Allegato “Pagamenti online”

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

BCC Pay 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. Inoltre, l’Emittente, nei casi in cui dovesse rilevare, tramite le proprie procedure di sicurezza, un rischio di frode nei pagamenti, invia una tempestiva notifica al Titolare. A seconda dell’entità del rischio connesso all’operazione, l’Emittente e/o la Banca si riservano 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.

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 (da non conservare insieme alla Carta stessa e da non rivelare a terzi), nonché i mezzi tecnologici utilizzati per eseguire disposizioni online (ad esempio: personal computer, smartphone e tablet).

Relativamente a questi ultimi, si suggerisce di evitare l’utilizzo di computer pubblici per accedere alla propria area riservata o per effettuare acquisti sul web; è opportuno evitare il salvataggio automatico delle password ed è buona abitudine effettuare sempre il log-out dai siti e-commerce una volta terminata la transazione. Inoltre, è consigliato verificare sempre che l’indirizzo nella barra di navigazione del browser venga raggiunto tramite protocollo HTTPS (solitamente accompagnato dall’icona di un lucchetto chiuso), che garantisce una maggiore sicurezza nella navigazione. Si raccomanda di digitare l’indirizzo del sito da visitare direttamente nella barra di navigazione e di non seguire link presenti in email o in altri portali web.

Nel caso di **pagamenti effettuati tramite personal computer** (PC), si suggerisce di:

- utilizzare un software di sicurezza (antivirus), aggiornarlo periodicamente ed effettuare regolarmente scansioni complete di tutti i file del PC;
- utilizzare un firewall personale, che filtri tutti i dati in entrata e in uscita dal dispositivo;
- 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;
- installare gli aggiornamenti e le patch di sicurezza di browser e applicazioni;
- eliminare periodicamente i cookies e i file temporanei Internet utilizzando le opzioni del browser;
- proteggere il PC con una password, da non rivelare a terzi;
- non lasciare mai il dispositivo incustodito in aree pubbliche;
- impostare il blocco automatico del PC quando entra in stand-by;
- non installare 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;
- non salvare informazioni finanziarie sul dispositivo (ad esempio: PIN, numero della Carta o password di accesso all’area riservata);
- in caso di interventi di assistenza o manutenzione del dispositivo, eliminare le informazioni riservate;
- se il medesimo PC viene condiviso con altre persone, è opportuno che anch’esse adottino le stesse misure di sicurezza.

Quando i **pagamenti** vengono effettuati **con smartphone o tablet**, è opportuno:

- scaricare sempre gli ultimi aggiornamenti ufficiali del Sistema Operativo;
- installare ed aggiornare periodicamente un software di sicurezza (antivirus);
- disattivare Wi-Fi, geolocalizzazione e bluetooth quando non necessari;
- scaricare esclusivamente applicazioni ufficiali provenienti da store affidabili, prestando attenzione alle autorizzazioni e ai permessi richiesti dalle app stesse. È sempre bene, inoltre, esaminare i feedback rilasciati altri utenti;

- proteggere il dispositivo con password, PIN e, laddove disponibili, con sistemi di riconoscimento biometrico (ad esempio: impronta digitale, riconoscimento facciale);
- non salvare informazioni finanziarie sul dispositivo (ad esempio: PIN, numero della Carta o password di accesso all'area riservata);
- impostare il blocco automatico del dispositivo quando entra in stand-by;
- qualora possibile, attivare la crittografia del dispositivo 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;
- evitare di eseguire operazioni cosiddette di "jailbreak" o "rooting", procedure che rimuovono le restrizioni software imposte dal Sistema Operativo, poiché possono comportare una significativa riduzione della sicurezza del dispositivo.

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 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.

Si fa presente che in nessuna delle comunicazioni inviate da BCC Pay 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 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 allo sportello di filiale.
In caso di dubbi o chiarimenti, è a disposizione il **Servizio Clienti al numero** 06.80.80.800*.

Ulteriori consigli

È importante effettuare una valutazione attenta prima di allegare alle e-mail, o inviare attraverso altri canali, immagini relative agli strumenti di pagamento. In particolare, è bene evitare di inviare via telefono cellulare, fax o e-mail la fotografia di un assegno per concludere una transazione commerciale.
Inoltre, quando si riceve un buono d'acquisto via e-mail da un esercente, è opportuno verificare la provenienza del messaggio prima di fornire qualsiasi dato o informazione personale.

In caso di problemi riscontrati durante una disposizione online, oppure in caso di frode o utilizzo sospetto della Carta, il Titolare è tenuto a contattare il Servizio Clienti (al numero sopraindicato) e segnalare l'accaduto.

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