PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 7 - numero 1198 di martedì 08 marzo 2005

Home banking e sicurezza

Dalla Polizia di Stato un vademecum contro il fenomeno del "phishing".

Pubblicità

Anche la Polizia di Stato si mobilita contro il phishing, una particolare forma di frode condotta con line con l'involontario aiuto della vittima, che viene indotta a fornire i dati con i quali accede al proprio conto corrente tramite il sistema di home banking.

Dopo una comunicazione inviata all'Abi (Associazione Bancaria Italiana), per invitare gli istituti di credito ad informare i loro clienti su questo tipo di rischio, la Polizia ha pubblicato sul sito web istituzionale un sintetico vademecum, illustrando per prima cosa le modalità della truffa.

La truffa viene condotta mediante una e-mail con lay-out, logo e indirizzo di provenienza che fanno pensare ad una e-mail proveniente da un istituto di credito.
L'e-mail truffaldina avverte l'utente che si è presentato un problema al sistema di "home banking" e lo invita a cliccare su un link.
L'utente viene così collegato ad un sito web fittizio e invitato ad inserire "user-id" e "password" di accesso all'home banking.
Quando la vittima inserisce i dati, viene avvertita che per "assenza di collegamento non è possibile la connessione". I dati sono già a questo punto in possesso dei truffatori, che possono così liberamente operare dal conto corrente della vittima...

Di seguito riportiamo i consigli forniti dalla Polizia:
1.Gli istituti bancari e le aziende serie non richiedono mai password, numeri di carte di credito o altre informazioni personali in un messaggio di posta elettronica. L'unica circostanza in cui viene richiesto il numero della vostra carta di credito è nel corso di un acquisto on-line che avete voi deciso di fare.
2. Non bisogna rispondere mai a richieste di informazioni personali (PIN, password ecc), anche se provenienti dal vostro istituto di credito, ricevute tramite posta elettronica. Nel dubbio, telefonare all'istituto che dichiara di avervi inviato l'e-mail chiedendo una conferma.
3. Per essere sicuri di accedere ad un sito web "reale" di un istituto bancario è indispensabile digitare il rispettivo indirizzo URL nella barra degli indirizzi, diffidando di link ricevuti via e-mail. Segnalare il sospetto di abuso alla banca.
4. È fondamentale esaminare regolarmente i rendiconti bancari e della carta di credito e in caso di spese o movimenti bancari non riconosciuti informare immediatamente telefonicamente il proprio istituto bancario o la società emittente della propria carta di credito.
5. In caso di sospetto di uso illecito delle proprie informazioni personali per operazioni di phishing occorre informare immediatamente la Polizia Postale e delle Comunicazioni.
