

Phishing: unica e-mail per Banca Intesa, San Paolo IMI e Fineco

Il panorama del phishing nostrano si è arricchito oggi di un nuovo caso che tenta di colpire contemporaneamente i clienti di tre differenti istituti di credito: Banca Intesa, Fineco e San Paolo IMI.

Se le prime due banche non rappresentano una "novità" l'intenzione di colpire il San Paolo IMI rappresenta di fatto per i phisher la possibilità di centrare nuove ignare vittime utilizzando per l'occasione una nuova e-mail:

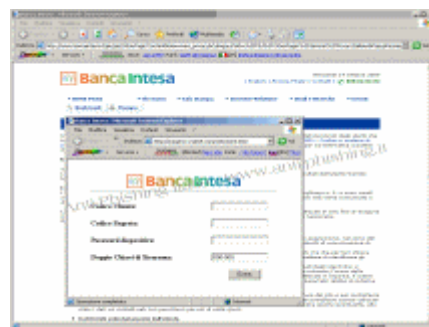


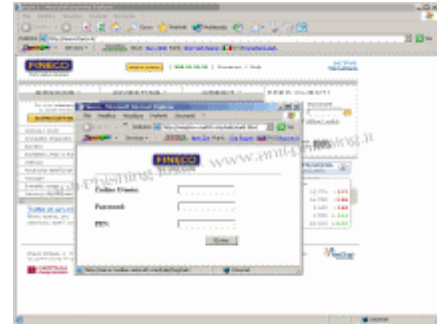
Anche se di per se è altamente improbabile che tre banche utilizzando un'unica e-mail chiedano ai loro clienti l'aggiornamento dei propri dati personali, la presenza ancora una volta di un italiano tradotto dovrebbe mettere in allarme anche gli utenti più distratti e disinformati.

Aggiornamento: In data 22 ottobre la stessa e-mail è stata riutilizzata dai phisher, sfruttando questa volta un'apposita tecnica anti-spam.



Per cercare di raccogliere i codici di accesso ai conti on-line delle malcapitate vittime i phisher utilizzano come già avvenuto lo scorso 10 ottobre la tecnica della finestra di pop-up visualizzata insieme al vero sito della banca in questione.





Infatti cliccando su uno dei tre link proposti all'interno dell'e-mail divisi a secondo della propria banca l'utente viene re-indirizzato attraverso tre versioni nazionali di Google prima di essere trasportato su un apposito redirect registrato presso il russo Da.ru il quale termina il depistaggio dell'utente inviandolo verso il vero sito dove si consuma la truffa il quale visualizza il vero sito della banca insieme all'apposito pop-up truffaldino.

Dettagli: I link proposti nell'e-mail hanno in realtà la seguente natura:

<http://www.google.pn/url?q=http://www.google.dk/url?q=http://www.google.vg/url?q=http://%25%09%2509%253%37%35pw%09%6c%6ejw%2ED%09%61%2e%09R%75/>

Per i primi passaggi attraverso Google sono stati utilizzati 45 redirect nazionali mentre l'URL codificato corrisponde a 36 siti Da.ru.