BANCA POPOLARE
DI PUGLIA E BASILICATA

SICUREZZA DEI PAGAMENTI ON LINE

Da sempre Banca Popolare di Puglia e Basilicata pone al centro del rapporto di fiducia con i propri Clienti la sicurezza nelle transazioni. A tal fine, infatti, adotta sistemi di controllo e protezione sempre più sofisticati a tutela della tranquillità dell'utente durante la navigazione in internet.
Per un più responsabile utilizzo dei diversi dispositivi, la Banca offre una serie di suggerimenti e consigli:

Gli acquisti online

BPPB adotta i sistemi di criptazione più avanzati a garanzia della riservatezza e al fine di proteggere e codificare il traffico di informazioni che transitano su internet. In caso di inattività protratta per oltre 15 minuti, il sistema interrompe automaticamente la connessione. Per ricominciare ad operare è necessario collegarsi nuovamente al sito.
A tutela dei propri clienti BPPB dispone dei seguenti sistemi di sicurezza:

Token
È un dispositivo digitale altamente affidabile che consente di operare online con estrema sicurezza. La Banca sta dotando tutti i clienti di questo strumento. Se non lo hai ancora ritirato, recati subito nella tua filiale. Per aumentare il livello di sicurezza, il Servizio dispositivo usa un sistema che unisce due codici fissi (il Codice Utente e la Password) e un codice monouso variabile (il codice OTP). Il Codice Utente è univocamente assegnato e non modificabile mentre la Password può essere personalizzata. Il Codice OTP è generato dall'apposito token sincronizzato col server centrale. Con il Servizio di Internet Banking di BPPB il cliente può quindi operare in tutta tranquillità, avendo cura di custodire separatamente i suoi codici personali e il token OTP nel modo che ritiene più sicuro.

Verified by Visa/Mastercard secure code
Sono i sistemi di sicurezza creati dai circuiti internazionali VISA e MasterCard e permettono di acquistare online utilizzando una password, personalizzabile in qualsiasi momento. In questo modo nessuno può utilizzare i dati per fare acquisti sui siti convenzionati e con la dizione "Verified by Visa/MasterCard secure code".
In ogni caso, ti suggeriamo di seguire poche e semplici regole:

1. Verifica che il venditore sia un esercizio reale, meglio se conosciuto, e che il sito indichi tutti i suoi dati, compreso l'indirizzo
2. Diffida degli accessi gratuiti a siti che richiedono i dati della carta di credito
3. Evita di inserire il numero della carta in siti non protetti da sistemi di sicurezza internazionali

Phishing

In alcuni periodi dell'anno, soprattutto in prossimità delle feste come Natale e Pasqua o della partenza per le vacanze estive, si verificano tentativi di truffe via internet tra le quali la più diffusa è quella che in gergo informatico viene chiamata "phishing" (furto di identità). Con essa vengono acquisiti i dati generali e l'identità digitale degli utenti.
La modalità con cui si concretizza questa truffa online è molto semplice e consiste nel ricevere una email contraffatta, che sembra provenire dalla banca perché riproduce il nome, la grafica, il logo e il layout tipico dei servizi bancari, e spinge l'utente, ad esempio con una richiesta di verifica dati o con il download di qualche aggiornamento, a digitare i propri codici di accesso al conto corrente (es. username e/o password), ovvero fornire informazioni personali. Queste attività sono illegali e sono utilizzate per ottenere come detto l'accesso a informazioni personali o riservate con la finalità del furto di identità.
Al fine di mitigare i rischi connessi al fenomeno del phishing, la BPPB ha implementato il sistema di autenticazione forte dell'utente.
BPPB non richiede mai, direttamente o tramite terzi, informazioni personali o codici di accesso ai servizi di internet banking. Le comunicazioni della Banca, anche quelle relative all'uso corretto e sicuro del servizio internet banking vengono fornite nell'area riservata del rapporto web (Comunicazioni), ovvero, nei casi in cui i clienti abbiano abilitati i relativi servizi, mediante posta elettronica certificata (PEC) o servizio di SMS Alert.

Ecco alcune semplici regole che possono aiutarti a non cadere in questo tipo di truffe:

- Diffida di qualunque mail che ti richieda l'inserimento di dati riservati riguardanti codici di carte di pagamento, chiavi di accesso al servizio di home banking o altre informazioni personali.
- È possibile riconoscere le truffe via e-mail con qualche piccola attenzione. Generalmente queste email 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. Nel caso in cui ricevi un'e-mail contenente richieste di questo tipo, non rispondere ma cestinala subito ed eventualmente informa la Banca tramite il call center.
- Non cliccare su link presenti in e-mail sospette, questi collegamenti potrebbero condurti a un sito contraffatto, difficilmente distinguibile dall'originale. Anche se sulla barra degli indirizzi del browser viene visualizzato l'indirizzo corretto, non ti fidare: è possibile infatti per un hacker visualizzare nella barra degli indirizzi del tuo browser un indirizzo diverso da quello nel quale realmente ti trovi.
- Diffida se improvvisamente cambia la modalità con la quale ti viene chiesto di inserire i tuoi 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, contatta la Banca tramite il call center. Infatti ogni variazione alle modalità di accesso ai nostri servizi on line, ti verrà sempre comunicata in anticipo.
- Controlla regolarmente gli estratti conto del tuo conto corrente e delle carte di credito per assicurarti che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contatta la Banca e/o l'emittente della carta di credito.
- 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 tuo browser sia aggiornato; in caso contrario, è consigliabile scaricare e installare le patch.
- Modificare frequentemente la password, utilizzando l'apposita funzionalità presente nella sezione "SICUREZZA →GESTIONE CREDENZIALI".
- I codici di identificazione e di autenticazione sono strettamente personali: non divulgarli assolutamente a terze persone e vanno custoditi separatamente.
- È opportuno effettuare l'operazione di Logout (cliccando sull'apposito tasto) quando si termina la navigazione sul sito o quando ci si allontana dal computer che si sta utilizzando.
- Internet è un po' come il mondo reale: come non daresti a uno sconosciuto il codice PIN del tuo bancomat, allo stesso modo occorre essere estremamente diffidenti nel consegnare i tuoi dati riservati senza essere sicuri dell'identità di chi li sta chiedendo. In caso di dubbio, rivolgiti alla Banca.

Memorizzazione dei codici d'accesso

Spesso, quando in una pagina web vengono inseriti codice utente e password appare una finestra del browser che chiede "Si desidera salvare la password in modo da non doverla ridigitare alla visita successiva"? Se si risponde con 'Sì' il browser memorizza questi dati che al collegamento successivo vengono suggeriti in automatico all'utente.
Questa funzione può compromettere la sicurezza, specialmente in casi dove più persone accedono allo stesso PC. Perciò consigliamo di disattivare questo completamento automatico.