

INFORMATIVA SUL SISTEMA SECURECALL

Le frodi elettroniche: "phishing", "smishing" e siti internet falsi

L'utilizzo del dispositivo Token è stato introdotto allo scopo di 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, realizzati mediante strumenti informatici e 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.

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. Si raccomanda pertanto di non comunicare mai a terzi le proprie credenziali di accesso, i codici generati dal Token o altri codici dispositivi, di verificare sempre l'autenticità del sito internet utilizzato per accedere ai servizi di Internet Banking e di prestare particolare attenzione alle comunicazioni ricevute tramite e-mail o SMS che richiedano l'inserimento di dati riservati o l'esecuzione di operazioni urgenti.

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 assolve proprio a tali funzioni.

Che cos'è il servizio SecureCall

SecureCall permette di autorizzare le operazioni dispositive effettuate con l'applicativo di Internet banking BPF OnLine attraverso una semplice chiamata dal proprio cellulare ad un numero verde.

SecureCall è ad oggi uno dei sistemi di autorizzazione più sicuri sul mercato. È semplice da utilizzare e non richiede ulteriori password o altri strumenti che non sempre si hanno a portata di mano (es. dispositivi token).

Sicurezza offerta

L'utilizzo del servizio SecureCall consente di rafforzare la sicurezza in fase di accesso al servizio di Internet Banking e di inserimento delle operazioni dispositive effettuate tramite lo stesso, assicurando che l'autorizzazione dell'operazione avvenga attraverso un canale distinto da quello utilizzato per l'inserimento dei dati on-line. In particolare, l'operazione viene predisposta tramite la rete Internet,

mentre la conferma è eseguita mediante chiamata telefonica dalla rete mobile associata al cliente. Tale separazione dei canali riduce il rischio di utilizzi non autorizzati e contribuisce a garantire che le disposizioni siano confermate esclusivamente dal titolare abilitato al servizio.

Modalità di accesso e autorizzazione delle operazioni

In fase di accesso al servizio di Internet Banking, dopo l'inserimento delle credenziali personali, e in fase di autorizzazione delle operazioni dispositive, il sistema propone una schermata contenente le istruzioni necessarie per completare la procedura di autenticazione. In particolare, al cliente viene richiesto di effettuare, dal numero di telefono cellulare registrato presso la Banca e abilitato al servizio, una chiamata al numero verde indicato a video.

Durante la chiamata, il cliente dovrà digitare sulla tastiera del telefono il codice numerico di 4 cifre visualizzato sullo schermo, quando richiesto dal sistema. A seguito del corretto inserimento del codice, verrà mostrata a video la conferma dell'avvenuto accesso o del buon esito dell'operazione dispositiva.

Operazioni effettuate dall'estero

Nel caso in cui il cliente si trovi all'estero, dovrà selezionare l'opzione: *“Sono all'estero e voglio procedere alla conferma dell'operazione attraverso cellulare”*. In questo caso il cliente verrà chiamato automaticamente dal sistema sul numero di cellulare abilitato al servizio e dovrà digitare il codice visualizzato sullo schermo.

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.