Guida alla Sicurezza sui pagamenti via internet di Banca 5 – clientela Retail

Banca 5 adotta elevati standard tecnologici per garantire la protezione del tuo Home Banking e dei pagamenti via internet, ma la sicurezza dipende anche dal tuo comportamento. Questa guida ti aiuta a conoscere i rischi più comuni e ti suggerisce gli accorgimenti principali per un uso sicuro dei servizi di Home Banking e Mobile Banking.

Banca 5 non vi chiederà mai tramite e-mail di fornire le vostre credenziali di accesso o di seguire procedure alternative a quelle riportate in questa sezione.

Per qualsiasi domanda, delucidazione o segnalazione in merito alla sicurezza dei servizi di Banca 5, ti invitiamo a contattare il Servizio Clienti al numero 800.005.005.

CONTATTA SUBITO BANCA 5 SE HAI PERSO O SE TI HANNO RUBATO LE CREDENZIALI DI ACCESSO O SE RISCONTRI DELLE ANOMALIE NELLE TRANSAZIONI CHE HAI EFFETTUATO

In caso di furto, perdita di riservatezza o smarrimento delle credenziali di accesso (Userd id, password, telefono cellulare che riceve i codici via SMS o li genera tramite apposita funzionalità App), richiedi subito il blocco del servizio contattando il Servizio Clienti e invia copia di denuncia a Banca 5 entro 48 (quarantotto) ore. Se sei vittima di una frode e riscontri delle transazioni che non sono state disposte da te, o se noti delle anomalie nell'accedere al sito di Home Banking, nell'uso dell'App Mobile o nell'effettuare qualsiasi operazione di pagamento online, contatta il Servizio Clienti segnalando il problema.

Ti ricordiamo 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 relativa comunicazione di cui al presente paragrafo. 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, Banca 5 – 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 Banca 5 di dimostrare, anche in un momento successivo, che l'operazione di pagamento era stata autorizzata (in tal caso, Banca 5 ha il diritto di chiedere e ottenere dal Cliente la restituzione dell'importo rimborsato).

ACCESSO ALLA PIATTAFORMA E OPERAZIONI DISPOSITIVE

La piattaforma di Home Banking di Banca 5 è raggiungibile dal bottone "Login privati" esposto sul sito istituzionale della Banca https://www.banca5.com.

Le funzionalità di Mobile Banking sono fornite tramite le apposite App per iOS o Android.

Banca 5 adotta versioni aggiornate dei protocolli di crittografia per creare un canale sicuro di accesso via internet.

Per poter accedere via internet all'Home Banking di Banca 5 è necessario autenticarsi inserendo:

1. il proprio Userd id;
2. la password utente;
3. il codice numerico di 6 cifre (codice OTP) inviato via SMS al numero di cellulare certificato, oppure generato da apposita funzionalità dell'App (se disponibile).

In caso di primo accesso da un nuovo dispositivo tramite le apposite App per IOS e Android, sarà necessario autenticarsi inserendo:

1. il proprio Userd id;
2. la password utente;
3. il codice numerico di 6 cifre (codice OTP) inviato via SMS al numero di cellulare certificato, oppure generato da apposita funzionalità dell'App (se disponibile).

Per gli accessi successivi dallo stesso dispositivo e con la stessa utenza, basterà immetterre il prorio User id e la propria password, senza che venga richiesta l'immissione del codice OTP. Questo perché il dispositivo sarà già associato alla tua utenza in modo sicuro. Quando viene effettuato un accesso da dispositivo differente, oltre che la richiesta del codice OTP al primo accesso, verrà inviato un avviso di sicurezza alla mail indicata durante la fase di registrazione per notificare il *cambio dispositivo*, per assicurarci che si tratti di un accesso eseguito da te.

Questo schema di accesso è denominato autenticazione forte perché impiega più di due fattori di autenticazione: non solo la semplice combinazione di User id e password, ma un elemento aggiuntivo costituito dal codice OTP. A differenza delle normali password, i codici OTP sono "usa e getta", ovvero 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 richiedono l'immissione di un nuovo codice OTP, e sono effettuabili solo dopo aver completato l'accesso alla propria area privata Banca 5 .

Ad esempio, per disporre un bonifico il sistema richiede una serie di passaggi:

- accedere all'area privata di Banca 5 con autenticazione forte (codice utente, password e codice OTP se l'accesso avviene via internet o se è il primo accesso da App IOS o Android da nuovo dispositivo; codice utente e password se l'accesso viene effettuato da App IOS o Android da un dispositivo già associato);
- accedere alla sezione "Bonifico" e scegliere la funzione "Inserisci Nuovo Bonifico";
- immettere i dati del bonifico (beneficiario, importo, causale, ecc.);
- confermare la disposizione del bonifico inserendo un nuovo codice OTP.

In caso di inserimento di credenziali errate, dopo 5 tentativi consecutivi di accesso il sistema blocca temporaneamente il vostro codice utente per un periodo di tempo limitato stabilito dalla Banca. Per sbloccarlo immediatamente in autonomia, esegui un tentativo di accesso e segui le istruzioni di sblocco temporaneo riportate dall'interfaccia di login.

Se, consecutivamente a un blocco temporaneo, avvengono ulteriori tentativi di accesso falliti, il sistema provvedere a bloccare l'account utente in maniera permanente. Pertanto, se a seguito di un tentativo di Login il sistema vi notifica che il vostro account è in Blocco Permanente, contattate telefonicamente il Servizio Clienti al numero 800.005.005 che vi guiderà nella procedura di sblocco.

La sessione di accesso all'area privata Banca 5 viene interrotta automaticamente dal sistema dopo 20 minuti di inattività, per prevenire eventuali accessi indesiderati. Ti consigliamo comunque di effettuare esplicitamente la disconnessione dalla piattaforma non appena hai terminato le operazioni.

Le Credenziali di Sicurezza devono essere conservate distintamente e, per quanto riguarda la password di accesso, si raccomanda in particolare di:

- non lasciare traccia scritta o, comunque, di non custodirla mai insieme all'User id;
- cambiarla periodicamente dall'area privata di Banca 5 all'interno della sezione del profilo personale);
- non associarla a riferimenti strettamente personali quali compleanni o numeri di telefono;
- non memorizzarla nel browser (evitare cioè di sfruttare la modalità di completamento automatico).

Se non effettui nessun accesso per un periodo superiore ai 6 mesi, il tuo Used id verrà bloccato permanentemente. Qualora non utilizzi frequentemente il servizio di Home Banking o Mobile Banking, ti consigliamo di collegarti comunque periodicamente per mantenere attiva la tua utenza.

MONITORAGGIO DELLE TRANSAZIONI E SEGNALAZIONI DI POTENZIALI FRODI

Le strutture preposte da Banca 5 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 di Banca 5 dal tuo account risulti potenzialmente fraudolenta, Banca 5 ti potrà contattare comunicandoti gli estremi della transazione e procederà, con il tuo assenso, all'eventuale sblocco dell'operazione sospesa.

Per tutelare il cliente, la Banca potrà inoltre procedere al Blocco Permanente dell'account utente a fronte di sospetti abusi o frodi. Per sbloccare l'account, il cliente dovrà contattare il Servizio Clienti e seguire le procedure che verranno indicate.

DIFENDERSI DAL PHISHING E DALLE FRODI PIÙ COMUNI

Il *phishing* è una truffa informatica che ha l'obiettivo di rubare i dati di accesso personali alla propria Banca online, solitamente attraverso un adescamento che comincia da un'e-mail.

Il *social engineering*, impiegato nel *phishing*, è un insieme di tecniche ingannevoli per guadagnare la vostra fiducia e sottrarvi dati personali, password, ecc. Ad esempio, inviarvi un'e-mail 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* e come potete proteggervi al meglio.

COME AVVIENE

Arriva nella tua casella di posta elettronica un'e-mail che sembra provenire dalla tua Banca e ti dice che c'è un imprecisato problema al sistema di "Home Banking". Ti invita pertanto ad aprire la home page della Banca con cui hai il conto corrente gestito via web e di cliccare sul link indicato nella e-mail.
Importante: Banca 5 non invierà mai alcuna e-mail in cui vi si chiede di indicare o inserire i vostri dati di accesso al Servizio di Home Banking o Mobile Banking.

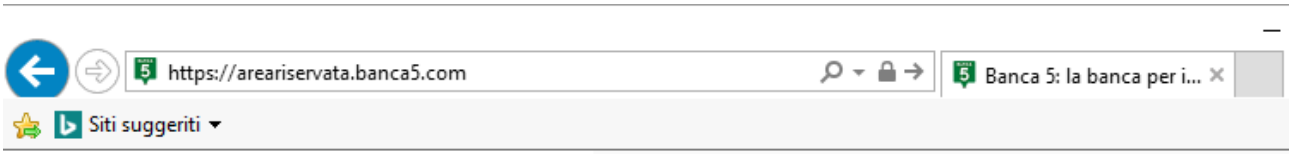
Subito dopo aver cliccato sul link ti si apre una finestra (pop-up) su cui digitare il codice utente, la password e il token di accesso all'Home Banking. Dopo pochi secondi, in generale, appare un altro pop-up che ti informa che il token non è stato riconosciuto e che è necessario inserirlo nuovamente (è questo il modo per sottrarti la password dispositiva). A questo punto qualcuno è entrato in possesso dei vostri dati e può fare operazioni dal vostro conto.

Le tecniche di phishing evolvono nel tempo e lo schema potrebbe essere leggermente differente da quello descritto qui sopra, tuttavia il passaggio fondamentale e obbligato è sempre quello dell'acquisizione delle tue credenziali di accesso con qualche scusa o trucco per farti credere che vi state collegando con Banca 5.

COME PROTEGGERSI

1. Non rispondere mai a e-mail 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, ma per qualsiasi necessità di accesso alla tua area privata Banca 5, collegati sempre prima manualmente a https://www.banca5.com e accedi dall'area di Login privati, oppure usa direttamente l'App Banca 5.
2. Conserva con la massima cura i codici di accesso.

L'area privata di Banca 5 è sempre identificabile dalla presenza di un lucchetto chiuso e dalla dicitura "https" 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 https://www.banca5.com e, dall'homepage, clicca su "Login privati" per accedere nuovamente.

PROTEGGERE IL PROPRIO PC DAI MALWARE

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: vi sono ormai diverse alternative, molte delle quali gratuite, sia su Windows che su Mac OS X.

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.

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.

ACCEDERE DA RETI PUBBLICHE O DA POSTAZIONI PUBBLICHE

Se accedi alla piattaforma di Home Banking o Mobile Banking di Banca 5 da reti WiFi pubbliche (ad esempio le reti Wi-Fi in treno, negli spazi pubblici, in aeroporto ecc.), devi prestare massima attenzione, cercando di:

- verificare che, durante il collegamento all'area privata, il browser esponga sempre, nella parte superiore, il prefisso https a fianco del nome "areariservata.banca5.com" , oltre alla presenza dell'icona di un lucchetto chiuso (come indicato nella sezione "proteggersi dal phishing");
- non memorizzare mai la password o l'User id, se il browser vi propone di salvarla scegliete sempre "no";
- effettuare subito la disconnessione dalla piattaforma al termine delle operazioni.

NORMATIVA DI RIFERIMENTO

La presente guida di sicurezza è redatta conformemente alla normativa "Disposizione di vigilanza le per le banche - Circolare n° 285 del 17 dicembre 2013, 16° aggiornamento del 17 maggio 2016".