Banca del Lazio Popolare

Consigli utili per navigare in sicurezza

DEVI SAPERE CHE

I pagamenti effettuati via internet sono protetti da una *"autenticazione forte dell'utente"*, in modo da garantirne l'autenticità. Si tratta di una procedura basata sull'utilizzo congiunto di due o più dei seguenti elementi:

- qualcosa che solo l'utente conosce (es. password, PIN, ecc.);
- qualcosa che solo l'utente possiede (es. telefono cellulare, carta di credito, token, ecc.);
- qualcosa che l'utente è (es. impronta digitale, timbro vocale, retina, iride, ecc.).

Le regole per la definizione delle credenziali utente prevedono l'assegnazione di una User ID e di un PIN, consegnato in busta chiusa e sigillata unitamente ad un dispositivo "One Time Password" (OTP), generatore di codici, non ripetibili, validi per 30 (trenta) secondi e da immettere per disporre operazioni di pagamento.
Per l'accesso al canale web, hai un numero massimo di 5 (cinque) tentativi di *login* o di autenticazione, mentre la sessione di lavoro, dopo un periodo di inattività di 30 minuti, scade e non è più utilizzabile.

RICORDA

Il PIN deve essere sostituito al primo accesso inserendo una password personale formata da almeno 8 (otto) caratteri (alfanumerici e speciali).
Il dispositivo "OTP" è personale e deve essere custodito accuratamente dal titolare del rapporto e non deve essere ceduto ad altri soggetti.

Per le carte di credito Cartasì e la carta prepagata con IBAN "BPLazio Card", la *"autenticazione forte dell'utente"* è assicurata dal sistema di protezione antifrode "3D Secure", da applicare per i pagamenti *online* effettuati con carta di credito su siti Internet convenzionati.
Per quanto concerne le carte di credito emesse da CartaSì, l'iscrizione al sistema deve essere effettuata direttamente sul portale della società emittente.
Per quanto attiene, invece, la carta "BPLazio Card", l'iscrizione al "3D Secure" deve essere effettuata tramite utilizzo del canale internet banking, inserendo una password OTP generata dal dispositivo collegato al rapporto di banca virtuale.
Per entrambe le carte, in fase di iscrizione verrà richiesto l'inserimento e la conferma di una password e di una frase identificativa. In fase di pagamento con carta di credito su un sito convenzionato "3D Secure", comparirà una apposita maschera riportante la frase identificativa scelta in fase di iscrizione al servizio, insieme ad un campo per l'inserimento della password. Una volta convalidata la password dall'ente emittente della carta, la transazione verrà completata.

RICORDA

La carta è personale e non deve essere ceduta.
Custodisci, inoltre, con la massima cura la password e la frase identificativa in luogo diverso da quello della carta.
In caso di smarrimento o di furto della carta di credito di Cartasì, rivolgiti al numero verde 800 151616; per le carte emesse dalla Banca Popolare del Lazio, rivolgiti alla Tua filiale di riferimento.

Consigli utili per navigare in sicurezza

ATTENTO AL 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.

RICORDA

Banca Popolare del Lazio non ti chiederà mai attraverso mail o contatti telefonici, dati di accesso personali come password, numero di carta di credito o di conto corrente, né tantomeno la loro modifica in caso di scadenza della password. 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*.
Se temi di essere stato vittima di una frode, inviaci immediatamente una segnalazione all'indirizzo ufficio.reclami@pec.bplazio.it, allegando l'email sospetta.

COME INDIVIDUARE IL TENTATIVO DI FRODE
Molti messaggi sono facilmente riconoscibili perché evidentemente contraffatti e presentano delle caratteristiche comuni:

- ✓ generalmente non sono personalizzati, hanno un contenuto generico di richiesta informazioni per un motivo non specificato quale ad esempio: smarrimento, scadenza, problemi tecnici;
- ✓ spesso sono minacciosi, cioè intimano la sospensione dell'account se l'utente non risponde o non compie l'azione richiesta;
- ✓ riportano contenuti in italiano sgrammaticato.

COME DIFENDERSI

- ➢ Attiva in internet banking il pacchetto *SMS Alert* Sicurezza per ricevere un messaggio sul tuo smartphone ogni volta che effettui un accesso sul tuo rapporto, un bonifico Italia o estero Area SEPA, un bonifico *Mybank*, il pagamento di un bollettino postale o una ricarica telefonica. L'attivazione del pacchetto SMS Alert Sicurezza può essere eseguita accedendo al menu "Altri Servizi", scelta "Alert", procedendo a configurare quelle di interesse.
- ➢ Non rispondere direttamente all'email sospetta ma contatta la tua filiale negli orari di sportello oppure chiama il servizio **Help Desk** al numero **800 119678**.
- ➢ Non cliccare sui link presenti nel messaggio perché potresti ritrovarti su un sito contraffatto che è difficile distinguere dall'originale;
- ➢ In caso di manutenzioni straordinarie o di indisponibilità dei servizi di Intenet Banking, chiama il numero di assistenza **Help Desk 800 119678** e non cliccare su *link* opzionali proposti.

Consigli utili per navigare in sicurezza

- La Banca Popolare del Lazio non chiede mai l'inserimento contemporaneo dei dati personali (Codice Cliente e PIN) e del Codice OTP;
- Se improvvisamente cambia la modalità attraverso cui sei abituato ad accedere al tuo servizio di Internet banking (es. un pop-up cioè una finestra più piccola rispetto a quella originale), non inserire i tuoi codici personali. Ogni variazione alle modalità di accesso ai nostri servizi on line, ti verrà sempre comunicata in anticipo;
- Accedi al sito internet della Banca digitando l'indirizzo www.bplazio.it nello spazio predisposto del tuo navigatore (*browser*) e da lì accedi alla sezione dedicata cliccando sull'apposito link;
- Evita il "salvataggio automatico" delle tue password quando navighi in rete;
- Verifica sempre, dopo aver inserito il tuo Numero Cliente e PIN, che l'indirizzo nella barra di navigazione del tuo browser sia un sottodominio di https://www.banking4you.it/fec/. Al riguardo, la sigla "https://" (*solitamente accompagnata da un lucchetto chiuso o da una scritta in verde*) indica l'utilizzo di un protocollo di cifratura dei dati trasmessi durante la connessione che garantisce una maggiore sicurezza nelle transazioni
- Non salvare l'indirizzo dell'Area riservata all'interno del menù "Preferiti" del tuo *browser*, potrebbe essere intercettato da virus presenti sul tuo computer;
- Aggiorna di frequente il tuo programma Antivirus e utilizza dispositivi di filtraggio affidabili (Firewall).

REGOLE PER I DISPOSITIVI "*MOBILE*"

Di seguito si riporta una sintesi dei principali comportamenti da tenere per un corretto utilizzo del proprio "dispositivo mobile" in termini di "sicurezza".

Regole generali

- ✓ Installa un software di sicurezza (antivirus) e tienilo sempre aggiornato, per evitare infezioni sul dispositivo.
- ✓ Tieni il Sistema operativo del *device* sempre aggiornato, scaricando gli ultimi aggiornamenti disponibili.
- ✓ Non lasciare mai il tuo dispositivo incustodito in aree pubbliche.
- ✓ Utilizza le funzioni di blocco della schermata di accesso del tuo dispositivo, e cambia spesso il codice.
- ✓ Elimina informazioni riservate dal dispositivo prima di qualsiasi intervento di assistenza o manutenzione.
- ✓ Non custodire informazioni finanziarie (numeri di carte di credito, *password* di accesso agli *store*, pin etc.) sul dispositivo.

Per l'installazione e la gestione delle APP

- ✓ Scarica applicazioni e software soltanto dagli *store* ufficiali e se possibile esamina i feedback di altri utenti.
- ✓ Durante l'installazione delle APP presta attenzione alle autorizzazioni e ai permessi richiesti dalle APP stesse.
- ✓ Interrompi il servizio APP di mobile banking se il tuo dispositivo viene rubato e comunica il furto alla tua Banca.

Consigli utili per navigare in sicurezza

"Come proteggersi dal PHISHING - Decalogo ABI Lab per i clienti"

ABI Lab, grazie all'attività della Centrale d'allarme per attacchi informatici il cui compito è quello di arginare l'evoluzione del fenomeno fraudolento del furto di identità elettronica tramite Internet, ha diffuso 2 decaloghi comportamentali diretti rispettivamente alle banche e alla clientela.

Qui di seguito riportiamo il secondo, in una versione aggiornata ed integrata con ulteriori contromisure.

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

2. E' 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 informazioni personali per motivi non ben specificati;
   - fanno uso di toni "intimidatori", ad esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'utente;
   - promettono remunerazione immediata a seguito della verifica delle proprie credenziali di identificazione;
   - non riportano una data di scadenza per l'invio delle informazioni.

3. Nel caso in cui riceviate un'e-mail con richieste di questo tipo, non rispondete ma informate subito la vostra banca tramite il Call Center o recandovi in Filiale;

4. Non cliccate su link presenti in e-mail sospette, in quanto potrebbero condurvi ad un sito contraffatto, difficilmente distinguibile dall'originale. Diffidate inoltre di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali, oppure sequenze casuali di caratteri;

5. Quando inserite dati riservati in una pagina web, assicuratevi che si tratti di una pagina protetta: l'indirizzo comincia con "https://" e non con "htpp://" e nella parte in basso a destra è presente un lucchetto. Al riguardo, si sottolinea la necessità di stabilire l'autenticità della connessione sicura facendo doppio click sul lucchetto in basso a destra e verificando la correttezza delle informazioni di rilascio e validità che compaiono per il relativo certificato digitale;

6. 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. In questo caso contattate la vostra banca tramite il Call Center o recandovi in Filiale;

7. 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;

8. Le aziende produttrici dei browser rendono periodicamente disponibili on-line e scaricabili gratuitamente degli aggiornamenti (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 ed installare le patch;

9. Sia le e-mail che i siti di phishing tentano spesso di installare sul computer della vittima codice malevolo atto a carpire le informazioni personali in un secondo momento, attivandosi nel momento in cui vengono digitate. Si può impedire tale operazione tenendo sempre aggiornato il software anti-virus;

10. In caso di dubbio, rivolgetevi alla vostra banca!