

## 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 all'acquisizione per scopi illeciti di dati riservati e/o user-id e password.

Il cosiddetto "**phishing**" ad esempio 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.

Le suddette e-mail contengono solitamente:

- una richiesta di risposta urgente, in cui l'utente fornisca informazioni riservate;
- collegamenti a siti internet del tutto identici al portale dell'istituto, ma gestiti dagli autori della truffa, in cui l'utente è ingannevolmente indotto ad inserire informazioni riservate;
- collegamenti al sito originale dell'istituto, ma che provocano l'apertura di una finestra in sovrapposizione (cosiddetta "pop-up") introdotta in modo fraudolento dai truffatori stessi, e in cui l'utente è ingannevolmente indotto ad inserire informazioni riservate.

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 suggerisce di:

1. **Custodire con cura i propri dati di accesso**, non salvandoli sul proprio computer, mantenendo separati username e password, e modificando periodicamente quest'ultima.
2. **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.
3. **Accedere sempre ai servizi online digitando [www.bpfondi.it](http://www.bpfondi.it)**, evitando di "cliccare" su eventuali collegamenti presenti nelle e-mail e di dare adito ad eventuali richieste in esse contenute.
4. **Assicurarsi che la pagina web in cui si inseriscono dati personali sia protetta**, diffidando dei "pop-up". Per verificare che la pagina web sia protetta, controllare che l'indirizzo sia preceduto da "https" e che sul browser sia presente l'icona che attesta il collegamento ad un sito protetto, solitamente posizionata in basso a destra e raffigurante un lucchetto chiuso.
5. **Controllare regolarmente gli estratti conto dei propri conti e depositi**, per assicurarsi che le transazioni riportate siano quelle realmente effettuate.
6. **Installare e mantenere costantemente aggiornato il software dedicato alla sicurezza**, in particolare: Sistema Operativo, Personal Firewall, Antivirus ed Anti-spyware.
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**