LA SICUREZZA DEI PAGAMENTI VIA INTERNET

Ecco alcune semplici regole e consigli per garantire la sicurezza dei tuoi dati e della tua Carta in internet.

Qui! Financial Services (di seguito QFS) ti offre la massima tranquillità anche in internet, grazie a servizi e accorgimenti appositamente pensati per garantire la sicurezza non solo della tua Carta - e del suo utilizzo -, ma anche dei tuoi dispositivi

Eventuali avvisi sull'utilizzo corretto e sicuro del servizio di pagamento via Internet ti saranno forniti attraverso l'area riservata della tua Carta (il tuo canale protetto), così come sarai informato sui rischi emergenti significativi (per esempio allerta circa il social engineering, pishing).

In caso di (possibili) pagamenti fraudolenti, incidenti sospetti o anomalie durante la sessione per i servizi di pagamento via Internet e/o possibili tentativi di social engineering, chiama il numero 199.824.834* attivo 24 ore su 24 richiedendo l'eventuale blocco cautelativo del tuo strumento di pagamento. Gli operatori di QFS procederanno a contattarti al numero che hai indicato al momento dell'attivazione dello strumento di pagamento.

QFS procederà anche attraverso l'area riservata a comunicarti eventuali attacchi, ad esempio le e-mail di pishing.

(*) numero a tariffazione specifica, con costo dichiarato prima dell'inizio della comunicazione telefonica

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 (*) e antispyware

• installa sempre gli aggiornamenti 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 (**) 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. Per i consigli su come creare e gestire password e credenziali, ti invitiamo a leggere la sezione dedicata

(*) 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.

(**) 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

Password: come crearle e proteggerle

Per motivi di sicurezza l'accesso ad alcune reti o servizi richiede credenziali e password. Queste ultime inoltre vengono utilizzate anche per la protezione di dispostivi personali, per evitare l'accesso a persone non autorizzate. Ecco allora qualche suggerimento per creare - e custodire - una password sicura e facilmente memorizzabile da te, ma non facilmente intuibile da altri:

• crea la tua password componendola con 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

• usa combinazioni di caratteri alfanumerici

• 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 e 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. Ti ricordiamo che Qui! Financial Services non ti chiederà mai di comunicare o inviare la tua password né telefonicamente né via mail

Tutela i tuoi acquisti in internet

Con Qui! Financial Services puoi utilizzare la tua Carta in tutta tranquillità anche per le tue spese online, grazie al servizio 3D Secure. Con il nome 3D Secure si definisce il sistema di protezione degli acquisti online tramite "MasterCard SecureCode" studiato dal circuito internazionale MasterCard.

Attivare il servizio 3D Secure garantisce una tutela per i tuoi acquisti online, permettendo di prevenire eventuali utilizzi illeciti della tua Carta sul web. Con l'iscrizione al servizio 3D Secure eviti che il tuo numero di Carta venga usato per pagamenti online a tua insaputa.

Per attivare il 3D Secure, è necessario entrare nell'area riservata della tua Carta e seguire le istruzioni presenti.

Inoltre Qui! Financial Services ti garantisce la possibilità di poter bloccare l'operatività dei

pagamenti e-commerce e MO.TO per problemi di sicurezza. Compila in tutte le sue parti il modulo che trovi allegato a questo documento e segui le istruzioni per l'invio. Potrai revocare un ordine di pagamento fino a quando questo non è stato ricevuto da Qui! Financial Services. Troverai anche le indicazioni per contattarci e "sbloccare" l'operazione di pagamento via internet.

Cosa fare in caso di furto/smarrimento dei tuoi dispositivi o delle tue carte o in caso di pagamenti anomali

Se perdi, o ti vengono sottratti, i tuoi dispositivi personali o le tue Carte,o in caso di abuso riscontrato o sospetto (per maggiori dettagli ti invitiamo a leggere anche la sezione dedicata al phishing) è importante agire tempestivamente. In questi casi, contatta immediatamente il Servizio Clienti (attivo 24 ore su 24) per bloccare immediatamente la tua Carta.

Verifica eventuali pagamenti sospetti e, se del caso, attivare la procedura di richiesta rimborso.

Protocollo di sicurezza

Tutti i dati e le informazioni sono protetti con il sistema più avanzato di crittografia TLS 1.2 con cifratura AES a 128 bit.

Attento al Phishing

Anche in internet, ci sono diversi pericoli. Una truffa molto diffusa è il phishing, una pratica illegale messa in atto da malintenzionati che, inviando agli utenti messaggi email rassomiglianti - nei contenuti e nella grafica - a quelli di aziende note, cercano di carpire informazioni riservate e sensibili (codici di accesso, dati della carta o personali) tramite link a siti simili a quelli reali.

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

• Indirizzo internet contraffatto

Come riconoscere quindi un indirizzo potenzialmente pericoloso? La parte iniziale deve essere caratterizzata dalla presenza dell'"https": significa che quel sito utilizza protocolli sicuri per la gestione dei dati personali.

• 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.

Inoltre: un sito sicuro e certificato che adotta i protocolli di sicurezza per la gestione dei dati, riporta sempre nella finestra del browser – in basso a destra o nella barra degli indirizzi - l'icona del lucchetto, che definisce il sito come sicuro. Devi quindi diffidare dei siti che richiedono l'inserimento di dati sensibili (Login o Password, dati della carta di credito o personali) e che non riportano l'icona del lucchetto: i dati inseriti in quella pagina saranno facilmente trafugabili. Se poi vuoi essere sicuro dell'attendibilità del sito, fai doppio click sull'icona del lucchetto: una scheda ti aiuterà a verificare che le credenziali di sicurezza siano effettivamente quelle del sito che stai visitando.

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. Qui! Financial Services non ti chiederà mai di comunicare o inserire telefonicamente i tuoi codici identificativi.

Social engineering

Il social engineering, impiegato nel phishing, è un insieme di tecniche ingannevoli per guadagnare la vostra fiducia e sottrarvi dati personali, password, ecc. Ad esempio, inviarvi un'e-mail facendo finta di essere un vostro collega, un vostro amico, o la vostra banca per chiedervi informazioni riservate, è una delle tecniche più diffuse di social engineering.

Come si può evitare di rimanerne vittima?

Sospettate delle telefonate da parte di sconosciuti o e-mail da parte di soggetti che dicendo di appartenere a fantomatiche ditte chiedono di avere notizie su vostri dati.

Non rivelare informazioni personali o finanziarie tramite e-mail e non rispondere ad e-mail che richiedono tali dati. Questo vuol dire pure non cliccare su link di tali e-mail. Informazioni sui vostri pagamenti o sul vostro strumento di pagamento li trovate all'interno dell'area riservata collegandovi al link che vi è stato fornito da QFS. L'area privata di QFS è sempre identificabile dalla presenza di un lucchetto chiuso e dalla dicitura "https" nella barra degli indirizzi.

Responsabilità di Qui! Financial Services e del Titolare della Carta per le operazioni in internet

Sia Qui! Financial Services che il Cliente (Titolare della Carta) devono garantire, ciascuno per la propria parte, l'uso corretto e sicuro dei pagamenti in internet. In particolare, come Cliente, sei responsabile della tua Qui Card, e sei tu a dover rispondere legalmente delle operazioni effettuate dallo strumento di pagamento a te intestato.

Devi custodire con cura la tua Carta, il PIN e gli eventuali altri i codici di sicurezza e usarla correttamente. In caso di anomalie o problemi riscontrati durante le operazioni di pagamento in internet, o in caso di abuso o utilizzo sospetto della tua Carta, devi immediatamente contattare il Servizio Clienti.

Lato suo, Qui! Financial Services mette a disposizione della Clientela il Servizio Clienti, disponibile 24 ore su 24, per bloccare la Carta (e quindi il suo utilizzo). Inoltre, in caso di spese non autorizzate dal Cliente, Qui! Financial Services garantisce il rimborso del relativo importo, dopo aver effettuato tutte le verifiche e secondo quanto previsto dal contratto.

MODULO DI ATTIVAZIONE/DISATTIVAZIONE OPERATIVITÀ PAGAMENTI INTERNET

QUI! CARD
QUI! FINANCIAL SERVICES

Spett.le
Servizio Assistenza Clienti QUI! CARD
Casella Postale 1093
Genova Centro
16121 Genova

Con la presente, io sottoscritto _____
nome e cognome

titolare della carta numero |_|_|_|_|_|_|******|_|_|_|_|
inserire solo le prime 6 e le ultime 4 cifre

richiedo di

☐ **DISATTIVARE**

☐ **ATTIVARE**

l'operatività e-commerce associata alla mia carta, ossia la possibilità di effettuare pagamenti via internet di prodotti o servizi utilizzando la carta sovraindicata.

Tale scelta può essere revocata in qualsiasi momento, previa nuova compilazione di questo modulo.

ATTENZIONE: allegare al modulo anche una copia fronte/retro di un proprio documento d'identità in corso di validità.

In fede,

_____ _____
luogo e data firma

Nota: in caso di carta aziendale la richiesta deve essere firmata anche dal Legale Rappresentante dell'Azienda oltre al Titolare carta e deve essere corredata di timbro dell'azienda. E' necessario allegare anche una copia fronte/retro del documento d'identità del Legale Rappresentante.

_____ _____
luogo e data timbro e firma del legale rappresentante