

# Un esempio di phishing

(i tutorial di Alessandro de Simone)

Copyright Alessandro de Simone 2007 ([www.alessandrodesimone.net](http://www.alessandrodesimone.net)) - È vietato trascrivere, copiare, stampare, tradurre, riprodurre o divulgare il presente documento, anche parzialmente, senza l'autorizzazione scritta dell'autore. I siti Internet, le case editrici e le pubblicazioni di settore che intendano utilizzare questo documento possono contattare l'autore ([www.alessandrodesimone.net](http://www.alessandrodesimone.net)) per gli accordi del caso.

Copyright Alessandro de Simone 2007 ([www.alessandrodesimone.net](http://www.alessandrodesimone.net)) – No transcribing, no copyng, no reproducing, no translating, no printing, no publishing this document – even if partially – without author's written authorization. Websites and publishing house who wish to employ this document must write the author ([www.alessandrodesimone.net](http://www.alessandrodesimone.net)).

## Definizioni

Con il termine di *phishing* si intende l'atto del *pescare* che, metaforicamente, si può tradurre con un poco lusinghiero “*prendere all'amo gli ingenui*”. Eh, sì, perché bisogna essere proprio ingenui (o poco informati) per cadere nella trappola. Per comprendere come siano possibili truffe informatiche è bene partire da alcune definizioni.

Consideriamo un qualsiasi indirizzo web, come il mio: [www.alessandrodesimone.net](http://www.alessandrodesimone.net)

- Il suffisso *net* – parente prossimo di *com*, *org*, *gov* (e di tutte le nazioni: *it*, *us*, *fr*...) – è il cosiddetto **Top Level Domain** (in italiano: **dominio di primo livello**), la cui gestione è affidata all'organizzazione IANA (*Internet Assigned Numbers Authority* – [www.iana.org](http://www.iana.org)), autorità internazionale che si occupa perfino di assegnare la gestione del numero delle porte di un PC (argomento che esula dal presente Tutorial). Il dominio di primo livello non può essere creato a piacere dalla comune utenza, ma solo scelto – tra quelli disponibili(\*) – per gestire un proprio sito. (\*)alcuni *Top Level* (*gov*, *tv* ed altri) sono riservati a enti governativi o organizzazioni ben definite.
- Il nome *alessandrodesimone* è il cosiddetto **dominio di secondo livello**; può essere scelto a piacere dall'utente, purché non già appartenente ad altro soggetto.
- La generica sigla iniziale *www* indica lo spazio web in cui il dominio di secondo livello è registrato (per chi no lo sapesse, c'è anche *www1*).

In definitiva, la cosiddetta *Home Page* di un qualunque sito si trova nella cartella principale che il provider ha riservato al legittimo possessore di quel sito. Quest'ultimo (il possessore, non il sito) può creare (quasi) infinite cartelle e sottocartelle, in cui inserire tutte le pagine che desidera. Esempi, sempre riferiti al mio sito, sono...

<http://www.alessandrodesimone.net/curriculum/index.htm>

[http://www.alessandrodesimone.net/Foto/reunion\\_mare\\_tramonti.html](http://www.alessandrodesimone.net/Foto/reunion_mare_tramonti.html)

...che, come si può notare, sono posizionate **a destra** dell'indirizzo completo di secondo livello, subito dopo il carattere *slash* (*/*). In linea di massima, nessuno mi può impedire di creare – e di gestire – all'interno del mio sito una pagina di questo tipo:

<http://www.alessandrodesimone.net/bancaplanetaria>

...in cui potrei decidere, per esempio, di trattare argomenti di carattere economico / finanziario nella sezione del mio sito intitolata *BancaPlanetaria*.

Le potenzialità di Internet, tuttavia, mi permettono di gestire livelli superiori al secondo (cioè terzo, quarto...) il cui nome è posizionato **a sinistra** dell'indirizzo completo, separato solo dal carattere punto (*.*) Esempio:

<http://www.bancaplanetaria.alessandrodesimone.net/>

Il trucco è tutto lì: anzitutto occorre, subdolamente, “nascondere” il nome del secondo livello (*alessandrodesimone*), lasciando però ben visibile quello di terzo livello:

<http://www.bancaplanetaria.alessandrodesimone.net/>

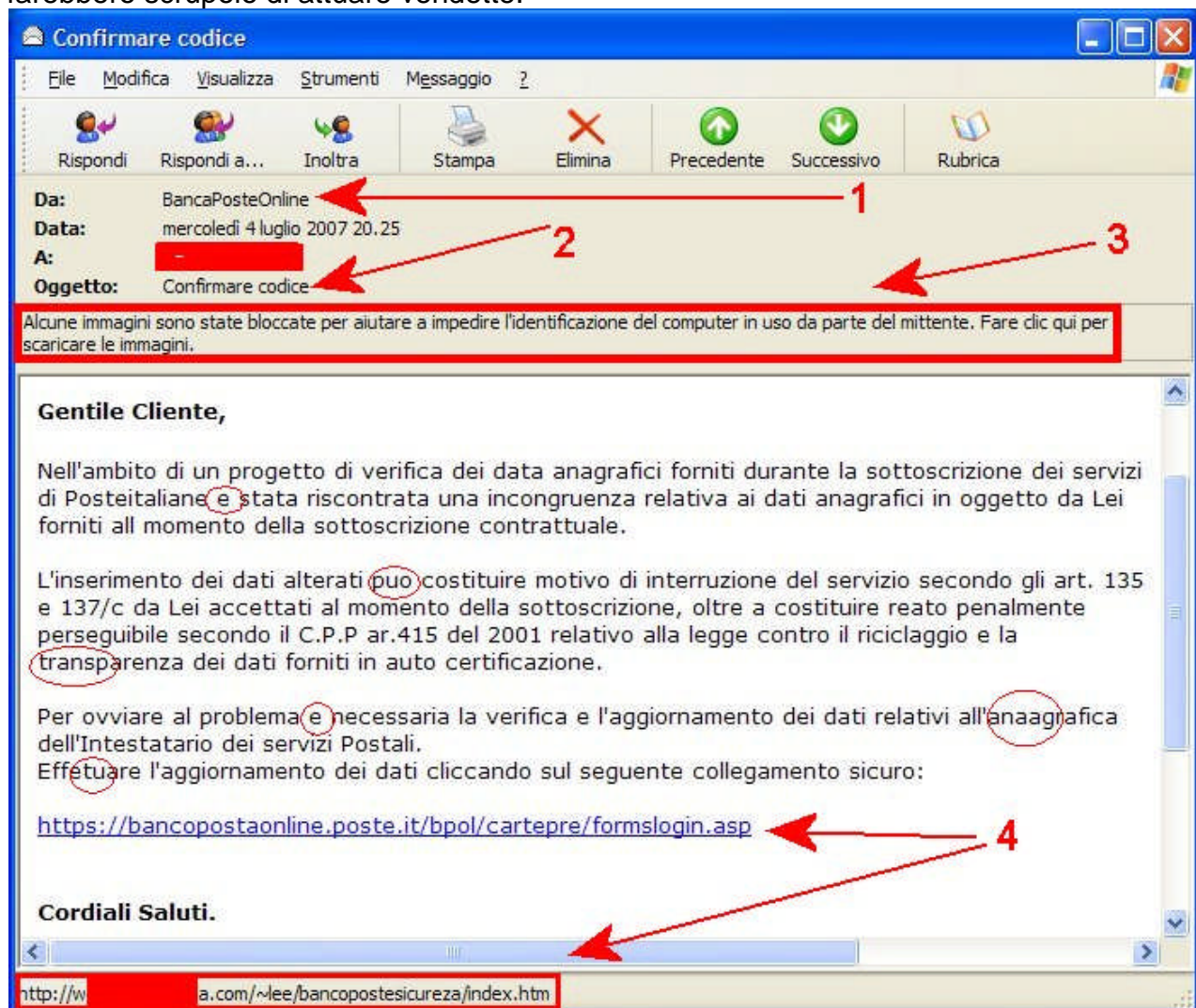
Subito dopo basterà “avvicinare”, sospingendolo verso sinistra, il nome del *Top Level Domain* a quello del terzo livello:

<http://www.bancaplanetaria.net/>

A questo punto la truffa è (quasi) fatta: chi legge il *link* penserà che, cliccandoci sopra, si aprirà il collegamento con la home page della *Banca Planetaria*, mentre – in realtà – si aprirà la pagina presente nel *terzo livello* del mio sito Internet. Se sono abbastanza abile da simulare – graficamente – la vera home page dell'ipotetica *Banca Planetaria*, la truffa si sta completando: sarà sufficiente aver inserito un *form* in cui l'utente è invitato a digitare *userID* e *password* che potranno essere comodamente inviati al mio indirizzo personale di posta elettronica; con le conseguenze che è facile immaginare.

## Un esempio pratico

Spesso ricevo mail di *phishing* che, ovviamente, mi guardo bene dall'aprire. Stavolta, tuttavia, sono stato costretto a farlo per... documentare il presente Tutorial ! Nella figura sottostante riporto la schermata della mail ricevuta, in parte opportunamente schermata sia per questioni di privacy, sia per evitare spiacevoli inconvenienti: non dimentichiamo che le truffe sono opera di associazioni per delinquere internazionali, che di certo non si farebbero scrupolo di attuare vendette.



Nella figura, indicato con **1** è l'indirizzo di provenienza che, nel caso specifico, **sembra** quello ufficiale di *BancoPostaOnline*. Non è questa la sede per spiegare in che modo manipolare l'indirizzo di un mittente (né tanto meno – se lo sapessi – mi azzarderei a spiegarlo: la diffusione di notizie di questo tipo è penalmente perseguibile), ma è bene sapere che, purtroppo, si tratta di una procedura quanto mai semplice. Per evitare spiacevoli equivoci, sappiate che le Forze dell'Ordine sono in grado di risalire al mittente autentico: vi sconsiglio di fare esperimenti dalle conseguenze forse devastanti per la vostra tranquillità familiare.

Tornando all'argomento, l'errore di battitura indicato con **2** (e tutti gli altri cerchiati in rosso nel testo della mail) dovrebbero insospettire il suo destinatario. Come già detto, si tratta di organizzazioni malavitose internazionali, che per nostra fortuna non sono in grado di tradurre in modo adeguato il testo originario. Tengo a sottolineare, però, che di recente le traduzioni dei truffatori sono sempre più precise ed è presumibile che diventeranno perfette tra breve tempo.

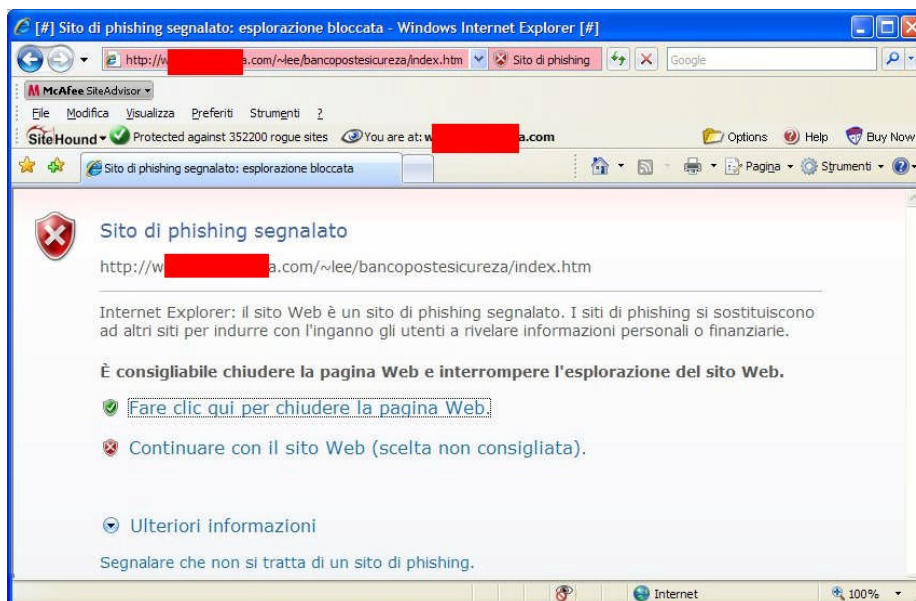
Anche l'avviso **3**, che compare se il PC è sufficientemente protetto da azioni di spionaggio relativamente banali, dovrebbe insospettire l'utente e metterlo in guardia.

Ciò che rappresenta la dimostrazione inequivocabile che si tratta di una mail truffaldina è il link evidenziato dal numero **4**. In pratica, posizionando il puntatore del mouse sull'indirizzo consigliato – **apparentemente lecito** (freccia superiore di 4) – in realtà si verrà proiettati verso il sito Internet indicato in basso nella barra di stato (freccia inferiore 4) che non può fare a meno di evidenziare l'indirizzo reale e completo (parzialmente nascosto per i motivi prima citati). Si tratta quindi, nel caso specifico, di un link che nasconde una parte consistente del reale sito internet al quale si verrebbe indirizzati cliccandoci sopra.

## Ulteriore aiuto

Per scrivere il presente Tutorial ho voluto rischiare (si fa per dire...) simulando l'azione di un utente sprovveduto e ingenuo cliccando, quindi, sul *link* contenuto nella mail. Naturalmente il mio PC è pieno zeppo di sistemi di sicurezza che hanno fatto bene il loro lavoro: è infatti subito comparsa la schermata riprodotta qui a lato che precisava, senza mezzi termini, la natura *phishing* del sito che stavo per visitare. Ho quindi preferito interrompere la procedura, limitandomi a catturare la schermata, ma solo per riprodurla in questo Tutorial.

Per ora un solo avvertimento: **diffidate di qualunque mail che chieda dati personali, userID e password.**



**Il presente Tutorial è stato modificato il giorno 5 luglio 2007  
Per ulteriori aggiornamenti consultare il sito [www.alessandrodesimone.net](http://www.alessandrodesimone.net)**