Banca Popolare di Fondi
Fondata nel 1891

INFORMATIVA ANTITRUFFA

Si segnala che negli ultimi anni si sono verificati, in particolare a danno dei clienti dei servizi bancari on-line, numerosi tentativi di furto finalizzati sia all'appropriazione fraudolenta di credenziali di accesso a tali servizi e di altre informazioni riservate, sia al trasferimento fraudolento di denaro verso altri conti bancari.

Le modalità attraverso le quali vengono realizzate tali frodi sono in continua evoluzione e comprendono sia tecniche informatiche sia strumenti di comunicazione elettronica.

È nota, ad esempio, l'esistenza del cosiddetto **"phishing"**, che consiste nell'invio di e-mail apparentemente provenienti dal proprio istituto bancario o da altri soggetti affidabili, nelle quali viene richiesto di fornire informazioni riservate, quali codici di accesso, credenziali personali o altri dati sensibili, oppure di accedere a collegamenti ipertestuali che rimandano a pagine web fraudolente.

Analoga finalità presenta il fenomeno dello **"smishing"**, che consiste nell'invio di messaggi SMS fraudolenti, apparentemente provenienti dalla banca o da altri soggetti di fiducia, contenenti richieste di dati riservati o inviti ad accedere a collegamenti presenti nel messaggio, facendo leva su fittizie operazioni fatte con la carta o fantomatici blocchi della stessa.

Analogamente esiste il cosiddetto **“vishing”**, che consiste in chiamate telefoniche fraudolente, apparentemente provenienti dalla banca o da altri soggetti affidabili, mediante le quali il cliente viene indotto, spesso facendo leva su presunte urgenze o anomalie di sicurezza, a comunicare credenziali di accesso, codici dispositivi, codici generati dal Token o altre informazioni riservate.

Si segnala inoltre la diffusione di **siti internet falsi**, realizzati per riprodurre fedelmente l'aspetto grafico dei siti istituzionali della banca o di altri operatori, allo scopo di indurre il cliente ad inserire le proprie credenziali di accesso o altri dati riservati, che vengono successivamente utilizzati per finalità illecite.

Un’ulteriore tipologia di truffa è il cosiddetto **“man in the middle”**. In questo caso, un software malevolo infetta il computer del cliente e si inserisce nella navigazione dopo l’accesso all’Internet Banking. Il cliente può quindi visualizzare una falsa richiesta di inserimento del codice token, che viene subito utilizzato dai truffatori, a sua insaputa, per disporre un’operazione fraudolenta.

È altresì opportuno prestare particolare attenzione ai messaggi che segnalano presunti problemi di sicurezza, blocchi dell'utenza, anomalie del conto corrente o richieste di aggiornamento delle credenziali, soprattutto quando inducono ad agire con urgenza. La banca non richiede mai, tramite e-mail, SMS o telefono, la comunicazione delle credenziali di accesso, dei codici generati dal Token o di altri codici dispositivi.

Per questo motivo la Banca Popolare di Fondi suggerisce di rispettare le seguenti regole di sicurezza:

1. **Installare e mantenere costantemente aggiornati i software dedicati alla sicurezza dei PC**, quali, a titolo esemplificativo e non esaustivo, Antivirus, Anti-spyware e Firewall, verificandone periodicamente il corretto funzionamento.

2. **Custodire con cura i propri dati di accesso**, non salvandoli sul proprio computer, mantenendo separati username e password che devono rimanere strettamente riservati.

3. **Non fornire MAI le proprie password, i codici dispositivi o altri codici di sicurezza** tramite e-mail, SMS, telefono o altri canali di comunicazione, anche qualora il mittente sembri riconducibile alla banca. Si precisa che nessun dipendente della Banca è autorizzato a richiederli; pertanto, la banca non invierà mai richieste in tal senso, sia di persona sia tramite telefono, posta, e-mail o altro mezzo.

4. **Accedere ai servizi esclusivamente mediante il sito internet ufficiale della banca**, raggiungibile digitandone direttamente l'indirizzo **www.bpfondi.it**, evitando di cliccare su eventuali collegamenti contenuti in e-mail, SMS o altri messaggi ricevuti.

5. **Verificare attentamente che la pagina web in cui si inseriscono dati personali sia in modalità protetta**, controllando la presenza del protocollo **https** prima dell'indirizzo del sito e del simbolo del lucchetto chiuso, o similari, nella barra del browser.

6. **Prestare la massima attenzione alla presenza di pagine o maschere "manipolate"**, ovvero che presentino differenze, più o meno evidenti, rispetto a quelle del sito di Internet banking, oppure contenuti sospetti (ad esempio messaggi non in lingua italiana); in tali casi interrompere immediatamente la navigazione.

7. **Non inserire mai la password se non si sta eseguendo l'accesso al servizio di Internet banking raggiunto dal sito della Banca.**

8. **Controllare regolarmente gli estratti conto ed i movimenti dei propri conti e depositi**, segnalando tempestivamente alla banca qualsiasi operazione non riconosciuta.

9. **Contattare immediatamente la propria filiale o l'Help Desk** nei seguenti casi:
    - Sono stati forniti a terzi i propri codici di accesso;
    - È stata dimenticata la propria password o persa la busta PIN per il primo accesso (prima di essersi collegati per la prima volta);
    - Sono state ricevute e-mail, SMS o chiamate "sospette";
    - Si notano transazioni sospette ed inattese nell'estratto conto.