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* / *s.m.s.*, di fornire le credenziali di accesso 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 delle credenziali di accesso (*username*, *password*, codice *p.i.n.*) o di furto / smarrimento dello *smartphone* con accesso al servizio di *mobile banking*, il Cliente deve richiedere subito il blocco dell'utenza, contattando il servizio clienti al numero 800970663 o all'indirizzo *e-mail* servizioclienti@contoprogetto.it oppure utilizzando le funzioni "blocca *account*" o "blocco utenza" disponibili sul canale digitale, e inviando copia di denuncia alla Banca entro 48 (quarantotto) ore. Se il Cliente è vittima di una frode e riscontri delle transazioni che non sono state da lui disposte, o se nota delle anomalie nell'accedere al canale digitale o nell'effettuare qualsiasi operazione di pagamento *online*, segnala il problema in forma scritta al servizio clienti.

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 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 una sezione (portale di attivazione) dedicata al Conto *Key* esposta sull'*home page* dove il Cliente sottoscrive il contratto di conto corrente, e da un'area riservata al servizio di *internet home banking* accessibile dal Cliente, tramite autenticazione, cliccando sul bottone "Sono un privato" esposto sull'*home page* e, quindi, sul bottone "HOME BANKING".

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

La Banca adotta versioni aggiornate dei protocolli di crittografia per creare un canale sicuro di accesso via *internet*.

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;
- scarica l'*app* sul proprio *smartphone* e accede alla stessa;
- inserisce il codice utente (*username*) e la *password* temporanea;
- sceglie una nuova *password*;
- sceglie un codice *p.i.n.* (*personal identification number*) di 5 (cinque) cifre, ai fini dell'installazione del *token software smartOTP* sul proprio *smartphone*.

Per i successivi accessi al servizio di *mobile banking*, il Cliente utilizza la *password* e il codice *p.i.n.* (*personal identification number*).

Quando viene effettuato un accesso da uno *smartphone* differente, viene rilevato che il *token software smartOTP* è già installato su un altro dispositivo e viene richiesto al Cliente se vuole migrare la licenza; in caso di risposta affermativa, il Cliente viene indirizzato al processo di *enrollment* che permette di installare il *token software* sul nuovo dispositivo.

Per il servizio di *internet home banking* tramite *tablet* o *pc*, il Cliente - sia per il primo accesso che per quelli successivi - utilizza tutti i citati strumenti, ossia:

1. il codice utente (*username*);
2. la *password*;
3. il codice *p.i.n.* (*personal identification number*) di 5 (cinque) cifre, da valorizzare sul proprio *smartphone*, a seguito di notifica *push.*

Questi schemi di accesso sono denominati ad autenticazione forte perché impiegano più di due fattori di autenticazione, ossia, non solo la semplice combinazione di codice utente e *password*, ma un elemento aggiuntivo costituito dalla *smartOTP*, ossia una "*one time password*" generata dall'applicazione installata sullo *smartphone* del Cliente (cd. "*token software*"), a seguito della valorizzazione del codice *p.i.n*. A differenza delle normali *password*, i codici *OTP* sono "usa e getta", ossia sono validi per una durata limitata ed ogni codice è utilizzabile una sola volta. Per l'operazione successiva bisogna aspettare la generazione di un nuovo codice.

Tutte le operazioni dispositive tramite il canale digitale richiedono un'ulteriore autorizzazione che potrà essere data inserendo nuovamente il codice *p.i.n.* scelto e sono effettuabili solo dopo aver completato l'accesso al canale medesimo.

In caso di inserimento di *password* errata, il Cliente 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 5 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, riceve tramite *e-mail* un codice *OTP* aggiuntivo da inserire a sistema;
- se sbaglia ad inserire il codice *OTP*, il Cliente deve attendere 15 minuti prima di riprovare ad accedere;

- se inserisce correttamente il codice *OTP*, 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 *p.i.n.*; l'utenza viene, quindi, sbloccata ed il Cliente potrà effettuare nuovamente l'accesso.

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 5 minuti di inattività, per prevenire eventuali accessi indesiderati. Si consiglia, comunque, di effettuare esplicitamente la disconnessione dalla piattaforma non appena sono terminate le operazioni.

Le credenziali di accesso devono essere conservate distintamente e, per quanto riguarda la *password* e il codice *p.i.n.*, si raccomanda in particolare di:

- non lasciare traccia scritta o, comunque, di non custodirle mai insieme all'*user id*;
- cambiarle periodicamente dall'area privata all'interno della sezione del profilo personale;
- non associarle a riferimenti strettamente personali, quali compleanni o numeri di telefono;
- non memorizzarle nel *browser* (evitare cioè di sfruttare la modalità di completamento automatico).

La *password* ed il codice *p.i.n.* hanno una validità di 180 giorni.

MONITORAGGIO DELLE TRANSAZIONI E SEGNALAZIONI DI POTENZIALI FRODI

Le strutture preposte della Banca monitorano e investigano eventuali transazioni anomale e, in caso di sospetta frode, potrebbero bloccare le transazioni investigate o sospenderle per il tempo necessario a mettersi in contatto con i clienti interessati e verificare l'effettiva autenticità delle operazioni disposte.

Pertanto, nel caso in cui una transazione originata nell'area privata risulti potenzialmente fraudolenta, la Banca potrà contattare il Cliente comunicandogli gli estremi della transazione e procederà, con il suo assenso, all'eventuale sblocco dell'operazione sospesa.

Per tutelare il Cliente, la Banca potrà, inoltre, procedere al blocco dell'utenza a fronte di sospetti abusi o frodi. Per sbloccare l'utenza, il Cliente dovrà procedere come sopra segnalato.

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

Il *phishing* / *smshing* 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 *s.m.s*.

Il *social engineering*, impiegato nel *phishing* / *smshing*, 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 *s.m.s.* 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 spieghiamo ora come avviene un tipico tentativo di *phishing* / *smshing* e come potete proteggervi al meglio.

<u>COME AVVIENE</u>

Arriva un'*e-mail* nella tua casella di posta elettronica o un *s.m.s.* sul tuo *smartphone* che sembrano provenire dalla Banca, nei quali ti viene richiesto di inserire le credenziali, 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 medesime.

Importante: la Banca non ti chiederà mai tramite telefonata / *e-mail* / *s.m.s.* di fornire le credenziali di accesso al canale digitale.

Le tecniche di *phishing* / *smshing* 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 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. Ricorda, come già anticipato, che la Banca non richiederà mai telefonicamente le tue credenziali di accesso.

COME PROTEGGERSI

1. Non rispondere mai a *e-mail* / *s.m.s.* 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* / *s.m.s.*, 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*.
2. Conserva con la massima cura le credenziali di accesso.

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.

Infine, ti consigliamo di mantenere operativo il servizio di sicurezza di "*alert s.m.s.* / *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.

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 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 (che terminano con .*exe*) e non installare *software* 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.

A seconda dei tuoi fornitori di accesso a *internet* e di servizi di posta elettronica, ti suggeriamo di valutare l'attivazione e il mantenimento di servizi *antispam* e di dispositivi *firewall*.

PROTEGGERE IL PROPRIO *SMARTPHONE*

Installa e mantieni sempre aggiornati *antivirus*, sistema operativo e applicativi e ricorda di disattivare *wi-fi*, geolocalizzazione e *bluetooth* quando non li usi.

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*.

ACCEDERE DA RETI PUBBLICHE O DA POSTAZIONI PUBBLICHE

Se accedi al canale digitale da reti *wi-fi* pubbliche (ad esempio, le reti *wi-fi* in treno, negli spazi pubblici, in aeroporto ecc.), devi prestare massima attenzione, e in particolare devi:

- verificare che, durante il collegamento all'"area privati" del sito *internet* della Banca, sia presente l'icona di un lucchetto chiuso nella barra degli indirizzi (come indicato nella sezione "Difendersi dal *phishing* / *smshing* / *vishing* e dalle frodi più comuni");
- non memorizzare mai le credenziali di accesso; se il *browser* vi propone di salvarle, scegli sempre "no";
- effettuare subito la disconnessione dalla piattaforma al termine delle operazioni.