

## E' allarme "phishing"

Situazione al

08/2017

E' allarme "phishing"

### **Internet: Attenzione a chi vi chiede informazioni sui vs. dati personali via e-mail!**

L'ultima frontiera delle truffe online si chiama "phishing" (dall'inglese pescare) e consiste nell'inviare - direttamente nella casella elettronica di ignari utenti, attraverso una massiccia opera di spam - una e-mail allo scopo di carpire informazioni sensibili, come i dati di carta di credito, username e password, dati del conto corrente ecc ...

Tra i tentativi di phishing-truffa registrati ci sono quelli che per molto tempo hanno preso di mira il sito di Poste Italiane e anche parecchi consumatori altoatesini.

Ricordiamo che il meccanismo di questa tipologia di truffe è molto semplice: l'utente riceve un' email nella quale viene invitato a riempire un modulo (incluso nella stessa e-mail o in una pagina Web di cui viene fornito il link) con i propri dati personali. Compilando tale modulo - naturalmente fasullo - gli ignari utenti finiscono per svelare le password e i propri numeri di carta di credito, che possono così essere utilizzate dal "cracker" per compiere operazioni illegali.

Ecco i consigli messi a punto dalla Polizia Postale - per non abboccare a questo tipo di truffe:

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 online 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. E' possibile segnalare il sospetto di abuso anche via e-mail. Molte banche ed aziende dispongono infatti anche di un indirizzo di posta elettronica specifico per denunciare questo tipo di illeciti. 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 links ricevuti via e-mail.

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.

A questo indirizzo della Polizia Postale, <http://www.poliziadistato.it/articolo/748/> è possibile fare le segnalazioni.