GUIDA ALLA SICUREZZA SUI PAGAMENTI VIA *INTERNET*

La presente guida di sicurezza è redatta conformemente alla Circolare Banca d'Italia 17 dicembre 2013, n. 285, e s.m.i., "Disposizione di vigilanza per le banche".

La Banca adotta elevati *standard* tecnologici per garantire la protezione dei servizi di *internet home banking* / *mobile banking* e dei pagamenti via *internet*, ma la sicurezza dipende anche dal comportamento del Cliente.

Questa guida aiuta il Cliente a conoscere i rischi più comuni e suggerisce gli accorgimenti principali per un uso sicuro del canale digitale, accessibile dal Cliente medesimo con due modalità distinte, il servizio di *internet home banking* ed il servizio di *mobile banking*.

La Banca non chiederà mai al Cliente, tramite telefonata / *e-mail* / *sms*, di fornire uno o più codici di accesso (*password*, *PIN*) al canale digitale o di seguire procedure alternative a quelle riportate nel presente documento.

IL CLIENTE DEVE CONTATTARE SUBITO LA BANCA SE HA PERSO O SE GLI HANNO RUBATO LE CREDENZIALI DI ACCESSO O LO *SMARTPHONE* O SE RISCONTRA DELLE ANOMALIE NELLE TRANSAZIONI CHE HA EFFETTUATO.

In caso di furto, perdita di riservatezza o smarrimento di una o più credenziali di accesso (*username*, *password*, codice *PIN*) il Cliente deve richiedere senza ulteriore indugio il blocco dell'utenza, contattando, il servizio clienti al numero 800970663 o gli indirizzi *e-mail* dedicati alla clientela, servizioclienti@bancaprogetto.it (a disposizione dei clienti Privati) e supportocontoimprese@bancaprogetto.it (a disposizione dei clienti Imprese); analoga azione deve essere intrapresa dal Cliente in caso di furto o smarrimento dello *smartphone* con accesso al servizio di *mobile banking* inviando inoltre entro 48 (quarantotto) ore, ai suddetti recapiti *e-mail,* copia di denuncia alle autorità competenti.

Se il Cliente, vittima di una frode, dovesse riscontrare transazioni non da lui disposte, o se dovesse notare anomalie nell'accesso al canale digitale o nell'esecuzione di qualsiasi operazione di pagamento *online*, deve segnalare il problema in forma scritta (*e-mail*) agli indirizzi dedicati del servizio clienti. Inoltre, il Cliente ha la possibilità di utilizzare autonomamente le funzioni "blocca *account*" o "blocco utenza" disponibili sul canale digitale.

Si ricorda che, salvo il caso in cui abbia agito in modo fraudolento, il Cliente non sopporta alcuna perdita derivante dall'utilizzo di uno strumento di pagamento smarrito, sottratto o utilizzato indebitamente, intervenuto dopo l'esecuzione della citata comunicazione al servizio clienti. Salvo il caso in cui il Cliente abbia agito con dolo o colpa grave, ovvero non abbia adottato le misure idonee a garantire la sicurezza delle credenziali di accesso (*username*, *password, PIN*) prima di effettuare la suddetta comunicazione alla Banca, il Cliente può essere chiamato a sopportare, per un importo non superiore a Euro 150,00 (centocinquanta/00), la perdita derivante dall'utilizzo indebito dello strumento di pagamento medesimo, conseguente al furto / smarrimento dello stesso.

Nel caso di un'operazione di pagamento non autorizzata, la Banca - effettuate le verifiche del caso, anche sulla base di quanto prodotto dal Cliente - rimborsa al Cliente l'importo dell'operazione e, laddove per l'esecuzione sia stato addebitato il conto, riporta lo stesso nello stato in cui si sarebbe trovato se l'operazione di pagamento non autorizzata non avesse avuto luogo. In caso di motivato sospetto di frode, la Banca può sospendere il rimborso, dandone immediata comunicazione al Cliente. Il rimborso non preclude la possibilità per la Banca di dimostrare, anche in un momento successivo, che l'operazione di pagamento era stata autorizzata (in tal caso, la Banca ha il diritto di chiedere e ottenere dal Cliente la restituzione dell'importo rimborsato).

ACCESSO AL CANALE DIGITALE E OPERAZIONI DISPOSITIVE

Il sito *internet* www.bancaprogetto.it è caratterizzato da un'area riservata al servizio di *internet home banking* accessibile dal Cliente, tramite autenticazione, cliccando sul bottone "HOME BANKING" (per i clienti Privati) o "BUSINESS BANKING" (per i clienti Imprese).

Le funzionalità di *mobile banking* sono fornite tramite le apposite *app* per iOS o Android, scaricabili dai relativi *app store*.

La Banca protegge la trasmissione dei dati attraverso sistemi di crittografia che consentono di stabilire un canale sicuro di accesso via *internet*.

Il servizio utilizza un sistema combinato di credenziali di accesso (*username* e *password*) impostati in "fase di primo accesso" e, per aumentare il livello di sicurezza, in "fase di apertura" del conto viene richiesto un Codice *PIN* (*personal identification number)* di sicurezza, scelto dal cliente, da utilizzare per accedere al servizio e confermare le operazioni dispositive.

Il primo accesso al canale digitale deve avvenire tramite il servizio di *mobile banking*.

In particolare, una volta attivato il conto corrente, il Cliente:

- riceve dalla Banca via *e-mail* il codice utente (*username*) e, via *sms*, una *password* temporanea (cliente Privato); riceve dalla Banca via *sms* il codice utente (*username*) e, via *mail*, una *password* temporanea (cliente Impresa);
- scarica l'*app* sul proprio *smartphone* e accede alla stessa;
- inserisce il codice utente (*username*) e la *password* temporanea;
- sceglie, obbligatoriamente, una nuova *password*;
- sceglie un codice *PIN* (*personal identification number*) di 5 (cinque) cifre, ai fini dell'abilitazione del *token software* (c.d. *smartOTP)* sul proprio *smartphone*.

Il Cliente può cambiare, in qualsiasi momento, i propri codici di accesso (*password, PIN*) in modo autonomo, riservato e gratuito, all'interno della propria Area Personale.

Il *token software* (*smartOTP*) può essere abilitato simultaneamente su un solo dispositivo (*smartphone*), quando il sistema rileva l'accesso da un dispositivo differente richiede al Cliente se vuole sostituire l'abilitazione dal vecchio al nuovo dispositivo; in questo caso il Cliente viene indirizzato al processo di *enrollment* che ne permette la nuova abilitazione.

Per i successivi accessi al servizio di *mobile banking*, il Cliente utilizza la *password* ed il riconoscimento biometrico o, in caso di mancata abilitazione di quest'ultimo, il codice *PIN* precedentemente impostato.

Per il servizio di *internet home banking* tramite *tablet* o *pc*, il Cliente - sia per il primo accesso che per quelli successivi - utilizza tutte le credenziali di accesso, ossia:

1. il codice utente (*username*);
2. la *password*;
3. la validazione dell'accesso mediante l'utilizzo del *token software* (*smartOTP*) sul proprio mobile eseguendo l'approvazione di una *push notification* o l'inserimento di una *OTP* generata in seguito alla scansione *del QR* code visualizzato sul *tablet* o *pc.*

Questi schemi di accesso, utilizzati anche per la validazione di tutte le operazioni dispositive, sono denominati ad autenticazione forte (c.d. *SCA - Strong Customer Authentication*) perché impiegano più di due fattori di autenticazione, ossia, non solo la semplice combinazione di codice utente e *password*, ma un elemento aggiuntivo costituito, nello specifico, dall'utilizzo del *token software (smartOTP)* autorizzato mediante inserimento del *PIN* e/o riconoscimento biometrico.

Per il Cliente Privato in caso di ripetuto inserimento di *password* errata, ha la possibilità di sbloccare l'utenza per l'accesso ai servizi di *internet home banking* e *mobile banking* tramite una funzione di *self reset*, secondo gli *step* di seguito riportati:

- in occasione del primo accesso dall'*app mobile*, il Cliente imposta 5 domande e risposte di sicurezza (ad es., la tua città preferita, ecc.);
- nel caso in cui inserisca una *password* errata per 4 volte, il sistema avvisa il Cliente che ha a disposizione un ultimo tentativo prima del blocco dell'utenza;
- nel caso in cui il Cliente inserisca nuovamente una *password* errata, l'utenza si blocca; il Cliente clicca sul bottone "ti sei bloccato clicca qui", risponde a 2 delle domande di sicurezza impostate ed inserisce il codice *PIN*; l'utenza viene, quindi, sbloccata ed il Cliente potrà effettuare nuovamente l'accesso.

Per il Cliente Impresa è possibile sbloccare l'utenza per accedere ai servizi di *internet home banking* e *mobile banking* contattando l'assistenza dedicata.

Come sopra segnalato, il Cliente ha la possibilità di bloccare l'utenza, contattando il servizio clienti oppure utilizzando le funzioni "blocca *account*" o "blocco utenza", disponibili sul canale digitale.

Il Cliente ha, inoltre, la possibilità di chiudere l'utenza e attivarne una nuova, contattando il servizio clienti al recapito telefonico / all'indirizzo *e-mail* sopraindicati.

La sessione di accesso all'area privata viene interrotta automaticamente dal sistema dopo 20 minuti di inattività, per prevenire eventuali accessi indesiderati. Si consiglia, comunque, di effettuare esplicitamente la disconnessione dalla piattaforma non appena sono terminate le operazioni.

La *password* ha una validità di 90 giorni.

Le credenziali di accesso (*username*, *password* e *PIN)* devono essere conservate distintamente e, per quanto riguarda la *password* e il codice *PIN*, si raccomanda in particolare di:

- non diffonderle attraverso strumenti di comunicazione (social network, e-mail, telefono, etc.);
- non comunicarle ad amici, conoscenti o ad operatori di qualsiasi *Customer Care*;
- prima di effettuare il "Log In" al sito *Home Banking*, verificare ed eventualmente disattivare la funzione di "salvataggio automatico";
- custodire le credenziali (*username*, *password* e *PIN)* con cura, in modo da evitare che altri ne vengano a conoscenza, evitando, per quanto possibile, di annotarli su carta o su dispositivi (*PC, tablet, smartphone*, etc.), assicurandosi di conservarli eventualmente in posti diversi e comunque non accessibili da persone da non autorizzate.

Si raccomanda inoltre di proteggere i dispositivi da cui si accede al portale della Banca, o in cui se ne utilizzi l'App mobile ufficiale, con un metodo di blocco che preveda per lo sblocco l'inserimento di un *PIN*, un segno o il riconoscimento biometrico (Face ID / impronta digitale).

Al fine di creare e gestire una password in modo corretto e sicuro ed evitare l'accesso a persone non autorizzate, di seguito alcune semplici regole:

- scegliere una *password* che abbia una lunghezza minima di 10 caratteri e massima di 64 caratteri, utilizzando almeno un numero, una lettera maiuscola, una minuscola ed un carattere speciale;
- non includere al suo interno codici/parole facilmente intuibili, quali ad. es. il codice utente, la mail di registrazione, il nome o cognome, la tua data/anno di nascita, il nome tuoi familiari etc;
- modificare la password frequentemente (almeno ogni 90 giorni), e comunque ogniqualvolta si abbia il minimo dubbio che qualcuno, in modo fraudolento, ne sia venuto a conoscenza, accertandosi di scegliere una password che sia diversa dalle ultime 10 inserite (il sistema dell'Home Banking le memorizza e non permette di riutilizzarle).
- scegliere una password diversa da quelle normalmente utilizzate per altri servizi su Internet (e-mail, social network, e-commerce, etc.)

MONITORAGGIO DELLE TRANSAZIONI E SEGNALAZIONI DI POTENZIALI FRODI

Il servizio Home Banking prevede che gli accessi (o i tentativi di accesso) e le operazioni effettuate siano costantemente monitorati dalle strutture preposte della Banca, per permettere di intervenire tempestivamente, anche con blocchi operativi temporanei, sia delle singole transazioni che dell'utenza, nel caso in cui si verifichino abusi, situazioni anomale o tentativi di frode. In caso di anomalie o di incidenti sospetti durante le tue sessioni di pagamento, contatta subito il nostro Customer Care.

La Banca potrà contattare il Cliente in caso di anomalie per verificare l'effettiva autenticità delle operazioni investigate.

DIFENDERSI DAL *PHISHING* / *SMISHING* / *VISHING* E DALLE FRODI PIÙ COMUNI

Il *phishing* / *smishing* sono truffe informatiche che hanno l'obiettivo di rubare i dati di accesso personali alla propria Banca *online*, solitamente attraverso un adescamento che comincia da un'*e-mail* o da un *sms*

Il *social engineering*, impiegato nel *phishing* / *smishing*, è un insieme di tecniche ingannevoli per guadagnare la vostra fiducia e sottrarvi dati personali, *password*, ecc. Ad esempio, inviarvi un'*e-mail* o un *sms* facendo finta di essere un vostro collega, un vostro amico, o la vostra Banca, per chiedervi informazioni riservate, è una delle tecniche più diffuse di *social engineering*.

Ti consigliamo quindi di mantenere sempre operativo il servizio di sicurezza di "alert sms / e-mail", attivato dalla Banca con l'apertura del conto, il quale consente di essere avvisato, al proprio numero di cellulare e/o all'indirizzo e-mail indicato, delle principali operazioni effettuate.

Ti spieghiamo ora come avviene un tipico tentativo di *phishing* / *smishing* e come potete proteggervi al meglio.

COME AVVIENE

Arriva un'*e-mail* nella tua casella di posta elettronica o un *sms* sul tuo *smartphone* che sembrano provenire dalla Banca, nei quali ti viene richiesto di inserire una o più credenziali (*username*, *password, PIN)*, accedendo al canale digitale tramite un *link* apparentemente autentico che in realtà collega ad un sito clone che consente ai malintenzionati di entrare in possesso delle credenziali (*username*, *password, PIN)* medesime.

Importante: la Banca non ti chiederà mai tramite telefonata / *e-mail* / *sms* di fornire i tuoi codici di accesso (*password, PIN)* al canale digitale.

Le tecniche di *phishing* / *smishing* evolvono nel tempo e lo schema potrebbe essere differente da quello sopradescritto; tuttavia, il passaggio fondamentale e obbligato è sempre quello dell'acquisizione delle tue credenziali di accesso (*username*, *password, PIN*), con qualche scusa o trucco per far credere che ti stai collegando con la Banca.

Il *vishing* è un'evoluzione del *phishing*. Si viene contattati telefonicamente da un presunto operatore della Banca (anche attraverso una voce pre-registrata) che tenta di carpire, con il pretesto di risolvere dei problemi, le credenziali di accesso (*username*, *password, PIN)*. Ricorda, come già anticipato, che la Banca non richiederà mai telefonicamente i tuoi codici di accesso (*password, PIN*).

COME PROTEGGERSI

Non rispondere mai a *e-mail* / *sms* come quelle descritte sopra e non fornire per nessuna ragione i tuoi dati di accesso a terzi. Non cliccare mai su *link* che ti vengono proposti via *e-mail* / *sms*, ma per qualsiasi necessità di accesso alla tua area privata, collegati sempre prima manualmente al sito *internet* della Banca e accedi dal bottone "area privati", oppure usa direttamente l'*app*.

L'"area privati" del sito *internet* della Banca è sempre identificabile dalla presenza dell'icona di un lucchetto chiuso nella barra degli indirizzi.

In mancanza di queste caratteristiche, il tuo *pc* potrebbe essere stato indirizzato a un sito fraudolento: chiudi la finestra del *browser* e aprine una nuova, inserendo manualmente l'indirizzo *web* della Banca e, dall'*homepage*, clicca sul bottone "area privati" per accedere nuovamente.

Inoltre, utilizza esclusivamente l'*app* ufficiale e, in fase di installazione, fai attenzione ai permessi richiesti, assicurandoti che siano strettamente connessi al servizio che intendi utilizzare.

PROTEGGERE IL PROPRIO *PC*

La prima regola per disporre di un ambiente sicuro per accedere a servizi di pagamento *online* è mantenere aggiornato il *browser* e il sistema operativo del proprio *pc*, effettuando gli aggiornamenti *software* proposti periodicamente dai produttori.

In secondo luogo, è indispensabile dotarsi di un *software antivirus* e mantenerlo aggiornato.

Da diversi anni sono in circolazione alcuni *malware* (*virus*) denominati "*trojan* bancari" che, una volta installati sul vostro *pc*, sono in grado di intercettare le vostre credenziali bancarie (*username*, *password, PIN*) mentre navigate sui siti di *home banking* e di utilizzarle in tempo reale per transazione fraudolente disposte via *internet* da malintenzionati. Normalmente, queste minacce vengono identificate ed eliminate dai *software antivirus*, a patto che vengano regolarmente aggiornati. Non aprire, comunque, mai allegati o *link* sospetti, soprattutto nel caso di *file* eseguibili (ad esempio che terminano con *.exe*) e non installare *software/app* se non sei certo che siano affidabili.

Elimina periodicamente i *cookies* e i file temporanei *internet*, utilizzando le opzioni del tuo *browser*.

Non utilizzare memorie esterne (come chiavette *usb*) di dubbia provenienza; verifica la sicurezza di questi dispositivi, facendo le scansioni automatiche previste dai principali *software antivirus* al momento dell'installazione.

PROTEGGERE IL PROPRIO *SMARTPHONE*

Mantieni sempre aggiornati all'ultima versione disponibile sistema operativo e applicativi e ricorda di disattivare *wi-fi* e *bluetooth* quando non li usi mantenendo invece sempre attiva l'opzione di *find devices* (c.d. trova telefono).

Scarica le app solo dagli store ufficiali ponendo attenzione a limitare le autorizzazioni richieste a quelle strettamente necessarie al servizio offerto.

Per maggiore sicurezza imposta il blocco automatico del tuo *smartphone* quando entra in *stand-by* e, per proteggere i tuoi dati, quando possibile, attiva la crittografia del *smartphone* e della *memory card*.

Le 8 regole per proteggerti dalle frodi online

1. Fai sempre attenzione alle e-mail false

Il Phishing è un tentativo di truffa che "non viola" i sistemi di Home Banking (che garantiscono comunque la massima sicurezza), ma tenta di acquisire le tue credenziali (*username*, *password, PIN*) e/o i tuoi dati riservati. Come si verifica: L'utente riceve una e-mail, da un indirizzo e con una grafica del tutto simile a quelle della Banca, in cui viene invitato a collegarsi ad un link; cliccando si accede ad un sito simile a quello della Banca. Nel "falso sito" viene richiesto l'inserimento dele proprie credenziali di accesso (*username*, *password, PIN*). Seguendo le istruzioni riportate, è il cliente stesso a trasmettere ai "truffatori" le proprie credenziali di accesso. Come tutelarti: Non inserire mai i tuoi dati personali o le tue credenziali (*username*, *password, PIN*) all'interno di link ricevuti via e-mail. Banca Progetto non richiederà mai i tuoi codici di accesso (*password, PIN*) tramite e-mail. Cerca di identificare le e-mail false: solitamente non sono personalizzate, dichiarano motivazioni di invio non precise, come ad esempio la scadenza o lo smarrimento dele credenziali di accesso (*username*, *password, PIN*), fantomatici problemi tecnici o di sicurezza. Spesso minacciano la sospensione del servizio in caso di

mancata risposta. Non cliccare su link e non aprire file allegati alle e-mail, soprattutto se di dubbia provenienza: i siti web "truffa" non vanno mai visitati ed i file allegati non devono mai essere scaricati sul proprio PC. Segnala di aver ricevuto una e-mail sospetta: nel caso in cui ricevi una e-mail e non sei completamente sicuro della sua autenticità, puoi chiamare il Numero Verde 800.970.663 per verificarne l'autenticità.

2. Controlla la sicurezza di ogni sito prima di fornire dati riservati

Prima di inserire in un sito web le tue credenziali (*username*, *password, PIN*) o numeri di carte di credito/debito, ti consigliamo di verificare sempre che la trasmissione dei dati del sito web che stai utilizzando sia "sicura" e che il sito web sia autentico. In particolare, ricordati di verificare sempre la presenza del prefisso "https://" nell'indirizzo web. Per aumentare il livello di sicurezza, è molto importante che anche il tuo PC e i tuoi dispositivi siano sempre protetti dalle minacce online. Assicurati di avere un antivirus aggiornato all'ultima versione!

3. Non effettuare il salvataggio automatico delle password sul PC o sul browser

Le tue credenziali di accesso ai servizi bancari (*username*, *password, PIN*) non dovrebbero mai essere salvate nella memoria del tuo PC o in quella del browser. Puoi comunque disabilitare e cancellare le password già salvate per altri servizi dalle impostazioni del browser.

4. Proteggi il computer con antivirus e dispositivi di filtraggio

L'antivirus è un ottimo strumento per stare al sicuro da tentativi di intrusione e virus, alcuni dei quali mirano a sottrarre le tue credenziali di accesso (*username*, *password, PIN*) e dati personali. Ricordati di effettuare periodicamente i vari aggiornamenti generalmente segnalati online dal produttore anche nel proprio sito. Assicurati che la soluzione che scegli sia impostata in modo da risultare efficace anche su eventuali periferiche esterne collegate (ad. es. auto scansione delle periferiche USB).

Inoltre, può essere utile utilizzare programmi per la gestione della posta elettronica (es. Outlook) perché sono in grado di attenuare i rischi filtrando molte e-mail sospette attraverso la funzione di *anti-spam*.

Un'ulteriore protezione contro gli hacker, facilmente scaricabile da Internet o acquistabile, è rappresentata dai dispositivi firewall, che tengono sotto controllo ciò che entra e ciò che esce dal PC, proprio come dei "buttafuori" digitali.

5. Evita la condivisione di file su Internet

Condividere file su Internet (con i software per scaricare mp3, video, etc.) significa lasciare una "porta aperta" e quindi permettere l'accesso a "ospiti" indesiderati. Particolari software denominati spyware, possono avere facile accesso e "catturare" via Internet le tue informazioni personali a tua insaputa. Evita quindi di condividere file se vuoi aumentare la sicurezza.

6. Aggiorna spesso il Sistema Operativo

Le aziende produttrici dei Sistemi Operativi rendono disponibili gli aggiornamenti, scaricabili gratuitamente online. Si tratta delle cosiddette Patch, che incrementano, tra l'altro, la sicurezza dei programmi. Assicurati di scaricare e installare solo gli aggiornamenti ufficiali. Stessa attenzione deve essere posta nell'eseguire costantemente gli aggiornamenti disponibili per i dispositivi mobile utilizzati.

7. Utilizza dispositivi e reti sicure e proteggi la tua rete privata

Si raccomanda di utilizzare sempre un PC sicuro per collegarsi al sito della Banca, evitando per esempio di operare da internet point o di collegarsi da dispositivi non personali. Cerca di evitare di accedere ai servizi di banking collegandoti da una rete wi-fi pubblica (es. spazi pubblici, treno, aeroporto ecc.): i tuoi dati potrebbero essere sottratti facilmente da malintenzionati. In caso di utilizzo di una rete wi-fi domestica porre attenzione nel proteggere l'accesso alla rete mediante una password complessa che impedisca connessioni dall'esterno, ricordando che la rete è visibile anche al di fuori dei confini perimetrali della vostra abitazione.

8. Resta informato sui pericoli digitali

Informati sulle campagne fraudolente in atto ed approfondisci i temi di sicurezza leggendo i vademecum di ABI (l'Associazione bancaria italiana) su come operare online in piena sicurezza e sul furto di identità digitale.