Scheda Informativa

SICUREZZA DEI PAGAMENTI VIA INTERNET

INBANK

Il presente documento ha l'obiettivo di mostrare alcuni dei principali suggerimenti sull'utilizzo sicuro e consapevole del servizio "Inbank – Servizio Internet Banking". Di seguito verranno quindi presentate le informazioni principali legate alla sicurezza del servizio di pagamento via internet.

La Banca sarà sempre a disposizione dei Clienti per approfondimenti e ulteriori informazioni riguardanti questi aspetti; sono inoltre disponibili contenuti aggiornati sulla sicurezza sul sito del servizio Inbank.

1. Requisiti Tecnologici

Collegamento via Internet

Per poter usufruire del servizio Inbank è necessario disporre di un collegamento alla rete internet tramite un ISP - Internet Service Provider a scelta (le spese di collegamento telefonico sono a carico del chiamante).

Dispositivi (requisiti hardware)

Per accedere al servizio Inbank è sufficiente disporre di dispositivi connessi alla rete internet (personale computer, smartphone, ...).

Requisiti Software

Il servizio Inbank è fruibile attraverso l'utilizzo di sistemi operativi e browser supportati il cui elenco, comprensivo del dettaglio sulla versione, è disponibile e costantemente aggiornato sul sito del servizio Inbank. Inoltre per un uso sicuro del servizio Inbank, si suggerisce di dotarsi di un software antivirus, costantemente aggiornato e installato sul dispositivo. Per approfondimenti e consigli per un utilizzo efficace dell'antivirus, si faccia riferimento alla sezione dedicata sul sito del servizio Inbank.

2. Sicurezza On-line

Per proteggere da frodi, accessi e modifiche non autorizzate a tutti i dati di pagamento sensibili identificati, sono implementati opportuni presidi di sicurezza tramite misure tecnologiche (ad esempio tramite l'utilizzo di crittografia) e procedure per garantire il controllo accessi e la tracciatura delle attività.

Sicurezza del canale di comunicazione

Per tutti gli scambi di dati di pagamento sensibili via Internet, è garantita la sicurezza dei canali di comunicazione tra le parti coinvolte grazie a:

- Misure di crittografia end to end per tutta la durata della sessione;
- Tecniche di cifratura robuste e ampiamente riconosciute.

Verifica del protocollo

Controllare che l'URL della pagina di Internet Banking inizi con https://www.inbank.it in particolare, la presenza dell'intestazione "https" indica che la navigazione sta avvenendo su una pagina crittografata e quindi sicura. Inbank dispone di crittografia certificata da una Certification Autority riconosciuta e accreditata nel mondo per la sicurezza in internet.

Misure di identificazione dell'utente

L'inoltro dei pagamenti via Internet, così come l'accesso ai dati sensibili relativi ai pagamenti in internet (dati che possono potenzialmente essere utilizzati per perpetrare una frode) sono protetti da un sistema di strong customer authentication, attraverso l'utilizzo, in aggiunta alla verifica di userID e password, dell'apposito strumento di sicurezza fornito al Cliente dalla Banca.
Tale strumento di sicurezza aggiuntivo viene richiesto al momento dell'autorizzazione dell'operazione e può essere uno dei seguenti strumenti di sicurezza proposti dalla Banca:

- Token OTP fisico
- Mobile OTP

Token OTP fisico

È un dispositivo fisico strettamente personale dotato di display ed in grado di generare a cadenza regolare di pochi secondi, codici numerici monouso (di seguito OTP - one time password). Il Token ha le dimensioni di un portachiavi ed è contrassegnato da un codice matricola numerico.
Il token viene consegnato al Cliente della Banca, nello stato di

conservazione e nelle condizioni idonee all'uso. Il token viene attivato dalla Banca entro le ore 24 del giorno successivo al ritiro da parte del Cliente. Alla cessazione del funzionamento del token il titolare della stazione, 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 intervento sullo stesso.

Mobile OTP

Il funzionamento di tale strumento prevede che il titolare Cliente riceva un messaggio (tramite canale SMS o tramite apposita applicazione di sicurezza) sul numero di cellulare fornito dal Cliente Inbank, ogniqualvolta si renda necessario l'inserimento del codice OTP - one time password.
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.

Raccomandazioni per l'utilizzo sicuro del proprio dispositivo mobile:

- Proteggere sempre l'accesso al dispositivo mediante PIN;
- Nel caso di utilizzo del browser del dispositivo mobile evitare di memorizzare la password di accesso ad Inbank;
- Nel caso di furto o smarrimento del dispositivo mobile contattare il proprio operatore telefonico per il blocco della SIM.

Procedura di inoltro e autorizzazione operazioni di pagamento

Il sevizio 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 lo strumento di sicurezza [1];
4. Feedback di conferma di inoltro della disposizione alla Banca.

1 Sono previste specificità che possono derogare il processo di autorizzazione tramite strumento di sicurezza, in funzione della natura della disposizione di pagamento (esempio: lo strumento di sicurezza non è richiesto per disposizioni di "invio denaro circuito Jiffy" di importo limitato)

3. Ulteriori misure di sicurezza

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

Requisiti di autenticazione

Per aumentare il livello di sicurezza nella fase di autenticazione è definito un limite massimo di cinque tentativi falliti di login o di autenticazione; al superamento di tale limite l'accesso al servizio è bloccato.
Nell'utilizzo del servizio Inbank tramite applicazione, il Cliente può impostare in autonomia un "pin rapido" per l'accesso all'applicazione stessa. L'attivazione del pin rapido deve essere autorizzata dall'inserimento del codice OTP generato dallo strumento di sicurezza in uso dal Cliente.

Minuti di inattività (controllo automatico sull'attività di una postazione)

Al fine di prevenire utilizzi fraudolenti, nel caso in cui un'utenza connessa rimanga inattiva per un determinato lasso di tempo (più del numero di minuti specificati dal Cliente o dalle impostazioni di default), il sistema provvede a disconnetterla automaticamente. È possibile settare questa impostazione in autonomia sulla sezione preferenze all'interno della propria area riservata di Inbank.

Pin Trading

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

Limiti Operativi impostati dalla Banca

Per maggiore sicurezza alcune funzionalità dispositive di pagamento hanno dei limiti (es: massimali giornalieri, mensili) impostati dalla Banca. Superato tale limite, il sistema impedisce l'invio di ulteriori disposizioni nello stesso periodo.

Limiti Operativi impostati dal Cliente

Il Cliente Inbank può provvedere autonomamente a ridurre, secondo necessità, i limiti operativi impostati dalla Banca, fino all'azzeramento del limite stesso (con conseguente indisponibilità dei servizi che ad esso fanno riferimento).
Con un apposito messaggio il Cliente Inbank, abilitato ai servizi alert sms, potrà definire un importo massimo per limitare l'invio di alcune disposizioni di pagamento. Tale limitazione avrà effetto anche sulle eventuali utenze secondarie. L'invio del messaggio è subordinato all'utilizzo esclusivo del numero cellulare dell'utenza Inbank.

Messaggi Alert

Il Cliente ha la facoltà di richiedere alla Banca l'attivazione del servizio Alert (tramite canale SMS o tramite apposita applicazione di sicurezza), che lo avvisa quando vengono effettuate disposizioni di pagamento (bonifici SCT Sepa Credit Transfert, bonifici estero, ...) superiori ad una certa soglia fissata dalla Banca stessa. Inoltre il Cliente ha la possibilità di attivare la ricezione di un messaggio in occasione di ogni accesso ad Inbank con la propria utenza.

Alert email

Il Cliente ha la facoltà di attivare il servizio di Alert email che lo informa ogniqualvolta venga inviata una disposizione di pagamento (bonifici SCT, bonifici estero, ...), oltre che ad ogni modifica della sezione "Preferenze". Il servizio, infine, invia al Cliente ogni lunedì della settimana, la lista degli accessi effettuati ad Inbank con la sua utenza.

4. Consigli per la Sicurezza

Inbank, internet e il computer personale sono strumenti sofisticati, è importante conoscere i comportamenti corretti da seguire in tema di sicurezza online per evitare un utilizzo irresponsabile.
La posta elettronica che giunge da indirizzi sospetti o che richiede di seguire link anomali, i programmi che invitano a scaricare documenti sospetti o che provengono da fonti inattese possono veicolare contenuti dannosi. Non verranno mai richieste credenziali o informazioni personali al di fuori del servizio Inbank.

Al fine di presidiare la navigazione nel web ai massimi livelli è necessario installare dei software di protezione (ad esempio un antivirus e un firewall) e mantenere sempre aggiornato il proprio sistema operativo e tutti i programmi installati. É importante effettuare delle scansioni periodiche con l'antivirus installato sul pc per verificare la presenza di eventuali virus o trojan.

Navigare con intelligenza

Le frodi sono sempre in agguato ma basta un minimo di attenzione per evitarle. É sempre consigliato digitare gli indirizzi web direttamente nella barra di navigazione, controllando in anticipo la destinazione del link. Per eventuali dubbi è possibile verificato il certificato del sito cliccando due volte sull'icona del lucchetto.

Variare frequentemente la password di accesso

È consigliabile scegliere una password "forte", che contenga almeno un carattere delle seguenti categorie: lettere maiuscole, lettere minuscole e numeri. Si sconsiglia fortemente di salvare i propri codici di autenticazione (userID e password) in un file localizzato nel computer o nel browser utilizzato.

Massimo controllo del conto online

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

Aggiornamento recapiti

Il numero di telefono cellulare e l'indirizzo email del Cliente sono elementi fondamentali per la gestione della sicurezza; si consiglia al Cliente di tenerli costantemente aggiornati e di comunicare ogni loro variazione alla Banca.

Servizio Assistenza Inbank

Per segnalare eventuali tentativi di frode telefonare al numero verde 800-837455 oppure al numero nero 080 5692856 (per assistenza ai Clienti che chiamano dall'estero).

5. Frodi classiche On-line

La posta elettronica è lo strumento principale utilizzato per le frodi online. Spacciandosi per la Banca, i truffatori potrebbero richiedere i dati personali facendo leva sulla buona fede del Cliente.
Ecco alcuni semplici consigli per evitare di incorrere in queste truffe: una su tutte, il cosiddetto Phishing.

Phishing: cos'è e come funziona?

Tradizionalmente il mezzo principale per cadere in una truffa è la posta elettronica. La minaccia maggiore che incombe sugli utenti online è la pratica chiamata Phishing, termine inglese che nel caso delle frodi online assume il significato di "spillare dati sensibili": lo scopo dei truffatori è quello di conoscere le informazioni personali degli utenti legittimi.

Mail falsa

Nessuna Banca richiederà mai per posta elettronica le credenziali di accesso. Le mail contraffatte hanno lo scopo di indurre gli utenti ad adottare comportamenti non sicuri simulando con una grafica simile all'originale, una comunicazione ufficiale.

Link al sito contraffatto

Lo scopo della mail fraudolenta è quello di appropriarsi delle credenziali di accesso, allarmando il Cliente con avvisi di particolari problemi verificatisi, quali presunti controlli di sicurezza o aggiornamenti. In questo modo, si induce l'utente a cliccare su un link presente nella mail che dovrebbe condurlo alla presunta pagina di autenticazione del sito Inbank.
Il sito non è che una copia fittizia del sito originale: pertanto, accedendovi e digitando codice utenza e password si consegnano direttamente i dati nelle mani del truffatore.

Cosa si può fare?

Cadere nella truffa è solo frutto di disattenzione. L'indirizzo del sito di Inbank è sempre www.inbank.it.
Di seguito alcune regole base di buona condotta:

- La posta elettronica che giunge da indirizzi sospetti e richiede di seguire link anomali va trattata con attenzione;
- Non saranno mai richieste credenziali o informazioni personali da un canale diverso da Inbank;
- Accedere al sito di Inbank solo direttamente dalla barra degli indirizzi senza seguire link esterni; cliccare su link presenti nelle mail sospette è una pratica potenzialmente pericolosa.

6. Nuove minacce on-line

Le credenziali di accesso e la password sono merce preziosa per i malintenzionati: infatti, è molto più facile rubare queste informazioni che violare i sistemi di sicurezza di Inbank. Prevenire questi nuovi tentativi di frode è più facile se si conosce il loro funzionamento.

Come funzionano?

I tentativi di frode più moderni cercano di sfruttare la disattenzione e la buona fede del Cliente; in questi casi non si punta a violare i sistemi di home banking, che sono di per sé estremamente difficili da aggirare, ma si cerca piuttosto di ingannare gli utenti per farsi consegnare le credenziali di accesso e le password di conferma delle disposizioni.

Furto delle credenziali

Un Trojan è un programma che opera sul dispositivo dell'utente per conto di un malintenzionato, detto hacker. Grazie al Trojan, l'hacker richiede o memorizza le credenziali di accesso ad Inbank, la password dispositiva (codice OTP) utilizzando questi dati per accedere ad Inbank e mettere in atto una frode.

Cosa si può fare?

Diffidare quindi da ogni richiesta di password che venga proposta in modalità diverse rispetto a quelle usuali di Inbank. Per segnalare una di queste anomalie è importante non fornire le credenziali, terminare la navigazione e comunicare l'accaduto alla propria Banca o all'assistenza Inbank.

7. Glossario

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

Antivirus Si tratta di un programma che riesce a rilevare ed eliminare il Malware presente in un PC. Un antivirus ricerca all'interno della memoria del PC delle particolari sequenze di dati che denotano la presenza di Malware, dette "firme"; per questo l'antivirus è efficace solo se costantemente aggiornato alle firme più recenti.

Firewall Un firewall è un componente, hardware o software, che filtra il traffico di rete che fluisce tra un PC e internet; applicando particolari regole di sicurezza, il firewall scarta eventuali dati che non rispettano i parametri di sicurezza.

Hacker Persona che mira ad entrare in computer o reti informatiche altrui per motivi di lucro o anche per un semplice senso di sfida.

Keylogging Un keylogger è un software che riesce a intercettare tutto ciò che viene digitato dalla tastiera di un certo computer. Può essere utilizzato per scopi malevoli in quanto permette all'hacker di ritrovare le informazioni relative a nome utente e password digitati dall'utente. L'hacker può successivamente sfruttare le legittime credenziali dell'utente per frodare l'utente stesso.

Malware Con malware si intende un software creato per arrecare danno al computer su cui viene eseguito, all'utente del computer o ad un obiettivo esterno. Sono esempi di malware i Virus e i Trojan. Il malware viene sfruttato dall'hacker malintenzionato per ricavare denaro tramite frodi online, con l'aiuto o meno di eventuali Money mules.

Phishing Si intende con phishing il furto di credenziali ottenuto tramite tecniche di ingegneria sociale. Scopo del furto di identità è quello di accedere alle informazioni personali del truffato e sottrargli denaro tramite transazioni online. La truffa viene portata avanti mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli che imitano la grafica dei siti istituzionali, portando il truffato a rivelare informazioni personali.

Spam

Come Spam vengono definiti tutti quei messaggi di posta elettronica recapitati nella nostra casella di posta che non sono stati direttamente "sollecitati", e che potremmo definire anche come insieme di posta indesiderata. Lo Spam rappresenta un vettore per truffe e raggiri di diversa natura, soprattutto furti di identità, che si sono evoluti fino a trasformarsi in altre forme di minacce quali ad esempio il phishing.

Trojan

Si tratta di malware distribuiti in modo fraudolento. Simili a virus, si attivano all'arrivo di determinati segnali dall'esterno detti trigger. Sono software riconfigurabili dall'esterno ed adattabili.

Virus

Un virus è un tipo di malware che è in grado, una volta eseguito, di infettare dei file e di riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente. Solitamente un virus danneggia direttamente solo il software della macchina colpita

INBANK

ED.09/2016