SICUREZZA DEI PAGAMENTI VIA INTERNET

I Clienti Carifermo hanno la possibilità di effettuare pagamenti su internet attraverso:

- il portale di Internet Banking "**Carifermonline**", destinato alla clientela privata, che consente di disporre dei vari servizi di pagamento e di accedere al servizio di trading online. Al portale è possibile accedere sia da web che da APP "Carifermo Mobile";
- il portale di Internet Banking "**Prima Web**", destinato alla clientela imprese, che consente di effettuare tutte le operazioni previste dal circuito Corporate Banking Interbancario (CBI) ed una serie di funzionalità informative e dispositive sui rapporti Carifermo;
- la carta di debito "**Carifermo Pay Internazionale**", nelle versioni e-commerce e contactless, che può essere utilizzata per acquisti sui siti di commercio elettronico, convenzionati con il circuito Maestro.

I canali per i pagamenti via internet messi a disposizione dalla Carifermo sono sicuri, ma è importante che l'utente conosca i rischi del web e metta in atto alcuni accorgimenti al fine di ridurre i rischi di frode.

Per i pagamenti effettuati attraverso le Carte di Pagamento Nexi (Credit, Prepaid e Debit), si rimanda al documento sulla sicurezza dei pagamenti fornito al momento del collocamento della carta e disponibile anche sul sito www.nexi.it, nonché ai regolamenti tempo per tempo vigenti e disponibili anch'essi sul sito www.nexi.it.

COME PROTEGGERE IL PROPRIO DISPOSITIVO DI ACCESSO AD INTERNET

L'accesso ad Internet può avvenire da differenti dispositivi (PC, smartphone e tablet) per i quali è necessario ridurre il rischio di attacco da virus o malware, che sarebbero in grado di acquisire informazioni, dati personali ed il controllo del dispositivo.

Lato utente, mettere in atto alcune semplici regole di comportamento permette di operare con una maggior sicurezza:

- installare un software antivirus e tenerlo costantemente aggiornato;
- tenere costantemente aggiornato il browser utilizzato per la navigazione in Internet (Microsoft Edge, Google Crome, Firefox, ecc.) all'ultima versione disponibile;
- utilizzare sistemi in grado di prevenire attacchi ed intrusioni quali, ad esempio programmi antispyware, firewall, antispam, antiphishing;
- non installare software scaricato da Internet proveniente da fonti non affidabili;
- non aprire link, file scaricati da Internet o allegati di posta elettronica di cui non si conosce la provenienza;
- diffidare delle e-mail di mittenti sconosciuti che spesso contengono messaggi impersonali; è consigliabile non aprirle ma cancellarle, senza aprire allegati o senza cliccare su link in esse contenuti;
- evitare di utilizzare programmi di "file sharing", in quanto impediscono di tracciare la provenienza dei files;
- non autorizzare attività di controllo remoto da parte di soggetti non affidabili;

- non utilizzare né la modalità di memorizzazione automatica delle password né quella di completamento automatico dei form, soprattutto se il dispositivo utilizzato per l'accesso ad Internet viene utilizzato da più persone; tutti i browser (Microsoft Edge, Google Crome, Firefox, ecc.) consentono di disattivare queste funzioni.

COME PROTEGGERE LE CREDENZIALI DI ACCESSO E DI DISPOSIZIONE DI PAGAMENTO

All'attivazione di un rapporto di Internet Banking (Carifermonline o Prima Web), ad ogni Cliente viene assegnato un identificativo utente (user id) ed una password, che rappresentano le credenziali di accesso al servizio. La password per il primo accesso viene assegnata dalla Banca sotto forma di un PIN (valido solo per il primo accesso), che dovrà essere sostituito con una password definita direttamente dal Cliente.
In fase di accesso al servizio, anche se si dispone di un IB informativo, è necessario un ulteriore codice di autenticazione (c.d. SCA - Strong Customer Authentication), che può essere di varia natura (OTP "one time password", dati biometrici, notifica su APP, ecc.) e generato da differenti dispositivi messi a disposizione dalla Banca (Token fisico, Secure Call, MobileToken).
Per quanto riguarda le autorizzazioni delle disposizioni di pagamento, è necessario un codice legato dinamicamente all'importo della transazione da eseguire e al beneficiario del pagamento stesso, che può essere generato da differenti dispositivi messi a disposizione dalla Banca (Token fisico, Secure Call, Mobile Token, SMS).

I codici di accesso e di disposizione di pagamento sono strettamente personali e devono essere utilizzati esclusivamente dall'utente a cui sono stati assegnati o che li ha definiti; pertanto è consigliabile:

- effettuare prima possibile il primo accesso, utilizzando il PIN consegnato dalla Banca, ed impostare una password di propria scelta;
- cambiare frequentemente la password di accesso, anche prima della sua scadenza;
- custodire con cura i codici di accesso per evitare che altre persone ne vengano a conoscenza;
- evitare di portare con sé i codici di accesso trascritti su carta o memorizzati su smartphone, per evitare che possano essere sottratti o smarriti;
- non comunicare a nessuno i codici, anche se richiesti telefonicamente o via mail;
- nel caso in cui si utilizzi il dispositivo Token, custodirlo con la massima cura;
- nel caso in cui si utilizzi un sistema di autenticazione legato al numero di cellulare (Secure Call) o allo smartphone/tablet (APP Carifermo Mobile), segnalare immediatamente la perdita di possesso o l'utilizzo non autorizzato del dispositivo e richiedere all'Assistenza Clienti Carifermo il blocco del servizio.

Alcuni consigli per creare una password sicura:

- definire una password di lunghezza adeguata, superiore agli otto caratteri obbligatori;
- usare lettere minuscole e maiuscole, cifre e caratteri speciali (come @#$%^&);
- non usare parole banali (es. "password", "1234") o il proprio user id;
- non usare parole comuni o che possono essere facilmente identificate, come, ad esempio nomi di familiari, date di compleanno o altri dati personali, ecc.;

- non riutilizzare password già impiegate per la registrazione su altri siti internet.

Si evidenzia che i dipendenti ed i collaboratori della Carifermo non sono a conoscenza della password di accesso al servizio di Internet Banking o dei codici generati dai sistemi di autenticazione, e non hanno la necessità di averne visione; pertanto la Banca non richiederà mai all'utente queste informazioni.

COME UTILIZZARE IN SICUREZZA IL PORTALE DI INTERNET BANKING

Di seguito si riportano alcuni semplici consigli su come accedere in maniera sicura ai servizi Carifermonline o Prima Web dal proprio PC, tablet o smartphone tramite browser (Microsoft Edge, Google Crome, Firefox, ecc.):

- accedere da postazioni o terminali mobili di cui si conosce il grado di sicurezza, evitando l'utilizzo di postazioni condivise (es. internet cafè);
- accedere ai servizi di Internet Banking direttamente dal sito www.carifermo.it, evitando di usare altri link, ad esempio contenuti in e-mail, SMS o banner pubblicitari;
- verificare che nel momento in cui viene chiesta la password di accesso al portale il browser indichi nella barra dell'indirizzo:
    - il sito www.banking4you.it, (per Carifermonline) o il sito www2.csebo.it (per Prima Web), gestiti da CSE - Consorzio Servizi Bancari scarl;
    - il protocollo "https" ed il lucchetto verde, che garantiscono che la connessione al sito è sicura;
- al termine della sessione di lavoro sul portale di Internet Banking, chiudere sempre cliccando sul pulsante “Esci” e chiudere il browser; il consiglio è particolarmente importante se si sta accedendo da una postazione che viene utilizzata da più persone.

Per gli utenti di Carifermonline: nel caso di accesso da smartphone o tablet è consigliabile utilizzare l'APP Carifermo Mobile, scaricabile da Google Play o Huawei AppGallery (versione Android) e da Apple Store (versione IOS).

COME UTILIZZARE IN SICUREZZA L'APP CARIFERMO MOBILE

L'APP Carifermo Mobile garantisce la massima protezione in caso di utilizzo del servizio di Internet Banking Carifermonline da dispositivo mobile. Tuttavia è necessario osservare comportamenti adeguati per evitare di ridurre involontariamente il livello di sicurezza del servizio, come:

- non registrare le credenziali di accesso o il Mobile PIN (MPIN) del sistema di autenticazione Mobile Token nella rubrica contatti, in documenti salvati sul dispositivo o altre APP;
- non permettere ad altre persone di utilizzare il dispositivo;
- se si utilizza l'autenticazione con impronta digitale (es. Touch ID) o con riconoscimento facciale (es. Face ID), verificare preventivamente che nelle impostazioni del sistema operativo non siano registrate impronte o volti di altre persone. In caso contrario, è consigliabile non attivare questa funzionalità;
- se si scaricano documenti dall'APP (ad esempio estratti conto) nelle memorie del dispositivo, evitare di condividerli e cancellarli quando non sono più necessari; considerare

che potrebbero essere acceduti da APP non affidabili o salvati in automatico su servizi cloud.

COME RICONOSCERE I TENTATIVI DI PHISHING

Il phishing è un tipo di truffa effettuata su Internet attraverso la quale, generalmente attraverso messaggi di posta elettronica, un soggetto cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile. Questi messaggi fraudolenti imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi e richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio.

A volte le e-mail di phishing:

- sembrano provenire dalla propria Banca o comunque da Banche con cui non si hanno rapporti;
- contengono errori grammaticali, frasi sconnesse o incomprensibili;
- adducono motivazioni generiche o improbabili;
- fanno riferimento a presunti problemi di sicurezza o al fatto che i rapporti o i mezzi di pagamento sono stati bloccati o stanno per esserlo.

La Banca non invia in nessun caso ai propri Clienti messaggi di posta elettronica o SMS contenenti richieste di informazioni riservate o link al portale di Internet Banking.

Quando si riceve un messaggio di posta elettronica che si sospetta essere un tentativo di phishing, per evitare conseguenze basta seguire alcune semplici regole:

- evitare di aprirlo e cancellarlo;
- evitare tassativamente di aprire o eseguire gli allegati in esso contenuti, che potrebbero installare programmi (malware) in grado di rubare informazioni personali o monitorare l'attività dell'utente;
- non cliccare sui link presenti nel testo, che possono far accedere a siti internet contraffatti che solo nell'aspetto sono identici a quello della Banca ma il cui unico scopo è sottrarre le password di accesso dell'utente;
- non inserire mai le proprie credenziali (nome utente e password) o i codici generati dai sistemi di autenticazione sul sito che si apre dopo aver cliccato sui link presenti nella mail.

Nel caso si sospetti che la propria password sia stata compromessa, contattare prima possibile il servizio di Assistenza Clienti Carifermo per il blocco del servizio.

COSA FARE IN CASO DI SOSPETTA FRODE

L'utente deve prestare attenzione ad alcuni segnali o eventi che possono far sospettare un tentativo di frode:

- è possibile rilevare eventuali operazioni non riconosciute controllando regolarmente i movimenti del proprio conto corrente;
- è possibile rilevare eventuali accessi fraudolenti controllando la data e l'ora dei precedenti accessi effettuati.

  - Carifermonline: funzione ALTRI SERVIZI / ULTIMI ACCESSI;
  - Prima Web: funzione FUNZIONI UTENTE / INFOLOGIN e IB / ALTRI SERVIZI / ULTIMI ACCESSI; gli utenti che non hanno abilitata quest'ultima funzione possono richiederne l'attivazione rivolgendosi alla propria filiale Carifermo;
- Nell'utilizzo del portale di Internet Banking prestare attenzione ad eventuali modalità operative diverse da quelle consuete, soprattutto in fase di inserimento dei dati personali o di codici di accesso/autorizzativi;
- fare attenzione se appaiono richieste di inserimento dei codici generati dai sistemi di autenticazione che possono provenire da software malevoli installati ad insaputa dell'utente. Infatti, secondo l'utilizzo corretto, l'inserimento del codice viene richiesto solo:
  - all'accesso al servizio, dopo aver inserito correttamente user id e password;
  - nella fase della conferma di una disposizione di pagamento (es. bonifico, ricarica telefonica, ecc.);
- verificare gli alert di sicurezza (servizi opzionali) inviati dalla Banca via SMS o e-mail, a fronte di operazioni effettuate su Internet Banking o con carte di debito.

In caso di sospetta frode o compromissione della postazione utilizzata per l'accesso al servizio di Internet Banking, l'utente deve rivolgersi appena possibile all'Assistenza Clienti Carifermo, telefonicamente o per e-mail.
Nel caso in cui la Banca, nell'ambito dei controlli effettuati sull'operatività tramite Internet Banking, abbia evidenza di una operatività sospetta, gli operatori dell'Assistenza Clienti contatteranno telefonicamente il Cliente per le necessarie verifiche.

COME AUMENTARE IL LIVELLO DI SICUREZZA DEI SERVIZI DI PAGAMENTO VIA INTERNET MESSI A DISPOSIZIONE DALLA BANCA

È vivamente consigliato agli utenti utilizzare tutti gli strumenti che la Banca mette a disposizione per ottenere il massimo livello di sicurezza nei pagamenti su internet.

Internet Banking Carifermonline con profilo dispositivo

- Personalizzazione di limiti massimi di importo (giornaliero, mensile e per operazione) e di numero di operazioni giornaliere, previsti su alcune tipologie di operazioni dispositive (escluse operazioni disposte sul Corporate Banking Interbancario). Al momento dell'attivazione del servizio il Cliente può accettare i massimali standard proposti dalla Banca o definirli in base alle proprie esigenze.
  Successivamente i massimali possono essere ridotti direttamente dal Cliente utilizzando le funzionalità del portale di Internet Banking. Per aumentarli, invece, è necessario rivolgersi alla propria Filiale Carifermo.
- Servizio di alert via SMS o e-mail, che avvisa il Cliente nel momento in cui autorizza un'operazione di pagamento; è previsto su alcune tipologie di operazioni dispositive (bonifico SEPA, bonifico estero, versamento con bollettino postale, pagamento tramite MyBank), di importo superiore alle soglie preimpostate. Gli alert di sicurezza possono essere attivati direttamente dall'utente utilizzando le funzionalità del portale di Internet Banking.

Internet Banking Prima Web

Servizio di alert via SMS o e-mail, che avvisa il Cliente nel momento in cui autorizza un'operazione di pagamento; è previsto su alcune tipologie di operazioni dispositive (bonifico, versamento con bollettino postale, pagamento tramite MyBank, distinta di bonifici SEPA o estero), di importo superiore alle soglie preimpostate. Gli alert di sicurezza possono essere attivati rivolgendosi all'Assistenza Clienti oppure direttamente alla propria Filiale Carifermo.

Carte di debito

- Servizio di alert via SMS, che avvisa il titolare della carta nel momento in cui effettua un prelevamento da ATM o un'operazione di pagamento tramite POS o su internet, se di importo superiore alle soglie concordate con la Banca; è previsto su tutte le carte di debito emesse da Carifermo, da richiedere in Filiale.
- Servizio 3D Secure e codice Key6, per l'utilizzo della carta "Carifermo Pay Internazionale" (collocata dalla Banca da luglio 2015) sui siti di commercio elettronico che espongono il marchio MAESTRO; per l'attivazione è necessario utilizzare il servizio di Internet Banking Carifermonline.

Per qualsiasi informazione su come attivare questi strumenti, è possibile rivolgersi all'Assistenza Clienti oppure direttamente alla propria Filiale Carifermo.

COMUNICAZIONI DA PARTE DELLA BANCA

La Carifermo avrà cura di tenere periodicamente aggiornati i propri Clienti circa il tema della sicurezza dei pagamenti via Internet, attraverso:

- il proprio sito www.carifermo.it (Home / PERSONE E FAMIGLIE / CONTI CORRENTI E SERVIZI / Servizi digitali / Sicurezza sui canali digitali);
- le comunicazioni allegate agli estratti conto o altri documenti inviati in formato cartaceo o elettronico;
- la gestione messaggi, riservata ai clienti che utilizzano gli applicativi
    - Carifermonline: icona con casella email in alto a destra, sotto il nome utente;
    - Prima Web: funzione IB / ALTRI SERVIZI / COMUNICAZIONI; gli utenti che non hanno abilitata tale funzionalità possono richiederne l'attivazione rivolgendosi alla propria Filiale Carifermo.

  La gestione messaggi è un canale sicuro: per accedervi è necessario entrare nel portale di Internet Banking attraverso le proprie credenziali e con il codice generato dal sistema di autenticazione utilizzato.

La Banca non invia alla Clientela comunicazioni relative la sicurezza utilizzando la posta elettronica, in quanto tale canale non è considerato sicuro e non permette di essere certi dell'identità del mittente del messaggio.

ASSISTENZA CLIENTI

La Carifermo mette a disposizione dei propri Clienti un servizio di assistenza tramite operatore a cui è possibile rivolgersi per problemi di accesso al servizio e per problemi tecnici e funzionali relativi all'utilizzo della procedura.

Il servizio di assistenza può essere contattato per posta elettronica o per telefono negli orari e ai recapiti sotto indicati. Gli operatori forniranno una risposta tempestiva tramite lo stesso canale.

	Carifermonline	**Prima Web**
Telefono	800-328-657 (dall'estero +39-0514992164)	800-328-657 (dall'estero +39-0514992164)
Posta elettronica	tecsupport@csebo.it	helpdeskhc@csebo.it
Orari	Tutti i giorni senza limitazione di orario (H24)	Tutti i giorni feriali dalle 8.00 alle 20.00