INFORMATIVA SULL'IMPIEGO DEL TOKEN MOBILE

Le frodi elettroniche: "phishing" e "malware"

L'utilizzo dello strumento Token mobile è stato introdotto allo scopo garantire al cliente una maggiore protezione contro le minacce on-line, in particolare il furto di identità e l'appropriazione dei dati di accesso ai servizi bancari per uso fraudolento, che vengono eseguiti sfruttando la rete internet.

E' nota ad esempio l'esistenza del cosiddetto "**phishing**", che consiste nell'invio di e-mail da parte di organizzazioni criminali, ma in apparenza provenienti dal proprio istituto bancario (del quale è riprodotta fedelmente anche l'impostazione grafica), in cui si richiede di fornire informazioni riservate.

Si segnala inoltre la diffusione di particolari tipi di "virus" informatici, denominati "**spyware**" o "**malware**", che possono installarsi sul PC del cliente a sua insaputa durante la navigazione in internet. Questi software sono in grado di spiare informazioni personali, inclusi i codici di accesso, per trasmetterli poi a frodatori che li utilizzeranno per scopi illeciti.

La direttiva PSD2

Dal 14/09/2019 è in vigore la Direttiva sui Servizi di Pagamento, nota con l'acronimo PSD2, che si pone l'obiettivo primario di rendere più conveniente la gestione dei pagamenti in Europa, rafforzando al contempo la tutela degli utenti, la trasparenza e la sicurezza.

Con particolare attenzione al tema della sicurezza, la direttiva regola i requisiti obbligatori cui la Banca deve conformarsi, introducendo alcune misure rafforzate di autenticazione, al fine di identificare in maniera sicura il cliente preservando così la riservatezza e l'integrità dei suoi dati.

In particolare è reso obbligatorio l'utilizzo di standard più stringenti di sicurezza che richiedono:

- L'accertamento dell'identità del cliente attraverso due o più strumenti di autenticazione, c.d. "Autenticazione Forte" o "Strong Customer Authentication" (SCA);
- L'utilizzo di collegamenti dinamici che certifichino l'unicità della transazione ("Collegamento Dinamico" o "Dynamic Linking"). Tale sistema impone che l'autenticazione di ciascuna operazione di pagamento avvenga tramite un codice univoco associato a quella transazione e alle sue caratteristiche (importo, beneficiario).

L'utilizzo del dispositivo Token mobile assolve proprio a tali funzioni.

Che cos'è il "Token mobile"

Il token mobile è lo strumento di autorizzazione integrato nell'App "BPFondi Mobile", con il quale è possibile autorizzare l'accesso da Home Banking e App bancaria e confermare le operazioni dispositive .

L'app "BPFondi Mobile", è disponibile su tutti i tablet e smartphone iOS e Android.

Sicurezza offerta

L'utilizzo del Token mobile garantisce al cliente che le operazioni on-line siano effettuate solo da chi è in possesso di tale strumento (oltre che della password di accesso all'applicativo bancario). Inoltre, il PIN personalizzato garantisce un'ulteriore sicurezza e protezione dalle frodi nell'uso dell'Internet Banking, sia da Home Banking che da App.

Attivazione del "Token mobile"

L'attivazione del Token mobile avviene direttamente dalla App BPFondi Mobile.

Dopo aver effettuato l'accesso in BPFondi Mobile, tramite credenziali di autenticazione o tramite

riconoscimento biometrico/Face ID (se già attivato), è necessario seguire i semplici passaggi visualizzati sullo schermo per l'attivazione. In particolare:

· selezione di uno dei numeri di cellulare, indicati alla filiale, su cui ricevere (via SMS) il codice temporaneo da inserire nell'apposito campo.

· abilitazione del Token mobile, indicando il numero di cellulare e impostando un mobile pin personalizzato.

Accesso e autorizzazione delle operazioni

Ad ogni accesso sul portale di Home Banking oppure eseguendo una funzione dispositiva si potrà scegliere di ricevere una notifica push sull'App con gli estremi dell'operazione da autorizzare tramite mobile pin.

Qualora il dispositivo non sia collegato ad internet o non ci sia rete, è possibile inquadrare, tramite la specifica funzione prevista nel menu "Token Mobile" dell'App, un Qr-code per proseguire nell'operatività.

Servizio clienti

Per le richieste di assistenza è possibile contattare il nostro servizio clienti al seguente numero verde: **800.555.812**.

Il servizio è attivo tutti i giorni, festivi compresi, 24 ore su 24.

Oltre che mediante il numero verde i clienti possono contattare l'Help Desk anche tramite l'indirizzo email: ***tecsupport@csebo.it***

Le aree di copertura del servizio sono relative a:

- richieste di supporto nell'esecuzione delle varie funzionalità delle applicazioni di Internet Banking;
- sblocco dei tentativi di accesso errati effettuati dai clienti, nella digitazione della password.