INFORMATIVA SULLA SICUREZZA CORPORATE E MOBILE BANKING

Credenziali di Sicurezza Personalizzate previste per Corporate e Mobile Banking destinati ai clienti "Business"

Per accedere al Corporate e Mobile Banking vengono richieste le seguenti Credenziali di Sicurezza Personalizzate:

- il Codice Postazione che è quello indicato nel contratto e inviato tramite email all'indirizzo riportato nel contratto stesso;
- il Codice PIN scelto dall'Utente con l'accortezza che non sia un codice di semplice intuizione né contenga riferimenti progressivi o identici;
- la Password scelta dall'Utente dopo l'accesso iniziale (al primo accesso è richiesta la password fornita dalla Banca e ricevuta tramite SMS). La Password non deve essere di semplice intuizione evitando riferimenti personali o familiari. E' inoltre necessario modificare periodicamente la password a tutela dell'Utente nonché per evitare il blocco del dispositivo trascorsi 180 giorni dall'ultima modifica,
- il codice OTP (One Time Password) generato dal Token Hardware assegnato dalla Banca all'Utente per autorizzare le disposizioni incluse quelle di pagamento.

L'Utente deve conservare le Credenziali di Sicurezza Personalizzate con cura, evitando di comunicarle o consegnarle a terzi.

Protocollo di sicurezza

Tutti i dati e le informazioni, su PC e App della Banca, sono protetti con il sistema più avanzato di crittografia SSL a 128 bit.

Per entrare nel sito della Banca deve essere sempre:

- verificato che la trasmissione dei dati sia protetta (presenza di un lucchetto chiuso sulla finestra del browser);
- verificato che sia presente il prefisso https://
- effettuato l'accesso dal sito istituzionale della Banca www.crvolterra.it evitando l'accesso da link diversi;
- verificato di non aver memorizzato la password sul sistema di navigazione.

Tentativi di accesso

Per la sicurezza e tutela dell'Utente, sono a disposizione tre tentativi consecutivi per la corretta digitazione della password o del PIN.
Al terzo tentativo errato l'applicativo viene bloccato dal sistema.
Il blocco del dispositivo può essere resettato dalla Banca.

Durata della sessione inattiva

Per la sicurezza e tutela dell'Utente, trascorsi 20 minuti di inattività, la connessione con la Banca decade ed apparirà un avviso di sessione scaduta.
Per rientrare deve essere nuovamente eseguito l'accesso.

Procedura di pagamento via Internet

Le disposizioni di pagamento disposte prevedono un'operatività progressiva:

- *inoltro*: operazione tramite la quale l'Utente predispone ed inserisce - con valorizzazione di tutti i campi obbligatori previsti - una disposizione;
- *salvataggio:* operazione – facoltativa – che permette di salvare la disposizione inserita prima dell'autorizzazione;
- *autorizzazione:* operazione che - tramite digitazione del codice OTP prodotto dal Token Hardware o Software - permette l'autorizzazione della disposizione. Con tale azione la disposizione viene trasmessa al servizio di riferimento della disposizione per la registrazione sul conto corrente e l'inoltro alla controparte;
- *esito:* la conferma dell'esecuzione della disposizione autorizzata viene comunicata all'Utente tramite email nonché resa visibile sul conto corrente con registrazione contabile.

Orientamenti per la sicurezza dei dispositivi

Si consiglia di dotare i propri dispositivi (PC, tablet, smartphone) con programmi Antivirus efficienti (per proteggerlo da virus, malware, browser o man in the middle, spyware, app non sicure e altre minacce) e Firewall (per proteggerlo da intrusioni indesiderate), non rispondere ad email sospette quali cd. "phishing" o SMS contenenti link cd "smishing "e di mantenere aggiornata la sicurezza di questi programmi.
Analoga cura deve essere seguita nella custodia dei dispositivi/codici autorizzativi (OTP)
I comportamenti, per limitare la possibilità di subire attacchi, debbono essere orientati alla conservazione con cura ed in luogo separato delle Credenziali di Sicurezza Personalizzate, nonché nell'evitare di aprire o rispondere ad email o sms sospetti o ricevuti da nominativi sconosciuti (nella quale vengono richieste TUTTE le informazioni personali).
In caso ricezione tramite mail di fatture sospette contattare sempre il proprio fornitore verificando l'IBAN di accredito.
In caso di comunicazione di variazione coordinate bancarie del fornitore, tramite mail, si prega di verificare direttamente con il fornitore la correttezza del'IBAN (in caso di frode la descrizione dell'intestazione del rapporto di accredito potrebbe non venire modificatam oer non destare sopsetti, mentre l'IBAN puo' essere stato modificato).

Procedura in caso di abuso riscontrato o sospetto

Nel caso di abuso riscontrato o sospetto, per evitare possibili ricadute negative in termini di sicurezza, l'Utente deve:

- eseguire in autonomia senza indugio il blocco del servizio digitando tre volte consecutive in maniera errata la password di accesso o, qualora impossibilitati, comunicare l'evento alla Banca od al soggetto terzo designato per l'esecuzione del blocco
- inviare senza indugio alla Banca segnalazione su (presunti) pagamenti fraudolenti, incidenti sospetti o anomalie durante la sessione per i servizi di pagamento via Internet accedendo al sito istituzionale della Banca alla sezione "Contatti" e compilando il form predisposto sotto la voce "Sicurezza pagamenti via Internet" o contattando la Banca.

La Banca, eseguiti i controlli del caso, fornirà risposta all'Utente direttamente nell'applicativo. **Procedura di segnalazioni di sicurezza**

I dispositivi (PC, tablet, smartphone) e le Credenziali di Sicurezza Personalizzate sono elementi interfunzionali.
Il possibile abuso, perdita o furto necessità da parte dell'Utente di immediate azioni volte a impedire l'utilizzo fraudolento.

- *perdita e furto delle Credenziali di Sicurezza Personalizzate:* l'Utente deve comunicare senza indugio il furto, lo smarrimento o furto delle Credenziali di Sicurezza alla Banca od al soggetto terzo designato;
- *perdita e furto dei dispositivi e tentativi di intrusione:* l'Utente deve comunicare senza indugio il furto, lo smarrimento o l'indebita intrusione dei propri dispositivi (PC, tablet, smartphone, token) alla Banca od al soggetto terzo designato a tutela della riservatezza delle informazioni e sicurezza del servizio.

Responsabilità dell'Utente e della Banca

Nell'uso del servizio di pagamento, l'Utente assume responsabilità:

- in mancanza di rispetto dei termini e delle condizioni contrattuali;
- in mancanza dell'immediata adozione di tutte le misure idonee a garantire la sicurezza del servizio e delle Credenziali di Sicurezza Personalizzate;
- sulla perdita derivante dall'utilizzo indebito del servizio conseguente al furto o smarrimento o uso non autorizzato delle Credenziali di Sicurezza Personalizzate per un importo comunque non superiore complessivamente a 50 euro, salvo il caso in cui abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la sicurezza delle Credenziali di Sicurezza Personalizzate;
- nella trasmissione dei dati tramite la rete Internet pubblica, per i quali assume piena e totale responsabilità, essendo a conoscenza dei rischi insiti nell'utilizzo dei dispositivi per usufruire del servizio;

nella trasmissione dei dati tramite contatto telefonico con sconosciuti, per i quali assume piena e totale responsabilità, essendo a conoscenza dei rischi insiti nella divulgazione a terzi di tali dati.
Nell'uso del servizio di pagamento, la Banca assume responsabilità:

- affinché l'Utente abbia sempre a sua disposizione strumenti adeguati per effettuare in modo efficace la notifica in caso di furto, smarrimento, appropriazione indebita o uso non autorizzato delle Credenziali di Sicurezza Personalizzate per il blocco del servizio e richiedere lo sblocco del servizio;
- sull'impedimento di qualsiasi uso del servizio dopo il blocco del servizio;
- sui rischi derivanti dalla spedizione delle Credenziali di Sicurezza Personalizzate;
- sui rischi connessi alla continuità operativa del servizio;
- sui rischi connessi alla sicurezza informatica del servizio.

Difesa dai Rischi

AVVISO EMAIL OPERAZIONI INTERNET
Il servizio invia automaticamente, per ogni disposizione impartita, email al riferimento presente nel contratto, in modo tale che l'Utente possa avere immediata evidenza delle operazioni disposte ed autorizzate dal canale.

AVVISO SMS PRINCIPALI OPERAZIONI SUL CONTO CORRENTE
Può essere richiesto il servizio di notifica a pagamento tramite SMS per la ricezione di un messaggio per le principali operazioni transitate sul conto corrente.

COMUNICAZIONI PERIODICA SULL'USO CORRETTO E SICURO DEL SERVIZIO
L'Utente sarà informato dalla Banca tramite avviso nel proprio applicativo internet sulle novità in materia di sicurezza del servizio.

CONTROLLO DELLA SITUAZIONE CONTABILE
E' necessario che l'Utente verifichi spesso – on line o tramite app – i movimenti del conto corrente per accorgersi di eventuali operazioni non conformi.

PROTEZIONE DEI DATI PERSONALI
Sulla rete Internet è meglio essere estremamente diffidenti nel consegnare i propri dati riservati senza essere certi dell'identità di chi li sta chiedendo.

Tentativi di "phishing", "smishing", "social engineering", "malware" e "vishing" sono sempre più diffusi.

Il "phishing" è una truffa informatica per carpire le Credenziali di Sicurezza Personalizzate attraverso false email, apparentemente provenienti dalla Banca, composte utilizzando logo, nome e il layout tipico dell'azienda imitata. Nella falsa email, ad esempio a causa di un imprecisato problema al sistema di "Corporate Banking", viene spesso richiesto di accedere all'home page del sito della Banca tramite un link da cliccare indicato nella email stessa. Procedendo e digitando le Credenziali di Sicurezza Personalizzate, qualcuno si impossesserà di tali dati.
Se ricevuta una email sospetta come quella appena descritta, non deve essere risposto né deve essere cliccato sui link presenti nella email. La email non deve essere aperta ma cestinata subito !

Lo smishing è una forma di phishing in cui un hacker utilizza un messaggio di testo convincente per indurre i vari destinatari a cliccare su un link e fornire delle informazioni private e riservate o a scaricare programmi dannosi su uno smartphone.

Il "social engineering " è una truffa informatica usata da chi che conosce alcuni elementi personali dell'Utente ma non tutti. Nascondendo la propria identità, viene carpita la fiducia dell'interlocutore (tramite email o via telefono) fino a ricavare le informazioni necessarie.

Il "malware" è un truffa informatica che prevede l'installazione di virus tramite software creati per causare danni più o meno gravi al dispositivo su cui viene installato, quali ad esempio la cattura delle Credenziali di Sicurezza Personalizzate e per modificare le disposizioni impartite. Tali software possono venire installati tramite Internet oppure aprendo email sospette (ad esempio fatture o promozioni) o inviate da nominativi sconosciuti. La soluzione più efficace è quella di installare sui dispositivi Antivirus efficienti e certificati. Tra i vari software i più comuni sono:
o *MITM (man-in-the-middle)* o *BITM (browser-in-the-middle)*: software usato per intercettare e per modificare i messaggi e la destinazione dei pagamenti tramite introduzione tra i server e le trasmissioni;
o Keylogger: software in grado di registrare tutto ciò che l'Utente digita su una tastiera o incolla;
o *Spyware*: software usato per raccogliere informazioni dal sistema dell'Utente e per trasmetterle ad un destinatario interessato;
o *Trojan horse*: software che contiene istruzioni che vengono eseguite all'insaputa dell'Utente;
o *Worm*: software che modifica il sistema operativo del sistema dell'Utente in modo da essere eseguito automaticamente;

Il "vishing" è una forma di truffa simile al phishing, basato su una comunicazione telefonica. Qualcuno simulando l'esistenza di un call center e qualificandosi come CRV, potrebbe richiedere, facendo leva sulla maggiore fiducia che si ripone in una persona autorizzata, di fornire i tuoi dati personali o codice autorizzativi per i più svariati motivi.

La Banca non richiede mai, direttamente o tramite terzi, informazioni personali o le Credenziali di Sicurezza Personalizzate per i servizi di Corporate e Mobile Banking.

Ecco alcune semplici regole per evitare di cadere in questo tipo di truffe:

- diffidare di qualunque email che richieda l'inserimento di dati riservati riguardanti le Credenziali di Sicurezza Personalizzate o altre informazioni personali;
- è possibile riconoscere le truffe via email con qualche piccola attenzione; generalmente:
  - 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;
  - non riportano una data di scadenza per l'invio delle informazioni.
- nel caso in cui venga ricevuta una email contenente richieste di questo tipo, non deve essere risposto né aperti gli allegati od i file eseguibili. L'email deve essere cestinata subito !
- non deve essere cliccato su link presenti in email sospette dato che i collegamenti potrebbero proseguire su di un sito contraffatto, difficilmente distinguibile dall'originale. Anche se sulla barra degli indirizzi del browser viene visualizzato l'indirizzo corretto, è bene non fidarsi: è possibile infatti visualizzare nella barra degli indirizzi del browser un indirizzo diverso da quello reale;
- diffidare inoltre di email con indirizzi web molto lunghi, contenenti caratteri inusuali, quali in particolare @ o con errori grammaticali;
- inserire i dati riservati esclusivamente in una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con "https://" e non con "http://" e nella pagina è presente un lucchetto chiuso;
- diffidare del cambio di modalità con la quale viene chiesto l'inserimento delle Credenziali di Sicurezza Personalizzate se non provenienti dal sito istituzionale: tramite pop-up, con dimensioni diverse, in lingua diversa;
- diffidare da email o telefonate non richieste da persone che chiedono informazioni dettagliate o complete. Spesso oltre le Credenziali di Sicurezza Personalizzate vengono richiesti anche tutti i riferimenti anagrafici, personali e comportamentali.