



Internet è entrato nelle nostre case anche per quanto riguarda le diverse operazioni bancarie. A fronte di uno strumento che offre comodità e semplicità di utilizzo è importante però osservare alcune semplici funzionalità che permettono di elevare la protezione ed il controllo sugli strumenti di pagamento.





## Strumenti di sicurezza INBANK

### Servizio TOKEN



Disponibile gratuitamente per i clienti della Cassa Rurale Alta ValdiSole e Pejo, è un dispositivo collegato alla propria postazione InBank Base e InBank Gold che aumenta la protezione dei dati personali e dei pagamenti.

Una volta attivato, l'entrata in InBank e l'invio di una disposizione di pagamento sarà possibile esclusivamente dopo la digitazione della password generata in tempo reale da questo dispositivo. L'associazione del TOKEN alla propria stazione InBank avviene seguendo questi passi operative

Accedere alla propria stazione InBank	
Cliccare sul pulsante <b>"PROFILO"</b> e selezionare la voce <b>"Token"</b> e successivamente <b>"Associazione"</b> .	
A questo punto verrà visualizzata la maschera di Associazione TOKEN. Cliccare sull'icona rappresentata in figura e quindi selezionare <b>"Conferma"</b> .	
Nella prossima schermata premere nuovamente sul pulsante rappresentato in figura e quindi nuovamente su <b>"Conferma"</b>	
Al termine dell'associazione dovrebbe apparire il seguente messaggio	
<b>Per rendere effettive le modifiche è necessario uscire da InBank e rientrare.</b>	

## OBIETTIVO SICUREZZA

### **Blocco/sblocco operatività via SMS** *(servizio attivabile presso gli sportelli della Cassa Rurale)*

Inviando un semplice SMS è possibile inibire (e disinibire) la possibilità di inviare disposizioni di pagamento dalla propria stazione InBank sia verso l'Italia che verso i paesi esteri.

Sintassi del messaggio SMS:

**BPI 12345678** blocco disposizioni Bonifico Italia, Stipendio e Bonifico estero

**BPI 12345678 BOE** blocco solo disposizioni Bonifico estero

**SPI 12345678** sblocco disposizioni Bonifico Italia, Stipendio e Bonifico estero

**SPI 12345678 BOE** sblocco solo disposizioni Bonifico estero

dove **12345678** sta per il codice dell'utenza INBANK (principale).

Il messaggio deve pervenire esclusivamente dal numero di cellulare abilitato dalla Cassa Rurale, al numero **+39 339 9942024**. Non sono previsti SMS di risposta se non nei casi di errore.

### **Alert su disposizioni di bonifico** *(servizio attivabile presso gli sportelli della Cassa Rurale)*

Il servizio di Alert avvisa tramite un SMS l'avvenuta disposizione di un bonifico *(avente un importo superiore alla soglia stabilita dal cliente)* eseguito dalla propria stazione InBank. Questo Alert consente al cliente di intervenire tempestivamente in caso di truffe per bloccare il pagamento stesso.

### **Controllo operatività via email** *(servizio gratuito attivabile direttamente dall'utente)*

Questo servizio notifica via e-mail (inviata all'indirizzo e-mail specificato dall'utente) tutte le operazioni inviate dalla stazione InBank. Nello specifico vengono notificate:

- Data e ora degli accessi effettuati sulla stazione InBank; l'email viene inviata la domenica con cadenza settimanale;
- Segnalazioni dei bonifici effettuati;
- Eventuali modifiche apportate al proprio profilo utente.

L'attivazione avviene seguendo questi passi operativi:

<b>Accedere alla propria stazione InBank</b>	
Cliccare sul pulsante "PROFILO" e selezionare la voce "Preferenze".	 <p>The screenshot shows a navigation menu with two main tabs: "Comunicazioni" and "Profilo". Under the "Profilo" tab, a list of options is displayed: "Sicurezza (modifica password)", "Token", "Preferenze" (highlighted in dark blue), "Multiutenza", "Rapporti ordinante", "Soglie", "Allinea archivi Iban", and "Archivio contatti".</p>

## OBIETTIVO SICUREZZA

Nella schermata visualizzata inserire all'interno del campo "Email" (segnalato dalla freccia) il proprio indirizzo email al quale verranno inviate le notifiche. Una volta inserito l'indirizzo è necessario cliccare sul tasto "Modifica Profilo" presente in fondo alla finestra.

**Preferenze**

**Impostazioni personali**

Segnalazioni tramite Messaggi Ricevuti per: esiti di incasso insoluti, richieste di Allineamento Archivi Rid stornate/rifiutate ed avvisi di scadenza scaduti

**Email periodica per resoconti di sicurezza**

Abilita email periodica per resoconti di sicurezza

**Tipologia file di esportazione (formato CBI e CSV)**

Compatibilità sistema operativo  Windows  Unix

**Email**

Email

**Minuti di inattività**

Minuti di inattività

**Limiti operativi**

Limite per le disposizioni di pagamento: Bonifici Italia, Stipendi, Bonifici estero  €

Limite per tutte le disposizioni di incasso  €

Limite ordine trading  €

Limite giornaliero assegnato dalla banca per: Bonifici Italia, Stipendi, Bonifici estero

Limite assegnato dalla banca per la distinta di Bonifico Estero

Residuo giornaliero pagamenti

**Blocco via SMS di invio disposizioni**

Bonifico italia e stipendi  Non bloccato

Bonifico estero  Non bloccato

### Codice Personale Segreto (CPS)

E' offerto ai clienti che utilizzano in InBank **in sola consultazione** dei movimenti dei rapporti e permette di innalzare il livello di sicurezza offerto dalla sola password alfanumerica.

Il Codice Personale Segreto è costituito da una sequenza di valori numerici casuali la cui posizione è individuata da un carattere alfabetico in forma di semplice tabella (si veda la figura 1)

		MARIO ROSSI																			
		CODICE PERSONALE SEGRETO (CPS)																			
Posizione		A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V
Valore CPS		0	9	7	7	3	8	9	7	9	4	0	9	7	7	3	8	9	7	9	4

Figura 1 - Esempio di CPS.

Il CPS assegnato, dovrà essere stampato e conservato con cura, per poi essere utilizzato nella fase di login. Il codice CPS è disponibile in due diverse dimensioni (tascabile ed esteso) per facilitarne l'uso e la conservazione.

## OBIETTIVO SICUREZZA

Ogniqualvolta sarà richiesta l'autenticazione con CPS, si dovrà cliccare sull'apposito tastierino a video i tre "valori CPS" numerici corrispondenti alle tre diverse posizioni indicate. Per evitare che queste informazioni sensibili possano essere intercettate, la posizione dei tasti sarà variabile e di volta in volta modificata.

A titolo esemplificativo, si veda il processo simulato nelle immagini sottostanti. Nell'esempio la procedura richiede all'utente di identificare il valore CPS corrispondente alla posizione "M" che è facilmente identificabile sul CPS. Infine, utilizzando il tastierino virtuale, l'utente dovrà immettere il valore numerico corrispondente alla posizione richiesta. Questo processo va ripetuto per tutti i tre valori richiesti.

In caso di furto o smarrimento del codice CPS stampato, sarà necessario contattare la Cassa Rurale Alta ValdiSole e Pejo per l'attribuzione di un nuovo codice CPS.



Figura 2 - I tre passi da eseguire per autenticarsi utilizzando il CPS.

### **Raccomandazioni**

Il TOKEN innalza notevolmente il livello di sicurezza della propria stazione InBank. Nonostante questo si consiglia caldamente l'utilizzo combinato di più servizi di sicurezza scegliendo tra quelli disponibili. (il token esclude CPS e viceversa)

In tal senso è buona norma abbinare al TOKEN anche il servizio di "Alert su disposizioni di bonifico" sulle disposizioni (via e-mail o via SMS) oppure il servizio "Blocco/sblocco operatività via SMS". Si consiglia di accedere ai servizi di InBank 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:

## OBIETTIVO SICUREZZA

---

- 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

Si invita inoltre ad una attenta lettura dei “consigli sulla sicurezza” reperibili nella home page del servizio InBank.