FOGLIO INFORMATIVO

3q - Servizi Telematici CRVONLINE PRIVATI offerto ai consumatori

Servizio offerto a chi desidera un canale Internet per l'esecuzione di operazioni a carattere informativo e dispositivo sui rapporti abilitati, compresa la negoziazione di valori.

INFORMAZIONI SULLA BANCA

CASSA DI RISPARMIO DI VOLTERRA S.p.A.
Sede Legale: Piazza dei Priori, 16/18 – 56048 Volterra (PI)
Tel.: 0588 91111- Fax: 0588 86940
Indirizzo e-mail: info@crvolterra.it
Sito internet: www.crvolterra.it
Codice ABI: 06370
Cap. Sociale € 101.364.400,00
C.F., P.IVA e numero iscrizione Registro Imprese di Pisa: 01225610508
Numero di iscrizione all'albo delle banche presso la Banca d'Italia: 5176.30
Aderente al Fondo Interbancario di Tutela dei Depositi e al Fondo Nazionale di Garanzia

COSA SONO I SERVIZI TELEMATICI

Struttura e funzione economica

Il servizio consente alla clientela, tramite l'utilizzo di un computer collegato alla rete internet, di visualizzare ed operare sui rapporti intrattenuti con la Cassa, impartire disposizioni di incasso e pagamento, negoziare valori mobiliari ed ottenere informazioni di natura finanziaria, effettuare ricariche di telefoni cellulari.

Il riconoscimento dell'utente viene effettuato tramite codici di accesso univoci, composti da un CODICE UTENTE e da una PASSWORD.

Per l'Accesso al servizio, il Cliente deve utilizzare il codice OTP semplice generato, in modo casuale e randomico, dal Token.

Per l'Autorizzazione delle operazioni a carattere dispositivo, il Cliente deve utilizzare, ove previsto, il codice OTP dinamico generato, in modo casuale e randomico, dal Token.

Principali rischi

Tra i principali rischi, vanno tenuti presenti:

- lo specifico rischio connesso ad eventuali mal funzionamenti e ritardi delle reti telematiche bancarie e/o interbancarie;
- l'utilizzo fraudolento, da parte di terzi, dei codici personali di accesso del cliente nel caso di smarrimento e/o sottrazione, con conseguente possibilità di utilizzo da parte di soggetti non legittimati. Pertanto il cliente dovrà osservare la massima attenzione nella custodia degli stessi, nonché la massima riservatezza nell'uso; nei casi di smarrimento e/o sottrazione, il cliente è tenuto a richiedere immediatamente il blocco dei servizi secondo le modalità contrattualmente previste.

PRINCIPALI CONDIZIONI ECONOMICHE

SPESE

CRVONLINE Privati BASE Applicativo monobanca e monoutente, riservato a clientela privata. Consente l'esecuzione di operazioni a carattere informativo e dispositivo compresa la negoziazione di valori mobiliari con visualizzazione delle quotazioni di borsa in differita in tecnologia Pull. Canone:	€ 5,16 mensile
CRVONLINE Privati PREMIUM Applicativo monobanca e monoutente, riservato a clientela privata. Consente l'esecuzione di operazioni a carattere informativo e dispositivo compresa la negoziazione di valori mobiliari con visualizzazione delle quotazioni di borsa in tempo reale in tecnologia Pull, inoltre sono disponibili due Watch List (tecnologia Push e Pull), una sezione di Analisi tecnica per il breve e medio termine e funzioni di Portafoglio virtuale personalizzabile dal Cliente. Canone:	€ 15,00 mensile
Il canone mensile decorre: • - per l'attivazione - dal mese successivo a quello di attivazione con cadenza trimestrale posticipata • - per la disattivazione - dal mese di disattivazione con cadenza mensile posticipata.	
Commissione per riproduzione o mancata restituzione Token	€ 15,00
Bonifico-SEPA - Giroconti da canale Home Banking	€ 0,30
Bonifico-SEPA Istantaneo - Giroconti da canale Home Banking	€ 0,30
Bonifico-SEPA su Filiali CRV - da canale Home Banking/terze parti PISP ed Ordine Permanente di bonifico da canale Home Banking	€ 0,55
Bonifico-SEPA Istantaneo su Filiali CRV - da canale Home Banking/terze parti PISP e Ordine Permanente di bonifico Istantaneo da canale Home Banking	€ 0,55
Bonifico-SEPA su Filiali altre Banche da canale Home Banking/terze parti PISP ed Ordine Permanente di bonifico da canale Home Banking	€ 1,65
Bonifico-SEPA Istantaneo su Filiali altre Banche da canale Home Banking/terze parti PISP ed Ordine Permanente di bonifico Istantaneo da canale Home Banking	€ 1,65
Bonifico extra-SEPA e Bonifico extra Sepa Istantaneo (servizio disponibile entro il 09/07/2027) da canale Home Banking (Rientrano nella categoria dei "bonifici extra-SEPA" e dei "bonifici extra Sepa Istantanei", le disposizioni di pagamento in arrivo ed in partenza che non sono riconducibili rispettivamente alla tipologia dei bonifici SEPA e dei bonifici Sepa Istantanei, in tutte le divise, compreso l'euro, senza soglie/limiti di importo e senza distinzione di provenienza o destinazione dei fondi).	1,5 per mille sul controvalore importo del bonifico min. € 8,00
Spese postali (incluso swift) per bonifici extra-SEPA e extra Sepa Istantanei	€ 20,00 per singolo ordine
Spese reclamate per bonifici extra-SEPA e extra Sepa Istantanei (si applicano solo per bonifici con tutte le spese a carico dell'ordinante - cosiddette spese tipo OUR)	€ 35,00 per singolo ordine
Tasso di cambio per bonifici extra-SEPA e extra Sepa Istantanei	cambio "durante" meno scarto di cambio ("spread") 0,25 per cento

Operazioni valutarie (trasferimento di divisa estero e/o Euro) e compensazioni	1,5 ‰, minimo € 8,00, sul controvalore dell'operazione
Trasferimenti in divisa tra residenti	1,5 ‰, minimo € 8,00, sul controvalore dell'operazione
N.B. per operazioni valutarie e in cambi si intendono tutte quelle operazioni (operazioni in titoli, vendite, acquisti, trasferimenti, ecc.) che comunque inneschino una causale valutaria.	
Cambi a pronti per acquisto e vendita del momento ('durante') quotati dalla Cassa, rilevati dall'agenzia di contribuzione dei dati (al momento TELEKURS), comprensivi dello scarto di cambio ("SPREAD"):	
"SPREAD" da applicare su ns. acquisti divisa	+0,25 per cento
"SPREAD" da applicare su ns. vendite divisa	- 0,25 per cento
Messaggi SWIFT	€ 20,00 a messaggio
Operazioni da/verso paesi estero soggetti a controlli rafforzati la Cassa si riserva di recuperare una spesa per il disbrigo delle attività amministrative per la gestione della singola pratica	€ 100,00
Le condizioni per messaggi SWIFT e operazioni da/verso paesi estero soggetti a controlli rafforzati non tengono conto della imposta di bollo e di eventuali particolari spese aggiuntive sostenute e/o reclamate da terzi che verranno sempre recuperate a parte.	
Pagamento Bollettino bancario da canale Home Banking	€ 0,00
Pagamento Bollettino postale da canale Home Banking	€ 0,40 (più il rimborso delle commissioni richieste da Poste Italiane)
Pagamento Delega F24 da canale Home Banking	€ 0,00
Pagamento MAV da canale Home Banking	€ 0,00
Pagamento RAV da canale Home Banking	€ 1,03
Pagamento Ricarica Carta Prepagata da canale Home Banking	€ 1,00
Pagamento Ricariche telefoniche da canale Home Banking	€ 0,00
Pagamento CBILL/PAGOPA da canale Home Banking	€ 1,50 (compreso le commissioni richieste dal Biller)

Per le ulteriori condizioni vedi relativo foglio informativo Servizio di Pagamento e incasso collegati al Conto Corrente offerto ai Consumatori, Time Deposit, Deposito titoli a custodia e o amministrazione

VALUTE

Canone	13° gg lav del mese successivo al trimestre di competenza
Commissione per riproduzione o mancata restituzione Token	Data esecuzione
Bonifico-SEPA e SEPA Istantaneo- Giroconti da canale Home Banking	Data esecuzione
Bonifico-SEPA da canale Home Banking/terze parti PISP ed Ordine Permanente di bonifico da canale Home Banking	Data esecuzione 1 giorno lavorativo antecedente la Valuta Fissa Beneficiario, se indicata. In ogni caso la data valuta addebito non può precedere la data esecuzione
Bonifico-SEPA Istantaneo da canale Home Banking/terze parti PISP ed Ordine Permanente di bonifico Istantaneo da canale Home Banking	Data esecuzione
Bonifici extra-SEPA da canale Home Banking	Data esecuzione

Bonifici extra-SEPA Istantanei da canale Home Banking	Data esecuzione
Pagamento Bollettino bancario da canale Home Banking	Data esecuzione
Pagamento Bollettino postale da canale Home Banking	Data esecuzione
Pagamento Delega F24 da canale Home Banking	Data esecuzione
Pagamento MAV da canale Home Banking	Data esecuzione
Pagamento RAV da canale Home Banking	Data esecuzione
Pagamento Ricarica Carta Prepagata da canale Home Banking	Data esecuzione
Pagamento Ricariche telefoniche da canale Home Banking	Data esecuzione
Pagamento CBILL/PAGOPA da canale Home Banking	Data esecuzione

RECESSO E RECLAMI

Recesso dal contratto

Si può recedere dal contratto in qualsiasi momento, senza penalità e senza spese di chiusura mediante comunicazione scritta da inviare alla Banca a mezzo raccomandata con ricevuta di ritorno o mezzo equipollente.
Se il contratto è concluso o integrato mediante tecniche di comunicazione a distanza e, pertanto, senza la presenza fisica e contemporanea del Cliente e del personale della Banca, il Cliente che riveste la qualità di Consumatore ha facoltà di esercitare il proprio diritto di ripensamento, e quindi di recedere dal contratto, entro 14 (quattordici) giorni dalla data di conclusione dello stesso oppure - se successivo - dal giorno in cui il Cliente riceve le condizioni contrattuali insieme alle informazioni richieste ai sensi del Codice del Consumo. Il Cliente può recedere, per tale motivo, senza penali e senza doverne indicare la ragione, mediante comunicazione scritta da inviare alla Banca a mezzo raccomandata con ricevuta di ritorno o mezzo equipollente.

Recesso in caso di modifica unilaterale delle condizioni contrattuali

Fatto salvo quanto diversamente specificato con riferimento alla modifica dei tassi nella prestazione dei Servizi di Pagamento, qualsiasi modifica unilaterale delle condizioni contrattuali (ivi incluse del Documento di Sintesi) è comunicata dalla Banca al Cliente mediante comunicazione scritta, su supporto cartaceo o su altro Supporto Durevole, contenente la formula “Proposta di modifica unilaterale del contratto”, con preavviso minimo di due mesi dalla data prevista per l’applicazione delle modifiche. In caso di modifica del tasso di interesse collegata a modifica del tasso di riferimento, le relative informazioni saranno fornite al Cliente mediante resoconto periodico, essendo rese pubbliche presso le dipendenze le variazioni dei tassi di riferimento.
Il Cliente che non intende accettare le modifiche proposte dalla Banca:
(a) deve comunicare espressamente alla Banca il proprio rifiuto entro la data prevista per l'applicazione delle modifiche, e
(b) ha il diritto di recedere dal contratto a cui sono state apportate le modifiche, senza spese prima della data prevista per l'applicazione delle modifiche stesse.
In tale caso, in sede di liquidazione del rapporto, il Cliente ha diritto all’applicazione delle condizioni precedentemente praticate.

Tempi massimi di chiusura del rapporto contrattuale

N° 30 giorni.

Reclami

Per eventuali contestazioni inerenti il presente rapporto tra Banca e clientela, il Cliente può presentare reclamo, inviando comunicazione scritta all’Ufficio Reclami della Cassa all’indirizzo Cassa di Risparmio di Volterra Spa - Ufficio Reclami - Piazza dei Priori, 16/18 56048 Volterra (PI) - o per via telematica tramite il sito web della Cassa www.crvolterra.it, sezione “Reclami”. L’Ufficio Reclami riscontrerà il reclamo così ricevuto, inviando comunicazione scritta al Cliente:

- entro 15 Giorni Lavorativi dal ricevimento di un reclamo riguardante la prestazione di Servizi di Pagamento. Con riferimento a tali tipologie di reclamo, qualora la Banca non possa rispondere entro il termine indicato per motivi indipendenti dalla sua volontà, invierà una risposta interlocutoria, indicando chiaramente le ragioni del ritardo nella risposta al reclamo e specificando il termine entro il quale il Cliente otterrà una risposta definitiva, non superiore ai 35 Giorni Lavorativi;

- entro 60 giorni dalla data di ricezione di un reclamo riguardante tematiche diverse dalla prestazione dei Servizi di Pagamento.

Se il reclamo è ritenuto fondato, la Cassa comunica al Cliente le iniziative che si impegna ad assumere ed i tempi entro i quali verranno realizzate.

Risoluzione stragiudiziale di controversie e Mediazione

In mancanza di risposta scritta da parte dell'Ufficio Reclami entro i termini stabiliti ai sensi di quanto precede, ovvero nel caso in cui la risposta ottenuta sia ritenuta insoddisfacente, il Cliente, ove ne ricorrano i presupposti, prima di ricorrere al giudice può rivolgersi all'ABF - Arbitro Bancario Finanziario. Per conoscere le modalità e la relativa disciplina attuativa emanata dalla Banca d'Italia consultare il sito www.arbitrobancariofinanziario.it. E' sempre possibile ottenere ulteriori indicazioni rivolgendosi direttamente alla Banca, che mette a disposizione dei clienti presso i propri locali e sul proprio sito internet le guide relative all'accesso all'ABF, ovvero chiedendo informazioni presso le sedi della Banca d'Italia aperte al pubblico.
In alternativa all'ABF o per le questioni che esulano la sua competenza, il Cliente, anche in assenza di preventivo reclamo alla Banca e prima di ricorrere all'autorità giudiziaria, può attivare -singolarmente o in forma congiunta con la Banca - una procedura di conciliazione finalizzata al tentativo di trovare un accordo. La domanda di mediazione è presentata mediante deposito di un'istanza presso un Organismo determinato ai sensi del Decreto Legislativo n. 28/2010 e successive modifiche e integrazioni.
In ogni caso, l'istanza di risoluzione stragiudiziale delle controversie ai sensi di una delle procedure precedentemente descritte costituisce condizione di procedibilità della eventuale domanda giudiziale.

INFORMATIVA SULLA SICUREZZA HOME E MOBILE BANKING

Credenziali di Sicurezza Personalizzate previste per Home e Mobile Banking destinati ai clienti "Privati"

Per accedere ed utilizzare l'Home e Mobile Banking vengono richieste le seguenti Credenziali di Sicurezza Personalizzate:

- il Codice Utente che è quello indicato nel contratto e inviato tramite email all'indirizzo riportato nel contratto stesso;
- 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) semplice generato dal Token assegnato dalla Banca all'Utente per l'accesso ai servizi;
- il codice OTP (One Time Password) dinamico generato dal Token assegnato dalla Banca all'Utente per autorizzare la disposizione, legando in maniera univoca il beneficiario e l'importo della disposizione (incluso quella di pagamento).

Dopo l'accesso iniziale, il servizio chiederà di rispondere ad almeno tre domande di sicurezza per permettere, in futuro, in caso di blocco del servizio, di poterlo riattivare in completa autonomia senza necessità di ricorrere al servizio di Assistenza della Banca.
L'Utente deve conservare le Credenziali di Sicurezza Personalizzate con cura, evitando di comunicarle o consegnarle a terzi.

Requisiti Hardware e Software del PC dell'Utente

I requisiti minimi per gli applicativi di Home e Mobile Banking sono i seguenti:

Home Banking

- Hardware: non previsti requisiti minimi

- Software: previsti i seguenti requisiti minimi
  - ✓ MICROSOFT INTERNET EXPLORER versione IE7 e superiori
  - ✓ CHROME versione 5 e superiori
  - ✓ FIREFOX versione 5 e superiori
  - ✓ OPERA versione 11 e superiori
  - ✓ SAFARI versione 4 e superiori

Mobile Banking

- Hardware Smarthphone e Tablet: non previsti requisiti minimi
- Software Smarthphone e Tablet Software: previsti i seguenti requisiti minimi
  - ✓ APPLE IOS SAFARI MOBILE versione 5 e superiori
  - ✓ ANDROID MOBILE GOOGLE CHROME versione 3 e superiori

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.
Al terzo tentativo errato l'applicativo viene bloccato dal sistema.
Il blocco del dispositivo può essere resettato dalla Banca o, se trattasi di un Home Banking "Privati", in autonomia dall'Utente tramite le risposte segrete di sicurezza.

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;
- *autorizzazione:* operazione che - tramite digitazione del codice OTP dinamico prodotto dal Token - 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

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” e mantenere aggiornata la sicurezza di questi programmi.
Analoga cura deve essere seguita nella custodia dei dispositivi.
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 sospette o ricevute da nominativi sconosciuti (nella quale vengono richieste TUTTE le informazioni personali).

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.

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 ALL'ACCESSO INTERNET
Può essere richiesto il servizio di notifica gratuito tramite SMS per la ricezione di un messaggio per ogni accesso effettuato al servizio di Home e Mobile Banking Privati.

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", "social engineering" e "malware" 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 "home 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 !

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;
La Banca non richiede mai, direttamente o tramite terzi, informazioni personali o le Credenziali di Sicurezza Personalizzate per i servizi di Home 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.

GLOSSARIO

Bonifico – SEPA	Con il bonifico la banca/intermediario trasferisce una somma di denaro dal conto del cliente a un altro conto, secondo le istruzioni del cliente, verso paesi SEPA.
Bonifico – extra SEPA	Con il bonifico la banca/intermediario trasferisce una somma di denaro dal conto del cliente a un altro conto, secondo le istruzioni del cliente, verso paesi non-SEPA.
Bonifico Sepa Istantaneo e Bonifico -extra SEPA Istantaneo	E' un bonifico SEPA e Extra SEPA che è eseguito immediatamente, 24 ore al giorno, in qualsiasi giorno di calendario con diponibilità immediata da parte del Cliente Beneficiario per un importo massimo tempo per tempo stabilito dall'Istituto
Cambio "durante"	Il tasso di cambio di una divisa reso disponibile da un fornitore al momento della consultazione
CRVONLINE	Applicativo che consente, tramite rete internet, l'esecuzione di operazioni a carattere dispositivo e informativo
CODICE UTENTE	Codice personale di accesso stabilito dalla Cassa

CODICE OTP semplice	Acronimo di One Time Password. Codice semplice generato dal Token e calcolato in modo casuale e randomico.
CODICE OTP dinamico	Acronimo di One Time Password. Codice dinamico univoco - che lega i beneficiari e gli importi delle disposizioni - generato dal Token e calcolato in modo casuale e randomico
Ordine permanente di bonifico	Trasferimento periodico di una determinata somma di denaro dal conto del cliente a un altro conto, eseguito dalla banca/intermediario secondo le istruzioni del cliente.
PASSWORD	Codice personale di accesso stabilito dal Cliente
Ricarica carta prepagata	Accreditamento di somme su una carta prepagata.
Spread	Scarto calcolato sul cambio di acquisto o vendita
Tasso di cambio (fonte di riferimento)	Indica la fonte di riferimento del tasso di cambio (ad esempio, listino cambi presso la filiale)
TOKEN	Dispositivo che genera l'OTP
Servizi di pagamento	Servizi che consentono di versare, trasferire, prelevare o ricevere somme di denaro a valere su un Conto di Pagamento, attraverso determinate modalità operative specificate nelle Condizioni per l'Erogazione dei Servizi di Pagamento. Rientrano, ad es., i servizi relativi ai prelievi e ai versamenti di contante, i bonifici, gli addebiti diretti (SDD), i pagamenti a mezzo di carte di debito, di credito o dispositivi analoghi. Non rientrano in tale definizione invece, le convenzioni di assegno nonché tutti i servizi che consentono operazioni di pagamento basati su uno dei seguenti tipi di documenti cartacei: assegni, effetti cambiari, voucher, traveller's cheque e vaglia postali.