BFF
a bank like no other®

CONTO DEPOSITO
FACTO

Linee guida e orientamenti per la sicurezza dei pagamenti online.

Il presente documento riporta le principali informazioni legate alla sicurezza dei pagamenti via internet e alcuni suggerimenti sull'utilizzo sicuro e consapevole di Conto Facto, il conto deposito di BFF Bank S.p.A. (la "Banca"). La Banca sarà sempre a disposizione per approfondimenti e ulteriori informazioni riguardanti questi aspetti.

1. Accesso al sito internet ed esecuzione delle disposizioni

Requisiti tecnologici
Per poter accedere a Conto Facto è necessario disporre di un collegamento alla rete internet tramite un ISP (Internet Service Provider) a scelta e dotarsi di un dispositivo (es. personal computer, tablet) in grado di stabilire una connessione internet sicura tramite l'utilizzo di un antivirus e un firewall aggiornati.
Il servizio è fruibile attraverso l'utilizzo di sistemi operativi e browser supportati.

Le tue credenziali
Per accedere a Conto Facto e impartire disposizioni tramite il sito internet della Banca è necessario utilizzare i codici di sicurezza forniti dalla medesima Banca. Username e password sono le tue chiavi di accesso a Conto Facto: proteggile come se fossero le tue chiavi di casa! Non scriverle sul cellulare o su supporti che possono essere sottratti.

Una password efficace:
- non contiene informazioni personali (data di nascita, nome e cognome);
- non contiene sequenze di lettere o numeri (es. 1234, abcd);
- non è la stessa per tutti gli accessi (conto, email, siti internet);
- deve essere cambiata almeno ogni tre mesi.

Dopo aver effettuato 5 tentativi errati, la password sarà bloccata e sarà necessario richiedere una nuova emissione. Al fine di prevenire utilizzi fraudolenti, nel caso in cui un'utenza connessa rimanga inattiva per un determinato lasso di tempo, il sistema provvede a disconnetterla automaticamente.

Diffida se improvvisamente cambia la modalità con la quale ti viene chiesto di inserire i codici di accesso: ad esempio, se questi vengono chiesti non tramite una pagina del sito, ma tramite pop-up (una finestra aggiuntiva di dimensioni ridotte). In questo caso, contatta la Banca tramite il Servizio Clienti al numero 800.53.80.77.

Verifica del protocollo
Assicurati che le pagine web in cui si inseriscono le credenziali di accesso e i dati personali siano protette, diffidando dei "pop-up". Per verificare che la pagina web sia protetta, controlla che l'indirizzo sia preceduto da "https://" e che sul browser sia presente l'icona che attesti il collegamento a un sito protetto, solitamente raffigurante un lucchetto chiuso accanto all'indirizzo internet.

Al momento di uscire dal sito, seleziona "LOGOUT" prima di chiudere la pagina, indipendentemente dal tipo di dispositivo che stai utilizzando.

Sicurezza del canale di comunicazione
Per tutti gli scambi di dati di pagamento 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.

Il codice OTP e la Secure Call
Ogni volta che dovrai attivare un vincolo, variare il conto predefinito, richiedere l'estinzione del conto o modificare i tuoi contatti, ti sarà inviato un codice OTP (One-Time Password) per confermare l'operazione richiesta. L'OTP è un codice valido solo per una singola sessione di accesso o transazione.

I codici OTP saranno inviati tramite email o SMS in base al canale da te selezionato per l'invio del codice di conferma o su entrambi i canali per le modifiche del conto predefinito e dei canali di contatto.

Per garantire invece una maggiore sicurezza sui bonifici in uscita verso il conto predefinito, è previsto un ulteriore strumento di autenticazione: la Secure Call. Tale dispositivo rappresenta la migliore tecnologia oggi disponibile per evitare il rischio di frodi informatiche.

Le sue principali caratteristiche sono:
- disponibilità 24 ore su 24;
- nessuna procedura di installazione;
- non devi ricordare nessuna password;
- servizio totalmente gratuito.

Ogni volta che dovrai richiedere un bonifico in uscita verso il tuo conto predefinito, ti verrà fornito un codice OTP, in grado di ridurre il rischio di intercettazioni e riutilizzi impropri.
Per confermare l'operazione richiesta dovrai quindi:
- chiamare il numero verde dedicato utilizzando il numero di cellulare associato alla tua posizione;
- digitare, quando richiesto, il codice OTP sulla tastiera del tuo telefono cellulare.

Se la Secure Call è stata effettuata correttamente, sarà sufficiente cliccare sul tasto "Conferma" per autorizzare l'operazione.

Attenzione:
Nessun dipendente della Banca è autorizzato a richiedere i tuoi codici di accesso. La Banca non invierà mai alcuna richiesta in tal senso, sia essa effettuata di persona oppure tramite telefono, posta, email o altro mezzo.

2. Regole per difendersi

I personal computer, gli smartphone e tutti i dispositivi utilizzati per l'accesso ad internet 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.

Al fine di presidiare la navigazione ai massimi livelli è necessario:
- proteggere i propri dati personali e custodire con cura i propri dati di accesso al sito (username e password), non salvandoli sul proprio computer, mantenendo separati username e password, e modificando periodicamente quest'ultima;
- non fornire MAI le proprie password a terzi;
- accedere sempre ai servizi online digitando *https://www.contofacto.it/bff/login*, evitando di "cliccare" su eventuali collegamenti presenti nelle email e di dare seguito ad eventuali richieste in esse contenute;
- prestare la massima attenzione alla presenza di pagine "manipolate", ovvero che presentano un aspetto grafico differente rispetto a quelle dell'applicativo di internet banking, oppure con dei contenuti sospetti (es. messaggi non in lingua italiana);
- controllare regolarmente gli estratti conto dei propri depositi, per assicurarsi che le transazioni riportate siano quelle realmente effettuate;

Per proteggerti da minacce che potrebbero compromettere la sicurezza dei tuoi dati e dei tuoi dispositivi, ti consigliamo di:
- non scaricare mai programmi che provengano da siti sospetti o di dubbia reputazione;
- non condividere file su internet. Condividere file su internet significa lasciare una "porta aperta" a rischio di virus e/o intrusioni dall'esterno. Particolari software, denominati spyware (tipi di software che raccolgono informazioni riguardanti l'attività online di un utente come siti visitati, acquisti eseguiti in rete, etc. senza il suo consenso), possono avere facile accesso al tuo computer e "catturare" via internet informazioni personali a tua insaputa;
- non aprire email sospette che hanno un allegato, anche quando conosci il mittente (potrebbe essere contraffatto);
- diffida di qualunque email che ti richieda l'inserimento di dati riservati riguardanti i codici di accesso al servizio di home banking o altre informazioni personali. La Banca non richiede tali informazioni via email;
- non scaricare mai programmi sotto forma di ActiveX. L'ActiveX è un'estensione che, integrata in un'applicazione predisposta all'utilizzo di questa tecnologia, permette di aggiungere nuove potenzialità, comandi ed eventualmente semplificare alcuni processi, soprattutto nell'ambito dello sviluppo di software. Nel caso in cui visiti pagine che richiedono questa operazione, inseriscile nell'elenco dei siti con restrizione del tuo browser;
- mantenere aggiornato il tuo sistema operativo e il tuo browser scaricando le opportune "patch" (porzione di software progettata per aggiornare o migliorare un programma). Ciò include la risoluzione di vulnerabilità di sicurezza e altri bug generici: tali patch vengono anche chiamati fix o bugfix. Mediante patch vengono anche migliorate l'usabilità e le prestazioni dell'applicazione dal sito internet del fornitore del sistema;
- installare un programma antivirus e aggiornarlo frequentemente;
- installare possibilmente un personal firewall (componente per la sicurezza informatica con lo scopo di controllare gli accessi alle risorse di un sistema filtrando tutto il traffico che tale sistema scambia con l'esterno);
- non consentire, durante la navigazione in internet, che vengano eseguite attività da remoto senza la tua autorizzazione e consenti l'installazione dal web dei soli programmi di cui è possibile verificare la provenienza e l'affidabilità.

3. Cosa fare nel caso in cui...?

Hai il dubbio di aver subito una frode o un tentativo di frode?
Se pensi di aver subito una frode o un tentativo di frode, rivolgiti subito alla Banca telefonando al Servizio Clienti (contattando il Numero Verde 800.53.80.77) oppure tramite l'area riservata del sito internet.

Dopo averlo comunicato alla Banca, rivolgiti alle Autorità competenti (ad esempio Polizia o Carabinieri), che sono a tua disposizione 24 ore su 24, anche tramite un apposito sito internet *https://www.commissariatodips.it/*.

Qualcuno è venuto a conoscenza o sospetti che sia venuto a conoscenza delle tue credenziali?
In caso di smarrimento, furto, appropriazione indebita o uso (ovvero sospetto di uso) non autorizzato delle tue credenziali di accesso, è necessario informare immediatamente la Banca telefonando al Servizio Clienti (contattando il Numero Verde 800.53.80.77) oppure tramite l'area riservata del sito internet.

La Banca provvederà a bloccare i codici di accesso nei tempi tecnici necessari e avvierà immediatamente le proprie verifiche:
- nel caso in cui non emergano anomalie, la Banca ti informerà tempestivamente di tale circostanza;
- nel caso in cui emergano anomalie, la Banca ti comunicherà tempestivamente che le verifiche effettuate hanno evidenziato delle anomalie e una potenziale frode/violazione della sicurezza e che, pertanto, è stato richiesto l'intervento della Polizia Postale, che avvierà la propria indagine. Il cliente dovrà comunque fornire conferma scritta della propria comunicazione mediante lettera raccomandata o fax entro le successive 48 ore. La Banca ti terrà costantemente informato sullo stato di avanzamento dell'indagine e ti comunicherà l'esito dell'incidente.

Hai smarrito oppure ti hanno rubato il cellulare certificato?
Cambia la password definitiva di accesso al sito direttamente dalla tua area riservata accedendo alla sezione "I MIEI DATI – Cambia password definitiva" e contatta il Servizio Clienti al numero 800.53.80.77 per informare la Banca dell'accaduto.

Non ricordi più la tua username?
Accedi alla sezione "ASSISTENZA - Contatta Operatore" con le credenziali di accesso TEMPORANEE in tuo possesso e un operatore del Team Conto Facto provvederà a comunicartela nuovamente in tempo reale tramite il servizio di messaggistica istantaneo.

Non ricordi più la password definitiva di accesso al sito?
Accedi alla sezione "ASSISTENZA - Contatta Operatore" con le credenziali di accesso TEMPORANEE in tuo possesso e un operatore del Team Conto Facto provvederà ad inviartene una nuova tramite SMS al numero di cellulare indicato in fase di registrazione.

Necessiti di assistenza relativamente alla sicurezza nei pagamenti?
Per qualsivoglia ulteriore domanda o richiesta di assistenza relativamente alla sicurezza dei pagamenti puoi rivolgerti al Servizio Clienti chiamando il numero 800.53.80.77 attivo dal lunedì al venerdì dalle 09:00 alle 17:45.

Necessiti di inviare un reclamo in materia di sicurezza nei pagamenti?
Per reclami relativi alla sicurezza nei pagamenti, puoi rivolgerti all'Ufficio Reclami della Banca, Viale Lodovico Scarampo, 15
20148 Milano,
fax: +39.02.49905.303
posta elettronica: reclami@bff.com
posta certificata: reclami@pec.bancafarmafactoring.it

4. Principali tipologie di frodi e attacchi informatici

La posta elettronica è lo strumento principale utilizzato per le frodi on-line. 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
Il "phishing" è una delle tecniche più diffuse di frode informatica ideata per compiere furti di identità digitale. Le truffe informatiche di questo genere, denominate phishing, consistono nella creazione e nell'uso di email o siti web apparentemente legati a istituzioni finanziarie e hanno possibilità di successo solo se i truffatori riescono ad appropriarsi delle credenziali personali di accesso, nonché di quelle dispositive dei titolari dell'home banking.

Le email di phishing contengono tipicamente un link che conduce a pagine web del tutto simili a quelle della banca, dove l'utente viene invitato ad inserire dati relativi al proprio conto. È possibile riconoscere le truffe via email con qualche piccola attenzione. Generalmente queste email:
- non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici);
- fanno uso di toni "intimidatori", ad esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'utente;
- promettono remunerazione immediata a seguito della verifica delle proprie credenziali di identificazione.

Social Engineering
Il "social engineering" consiste in tecniche impiegate per manipolare le persone allo scopo di ottenere informazioni (per esempio, via email o telefonate) o recuperare informazioni dai social network, per finalità fraudolente o per ottenere l'accesso non autorizzato a un computer o alla rete.

Malware
Il "malware" consiste in un programma informatico usato per disturbare le operazioni svolte da un dispositivo, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata.

5. Canale protetto e aggiornamenti in tema di sicurezza

La Banca invia le proprie comunicazioni periodiche per quanto riguarda l'uso corretto e sicuro dei servizi di pagamento via internet mediante il proprio sito internet. Bisogna, pertanto, diffidare da qualsiasi comunicazione a nome della Banca ricevuta tramite canali diversi, ad esempio tramite email.

La Banca riesamina e aggiorna il presente documento periodicamente, nonché in occasione di ogni modifica alle proprie procedure di sicurezza e in presenza di nuovi rischi emergenti significativi, di volta in volta individuati.
Ogni modifica e/o integrazione alla presente informativa viene comunicata al cliente mediante il suddetto canale protetto.