INFORMATIVA SULL'IMPIEGO DEI DISPOSITIVI TOKEN

Le frodi eletroniche: "phishing" e "malware"

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

Che cos'è il "token"

Il token è un dispositivo elettronico dotato di display, che genera, a fronte della pressione di un apposito tasto, e per una durata di alcuni secondi, un codice numerico di 6 cifre (codice token), che dovrà essere inserito per l'autenicazione e per l'autorizzarzione delle operazioni bancarie (ad esempio bonifici, pagamenti MAV, RAV, ordini titoli, etc.). Ad ogni pressione del tasto il dispositivo genera un nuovo codice numerico diverso dai precedenti.

Si tratta di una sorta di password "monouso", che va inserita nell'apposito campo di conferma nella fase conclusiva delle operazioni.

Sicurezza offerta

L'utilizzo del token 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, poiché il codice cambia di volta in volta, non c'è il rischio che questo possa essere usato da altri dopo essere stato "spiato".

Modalità di utilizzo in fase di autenticazione

Dopo aver inserito le credenziali di accesso all'applicativo di internet banking, verrà proposta una maschera che richiederà l'inserimento del codice token (OTP).

Per completare l'accesso, accendere il dispositivo premendo il tasto **OK** e successivamente premere il tasto numerico **1**. Sul display apparira il codice numerico a 6 cifre generato dal dispositivo che dovrà essere inserito nella maschera.

Autorizzazione delle operazioni

Una volta confermata l'operazione che si desidera effettuare e compilati i dati richiesti, verrà presentata una maschera con le istruzioni operative, che prevedono l'accensione del dispositivo premendo il tasto **OK** e la selezione della funzione OTP collegata all'operazione, premendo il tasto numerico **3**.

A questo punto va digitato sul tastierino numerico del dispositivo token il codice mostrato a video nella maschera di conferma, premendo poi il tasto **OK**. Verrà mostrato sul display il codice token da inserire nella maschera per confermare l'operazione.

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.