La sicurezza di Online Banking: dipende da voi!

Rendete la vita diffi cile ai malintenzionati, osservando scrupolosamente le seguenti norme di sicurezza!
Pensate alla circolazione stradale: non basta essere al volante di un'auto sicura. Per muoversi senza correre rischi, sono necessari anche una guida attenta, la perfetta conoscenza delle insidie presenti sulla strada e il rispetto delle regole del traffi co. Lo stesso vale per internet: solo la combinazione di sicurezza della tecnologia Raiffeisen, consapevolezza dei rischi e comportamento responsabile da parte dell'utente può garantire un livello ottimale di sicurezza.

Ecco come rendere sicuro il vostro computer:

» Installate un programma **antivirus** e tenetelo costantemente aggiornato. Vi consigliamo di utilizzare ROL Secure, che ha previsto una speciale protezione per l'home banking.

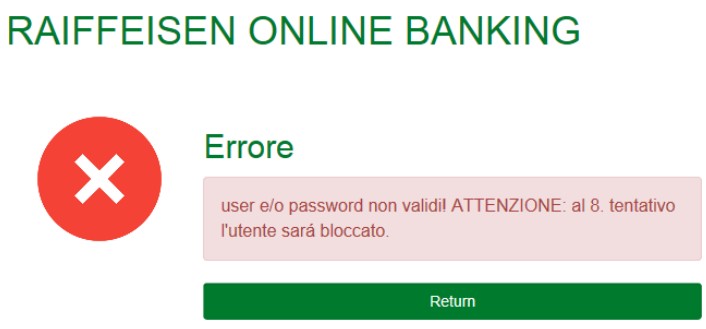
» Prestate sempre attenzione agli ultimi **aggiornamenti sulla sicurezza** per il vostro sistema operativo, il vostro browser e gli altri software, installandoli immediatamente.

» Siate cauti con i **fi le e i link** presenti su internet o inviati in allegato a un'e-mail: aprite solo quelli provenienti da fonti affi dabili. In caso di dubbio, non esitate a chiedere spiegazioni al mittente.

» **I programmi disponibili su internet** possono essere stati contraffatti. Per questo, acquistate il software (ad es. browser, protezioni antivirus, ecc.) solo dai siti internet dei produttori o direttamente nei negozi specializzati.

» Siate particolarmente **prudenti quando utilizzate computer pubblici** (ad es. in hotel, negli internet café), evitando l'immissione di dati confi denziali.

Se sbagliate a digitare:
Se immettete una password sbagliata, comparirà esclusivamente l'avviso riportato.



In caso di aviso diverso, vi raccomandiamo di non eseguire alcuna operazione con il Vostro computer e di rivolgervi immediatamente a noi.

Come riconoscere una possibile minaccia:

Il vostro computer è già infettato o siete stati attirati con l'inganno su un sito internet contraffatto?

» Osservate il vostro browser durante l'utilizzo di Raiffeisen Online Banking: la pagina visualizzata nella barra degli indirizzi al momento dell'accesso deve iniziare sempre con http**s**://. La **"s"** indica che la connessione è sicura. Non digitate mai dati confi denziali, se non è presente questa **"s".**

» Prima d'inviare un bonifi co, verifi cate ulteriormente i dati visualizzati. Se notate qualche anomalia rispetto a quelli appena digitati, informate immediatamente la vostra banca.

» Il vostro Raiffeisen Online Banking riporta sempre data e ora dell'ultimo login. Verifi cate che questi dati siano corretti.

» La vostra banca non vi chiederà mai di fornire per e-mail la password o altri dati d'accesso. Per nessuna ragione comunicate a terzi queste informazioni e non rispondete alle e-mail che, in caso di mancata risposta, minacciano conseguenze negative, come il blocco del conto.

» In ogni caso, se avete dubbi o vi salta all'occhio qualche anomalia, non esitate a contattarci.

» Attivate il servizio informativo alert-SMS di Raiffeisen Online. Sarete avvisati ogni volta che viene eseguita una determinata transazione così che, in caso di accesso non autorizzato al vostro conto, possiate intervenire tempestivamente!
» Verifi cate costantemente l'estratto conto e segnalate eventuali irregolarità o dubbi.

Cos'altro c'è da sapere…

» Al momento dell'accesso al Raiffeisen Online Banking l'autorizzazione di una transazione viene richiesto una password.

» Se avete il sospetto che la password sia fi nito nella mani sbagliate, potete disattivarla attraverso la nuova immissione di una password rigenerato. Se possibile, la nuova password dev'essere digitata su un dispositivo diverso.

Siamo a disposizione:
la vostra Cassa Raiffeisen e il centro servizi
tel.: 800 031 031
e-mail: info@raiffeisen.it

Raiffeisen Meine Bank

Guida per un utilizzo sicuro dei Servizi 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.

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;

Siamo a disposizione:
la vostra Cassa Raiffeisen e il centro servizi
tel.: 800 031 031
e-mail: info@raiffeisen.it

Raiffeisen Meine Bank

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

• 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 (p.es. se vengono richiesti più password);

• astenersi dal generare un secondo o terzo password in quanto il primo vale fino all‘accettazione da parte del sistema Raiffeisen;

• 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 movimen tazioni 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 (decreto legislativo n. 196/2003 - allegato B).

Siamo a disposizione:
la vostra Cassa Raiffeisen e il centro servizi
tel.: 800 031 031
e-mail: info@raiffeisen.it

Raiffeisen Meine Bank