Scheda Informativa Inbank

SICUREZZA DEI PAGAMENTI VIA INTERNET

La presente scheda informativa ha l'obiettivo di illustrare le principali raccomandazioni per un utilizzo sicuro e consapevole del servizio di home banking "Inbank – Servizio Internet Banking" sia via web "Inbank Web" che via App "Inbank App" e della relativa applicazione di sicurezza "Inbank Notify".

Ricordiamo che la Banca sarà sempre a disposizione dei Clienti per approfondimenti e ulteriori informazioni riguardanti questi aspetti; inoltre, sul sito web dedicato al servizio Inbank è presente una sezione dedicata alla sicurezza.

1. Requisiti Tecnologici

COLLEGAMENTO AD INTERNET

Per usufruire del servizio Inbank è necessario disporre di un collegamento alla rete internet messo a disposizione da un fornitore di servizi internet a scelta (ISP - Internet Service Provider). Le spese del collegamento ad Internet sono a carico del Cliente.

DISPOSITIVI (REQUISITI HARDWARE)

Per accedere al servizio Inbank è sufficiente disporre di un dispositivo connesso alla rete internet quale ad esempio un computer o uno smartphone personale. La funzionalità di riconoscimento biometrico richiede uno smartphone che la supporti (es. il lettore di impronte digitali).

REQUISITI SOFTWARE

L'elenco dei sistemi operativi e dei browser supportati per l'utilizzo del servizio Inbank, comprensivo del dettaglio sulle versioni, è disponibile e costantemente aggiornato sul sito del servizio Inbank.

2. Autenticazione forte della Clientela

Per proteggere la Clientela da frodi, accessi e modifiche non autorizzate a tutti i dati di pagamento sensibili identificati, il servizio Inbank dispone di misure tecnologiche per l'autenticazione forte della Clientela nel seguito elencate.

MISURE DI IDENTIFICAZIONE DELL'UTENTE

Per identificare il Cliente sono disponibili differenti modalità di autenticazione per accedere al conto o per autorizzare/ disporre delle operazioni.

Nella fase di accesso al conto al Cliente verrà richiesta la propria combinazione di UserID e password in aggiunta ad un codice OTP (dall'inglese One Time Password, indica un codice numerico casuale monouso generato dagli appositi strumenti di sicurezza forniti al Cliente dalla Banca), la combinazione di questi tre elementi è denominata SCA (Strong Customer Authentication) o autenticazione forte del Cliente. Qualora l'accesso al conto venga effettuato attraverso App, al primo accesso è necessaria la combinazione UserID, password e codice OTP, per gli accessi successivi il codice OTP non è richiesto. In aggiunta, per accedere all'applicazione è possibile impostare un unico PIN applicazione per l'accesso che può essere associato al riconoscimento biometrico dello smartphone.

Per autorizzare/ disporre delle operazioni è necessario aver eseguito l'accesso al conto con le modalità sopra elencate, in aggiunta viene richiesto un ulteriore codice OTP valido per la singola operazione (dynamic linking). In alternativa, è possibile autorizzare/ disporre delle operazioni con il riconoscimento biometrico qualora fosse stato impostato.

La combinazione UserID e password, gli OTP ed eventuali ulteriori PIN impostati sono STRETTAMENTE PERSONALI e come tali non devono essere condivisi con alcun soggetto terzo. La conoscenza esclusiva da parte del Cliente di tali informazioni strettamente personali è infatti un elemento imprescindibile per l'autenticazione forte del Cliente.

Gli strumenti di sicurezza che forniscono i codici OTP sono:

- Token fisici
- OTP Mobile

OTP DA TOKEN FISICO

Il token fisico è un dispositivo strettamente personale dotato di display in grado di generare sia codici OTP che codici per firmare le disposizioni. Il token viene consegnato al Cliente, nello stato di conservazione e nelle condizioni idonee all'uso. Alla cessazione del funzionamento del token il titolare potrà richiedere il rilascio di un nuovo token. Il token viene consegnato dalla Banca al Cliente, il quale deve farne un utilizzo esclusivamente personale. Il Cliente ha l'obbligo di custodire e conservare il token con diligenza, separatamente dagli altri codici identificativi del servizio Inbank, e di servirsene appropriatamente per l'uso cui è destinato astenendosi da qualsiasi modifica/ intervento sullo stesso.

OTP DA MOBILE

Il funzionamento di tale strumento prevede che il Cliente riceva un messaggio SMS sul numero di cellulare fornito al momento della stipula del contratto o una notifica push tramite l'apposita applicazione di sicurezza installata sul proprio telefono cellulare, ogniqualvolta si renda necessario l'inserimento del codice OTP. Il messaggio conterrà:

- Il codice OTP che il Cliente dovrà inserire per autorizzare l'operazione;
- Il riepilogo dei principali dati dell'operazione che si sta eseguendo.

PIN TRADING

Nell'utilizzo del servizio Inbank trading, il Cliente può impostare in autonomia un codice alfanumerico per autorizzare gli ordini di trading.

PIN APPLICAZIONE

Nell'utilizzo del servizio Inbank tramite App, il Cliente può in autonomia sostituire la combinazione UserID, password e OTP con un unico PIN applicazione per accedere all'App, tale PIN può anche essere associato ad un riconoscimento biometrico.

RICONOSCIMENTO BIOMETRICO

Nell'utilizzo del servizio Inbank tramite App, il Cliente impostando il PIN applicazione può associarvi anche un riconoscimento biometrico utilizzabile sia per accedere all'App che per autorizzare/ disporre delle operazioni di pagamento. Inbank App e Inbank Notify non trattano in alcun modo i dati biometrici in quanto ricevono solo una notifica dell'avvenuta verifica o meno del riconoscimento da parte della funzionalità di riconoscimento biometrico dello smartphone.

DYNAMIC LINKING

Il Dynamic Linking è un fattore di sicurezza che collega in modo dinamico ed indissolubile i dati della transazione bancaria che si sta eseguendo con l'OTP che viene generato per autorizzare l'operazione di pagamento (ad esempio, un bonifico). Il Dynamic Linking è quindi strettamente collegato al metodo di SCA utilizzato dal cliente, ed insieme forniscono un rafforzamento della sicurezza dei pagamenti on line.

PROCEDURA DI AUTORIZZAZIONE OPERAZIONI DI PAGAMENTO

Il servizio Inbank prevede le seguenti fasi operative per l'invio alla propria Banca della disposizione di pagamento:

1. Inserimento dati della disposizione;
2. Verifica dei dati della disposizione;
3. Autorizzazione tramite gli strumenti di sicurezza tempo per tempo vigenti;
4. Messaggio di conferma di inoltro della disposizione alla Banca.

3. Misure di sicurezza

Per aumentare il livello di sicurezza delle operazioni effettuate tramite internet, sono applicate e messe a diposizione del Cliente ulteriori misure di sicurezza.

SICUREZZA DELLE COMUNICAZIONI

Per tutti gli scambi di dati di pagamento sensibili via Internet, è garantita la sicurezza dei canali di comunicazione tra le parti coinvolte grazie alla crittografia tra i nostri sistemi e il dispositivo del Cliente per tutta la durata della sessione.

CONTROLLO DI INATTIVITÀ

Nel caso in cui un'utenza connessa rimanga inattiva per un determinato lasso di tempo, il sistema provvede a disconnettere l'utente in modo automatico dopo cinque minuti di inattività.

LIMITI OPERATIVI

Per maggiore sicurezza alcune funzionalità dispositive di pagamento hanno dei limiti predefiniti (es: massimali giornalieri, mensili) impostati dalla Banca. Superato tale limite, il sistema impedisce l'invio di ulteriori disposizioni nello stesso periodo. Il Cliente, qualora lo ritenesse necessario, può richiedere di ridurre o aumentare i massimali di spesa in base alle proprie esigenze.

REQUISITI DI AUTENTICAZIONE

Per aumentare il livello di sicurezza nella fase di login e autenticazione è stato impostato un limite massimo di cinque tentativi falliti, al superamento di tale limite, l'accesso al servizio viene bloccato. Per richiedere lo sblocco è necessario contattare la propria filiale di fiducia.

MESSAGGI ALERT

I messaggi di Alert vengono attivati in fase di censimento del servizio Inbank ed utilizzano due canali di inoltro:

SMS/ Notifica Push: il Cliente riceverà un SMS al numero di cellulare indicato in fase di attivazione del servizio Inbank. In alternativa, qualora il Cliente abbia installato e configurato l'apposita applicazione di sicurezza, si riceverà una notifica push direttamente sul proprio cellulare.

Mail: Il Cliente riceverà una mail all'indirizzo di posta elettronica indicato in fase di attivazione del servizio Inbank.

I messaggi di Alert avvisano il Cliente quando vengono effettuate disposizioni di pagamento (Bonifici SCT Sepa Credit Transfer, Bonifici esteri, etc.).

Tali messaggi sono estremamente IMPORTANTI perché servono a rendere informato il Cliente delle disposizioni effettuate con le sue credenziali anche nel caso non siano state da lui personalmente disposte (in caso di Frode).

Qualora il Cliente lo ritenesse necessario vi è la possibilità di attivare l'invio di messaggi di Alert in occasione di ogni accesso al servizio Inbank con le proprie credenziali.

4. Raccomandazioni per la Sicurezza

Per un utilizzo sicuro e responsabile del servizio di home banking e dei dispositivi personali di seguito sono presenti alcuni comportamenti sicuri da seguire. Per maggiori informazioni è possibile visitare la sezione dedicata alla sicurezza sul sito web dedicato al servizio Inbank.

VERIFICA IL PROTOCOLLO E IL SITO WEB

Il sito web del servizio Inbank è raggiungibile al seguente URL: https://www.inbank.it/. In particolare, la presenza dell'intestazione "https" indica che la navigazione è cifrata e quindi i dati trasmessi non possono essere letti o manipolati da terze parti. Il resto dell'URL deve essere esattamente come riportato in precedenza, la presenza di caratteri, numeri o simboli tra le barre oblique indica una pagina web di internet banking non originale o contraffatta.

Per una maggiore sicurezza si consiglia di digitare l'URL presente sopra direttamente nella barra degli indirizzi del browser utilizzato e di aggiungere il sito web ai preferiti, in tal modo per verificare l'autenticità del sito si avranno a disposizione due elementi visivi: "il lucchetto" che indica una connessione cifrata e "una stellina" che indica il sito preferito.

UTILIZZA I DISPOSITIVI IN SICUREZZA

Per accedere al servizio Inbank in sicurezza si raccomanda di:

- Proteggere il dispositivo mediante PIN, password o biometria;
- Non memorizzare la password di accesso al servizio Inbank nel browser utilizzato;
- Installare solo applicazioni presenti sugli store ufficiali;
- Controllare periodicamente le autorizzazioni concesse alle applicazioni installate;
- Aggiornare regolarmente il dispositivo e le applicazioni installate.

UTILIZZA PASSWORD FORTI

Una password è una delle "chiavi" per accedere al servizio Inbank per questo non deve essere inferiore ad otto caratteri e deve contenere almeno un carattere delle seguenti categorie: lettere maiuscole e minuscole, numeri e caratteri speciali. Inoltre, una password per essere forte, oltre che rispettare i vincoli sopra descritti, deve essere semplice da memorizzare.

CONTROLLA IL CONTO ONLINE

Visualizzare regolarmente i movimenti dei propri rapporti è buona norma per mantenere un controllo costante sulla propria operatività.

AGGIORNA I RECAPITI

Essendo il numero di telefono cellulare e l'indirizzo e-mail del Cliente elementi fondamentali per la gestione della sicurezza è importante tenerli costantemente aggiornati comunicando alla propria filiale di fiducia ogni loro variazione.

UTILIZZA UN ANTIVIRUS O ANTIMALWARE

Verifica che sui dispositivi utilizzati per accedere all'servizio Inbank sia installato e costantemente aggiornato un software antivirus/ anti-malware.

5. Frodi classiche On-line

Una frode può presentarsi con modalità differenti attraverso molteplici canali di comunicazione. Le tecniche di frode evolvono in continuazione, quindi occorre sempre diffidare delle comunicazioni che richiedono dati personali facendo leva sulla buona fede del Cliente. Di seguito le truffe più ricorrenti.

Phishing
Simulando una comunicazione ufficiale il tuffatore invia un'e-mail che presenta un problema da risolvere, un'offerta da non perdere, la disponibilità a essere ricontattati, la richiesta di cliccare su un link o di scaricare e aprire allegati. Spesso il mittente o la pagina di login alla quale l'eventuale link rimanda appaiono molto simili al mittente tipico o alla pagina originale, presentando solo piccole differenze (ad esempio l'aggiunta della richiesta del numero telefonico). Le comunicazioni della tua Banca non avranno mai link a pagine o applicazioni esterne in cui sia richiesto l'inserimento di informazioni riservate.

Vishing
Chiamando e presentandosi come operatore di banca, assistente Inbank o funzionario pubblico (spesso simulando i numeri conosciuti o salvati in rubrica) il truffatore richiederà codici di accesso e/o OTP. Tale chiamata è spesso preceduta da e-mail di phishing o SMS di smishing. Nessun operatore di Banca è autorizzato a richiedere credenziali di accesso e/o OTP.

Smishing
I truffatori inviano SMS presentando un problema da risolvere o un'offerta da non perdere, chiedendo di essere ricontattati o di cliccare su un link, spesso simulando i numeri conosciuti e salvati in rubrica. Le comunicazioni della tua Banca non avranno mai link a pagine o applicazioni esterne in cui sia richiesto l'inserimento di informazioni riservate.

Applicazioni
I truffatori pubblicano applicazioni per smartphone che imitano applicazioni conosciute, o distribuiscono programmi per il computer personale con all'interno malware in grado di esfiltrare UserID e password, di modificare il destinatario delle transazioni disposte o di controllare da remoto il dispositivo.

COME EVITARE UNA TRUFFA

Diffida sempre delle comunicazioni ricevute indipendentemente dalla modalità di ingaggio quali una mail, un SMS, una chiamata, etc. Nel caso si ricevessero comunicazioni come quelle elencate in precedenza e/o inattese e/o differenti dal solito si raccomanda di:

- Non fornire informazioni personali, codici di accesso e/o OTP
- Non cliccare su link presenti in e-mail o SMS, ma digitare l'URL del servizio Inbank https://www.inbank.it/ direttamente nella barra di navigazione del browser
- Non procedere e contatta la tua filiale di fiducia con un numero già in tuo possesso

RICHIEDI ASSISTENZA

In caso di frode, furto o smarrimento del dispositivo mobile contatta la filiale di fiducia per il blocco della postazione. Nel caso non fosse possibile contattare immediatamente la propria filiale, la postazione può essere bloccata in autonomia inserendo intenzionalmente la combinazione UserID e password con quest'ultima intenzionalmente errate almeno cinque volte (cfr. la sezione "Requisiti di autenticazione").

6. Glossario

Lista dei termini più utili per usare correttamente l'Internet Banking.

ANTIVIRUS/ ANTIMALWARE

Programma che, se costantemente aggiornato, riesce a rilevare e bloccare malware e virus presenti su un dispositivo.

FIREWALL

Componente, hardware o software, che filtra il traffico di rete che fluisce tra un dispositivo e la rete internet. Il firewall blocca eventuali dati che non rispettano i parametri di sicurezza al fine di proteggere da intrusioni indesiderate.

CYBER CRIMINALE o HACKER

Esperto informatico (o gruppo di individui organizzato) che mira a violare reti informatiche e dispositivi altrui per sottrarre dati, spesso a scopo di lucro.

MALWARE (Virus, Trojan, Worm, etc.)

Software malevolo usato per arrecare un danno al computer e/o sottrarre informazioni. Possono essere presenti in allegati, dispositivi USB o scaricati attraverso la rete internet, hanno l'abilità di infettare il dispositivo e i sistemi che condividono la stessa rete.

RANSOMWARE

Malware che blocca l'accesso a dati e sistemi tramite cifratura dei file. Una volta compromesso il sistema, compare generalmente un messaggio in cui è richiesto il pagamento di un riscatto in cambio della chiave di decifratura dei file.

PHISHING

Truffa che consiste nell'invio di e-mail, SMS (nel qual caso si parla di «smishing») o chiamate («vishing») fraudolenti che sembrano provenire dalla tua banca o da enti affidabili e che mira a carpire dati riservati (password, PIN, etc.) o altre informazioni personali.

SCA (STRONG CUSTOMER AUTHENTICATION)

Autenticazione forte del cliente che permette di convalidare l'identificazione di un utente utilizzando due o più elementi di autenticazione appartenenti a categorie differenti quali: conoscenza (es. password, PIN), possesso (es. token, smartphone) o inerenza (es. impronta digitale).

SPAM

Messaggi di posta elettronica non verificati o fasulli. Generalmente finiscono nella cartella di posta indesiderata ma è sempre bene prestare attenzione per non incorrere in furti di identità digitale.

INBANK
ED.01/2023