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 online.

INDICE

1. COME ACCEDERE AL SERVIZIO DI INTERNET/MOBILE BANKING

COME ACCEDERE A YOUWEB
Sulla pagina d'accesso all'area riservata, inserisci il Codice identificativo e la tua Password Personale. Successivamente dovrai utilizzare uno strumento di autenticazione a scelta fra il Token App, integrato in YouApp, oppure il Token Fisico.

COME ACCEDERE A YOUAPP
YouApp è disponibile gratuitamente su **Google Play**, **App Store** e **Huawei AppGallery**. Dopo aver scaricato e certificato l'App, che verrà associata in maniera univoca al tuo smartphone e al tuo Codice Identificativo, per accedere e consultare la tua posizione sarà sufficiente inserire la Password Personale o, se abilitato, il riconoscimento biometrico.

Per utilizzare i servizi di internet e mobile banking in totale sicurezza, hai a disposizione due strumenti alternativi che ti serviranno per autorizzare gli accessi al conto e per operare online: il Token App oppure il Token Fisico.
Di seguito trovi le informazioni operative in base allo strumento che hai scelto.

2. ATTIVAZIONE DEL TOKEN APP

Il software di sicurezza, detto Token App, è integrato in YouApp, così puoi avere la tua Banca sempre a portata di mano. Con un unico strumento puoi consultare il conto corrente, effettuare e autorizzare operazioni in qualsiasi momento, sia da YouApp che da YouWeb. Alternativamente hai la possibilità di generare, direttamente dall'App, dei codici OTP che dovrai utilizzare per confermare le operazioni di pagamento che inserisci sul sito.

COME CERTIFICARE YOUAPP

Per utilizzare YouApp è necessario procedere con la **certificazione**: ogni installazione dell'App viene così associata ad un unico cliente. Il primo dispositivo (ad esempio lo smartphone) sul quale sarà certificata l'App diventa il tuo strumento di sicurezza (Token App) che utilizzi per generare i codici OTP, accedere al sito e per autorizzare tutte le tue operazioni. L'App installata sul primo dispositivo è definita "App primaria".

Segui questi semplici passaggi per certificare la tua App.

1. Scarica YouApp dallo Store e, dopo averla installata, inserisci il Codice Identificativo e la Password. Se è il tuo primo accesso ti sarà chiesto di modificare la Password.
2. Inserisci il codice OTP (One Time Password) che riceverai via Sms sul tuo numero di cellulare;
3. Scegli un nome da assegnare al tuo dispositivo e se abilitare la ricezione delle notifiche push.
4. Crea il tuo Codice Dispositivo* compreso tra 4 a 8 cifre. Se previsto dal tuo dispositivo, puoi attivare il riconoscimento biometrico (tramite impronta digitale o riconoscimento del viso) che utilizzerai in alternativa al Codice dispositivo.
5. La tua App è ora certificata e puoi procedere con la configurazione delle funzioni veloci e con la normale operatività.

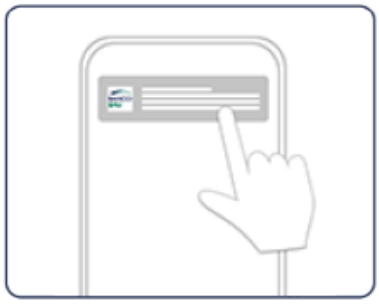
Se decidi di trasferire l'App primaria su un nuovo dispositivo, oltre alla conferma dei codici tramite Sms, ti verrà richiesto di confermare, tramite chiamata con voce registrata sul numero certificato, il codice visualizzato in App. Successivamente, dovrai inserire un ulteriore codice OTP inviato all'indirizzo email.

***ATTENZIONE: scegli con attenzione il tuo Codice Dispositivo, ti sarà richiesto ogni volta per confermare le operazioni di pagamento. Dopo 5 tentativi errati, per motivi di sicurezza, sarà bloccato. Per sbloccarlo disinstallare e reinstallare l'App e ripetere il processo di certificazione.**

3. COME UTILIZZARE IL TOKEN APP

3.1 - Nel servizio di Internet Banking "YouWeb"

Anche quando accedi da YouWeb tieni a portata di mano il tuo smartphone. Le operazioni di login o dispositive, per essere autorizzate, generano una notifica push che riceverai automaticamente sul tuo smartphone:



per completare l'operazione di login fai tap sulla notifica ricevuta;

per autorizzare le operazioni dispositive fai tap sulla notifica push e inserire il riconoscimento biometrico, se abilitato, oppure il Codice Dispositivo;

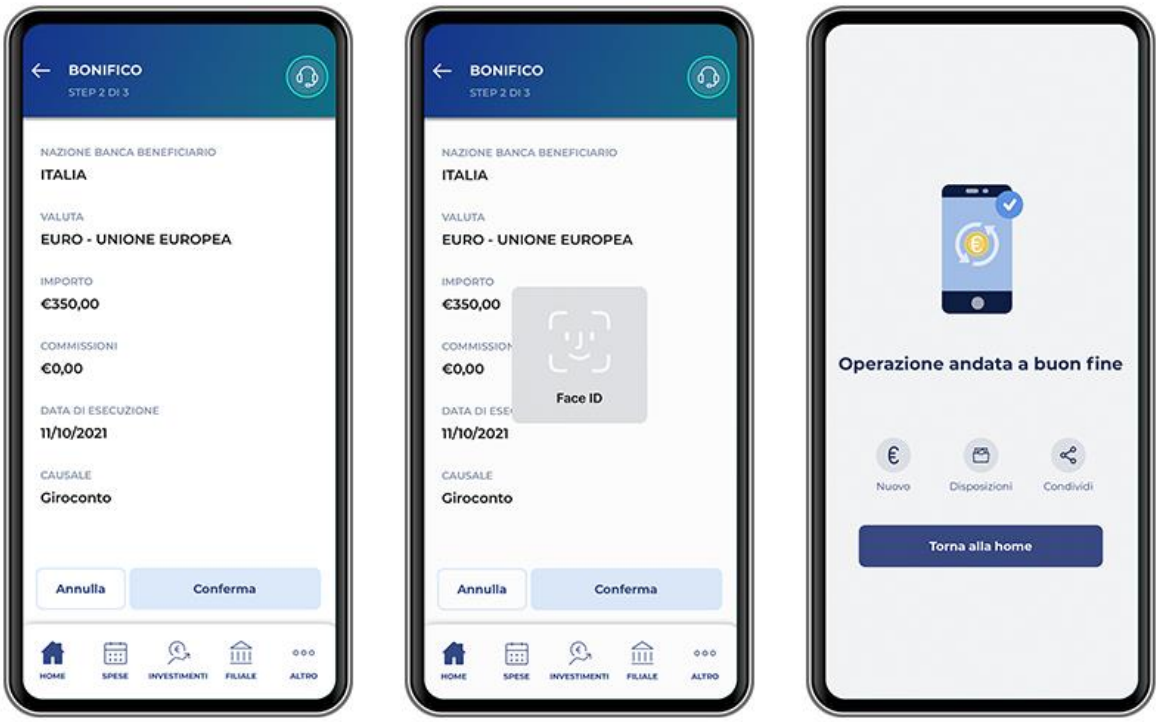
una pagina di conferma sul sito ti avviserà del buon esito dell'operazione.

Se il tuo telefono non dovesse ricevere la notifica push, potrai comunque generare un Codice OTP su YouApp; questa funzione è disponibile anche quando il tuo smartphone è offline:

- seleziona il link "clicca qui" presente nella pagina web che compare per autorizzare l'accesso/la disposizione;
- apri l'App sul tuo smartphone, utilizza la funzione veloce "Genera OTP" e inserisci nella pagina web il codice generato dall'App.

3.2 - Nel servizio di Mobile Banking "YouApp"

Il login viene effettuato con l'inserimento del riconoscimento biometrico, se abilitato, o con la Password Personale.
Le operazioni dispositive vengono autorizzate con l'inserimento del riconoscimento biometrico, se abilitato, o il Codice Dispositivo che hai scelto.



Con il Token App 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 – FAQ

1. E SE PERDO O MI RUBANO IL TELEFONO?
Contatta subito il Numero Verde 800 024 024. 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 al tuo Codice Identificativo, avrà attiva la funzionalità di Token App. Sarà la prima che certifichi e verrà chiamata "App primaria". Ti consigliamo, quindi, di eseguire la prima installazione sul dispositivo che porti sempre con te (smartphone). Se hai cambiato telefono puoi procedere alla certificazione dell'App primaria sul nuovo dispositivo.

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 App per autorizzare le operazioni da web. Puoi installare l'App anche sul tablet.

4. IL MIO TELEFONO È ABBASTANZA EVOLUTO?
L'App che integra le funzionalità di sicurezza è disponibile per:

- iPhone con iOS versione 16.0 o successive
- Android con versione 7.0 o successive

- Huawei Mobile Services

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

5. PERCHÉ IL MIO TELEFONO NON RICEVE LE NOTIFICHE PUSH?
Puoi controllare l'abilitazione delle notifiche push direttamente nelle Impostazioni del tuo device. Per ricevere le notifiche push è necessario siano attive. Nel caso in cui risultino già attive, controlla la connessione Internet del tuo telefono.

4. IL TOKEN TASTIERA

Se hai scelto il Token Tastiera 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. A ogni accesso al sito e per autorizzare le operazioni dispositive comparirà una schermata con la richiesta di un codice OTP di 6 cifre:

Attenzione: dopo cinque tentativi errati, per motivi di sicurezza, il Token Tastiera viene bloccato. Chiama il Numero Verde 800 024 024 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 venisse rubato devi subito chiedere che venga sospeso chiamando l'Assistenza Clienti. Potrai ritirare in agenzia un nuovo token.

5. IL TOKEN CARD (dispositivo non più commercializzato)

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 venisse rubato devi subito chiedere che venga sospeso chiamando l'Assistenza Clienti. Potrai ritirare in agenzia un nuovo token.

Il Token in formato Card, detto Token Card, è una carta sottile e flessibile come un bancomat, che genera codici OTP, utilizzabili come password usa e getta, una sola volta e validi per un intervallo di tempo ridotto. Anche il Token Card ti viene consegnato già attivo e può essere utilizzato da qualsiasi computer o dispositivo.
La pressione sul pulsante fa accendere/spegnere il display della Card e ottenere il codice OTP (One Time Password).

6. IL TOKEN AUDIO

Il nuovo Token offre un ritorno audio per tutte le icone, messaggi e numeri da immettere e visualizzare.
I messaggi audio possono essere trasmessi attraverso l'altoparlante interno del dispositivo, o tramite un auricolare per maggiore riservatezza.

È possibile modificare il volume, la lingua, la velocità di uscita delle parole audio, e può anche richiedere che l'uscita audio venga ripetuta.

Le funzionalità di uscita audio sono controllate premendo il tasto funzione insieme ad altri tasti, in modo simile a come il tasto shift sulla tastiera di un computer viene utilizzato per richiamare funzioni speciali.

Le combinazioni di funzioni e pressione dei tasti numerici per richiamare la funzionalità di controllo audio sono i seguenti:

- Tenendo premuto il Tasto funzione + il tasto 0: ripetizione ultimo messaggio audio.
- Tenendo premuto il Tasto funzione + il tasto 1: si passa alla selezione della lingua precedente nella lista, riproduce un messaggio audio con la lingua selezionata e continua.
- Tenendo premuto il Tasto funzione + il tasto 3: si passa alla selezione della lingua successiva nell'elenco, riproduce un messaggio audio con la lingua selezionata e continua.
- Tenendo premuto il Tasto funzione + il tasto 4: riduce la velocità audio, fornisce un feedback sulla nuova velocità e continua. Ci sono 8 possibili velocità.
- Tenendo premuto il Tasto funzione + il tasto 5: interrompe l'applicazione corrente e legge il numero di serie.

- Tenendo premuto il Tasto funzione + il tasto 6: aumenta la velocità audio, fornisce un feedback sulla nuova velocità e continua. Ci sono 8 possibili velocità.

- Tenendo premuto il Tasto funzione + il tasto 7: diminuisce il volume audio, e fornisce un feedback sul nuovo volume e continua. Ci sono cinque volumi differenti.

- Tenendo premuto il Tasto funzione + il tasto 9: aumenta il volume audio e fornisce un feedback sul nuovo volume e continua. Ci sono cinque volumi differenti.

Dopo che un controllo audio è stato eseguito, il Token Audio continua con il processo di applicazione corrente, (ad eccezione di 'tasto funzione + 5', spiegato in precedenza).

Se il tasto funzione viene premuto troppo a lungo senza che un altro pulsante venga premuto, la funzionalità del pulsante 'bloccato' inizia. Se il tasto viene rilasciato, il dispositivo torna operativo

7. 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 YouWeb 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 internet banking, di cui possiedi una copia.

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

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

8. PROTEGGI LA TUA IDENTITÀ ONLINE

L'identità online è l'insieme degli elementi che permettono a chi fornisce un servizio internet di riconoscerti. La tua identità online è composta da:

- Codice Identificativo: è il tuo codice cliente di 7 cifre che resta invariato nel corso del tempo.
- Password iniziale: è composta da 8 caratteri e ti è stata inviata via Sms sul tuo numero di cellulare. In occasione del primo accesso ai canali online ti sarà chiesto di modificare la Password iniziale 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 30 caratteri alfanumerici.
- Strong Authentication: il Token Fisico o il Token App (installato sul tuo smartphone) sono strumenti alternativi che permettono di realizzare un secondo livello di autenticazione e autorizzazione nella tua operatività online generando dei codici OTP.
- 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 online 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 online che di operazioni bancarie non riconosciute, contatta immediatamente l'Assistenza Clienti che si attiverà subito per:
- mettere in sicurezza nuovamente il tuo servizio on line;
- richiamare, ove necessario e possibile, la disposizione non riconosciuta.

8.1 - 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.

8.2 - 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 malware sono: virus, worm, trojan, spyware, dialer, keylogger.

La diffusione dei malware 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.

9. REGOLE PER LA TUA SICUREZZA

- Conserva tutti i dati che compongono la tua identità on line con la massima riservatezza: non memorizzare mai le tue password sul telefono, sul computer oppure sul browser;
- In generale BancoBpm non ti contatterà mai per chiederti le tue credenziali d'accesso o Codici OTP generate dagli strumenti di sicurezza, ricevute via SMS o email, non comunicare tali informazioni a nessuno;
- Non fermarti alle apparenze i messaggi di phishing possono essere inviati via email ed SMS e sembrare inviati dalla tua Banca. Non cliccare su link e/o allegati ricevuti via sms, e-mail o sistemi di messaggistica;
- la Banca non ti chiede mai di scaricare software o applicazioni utilizzando link inviati tramite sms o email; questa modalità viene usata dai truffatori per indurre i clienti a scaricare app pericolose per la sicurezza del telefono. Le app rese disponibili dalla Banca sono presenti solo sugli store ufficiali;
- non usare per i servizi bancari password già utilizzate per altri servizi;
- Abilita sempre sulle funzionalità di pagamento i servizi di notifica resi disponibili dalla tua banca tramite notifiche push, sms o email;
- 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;
- Ogni volta che hai un sospetto su quanto sta accadendo contatta la tua Banca per chiedere chiarimenti e verifiche ai numeri ufficiali presenti sul sito.

10. UTILIZZARE IN SICUREZZA L'INTERNET BANKING

- quando scegli la Password personale al primo accesso, che dovrà essere composta da un minimo di 8 ad un massimo di 30 caratteri alfanumerici, componila in maniera non banale e difficilmente riconducibile ad informazioni che riguardano te o la tua famiglia;
- accedi al sito digitando per esteso l'indirizzo del servizio direttamente nella barra del browser;
- 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

11. UTILIZZARE IN SICUREZZA LE CARTE DIGITALIZZATE

1. Se digitalizzi una carta Imposta sempre un PIN/ Password di accesso al telefono e preferisci una modalità di riconoscimento biometrico come l'impronta digitale o il riconoscimento facciale se il tuo device lo permette, per evitare un facile accesso ed utilizzo da parte di altri in caso di incustodita, smarrimento o furto;
2. Digitalizzare la tua carta solo sul tuo dispositivo personale, ricordati che, indipendentemente dal device utilizzato, sarai sempre ritenuto responsabile dei pagamenti effettuati con la tua carta digitalizzata;
3. Non rivelare mai i codici ricevuti via sms (OTP) relativi alla digitalizzazione delle tue carte a presunti operatori: la Banca non richiede mai tali codici, né telefonicamente né tramite e-mail

12. 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 email non attese;
- prestare sempre attenzione ai dati che ti vengono richiesti in fase di sottoscrizione di un servizio. 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 sul sito http://bancobpm.it, nella sezione disponibile prima dell'accesso all'area riservata del servizio di internet banking YouWeb.