FOGLIO INFORMATIVO

SERVIZI RAIFFEISEN ONLINE BANKING, CBILL e CBI

INFORMAZIONI SULLA BANCA

CASSA RAIFFEISEN CASTELROTTO - ORTISEI SOC. COOP.
VIA O.-V.-WOLKENSTEIN 9/A - 39040 - CASTELROTTO
Tel: 0471/711711
Fax: 0471/705375
E-mail: castelrotto.ortisei@raiffeisen.it
PEC: pec08056@raiffeisen-legalmail.it
Sito internet: www.raiffeisen.it/castelrotto-ortisei

Numero di iscrizione all'albo delle banche: 3650-9.0
aderente al Fondo di Garanzia dei Depositanti del Credito Coop. e al Fondo Nazionale di Garanzia di cui all'art. 62 del d.lgs. n. 415/96
Membro del sistema di tutela istituzionale Raiffeisen Südtirol IPS

CHE COSA È IL SERVIZIO RAIFFEISEN ONLINE BANKING, CBILL E CBI

Questi servizi consentono al Cliente di ottenere tramite internet informazioni e di usufruire di singoli servizi bancari in alternativa alla modalità ordinaria, operando direttamente a mezzo di apparecchiature compatibili con quelle all'uopo predisposte dalla Banca e collegate a proprie spese con la Banca.

Gli specifici servizi Raiffeisen Online Banking possono essere usufruiti per rapporti che il Cliente intrattiene presso la Banca stessa. Il servizio può essere sottoscritto anche in "versione light" con meno funzionalità.

Il servizi CBI del Consorzio Corporate Banking Interbancario consentono al Cliente di usufruire di una pluralità di funzioni rispetto ai rapporti intrattenuti presso qualsiasi Banca aderente all'accordo interbancario CBI.

Il servizio CBI - F24 riservato ai commercialisti e patronati consente a questi ultimi di inviare addebiti per pagamenti di F24 a valere sui conto correnti intestati ai clienti che gli hanno rilasciato specifica delega.

Il servizio CBILL consente al Cliente di visionare e di pagare le fatture emesse da un soggetto aderente a questo servizio.

L'utilizzo di questi servizi **presuppone** che il Cliente abbia delle conoscenze sufficienti per gestire in modo sicuro un accesso ad internet attraverso il proprio apparecchio (PC, Tablet, Smart-Phone).

I **principali rischi** legati a questi servizi consistono nel fatto che il Cliente, nonostante la Banca abbia adottato tutti i migliori accorgimenti della tecnica nota, può essere vittima di una frode informatica che provochi p.es. il furto delle credenziali, la cattura di schermate del PC, la modifica di pagine web per l'acquisizione fraudolenta della password e il controllo remoto del computer. Può succedere, inoltre, che sia impedito il regolare svolgimento delle attività previste dal Servizio a causa della temporanea interruzione o sospensione del Servizio stesso e che, pertanto, il Cliente si trovi nell'impossibilità di ricevere, inviare e/o elaborare i flussi per un certo periodo di tempo.

Al fine di **ridurre questi rischi**, a livello del Sistema Raiffeisen si ricorre a molteplici **misure di sicurezza** e alla messa a disposizione di **credenziali di autenticazione sicuri**. Inoltre **operano limiti dispositivi** che il Cliente può ridurre ulteriormente.
Si raccomanda al Cliente di attivare una delle seguenti misure di sicurezza:
"**SMS Alert**": Messaggi SMS al numero telefonico convenuto nei casi in cui viene effettuato l'accesso al servizio Raiffeisen Online Banking e/o vengono disposti bonifici in uscita.
"**E-Mail Alert**": E-Mail all'indirizzo E-Mail convenuto nei casi in cui viene effettuato l'accesso al servizio Raiffeisen Online Banking e/o vengono disposti bonifici in uscita.

Infine è in ogni caso necessario che il Cliente rispetti **le regole di comportamento** descritte nella "Guida per un utilizzo sicuro dei Servizi Raiffeisen Online Banking, CBILL e CBI".

CONDIZIONI ECONOMICHE

VOCI DI COSTO

	PREZZO
Spese fisse	
Raiffeisen Online Banking e CBI	
canone annuo CBILL incluso	0,00 euro
canone annuo CBILL e CBI incluso	0,00 euro

Momento limite giornaliero (cut-off)	
Momento limite del giorno operativo agli effetti della ricezione dell'ordine	
del Cliente in	
giorni operativi bancari (vedi contratto di conto corrente)	16:00:00 ore
giorni semifestivi (vedi contratto di conto corrente)	12:00:00 ore
per bonifici urgenti in	
giorni operativi bancari (vedi contratto di conto corrente)	15:00:00 ore
giorni semifestivi (vedi contratto di conto corrente)	11:00:00 ore
Bonifico istantaneo (SCT Instant Payment)	
Il bonifico può essere eseguito nel ROB ad ogni ora, a condizione che siano soddisfatti tutti i requisiti e che la banca destinataria abbia aderito a tale servizio. Questo bonifico SEPA non potrà essere revocato, in quanto il medesimo viene eseguito immediatamente.	

Help Desk	
negli orari d'ufficio della Banca	Tel. 0471 711711
fuori dagli orario d'ufficio	----------

RECESSO E RECLAMI

Recesso dal contratto
Le parti contraenti hanno facoltà di recedere dal contratto in qualunque momento, con preavviso di almeno un mese.
Qualora sussista un giustificato motivo ai sensi dell'articolo 33 comma 3 del decreto legislativo n. 206/2005 (Codice del Consumo), ovvero sia necessario tutelare l'efficienza e la sicurezza del Servizio, la Banca può recedere anche senza preavviso e dandone immediata comunicazione alla controparte.
Nel caso di recesso, sia della Banca che del Cliente, la Banca è tenuta ad effettuare il Servizio per tutti i flussi pervenuti entro il giorno lavorativo precedente la data di efficacia del recesso.

Tempi massimi di chiusura del rapporto contrattuale
La chiusura del rapporto coincide con la data di efficacia del recesso, salvo l'obbligo per il Cliente di precostituire i fondi motivatamente richiesti dalla Banca per chiudere partite eventualmente ancora sospese.

Reclami
Il Cliente può presentare un reclamo all'intermediario, anche per lettera raccomandata A/R o per via telematica (CASSA RAIFFEISEN CASTELROTTO - ORTISEI SOC. COOP., VIA O.-V.-WOLKENSTEIN 9/A, 39040 CASTELROTTO, PEC08056@RAIFFEISEN-LEGALMAIL.IT, CASTELROTTO.ORTISEI@RAIFFEISEN.IT, fax: 0471/705375).
Il Cliente rimasto insoddisfatto o il cui reclamo non abbia avuto esito nel termine di 60 giorni dalla sua ricezione ovvero, in caso di servizi di pagamento, entro 15 giorni lavorativi, può presentare ricorso all'Arbitro Bancario Finanziario (ABF) entro 12 mesi dalla presentazione del reclamo. Per ulteriori informazioni si consulti il sito www.arbitrobancariofinanziario.it, oppure si contatti una Filiale della Banca d'Italia o la Banca.
Il Cliente può - singolarmente o in forma congiunta con la Banca - attivare una procedura di conciliazione finalizzata al tentativo di trovare un accordo. Detto tentativo sarà esperito dall'Organismo di conciliazione bancaria costituito dal Conciliatore BancarioFinanziario - Associazione per la soluzione delle controversie bancarie, finanziarie e societarie - ADR (www.conciliatorebancario.it).
Qualora il Cliente intenda, per una controversia relativa all'interpretazione ed applicazione del contratto, rivolgersi all'autorità giudiziaria, deve preventivamente, pena l'improcedibilità della relativa domanda, avvalersi di uno dei procedimenti per la risoluzione stragiudiziale delle controversie (mediazione presso soggetto autorizzato, mediazione presso soggetto autorizzato e designato in contratto o citato procedimento presso l'Arbitro Bancario Finanziario-ABF); ciò ai sensi dell'art. 5 comma 1-bis del d.lgs. 28/2010. La procedura di mediazione si svolge davanti all'organismo territorialmente competente e con l'assistenza di un avvocato.

LEGENDA

App	Abbrevviazione di "applicazione"; indica un software informatico dedicato a dispositivi mobili come p.e. smartphone e tablet.
Banca Passiva	Banca che scambia i flussi con il Cliente tramite la Banca Proponente o Istituto di pagamento.

Banca Proponente	Banca che offre il Servizio CBI, ne garantisce la corretta erogazione, realizza e gestisce il collegamento ed il colloquio con il Cliente.
CBI	Marchio di Corporate Banking Interbancario.
CBILL	Denominazione del servizio di e-Billing offerto da Corporate Banking Interbancario.
Delega F-24	Disposizione di pagamento di tasse, imposte, premi e contributi previdenziali.
e-Billing	Abbreviazione del termine "electronic billing" ossia fattura trasmessa e pagata tramite canali telematici.
Lettore	Uno degli strumenti (credenziali di autenticazione) con i quali il Cliente si identifica nell'applicativo nei confronti della Banca.
Rete internet	Sistema di interconnessione tra pc che consente la trasmissione di informazioni in tutto il mondo.
Servizio CBI	Il servizio di "Corporate Banking Interbancario" che è costituito dalle Funzioni del Servizio pubblicate sul portale del Consorzio CBI (www.cbi-org.eu).

Raiffeisen

Guida per un utilizzo sicuro dei servizi Raiffeisen Online Banking, CBILL e C.B.I.

Il presente documento costituisce parte integrante del contratto relativo ai servizi Raiffeisen Online Banking, CBILL e C.B.I.

La Banca, nell'offrire i servizi per l'accesso telematico a rapporti bancari, adotta i migliori accorgimenti dell'attuale tecnologia e ricorre a molteplici misure di sicurezza e alla messa a disposizione di credenziali di autenticazione sicuri. Ciò nonostante permane la possibilità che il Cliente possa subire una frode informatica. Pertanto, oltre alle misure di sicurezza adottate dalla Banca, è necessario che il Cliente abbia delle conoscenze sufficienti per gestire in modo sicuro l'accesso ad internet attraverso il proprio apparecchio.

Il principale rischio del servizio consiste nel fatto che il Cliente possa essere vittima di un attacco informatico realizzato verso il dispositivo utilizzato dal Cliente stesso che provochi p.es. il furto delle credenziali, la cattura di schermate del PC, la modifica di pagine web per l'acquisizione fraudolenta della password ed il controllo remoto del computer.
Può, infatti, succedere che il Cliente riceva un messaggio di posta elettronica che imiti la grafica del sito bancario. Questa E-mail, che ha come unico scopo quello di ottenere la password che autorizza i pagamenti, invita il destinatario a seguire un link, presente nel messaggio, che però non porta al sito web ufficiale della Banca, bensì ad una copia fittizia apparentemente simile al sito ufficiale, situata sul server controllato da un altro soggetto. Tale tipo di truffa via internet, detta "phishing", può essere realizzata anche mediante l'invio di SMS. Al riguardo si fa presente che la Banca non invia mai delle comunicazioni (e-mail o SMS) nelle quali invita il Cliente ad inserire le sue credenziali di autenticazione.

Vi sono, inoltre, diverse forme di attacco che mirano a fare entrare un malware (c.d. Banking Trojan) nel computer. Ciò può avvenire attraverso le più svariate vie, come p.es. tramite una e-mail con allegati, un link contenuto in una e-mail diretto ad un sito web infettante ovvero semplicemente consultando dei siti web infetti (c.d. drive-by-download). Di solito il Banking Trojan viene installato definitivamente sul disco rigido del computer. Vi sono però anche altre varianti del malware che si trovano nella memoria operativa del computer e che, pertanto, non lasciano tracce rivelatrici sul disco rigido. Una volta che il malware è divenuto attivo sul PC, l'organizzazione criminale può ricorrere a diverse tecniche per raccogliere illecitamente dati, tra cui p.es. l'intercettazione dei campi di inserimento (p.es. della password o dei dati della carta di credito), la rappresentazione di siti web falsificati, il blocco dell'accesso al Servizio, la modifica degli abbinamenti tra il dominio e l'indirizzo IP, la disattivazione di antivirus installati, la modifica dei dati inseriti (p.es. nel corso di un bonifico) e addirittura l'accesso in remoto al computer.

Per tali motivi è necessario adottare tutte le misure precauzionali che permettono di evitare l'effettuazione di operazioni in un ambiente infetto ove vi sia il potenziale pericolo di presenza di malware. Si sconsiglia di compiere un'operazione con un dispositivo non conosciuto (p.es. utilizzo di un PC in un Internet café). Qualora l'accesso ai servizi telematici venga effettuato da un proprio dispositivo elettronico, prima di effettuare l'operazione online, bisogna verificare che il dispositivo abbia un sistema operativo aggiornato con tutte le patch di sicurezza, le ultime versioni di software utente (p.es. Acrobat Reader) e un antivirus costantemente aggiornato.

I requisiti citati costituiscono precauzioni e strumenti di minima, irrinunciabili per un'efficace difesa contro possibili attacchi informatici. Inoltre è importante che il Cliente fornisca la massima collaborazione alla propria Banca ed aiuti, soprattutto nel proprio interesse, a prevenire gli attacchi suddetti, rispettando le seguenti regole di comportamento.

La Banca può negare l'accesso al Servizio se il dispositivo del Cliente non soddisfa i requisiti tecnici minimi indicati nel Manuale tecnico.

In generale, occorre:
- dotarsi di un antivirus attivo e costantemente aggiornato e di appositi firewall;
- accedere al servizio da postazioni proprie e periodicamente controllate;
- proteggere la propria postazione con una password di almeno 8 caratteri, non agevolmente

riconducibili alla persona e sostituire la stessa almeno ogni 6 mesi;
- controllare regolarmente gli estratti conto e le operazioni eseguite tramite i servizi internet.

Con riguardo all'utilizzo del servizio, è necessario:
- custodire e utilizzare le credenziali di autenticazione con la massima accuratezza;
- non conservare insieme i diversi elementi delle credenziali di autenticazione;
- non cedere le credenziali di autenticazione a terzi;
- denunciare tempestivamente il furto, lo smarrimento, la distruzione o un qualsiasi altro uso non autorizzato dello strumento di pagamento e/o delle credenziali di autenticazione;
- prestare massima attenzione ai diversi metodi di potenziale attacco informatico tra cui le cosiddette E-mail civetta, le false comunicazioni di scadenza, l'invito a seguire un certo link.

Si raccomanda la verifica degli accessi e delle operazioni tramite il servizio SMS-Alert e/o e-mail-Alert.

Al momento dell'accesso al servizio è necessario:
- seguire le istruzioni fornite dalla Banca nel Manuale tecnico;
- verificare costantemente la presenza dell'acronimo di protocollo "https" e il simbolo della chiavetta nella stringa operativa, che sono quelli di una pagina web protetta e che si distinguono dall'acronimo di protocollo "http";
- astenersi da un ulteriore utilizzo del servizio e darne immediata comunicazione alla Banca - anche attraverso il numero verde pubblicato sul sito - se si notano irregolarità o malfunzionamenti del sistema;
- chiudere l'applicazione cliccando sull'apposito pulsante ("uscita") una volta terminate le operazioni.

Per le aziende è, inoltre, necessario:
- accedere al servizio da postazioni gestite professionalmente;
- definire e divulgare una policy aziendale in materia di sicurezza informativa relativamente all'utilizzo dei servizi internet banking;
- definire per iscritto gli utenti da abilitare all'utilizzo del servizio internet banking e gestire i loro profili d'accesso;
- avviare periodicamente iniziative di informazione e/o di formazione all'interno dell'azienda in materia di sicurezza rivolte agli utenti abilitati al servizio internet banking;
- comunicare agli utenti abilitati i canali di comunicazione con la Banca per poter gestire più rapidamente le anomalie/inefficienze riscontrate nello svolgimento delle operazioni in modo da avere tempestive indicazioni su come comportarsi e su come prendere opportuni provvedimenti in relazione a quanto riscontrato;
- limitare la navigazione sul web e la possibilità di installare programmi dei quali non è possibile verificare la provenienza;
- differenziare i profili degli utenti in base alle specifiche esigenze operative e limitare/eliminare i diritti di amministratore sulle singole postazioni - in alternativa svolgere tutte le movimentazioni bancarie da un PC dal quale sono particolarmente controllati e profilati l'utilizzo della posta elettronica e la navigazione in rete;
- rispettare le misure minime di sicurezza prescritta dalla normativa in materia di privacy.