Esempio pratico/reale di un tentativo di phishing. Purtroppo, troppo spesso accade che arrivano email, in particolar modo per gli italiani, tentativi di phishing usando come esca account delle poste (PostePay). Vediamo insieme un esempio pratico: mi è arrivata oggi la seguente email:

----------< begin >----------

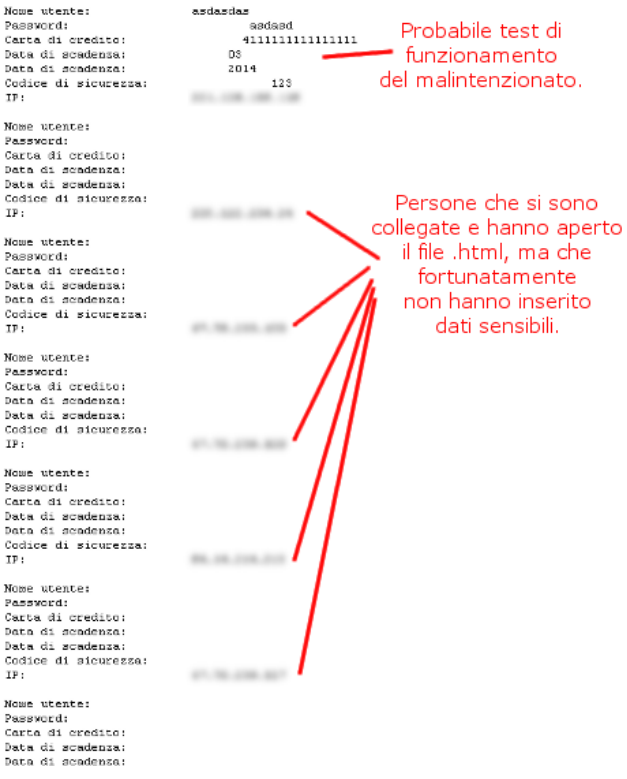
```
Gentile Titolare,

-----------------------------------------------------------------

Abbiamo rilevato attivita irregolari sul tuo conto Poste.it. Per la tua protezione, e necessario verificare
questa attivita prima di poter continuare a utilizzare il vostro conto. Si prega di scaricare il documento
allegato alla presente-mail a rivedere le attivita del proprio account. Se scegli di ignorare la nostra
richiesta, ci lasciano scelta di sospendere temporaneamente il tuo account.

-----------------------------------------------------------------
--------------------------------

Ti ricordiamo che tramite il sito Poste.it puoi mantenerti sempre aggiornato sulle opportunita' e sui vantaggi
che Postepay ti riserva.
```

----------< end >----------

In allegato si trova un file .zip che l'ignaro utente, in buona fede, aprirà ed'estrarrà il file/collegamento "*Verificare.il.tuo.account.Postepay.html*". La vittima aprirà il collegamento e, se connesso a internet, gli script al interno del .html provvederanno a caricare dal sito ufficiale "www.postepay.it" i contenuti come il tipo di form, le varie immagini originali, la pubblicità, etc. Devo dire, che avendone visti a centinaia, questo è uno dei meglio-costruiti che abbia visto finora. A parte qualche imperfezione come la navigation-bar blu, alla quale mancano alcuni collegamenti e il form di login in alto a destra. Ma per qualcuno che va di fretta o sta poco attento non se ne accorge neanche.

Come abbiamo visto, in se la pagina di phishing è piuttosto benfatta, perché scarica i contenuti in tempo reale direttamente dal sito originale. Ora cosa succede, la vittima, sempre in buona fede, inserisce i propri dati per la cosiddetta verifica dei dati. Purtroppo però, una volta premuto "Accedi", tutti i dati inseriti vengono inviati a un server apposito. Per capire meglio, vedesi il sorgente della pagina. In questo caso i dati vanno inviati a "d.php".

http://211.221.247.22/d.php



Una volta che lo script d.php ha immagazzinato i dati, provvederà immediatamente a reindirizzare la vittima al sito www.postepay.it originale e l'utente, se veramente ha inserito i dati, rimarrà ignaro di quello che è appena accaduto. Il caso che stiamo esaminando, lo script d.php salva i dati nel file "sex.txt". Qui a lato vediamo le prime righe.

Purtroppo però mentre visionavo il file, ho notato che, da un lato fortunatamente non ci casca praticamente nessuno. Ma purtroppo qualcuno era troppo in buona fede, e da quello che ho visto i dati sono decisamente realistici, quindi non si tratta di un test. Vedesi sotto:

```
Nome utente:          cristina
Password:
Carta di credito:
Data di scadenza:
Data di scadenza:
Codice di sicurezza:
IP:
```

Spero di cuore che non vi fate fregare facilmente da queste cattiverie!

Cordiali saluti a tutti
occasus

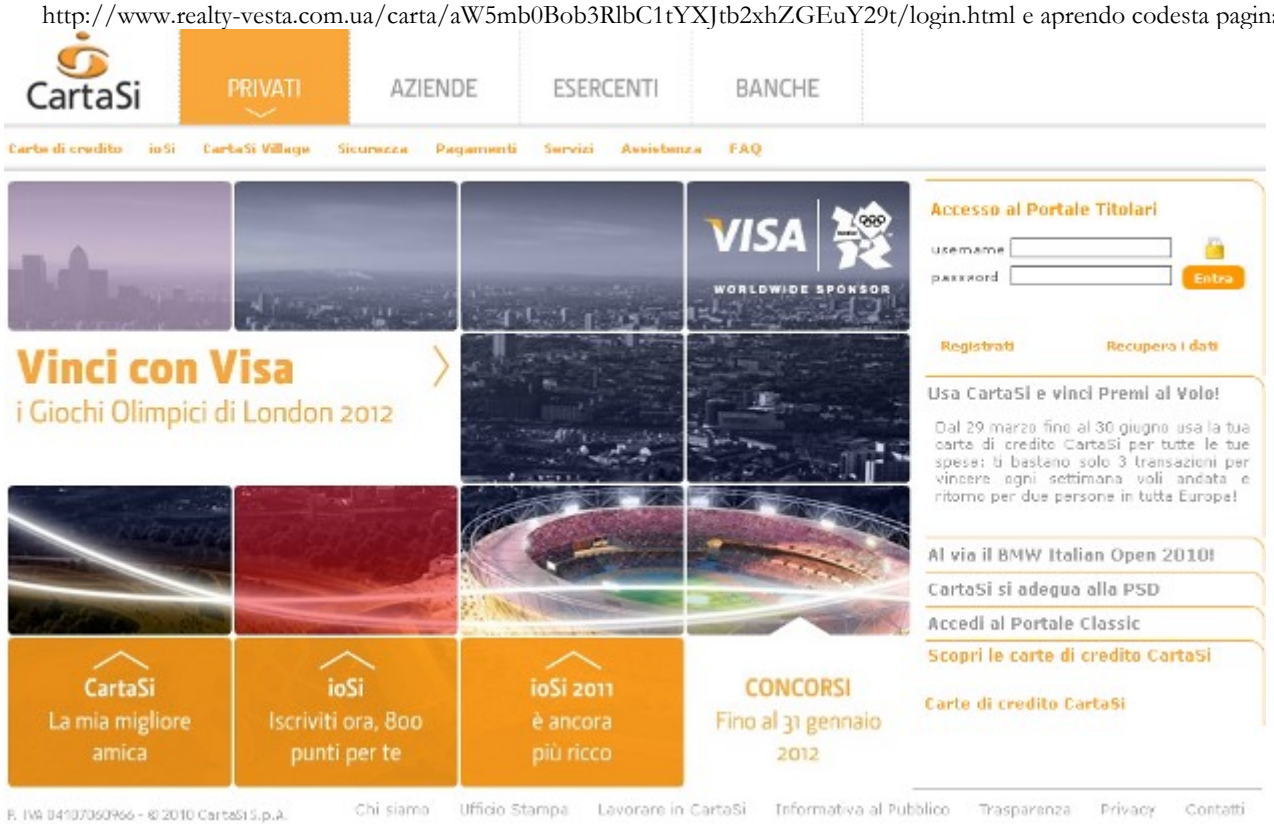
Vediamo oggi un altro esempio pratico di phishing. Questa volta i malintenzionati tentato di reperire account di PayPal (noto sistema di pagamento). Di seguito il testo del email:

```
----------< begin >----------
Gentile cliente,

Abbiamo bisogno del suo aiuto per risolvere un problema che si e verificato con il tuo conto.
Pertanto, alcune funzionalità del tuo conto rimarranno temporaneamente limitate fintanto che il problema non
verra risolto.

La procedura è molto semplice:
1 - Cliccare sul link qui sotto per aprire una finestra del browser sicuro.
2 - Confermare che tu sei il titolare del conto e segui le istruzioni.

Accedi al Portale on-line

Grazie per aver utilizzato i nostri servizi online.
Servizio Sicureza Carta Si 2012
----------< end >----------
```

Email mittente: PayPal <cjcnjr@katamail.com>
Oggetto: Misure di sicurezza E705.

Anche qui per chi ne riceve molti di tentativi di phishing si accorge subito che qualcosa non quadra. Vediamo di analizzare le parti che non sono proprio "attendibili".

01) l'email del mittente è decisamente sospetto, perché un'azienda come PayPal **non scriverà mai** da un account di katamail
02) un'azienda come PayPal **non chiederà mai** di inserire i propri dati da nessun'altra parte che non direttamente sul loro sito ufficiale
03) al interno del testo del messaggio vieni reindirizzato al seguente link:
http://www.realty-vesta.com.ua/carta/aW5mb0Bob3RlbC1tYXJtb2xhZGEuY29t/login.html e aprendo codesta pagina arriviamo qui:



Ora, se analizziamo per bene questa pagina, notiamo talmente tante informazioni che devono per forza lasciarci allibiti. Da nessuna parte c'è scritto PayPal. I "Concorsi" sono fino al 31 gennaio 2012 (premessa oggi siamo il 08 ottobre 2012). Il BMW Italian Open fa riferimento al 2010... etc. c'è ne sarebbero tantissimi da mettere in discussione. Un'altra cosa interessante è che non va da cliccare da nessuna parte. Solo il tasto "Entra" (dopo aver ovviamente inserito i dati). È inutile dire che il sito Reality-Vesta.com.ua non c'entra proprio nulla con PayPal o Carta Sì!!! Ricordatevi che nella barra degli indirizzi dovreste anche connettervi sempre anteponendo "https" come protocollo. Perché così avrete la certezza dei certificati. Ad'esempio:
https://www.paypal.com oppure https://www.cartasi.it capito? Quindi sempre occhio, prima di inserire dati, controllare sempre la barra degli indirizzi e se avete dei dubbi ricontrollate fino allo sfinimento! Guardando un po'il sorgente della pagina, si scopre che nei meandri di questo pseudo-sito c'è anche una versione piú vecchia del template di phishing... Se volete potete dare un'occhiata voi stessi.

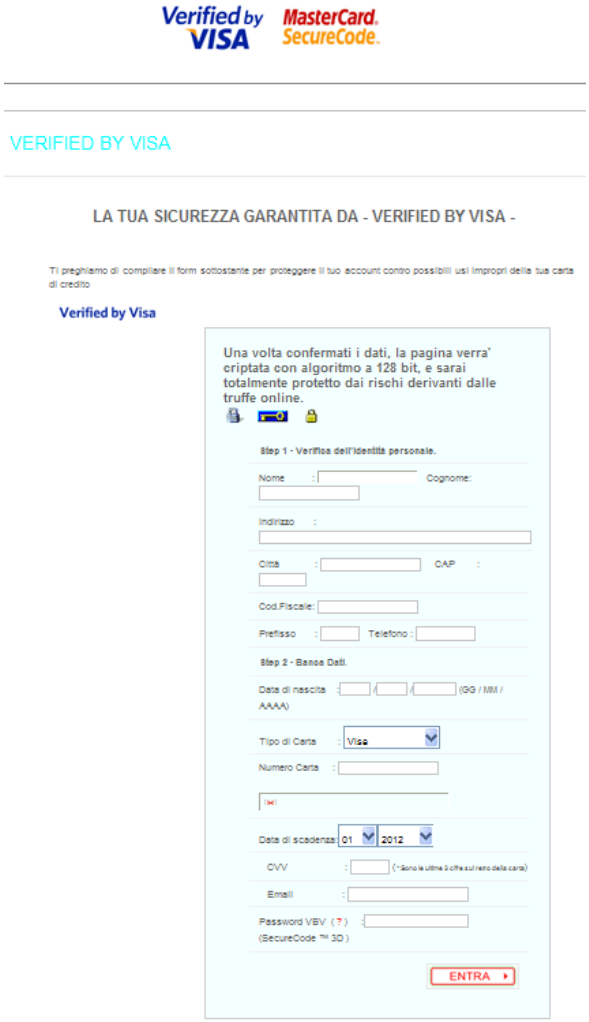
Spero di cuore che non vi fate fregare facilmente da queste cattiverie!

Cordiali saluti a tutti
occasus

Terzo stupido esempio di phishing. Spesso quando arrivano email che si spacciano per Visa o Mastercard etc. allegano oltre al solito testo di "invito-a-farmi-fregare"... aggiungono spesso un file .mht. Nel mio caso "Cliente.mht".

```
----------< begin >----------
Abbiamo rilevato attivita irregolari sul tuo conto Visa/Mastrecard.
Per la tua protezione,e necessario verificare questa attivita prima di poter continuare a utilizzare il vostro
conto Visa/Mastercard.
Si prega di scaricare il documento allegato alla presente-mail a rivedere le attivitadel proprio account.
Se scegli di ignorare la nostra richiesta, ci lasciano scelta di sospendere temporaneamente il tuo account.
Il crescente numero di attacchi di phishing sui nostri clienti ci ha fatto modificare la nostra politica sulla
privacy e anche per essere piu rigorosi sul numero di tentativi di login falliti.
Si prega di seguire attentamente le nostre indicazioni e sara in grado di ripristinare l'accesso al conto in
pochi minuti.

© Copyright visaitalia 2012 Tutti i diritti riservati
----------< end >----------
```

Il messaggio è nuovamente palesemente truffaldino. L'unico punto a vantaggio, è che l'email del mittente è piuttosto credibile, infatti è support@visa.com. Comunque, ritornando al file .mht, giá il tipo di file è un po'un pugno nell'occhio, perché si tratta di un modo di salvare una pagina web completa (sottoforma di archivio) il quale contiene piú parti. Comunque si puó fare un po'di ricerca per chi interessa. La pagina, un po'scarna si presenta come sotto a destra. Con altri browser non dovrebbe neanche aprirsi... Perché al momento in cui scrivo, mi pare che solo IE supporta questo formato.



La storia è sempre la solita... L'ignaro crede di fare qualcosa di positivo, ma... In questo caso vediamo nel sorgente che, una volta inseriti tutti i dati, premendo su ENTRA, esso non fa altro che mandare tutti i singoli dati (ovviamente in chiaro) alla seguente web application:

http://66.7.217.64/~ccarttas/tools/mail.php

Qui, tutto è sospetto! Innanzitutto non è httpS - come lo sono praticamente tutti, e dico tutti i sistemi online che hanno a che fare con denaro. Inoltre l'IP, è semplicemente uno dei box di HostDime.com. In pratica quei web-hosters gratuito come "altervista.org" oppure "aruba.it" etc. Infatti il sito (box) del malintenzionato ha come nickname "~ccarttas". Infine se continuate a guardare bene, vedrete altri link che in effetti non c'entrano nulla con Visa & Co.

http://www.infohouse.jp
http://www.verifiedbyvis.eu.pn (che peró è: http://www.freehostingeu.com)

Infine, una volta clickato su ENTRA, e dopo che avrá salvato da qualche parte i dati inseriti, da brava, la web-app vi reindirizzerà prontamente sul sito reale (quello vero) di Visa...

Alla fine i sistemi di phishing non sono cosí diversi l'uno dal altro... In sostanza si riceve un'inaspettata email che spiega di dover effettuare l'accesso altrimenti [...] Dopodiché i dati vengono carpiti e si viene reindirizzati. A quel punto il malintenzionato ha giá tutti i dati da poter rivendere oppure utilizzare.

Cordiali saluti a tutti
occasus

Benvenuti nel quarto esempio. Inizio con il ricordare, che questo thread è fatto a titolo di esempio per quelle persone che sono poco pratiche in generale con il pc e comunicazioni che possono arrivare alla propria email. Questa volta parliamo di CartaSì. Ecco il solito testo del messaggio fraudolento:

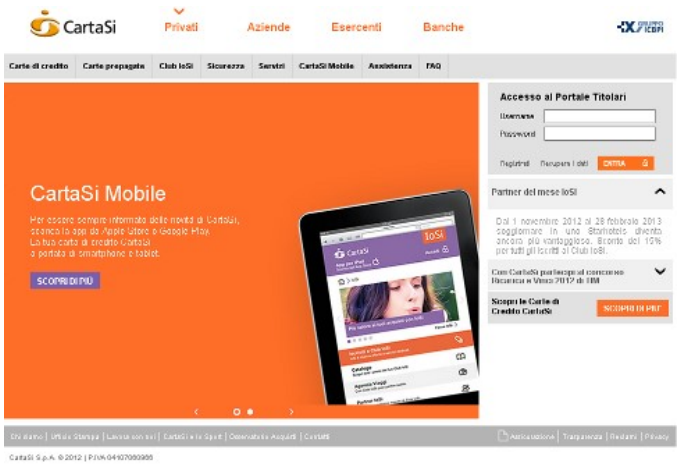
```
----------< begin >----------
Gentile Titolari,
CartaSi svolge una costante azione di monitoraggio a fronte di utilizzi fraudolenti.
A fronte di tale azione si rende pertanto necessario istituire blocchi temporanei all`utilizzo dela tua CartaSi.

Per mantenere attiva la tua carta si prega di aggiornare le tue informazioni.
Si prega di fare clic sul link del sito cartasi qui sotto per fare l'aggiornamento dei dati:

http://www.cartasi.it

Grazie per aver utilizzato i nostri servizi online.

P. IVA 04107060966 - © 2012 CartaSi S.p.A.
----------< end >----------
```

Bueno, dopo i 3 esempi precedenti, abbiamo già capito come analizzare questo tipo di messaggio. Elenchiamo i punti più salienti (importanti) del email - che si può definire quasi "divertente".
*** Mittente:** CartaSi [iosi@cartasi.it] (in realtà l'email è credibile)
*** Soggetto:** Aggiorna i dati (non abbastanza convincente)
*** Riferimento:** "Titolari" (decisamente non credibile)
*** Grammatica:** (decisamente da prima elementare)
*** P.Iva: 04107060966** (incredibile ma vera)
*** Metdodo phishing effettivo:** (testualmente il sito CartaSi.it è credibile, ma il solito problema di indirizzamento verso il male ignoto è presente, infatti il link va a:

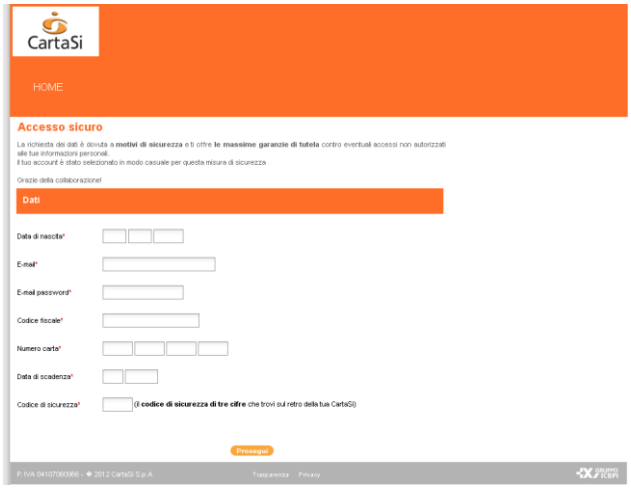
`http://69.162.73.82/faq/images/Image/it/login/to/your/account/and/save/information/fast/login/account/`
... il quale carica dei contenuti, principalmente funzioni base e immagini. Questo però mi reindirizza immediatamente al seguente:
`http://mydomainmonitoring.com/cache/cache/com_files/it/FAQ/carta/cancun/login.htm`

Ora, osservate quanto contorti sono i link... Qui succede quello che succede negli altri esempi, inseriamo user e pass, poi "Entra" i dati vengono scritti in chiaro in un database del malintenzionato. Subito arriviamo alla pagina piú pericolosa "login.php" (notare l'estensione) che provvederà poi a carpire **tutti i dati possibili...** Dopodiché veniamo subito reindirizzati sul sito reale di CartaSi!

ORIGINALE



PHISHING



I 2 a destra sono i fake.

Una cosa piuttosto interessante, è che curiosando nei meandri delle pagine di phishing, non so come, ho trova il file "k.tgz". La cosa fantastica, da un certo punto di vista, è si tratta di una web-shell (in questo caso l'autore è oRB. Goduria :) La trovate in allegato! Al quale si può accedere usando la password: " stingermissile7".
(MD5: d50800106e7bdf16f9d021a7f7035b20).

`http://69.162.73.82/faq/images/0fe023nfc.php`

Cordiali saluti a tutti
occasus