Euroconference NEWS
L'INFORMAZIONE QUOTIDIANA DA PROFESSIONISTA A PROFESSIONISTA
Direttori: Sergio Pellegrino e Giovanni Valcarenghi

Edizione di mercoledì 16 luglio 2014

SOLUZIONI TECNOLOGICHE

Sicurezza, attenti ai messaggi di Facebook!

di **Teamsystem.com**

Siamo abituati a pensare che le arrivino sul nostro computer , con le solite mail scritte in italiano sgrammaticato e, quindi, facilmente riconoscibili. Ormai non è più così. Troppo spesso dimentichiamo che l'interesse principale di chi diffonde è produrre il e i ormai sono diventati piattaforme sempre più utilizzate per le proprie attività criminali. Lo rivela uno studio condotto da , colosso mondiale dei software di sicurezza.

Secondo la ricerca, il **21,89 % delle minacce** di **phishing** arriva ormai tramite **messaggi che imitano Facebook**. Ricordiamo: il phishing è quella pratica che cerca di adescare le persone con email fasulle che invogliano a inviare dati sensibili, spacciandosi per messaggi di banche o amici.

Facebook funziona

Il concetto è semplice: ormai tutti sanno che un messaggio scritto male, proveniente da un indirizzo sconosciuto, spesso generato automaticamente da un computer, non verrà quasi mai aperto. Ma solitamente **ci si fida di Facebook** ed è per questo che molti messaggi imitano la grafica e lo stile del celebre social network per invitare i destinatari a fare clic. "Nello scorso anno – dichiarano dai laboratori Kaspersky – abbiamo registrato oltre **600milioni di tentativi** dei nostri utenti, di accedere a pagine di **phishing**. Di questi, quasi il **22%** era stato causato da **messaggi che imitavano Facebook"**. Nel 2014 la situazione non sembra essere cambiata. In **Italia** in particolare la percentuale di minacce veicolate in questo modo va **dal 9 al 12%.**

Le strategie dei cybercriminali

Come fanno i malintenzionati per convincerci a fare clic su un falso messaggio?

1. Inviano **notifiche** che sembrano del tutto **simili** a quelle dei social network.
2. Fanno partire le email da **account di posta compromessi**, quindi ci ritroviamo nella posta finti messaggi di Facebook che arrivano da **nostri conoscenti** e siamo naturalmente portati a fidarci.
3. Fanno partire le comunicazioni da **veri account** di Facebook per i quali sono stati **rubati**

i dati di accesso. In questo caso le comunicazioni arrivano da account reali, ma ci portano su siti infetti.
4. Scrivono falsi messaggi nei forum di discussione per invogliarci a fare clic.
5. Fanno apparire i messaggi nei risultati dei motori di ricerca.
6. Usano banner con immagini attraenti o finte notifiche di Facebook.

Unico scopo: rubare i dati

Lo scopo di un messaggio di phishing è **rubare i nostri dati**. Quindi una volta fatto clic su uno di questi finti messaggi, viene richiesto di inserire le proprie credenziali di accesso, ricorrendo alle scuse più strane, dopodiché si viene reindirizzati alle vere pagine di Facebook per dissipare qualsiasi dubbio di frode.

Se gli adulti sono più smaliziati, spesso a cadere nel tranello dei finti messaggi sono soprattutto gli **utenti più giovani** che nutrono una fiducia, in molti casi eccessiva, nei confronti dei social network. Se viene compromesso l'account di nostro figlio o nostro nipote di 15 anni, riceveremo da lui delle notifiche di phishing e saremo subito tentati di fare clic.

Spesso, per costringere ad aprire i messaggi di phishing, i responsabili inviano comunicazioni intimidatorie che minacciano, per esempio, il blocco dell'account se non si esegue una determinata operazione che consiste, tanto per cambiare, nell'inserimento dei propri dati di accesso.

Il consiglio migliore è di **non rispondere a queste mail** e **collegarsi** sempre **direttamente** al sito di Facebook, ma **mai** utilizzare i collegamenti di un
messaggio di posta che ci appare anche minimamente sospetto.

Ecco un esempio di finto messaggio di Facebook che invita a leggere qualcosa che ci siamo persi. Spostando il cursore del mouse (senza fare clic) sul link del messaggio, vediamo che compare un indirizzo sconosciuto e non è certamente quello del vero Facebook.