

Impianti Informatici

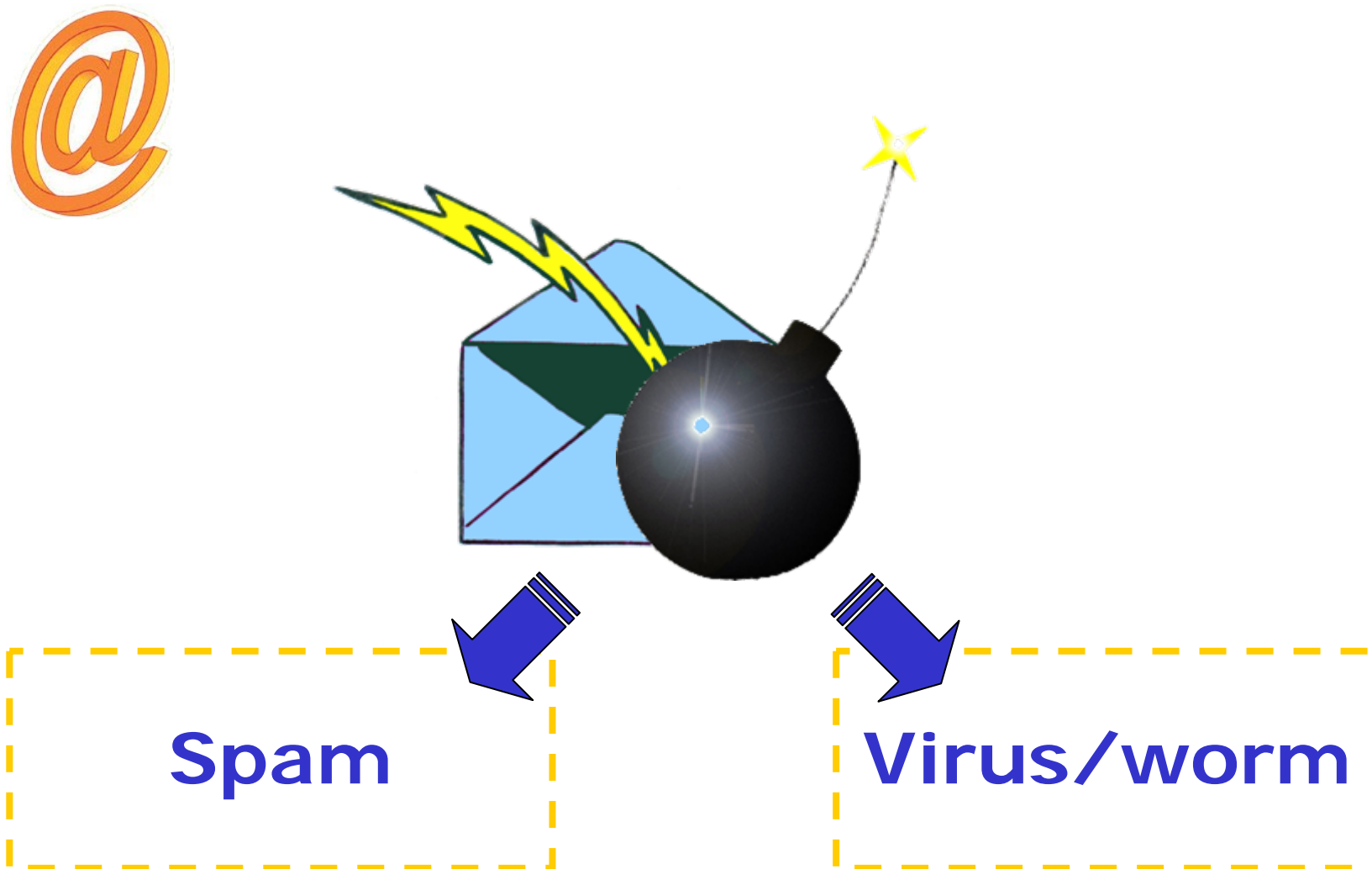
 POLITECNICO DI MILANO



Spam



Minacce alla posta elettronica





Spam: definizione

**Comunicazione
elettronica**

massiva

non richiesta

“Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it.”

“Internet spam is one or more unsolicited messages, sent or posted as part of a larger collection of messages, all having substantially identical content”



“Monty Python's Flying Circus”



Tipologie di spam

UCE (**U**nsolicited **C**ommercial **E**mail): messaggi di carattere commerciale con invio massivo.

UBE (**U**nsolicited **B**ulk **E**mail): messaggi non commerciali con invio massivo

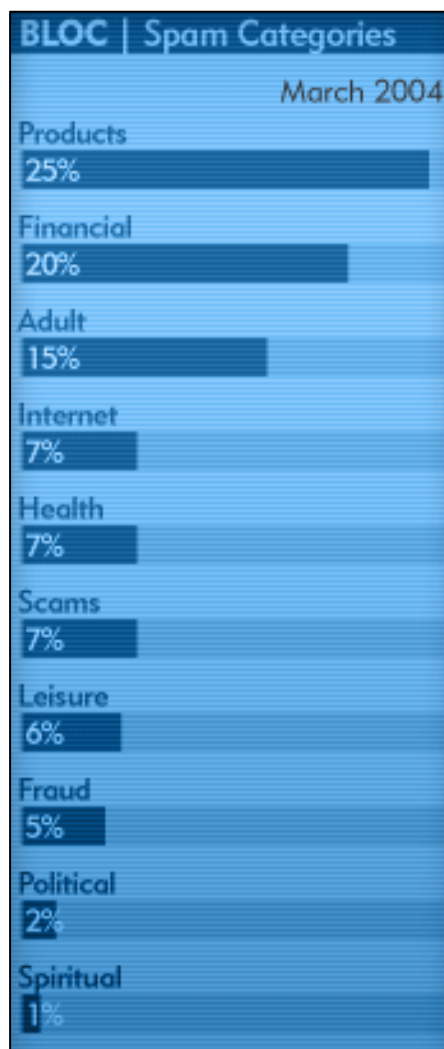
- Catene di S.Antonio
- Truffe
- Richieste di aiuto

unsolicited

Libertà di parola

?

Internet pubblico



Spam più diffusi:

- Prodotti farmaceutici/finanziari
- Prodotti VM18
- Perdita di peso
- Software pirata
 - Anti-spam
- Truffe
 - MMF (make money fast)
 - Vincite ai Casinò
- Dialer (Numerazioni a “*valore aggiunto*”)





Fenomeni correlati

Phishing:

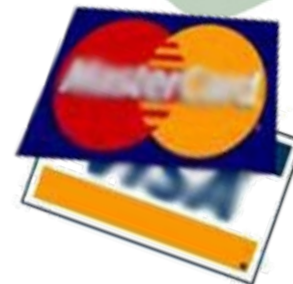
- Richiesta di
 - Indirizzo e-mail
 - Numero di carta di credito
- Da un sito che sembra legittimo
 - Ex: richieste fasulle da parte di Ebay, Paypal ecc.
 - Ai fini di truffa o raggio

Ingegneria sociale



Scam:

- Indica truffe via e-mail.
- *Nigerian Scam*:
 - Con la promessa di trasferire denaro, viene organizzato un raggio.

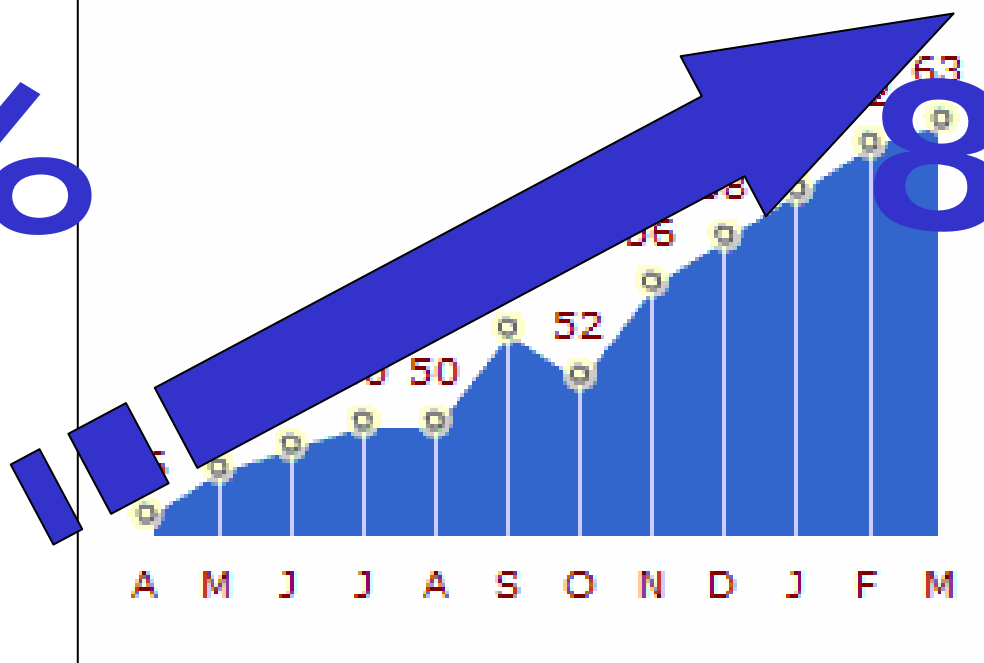




Spam and Fraud Statistics

**Percentages of Total Internet Email
Identified as Spam**

63% spam in March 2004



Fonte: <http://www.brightmail.com>



Gli spammer

Il 90% dello spam proviene da un gruppo di persone molto ristretto (circa 200) e noto.

156 milioni di
indirizzi per 200 \$

2005:
7,3 bilioni di \$

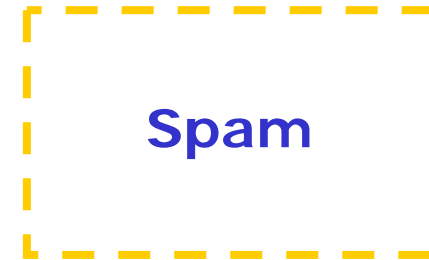
Raccolgono le “ordinazioni” da organizzazioni che vogliono pubblicizzare un prodotto o servizio

Sfruttano risorse Internet

- proprie
- altrui (pc “zombie” di utenti ignari)



≠



Pubblicità pagata dal destinatario anche se non acquista il prodotto.

Costi di invio praticamente nulli

percentuale di acquisto

0,0000001%



I costi dello spam

Provider:

- Banda
- Risorse
 - Hardware
 - Software
 - Personale
- Immagine

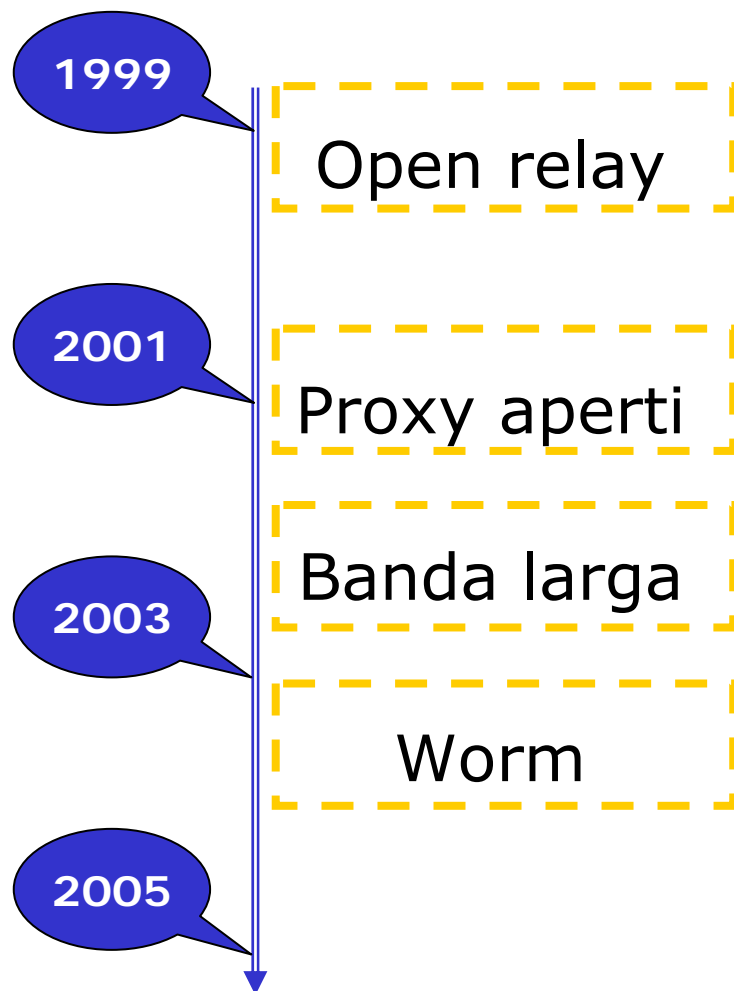
Utenti:

- Perdita di tempo
- Risorse di elaborazione
- Memoria
- Connettività

costo per gli utenti finali

10 miliardi €/anno

2001





E-mail harvesting

Estrapolazione di tutto ciò che contiene @

- Siti Web, Forum, Blog, gruppi di discussione,...



Rubrica di un conoscente infettato da un virus

- Fonte di indirizzi *puliti*

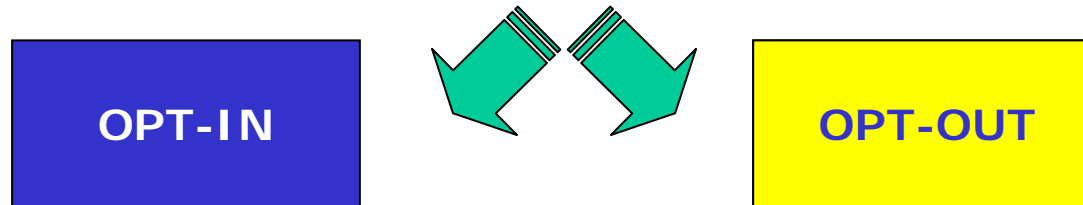
Indovinato da un attacco a vocabolario

- angelo@dominio.it
- antonio@dominio.it
- ...

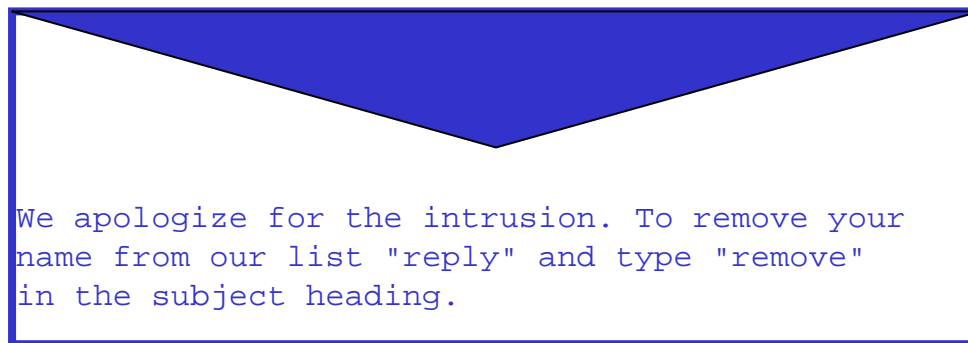




Politiche opt-in e opt-out



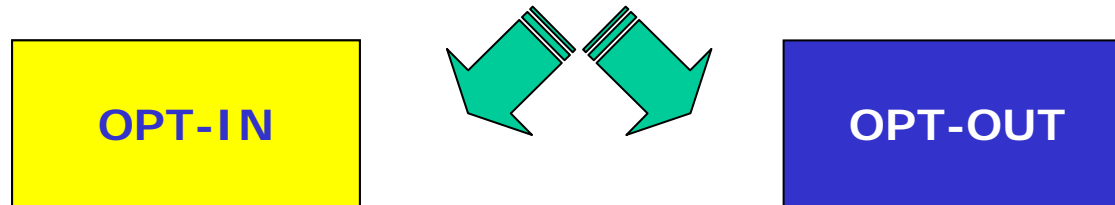
Occorre una richiesta da parte dell'utente per essere rimosso dagli elenchi



- Unica certezza: lo spammer saprà che l'indirizzo esiste
- Il ricevente deve attivarsi



Politiche opt-in e opt-out



Per iniziare a ricevere messaggi sull'argomento occorre farne esplicita richiesta

- Conferma di iscrizione
- L'utente può rimuoversi dall'elenco

Aspetti legali: USA

Junk Fax Law

- Tutela all'abuso di fax



CAUCE (Coalition Against Unsolicited Commercial E-Mail): coalizione costituita con l'obiettivo di estendere il modello della Junk Fax Law alle e-mail

Legge federale CAN-SPAM 2003

- Politica OPT-OUT
- Vietato lo spam di natura fraudolenta
 - Mittente non identificato



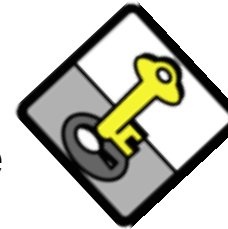


Aspetti legali: Italia

Europa: Direttiva 2002 → OPT-IN

Italia:

- Legge 675/96 (Legge sulla privacy)
 - Indirizzo e-mail come dato personale
- D.L. 196/03:
 - Divieto di inviare messaggi senza il preventivo consenso dell'interessato (art.130, commi 1 e 2)
 - Divieto di utilizzare un mittente non identificabile o irraggiungibile (art.130, comma 5)
 - Il Garante per la privacy può prescrivere al provider sanzioni per gli spammer (art 130, comma 6).



Impianti Informatici

 POLITECNICO DI MILANO



Spam

Non affidabili

- Mittente
- Indirizzo IP del mittente
- Intestazioni delle e-mail, ad eccezione dell'ultima inserita

Affidabili

- Indirizzo IP del mail server
- Testo del messaggio



Blacking list

Content filtering



Caso reale: IP mittente “nascosto”

Header sicuramente
corretto

19

HELO

Received: from servidor2.bauer.es ([195.61.24.2]) by smv198-mc.mail.com (8.9.3/8.9.1SMV070400) with SMTP id WAA21539; Wed, 21 Mar 2001 22:22:33 -0500 (EST)

Received: from myrop (ew6.southwind.net [216.53.98.70]) by onyx.southwind.net from homepage.com (114.230.197.216) by newmail.spectraweb.ch from default (m202.2-25.warwick.net [218.242.202.80]) by host.warwick.net (8.10.0.Beta10/8.10.0.Beta10) with SMTP id e9GKEKk19201

([63.44.155.8]) by servidor2.bauer.es (Lotus SMTP MTA v4.6.1 (569.22.6-1998)) with SMTP id C1256A17.00129C3A; Sun, 22 Mar 1970 04:23:31 +0100

Message-ID:

<0000749b6e86\$00001ced\$00007697@mcpeely.concentric.net(mcfeely.concentric.net [217.15.198.83]) by darius.concentric.net(8.9.1a/(98/12/15 5.12)) id PAA04003 from default (m202.2-25.warwick.net[218.242.202.80]) by host.warwick.net (8.10.0.Beta10/8.10.0.Beta10) with SMTP id e0GKEKk19201>

Subject: Viagra Alternative & FREE Herbs!

Date: Wed, 21 Mar 2001 14:15:27 -0800

X-Priority: 1

X-MSMail-Priority: High

Indirizzo IP mittente

Probabile bug nel server
servidor2.bauer.es

→ Servidor2.bauer.es è
un relay aperto



Host: smtp.polimi.it - Port: 25

220 polimi.it ESMTP Sendmail 8.13.3/8.13.3; Tue, 15 Mar 2005 10:17:14 +0100

HELO polimi.it

← **Server msg**
Client msg

250 polimi.it Hello fwvplab.elet.polimi.it [131.175.124.136], pleased to meet you

MAIL FROM:<myAddress@polimi.it>

250 2.1.0 <myAddress@polimi.it>... Sender ok

RCPT TO:<otherAddress@host.it>

250 2.1.5 <otherAddress@host.it>... Recipient ok

DATA

354 Please start mail input.

Inizio del messaggio

etc

etc

etc

Fine del messaggio

.

250 Mail queued for delivery.

QUIT

221 Closing connection. Good bye.



Camuffamento degli URL

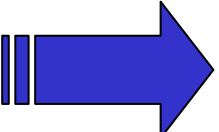
<http://3154189391/>

 <http://188.1.28.79/>

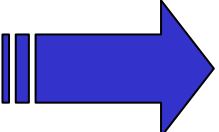
<http://0274.01.034.0117/>

 <http://188.1.28.79/>

<http://356276@202818865/abcd/def.htm/>

 [http:// 12.22.197.49/abcd/def.htm/](http://12.22.197.49/abcd/def.htm/)

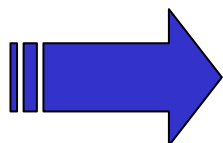
<http://209.21.162.23@23.178.75.110@216.35.27.167/>

 <http://216.35.27.167/>

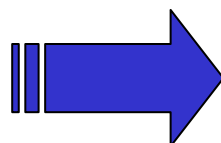


Camuffamento degli URL

<http://3%3562%376@20%3281%3886%35/%61%62c%64/def.htm>

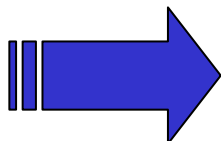


<http://356276@202818865/abcd/def.htm/>

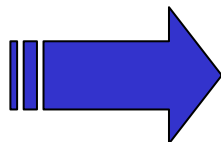


<http://12.22.197.49/abcd/def.htm/>

<http://donkin.org/bin/view/Test/жзжİÿÿ/ÉŸ' γεΘ<ζιüĩŸΓλζδЛЬ°ҢЙЙ>



<http://donkin.org/bin/view/Test/%A4%B3%A4%CE%A5%AB%A5%C6%A5...>



<http://205.196.211.91/>



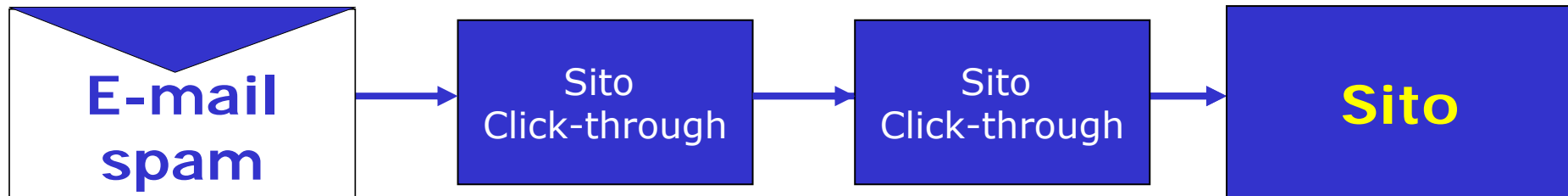
Siti click-through

Sito Click-through

- Piccolo sito
- Contenuto non significativo
- Tramite verso il “vero sito” che si vuole pubblicizzare

Può anche esserci una catena di siti click-through:

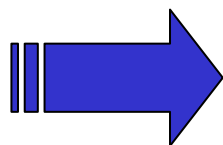
- Metodi utilizzati:
 - Semplice link HTML
 - HTML nascosto da codice javascript



Esempio: sito click-through

Spam

<http://3%36%32%36%30%34%36%34%36%38%2f%62%69%7a%34%2f%62%69%7a%34%33%33%33/start.html>



<http://216.33.20.4/biz4/biz4333/start.html>

Click-through

``
 Click Here To Continue to the quick pre-qualification form ``

Sito

`<TD width="548">`

`<FORM action="http://206.253.222.112/loanform/cgi-bin/file.cgi" method="POST">`

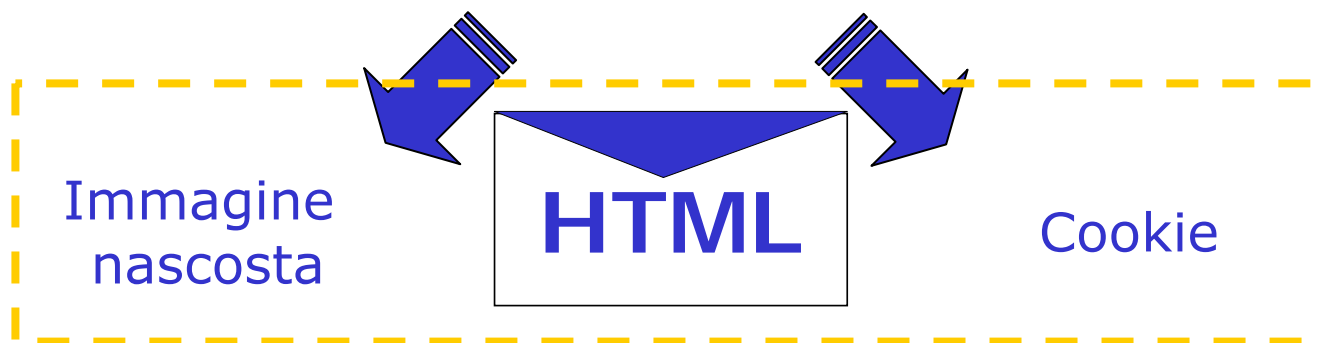
`Fill out this short form to receive`
 your free loan quote. ` `



**E-mail
spam**

Sito
Click-through

Sito



If you do not wish to receive these special e-catalogs from Spamming Magazines, then reply to this email with the word "remove" in the subject line.

Happy shopping and have a great holiday season from all of us at Spamming Magazines.

<IMG height=1

src=http://spammer_site.com/asp/email_type.asp?id=123456789

width=1>



Mostra: Tutti

Oggetto	Data
[SPAM] Special Rx	01/05/2005 ...
[SPAM] hi honey	01/05/2005 ...
[SPAM] economic well, rates at 3.52% b	01/05/2005 ...
Re: Pharmaacy 92-LWK	01/05/2005 ...
[SPAM] Don't worry about Erectile Dysfunction.	01/05/2005 ...
[SPAM] better late than never	01/05/2005 ...
[SPAM] get MEDICINES delivred	01/05/2005 ...

Thunderbird pensa che questa sia posta indesiderata!

Oggetto: Re: Pharmaacy 92-LWK
Da: Morgane Duckworth <DuckwoMorgan8955@khcoi.com>
Data: 01/05/2005 04:43
A: Leon Tracy <abuse@people.it>

Hello, Do you want to spendd LESS on your medications?

Visit PahrmacyByyMail SHOP and SAVE Over 70%

V 1A GR A VALI UM C IAL IS XA NA X and many other

Try us and you will NOT BE DISAPPOINNTED!.
Have a Nice Day.

- Mittente e nome del destinatario palesemente fasulli.

- Lo spammer "cerca" il contatto attraverso la sua e-mail o il link all'interno del messaggio.

- Il subject è una "finta" risposta

Regola #1: lo spammer mente.

Regola #2: mai rispondere allo spam.

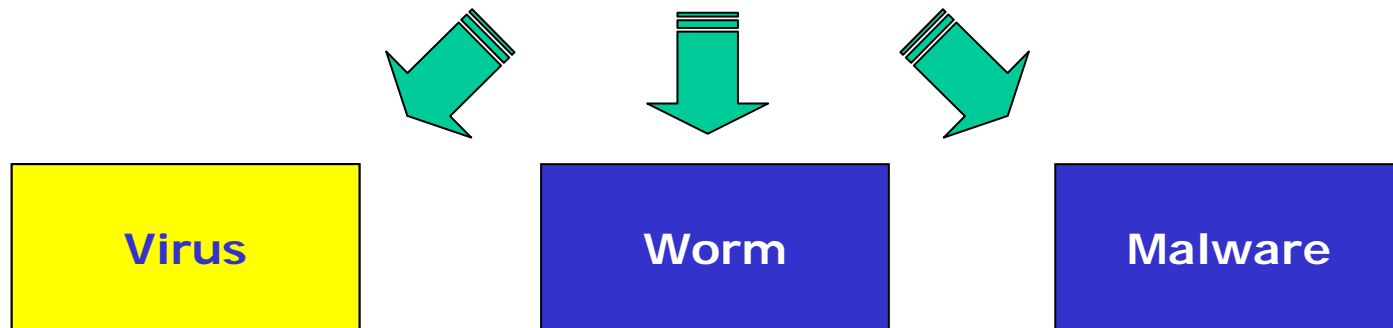
Alcune parole vengono volutamente scritte in modo errato per eludere i filtri.

Ex: spendd, ByyMail, DISAPPOINNTED, V 1A GR A, Pharmaacy

Corpo del messaggio



Virus, worm e malware

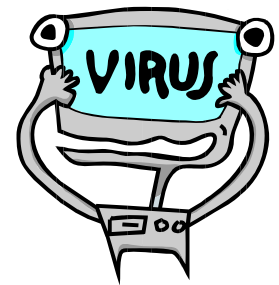


Frammento di codice

- Capacità di autoreplicarsi
- Infetta un *ospite* (e.g. eseguibile)
- Causa effetti indesiderati

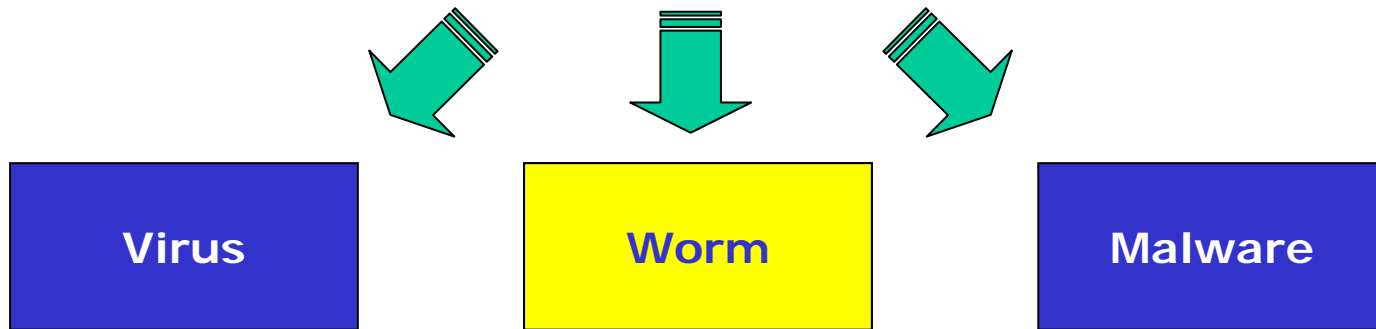
Si diffonde a causa dell'esecuzione dell'*ospite*

- Programma infetto
- File word con macro virale
- Boot infetto





Virus, worm e malware



Programma autonomo

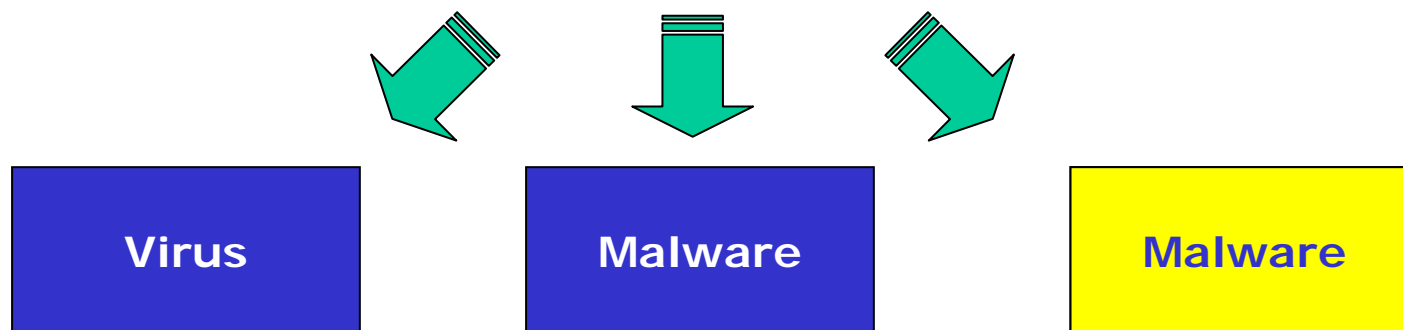
- Capacità di autoreplicarsi
- Spesso inviato tramite e-mail

Effetti:

- Sola propagazione
- Sfrutta risorse computer ospite



Virus, worm e malware



Categoria di programmi dannosi (non virali):

- *Spyware*: raccoglie e invia informazioni dal computer su cui gira
- *Trojan Horse*: consente l'ingresso di una terza parte nell'ospite
- *Backdoor*: consente all'aggressore di prendere controllo del computer da remoto





Interazione spam-virus

Molti worm installano una *backdoor* sulla macchina ospite.

- Legame sempre più stretto tra spammer e virus-writer
- La macchina ospite diventa un proxy aperto
- Hanno server SMTP per diffondersi

Il target ideale è l'utente ADSL

- Sempre connesso
- Senza alcuna forma di tutela

Impianti Informatici



POLITECNICO DI MILANO

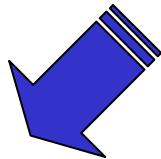


Spam



Spam: tecniche di contenimento

Spam



Accordi tra:
Utenti
Amministratori
Legislatori



Filtraggio in ricezione:
Blacklist e blocking list
Content Filtering



Insieme di indirizzi IP potenziali sorgenti di spam.

- Open relay
- Proxy aperti

Modalità di creazione:

- Automatiche:
 - *Spamtrap* (honeypot)
 - Account creato per ricevere SOLO e-mail di spam
 - Potente strumento per soluzioni anti-spam
- Manuali:
 - Segnalazioni
 - Collaborazione fra ISP



Blocking list

Insieme di indirizzi IP potenziali sorgenti di spam

- Appartenenti a particolari classi e tipologie
 - Intere nazioni
 - Indirizzi dinamici



Blacklist e blocking list: funzionamento

Blacklist e blocking list agiscono a monte della ricezione del messaggio

- Il messaggio non viene ricevuto dal destinatario

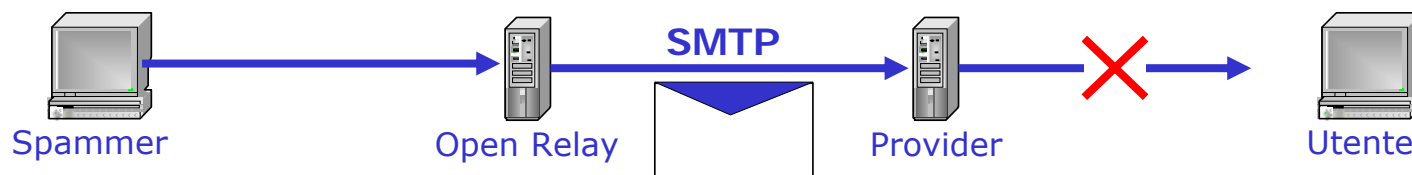
Messaggio accettato solo se l'IP del server mittente **NON** è in una di queste liste.

- Si usa il DNS → DNSBL

Blacklist e blocking list possono avere effetti negativi se non usate correttamente

- ex. blocco intere aree di internet

Il provider può utilizzare una o più di queste liste





Notifica di rifiuto

Messaggio considerato spam

- Respinto da una lista
- Il mittente riceve una comunicazione
 - Delivery Status Notification (DSN)
- Motivo del rifiuto
- Contatti in caso di errore

DSN

This is the Postfix program at host fatigauhu.taloha.tk.

I'm sorry to have to inform you that your message could not be delivered to one or more recipients.

It's attached below. For further assistance, please send mail to <postmaster>. If you do so, please include this problem report. You can delete your own text from the attached returned message.

The Postfix program

<username@domain.com>: Client host 213-35-180-216-dsl.lsn.estpak.ee[213.35.180.216]: 554 Service unavailable; Client host [213.35.180.216] blocked using dnsbl.njabl.org; open proxy -- 1049591101.
Please, contact postmaster@domain.com for more informations.



Content filtering

Si basa sul contenuto dell'e-mail

Ricerca indicazioni caratteristiche dei messaggi di spam

- Immagini
- HTML
- Parole chiave in precedenti messaggi non richiesti
- ...

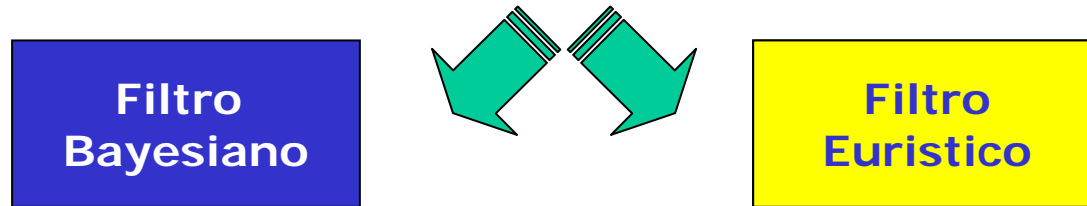
Filtraggio a posteriori

Dispone di informazioni maggiori rispetto a blacklist e blocking list

Conseguenze del filtraggio:

- E-mail marcate come *spam*
- E-mail spostate in apposite cartelle nella user mailbox

Content filtering: filtri



Basato su “impronte” di spam:

Assegna un punteggio a frasi/modelli nel messaggio

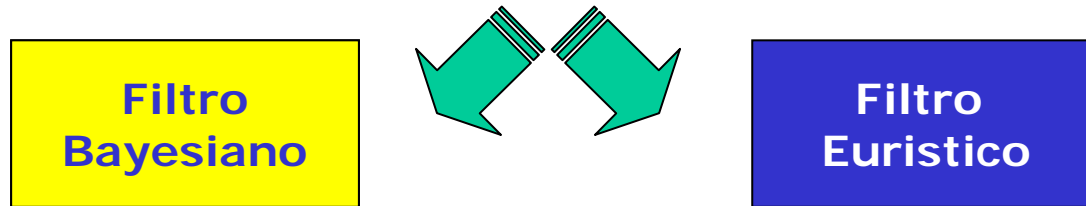
- Positivo se ritenuta spam
- Negativo altrimenti

Il numero di falsi positivi è praticamente nullo

Alto costo manutenzione:

- Il database necessita di aggiornamenti continui

Content filtering: filtri



Basato su tecniche di apprendimento automatico (machine learning)

Basso costo di manutenzione

Se “istruito” correttamente ha un basso numero di falsi positivi

Il sistema può essere ingannato di proposito inquinando così i database

- Inviando mail “buone” contenenti parole tipiche dello spam
- Inviando mail di “spam” contenenti parole comuni



Content Filtering: elusione

Gli spammer cercano di eludere il filtraggio

Inseriscono parole “buone”

- Nascoste all'utente
- Visibili al filtro

```
<DIV><FONT style="FONT-SIZE:  
1px">ensorious coriander jowly bender hatchet  
convert leek henpeck shanghai besse...
```

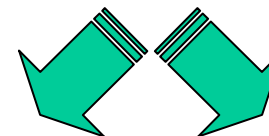
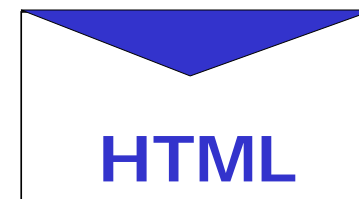
If you are paying more than 3.6% on your mortgage,
we can slash your payment!

GUARANTEED LOWEST RATES ON THE PLANET

APPROVAL REGARDLESS OF CREDIT HISTORY!

Start saving today

[Show Me The Lowest Rates](#)

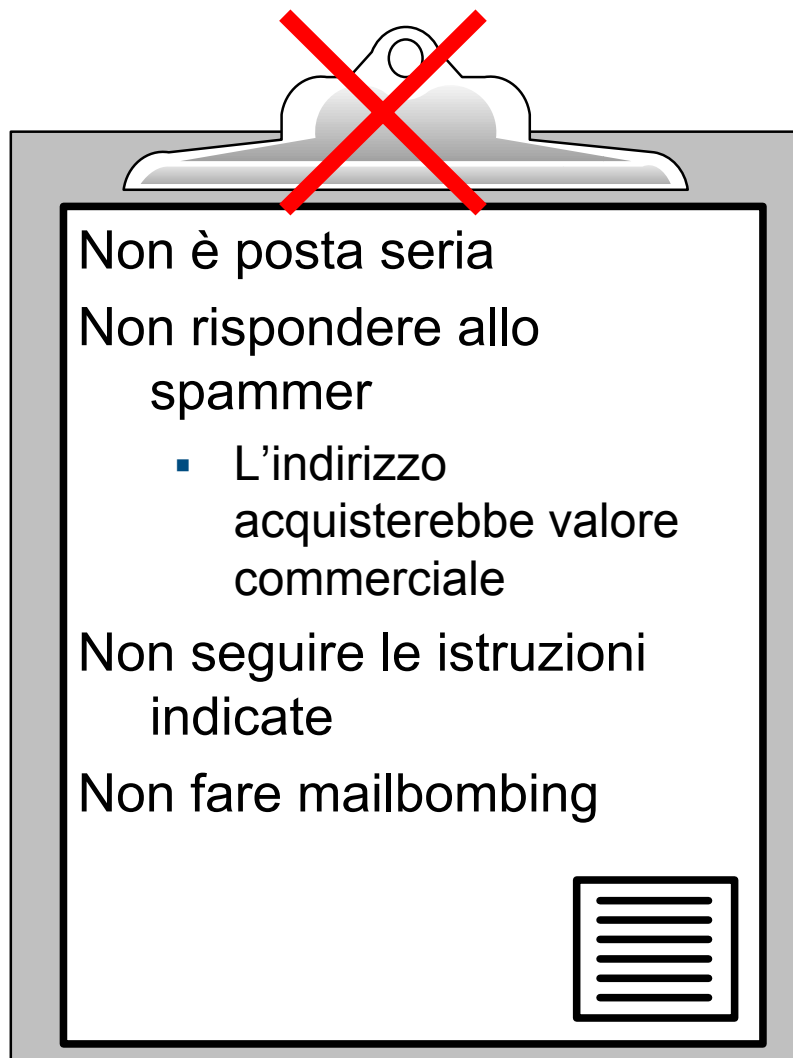


Carattere bianco
su sfondo bianco

Carattere
minuscolo



Spam: cosa fare e cosa non fare





Virus, worm, malware: prevenzione

