INFORMAZIONI SULLA SICUREZZA DEI PAGAMENTI VIA INTERNET (SERVIZIO BPIOL)

Ed. Febbraio 2017

Indice

1. CARATTERISTICHE DEL SERVIZIO

BancoPostaImpresa Online (di seguito anche il “Servizio” o “BPIOL”) è il servizio di Remote Banking che Poste Italiane mette a disposizione delle Imprese, delle Associazioni, della Pubblica Amministrazione Centrale e Locale, delle Ditte individuali e dei Liberi Professionisti per accedere ai servizi finanziari del/i proprio/i conto/i BancoPosta collegandosi direttamente al sito di Poste Italiane www.poste.it.
Il cliente dovrà dotarsi, a propria cura e spese, di un dispositivo (Es. personal computer) in grado di stabilire una connessione Internet sicura tramite l’utilizzo di un antivirus ed un firewall aggiornati. BancoPosta consiglia di non installare software e di non scaricare file di provenienza sconosciuta poiché potrebbero contenere virus (es. Malware, Trojan, ecc.).

La piattaforma telematica, caratterizzata da elevata sicurezza, consente di gestire online (in funzione del profilo scelto dal cliente), comodamente dal proprio ufficio e in tutta sicurezza, incassi e pagamenti e di conoscerne gli esiti, oltre al saldo e ai movimenti dei propri conti, sia per i rapporti accesi in BancoPosta che per quelli accesi presso altri operatori bancari in quanto Poste Italiane ha aderito al Consorzio CBI (Customer to Business Interaction).

Gli elementi necessari per l’accesso al servizio sono i seguenti:
- codice azienda;
- codice utente (per l’Amministratore di Sistema coincide con il codice azienda);
- password.

Per autorizzare le operazioni dispositive, a seconda del profilo scelto, è necessario utilizzare:

- BPIOL Key con relativa Smart Card e certificato di firma digitale nominativo; PIN e PUK del certificato **(Profili Info, Mono e, Multi)**

  Oppure

- Numero del telefono Cellulare abilitato e certificato alla ricezione di Codici OTP (One Time Password) via SMS **(Profilo Easy)**

La validazione delle operazioni, sia singole che massive avviene tramite l’apposizione del codice PIN della Smart CARD o tramite l’inserimento del codice OTP ricevuto tramite SMS sul proprio numero di telefono cellulare certificato. Entrambe le soluzioni garantiscono un elevato standard di sicurezza.

Nel caso in cui le operazioni debbano essere autorizzate da più soggetti congiuntamente, è possibile utilizzare solo la BPIOL key e pertanto tale operatività non è consentita sul profilo EASY.
L’apposizione delle firme multiple può essere gestita in modalità “sincrona” o “asincrona”. Nella modalità asincrona l’apposizione delle firme con il relativo PIN può avvenire in momenti diversi e non è necessario che i vari soggetti autorizzati a disporre sul conto utilizzino nello stesso istante il medesimo dispositivo connesso ad internet. Alcune operazioni (ad es. un Postagiro) potranno essere effettuate solo in modalità sincrona e di conseguenza l’apposizione delle varie firme digitali dovrà necessariamente avvenire nello stesso momento.

2. COME RICHIEDERE L'ATTIVAZIONE DEL SERVIZIO

Per attivare il servizio di Remote Banking:

- Per chi non è titolare di nessun conto corrente BancoPosta, è necessario richiedere l'apertura di un Conto Corrente BancoPosta e l'attivazione del Servizio sottoscrivendo l'apposito documentazione contrattuale messa a disposizione da Poste Italiane.
- Per chi è già titolare di un conto corrente BancoPosta, è necessario richiedere l'attivazione del Servizio sottoscrivendo l'apposita documentazione contrattuale messa a disposizione da Poste Italiane.

I titolare del/dei conto/conti è tenuto ad indicare i soggetti autorizzati ad operare e movimentare il/i conto/i attraverso il Servizio di Remote Banking ed il soggetto incaricato di gestire le attività connesse alla configurazione ed utilizzo del servizio stesso (Amministratore di Sistema). I soggetti autorizzati a disporre sul/sui conto/i devono obbligatoriamente sottoscrivere lo specimen delle firme (Modulo CH7), al momento dell'apertura del Conto Corrente o contestualmente alla richiesta di attivazione del Servizio, oltre che compilare l'apposita sezione della documentazione contrattuale messa a disposizione da Poste Italiane.

Nel caso di richiesta presso l'Ufficio Postale da parte di Liberi Professionisti, Ditte Individuali e Condomini l'attivazione del Servizio di Remote Banking è immediata e le credenziali di accesso vengono comunicate all'Amministratore di Sistema con le seguenti modalità:

- codice azienda ed il codice utente: tramite un'apposita lettera consegnata in Ufficio Postale o trasmessa via e-mail/PEC;
- password di primo accesso: tramite un SMS, inviato al numero di cellulare comunicato contestualmente alla richiesta di attivazione del Servizio.

In caso di richiesta presso l'Ufficio Postale da parte di soggetti non compresi nelle sopra citate categorie, o di richiesta effettuata fuori dai locali commerciali di Poste Italiane, l'attivazione del Servizio non è immediata ed è pertanto differita rispetto al momento di sottoscrizione della richiesta.
In caso di attivazione del Servizio non contestuale al momento della richiesta il codice azienda ed il codice utente sono inviati tramite mail/Pec e la password via SMS. In alcuni casi, se richiesto, tutte le credenziali potranno essere inviate in busta cieca tramite posta ordinaria.

Tramite le credenziali ricevute, l'Amministratore di Sistema può accedere al sito internet messo a disposizione da Poste Italiane e provvedere ad abilitare all'utilizzo del Servizio gli altri soggetti appositamente autorizzati ed indicati dal titolare del/dei conto/i.

3. COME ACCEDERE E CONFIGURARE IL SERVIZIO

Per utilizzare il Servizio l'Amministratore di Sistema deve:
- accedere al sito di Poste: www.poste.it;
- cliccare nella sezione business relativa a "Professionisti e/o PMI" e/o "Imprese e P.A.";
- cliccare su "BancoPostaImpresa Online";
- inserire le credenziali di accesso (codice azienda, codice utente, password).

Dopo aver effettuato il primo accesso, l'Amministratore di Sistema provvede ad effettuare il cambio password ed in seguito, se il profilo attivato prevede l'utilizzo della BPIOL KEY come strumento autorizzativo, deve:

- richiedere il proprio certificato di firma digitale;
- monitorare lo stato della richiesta attraverso l'apposita funzionalità online: quando in stato "spedito", stato che evidenzia l'avvenuta spedizione del Kit BPIOL all'Ufficio Postale, ed una volta ricevuti i codici PIN e PUK, il cliente dovrà recarsi presso l'UP indicato in fase di richiesta online del certificato e ritirare la propria BPIOL Key (il dispositivo token USB con a bordo la Smart Card ed il certificato di firma digitale) e sottoscrivere le condizioni contrattuali relative all'utilizzo della firma digitale;
- accedere al Servizio ed entrare nell'apposita sezione dedicata alla configurazione ed abilitazione dei soggetti autorizzati ad effettuare operazioni informative e dispositive (Utenti Firmatari) ed i soggetti autorizzati ad effettuare operazioni informative ed a predisporre i flussi per le operazioni dispositive senza la possibilità di poterli autorizzare ed inviare (Operatori); generare le credenziali di accesso per ciascun Utente Firmatario e/o Operatore ed abilitarli all'utilizzo del Servizio apponendo la propria firma digitale;
- comunicare le credenziali di accesso a ciascun Utente Firmatario ed Operatore.

Una volta abilitati dall'Amministratore di Sistema, gli Utenti Firmatari e gli Operatori devono cambiare anch'essi la propria password.
Al primo accesso al sistema, anche gli Utenti firmatari possono richiedere a loro volta il proprio certificato di Firma Digitale con le stesse modalità previste per l'Amministratore di Sistema.
L'Amministratore di Sistema per eseguire tutte le operazioni di configurazione ed abilitazione online e gli Utenti Firmatari per eseguire operazioni dispositive a valere sul/sui conto/i devono utilizzare la BPIOL Key, una chiave USB contenente una Smart card dotata di certificato di firma digitale .

La richiesta del Kit BPIOL di firma digitale può essere effettuata esclusivamente online dalla sezione "Funzioni Generali/ Firma Digitale/Richiesta BPIOL Key" ed è consentito l'inserimento di **una sola richiesta per Codice Fiscale**. Il richiedente può monitorare online lo stato della sua richiesta (stato certificato **Richiesto/Inviato/In carico/Emesso/Spedito**).

Se il profilo attivato prevede l'utilizzo di un codice OTP via SMS come sistema autorizzativo, l'Amministratore di Sistema accede al Servizio con le stesse modalità sopra indicate (inserimento cod. azienda, cod. utente e password).
Dopo aver effettuato il primo accesso l'Amministratore di Sistema provvede ad effettuare online il cambio password, la conferma dei dati aziendali e a certificare il proprio numero di telefono comunicato in UP per operare tramite OTP accedendo dalla Sezione Funzioni Generali/Gestione Sicurezza/Certificazione numero cellulare.

Dopo aver confermato il numero è necessario certificarlo tramite l'inserimento di una prima OTP che dovrà avvenire entro 90 secondi dalla ricezione via SMS.

Al termine del processo di certificazione del numero cellulare, l'Amministratore di Sistema è automaticamente abilitato ad utilizzare tutte le funzioni messe a disposizione dal Servizio, compreso autorizzare operazioni dispositive a valere sui conti.

L'Amministratore di Sistema abilita all'utilizzo del Servizio ogni eventuale Utente Firmatario e ne genera le relative credenziali di accesso.

4. COME EFFETTUARE OPERAZIONI DISPOSITIVE E INFORMATIVE

Dopo aver eseguito l'accesso al Servizio come descritto nel paragrafo 3, dalla sezione dedicata ai Servizi Informativi di BPIOL è possibile visualizzare ed eventualmente scaricare sul proprio PC le rendicontazioni giornaliere relative ai saldi e ai movimenti di conti correnti BancoPosta piuttosto che gli esiti delle operazioni dispositive (ad es. gli esiti dei bonifici).

La modalità di autorizzazione di tutte le operazioni dispositive avviene, a seconda del profilo attivato tramite l'apposizione della firma digitale (BPIOL Key) o, in alternativa, mediante l'inserimento di un codice OTP ricevuto via SMS.

4.1. FIRMA TRAMITE BPIOL KEY (PROFILI INFO, MONO E MULTI)

Per procedere con la firma è necessario inserire la BPIOL Key nell'apposita porta USB del PC, al fine di identificare il dispositivo e caricare il certificato di firma digitale.

Per autorizzare la disposizione è necessario inserire il codice PIN ricevuto all'indirizzo indicato nella fase di richiesta del certificato.

L'errato inserimento del codice PIN per 6 volte consecutive genera il blocco della Smart Card.
Lo sblocco è consentito tramite l'apposita funzione della BPIOL Key che richiede l'inserimento del codice PUK (ricevuto unitamente al codice PIN) secondo le modalità indicate nella guida d'uso della BPIOL key presente all'interno della sezione Funzioni generali/istruzioni operative/Manuali online/Manuale BPIOL Key.

Entrambi i codici PIN e PUK sono forniti dalla Certification Authority, non sono modificabili dall'utente e, come la Smart Card, sono da considerarsi strettamente personali.
La modalità di autorizzazione delle operazioni dispositive tramite firma digitale permette l'autenticazione dell'Utente Firmatario, garantisce l'integrità del flusso e la non ripudiabilità dell'operazione.

FIRMA SINGOLA
Dal momento della selezione del flusso di disposizioni, cliccando sul pulsante "Crea Flusso" si visualizza la pagina di apposizione della firma.
Inserendo la BPIOL Key nella porta USB del computer e cliccando sul tasto "Ricarica Dispositivi" è visualizzato e già preselezionato il certificato presente nel dispositivo.

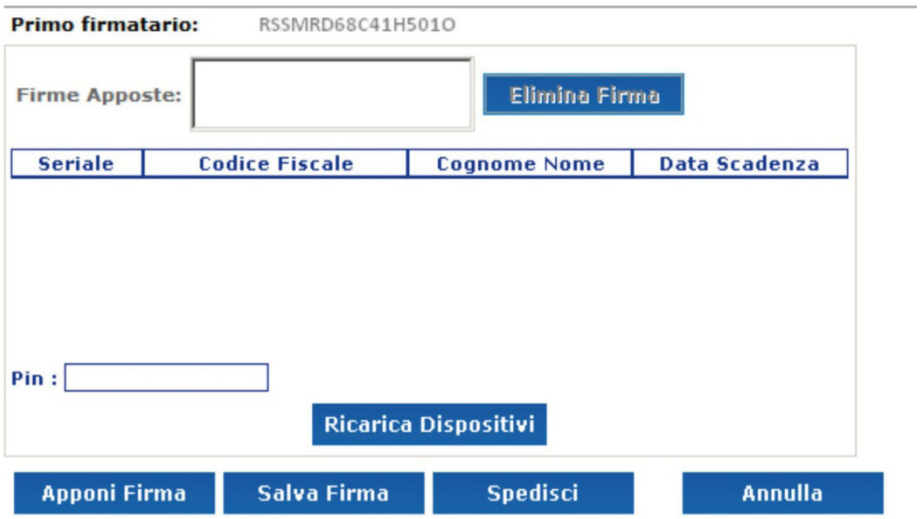
Successivamente è necessario inserire il PIN del certificato di firma digitale selezionato e cliccare sul pulsante “Apponi Firma”, per apporre la firma sul flusso.

Quando nel box Firme Apposte si visualizza il codice fiscale del titolare della firma già apposta, cliccare sul pulsante “Salva Firma” per memorizzare la firma e spedire il flusso successivamente, oppure sul pulsante “Spedisci” per spedire il flusso.

La pagina successiva presenta l’esito dell’operazione ed i link di accesso alle funzioni di verifica della spedizione:

FIRMA CONGIUNTA

In caso di firma congiunta è possibile firmare utilizzando le BPIOL Key dei rispettivi firmatari.
La modalità prevede l’apposizione di una prima firma attraverso uno dei due dispositivi, esattamente come nel caso di firma singola, e cliccando sul pulsante “Salva Firma”.



Il secondo firmatario, nella medesima sessione (obbligatorio per le operazioni in tempo reale, come ad es. postagiro online) o anche accedendo al servizio BPIOL successivamente da altra postazione, visualizza il codice fiscale del primo firmatario e ripete l'operazione di "Ricarica Dispositivi" e "Apponi Firma" per l'apposizione della seconda firma.
Cliccare infine sul pulsante "Spedisci" per spedire il flusso e accedere alla pagina di esito dell'operazione contenente i link per la verifica dell'esito della spedizione.

Solo dopo aver eseguito i passi necessari per autorizzare un'operazione dispositiva, l'operazione si intende eseguita e non più revocabile.
L'utente può visualizzare ed eventualmente scaricare sul proprio computer i dati che riceve dalla Banche con cui opera, tra cui le rendicontazioni giornaliere relative ai saldi e ai movimenti dei suoi conti correnti ordinari, dei rapporti di portafoglio e dei dossier titoli, oltre che l'esito delle operazioni dispositive quali gli esiti dei bonifici, le rendicontazioni delle deleghe 24, ecc.
Le conferme di avvenuta esecuzione delle operazioni dispositive devono essere sempre controllate; è importante verificare che siano state addebitate solo le operazioni effettuate.

4.2. INSERIMENTO OTP (PROFILO EASY)

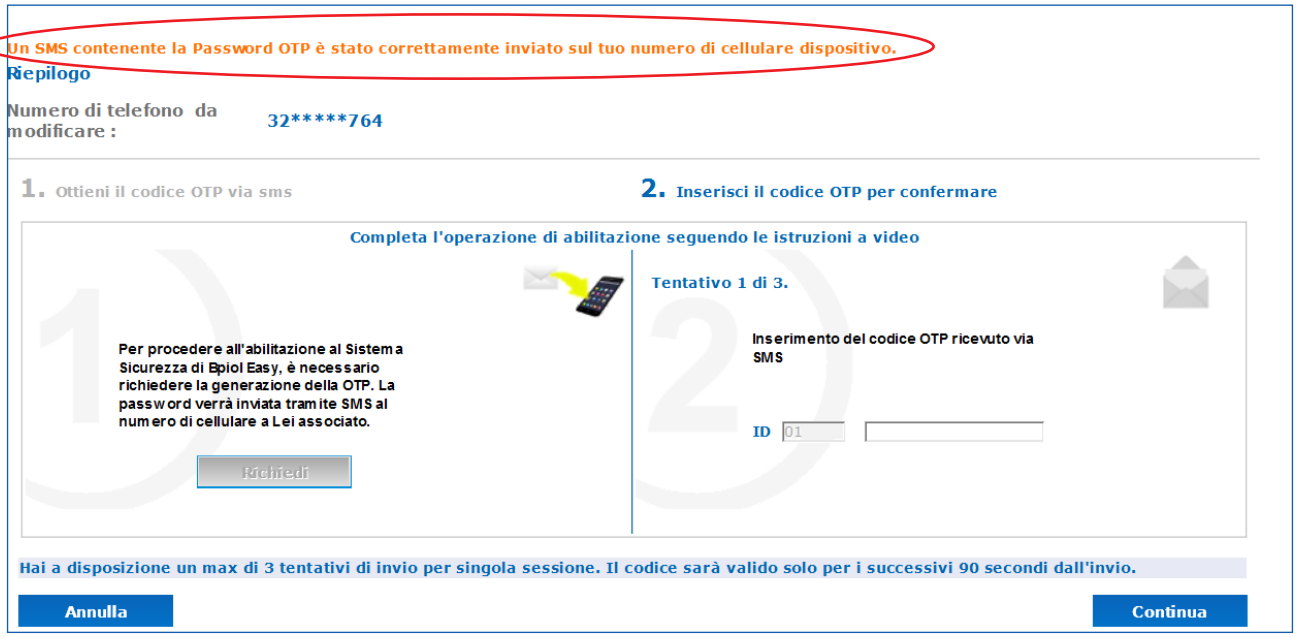
Una volta certificato il numero di cellulare, l'Amministratore di Sistema e gli Utenti Firmatari possono autorizzare le operazioni dispositive tramite l'inserimento di un codice OTP ricevuto via SMS sul proprio numero di cellulare.

Prima di procedere ad autorizzare le operazioni dispositive viene messo a disposizione un riepilogo dell'operazione stessa.

Di seguito un esempio delle le schermate che descrivono la procedura di autorizzazione tramite OTP:

Premendo il pulsante "Annulla", l'utente può scegliere di annullare la disposizione e di tornare alla maschera di compilazione della disposizione.

Premendo il pulsante “Richiedi” verrà inviato un SMS sul numero di cellulare dell’Utente Firmatario certificato contenente la password OTP.



Una volta inserito il codice OTP nel relativo campo, l’Utente Firmatario può procedere scegliendo di premere uno dei due tasti abilitati:
1) “Annulla”, per annullare l’operazione di Firma e tornare alla maschera di compilazione della disposizione;
2) “Continua”, per procedere con l’esecuzione della disposizione.

La transazione termina con la visualizzazione di una maschera riepilogativa dell’operazione svolta e l’invito a verificarne l’esito tramite i link indicati.

5. FURTO O SMARRIMENTO E UTILIZZO NON AUTORIZZATO DELLE CHIAVI DI ACCESSO E UTILIZZO DEL SERVIZIO: PROCEDURE DA SEGUIRE E RESPONSABILITÀ

In caso di smarrimento o furto, nonché di uso non autorizzato o sospetto degli strumenti identificativi (codice azienda, codice utente e password) e operativi (BPIOL Key, PIN e PUK della BPIOL Key) o del numero di cellulare indicato per ricevere i codici OTP, il Cliente è tenuto a comunicare immediatamente l'accaduto a Poste Italiane, con le modalità di seguito indicate non appena ne viene a conoscenza ed altresì a sporgere tempestivamente denuncia alle Autorità competenti.

5.1 USO NON AUTORIZZATO O SOSPETTO (FRODI)

In caso di abuso riscontrato o sospetto (frodi) il cliente deve contattare il numero verde 800.00.33.22 per le opportune azioni di contrasto.

5.2 PASSWORD AMMINISTRATORE DI SISTEMA

Per richiedere una nuova password di Amministratore di Sistema il cliente dovrà contattare il call center al numero verde 800.00.33.22 che dopo aver effettuato il riconoscimento provvederà ad inviare una nuova busta cieca o un nuovo sms a seconda della tipologia di contratto sottoscritto.

5.3 BPIOL KEY (DISPOSITIVO FISICO, PIN E PUK) DISPOSITIVO MOBILE E NUMERO CELLULARE

Se il furto o lo smarrimento, l'uso non autorizzato o sospetto riguarda la BPIOL KEY, il cliente potrà richiedere l'immediata sospensione del relativo certificato di firma digitale dal sito poste.it seguendo la procedura guidata:

Come riportato nella figura sopra, nel caso di dimenticanza oppure furto, smarrimento, nonché uso non autorizzato o sospetto anche dei codici di sospensione il cliente può telefonare al Servizio Clienti BancoPostarisponde al numero gratuito 800.00.33.22.

Inoltre, nell'ambito dell'utilizzo della BPIOL Key il cliente può richiedere, oltre alla Sospensione immediata del certificato, anche la:

- **Sospensione differita** solo per casi non urgenti e non richiesti online; in questo contesto, ha effetto entro due giorni dalla richiesta;
- **Revoca** (ad es. per blocco del codice PUK, *il certificato di firma digitale non può essere riattivato ed il cliente deve richiedere l'emissione di uno nuovo*);
- **Riattivazione** (nel caso si voglia riutilizzare il certificato, che era stato sospeso in modalità immediata o differita, fino alla sua naturale scadenza).

Si ricorda che il certificato di firma digitale della BPIOL Key scade dopo 3 anni dall'attivazione dello stesso, e può essere rinnovato per altri tre anni, purché il rinnovo avvenga prima della scadenza. La procedura di rinnovo deve essere effettuata online e può essere eseguita solo nel periodo compreso tra 60 giorni solari precedenti la scadenza del certificato e la scadenza stessa.

Il rinnovo può essere fatto una sola volta prorogando la validità del certificato di 3 anni. Se il certificato non viene rinnovato entro la prima scadenza oppure trascorsi tre anni dal rinnovo, dovrà essere richiesto un secondo certificato, direttamente da BPIOL, attraverso la procedura disponibile online (FUNZIONI GENERALI/Firma digitale/Richiesta BPIOL Key).

In caso di furto o smarrimento del dispositivo mobile o nel caso di smarrimento, sospetta frode o abuso del numero di cellulare indicato per la ricezione dei codici OTP è necessario richiedere immediatamente il blocco dell'utenza telefonica contattando il Servizio Clienti BancoPostarisponde al numero verde gratuito 800.00.33.22

Il Cliente è responsabile per le operazioni effettuate on line a seguito degli eventi di smarrimento, furto, uso non autorizzato o sospetto degli strumenti identificativi ed operativi fino al momento della comunicazione di tali eventi a Poste Italiane, nel limite di Euro 150,00 (centocinquanta/00), fatti salvi i casi in cui il Cliente abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la protezione e sicurezza degli stessi. In tali casi, il Cliente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di Euro 150,00 (centocinquanta/00). Poste Italiane rimane esonerata da qualsiasi responsabilità per le operazioni disposte anteriormente alla ricezione della comunicazione di smarrimento, furto o uso non autorizzato o sospetto dei codici e degli strumenti operativi quando la comunicazione stessa non sia stata effettuata secondo le modalità e tempistiche indicate nel presente paragrafo e nelle condizioni contrattuali del Servizio.

Successivamente al momento in cui la comunicazione di cui sopra risulti opponibile a Poste Italiane, quest'ultima impedisce qualsiasi utilizzo dei codici e degli strumenti operativi e il Cliente non sopporta le perdite derivanti dalle operazioni di pagamento non autorizzate senza alcun limite di importo, salvo i casi in cui abbia agito in modo fraudolento, con dolo o colpa grave.
Poste Italiane assicura che: (i) i codici e gli strumenti operativi consentono l'utilizzo del Servizio in modo protetto, garantendo elevati standard di sicurezza; (ii) i codici e gli strumenti operativi e i dati relativi alle operazioni eseguite non siano accessibili a soggetti diversi dal Cliente; (iii) il Cliente sia sempre nella condizione di eseguire la comunicazione avente ad oggetto il furto, lo smarrimento, l'uso non autorizzato o sospetto dei codici e degli strumenti operativi.
Poste Italiane tutela costantemente i dati dei suoi clienti attraverso l'adozione dei più moderni sistemi di sicurezza e fornisce tutte le informazioni utili per usufruire in modo sicuro dei servizi di pagamento via Internet. Per ulteriori dettagli è disponibile apposito materiale informativo sul sito Internet https://www.picert.it/.

6. NON FUNZIONAMENTO O DANNEGGIAMENTO DELLA BPIOL KEY

Nel caso di non funzionamento o danneggiamento della BPIOL Key, il Cliente può richiederne la sostituzione presso l'Ufficio Postale di riferimento del Conto. In questi casi il Cliente dovrà compilare l'apposito modulo e riconsegnare il kit di firma digitale in suo possesso e si procederà alla revoca dello stesso a alla richiesta di un nuovo certificato.

7. REGOLE PER LA SICUREZZA

Di seguito, alcune semplici regole da seguire per accedere a BancoPostaImpresa Online con la massima sicurezza.

7.1. PROTEZIONE DEI CODICI E DEGLI STRUMENTI OPERATIVI (PASSWORD, PIN DELLA BPIOL KEY, PUK DELLA BPIOL KEY)

I codici sono strettamente personali e pertanto devono essere custoditi dal Cliente con la massima cura, mai comunicati ad altri adottando misure idonee a garantire la sicurezza e riservatezza.
È preferibile non conservare i codici insieme, né annotarli su unico documento.

Per una maggiore sicurezza si consiglia di modificare periodicamente le Password. Il sistema impone comunque un cambio della password obbligatorio ogni 180 giorni. È consigliato utilizzare una Password con le seguenti caratteristiche:
- lunghezza minima: 12 caratteri per l'Amministratore di Sistema e 8 caratteri per gli Utenti firmatari e gli Operatori Semplici (obbligatorio);

- che contenga almeno una lettera maiuscola, una lettera minuscola, un numero e un carattere speciale (è obbligatorio almeno un carattere speciale);
- che non corrisponda o contenga riferimenti a dati personali (ad es. indirizzo, telefono, codice fiscale, numero della patente, nomi propri, date di nascita, ecc…) o agevolmente riconducibili all'utente;
- che non sia uguale alle password precedenti.

È importante, non utilizzare la stessa Password utilizzata per accedere ad altri siti web.

7.2 RICEZIONE DI E-MAIL SOSPETTE (PHISHING)

L'accesso al servizio BancoPostaImpresa Online deve essere effettuato partendo dall'indirizzo www.poste.it o dall'indirizzo https://bancopostaimpresaonline.poste.it/bpiol1/ nel browser internet, evitando di accedere da link presenti all'interno di email "sospette".
Poste Italiane, direttamente o tramite terzi, non richiede mai ai propri clienti, attraverso messaggi di posta elettronica, telefonate o lettere, di fornire i codici di accesso personali quali il Codice Utente, la Password, il PIN o il PUK.

7.3 INSERIMENTO DEI DATI PERSONALI

Diffidare di improvvisi cambiamenti nella modalità con cui viene chiesto di inserire i codici di accesso a BancoPosta Impresa Online: ad esempio, se questi vengono chiesti non tramite una pagina del sito, ma tramite pop-up (una finestra aggiuntiva di dimensioni ridotte) e in tutti i casi in cui viene richiesto di utilizzare modalità diverse da quelle indicate nelle presenti istruzioni operative.
In questi casi, contattare immediatamente Poste Italiane chiamando il numero gratuito 800.00.33.22 oppure inviando un'e-mail a info@poste.it.

7.4 LOGICA DI ACCESSO AL SITO

L'accesso al sito deve avvenire digitando l'indirizzo www.poste.it o l'indirizzo https://bancopostaimpresaonline.poste.it/bpiol1/ direttamente nel browser Internet.
Poste Italiane è costantemente impegnata a tutelare i dati dei suoi clienti attraverso l'adozione dei più moderni sistemi di sicurezza. Questi sistemi garantiscono comunicazioni affidabili e sicure attraverso l'adozione del protocollo HTTPS.
È quindi importante che durante l'inserimento dei dati riservati nella pagina web, ci si assicuri che si tratti di una pagina protetta. Le pagine protette sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con "https://" e non con "http://".
Inoltre, le pagine protette contengono un lucchetto nella parte in alto a sinistra della barra degli indirizzi del browser.
Cliccando due volte sul lucchetto, è possibile verificare l'esistenza di un "certificato" che garantisce l'autenticità del sito.
È importante controllare a chi (e da chi) è stato rilasciato il certificato; in questo caso, deve risultare che il certificato sia rilasciato a POSTE ITALIANE S.p.A.

7.5 AGGIORNAMENTO DI SOFTWARE PER LA SICUREZZA INFORMATICA

Il sistema operativo e i programmi di protezione del computer (antivirus, antispyware, ecc.) devono essere costantemente aggiornati. Le aziende produttrici dei software rendono periodicamente disponibili online (e scaricabili gratuitamente) aggiornamenti (cosiddette patch) che incrementano la sicurezza del sistema operativo e del browser. Sui siti di queste aziende è anche possibile verificare che il proprio browser sia aggiornato; in caso contrario, è consigliabile scaricare e installare le patch.

7.6 CONTROLLO DELLE OPERAZIONI EFFETTUATE

Gli estratti conto e le conferme di avvenuto pagamento devono essere sempre controllate; è importante verificare che siano state addebitate solo le operazioni effettuate. La data e l'ora dell'ultimo accesso, presenti nella pagina di benvenuto BancoPostaImpresa Online, rappresentano un valido strumento di controllo.