

PHISHING, QUANDO LA TRUFFA CORRE SU INTERNET: 2 DENUNCE

5 Agosto 2010

L'AQUILA – Due nuovi casi di truffa informatica all'Aquila, un fenomeno che dopo un'escalation negli scorsi anni adesso vive una fase di stallo, in lotta tra sistemi d'attacco ai computer sempre più agguerriti e difese antivirus e antitruffa sempre più sofisticate.

Il termine più usato per queste truppe è "phishing", storpiatura di "pescare" in inglese, proprio perché i truffatori lanciano esche sulla rete in attesa che qualcuno abbocchi.

Lo scopo della truffa è carpire dati personali o parole d'accesso ai conti bancari o postali sul web delle vittime, per poterli poi usare a proprio piacimento.

A tenere sotto controllo il fenomeno in Italia è la polizia Postale, che proprio oggi ha diffuso la notizia dei due nuovi casi aquilani, casi che in provincia raggiungono la soglia di qualche decina ogni anno.

[L'AQUILA, DUE DENUNCE PER TRUFFA INFORMATICA](#)

La truffa si sviluppa in due possibili modi diversi. O attraverso un virus, che si infila nel computer dell'utente ignaro, che non se ne accorge nemmeno e deve solo sperare di avere un buon antivirus. Oppure, ed è il caso ormai più diffuso, tramite email trappola, che hanno però bisogno dell'azione avventata della vittima per scatenarsi.

Le email fittizie sono intestate a enti tra i più disparati, sfruttando marchi di cui una persona sia portata a fidarsi: eBay, Poste Italiane, banche, assicurazioni eccetera. Il messaggio riguarda sempre l'aggiornamento di sistemi di sicurezza, il cambiamento delle password, il rischio di cancellazione di un'utenza. Ma ormai ci sono anche le truffe più sfacciate, che chiedono di cliccare un link per avviare un servizio antitruffe!

Se il truffato clicca sul link che gli viene mostrato, quale che sia il messaggio, e nella pagina che si apre inserisce le proprie informazioni di login, dà ai programmi nocivi la possibilità di accedere ai suoi dati personali, donando in pratica ai truffatori le chiavi delle sue finanze su Internet.

La Polpost fa notare che mentre in passato le contraffazioni erano grossolane, con l'uso di traduttori automatici che faceva avere ai messaggi sgrammaticature evidenti, adesso i sistemi si sono raffinati e servono alcuni trucchetti per riconoscere i messaggi nocivi.

"In primis – spiegano dalla Polpost – è importante avere installato sul computer un buon servizio antispam: già quello da solo neutralizza la maggior parte delle minacce. Inoltre, si può avvicinare il puntatore del mouse al link del messaggio sospetto senza cliccare, e controllando in basso a quale link porta: di solito non è mai il sito esatto della banca che viene citata. Inoltre, le pagine sicure hanno sempre l'icona di un lucchetto visibile in basso sul browser".

Meno diffuse, ma pur sempre presenti, le truffe che richiedono un pagamento da far fare in concreto agli utenti. Una società tedesca, spiega la Polpost aquilana, era specializzata in questo campo, con la richiesta di invio di denaro tramite bollettini per usufruire di un servizio di scaricamento di brani musicali. (*alb.or.*)