**La posta elettronica**

**Come funziona**

Le similitudini tra la posta tradizionale e quella elettronica sono notevoli:

La posta elettronica non è altro che un messaggio che viene spedito da un computer all'altro, più o meno come una lettera che viene spedita da una persona ad un’altra.

La lettera nel suo viaggio transita negli uffici postali di partenza e di arrivo. Allo stesso modo una email passa da un Mail Server ad un altro. Un Mail server non è altro che un computer in cui esiste fisicamente la cassetta postale (elettronica) del destinatario.

Per poter ricevere una lettera è necessario avere un proprio indirizzo (solitamente quello di casa o dell'ufficio). Per poter ricevere una email è necessario possedere un account su un Mail Server, che serve quindi ad identificarci, proprio come un indirizzo identifica il posto in cui viviamo.

Un sistema di email è piuttosto semplice ed è basato su pochi componenti. La cassetta postale di un utente non è altro che un puro e semplice file testo. Se avete un account del tipo nome.cognome@email.it significa che sul Mail Server di email.it esisterà un file testo di nome mariorossi.txt che conterrà tutte le mail ricevute (e non solo).

Un tempo, era possibile inviare email che contenessero solo dei messaggi testuali (un po’ come gli SMS dei telefoni cellulari, anche se di dimensioni più grandi). Negli anni, con l'introduzione del MIME (Multipurpose Internet Mail Extension), le email si sono arricchite notevolmente grazie alla possibilità di allegare file di qualsiasi genere al testo (documenti, immagini, foto, musica e persino video).

Ogni file che viene allegato subisce un processo di codifica (encoding) che lo trasforma in un semplice file di testo che può essere quindi gestito allo stesso modo del testo del messaggio. Quando la mail raggiungerà il destinatario, l'allegato verrà decodificato e tornerà al suo aspetto originale.

**L'indirizzo email**

Un indirizzo email (ad esempio fabio.colombo@email.it) è composto da due parti:

Il primo nome (fabio.colombo) è il cosiddetto account che indica la cassetta di posta dell'utente. Il secondo (email.it) è il nome del dominio ed indica il Mail Server in cui l'account fabio.colombo ha una cassetta di posta elettronica.

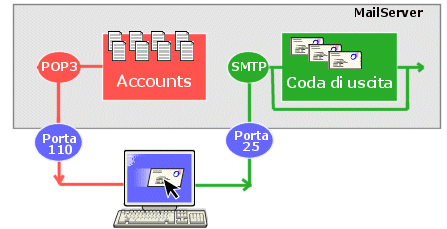
Il carattere @ (che si pronuncia AT) serve a dividere i due nomi.

Se invio una mail a fabio.colombo@email.it, sto in pratica dicendo al mio server di inviare la email alla cassetta postale fabio.colombo che si trova sul Mail Server email.it.

Se non sapessi il nome dell'account o quello del server non potrei mai inviare una email. Sarebbe come inviare una cartolina senza specificare il nome del destinatario o l'indirizzo.

**Il sistema di posta elettronica**

Come detto in precedenza un sistema di email è molto semplice e basato su file di testo (che vengono usati per gestire ogni singolo account) e su due server che si occupano di inviare e ricevere le email.



Il server SMTP (Simple Mail Transfer Protocol) è quello che provvede a far uscire la posta. Volendo usare un analogia con la posta classica è il camioncino che ritira le lettere dalle cassette e le porta all'ufficio postale per cominciare il giro di consegna.

Il server che invece è addetto alla ricezione è il POP3 (POP = Post Office Protocol) o in alternativa l’IMAP (Internet Mail Access Protocol).

Per convenzione, ognuno dei protocolli usati usa una porta specifica: il server SMTP usa la porta 25, il POP3 la 110 e l'IMAP la 143.

**Il viaggio di una email**

Supponiamo che il signor Rossi (mariorossi@email.it) voglia inviare una email al suo amico Bianchi (carlobianchi@yahoo.com). Vediamo passo passo cosa succede sul web e quale viaggio compie la email:

Passo 1

Il signor Rossi usa (ad esempio) Microsoft Outlook per compilare la email e alla fine preme il tasto di Invio Mail per cominciare il processo di invio.

Passo 2

Outlook Express si connette al server SMTP di email.it usando la porta 25 e gli comunica l'indirizzo del mittente, quello del destinatario ed il contenuto della email.

Passo 3

Il server SMTP legge i dati e prende per prima cosa l'indirizzo del destinatario dividendolo in due parti:

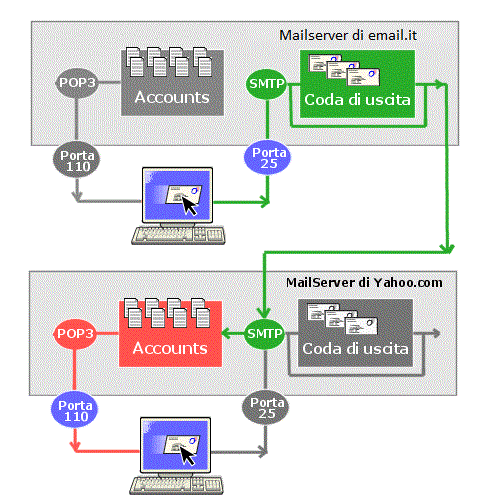
Il nome : carlobianchi

Il dominio : yahoo.com

Se il dominio è lo stesso del mittente (non è il nostro caso), ciò avrebbe significato che entrambi gli utenti hanno un account sulla stessa macchina per cui l'SMTP si sarebbe limitato ad inoltrare il messaggio al POP3 che lo avrebbe recapitato nella di Bianchi.

Nel nostro caso i domini sono differenti per cui l'SMTP server deve rintracciare l'altra macchina a cui inviare i dati. Per fare questo si connette ad un DNS server (Domain Name Server) e gli "chiede" l’indirizzo IP del server yahoo.com a cui si dovrà connettere per inviare la email.

Passo 4

Una volta ottenuto l’indirizzo IP di yahoo.com, l'SMTP di email.it si connette ad esso ed inizia con lui lo stesso tipo di conversazione che era avvenuta nel punto 2 tra il Outlook Express e l'SMTP di email.it. L'unica differenza è che il server di Yahoo riconosce la cassetta postale carlobianchi sul suo dominio ed inoltra quindi il messaggio al POP server che lo inserisce nella mailbox del signor Bianchi.

Se per qualche motivo il server SMTP di email.it non fosse riuscito a connettersi al server SMTP di yahoo.com, la mail sarebbe rimasta in una coda e periodicamente l'invio sarebbe stato ritentato (solitamente ogni 4 ore e per un periodo massimo di circa 5 giorni dopo il quale la mail non consegnata ritorna al destinatario).

La conversazione tra due SMTP o tra il client Mail e l'SMTP è molto semplice e vale la pena mostrarne un esempio per capire meglio come funziona il protocollo SMTP (in verde potete identificare le richieste mentre in rosso le risposte del server SMTP):

helo Test

250 yahoo.com Hello email.it [212.97.34.7]], pleased to meet you

mail from: mariorossi@email.it

250 2.1.0 mariorossi@email.it... Sender ok

rcpt to: carlobianchi@yahoo.com

250 2.1.5 carlobianchi@yahoo.com... Recipient ok

data

354 Enter mail, end with "." on a line by itself

from: mariorossi@email.it

to:carlobianchi@yahoo.com

subject: Test di invio mail

Ciao Carlo, sto testando la mia mail

.

250 2.0.0 Message accepted for delivery

quit

221 2.0.0 Closing connection

Potete provare anche voi ad inviare una email instaurando un dialogo identico a quello appena visto. Non dovete far altro che connettervi (con il Telnet di Windows) ad un mail server sulla porta 25 e rispondere alle domande.

Nella lista seguente vengono elencati tutti i comandi che il server mail può capire:

HELO - Introduzione

EHLO - Introduzione e richiesta del modo esteso

MAIL FROM: - Specifica del mittente

RCPT TO: - Specifica del destinatario

DATA - Specifica del corpo del messaggio (To, From e Subject)

RSET - Reset

QUIT - Fine della sessione

HELP - Help sui comandi

VRFY - Verifica di un indirizzo

EXPN - Indirizzo esteso

VERB - Nascosto

**Pop3 e Imap**

Il server POP è ancora più semplice e svolge un’unica attività. Una volta riconosciuto l'utente loggato provvede ad accedere alla sua cassetta postale (in realtà un semplice file di tipo testo) e a renderla disponibile all'utente. Anche il POP3 ha una serie di comandi che potete testare con il telnet (stavolta connettendovi alla porta 110).

USER - Inserire la propria user ID

PASS - Inserire la porpria password

QUIT - Uscire dal POP3 server

LIST - Lista dei messaggi con relativa dimensione

RETR - Scaricare un messaggio fornendo il suo id

DELE - Cancellare un messaggio fornendo il suo id

TOP - Visualizzare le prime x righe di un messaggio fornendo il suo id e le linee da visualizzare

Il protocollo POP3 come abbiamo visto è molto semplice ed ha pochissimi comandi a disposizione. Negli anni, per far fronte ad alcune sue limitazioni è nato un nuovo protocollo chiamato IMAP. Con il protocollo IMAP è possibile ad esempio scaricare la posta dal server sul proprio Pc locale senza che essa venga cancellata fisicamente. Grazie a questa funzionalità è possibile quindi leggere e scaricare le proprie email sul proprio PC e/o sul proprio portatile.

**Approfondimento SMTP**

Il compito principale del protocollo SMTP è quello di trasferire (attraverso il protocollo TCP) un messaggio di posta elettronica dal mail server del mittente al mail server del destinatario. Per capire al meglio il funzionamento forniamo un esempio di invio di un messaggio di posta tra un utente A e un utente B:

L'utente A decide di mandare un messaggio di posta elettronica all'utente B. Aprirà dunque il suo user agent (ad es. Outlook), scriverà il messaggio, inserirà come destinatario l'indirizzo e-mail dell'utente B ed invierà il messaggio.

Lo user agent dell'utente A, a questo punto, invierà il messaggio al mail server dove è registrata la mail box dell'utente A dove questo verrà messo in una coda di messaggi in attesa di spedizione.

A questo punto quando è giunto il momento dell'invio del nostro messaggio il mail server apre una connessione TCP sulla porta 25 verso il mail server di destinazione e viene eseguita una handshake a livello applicativo tra client e server SMPT.

Se la connessione TCP viene instaurata in maniera corretta e senza problemi, il mail server dell'utente A invia il messaggio al mail server dell'utente B.

A questo punto il messaggio è arrivato al mail server di destinazione il quale metterà il messaggio nella giusta mail box.

L'utente B, quando vorrà, aprirà il suo User Agent e leggerà il messaggio di posta inviatogli dall'utente A.

Il protocollo SMTP è un protocollo molto vecchio anche rispetto al più comune HTTP.

Data la sua anzianità l'SMTP hai dei limiti implementativi che, al giorno d'oggi, sono abbastanza penalizzanti. L'SMTP, ad esempio, tratta il messaggio di posta elettronica con una codifica ASCII a 7 bit header e allegati inclusi. Ciò fa sì che se un utente voglia inviare per e-mail un file video quest'ultimo deve essere prima convertito in ASCII 7 bit e poi inviato. Quando il messaggio viene ricevuto dal destinatario lo user agent farà l'operazione inversa, ovvero decodifica il messaggio arrivatogli ricomponendo così il flusso video. E' evidente che viene posto un limite alla grandezza degli allegati inviabili in quanto l'operazione di codifica e decodifica è un processo abbastanza oneroso.

Altro problema che affligge il protocollo SMTP è legato alla sicurezza per l'invio dei messaggi. Questo perché l'SMTP non gestisce in alcun modo l'autenticazione dei mittenti permettendo così di inviare messaggi di posta elettronica modificando il campo dell'indirizzo e-mail del mittente (in questo modo quando la mail viene recapitata al destinatario, quest'ultimo vedrà come mittente l'indirizzo e-mail del fittizio mittente).

Data la presenza di questa falla di sicurezza, negli ultimi tempi, i mail server di quasi tutti i principali provider di posta elettronica hanno implementato un'estensione dell'SMTP chiamata SMTP-AUTH. Questa estensione richiede che l'email del mittente del messaggio corrisponda a quella autenticata (mediante username e password) per la mail box con la quale si effettua l'invio.

A questo punto ci si potrebbe chiedere: ma perché un protocollo così datato e con tali evidenti limitazioni non viene sostituito con un protocollo più giovane e più sicuro? Semplicemente perché il protocollo SMTP è presente in tantissime implementazioni e la sua sostituzione avrebbe costi immensi.

**Approfondimento POP3 (Post Office Protocol v.3)**

Caratteristica principale di questo protocollo è la semplicità di implementazione che si rispecchia, tuttavia, in scarse funzionalità.

Vediamo un esempio di funzionamento di questo protocollo:

L'utente decide di controllare la propria casella di posta. Per farlo attiva il suo User Agent (ad es. Outlook), il quale provvederà di instaurare una connessione TCP (sulla porta 110) col mail server.

Instaurata la connessione TCP entra in gioco il protocollo POP3. Quest'ultimo, come prima operazione, compie l'autenticazione al mail server inviando nome utente e password con i quali abbiamo registrato il nostro indirizzo e-mail. Le limitate funzionalità del protocollo si possono da subito evidenziare in quanto username e password vengono inviate in chiaro al mail server e quindi, in caso un malintenzionato sia in ascolto nella nostra rete, riuscirà ad ottenere i nostri dati di accesso alla mail box senza grossi problemi.

Conclusa la fase dell'autenticazione, il protocollo si preoccuperà di recuperare tutti i messaggi presenti nel mail server. Questa fase può essere svolta in due distinte modalità: scarica e cancella oppure scarica e mantieni. La prima modalità è poco usata in quanto una volta instaurata la connessione e scaricati tutti i messaggi sul computer locale quest'ultimi vengono tutti cancellati dal mail server. Ciò vuol dire che se un utente intende leggere la propria posta da un altro computer non potrà farlo in quanto tutti i messaggi sono stati eliminati dal server. Per ovviare a questo problema è stata introdotta la seconda modalità che rende possibile l'operazione di lettura di una mail box da computer diversi.

L'ultima operazione che compie il protocollo è l'aggiornamento della mail box (cancellando dal mail server i messaggi scaricati o quelli marcati dall'utente) al momento della chiusura dello user agent.

**Approfondimento IMAP (Internet Message Access Protocol)**

Questo protocollo è stato creato successivamente al POP3 al fine di risolverne alcune limitazioni tra cui, soprattutto, l'impossibilità per l'utente di operare direttamente sul mail server nella gestione ed organizzazione dei messaggi ricevuti.

Con il POP3, infatti, l'utente può creare cartelle e spostare messaggi da una cartella all'altra, ma solo a livello locale (cioè sul PC in uso) con l'evidente conseguenza di non poter usufruire di tale lavoro qualora ci si connetta mediante diverso PC.

Con il protocollo IMAP, viceversa, questa attività di organizzazione svolge i suoi effetti direttamente sul mail server con notevoli benefici in termini di portabilità (si pensi al vantaggio di aver sempre accesso alle proprie cartelle a prescindere che si utilizzi il PC di casa, quello dell'ufficio o uno smartphone!).

Purtroppo questi vantaggi portano, quale conseguenza, una maggior difficoltà implementativa di questo protocollo rispetto al vecchio POP3 e ciò spiega, almeno in parte, la sopravvivenza di quest'ultimo all'interno di numerosi mail server.

**Struttura di un messaggio di posta elettronica**

La struttura di una lettera spedita tramite il servizio postale ordinario consta di due elementi ben distinti: il contenuto all'interno della busta e le intestazioni che indicano a chi deve essere inviata la lettera e il suo recapito.

Un messaggio di posta elettronica possiede la stessa identica struttura: il body o corpo del messaggio che conterrà il messaggio informativo che vogliamo mandare e gli headers o intestazioni necessarie per la corretta ricezione del messaggio.

Gli headers

In ogni messaggio di posta elettronica sono presenti, obbligatoriamente, l'header FROM che contiene l'indirizzo e-mail del mittente del messaggio e l'header TO che contiene l'indirizzo e-mail del destinatario. Sono presenti anche degli header opzionali che elencati brevemente, sono:

Subject: Campo nel quale può essere inserito un titolo o una frase che riassuma brevemente il contenuto del messaggio inviato.

Cc (Carbon Copy): In questo campo potranno essere inseriti indirizzi e-mail in copia di conoscenza. In questa modalità i destinatari presenti nel campo TO del messaggio sono a conoscenza che il messaggio è stato inoltrato anche all'indirizzi e-mail presenti nel campo Cc. Per meglio capire come viene utilizzato questo campo facciamo un esempio pratico: ipotizziamo che un responsabile di un progetto affidi un lavoro a due dipendenti tramite un messaggio di posta elettronica. Nel corpo del messaggio verrà spiegato cosa dovranno fare, nel campo TO verranno inseriti gli indirizzi e-mail dei due dipendenti e nel campo Cc verrà, ad esempio, inserito l'indirizzo e-mail del direttore dell'azienda. Il campo Cc ha dunque scopo informativo non richiede nessun tipo di azione diretta e nell'esempio proposto informerà, al direttore dell'azienda, che un certo lavoro è stato assegnato ai due impiegati.

Bcc (Blind Carbon Copy): In questo campo possono essere inseriti uno o più indirizzi e-mail che riceveranno una copia di conoscenza del messaggio ma, a differenza di quanto accade nel campo Cc, il loro indirizzo email non sarà visibile agli altri destinatari dell'email.

Reply-to: In questo campo può essere inserito un indirizzo e-mail al quale recapitare eventuali messaggi di risposta. Questo campo è molto usato quando vengono inviate newsletter a degli utenti dove, a seconda del contenuto della newsletter ogni volta sarà possibile inserire diversi indirizzi e-mail di Reply-to.

Quelli elencati sino ad ora sono alcuni degli header utilizzabili direttamente dall'utente e che, pertanto, possono essere manipolati a piacimento mediante un comune applicativo come un client di posta o una web mail.

Altri header, invece, sono invisibili all'utente (e quindi non possono essere modificati manualmente attraverso le normali funzionalità di una mail) ma sono generati direttamente ed automaticamente dal mail server o dallo user agent. Tra questi segnaliamo:

Message-Id: Questo header viene generato ogni volta che viene creato un nuovo messaggio. Questo campo contiene un codice che ha come funzione l'identificazione del messaggio stesso.

Received: Questi header vengono aggiunti al messaggio tutte le volte che un mail server riceve il messaggio di posta elettronica. In questo campo viene inserita la data e l'ora dell'arrivo del messaggio e l'indirizzo IP del mittente. Questi campi risultano di vitale importanza nel caso in cui si voglia tracciare il percorso del messaggio di posta elettronica e capire da quale host è stato realmente inviato.

Header di controllo virus e spam: Questi header vengono generati tutte le volte in cui il messaggio viene analizzato da un antivirus o un servizio di antispam. All'interno di questi header possiamo leggere il tipo di controllo effettuato e l'esito del controllo.

**Il formato MIME**

Abbiamo detto che con la posta elettronica possiamo inviare, oltre che un normale testo ASCII, anche allegati di vario genere (immagini, video, MP3, ecc.). Per fare ciò si rende necessario specificare, sfruttando le intestazioni MIME (Multipurpose Internet Mail Extensions), il tipo di file che si allega.

Le due intestazioni principali, appartenenti alla famiglia MIME, che rendono possibile l'invio e la corretta interpretazione di messaggi di posta elettronica composti non solo da testo sono i seguenti:

Content-Type

Content-Transfer-Encoding

Content-Type

Questa intestazione è di vitale importanza per il corretto utilizzo, da parte del destinatario, del file allegato.

Il valore presente in questo campo avrà la struttura tipo/sottotipo: la parte denominata "tipo" indica il tipo di file presente (un'immagine, un video, un file audio, ecc.) mentre la parte denominata "sottotipo" indica l'estensione del file.

Per fare un esempio concreto, nel caso di invio di un video questo campo potrà essere

video/mpeg

mentre se inviassimo un file audio di tipo MP3 avremo

audio/mp3

Il contenuto del campo Content-Type permette allo user agent del destinatario di richiamare una funzione specifica per ogni tipo di dato che riceve. E' evidente che senza questa indicazione il destinatario riceverebbe un messaggio codificato in ASCII e non saprebbe che farci dato che, non conoscendo l'estensione di eventuali file allegati, non saprebbe quale funzione specifica richiamare per la fruizione del file.

**Content-Transfer-Encoding**

Questo secondo header è altrettanto essenziale per la corretta decodifica del messaggio di posta, in quanto contiene informazioni che indicano che il messaggio è stato codificato in ASCII e anche il tipo di codifica che è stato utilizzato.

I valori ammessi sono i seguenti:

7 bit: E' il valore di default in caso non venga specificato nessun valore. Indica che ogni singolo carattere ASCII è codificato da blocchi di grandezza 7 bit.

Binary: Indica che l'intero messaggio è in formato binario. Questa codifica è utilizzata per il trasferimento di immagini video e altri contenuti multimediali.

Quoted-Printable: Indica che il messaggio è stato precedentemente già codificato in formato ASCII. Dunque un messaggio di posta elettronica che presenta questo tipo di intestazione sostanzialmente non subirà nessun'altra codifica qualora il destinatario (trasformandosi in mittente) decida di inoltrarlo ad altri.

Base 64: E' un tipo di codifica nella quale tutto il messaggio viene codificato utilizzando uno specifico sotto-insieme di caratteri ASCII. Il fatto di lavorare su un sotto-gruppo di caratteri, permette di codificare il messaggio utilizzando solo 6 bit, uno in meno rispetto alla codifica di default, rendendo così il messaggio inviato, in termini di bit, più piccolo.

x-nome\_codifica: Questo valore indica che il messaggio è stato codificato utilizzando uno schema di codifica non standardizzato. Ciò può avere il vantaggio di poter codificare il messaggio in maniera migliore (nel caso si usi schemi di codifica avanzati), ma ha il grosso svantaggio che il destinatario del messaggio deve avere, sul proprio computer locale, lo schema di decodifica associato senza il quale il messaggio non potrà essere decodificato. Ciò rende questa modalità di codifica poco utilizzata.

**Sicurezza della posta elettronica**

**Spam**

Viene considerato spam ogni messaggio di posta elettronica atto a promuovere, pubblicizzare o informare l'utente di qualche prodotto o servizio senza che l'utente stesso abbia dato esplicito consenso alla ricezione di tali informazioni.

Negli ultimi anni gli enti preposti alla salvaguardia della Rete e della privacy degli utenti hanno deciso di porre un argine al fenomeno dello spam, sanzionando gli spammer con multe che, in Italia, possono arrivare fino a 250 Euro per ogni e-mail inviata anche se, purtroppo, essendo la grande maggioranza dello spam che riceviamo frutto dell'operato di spammer stranieri, sarà davvero difficilissimo far valere le proprie ragioni.

Quando si parla di spam, tuttavia, è molto importante non far confusione. Non tutti i messaggi che riceviamo contenenti pubblicità o informazioni commerciali possono essere definiti di spam!

Spesso si tratta di messaggi che ci vengono inviati a seguito di nostro consenso: è buona norma, quindi, tutte le volte che ci registriamo ad un servizio on-line, leggere la normativa della privacy associata, nella quale troveremo informazioni riguardo al trattamento dei nostri dati personali.

**Virus, malware e trojan**

Spesso un'e-mail viene inviata per il solo scopo di creare danni all'utente con l'invio di virus, malware e trojan. Il veicolo che viene utilizzato per mandare queste tipo di applicazioni dannose sono gli allegati, solitamente degli applicativi di estensione .exe (è buona norma non aprire gli allegati provenienti da indirizzi e-mail sconosciuti). C'è da dire che negli ultimi tempi gli algoritmi degli antivirus per rilevazione di codice nocivo in e-mail ed allegati si sono affinati sempre di più garantendo quindi un livello di sicurezza abbastanza elevato.

Phising

Questa tecnica ha come obiettivo finale l'acquisizione di dati sensibili personali come, ad esempio, i dati di accesso al conto corrente bancario o a servizi internet come E-Bay.

Facciamo un esempio per chiarire meglio il funzionamento di questa tecnica fraudolenta: aprendo la nostra casella di posta troviamo un messaggio - apparentemente proveniente da Poste Italiane dove, guarda caso, abbiamo un conto corrente - in cui ci viene chiesto di effettuare il login al nostro conto postale al fine di risolvere un qualche fantomatico problema. Poco sotto, per "nostra comodità", viene riportato un link per effettuare il login al servizio senza dover fare la fatica di digitare la URL del sito delle poste nel nostro browser. In buona fede ci clicchiamo sopra venendo, così, re direzionati verso un sito somigliante, in tutto e per tutto, a quello di Poste Italiane. Convinti di trovarci, effettivamente, sul sito delle Poste, inseriamo le nostre credenziali di accesso... per la gioia del phisher che, da questo momento, avrà pieno e libero accesso al nostro conto corrente.

Ma come si può identificare un tentativo di phising?

Partite dal presupposto che un ente come le Poste o la vostra Banca, in caso di problemi, non mandare MAI una e-mail con scritto di comunicargli nuovamente il vostro username e password perché hanno avuto problemi con database o server!!!

Solitamente il testo scritto contiene errori grammaticali o frasi sintatticamente non corrette. Questo perché la maggior parte dei responsabili di questi attacchi di phising solitamente sono stranieri e non conoscono l'italiano in maniera perfetta oppure utilizzano qualche strumento di traduzione automatica. Un ente come le Poste o la vostra banca non si sognerebbe mai di mandarvi una e-mail in italiano stentato, ne va della loro immagine!!!

Il sito linkato nell'e-mail, come detto precedentemente, presenterà una grafica del tutto identica all'ente simulato, con l'unica (non irrilevante) differenza che l'URL non sarà certamente quella del sito originale. Per intendersi non troverete nell'URL un indirizzo del tipo www.poste.it ma cose tipo poste-it.sito.com o conto-poste-it.xxx.

Normalmente, i siti degli istituti bancari offrono un collegamento protetto mediante il protocollo https:// (sul browser appare qualcosa di simile ad un lucchetto), mentre questi siti pretendono un login su comuni pagine web.

Insomma, con un po' di attenzione - almeno nei casi più frequenti - non è certo difficilissimo riconoscere questo tipo di frodi: è sufficiente un po' di buon senso, attenzione ed un pizzico di malizia nell'utilizzo di dati sensibili ed economicamente rilevanti.

Fonti:

mrwebmaster.it

comefunziona.net