

Banche online, truffatori a pesca

Si moltiplica il «phishing», l'abbeccamento via mail

L'attacco più feroce è partito la settimana scorsa verso Unicredit: dopo i casi di Banca Intesa, Poste Italiane e SanPaolo-Imi, torna a colpire il phishing («abbeccamento»), la frode via mail, la più temuta dalle banche online. In un modo tanto sofisticato come finora non si era mai visto in Italia. A circa un milione di persone, l'11 luglio, è stato inviato un messaggio di posta elettronica in italiano, con logo Unicredit Banca: «Egregi clienti — cominciava — Vi informiamo che in relazione al sovraccarico del nostro generale server (...) abbiamo un nuovo web server». Seguiva l'indirizzo: www.unicredits.com. Con la «s» dopo «unicredit» e «.com» invece di «.it». Un sito fasullo. Chi lo cliccava, si ritrovava su una schermata in tutto simile a quella di Unicredit, addirittura con il link per Patti chiari dell'Abi, l'associazione delle banche italiane guidata da Maurizio Sella, l'indicazione «area protetta» e, per colmo di beffa, persino l'allarme sul phishing: «Comunicazione urgente. In caso di e mail sospette non inserisca il codice».

Peccato che, inserendo su questo sito password e user id, le informazioni finissero ai truffatori. L'indirizzo www.unicredits.com fa infatti capo, attraverso una triangolazione Italia-Olanda, a un dominio coreano, dice Unicredit; o di Hong Kong, sostiene invece Massimo Penco, presidente e fondatore di Global Trust, società antifrode di Terni che ha studiato il caso. Lavora nell'Antiphishing Working Group e fa capo all'americana Entrust, quotata al Nasdaq. «Per la prima volta assistiamo a un phishing in lingua italiana, fatto da professionisti — dice Penco —. I due siti sono identici, tranne per le piccole differenze nell'indirizzo. Unicredit ha reagito avvertendo la clientela e la polizia postale ha filtrato tutte le persone che entravano nell'home banking, ma in generale le banche italiane devono fare qualcosa in più per difendersi. Il fenomeno è in crescita, crediamo che oltre 30 milioni di euro siano già stati sottratti in questo modo agli istituti di credito nel nostro Paese». «Abbiamo immediatamente avvertito sia la Guardia di finanza sia la polizia fiscale, che ha oscurato il sito mercoledì

scorso — confermano a Unicredit —. Abbiamo mandato una mail da allarme rosso a tutti i nostri 100 mila clienti. Ma è chiaro che il problema c'è». Anche perché, questa volta, l'unico modo per accorgersi del server fasullo erano i piccoli errori di grammatica nella mail: nell'indirizzo url al quale si veniva rimandati non c'erano infatti né strani numeri né simboli «%», che finora avevano permesso di riconoscere la frode.

Un'indagine di CommStrategy conferma del resto l'allerta massima. A giugno, dice la ricerca, nelle caselle di posta elettronica degli italiani sono arrivate 5 milioni e mezzo di e mail di phishing. E si stima che a dicembre le campagne di phishing saranno oltre 8 milioni. La ricerca rivela come nel primo trimestre 2005 le banche italiane abbiano rappresentato «il 3-5% dei brand colpiti». Ma «tra le prime 15 banche online, soltanto la metà fornisce nel sito informazioni sul phishing». «Il phishing ora è più sofisticato — conferma Paolo Barbesino, amministratore delegato di CommStrategy —. Ma servono grandi volumi perché la truffa abbia successo. L'invio è massiccio, si devono raggiungere i clienti della banca e, fra questi, quelli con poca familiarità informatica, che non si accorgono della frode. Ipotizziamo che su mille e-mail inviate i pirati peschino quattro sprovveduti: non è detto che la frode vada in porto, neanche con uno. Perché la banca si difende».



ALLERTA
Maurizio Sella
guida l'Abi

Messaggi fasulli
in italiano con
l'invito a digitare
i propri codici:
non fidatevi mai