Sicurezza dei dati su web

La salvaguardia delle informazioni costituisce elemento fondamentale nelle attività di ViViBanca. I dati sono gestiti dalle applicazioni che forniscono funzionalità agli utenti I cardini su cui si basa la sicurezza dell'informazione sono: Accesso, Riservatezza, Integrità, Distribuzione e Disponibilità.

Della garanzia, sicurezza ed affidabilità delle proprie applicazioni e comunicazioni sul web, ViViBanca si avvale dell'utilizzo di certificati digitali che adottano la tecnologia SSL Secure Socket Layer con soluzioni di crittografia delle informazioni e robuste procedure di autenticazione ad alto livello (il sistema di protezione maggiormente usato sul web).

Il livello di protezione funziona sul doppio riconoscimento dello user e della password assegnata ed è conforme alle norme internazionali per la sicurezza delle applicazioni web.

Tutte le operazioni/transazioni sono protette e certificate da Verisign che attesta la massima integrità e riservatezza dei dati trasmessi.

Minacce informatiche: phishing

Tra le minacce informatiche che si sono diffuse negli ultimi anni, si segnala il phishing, una frode informatica on-line che si concretizza mediante l'invio di e-mail contraffatte che hanno caratteristiche del tutto simili a quelle autentiche. In questo modo il ricevente, con la scusa di verificare la correttezza dei suoi dati personali e riservati, è invitato ad accedere ad un link che lo indirizza al sito del truffatore, richiedendogli di rivelare le proprie credenziali di accesso.

Tali siti pur rassomigliando a quelli ufficiali, sono solo una copia appositamente realizzata dal truffatore per carpire dati dagli utenti (codici di identificazione, codice utente, password). Una volta catturati, questi dati sono poi utilizzati per truffe, operazioni in denaro, oppure per condurre altri attacchi mirati di origine informatica.

Si consiglia pertanto, di non rispondere mai a messaggi di posta elettronica o telefonate con queste caratteristiche (richiesta di informazioni di accesso alla propria area riservata, dati riservati, riferimenti bancari) in quanto le policy di sicurezza di ViViBanca non prevedono, attraverso messaggi di posta elettronica, la richiesta di informazioni personali e dati di accesso all'area riservata del proprio sito.

Per identificare le situazioni potenzialmente pericolose, si raccomanda di prestare attenzione a: il contenuto del testo delle e-mail, spesso si fa riferimento a presunti problemi relativi al rapporto finanziario in corso o al proprio utente.

Sovente il nome del mittente simula un riferimento conosciuto, in realtà l'indirizzo indicato è falso.

Raccomandazioni generali per la sicurezza

Come regola generale si ricorda di:

- cambiare con buona frequenza i codici di accesso alla propria area riservata e conservare con cura gli estremi;
- non diffondere ad alcuno i propri codici di accesso ai servizi web ViViBanca;
- prestare attenzione alle e-mail che richiedono di comunicare i dati di accesso al sito ViViBanca;
- non aprire e-mail reputate sospette;
- dubitare delle comunicazioni di vincite a lotterie, con annesse richieste di pagamento per la riscossione del premio;
- nel caso di diffusione dei codici personali, modificare immediatamente la password di accesso ai servizi e avvisare ViViBanca inviando una e-mail a: websecurity@vivibanca.it;
- mantenere aggiornati il sistema operativo del proprio computer. i browser per la navigazione sul web ed il software dedicato alla sicurezza (antivirus, antispyware);
- effettuare l'installazione dei soli software sicuramente affidabili;
- non rispondere ed aprire e-mail sospette, evitando di cliccare sui link contenuti in essa.