IBAN Conto

Num. Pratica

MODULO DI ADESIONE

ibonline Conto Corrente (per privato consumatore)

Con la presente, io sottoscritto, i cui dati identificativi sono di seguito riportati ('Cliente')

Dati Personali Titolare

Nome e Cognome:	Luogo e data di nascita:
Codice fiscale:	Cittadinanza:
Sesso:	Stato civile:
Indirizzo di residenza:	
Informazioni di contatto	
N. tel. abitazione:	N. tel. cellulare:
E-mail:	

Chiedo l'apertura di ibonline conto corrente e, a tal fine:

- prendo atto che il servizio richiesto è riservato alle persone fisiche di maggiore età che abbiano cittadinanza e residenza fiscale esclusivamente italiana, pertanto, dichiaro di essere in possesso dei menzionati requisiti;
- dichiaro che la Banca in tempo utile, prima della sottoscrizione della presente proposta:
  a. mi ha messo gratuitamente a disposizione, su supporto digitale durevole, il Foglio Informativo che illustra le caratteristiche, i rischi e le condizioni economiche applicabili al servizio offerto;
  b. mi ha fornito gratuitamente, su supporto digitale durevole, una copia completa del Contratto, composta dal Foglio Informativo, che costituisce il frontespizio del Contratto, dal presente Modulo di Adesione, dalle Condizioni Generali di Contratto e dal Documento di Sintesi, comprensive della "Informativa rilasciata ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 (Regolamento generale sulla protezione dei dati);
- accetto integralmente le Condizioni Generali di Contratto e le condizioni economiche riportate nel Documento di Sintesi, che costituiscono parte integrante del Contratto;
- confermo espressamente la volontà di voler utilizzare i servizi di pagamento resi disponibili dalla Banca anche mediante la rete internet, autorizzandola al riguardo ad eseguire le operazioni da me disposte;
- confermo le informazioni fornite nel profilo personale riportato in calce al presente modulo. Prendo atto che, in caso di operazioni effettuate per conto di terzi, dovrò fornire tutte le indicazioni necessarie all'identificazione del titolare effettivo dell'operazione, come definito nell'informativa acclusa al menzionato profilo personale;
- prendo atto che in base alle informazioni fornite sono stato classificato quale Consumatore;
- sono consapevole che nei contratti stipulati a distanza il consumatore ha diritto di recedere, senza penali e senza dover indicare il motivo, nel termine di 14 (quattordici) giorni dalla data di conclusione del Contratto, inviando lettera raccomandata con ricevuta di ritorno a imprebanca S.p.A., Via Cola di Rienzo n. 240 – 00192, Roma;
- prendo atto che il Contratto si intenderà concluso solo al momento della ricezione della comunicazione della Banca di accettazione della presente proposta di apertura e che ai fini della conclusione del contratto è necessario:
  1. sottoscrivere il Contratto (in forma digitale) in segno di accettazione delle presenti condizioni generali e delle condizioni economiche riportate nel Documento di Sintesi;
  2. inviare alla Banca il Contratto sottoscritto e l'ulteriore documentazione richiesta ai fini dell'adempimento degli obblighi di adeguata verifica ai sensi della normativa antiriciclaggio.
- dichiaro di voler ricevere tutte le comunicazioni periodiche di cui al servizio solo in modalità telematica.

Sono consapevole che, in qualunque momento, potrò richiedere alla Banca di modificare la forma di comunicazione prescelta.

Firma Titolare

Data: 06/11/2025

Firma

Data: 06/11/2025

Firma

Dichiaro di approvare specificatamente anche ai sensi e per gli effetti di cui all'art. 1341 secondo comma cod. civ. le seguenti condizioni:

NORME CHE REGOLANO I CONTI DI CORRISPONDENZA E SERVIZI CONNESSI

SEZIONE I: CONDIZIONI GENERALI

Artt. 4 (Esecuzione incarichi conferiti dal cliente); **6** (Cointestazione del rapporto); **7** (Deposito firme autorizzate e poteri di rappresentanza); **8** (Elezione di domicilio e comunicazioni al Cliente); **10** (Garanzia e compensazione); **12** (Durata e Recesso); **13** (Modifica unilaterale delle norme e delle condizioni contrattuali).

SEZIONE II: CONDIZIONI RELATIVE AL CONTRATTO DI CONTO CORRENTE E AI SERVIZI CONNESSI
Artt. 20 (Accrediti sul conto); **22** (Chiusura contabile del conto corrente); **23** (Commissione di Istruttoria Veloce "CIV"); **24** (Sconfinamento); **27** (Invio ed approvazione delle comunicazioni periodiche); **31** (Cointestazioni).

SEZIONE III CONDIZIONI RELATIVE Al SERVIZI DI INCASSO E PAGAMENTO
Artt. 44 (Rifiuto della Banca a eseguire un ordine di pagamento); **48** (Responsabilità della Banca per mancata, inesatta o tardiva esecuzione di operazioni di pagamento); **46** (Operazioni di pagamento non autorizzate e non correttamente eseguite); **47** (Rimborso per operazioni di pagamento non autorizzate); **48** (Responsabilità della Banca per mancata, inesatta o tardiva esecuzione di operazioni di pagamento); **49** (Comunicazioni).

SEZIONE IV BONIFICI e SERVIZIO DI VERIFICA DEL BENEFICIARIO (VOP)
Artt. 54 (Accredito); **55** (Informazioni necessarie per l'esecuzione di un ordine di bonifico); **58** (Revoca del consenso all'esecuzione di un ordine di bonifico); **62** (Tasso cambio di riferimento).

SEZIONE V ADDEBITI DIRETTI IN CONTO CORRENTE
SOTTOSEZIONE A - Addebito Diretto SEPA (SDD)
Artt. 64 (Norme regolanti il servizio); **65** (Informazioni necessarie per l'esecuzione del servizio di addebito diretto Sepa (SDD)).

SEZIONE VI ALTRI PAGAMENTI
SOTTOSEZIONE A - Ricevute Bancarie (RiBa)
Artt. 71 (Norme regolanti il servizio); **72** (Informazioni necessarie per l'esecuzione); **74** (Revoca del consenso all'esecuzione dell'operazione).
SOTTOSEZIONE B - PAGAMENTO MAV - CBILL- RAV -RICARICHE TELEFONICHE – PAGAMENTI DI TASSE O TRIBUTI SU COMPILAZIONE MODULO F24 – BOLLETTINO POSTALE
Artt. 78 (Descrizione del servizio); **79** (Informazioni a supporto dell'esecuzione); **81** (Revoca del consenso).

NORME CHE REGOLANO IL SERVIZIO DI INTERNET BANKING

Artt. 87 (Disfunzioni del servizio); **88** (Sospensione del servizio); **89** (Durata del contratto e recesso); **90** (Strumenti di sicurezza); **91** (Cautele nell'utilizzo dei Servizi); **106** (Operatività tramite funzionalità di tipo informativo e dispositivo attraverso il Servizio Banking); 107 (Banca via internet).

NORME CHE REGOLANO IL SERVIZIO DI DEPOSITO VINCOLATO IN CONTO CORRENTE

Artt. 116 (Ammontare e durata del deposito vincolato); **119** (Estinzione Anticipata); **121** (Condizioni economiche).

Firma Titolare

Data: 06/11/2025

Firma

Data: 06/11/2025

Firma

CONSEGNA COPIA DEL CONTRATTO

Dichiaro di aver ricevuto copia di questo Modulo di Apertura, delle Condizioni Generali di Contratto, unitamente al Foglio Informativo frontespizio del Contratto, del Documento di Sintesi contenente le condizioni economiche che ho letto e che accetto integralmente.

Firma Titolare

Data: 06/11/2025

Firma

Data: 06/11/2025

Firma

MODULO STANDARD PER LE INFORMAZIONI DA FORNIRE AI DEPOSITANTI

Informazioni di base sulla protezione dei depositanti

I Suoi depositi presso imprebanca Spa sono protetti da	Fondo Interbancario di Tutela dei Depositi (FITD) Il FITD è un consorzio di diritto privato tra banche, ufficialmente riconosciuto dalla Banca d'Italia come sistema di garanzia dei depositi. L'adesione delle banche ai sistemi di garanzia dei depositi è obbligatoria per legge.
Limite di protezione	100.000 euro per depositante e per banca. In taluni casi, la legge prevede una tutela rafforzata per esigenze sociali (1)
Se possiede più depositi presso la stessa banca	Tutti i depositi presso la stessa banca sono cumulati e il totale è soggetto al limite di 100.000 euro. Laddove la banca operi sotto diversi marchi di impresa, tutti i depositi presso uno o più di tali marchi sono cumulati e coperti complessivamente fino a 100.000 euro per depositante.
Se possiede un conto cointestato con un'altra persona / altre persone	Il limite di 100.000 euro si applica a ciascun depositante separatamente
Tempi di rimborso in caso di liquidazione coatta amministrativa della banca	7 gg lavorativi a decorrere dalla data in cui si producono gli effetti del provvedimento di liquidazione coatta amministrativa della banca. Il diritto al rimborso si estingue decorsi 5 anni dalla data in cui si producono gli effetti del provvedimento di liquidazione coatta amministrativa della banca (2).
Valuta del rimborso	Euro o la valuta dello Stato in cui risiede il titolare del deposito
Contatti del sistema di garanzia dei depositanti	Fondo Interbancario di Tutela dei Depositi Via del Plebiscito, 102 - 00186 Roma www.fitd.it infofitd@fitd.it
Per maggiori informazioni	www.fitd.it

(1) Cfr. art. 96-bis.1, comma 4 del decreto legislativo n. 385/93 (Testo Unico delle leggi in materia bancaria e creditizia - TUB), come integrato dal decreto legislativo n. 30/2016.
(2) La decadenza è impedita dalla proposizione della domanda giudiziale, salvo che il processo si estingua, o dal riconoscimento del diritto da parte del sistema di garanzia (art. 96-bis.2, comma 4 del TUB, come integrato dal decreto legislativo n. 30/2016).

Dichiaro di aver ricevuto copia di questo Modulo standard per le informazioni da fornire ai depositanti:

Firma Titolare

Data: **06/11/2025**

Firma

Data: **06/11/2025**

Firma

Questionario per l'adeguata verifica della clientela ai sensi della Normativa Antiriciclaggio

Gentile Cliente,
I dati personali da riportare nel presente modulo sono raccolti per adempiere ad obblighi di legge (D.Lgs. n. 231/2007) in materia di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo. Il conferimento dei dati è, pertanto, obbligatorio. Il rifiuto di fornire le informazioni richieste può comportare l'impossibilità di attivare il rapporto o, in caso di rapporti continuativi già in essere, la loro chiusura. Il trattamento dei dati sarà svolto per le predette finalità anche con strumenti elettronici e solo da personale autorizzato in modo da garantire gli obblighi di sicurezza e la loro riservatezza. I dati saranno conservati per il periodo di tempo strettamente necessario al raggiungimento delle finalità sopra esposte e, in ogni caso, non oltre 10 anni dalla cessazione del rapporto. I dati non saranno diffusi, ma potranno essere comunicati ad Autorità e Organi di Vigilanza e Controllo. Potrà esercitare i Diritti a Lei riconosciuti, ai sensi degli artt. da 15 a 22 del Regolamento (UE) 2016/679, rivolgendosi al Titolare del trattamento: imprebanca S.p.A. Via Cola di Rienzo, 240 – 00192 Roma.
Ai fini della completezza delle informazioni di seguito riportate, anche relativamente alle sanzioni penali previste dal D.Lgs. 231/2007, La invitiamo a prendere visione delle informazioni rese in calce al presente modulo.

Dati Personali Titolare

Nome e Cognome:	Luogo e data di nascita:	
Codice fiscale:	Cittadinanza:	
Sesso:	Stato civile:	
Indirizzo di residenza:		
Tipo documento:	Numero documento:	
Rilasciato da:	Data emissione:	Data scadenza:
Tipologia professione:	Dettaglio professione:	
Attività economica:	Provincia attività:	
Finalità del rapporto:		
Provenienza denaro:		
Utilizzo del rapporto:		

Il sottoscritto, consapevole delle responsabilità penali derivanti da mendaci affermazioni in tal sede, dichiara di aver preso visione dell'informativa sugli obblighi di cui al D.Lgs. 231 del 21 novembre 2007 parte integrante del presente questionario, di aver fornito nel presente modulo tutte le informazioni necessarie ed aggiornate di cui è a conoscenza, garantisce che le stesse sono esatte, veritiere e aggiornate e si impegna a comunicarne ogni futura ed eventuale modifica.

Firma Titolare

Data: 06/11/2025

Firma

Data: 06/11/2025

Firma

Nota in tema di Normativa Antiriciclaggio

Obblighi del cliente

Art. 22 del D.Lgs. 231/2007

I clienti forniscono, sotto la propria responsabilità, tutte le informazioni necessarie e aggiornate per consentire ai soggetti destinatari del presente decreto di adempiere agli obblighi di adeguata verifica della clientela. Le imprese dotate di personalità giuridica e le persone giuridiche private ottengono e conservano, per un periodo non inferiore a cinque anni, informazioni adeguate, accurate e aggiornate sulla propria titolarità effettiva e le forniscono ai soggetti obbligati, in occasione degli adempimenti strumentali all'adeguata verifica della clientela.

Obbligo di astensione

Art. 42, comma 1 e 2 del D.Lgs. 231/2007

1. I soggetti obbligati che si trovano nell'impossibilità oggettiva di effettuare l'adeguata verifica della clientela, ai sensi delle disposizioni di cui all'articolo 19, comma 1, lettere a), b) e c), si astengono dall'instaurare, eseguire ovvero proseguire il rapporto, la prestazione professionale e le operazioni e valutano se effettuare una segnalazione di operazione sospetta alla UIF a norma dell'articolo 35.

2. I soggetti obbligati si astengono dall'instaurare il rapporto continuativo, eseguire operazioni o prestazioni professionali e pongono fine al rapporto continuativo o alla prestazione professionale già in essere di cui siano, direttamente o indirettamente, parte società fiduciarie, trust, società anonime o controllate attraverso azioni al portatore aventi sede in Paesi terzi ad alto rischio. Tali misure si applicano anche nei confronti delle ulteriori entità giuridiche, altrimenti denominate, aventi sede nei suddetti Paesi, di cui non è possibile identificare il titolare effettivo ne' verificarne l'identità.

Sanzioni penali

Art. 55, comma 1 e 3 del D.Lgs. 231/2007

1. Chiunque, essendo tenuto all'osservanza degli obblighi di adeguata verifica ai sensi del presente decreto, falsifica i dati e le informazioni relative al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione è punito con la reclusione da sei mesi a tre anni e con la multa da 10.000 euro a 30.000 euro. Alla medesima pena soggiace chiunque essendo tenuto all'osservanza degli obblighi di adeguata verifica ai sensi del presente decreto, in occasione dell'adempimento dei predetti obblighi, utilizza dati e informazioni falsi relativi al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione.

3. Salvo che il fatto costituisca più grave reato, chiunque essendo obbligato, ai sensi del presente decreto, a fornire i dati e le informazioni necessarie ai fini dell'adeguata verifica della clientela, fornisce dati falsi o informazioni non veritiere, è punito con la reclusione da sei mesi a tre anni e con la multa da 10.000 euro a 30.000 euro.

Titolare effettivo

Ai sensi dell'art. 1, comma 2, lettera pp), del D.Lgs. 21 novembre 2007, n. 231, si definisce "titolare effettivo" «la persona fisica o le persone fisiche, diverse dal cliente, nell'interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è istaurato, la prestazione professionale è resa o l'operazione è eseguita».

Persone politicamente esposte

Ai sensi dell'art.1, comma, 2, lettera dd), del D.Lgs. 21 novembre 2007, n. 231 sono "persone politicamente esposte" «le persone fisiche che occupano o hanno cessato di occupare da meno di un anno importanti cariche pubbliche, nonché i loro familiari e coloro che con i predetti soggetti intrattengono notoriamente stretti legami, come di seguito elencate:

1) sono persone fisiche che occupano o hanno occupato importanti cariche pubbliche coloro che ricoprono o hanno ricoperto la carica di:

1.1 Presidente della Repubblica, Presidente del Consiglio, Ministro, Vice-Ministro e Sottosegretario, Presidente di Regione, assessore regionale, Sindaco di capoluogo di provincia o città metropolitana, Sindaco di comune con popolazione non inferiore a 15.000 abitanti nonché cariche analoghe in Stati esteri;

1.2 deputato, senatore, parlamentare europeo, consigliere regionale nonché cariche analoghe in Stati esteri;

1.3 membro degli organi direttivi centrali di partiti politici;

1.4 giudice della Corte Costituzionale, magistrato della Corte di Cassazione o della Corte dei conti, consigliere di Stato e altri componenti del Consiglio di Giustizia Amministrativa per la Regione siciliana nonché cariche analoghe in Stati esteri;

1.5 membro degli organi direttivi delle banche centrali e delle autorità indipendenti;

1.6 ambasciatore, incaricato d'affari ovvero cariche equivalenti in Stati esteri, ufficiale di grado apicale delle forze armate ovvero cariche analoghe in Stati esteri;

1.7 componente degli organi di amministrazione, direzione o controllo delle imprese controllate, anche indirettamente, dallo Stato italiano o da uno Stato estero ovvero partecipate, in misura prevalente o totalitaria, dalle Regioni, da comuni capoluoghi di provincia e città metropolitane e da comuni con popolazione complessivamente non inferiore a 15.000 abitanti;

1.8 direttore generale di ASL e di azienda ospedaliera, di azienda ospedaliera universitaria e degli altri enti del servizio

sanitario nazionale;
1.9 direttore, vicedirettore e membro dell'organo di gestione o soggetto svolgenti funzioni equivalenti in organizzazioni internazionali;
2) sono familiari di persone politicamente esposte: i genitori, il coniuge o la persona legata in unione civile o convivenza di fatto o istituti assimilabili alla persona politicamente esposta, i figli e i loro coniugi nonché le persone legate ai figli in unione civile o convivenza di fatto o istituti assimilabili;
3) sono soggetti con i quali le persone politicamente esposte intrattengono notoriamente stretti legami:
3.1 le persone fisiche che, ai sensi del presente decreto, detengono, congiuntamente alla persona politicamente esposta, la titolarità effettiva di enti giuridici, trust e istituti giuridici affini ovvero che intrattengono con la persona politicamente esposta stretti rapporti d'affari;
3.2 le persone fisiche che detengono solo formalmente il controllo totalitario di un'entità notoriamente costituita, di fatto, nell'interesse e a beneficio di una persona politicamente esposta.»

Autocertificazione ai sensi del Foreign Account Tax Compliance Act ("FATCA") e del Common Reporting Standard OCSE ("CRS")

Dati Anagrafici del Titolare

Nome e Cognome:

Luogo e data di nascita:

Codice fiscale:

Cittadinanza:

Il sottoscritto dichiara:

a) di essere fiscalmente residente in Italia;

b) di non essere in possesso della cittadinanza degli Stati Uniti d'America o di altro Paese diverso dall'Italia;

c) di non avere la residenza fiscale negli Stati Uniti d'America o in altro Paese diverso dall'Italia.

Il sottoscritto si impegna a notificare ogni eventuale modifica delle informazioni sopra riportate entro il termine di 30 giorni dal verificarsi dell'evento. Inoltre, il sottoscritto dichiara di aver letto, compreso ed accettato quanto contenuto nella "Nota in tema di Normativa FATCA e Normativa AEOI/CRS" allegata alla presente autocertificazione.

Firma Titolare

Data: 06/11/2025

Firma

Data: 06/11/2025

Firma

Nota in tema di Normativa FATCA e Normativa AEOI/CRS

In data 8 luglio 2015 è entrata in vigore la Legge n. 95 del 18 giugno 2015, che disciplina gli adempimenti ai quali le Istituzioni Finanziarie italiane devono far fronte ai fini degli scambi automatici di informazioni derivanti dagli accordi internazionali con gli Stati Uniti e con altri Stati esteri (CRS - Common Reporting and Due Diligence Standard) in merito alla normativa FATCA (Foreign Account Tax Compliance Act) e alla normativa AEOI (Automatic Exchange Of Information). Ai sensi di tale Legge, le Istituzioni Finanziarie sono obbligate ad acquisire le informazioni relative ai conti finanziari aperti in Italia da tutti i soggetti (persone fisiche/entità) ovunque fiscalmente residenti.

Obblighi FATCA

L'acronimo FATCA individua una normativa statunitense, volta a contrastare l'evasione fiscale di contribuenti statunitensi all'estero, normativa questa in vigore dal 1° luglio 2014, i cui principi applicativi sono dettagliati all'interno del decreto del Ministero dell'Economia e delle Finanze del 6 agosto del 2015.
Le Istituzioni Finanziarie devono trasmettere su base annuale all'Agenzia delle Entrate, che a sua volta provvede ad inviare all'amministrazione fiscale statunitense (IRS – Internal Revenue Service), le seguenti informazioni relative a tale clientela: i dati identificativi dei titolari dei rapporti, i saldi dei rapporti stessi, le relative rendite finanziarie e, in futuro, gli interessi lordi derivanti dalla vendita di titoli. Le comunicazioni all'IRS da parte dell'Agenzia delle Entrate dei suddetti dati saranno effettuate su base annuale.

Obblighi AEOI

L'acronimo AEOI individua una normativa basata su accordi multilaterali tra i Paesi partecipanti, che ha lo scopo di combattere l'evasione fiscale internazionale ed impone alle Istituzioni Finanziarie di identificare i titolari di conti finanziari e stabilire se sono residenti fiscalmente in un'altra giurisdizione AEOI. L'entrata in vigore di AEOI decorre a partire dal 1 gennaio 2016, dalla cui data diviene obbligatoria l'acquisizione da parte delle Istituzioni Finanziarie delle informazioni ai fini dell'adeguata verifica fiscale per l'apertura di conti finanziari da parte di soggetti residenti in Stati diversi dall'Italia e dagli Stati Uniti d'America. Le disposizioni attuative della suddetta normativa sono contenute all'interno del decreto del Ministero dell'Economia e delle Finanze del 28 dicembre del 2015.
Le Istituzioni Finanziarie devono trasmettere su base annuale all'Agenzia delle Entrate, che a sua volta provvede ad inviare all'amministrazione fiscale dei Paesi partecipanti ad AEOI, le seguenti informazioni relative a tale clientela: i dati identificativi dei titolari dei conti finanziari e le dichiarazioni relative alla residenza fiscale, il saldo contabile, i ricavi e i proventi lordi nel caso in cui un cliente sia fiscalmente residente in uno degli Stati partecipanti all'accordo AEOI.

La Banca è tenuta pertanto a svolgere l'identificazione della clientela ai fini FATCA e AEOI e, per i clienti identificati come reportable, ad effettuare le sopra menzionate segnalazioni all'Agenzia delle Entrate.
Al cliente viene quindi richiesto di sottoscrivere un modulo di autocertificazione in cui, sotto la propria ed esclusiva responsabilità, dichiari il proprio status FATCA/CRS e l'impegno a comunicare tempestivamente ogni variazione dei dati. Il cliente, inoltre, si impegna a fornire opportuna documentazione giustificativa qualora lo status dichiarato si discosti dagli elementi a disposizione della Banca; in tale ipotesi il cliente dovrà fornire documenti che provino lo status dichiarato nell'autocertificazione. Inoltre, il cliente prende atto che la Banca potrà trasferire i suoi dati a fornitori terzi di servizi con lo scopo di effettuare l'identificazione della clientela.
Tutti i clienti che non forniscano i dati necessari all'identificazione e la relativa documentazione non potranno procedere con l'apertura di nuovi rapporti presso la Banca.

Consenso ai sensi del Regolamento Europeo, per la protezione dei dati, 679/2016

Dati Anagrafici del Titolare

Nome e Cognome:	Luogo e data di nascita:
Codice fiscale:	Cittadinanza:

Preso atto dell'informativa allegata resami ai sensi dell'art. 13 e 14 del Regolamento (UE) 2016/679, con la sottoscrizione del presente modulo dichiaro di esprimere in consenso al trattamento dei dati come segue:

Profilazione (paragrafo 3.3)

☐ Presto il consenso ☐ Nego il Consenso

Decisioni automatizzate (paragrafo 3.4)

☐ Presto il consenso ☐ Nego il Consenso

Marketing (paragrafo 3.5)

☐ Presto il consenso ☐ Nego il Consenso

Attività di Marketing per prodotti di terzi (paragrafo 3.6)

☐ Presto il consenso ☐ Nego il Consenso

Cessione di dati personali a terzi (paragrafo 3.7)

☐ Presto il consenso ☐ Nego il Consenso

Controllo della qualità dei servizi (paragrafo 3.8)

☐ Presto il consenso ☐ Nego il Consenso

Trattamento di categorie particolari di dati personali ("dati sensibili") (paragrafo 3.9)

☐ Presto il consenso ☐ Nego il Consenso

Firma Titolare

Data: 06/11/2025

Firma

Data: 06/11/2025

Firma

INFORMATIVA ANTITRUFFA

Le truffe online attualmente utilizzate per sottrarre i dati riservati in modo fraudolento possono essere ad esempio il **phishing**, lo **smishing** e il **vishing** ossia dei tentativi, da parte dei truffatori, per sottrarti informazioni personali, finanziarie o di sicurezza rispettivamente tramite mail, sms e telefonate contraffatte.
Il cosiddetto "phishing", ad esempio, consiste nell'invio di e-mail, solo in apparenza provenienti dal proprio istituto bancario (del quale è riprodotta fedelmente anche l'impostazione grafica), in cui si richiede al destinatario di fornire informazioni riservate. Spesso queste richieste sono motivate con ragioni di natura tecnica, falsi problemi di sicurezza o con l'attrattiva di ricevere premi e partecipare a concorsi.
Tuttavia, se presti attenzione e sai dove guardare, sarai in grado di smascherare i truffatori con facilità. Ecco qualche consiglio:

- **Diffida di chi ti chiede di installare nuove applicazioni, potrebbero essere usate per ottenere il controllo del tuo dispositivo**: la tua Banca non chiederà mai di installare nuove applicazioni, di terze parti o aggiornamenti in generale sui tuoi devices. Quella scelta spetta a te e solo a te.
- **Attento all'indirizzo del mittente nelle comunicazioni che ricevi**: Se è un indirizzo che non conosci, magari contenente dei nomi molto lunghi o caratteri insoliti, meglio diffidare.
- **La grammatica non è un'opinione**: Se visualizzi nel messaggio errori di grammatica, di traduzione o formattazione, non prendere in considerazione la comunicazione.
- **Pensaci due volte prima di cliccare i link presenti all'interno di e-mail e sms**: all'interno della mail o dell'sms possono esser presenti dei link che ti indirizzano verso siti, anche del tutto identici al portale dell'istituto, ma gestiti dagli autori della truffa, per richiederti l'inserimento delle tue credenziali bancarie.

Le possibili informazioni utilizzabili in modo illecito ed a danno del cliente possono essere:

- codici di accesso (username e password), che consentono ai truffatori di accedere ai servizi online del cliente e di operare in sua vece;
- dati relativi alle carte di credito, utilizzabili per acquisti all'insaputa e a spese del cliente;
- dati personali in genere.

Ricorda che imprebanca non ti chiederà mai di fornire le suddette informazioni e soprattutto le tue credenziali attraverso un'e-mail, un sms o una telefonata. Non rispondere mai a richieste di informazioni via e-mail sulle tue carte, sui tuoi conti o sui tuoi codici d'accesso all'Area Clienti.

Per quanto concerne i propri servizi online, la BANCA suggerisce di:

1. **Custodire con cura i propri dati di accesso**, non salvandoli sul proprio computer, mantenendo separati username e password, e modificando periodicamente quest'ultima.
2. **Non fornire MAI le proprie password ad alcuno**. Si precisa che nessun dipendente della banca è autorizzato a richiederle, pertanto la banca non le invierà mai qualsiasi richiesta in tal senso, sia essa effettuata di persona oppure tramite telefono, posta, e-mail o altro mezzo.
3. **Accedere sempre ai servizi online digitando** https://www.banking4you.it/apps/pib2/03403brand10/public/login evitando di "cliccare" su eventuali collegamenti presenti nelle e-mail e di dare adito ad eventuali richieste in esse contenute.
4. **Assicurarsi che la pagina web in cui si inseriscono dati personali sia protetta**, diffidando dei "pop-up". Per verificare che la pagina web sia protetta, controllare che l'indirizzo sia preceduto da "https" e che sul browser sia presente l'icona che attesta il collegamento ad un sito protetto, solitamente posizionata in basso a destra e raffigurante un lucchetto chiuso.
5. **Controllare regolarmente gli estratti conto dei propri conti e depositi**, per assicurarsi che le transazioni riportate siano quelle realmente effettuate.
6. **Installare e mantenere costantemente aggiornato il software dedicato alla sicurezza**, in particolare: Sistema Operativo, Personal Firewall, Antivirus ed Anti-spyware.
7. **Contattare immediatamente l'Help Desk nei seguenti casi**:
   - sono stati forniti a terzi i propri codici di accesso;
   - si sono ricevute e-mail "sospette";
   - si notano transazioni sospette ed inattese nell'estratto conto;

8. Durante la navigazione in internet, **installa solo programmi di cui puoi verificare la provenienza**.
9. **Fai attenzione a eventuali peggioramenti delle prestazioni generali** (rallentamenti, apertura di finestre non richieste, ecc.) o qualsiasi modifica improvvisa delle impostazioni di sistema, che possono indicare infezioni sospette.

INTERNET BANKING - GUIDA ALL'USO E SERVIZI ANTIFRODE

Accesso all'applicativo di Internet Banking

L'accesso ai servizi Internet Banking di ibonline è fruibile attraverso la pagina iniziale del sito web **http://www.ibonline.it/**, sezione "Accedi ad ib-online", oppure digitando direttamente **https://www.banking4you.it/apps/pib2/03403brand0/public/login**. Nella pagina successiva verranno richiesti i dati di autenticazione, costituiti dall'identificativo utente (user ID), indicato nella copia del contratto rilasciata dalla nostra filiale, e la Password personale, che per il primo collegamento è costituita dal Codice PIN, ricevuto dal cliente sul proprio numero di cellulare certificato, in fase di vendita dell'internet banking e che successivamente andrà modificata.

La sicurezza del servizio è garantita da un sistema di crittografia (protocollo SSL) che assicura la totale riservatezza dei dati scambiati tra il cliente e la banca.

Primo collegamento da internet banking o app ib-online

Per il primo collegamento, nella pagina di accesso dell'internet banking deve essere inserito il codice identificativo indicato sul contratto, e la password costituita dal Codice PIN ricevuto via sms.
L'applicazione mobile di ibonline è denominata "ib-online", per accedere alla stessa occorrerà prima procedere al download gratuito dal Play store Android https://play.google.com/store/apps/details?id=it.imprebanca.online.mobile&gl=IT, dall'Apple store https://apps.apple.com/it/app/ib-online/id1536420360o dal Huawey store https://appgallery.huawei.com/#/app/C104353511.
La password assegnata dalla banca è, per motivi di sicurezza, utilizzabile solo all'atto del primo collegamento. Subito dopo l'inserimento, la procedura propone una schermata in cui occorre impostare una nuova password personalizzata scelta dal cliente, come mostrato di seguito:

I campi vanno valorizzati come segue:
Pin: inserire il primo Pin ricevuto via sms
Nuova password: digitare una password personale compresa tra 8 e 20 caratteri;
Conferma nuova password: digitare nuovamente la propria password personale (come sopra).

Dopo aver cliccato sul tasto "cambio password", la procedura confermerà il corretto inserimento e dopo tale operazione l'unica password per accedere al servizio sarà quella personale. La nuova password sarà modificabile in qualsiasi momento utilizzando l'apposita funzione accessibile dal menu utente.

Attivazione servizio di sicurezza tramite APP Token

Il servizio di sicurezza tramite APP installabile su dispositivi mobili (Android, Huawei e IOS) è necessario per consentire le operazioni di tipo informativo e dispositivo (Strong Customer Authentication - SCA - autenticazione forte del cliente).
Per l'attivazione del servizio di sicurezza tramite APP Token occorre aver scaricato l'app ib-mobile.
Occorrerà aprire l'app ib-online, selezionare prima dell'accesso la funzione "Token mobile", tramite l'apposito pulsante posto in home page, per inserire un codice di sicurezza denominato "mPIN" (mobile PIN: chiave di sicurezza di 6 cifre da utilizzare per autorizzare le future operazioni) costituito da caratteri numerici a propria scelta ed infine cliccare su "AVANTI" per proseguire con la conferma dell'operazione.
Verrà poi inviato un SMS al numero registrato sullo smartphone che dovrà esser utilizzato per la conferma e l'attivazione del codice mPin inserito.

Compilazione obbligatoria risposte alle domande di sicurezza al primo accesso

Al primo login, risulterà obbligatorio per l'utente la compilazione delle risposte alle domande di sicurezza.
Tale funzionalità ha lo scopo principale di consolidare la sicurezza per gli utenti. Nel caso in cui il servizio Antifrode della Banca classifichi come "dubbia" una operazione in perimetro, l'utente dovrà dimostrare la sua identità mediante un meccanismo di "autenticazione per step", il quale consiste nel porre all'utente stesso 2 domande delle 6 configurate, per poter procedere con l'operatività il cliente dovrà rispondere correttamente ai due quesiti proposti.
Si specifica che non è prevista la modifica delle risposte di sicurezza fornite in configurazione, pertanto in caso di dimenticanza o di blocco delle domande, l'utente dovrà contattare il seguente indirizzo antifrode@imprebanca.it per chiedere il reset delle domande e al fine di impostare nuovamente le risposte.
Dopo aver effettuato il login, verrà richiesta la compilazione delle risposte relative alla configurazione dell'antifrode e l'utente non potrà accedere a meno che le risposte non vengano compilate e confermate.

Recupero della password

Per ciò che concerne la ri-emissione di codici, in caso di dimenticanza della password, il cliente dovrà procedere tramite la funzione di "recupero password" da internet-banking, al termine della procedura di reset, il PIN sarà spedito via SMS al numero di cellulare depositato. In questo caso l'utente dovrà ripetere la procedura come indicato nelle sezioni precedenti ("Primo collegamento da internet banking o app ib-online" e "Attivazione servizio di sicurezza tramite APP Token").

Procedura identificazione a distanza – Sblocco operatività della clientela

Nel caso in cui la procedura Antifrode per motivi di sicurezza blocchi l'operatività di un cliente, occorrerà eseguire la nuova funzione di identificazione a distanza della clientela disponibile in ambiente internet banking e nell'app Ib-online.
La procedura esporrà il seguente messaggio:

"La dispositiva è stata bloccata dal sistema antifrode. La invitiamo ad accedere tramite app Ib-online al seguente percorso "Profilo -> Sicurezza -> Riconoscimento a distanza" o tramite PC sull'Internet Banking al seguente percorso "Impostazioni -> Riconoscimento a distanza" e completare la procedura di identificazione a distanza. Al termine della procedura potrà inoltrare una e-mail, con oggetto "Richiesta sblocco User ID numero xxx (indicare proprio User ID)", indicando un recapito telefonico al quale poterla eventualmente contattare, a: antifrode@imprebanca.it".
Si specifica che per tali casistiche (blocco antifrode) non è possibile contattare il servizio di help desk internet banking che, laddove chiamato per tale tipologia di assistenza, dirotterà la chiamata verso la succursale di riferimento.

Attivazione notifiche push da app

In un contesto di crescente attenzione e tutela della sicurezza informatica del cliente, nell'app ib-online è possibile attivare e gestire le c.d. "notifiche PUSH", ossia al verificarsi di determinati eventi, il device del cliente su cui è attiva la APP genererà una notifica "push" che avvisa il cliente dell'operazione in essere. Nella sezione Profilo/Impostazioni dell'App Mobile è prevista la funzionalità "Attivazione notifiche push", nella quale l'utente può impostare quali notifiche push desidera ricevere.
La pagina di "attivazione" è suddivisa in più sezioni, entrando nella sezione "Sicurezza", al fine controllare ulteriormente tentativi fraudolenti, possono essere abilitate notifiche molto utili ed importanti circa la login, l'inserimento di credenziali errate o variate o l'avviso sui principali pagamenti. Per le condizioni economiche si rimanda ai fogli informativi e/o al contratto sottoscritto in fase di attivazione del servizio di Internet Banking.

Utilizzo della guida in linea

Il servizio Internet Banking dispone di una guida in linea, che contiene le descrizioni dettagliate e le indicazioni operative per le funzioni disponibili. Alla guida si accede digitando la ricerca desiderata all'interno della barra in alto "Che cosa stai cercando?"

Servizio clienti

Per le richieste di assistenza è possibile contattare il nostro servizio clienti al seguente numero verde:

- dall'Italia 800.28.39.86.
- dall'estero +39 051/4992171.

Il servizio è attivo tutti i giorni dalle 6.00 alle 24.00.
Oltre che mediante il numero verde i clienti possono contattare l'Help Desk anche tramite l'indirizzo e-mail: tecsupport@csebo.it
Le aree di copertura del servizio sono relative a:

- richieste di supporto nell'esecuzione delle varie funzionalità delle applicazioni di Internet Banking;
- sblocco dei tentativi di accesso errati effettuati dai clienti, nella digitazione della password.