LA SICUREZZA DEI PAGAMENTI VIA INTERNET

Si segnala che negli ultimi anni si sono verificati, in particolare ai danni di clienti dei servizi bancari online, numerosi tentativi di truffa finalizzati all'acquisizione per scopi illeciti di dati riservati e/o user-id e password.
Di seguito riportiamo comunque alcune informazioni generiche e consigli utili per garantire la sicurezza dei tuoi dati nei pagamenti eseguiti su internet.

Proteggi sempre i tuoi dispositivi personali

Se hai un PC, uno smartphone o un Tablet:

- installa e mantieni sempre aggiornato il software di protezione antivirus (1) e antispyware,
- installa sempre gli aggiornamenti ufficiali del sistema operativo e dei principali programmi che usi appena vengono rilasciati,
- installa gli aggiornamenti e le patch di sicurezza del browser e delle applicazioni,
- installa un firewall (2) personale,
- effettua regolarmente scansioni complete con l'antivirus
- non aprire messaggi di posta elettronica di cui non conosci il mittente o con allegati sospetti
- non installare applicazioni scaricate da siti non certificati o della cui attendibilità non sei sicuro
- se lo stesso PC/tablet/smartphone è usato anche da altre persone (familiari, amici, colleghi), fai in modo che adottino le stesse regole
- proteggi i tuoi dispositivi con PIN, password o altri codici di protezione. Di seguito riportiamo qualche suggerimento per creare - e custodire - una password sicura e facilmente memorizzabile da te, ma non facilmente intuibile da altri:
    - crea la tua password - che deve avere obbligatoriamente almeno 8 e massimo 20 caratteri - componendola usando combinazioni di caratteri alfanumerici, di cui almeno una lettera maiuscola. Utilizza ad esempio le iniziali di una frase che possa ricordare soltanto tu e non associabile ai tuoi dati anagrafici.
    - non utilizzare password condivise con altri servizi online
    - evita di utilizzare parole di senso comune o riferite alla tua vita privata o aziendale (es. nomi propri, codice fiscale, date di nascita, targa dell'auto, numero del badge personale)
    - non salvare la password nel browser ed evita per quanto possibile di annotarti la password per ricordarla. In ogni caso non conservarla insieme agli strumenti di pagamento
- non comunicare la password con amici, conoscenti, operatori del Servizio Clienti.

(1) Il software antivirus permette di tenere il proprio dispositivo al riparo da software indesiderati ("malware") che potrebbero essere installati senza *il consenso dell'utente, e carpire i dati di pagamento e altri dati sensibili del cliente a scopo fraudolento.*
(2) *Il firewall personale ha lo scopo di controllare e filtrare tutti i dati in entrata e in uscita del proprio dispositivo, aumentando il livello di sicurezza del dispositivo su cui è installato*

Importante: la Banca non fornisce supporto tecnico su antirivus, firewall e altre soluzioni installati sui dispositivi personali del Cliente, né può essere ritenuta responsabile per la configurazione degli stessi.

Attenzione al Phishing

Il cosiddetto “phishing” ad esempio consiste nell’invio di e-mail, solo in apparenza provenienti dal proprio istituto bancario o da aziende note/studi professionali (del quale è riprodotta fedelmente anche l’impostazione grafica), in cui si richiede al destinatario di fornire informazioni riservate. Spesso queste richieste sono motivate con ragioni di natura tecnica, falsi problemi di sicurezza o con l’attrattiva di ricevere premi e partecipare a concorsi.
Le suddette e-mail contengono solitamente:

- una richiesta di risposta urgente, in cui l’utente fornisca informazioni riservate.
- collegamenti a siti internet del tutto identici al portale dell’istituto, ma gestiti dagli autori della truffa, in cui l’utente è ingannevolmente indotto ad inserire informazioni riservate.
- collegamenti al sito originale dell’istituto, ma che provocano l’apertura di una finestra in sovrimpressione (cosiddetta “pop-up”) introdotta in modo fraudolento dai truffatori stessi, e in cui l’utente è ingannevolmente indotto ad inserire informazioni riservate.
- file allegati contenenti malwares (ovvero softwares usati per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata).

Possibili informazioni utilizzabili in modo illecito e a danno del cliente possono essere:

- codici di accesso (username e password), che consentono ai truffatori di accedere ai servizi online del cliente e di operare in sua vece.
- dati relativi alle carte di credito, utilizzabili per acquisti all’insaputa e a spese del cliente.
- dati personali in genere.

Ecco alcuni preziosi consigli per capire se ti trovi su un sito phishing o hai ricevuto una mail di phishing:

- **Indirizzo internet contraffatto**
  La parte iniziale di un sito che utilizza protocolli sicuri per la gestione dei dati personali deve essere caratterizzata dalla presenza della stringa ‘”**https**” e sul browser deve essere presente l'icona  che attesta il collegamento ad un sito protetto, solitamente posizionata in basso a destra.
- **Analizza il testo della comunicazione**
  Fai attenzione alle comunicazioni con errori ortografici e grammaticali e con un utilizzo scorretto della lingua italiana, probabilmente sono mail di phishing

Attenzione al Vishing

Il vishing è una forma di phishing basata sull’uso del telefono. Viene richiesto, tramite email o SMS, di chiamare un numero telefonico al quale comunicare i propri codici identificativi (Username/Email e Password). In alternativa, viene effettuata una chiamata preregistrata, in cui viene chiesta l’immissione e conferma dei codici identificativi.

PAGAMENTI CON CARTE DI CREDITO

Tutte le nostre carte di pagamento (carte di credito e carte prepagate) rispettano gli standard di sicurezza definiti dai Circuiti Internazionali:

- SecureCode™ per MasterCard®,
- Verified by Visa per VISA.

Il servizio:

- SecureCode™ per le carte MasterCard®,
- Verified by Visa per le carte VISA,

è un **protocollo di sicurezza che abbina la carta di pagamento ad un codice di sicurezza "usa e getta" di 6 cifre inviato via sms sul tuo cellulare certificato**. Questo codice temporaneo viene richiesto per autenticare il pagamento online su tutti i siti convenzionati.
Il corretto inserimento del codice di sicurezza "usa e getta" (Mastercard SecureCode o Verified By Visa) durante un acquisto presso un sito e-commerce di un negozio/esercente convenzionato conferma che sei il titolare della carta e quindi autorizzato ad effettuare la transazione. Se viene inserito un codice di sicurezza inesatto non sarà possibile finalizzare l'acquisto.
Così, anche se qualcuno conoscesse il numero della tua carta, l'acquisto non potrà essere finalizzato sul sito convenzionato senza il codice di sicurezza ricevuto via sms sul tuo telefono cellulare e valido solo per quella transazione.
Se utilizzi una carta di credito, per maggiori approfondimenti sulla sicurezza puoi comunque fare riferimento anche alle informazioni pubblicate nei siti delle società emittenti.

PAGAMENTI CON I NOSTRI SERVIZI ONLINE

Tutte le operazioni eseguite tramite i nostri servizi online sono protette dalla conferma finale che esegui chiamando dal telefono cellulare certificato il numero verde dedicato, inserendo poi il codice temporaneo di 4 cifre che ti viene comunicato di volta in volta, che cambia ogni 30 secondi.
Se non hai attivato il servizio secure call, hai a disposizione un token collegato all'internet banking che provvede a creare una one time password che utilizzi per confermare le tue operazioni on line.

- Se utilizzi il nostro servizio di Internet Banking, per maggiori approfondimenti sulla sicurezza puoi comunque fare riferimento anche alle informazioni pubblicate al seguente link:
  http://www.bancodilucca.it/ita/Privati/Internet-Banking/Informativa-Antitruffa---Happy-Banking
- Se utilizzi il nostro servizio di Corporate Banking, per maggiori approfondimenti sulla sicurezza puoi comunque fare riferimento anche alle informazioni pubblicate al seguente link:
  http://www.bancodilucca.it/ita/Aziende/Corporate-Banking/Informativa-Antitruffa---Comodo-Banking

PAGAMENTI CON ASSEGNI CIRCOLARI

Fai attenzione a non fotografare o inviare on line (via mail, tramite Whatsapp, o altro) ad altri i dati identificativi degli assegni circolari (quali importo, numero, eccetera); in questo modo eviterai a chiunque la possibilità di farne copia che potrebbe essere utilizzata in maniera impropria o in mala fede per una falsificazione del titolo. Se stai eseguendo un pagamento con un assegno circolare, per maggiori approfondimenti sulla sicurezza puoi comunque fare riferimento anche alle informazioni pubblicate al seguente link:
http://www.bancodilucca.it/ita/Trasparenza/Altri-documenti/TRUFFE-su-Assegni-Circolari

PRELIEVI SU ATM CON SERVIZIO SMARTCASH

I prelevamenti di contante che effettui presso i nostri ATM tramite il servizio SmartCash sono protetti dal PIN dell'APP che hai configurato sul tuo telefono cellulare certificato, PIN che tu stesso hai scelto e che digiti sull'ATM ogni volta che effettui un prelevamento di contante.