sapevi che...

tin.it

"phishing" è il nome di un insidioso crimine informatico?

I responsabili di questo particolare tipo di frode "pescano" i dati degli utenti tramite l'invio di messaggi e-mail che invitano a visitare falsi siti Web, cloni illegali di siti autorevoli e noti (Istituti di Credito, Internet Provider, siti di transazioni online, società importanti, ecc).

Con un pretesto del tipo "abbiamo esigenza di verificare i suoi dati", ecc., l'utente viene spinto su pagine web fasulle, dove viene invitato a lasciare i propri dati: generalità, password, codici di accesso a conti correnti, pin di registrazione alle pagine di transazioni online o, peggio, il numero di carta di credito.

Sia le e-mail che le pagine web fasulle sono studiate per sembrare messaggi ufficiali e pagine del sito dell'ente di fiducia.

Ecco alcuni consigli utili per difendersi dal phishing:

- E' buona regola non rispondere ad e-mail che richiedono dati personali e sensibili. E' infatti improbabile che un ente scriva chiedendo di inserire dati personali o password. Una richiesta simile, unita all'urgenza che il messaggio cerca di dare, è il primo sintomo di una trappola. In ogni caso, anche se ritenete autentico il messaggio, non è opportuno usare i link che contiene o rispondere utilizzando il tasto di "reply" o "rispondi" del programma di posta. Meglio aprire una nuova finestra Internet e visitare il sito ufficiale del presunto mittente, utilizzando link già noti.
- Ricordate che è sempre possibile (ed opportuno) contattare l'ente da cui sembra provenire il messaggio (per telefono, email, etc) per verificare l'autenticità dello stesso.
- Potete comunque sempre segnalare il tentativo di truffa alla Polizia Postale e delle Comunicazioni: per informazioni, il sito è al link **http://www.poliziadistato.it/pds/informatica/index.htm**.

Il Customer Care di Tin.it