?

Contatta subito il Customer Center al numero 800 880 088. In seguito potrai installare l'App su un nuovo smartphone.

2. E SE DISINSTALLO L'APP O CAMBIO TELEFONO?

Per motivi di sicurezza solo una installazione dell'App associata alla tua USERID avrà attiva la funzionalità di token digitale. Sarà la prima che certifichi.
Se hai cambiato telefono disattiva l'App precedente contattando il Customer Center all'800 880 088 prima di procedere alla nuova installazione.

3. E SE HO PIÙ TELEFONI?

L'app può essere installata su più telefoni ma le installazioni successive alla prima non avranno attiva la funzionalità di token digitale per autorizzare le operazioni da web.

4. IL MIO TELEFONO È ABBASTANZA EVOLUTO?

L'app che integra le funzionalità di sicurezza è disponibile per:

- iPhone con iOS versione 7.1 o superiore
- smartphone con Android versione 4.1 o superiore
- smartphone con Windows 10 Mobile o superiore

La possibilità di abilitare l'uso dell'impronta digitale verrà automaticamente proposta in fase di attivazione sui device che garantiscono un adeguato livello di sicurezza.

5. PERCHÉ IL MIO TELEFONO NON RICEVE LE NOTIFICHE PUSH?

Alcuni costruttori per massimizzare la durata della batteria impediscono la notifica ad applicazione chiusa, salvo impostazione di un parametro di configurazione del telefono. In particolare per i modelli Huawei occorre andare in Impostazioni > impostazioni avanzate > gestione batteria > App protette e abilitare l'app BPM Mobile.
Per i dispositivi Asus seleziona Gestione avvio automatico > App scaricate e di fianco all'icona dell'app BPM Mobile imposta l'avvio automatico su "Consenti".
A seguito della modifica dell'impostazione, per renderla effettiva, è necessario avviare almeno una volta l'app BPM Mobile.

4. ATTIVAZIONE DEL TOKEN

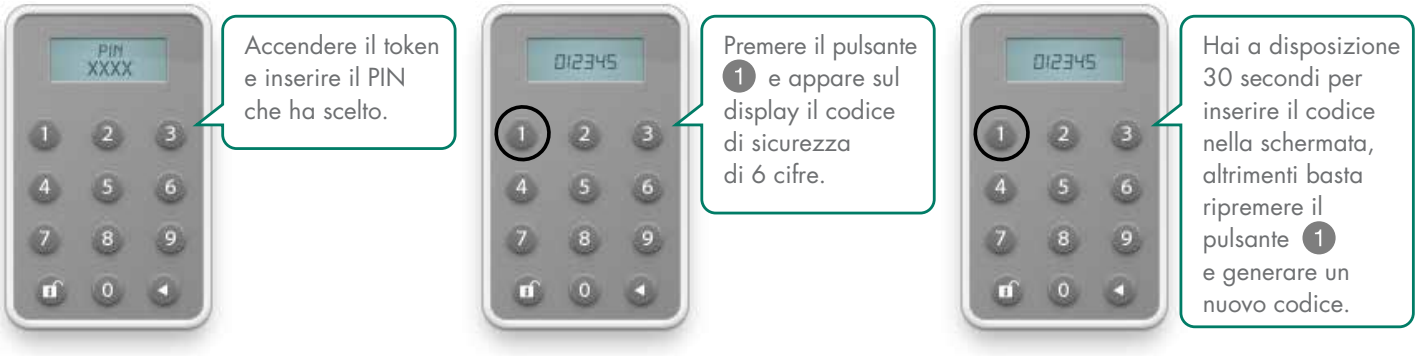
Se hai scelto il token fisico come strumento di Strong Authentication, **accendilo** tenendo premuto il pulsante ◀ e contemporaneamente il pulsante 🔓

Il token è protetto da un **PIN di 4 cifre** che potrai scegliere **alla prima accensione** e non è modificabile in futuro.

Per rendere operativo il token, occorre **attivarlo**: accedi al sito bpmbanking.it con USERID e password e in pochi passi verrai guidato per completare l'attivazione.

5. COME SI UTILIZZA

Una volta attivato il token, a ogni accesso al sito e per autorizzare le operazioni dispositive comparirà una schermata con la richiesta di un codice di sicurezza di 6 cifre:



Attenzione: dopo cinque tentativi errati, per motivi di sicurezza, il token fisico viene bloccato. Chiama il numero verde 800 880 088 in caso di blocco del dispositivo.

Ti ricordiamo che il tuo token è uno strumento importante per la tua sicurezza e lo devi trattare con la dovuta attenzione: **se dovessi perderlo o ti dovesse venire rubato devi subito chiedere che venga sospeso**, puoi farlo dal sito bpmbanking.it se disponi di una postazione autorizzata oppure puoi chiamare il numero verde 800 880 088. Potrai ritirare in agenzia il nuovo token.

ASSISTENZA SERVIZIO CLIENTI 800 880 088

Dal lunedì al venerdì dalle 8:00 alle 22:00 e il sabato dalle 9:00 alle 17:00

Il numero è a disposizione per assistenza e informazioni in caso di furto, smarrimento blocco del token o dell'App

6. CONSIGLI UTILI PER LA TUA SICUREZZA

La **sicurezza** è il risultato dell'azione combinata della banca e del modo in cui utilizzi internet.
Per garantire la sicurezza della tua operatività, la banca ha adottato delle misure che:

- evolvono nel tempo, in funzione delle nuove minacce da contrastare e dell'evoluzione della tecnologia a supporto;
- non violano la privacy del cliente;
- non impattano in maniera significativa sull'usabilità del servizio;
- rispettano i requisiti normativi di settore* e le best practice di sistema, in particolare per quanto riguarda l'utilizzo di meccanismi di autenticazione forte (Strong Authentication).

Il servizio BPM Banking rientra nella categoria di servizi di pagamento via internet, questo implica responsabilità ed obblighi da parte della Banca e dei suoi clienti.

Queste informazioni sono riportate nelle condizioni generali del contratto firmato dal cliente e dalla Banca in fase di attivazione del Servizio di Banca Multicanale, di cui possiedi una copia.

BPM Banking, al fine di rispettare i propri obblighi e, soprattutto, di permettere alla propria clientela di operare in semplicità e tranquillità, ha predisposto le misure di sicurezza che trovi descritte in questo manuale e sul sito. Le soluzioni adottate sono conformi alle migliori procedure in tema di sicurezza dei servizi di pagamento su internet ed a quanto definito dalle normative di settore.

In quanto cliente, anche tu hai degli obblighi che puoi facilmente rispettare seguendo le indicazioni che trovi di seguito. Inoltre, puoi costantemente reperire informazioni relative alla sicurezza sul sito di BPM Banking e tramite le comunicazioni che ti inviamo via email.

Quello che noi ti **mettiamo a disposizione** sono degli **strumenti** che tu devi imparare a conservare ed utilizzare per navigare sicuro.

7. PROTEGGI LA TUA IDENTITÀ DIGITALE!

L'identità digitale è l'insieme degli elementi che permettono a chi fornisce un servizio internet di riconoscerti.

La tua identità digitale BPM Banking è composta da:

- **USERID**: è il tuo codice cliente di 7 cifre che resta invariato nel corso del tempo.
- **Password iniziale**: ti viene assegnata in fase di attivazione del servizio e devi modificarla

** in particolare gli "orientamenti finali sulla sicurezza dei pagamenti via internet" emessi dall'Autorità Bancaria Europea.*

al primo accesso con una di tua scelta.
- **Password Personale**: è la password che scegli al primo accesso in occasione del **cambio password obbligatorio**. Con questa operazione sostituisci la password iniziale con una di tua scelta composta da un minimo di 8 ad un massimo di 16 caratteri alfanumerici.
- **Strong Authentication**: il token o l'App installata sul tuo smartphone sono strumenti alternativi che permettono di realizzare un secondo livello di autenticazione ed autorizzazione nella tua operatività online generando dei codici temporanei. Hanno sostituito la Carta dei Servizi Telematici utilizzata in precedenza.
- **Il numero di cellulare e l'indirizzo email**: sono fondamentali per tenere sotto controllo il tuo conto corrente. Ci permettono di contattarti velocemente per informarti o inviarti dati per completare le operazioni, per questo ti chiediamo che siano certificati e univoci e sempre aggiornati.

L'**identità digitale** può essere soggetta al rischio di **furto e utilizzo fraudolento da parte di terzi**.

Le frodi informatiche, tra cui le più diffuse sono il **phishing** ed il **crimeware**, consistono nell'utilizzare indebitamente informazioni personali di un soggetto, al fine di identificarsi, in tutto o in parte, nel soggetto stesso per compiere a suo nome azioni illecite (effettuare disposizioni bancarie oppure per ottenere credito tramite false credenziali).

ATTENZIONE se pensi di essere stato oggetto di una frode informatica, quindi sia in caso di furto di identità digitale che di operazioni bancarie non riconosciute, contatta immediatamente il servizio di assistenza clienti all'800 880 088 che si attiverà subito per:

- mettere in sicurezza nuovamente il tuo servizio on line;
- richiamare, ove necessario e possibile, la disposizione non riconosciuta.

7.1 COS'È IL PHISHING

Il phishing viene attuato da truffatori che, tramite l'invio di email portano l'utente su pagine fraudolente che richiedono l'inserimento di informazioni riservate. In genere sono pagine composte utilizzando il logo, il nome e il layout tipico dell'azienda imitata, come ad esempio una banca oppure una società emittente carte di credito.

I metodi più frequentemente utilizzati dai phisher sono:

- l'invio di false email o di falsi SMS contenenti link;
- pagine che si presentano durante la navigazione sul web;
- falsi annunci pubblicitari presentati sui motori di ricerca.

7.2 COS'È IL CRIMEWARE

Il crimeware viene attuato diffondendo, presso postazioni non adeguatamente protette, un codice malevolo (malware) in grado di rubare informazioni riservate del cliente e a volte prendere il controllo da remoto della postazione contaminata.

I più diffusi tipi di maleware sono: virus, worm, trojan, spyware, dialer, keylogger.

La diffusione dei maleware può avvenire secondo varie modalità:

- attraverso un supporto, quali ad esempio CD-Rom oppure Pen Drive;
- attraverso la posta elettronica e gli allegati contenuti nelle email;
- scaricando dati e programmi da internet oppure navigando su siti non sicuri.

8. UTILIZZARE IN SICUREZZA L'INTERNET BANKING

- **Conserva tutti i dati** che compongono la tua identità digitale con la **massima riservatezza**: non memorizzare mai le tue password sul telefono, sul computer oppure sul browser;
- quando scegli la Password Personale al primo accesso, che dovrà essere composta da un minimo di 8 ad un massimo di 16 caratteri (meglio se alfanumerici), componila in maniera non banale e difficilmente riconducibile ad informazioni che riguardano te o la tua famiglia;
- **non usare password già utilizzate** per altri servizi e modifica frequentemente le password di accesso al tuo servizio online;
- accedi al sito **digitando per esteso l'indirizzo del servizio direttamente** nella barra del browser;
- **non accedere al servizio da computer pubblici** o utilizzando reti Wi-Fi non sicure. Utilizzare computer in Internet Cafè, biblioteche oppure luoghi simili è rischioso perché potrebbero contenere malware in grado di registrare ciò che stai digitando; se utilizzi una rete non sicura i tuoi dati potrebbero essere facilmente intercettati;
- ricordati sempre di **mantenere aggiornati il tuo numero di telefono e il tuo indirizzo email**: ti permetterà di operare in completa sicurezza e ci darà la possibilità di contattarti tempestivamente in caso di necessità;
- quando hai terminato di utilizzare il sito della tua banca **effettua sempre il logout** per disconnettere la sessione;

Ti ricordiamo inoltre che la **Banca non richiede mai informazioni personali via email, telefono o SMS**. È quindi importante prestare attenzione alle comunicazioni, leggendo con cura i messaggi che ricevi. Le comunicazioni di phishing spesso sono generali, non si rivolgono specificatamente a te chiamandoti per nome e contengono errori ed imprecisioni.

9. IN GENERALE QUANDO SEI ONLINE RICORDATI DI:

- utilizzare sul tuo PC, tablet o smartphone antivirus e antispyware e aggiornali frequentemente;
- non inserire mai dati richiesti in comunicazioni di dubbia provenienza;
- prestare particolare attenzione ai pop up che si aprono automaticamente e verifica sempre l'effettiva url del sito passando il mouse sul link e leggendo l'indirizzo che compare nella barra inferiore del browser;
- non aprire allegati di posta elettronica inviati da mittenti sconosciuti o contenuti in mail non attese;
- quando sottoscrivi un servizio presta sempre attenzione ai dati che ti vengono richiesti. Tramite questionari molto lunghi, potresti essere indotto a fornire ad estranei delle informazioni personali non necessarie;
- **non divulgare sui social network informazioni che riguardano la tua identità** (data o luogo di nascita, indirizzo, numero di telefono);
- prestare attenzione ai permessi richiesti dalle applicazioni che usi sul telefono; potresti inavvertitamente autorizzare accessi alle informazioni contenute sullo smartphone (contatti, foto, documenti);
- non navigare e non scaricare materiali o applicazioni da siti non ufficiali o con una cattiva reputazione.

In qualsiasi momento trovi informazioni aggiornate in temi di sicurezza nel menù Sicurezza della pagina pubblica di bpmbanking.it

ASSISTENZA SERVIZIO CLIENTI 800 880 088

Dal lunedì al venerdì dalle 8:00 alle 22:00 e il sabato dalle 9:00 alle 17:00