

INFORMATIVA ANTITRUFFA

Si segnala che negli ultimi anni si sono verificati, in particolare ai danni di clienti dei servizi bancari online, numerosi tentativi di truffa finalizzati al trasferimento fraudolento di denaro verso altri conti bancari e all'acquisizione per scopi illeciti di dati riservati e/o user-id e password.

Le cosiddette truffe del tipo "**man in the browser**" ad esempio, consistono nell'infezione del personal computer del cliente da parte di software malevoli, i quali si inseriscono nella navigazione dell'utente successivamente alla fase di accesso all'applicativo di Internet Banking e presentano ad un certo punto una richiesta di inserimento del codice token, che verrà poi immediatamente utilizzato, all'insaputa del cliente, per effettuare un'operazione fraudolenta, tipicamente il trasferimento di una somma verso un conto corrente estero mediante un bonifico.

Un'altra tipologia di truffa è il cosiddetto "**phishing**", che consiste nell'invio di e-mail, solo in apparenza provenienti dal proprio istituto bancario (del quale è riprodotta fedelmente anche l'impostazione grafica), in cui si richiede al destinatario di fornire informazioni riservate. Spesso queste richieste sono motivate con ragioni di natura tecnica, falsi problemi di sicurezza o con l'attrattiva di ricevere premi e partecipare a concorsi.

Possibili informazioni utilizzabili in modo illecito e a danno del cliente possono essere:

- codici di accesso (username e password), che consentono ai truffatori di accedere ai servizi online del cliente e di operare in sua vece;
- dati relativi alle carte di credito, utilizzabili per acquisti all'insaputa e a spese del cliente;
- dati personali in genere.

Per quanto concerne i propri servizi online, la Banca Popolare di Fondi suggerisce di:

1. **Installare e mantenere costantemente aggiornato il software dedicato alla sicurezza**, in particolare: Antivirus, Anti-spyware, Firewall, etc.
2. **Custodire con cura i propri dati di accesso**, non salvandoli sul proprio computer, mantenendo separati username e password, e modificando periodicamente quest'ultima.
3. **Non fornire MAI le proprie password ad alcuno**. Si precisa che nessun dipendente della banca è autorizzato a richiederle, pertanto la banca non le invierà mai qualsiasi richiesta in tal senso, sia essa effettuata di persona oppure tramite telefono, posta, e-mail o altro mezzo.
4. **Accedere sempre ai servizi online digitando www.bpfondi.it**, evitando di cliccare su eventuali collegamenti presenti nelle e-mail e di dare adito ad eventuali richieste in esse contenute.
5. **Assicurarsi che la pagina web in cui si inseriscono dati personali sia protetta**, verificando che l'indirizzo sia preceduto da "https" o che sia presente l'icona che attesta il collegamento ad un sito protetto, solitamente raffigurante un lucchetto chiuso.
6. **Prestare la massima attenzione alla presenza di pagine o maschere "manipolate"**, ovvero che presentano un aspetto grafico differente rispetto a quelle dell'applicativo di internet banking, oppure con dei contenuti sospetti (es. messaggi non in lingua italiana).
7. **Non inserire mai il codice token se viene richiesto in una fase in cui non si sta eseguendo alcuna disposizione di pagamento**.
5. **Controllare regolarmente gli estratti conto dei propri conti e depositi**, per assicurarsi che le transazioni riportate siano quelle realmente effettuate.
7. **Contattare immediatamente l'Help Desk nei seguenti casi:**
 - Sono stati forniti a terzi i propri codici di accesso;
 - E' stata dimenticata la propria password o persa la busta PIN per il primo accesso (prima di essersi collegati per la prima volta);
 - Si sono ricevute e-mail "sospette";
 - Si notano transazioni sospette ed inattese nell'estratto conto.

BANCA POPOLARE DI FONDI
LA DIREZIONE