SICUREZZA DEI PAGAMENTI VIA INTERNET

Carifermo dà la possibilità ai propri clienti di effettuare pagamenti su internet attraverso:

- il portale di internet banking "**Carifermonline**", destinato alla clientela privata, che consente di disporre bonifici, versare tramite bollettini postali o bancari, effettuare pagamenti di MAV, RAV, F24, bollette CBILL e tramite MyBank, nonché effettuare trading online sul proprio dossier titoli;
- il portale di internet banking "**Prima Web**", destinato alle imprese, che consente di effettuare in modalità multibanca tutte le operazioni previste dal circuito CBI - Corporate Banking interbancario; su richiesta, possono essere attivate alcune funzionalità aggiuntive (bonifici per risparmio energetico, pagamento MAV e RAV, versamenti tramite bollettino postale, rendicontazione online dei documenti, ecc.);
- la carta di debito "**Carifermo Pay Internazionale e-commerce**" che può essere utilizzata per acquisti sui siti di commercio elettronico convenzionati con il circuito Maestro.

Gli strumenti messi a disposizione della propria clientela dalla Carifermo per effettuare pagamenti su internet sono sicuri. Tuttavia è molto importante che l'utente conosca i rischi del web e metta in atto alcuni accorgimenti per ridurre la possibilità di diventare vittima di una frode.

COME PROTEGGERE IL PROPRIO DISPOSITIVO DI ACCESSO AD INTERNET

L'accesso ad internet può essere effettuato da Personal Computer, smartphone e tablet.

E' importante ridurre il rischio che il dispositivo utilizzato possa essere infettato da virus o malware in grado di acquisire informazioni e dati personali o addirittura che possa essere controllato da un malintenzionato. Mettere in atto alcune semplici regole di comportamento permette di operare in sicurezza:

- installare un software antivirus e tenerlo costantemente aggiornato;
- tenere costantemente aggiornato il browser utilizzato per la navigazione in internet 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 consentono di disattivare queste funzioni.

COME PROTEGGERE I CODICI DI ACCESSO

Ad ogni cliente che attiva il servizio di internet banking, la Banca attribuisce un identificativo utente (user id) e consegna un PIN, valido solo per il primo accesso al servizio e che dovrà essere sostituito dall'utente con una password di sua scelta; inoltre, se sono attivati i servizi dispositivi, la Banca consegna un dispositivo elettronico (Digipass) che genera password monouso (token) da utilizzare al momento dell'accesso al servizio (login) e per confermare le operazioni di pagamento.

I codici di accesso sono strettamente personali: devono essere a conoscenza ed utilizzati esclusivamente dall'utente a cui sono stati assegnati, per cui è consigliabile:

- effettuare prima possibile il primo accesso utilizzando il PIN ed il token 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;
- custodire con cura il Digipass generatore della password monouso.

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.

Attenzione: i dipendenti e i collaboratori della Carifermo, compresi gli addetti all'Assistenza Clienti, non sono a conoscenza della password di accesso al servizio di internet banking o dei codici generati dal Digipass e non hanno bisogno di conoscerli. Perciò nessuna richiesta di questi dati verrà effettuata all'utente da parte della Banca.

COME ACCEDERE AL PORTALE DI INTERNET BANKING

Alcuni semplici consigli su come accedere in maniera sicura ai servizi Carifermonline o Prima Web dal proprio PC, tablet o smartphone tramite browser:

- 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 Carifermonline e Prima Web sempre 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, scaricabile da Google Play (versione Android) e da Apple Store (versione IOS).

COME RICONOSCERE I TENTATIVI DI PHISHING

Il phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato, generalmente attraverso messaggi di posta elettronica, 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 ma anche da banche con cui non si hanno rapporti;
- contengono errori grammaticali oppure 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.

Attenzione: 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 ma cancellarlo;
- evitare tassativamente di aprire o eseguire gli allegati in esso contenuti: questo potrebbe installare programmi (malware) in grado di rubare informazioni personali o monitorare l'attività dell'utente;
- non cliccare sui link presenti nel testo: questi possono 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 (utente e password) o il token su sito che si apre dopo aver cliccato sui link presenti nella mail.

Attenzione: Nel caso si sospetti che la propria password sia stata compromessa, contattare prima possibile il servizio di Assistenza Clienti 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 attraverso il portale di internet banking 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 di dati personali o di codici di accesso/autorizzativi;
- fare attenzione se appaiono richieste di inserimento del codice generato dal Digipass, che possono provenire da software malevoli installati ad insaputa dell'utente; nell'utilizzo corretto l'inserimento del token viene richiesto solo:
    - all'accesso al servizio, dopo aver inserito correttamente userid e password;
    - nella fase della conferma di una disposizione (es. bonifico, ricarica telefonica);
- 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, telefonicamente o per e-mail.

Nel caso in cui la Banca, nell'ambito dei controlli effettuati sull'operatività tramite internet banking, abbia evidenzia di una operatività sospetta, gli operatori dell'Assistenza Clienti contatteranno telefonicamente l'utente per le necessarie verifiche.

COME AUMENTARE ULTERIORMENTE IL LIVELLO DI SICUREZZA

E' 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 e di numero di operazioni, previsti su alcune tipologie di operazioni dispositive (escluse operazioni disposte sul Corporate Banking Interbancario).
  I massimali standard sono:

  Bonifici (SEPA ed esteri)
  Massimale per operazione: 30.000 euro
  Massimale mensile: 30.000 euro
  Massimale giornaliero: 30.000 euro
  Numero massimo operazioni giornaliere: 10
  Ricariche telefoniche
  Massimale per operazione: 250 euro
  Massimale mensile: 250 euro
  Massimale giornaliero: 250 euro
  Numero massimo operazioni giornaliere: 10
  Atri pagamenti (MAV, RAV, F24, CBILL, MyBank, bollettini bancari, bollettini postali)
  Massimale per operazione: 15.000 euro
  Massimale mensile: 15.000 euro
  Massimale giornaliero: 15.000 euro
  Numero massimo operazioni giornaliere: 10

I massimali possono essere ridotti direttamente dall'utente utilizzando le funzionalità del portale di internet banking. Per aumentarli, invece, l'utente deve rivolgersi alla propria filiale Carifermo.

- Servizio di alert via SMS o e-mail, che avvisa l'utente nel momento in cui autorizza una 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 l'utente nel momento in cui autorizza una 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 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 una operazione di pagamento tramite POS o su internet; è previsto su tutte le carte di debito emesse da Carifermo, da richiedere in filiale;
- Servizio 3D Secure per l'utilizzo della carta "Carifermo Pay Internazionale e-commerce" sui siti convenzionati con il circuito "Maestro"; per l'attivazione è necessario utilizzare il servizio di internet banking dispositivo Carifermonline.

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

COMUNICAZIONI DA PARTE DELLA BANCA

La Carifermo avrà cura di tenere periodicamente aggiornati i propri clienti riguardo la sicurezza dei pagamenti via internet attraverso:

- il proprio sito www.carifermo.it (Menu E-banking / Sicurezza);
- le comunicazioni allegate agli estratti di conto corrente o altri documenti inviati in formato cartaceo o elettronico;
- il canale Inbox riservato ai clienti che utilizzano gli applicativi:
  - Carifermonline: sezione COMUNICAZIONI nella parte sinistra della Home Page del servizio oppure dal menu ALTRI SERVIZI / COMUNICAZIONI;
  - Prima Web: funzione IB / ALTRI SERVIZI / COMUNICAZIONI; gli utenti che non hanno abilitata tale funzione possono richiederne l'attivazione rivolgendosi alla propria filiale Carifermo.

  La Inbox è un canale sicuro: per accedervi è necessario entrare nel portale di internet banking con le proprie credenziali.

Attenzione: la Banca non invia alla clientela comunicazioni inerenti 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 qualsiasi domanda, reclamo, richiesta di supporto e comunicazione di anomalie o incidenti riguardanti i pagamenti via Internet e relativi servizi.

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	0734/286443 – 497	0734/286464 – 401
Posta elettronica	supp.utenti@carifermo.it	
Orari	dal lunedì al venerdì 8.15-13.30 / 14.30-16.45	