CartaBCC

Allegato “Pagamenti Online”

Consigli utili per navigare in sicurezza e proteggere i dati della Carta

Numia S.p.A., in qualità di Emittente, garantisce ai Titolari Carta elevati standard di sicurezza nei pagamenti, ponendo in essere misure specifiche a tutela del cliente che riducano al minimo il rischio di frode, comportamenti anomali o altri abusi.
Rientrano in tale ambito, ad esempio, il **servizio SMS Alert** per le notifiche delle transazioni effettuate, nonché il sistema di controllo intelligente “**3D Secure**” per gli acquisti *online*, che verifica l’attendibilità dei siti Internet ed invia una password temporanea (OTP) per eventuali richieste di autenticazione.

In aggiunta alle misure di sicurezza messe in atto dall’Emittente, è necessario, al contempo, che il Titolare dello strumento di pagamento adotti degli accorgimenti atti a proteggere la propria Carta, le credenziali di sicurezza personalizzate, nonché i mezzi tecnologici utilizzati per eseguire disposizioni online (ad esempio: personal computer, smartphone e tablet).

Nel caso di Pagamenti Online ed altre Operazioni Dispositive effettuati tramite Personal Computer (PC), si raccomanda l’adozione delle seguenti Misure di Sicurezza e Prevenzione:

1	**Evitare l’utilizzo di personal computer pubblici** per accedere alla propria area riservata o per effettuare acquisti su internet
2	**Scaricare sempre gli ultimi aggiornamenti ufficiali del Sistema Operativo e dei programmi di utilità** installati sul PC (ad esempio: Microsoft Office, Adobe Acrobat Reader ecc.), oppure **attivare gli aggiornamenti automatici**. I vecchi Sistemi Operativi non più supportati dal produttore aumentano inoltre il livello di rischio
3	**Installare e tenere costantemente aggiornato un *software* di sicurezza (antivirus - antimalware)**, ed effettuare regolarmente scansioni complete di tutti i file del PC
4	**Tenere sotto controllo eventuali peggioramenti delle prestazioni e della velocità del PC**, in quanto potrebbero potenzialmente indicare la presenza di un contagio (virus, malware)
5	**Utilizzare un *firewall* personale** che filtri tutti i dati in entrata e in uscita dal PC
6	**Installare gli aggiornamenti e le *patch* di sicurezza di *browser web*** (Google Chrome, ecc.) e dei **componenti associati** (Java, Adobe, ecc.)
7	**Eliminare periodicamente i *cookies* e i file temporanei web** utilizzando le opzioni del *browser web*
8	**Non salvare le credenziali di accesso all’interno dei *browser web*** utilizzati per la navigazione dei siti internet
9	Verificare che **l’indirizzo nella barra di navigazione del *browser web* venga raggiunto tramite certificato di sicurezza SSL (“https://”, solitamente accompagnato dall’icona di un lucchetto chiuso)**, in quanto garantisce una maggiore sicurezza nella navigazione
10	**Digitare l’indirizzo del sito da visitare direttamente nella barra di navigazione e non seguire link presenti in e-mail o in altri portali web**
11	**Proteggere il PC con una *password*** che abbia le seguenti caratteristiche: ✓ sia **complessa**, ovvero che non sia una parola comune, che non utilizzi codici banali e facilmente associabili alla tua persona (data di nascita) e che non sia già utilizzati per servizi internet generici come posta elettronica, accessi a social network, ecc.; ✓ **contenga numeri, lettere maiuscole e minuscole e caratteri speciali** ✓ sia **semplice da ricordare (cd. “familiarità”)**
12	**Non lasciare mai il PC incustodito in aree pubbliche**
13	**Proteggere l’accesso al proprio PC con blocco automatico in caso di *stand-by*, password e/o PIN**
14	**Non installare software e/o applicazioni scaricate da siti non certificati o di cui non si è certi dell’attendibilità**. Se possibile, è sempre bene esaminare i *feedback* di altri utenti
15	**Non salvare informazioni finanziarie sul PC** (ad esempio: PIN, numero della Carta o *password* di accesso alle Aree Riservate). In caso di interventi di assistenza o manutenzione del PC **eliminare le informazioni riservate**
16	Se il medesimo PC viene condiviso con altre persone, **è opportuno che anch’esse adottino le stesse misure di sicurezza**

Quando i Pagamenti Online e le Operazioni Dispositive vengono effettuati tramite Device mobile (Smartphone e/o Tablet), è opportuno adottare questi Presidi Aggiuntivi:

1	**Scaricare sempre gli ultimi aggiornamenti ufficiali del Sistema Operativo e dei programmi di utilità** installati sul *device* (ad esempio: Microsoft Office, Adobe Acrobat Reader ecc.), oppure **attivare gli aggiornamenti automatici**. I vecchi Sistemi Operativi non più supportati dal produttore aumentano inoltre il livello di rischio
2	**Installare e tenere costantemente aggiornato un *software* di sicurezza (antivirus - antimalware)**
3	**Tenere sotto controllo eventuali peggioramenti delle prestazioni e della velocità del *device***, in quanto potrebbero potenzialmente indicare la presenza di un contagio (virus, malware)
4	**Disattivare Wi-Fi, geolocalizzazione e/o *bluetooth* quando non necessari**
5	**Scaricare e installare esclusivamente applicazioni ufficiali provenienti da *store* affidabili**, prestando attenzione alle **autorizzazioni** e ai **permessi richiesti dalle applicazioni stesse**. È sempre bene, inoltre, esaminare i *feedback* rilasciati altri utenti
6	**Installare le App MyCartaBCC e RelaxBanking sul proprio *device* personale**
7	**Impostare i PIN di accesso alle App MyCartaBCC e RelaxBanking** utilizzando gli stessi criteri di **complessità** e **familiarità** della credenziale personalizzata
8	Proteggere l'accesso al proprio *device* e alle App MyCartaBCC e RelaxBanking **con blocco automatico in caso di *stand-by*, password e/o PIN**. Laddove il *device* fornisca la funzionalità, è possibile utilizzare **sistemi di riconoscimento biometrico (impronta digitale, riconoscimento facciale, ecc.) in alternativa al codice PIN**: in tali circostanze è necessario assicurarsi che sul proprio dispositivo siano **registrati esclusivamente i dati biometrici del titolare del *device* personale e non anche quelli di terze figure** (ad es. componenti del nucleo familiare)
9	**Effettuare sempre il *log out* dalle App MyCartaBCC e RelaxBanking al termine del loro utilizzo**: a tutela di eventuali intromissioni: se il sistema riscontra la mancata esecuzione di azioni per 5 minuti, l'utenza verrà automaticamente scollegata
10	**Non salvare informazioni finanziarie sul *device*** (ad esempio: PIN, numero della Carta o *password* di accesso alle Aree Riservate)
11	**Qualora possibile, attivare la crittografia del *device* e della *memory card* esterna, nonché le funzionalità di "*remote lock*" e "*remote wiping*".** Queste ultime consentiranno, in caso di furto, di bloccare e cancellare i dati contenuti sul dispositivo *mobile* tramite un altro PC e/o *device*
12	**Eliminare le informazioni riservate in caso di interventi di assistenza o manutenzione del *device***
13	Evitare di eseguire operazioni cosiddette di "*jailbreak*" o "*rooting*", procedure che rimuovono le restrizioni *software* imposte dal Sistema Operativo, poiché possono impedire la corretta installazione delle **App MyCartaBCC e RelaxBanking** e comportare una significativa riduzione della sicurezza del *device*

In caso di problemi e/o anomalie riscontrati durante una disposizione *online*, oppure in caso di frode o utilizzo sospetto della Carta, il Titolare è **tenuto a contattare tempestivamente il Servizio Clienti** ai numeri di telefono evidenziati al seguente indirizzo https://www.cartabcc.it/Pagine/Assistenza/Contattaci.aspx e segnalare l'accaduto.

Laddove invece sia lo stesso Emittente a rilevare, tramite le proprie procedure di sicurezza, un potenziale rischio di frode nei pagamenti, provvederà alla trasmissione di una tempestiva notifica al Titolare. A seconda dell'entità del rischio connesso all'operazione, l'Emittente – anche sulla base delle segnalazioni pervenute dalla la Banca Collocatrice - si riserva di porre in essere le seguenti **misure aggiuntive**:

- richiesta di conferma dell'operazione tramite SCA (*strong customer authentication*);
- blocco dell'operazione;
- blocco temporaneo dell'operatività;
- blocco permanente dell'operatività;
- blocco dell'operatività su iniziativa del cliente;
- chiamata telefonica di verifica e conferma.

Si fa infine presente che in nessuna delle comunicazioni inviate da NumiaS.p.A. e/o dalla propria Banca Collocatrice in merito allo strumento di pagamento verrà richiesto di rivelare credenziali, codici di accesso, PIN, numeri delle Carte o informazioni personali del Titolare. Le informazioni di carattere personale (o i numeri delle Carte) che possono risultare utili per la gestione del servizio sono già a conoscenza dell'Emittente Carta e/o della Banca Collocatrice e non vi è quindi motivo di richiederle.
Qualora vi fosse necessità di comunicazioni al riguardo, il Titolare sarà invitato a recarsi alla propria filiale della Banca Collocatrice.
In caso di dubbi o chiarimenti, è a disposizione il **Servizio Clienti di Numia S.p.A. al numero** 06.80.80.800[1]

[1] Il costo della telefonata è a carico del Titolare secondo il piano tariffario concordato con il Proprio operatore telefonico.

Ulteriori consigli utili e Presidi di Sicurezza del Titolare per la prevenzione delle frodi connesse all'utilizzo della Carta di pagamento

Si richiamano di seguito ulteriori indicazioni utili e consigli da adottare nella gestione dei propri dispositivi e della propria Carta di pagamento:

1	Digitare sempre per esteso l'indirizzo Internet (*url*) di accesso alle pagine web https://www.cartabcc.it e https://www.relaxbanking.it, **evitando di utilizzare *link* presenti all'interno di e-mail o messaggi provenienti da social network (Facebook, Twitter, ecc.)**
2	**Controllare la presenza del lucchetto accanto all'indirizzo internet sulla barra degli indirizzi in fase di collegamento alle Aree Riservate**, a certificare la connessione sicura (l'indirizzo della pagina inizia per https://, invece di http://)
3	**Controllare bene i dati riportati sulle notifiche ricevute prima di autorizzare azioni e disposizioni di pagamento dalle App MyCartaBCC e/o RelaxBanking**
4	**Controllare sempre con attenzione le notifiche push, gli SMS e le e-mail di notifica che MyCartaBCC e RelaxBanking inviano per chiedere l'identificazione e per informare su azioni e/o operazioni effettuate**
5	**Non riferire mai a nessuno il codice OTP, anche se dichiara di essere un operatore del Servizio Clienti di Numia S.p.A. o della Banca Collocatrice**
6	**Conservare sempre separatamente le proprie credenziali di sicurezza personalizzate** (codici utente, *password* e PIN)
7	**Controllare regolarmente i dettagli e le informazioni contenuti sugli estratti conto**, al fine di verificare la bontà e correttezza delle transazioni riepilogate ed attivarsi tempestivamente alla segnalazione delle operazioni di pagamento non autorizzate in caso di anomalie riscontrate
8	Non aprire i messaggi di posta elettronica **di cui non sia immediatamente riconoscibile il mittente**
9	**Non inserire mai il codice OTP o il codice di attivazione delle App MyCartaBCC e RelaxBanking in pagine raggiunte cliccando su *link* presenti in e-mail ricevute sulla propria casella di posta elettronica**
10	**In caso di dubbi sulla sua provenienza**, verificare la genuinità di una richiesta di codice OTP - anche via SMS – **contattando il Servizio Clienti**
11	**Prestare particolare attenzione nella divulgazione e diffusione dei propri dati personali attraverso *social network*, e-mail, telefono ecc.**, al fine di prevenire che tali informazioni possano entrare in possesso a truffatori e che possano essere utilizzate per fini illeciti
12	Effettuare una valutazione attenta prima di allegare alle e-mail, o inviare attraverso altri canali, **immagini relative agli strumenti di pagamento elettronici**
13	**Verificare la provenienza del messaggio prima di fornire qualsiasi dato o informazione personale** quando si riceve un buono d'acquisto via *e-mail* da un esercente
14	Per gli acquisti *online* (E-commerce) e per verificare la veridicità e il livello del servizio, **è possibile utilizzare la piattaforma ShoppingVerify (https://it.shoppingverify.com/), un raccoglitore di giudizi critici e opinioni dei clienti che hanno acquistato da portali di *e-commerce* di tutto il mondo**.
15	**Prestare attenzione in caso di operazioni disposte presso ATM e Casse Self Assistite, adottando le seguenti precauzioni**: ✓ Prelevare il contante dai terminali inseriti all'interno delle filiali della Banca, evitando – laddove possibile – di utilizzare i terminali esposti su strada; ✓ In caso di prelievo di contante da terminali su strada, prediligere gli ATM posti in zone di passaggio, dove potrebbero essere notati eventuali comportamenti illeciti; ✓ Prestare attenzione alle condizioni del terminale (ad esempio: parti allentate/mancanti, pezzi di nastro adesivo), al fine di intercettare possibili manomissioni intervenute; ✓ Coprire sempre la tastiera con la mano o un oggetto mentre si procede alla digitazione del codice PIN della Carta di pagamento, al fine di prevenire eventuali casistiche in cui sia presente una microcamera che spia le credenziali inserite; ✓ Contattare immediatamente la Banca e procedere al blocco tempestivo della Carta di pagamento nel caso in cui il terminale non abbia erogato contante nonostante sia stato eseguito un ordine di prelievo, avendo altresì accortezza nel non allontanarsi dall'ATM fino a quando non viene ricevuta conferma dal Servizio Clienti di avvenuto perfezionamento del blocco della Carta di pagamento; ✓ Non gettare mai le ricevute di prelievo nelle immediate vicinanze del terminale, in quanto contenenti dati che possono permettere un furto d'identità.

Per ulteriori informazioni e dettagli in merito alle regole di comportamento da adottare per la sicurezza dei propri dispositivi e delle proprie credenziali personalizzate, nonché per avere aggiornamenti circa i principali meccanismi di frode rilevati a livello di sistema ed alle conseguenti azioni da adottare per riconoscerle e prevenirle, è possibile visitare il sito **https://www.stopfrodi.gruppoiccrea.it/**.

CartaBCC

Come proteggersi dal *phishing*: il decalogo di ABI Lab

Il Centro di Ricerca e Innovazione per la Banca, promosso dall'Associazione Bancaria Italiana (ABI), ha proposto dieci semplici regole a cui attenersi per proteggersi dal ***phishing***, la frode informatica ideata allo scopo di rubare i dati personali di un utente.
Il *phishing* avviene tramite un'e-mail contraffatta (o tramite SMS – in questo caso si parla di *smishing*), spesso con errori ortografici e grammaticali, che sembra provenire dalla Banca o dall'Emittente (poiché ne riproduce il nome, la grafica, il logo e il layout), la quale invita il destinatario ad aprire un link in cui inserire i codici segreti della Carta o del conto corrente.

Di seguito il decalogo "*anti-phishing*" stilato da ABI Lab:

1. Diffidate di qualunque e-mail che vi richieda l'inserimento di dati riservati riguardanti codici di carte di pagamento, chiavi di accesso al servizio di home banking o altre informazioni personali. La vostra banca non richiederà tali informazioni via e-mail.

2. È possibile riconoscere le truffe via e-mail con qualche piccola attenzione; generalmente queste e-mail:

- non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici);
- fanno uso di toni "intimidatori", ad esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'utente;
- non riportano una data di scadenza per l'invio delle informazioni;

3. Nel caso in cui riceviate un'e-mail contenente richieste di questo tipo, non rispondete all'e-mail stessa, ma informate subito la vostra banca tramite il call centre o recandovi in filiale;

4. Non cliccate su link presenti in e-mail sospette, in quanto questi collegamenti potrebbero condurvi a un sito contraffatto, difficilmente distinguibile dall'originale. Anche se sulla barra degli indirizzi del browser viene visualizzato l'indirizzo corretto, non vi fidate: è possibile infatti per un hacker visualizzare nella barra degli indirizzi del vostro browser un indirizzo diverso da quello nel quale realmente vi trovate;

5. Diffidate inoltre di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali, quali in particolare @;

6. Quando inserite dati riservati in una pagina web, assicuratevi che si tratti di una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con "https://" e non con "http://" e nella parte in basso a destra della pagina è presente un lucchetto;

7. Diffidate se improvvisamente cambia la modalità con la quale vi viene chiesto di inserire i vostri codici di accesso all'home banking: ad esempio, se questi vengono chiesti non tramite una pagina del sito, ma tramite pop-up (una finestra aggiuntiva di dimensioni ridotte). In questo caso, contattate la vostra banca tramite il call centre o recandovi in filiale;

8. Controllate regolarmente gli estratti conto del vostro conto corrente e delle carte di credito per assicurarvi che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contattate la banca e/o l'emittente della carta di credito;

9. Le aziende produttrici dei browser rendono periodicamente disponibili on-line e scaricabili gratuitamente degli aggiornamenti (cosiddette patch) che incrementano la sicurezza di questi programmi. Sui siti di queste aziende è anche possibile verificare che il vostro browser sia aggiornato; in caso contrario, è consigliabile scaricare e installare le patch;

10. Internet è un po' come il mondo reale: come non dareste a uno sconosciuto il codice PIN del vostro bancomat, allo stesso modo occorre essere estremamente diffidenti nel consegnare i vostri dati riservati senza essere sicuri dell'identità di chi li sta chiedendo. In caso di dubbio, rivolgetevi alla vostra banca!

In aggiunta al *phishing*, si raccomanda di fare attenzione anche al ***vishing***, termine inglese che unisce le due parole *voice* e *phishing*, una truffa effettuata tramite servizi di telefonia a seguito della quale si viene contattati da un presunto operatore della banca (anche attraverso una voce pre-registrata) che tenta di carpire, con l'inganno, informazioni private.