



Truffe e-banking? Paghino le banche

Succede in Corea del Sud dove il Governo intende costringere gli istituti del credito a coprire finanziariamente eventuali frodi commesse a danno dei loro correntisti via internet. I risarcimenti incoraggeranno gli utenti?

L'ultima iniziativa del Governo sudcoreano potrebbe sconvolgere il settore bancario locale. In controtendenza con le policy governative occidentali, il Ministro della Finanza ed Economia ([MoFE](#)) ha proposto una nuova legge che obbligherà le istituzioni finanziarie a **risarcire le vittime di frodi online**.

In questo quadro, dunque, le piattaforme elettroniche per l'e-banking e l'e-trading saranno sotto la totale responsabilità degli enti gestori: nel caso venga comprovato un **attacco informatico** che danneggi gli utenti, le banche saranno obbligate a coprire gli eventuali ammanchi sui conti.

[Korea Exchange Bank](#), insieme alle altre istituzioni finanziarie locali, hanno fatto fronte comune e probabilmente si opporranno in tutti i modi. La prima dichiarazione congiunta ha sottolineato che la prova di responsabilità dovrebbe essere **a carico degli utenti**. Saranno loro quindi a dover dimostrare che il danno è stato provocato da una mancanza da parte delle banche e non da un'imperizia personale. Una questione essenziale sulla quale l'Esecutivo ancora non si è espresso: nella bozza di legge comunque è inserita una norma che annulla qualsiasi risarcimento nel caso in cui l'utente non si sia preoccupato di proteggere adeguatamente password e PIN.

"Non vedo il bisogno di una legge di questo tipo. Le banche risarciscono già le vittime di frodi, nel rispetto delle policy per il cliente", ha dichiarato Richard Starnes, presidente della [Information Systems Security Association](#).

Il problema delle responsabilità sulle eventuali mancanze da parte degli utenti è un tema ampiamente dibattuto. Secondo gli ultimi dati della the [National Cyber Security Alliance](#), infatti, l'80% degli utenti sarebbe esposto alla maggior parte dei pericoli provenienti del Web. Più del 50% non disporrebbe di antivirus e di firewall giustamente configurati. Il 40% non sarebbe dotato di anti-spyware. In pratica, quattro utenti su cinque sarebbero sprovvisti di almeno uno dei tre strumenti base per la protezione informatica. Questi dati, secondo gli analisti, fanno da fondamento alle politiche delle aziende finanziarie. Nessuno vuol farsi carico delle **inadempienze** altrui. Il problema, però, è se gli utenti dispongano di tutte le informazioni necessarie per poter utilizzare i servizi online senza pericolo. Lo stesso vice presidente di AOL, Tatiana Platt, sostiene che "le persone coltivano un falso senso di sicurezza".

Negli USA, [FBI](#) e Federal Financial Institutions Examination Council ([FFIEC](#)) [hanno chiesto](#) alle banche di adottare nuovi sistemi di autenticazione a **due fattori**. Una soluzione avanzata per il riconoscimento degli utenti, che però potrebbe dimostrarsi totalmente inutile se utilizzata su PC completamente privi dei sistemi standard di protezione. Le statistiche confermano che un utente medio nel 70% dei casi **non è in grado** di riconoscere una mail legittima da una di [phishing](#). Si possono implementare, quindi, bunker avanzatissimi, ma se all'entrata il guardiano consuma quotidianamente una pennichella, il tutto è inutile.

Una legge, come quella coreana, che responsabilizza per primi gli enti finanziari coinvolti potrebbe aumentare gli investimenti per la sensibilizzazione degli utenti sui temi della sicurezza informatica e, forse, spingere più persone a servirsi dei sistemi di e-banking. Si vedrà.

Dario d'Elia

<http://www.webmasterpoint.org> 19/12/05