



## Strumenti di sicurezza SIMPLYBANK WEB

### Servizio TOKEN



Disponibile gratuitamente per i clienti della Cassa Rurale Alta ValdiSole e Pejo, è un dispositivo collegato alla propria postazione SimplyBank Web che aumenta la protezione dei dati personali e dei pagamenti. Esso genera una password dinamica di 8 cifre monouso, e quindi non identificabile.

### Certificato Client

E' un'impostazione di sicurezza da installare nel browser dell'utente attraverso una procedura guidata e contiene informazioni che identificano l'utente stesso in modo univoco. L'accesso al SimplyBank Web è permesso esclusivamente utilizzando il browser sul quale è installato il certificato valido. Esso fornisce una maggiore garanzia in quanto permette l'accesso esclusivamente all'utente che ha installato il certificato e dalla postazione sulla quale esso è installato. Quindi, anche se terze persone dovessero entrare in possesso delle credenziali dell'utente (userID e password), avrebbero l'accesso negato in quanto si collegherebbero da una postazione diversa da quella del cliente.

### Autenticazione login mediante squillo telefonico

E' un servizio di autenticazione che consente di validare l'accesso a SimplyBank Web mediante l'utilizzo di un cellulare o telefono fisso. L'utente che attiva questo sistema di sicurezza, prima di accedere a SimplyBank Web dovrà effettuare uno squillo dal numero telefonico associato alla propria utenza ad un numero telefonico opportunamente predisposto entro 30 secondi. Il sistema autorizzerà l'accesso solo se è pervenuta la chiamata nell'arco temporale definito e se il numero di telefono è valido.

### Autorizzazione disposizioni via SMS

E' un servizio che permette di autorizzare le disposizioni di pagamento mediante l'invio di un SMS inviato da un numero telefonico associato all'utente, contenente un numero di autorizzazione (token dispositivo) associato alle distinte inviate in una sessione di lavoro.

Nella pagina che notifica al cliente l'esito dell'invio della distinta di pagamento, saranno indicati il token dispositivo e il messaggio che invita il cliente ad autorizzare la disposizione attraverso l'invio di un messaggio SMS indicante tale token, entro 2 giorni.

Alla ricezione del messaggio SMS e dopo la validazione del numero di cellulare dal quale il messaggio è stato inoltrato il sistema autorizzerà le disposizioni.



### **Notifica disposizioni via SMS/via e-mail**

Il servizio permette di notificare agli utenti SimplyBank Web le disposizioni effettuate con la propria utenza. Al momento della contabilizzazione delle disposizioni, viene inviato all'utente un SMS (o una mail) riepilogativo per ogni tipologia di disposizione effettuata.

### **Notifica Login via SMS/via e-mail**

Il servizio permette di notificare agli utenti gli accessi effettuati attraverso la propria utenza. Ad ogni accesso, viene inviato un SMS (o una mail) al cliente.

### **Raccomandazioni**

Il TOKEN innalza notevolmente il livello di sicurezza della propria stazione SimplyBank Web. Nonostante questo si consiglia caldamente l'utilizzo combinato di più servizi di sicurezza scegliendo tra quelli disponibili.

In tal senso è buona norma abbinare al TOKEN anche il servizio di "Notifica Login" o "Notifica Disposizioni" (via e-mail o via SMS). Si consiglia inoltre di accedere ai servizi di Internet Banking cliccando l'apposito link presente sul sito ufficiale della Cassa Rurale Alta ValdiSole e Pejo raggiungibile all'indirizzo <http://www.cr-avaldisole.net>

### **Attenti al "Phishing"**

Una nuova frontiera della truffa on-line è rappresentata dal cosiddetto "Phishing". Questa tecnica è molto semplice ma anche molto efficace. Attraverso delle e-mail che sembrano provenire dalla propria banca questi "PIRATI INFORMATICI" invitano l'utente a compilare dei campi con i propri dati personali riuscendo in questo modo a sottrarre le credenziali di accesso e codici di vario genere.

Solitamente tale richiesta viene giustificata spiegando che problemi tecnici rendono necessario questa immissione di dati. Compilando questi moduli si forniscono i propri codici di accesso e i numeri delle proprie carte di credito.

Il fenomeno non è circoscritto agli istituti di credito ma è dilagato in tutto il mondo dell'e-business. Le e-mail e le pagine web ai quali si viene rimandati spesso rispecchiano esattamente i siti originali (stessi loghi, stessa grafica).

Come difendersi allora? Per difendersi è sufficiente seguire alcune piccole regole qui riportate:

- 1) Ricordarsi che gli istituti di credito NON richiedono mai password, numeri di carte di credito o altre informazioni personali via e-mail**
- 2) Diffidate delle e-mail che ha un tono intimidatorio o che minacciano la sospensione di servizi o pagamenti/accrediti. Spesso e volentieri queste e-mail contengono molti errori ortografici gravi (anche questo può essere un'allarme)**
- 3) Non rispondere mai a richieste di informazioni personali tramite e-mail (non fornire mai password o PIN).**
- 4) Diffidare dei link a siti esterni contenuti in questa tipologia di e-mail**

