

Impianti Informatici

POLITECNICO DI MILANO

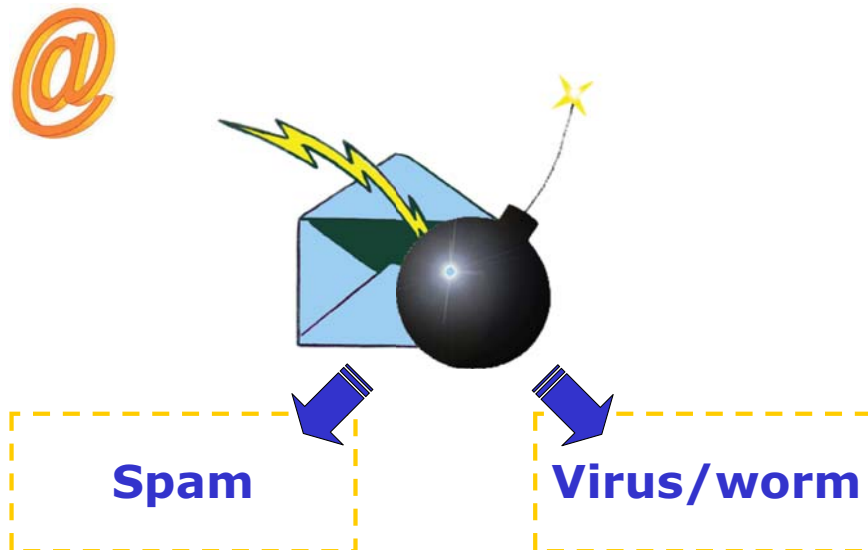


Spam



Minacce alla posta elettronica

2



Impianti Informatici

POLITECNICO DI MILANO



Spam: definizione

3

Comunicazione
elettronica

massiva

non richiesta



"Monty Python's Flying Circus"

Impianti Informatici

POLITECNICO DI MILANO



Tipologie di spam

4

UCE (Unsolicited Commercial Email): messaggi di carattere commerciale con invio massivo.

UBE (Unsolicited Bulk Email): messaggi non commerciali con invio massivo

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

unsolicited

Libertà di
parola

?

Internet
pubblico

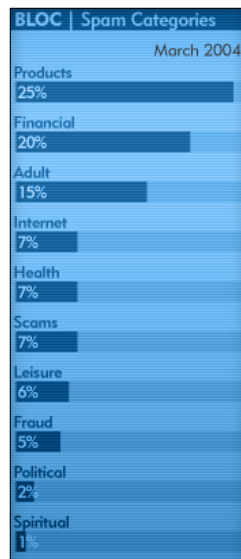
Impianti Informatici

POLITECNICO DI MILANO



Spam: contenuto

5



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")



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

Impianti Informatici

POLITECNICO DI MILANO



Fenomeni correlati

6

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 raggiro

Scam:

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



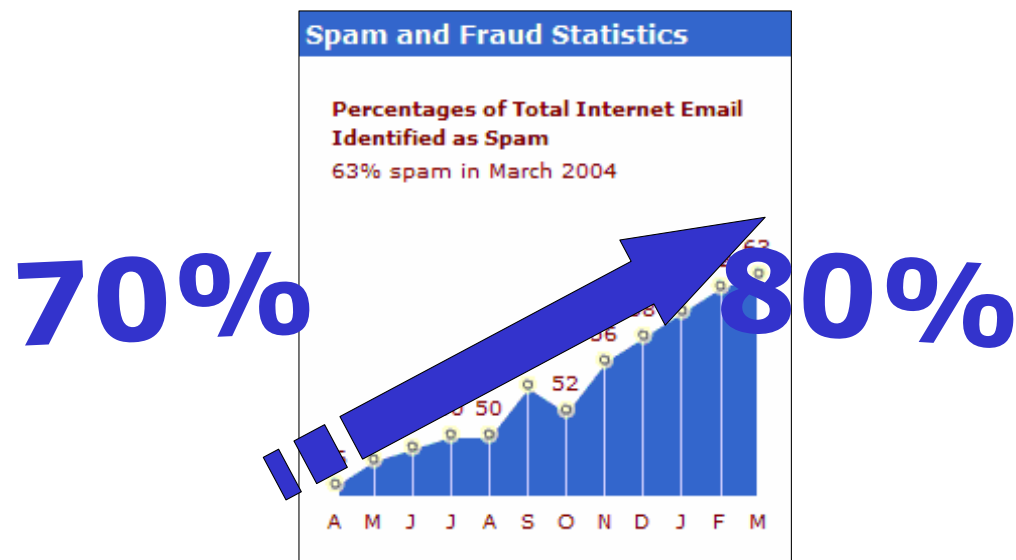
Impianti Informatici

POLITECNICO DI MILANO



Diffusione

7



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

Impianti Informatici

POLITECNICO DI MILANO



Gli spammer

8

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)

Impianti Informatici

POLITECNICO DI MILANO



≠



Pubblicità pagata dal destinatario anche se non acquista il prodotto.
Costi di invio praticamente nulli

percentuale di acquisto
0,0000001%



Provider:

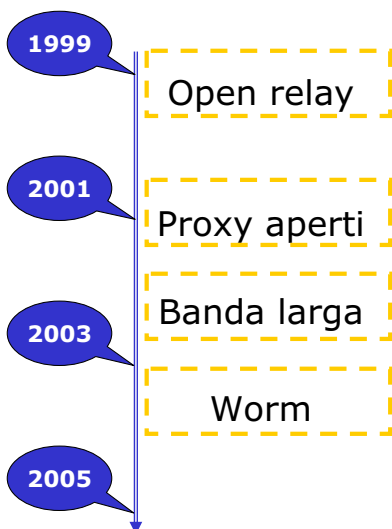
- Banda
- Risorse
 - Hardware
 - Software
 - Personale
- Immagine

Utenti:

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

costo per gli utenti finali

10 miliardi €/anno



Estrapolazione di tutto ciò che contiene @

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



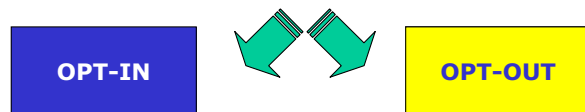
Rubrica di un conoscente infettato da un virus

- Fonte di indirizzi *puliti*

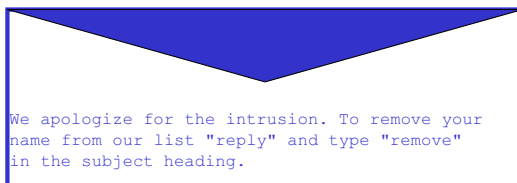
Indovinato da un attacco a vocabolario

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

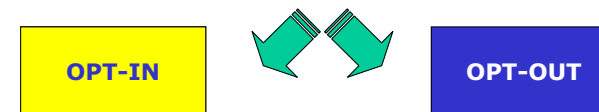




Occorre una richiesta da parte dell'utente per essere rimosso dagli elenchi



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



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

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



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



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



Spam: criteri di analisi

18

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
Blocking list

Content filtering

Impianti Informatici

POLITECNICO DI MILANO



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

Fonte: <http://www.collinelli.net/antispam>

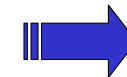
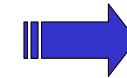
Impianti Informatici

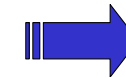
POLITECNICO DI MILANO



Camuffamento degli URL

20

<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://209.21.162.23@23.178.75.110@216.35.27.167/>

<http://216.35.27.167/>

Impianti Informatici

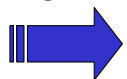
POLITECNICO DI MILANO



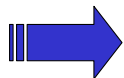
Camuffamento degli URL

21

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

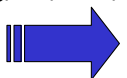


`http://356276@202818865/abcd/def.htm/`

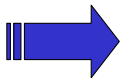


`http:// 12.22.197.49/abcd/def.htm/`

`http://donkin.org/bin/view/Test/жэжйу/É'yeΘ<ζιüŸΓλζδль°нйЙ`



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



`http://205.196.211.91/`

Impianti Informatici

POLITECNICO DI MILANO



Siti click-through

22

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



Impianti Informatici

POLITECNICO DI MILANO

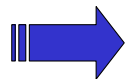


Esempio: sito click-through

23

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`

Click-through { `http://216.33.20.4/biz4/biz4333/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. `



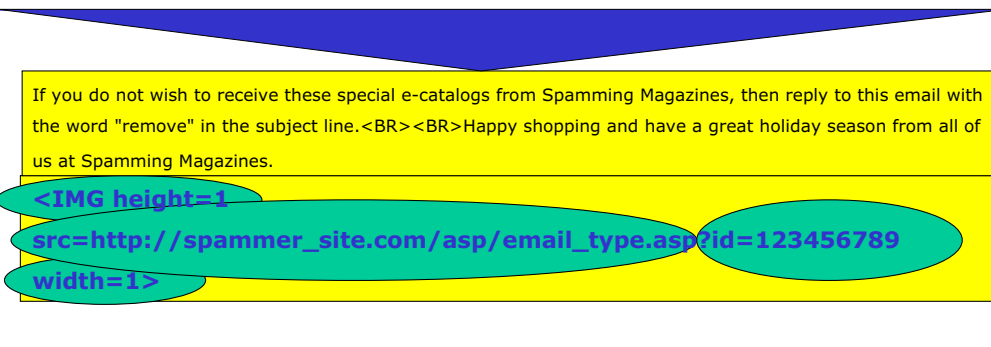
Impianti Informatici

POLITECNICO DI MILANO



Web bug

24



Impianti Informatici

POLITECNICO DI MILANO



Mostra: Tutti

• 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.

Thunderbird pensa che questa sia posta indesiderata!

Oggetto: Re: Pharmaacy 92-LWK

Da: Morgane Duckworth <DuckwoMorgan8955@khoo.com>

Data: 01/05/2005 04:43

A: Leon Tracy <abuse@people.it>

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

Visit PahrmaacyByyMail SHOP and SAVE Over 70%.

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

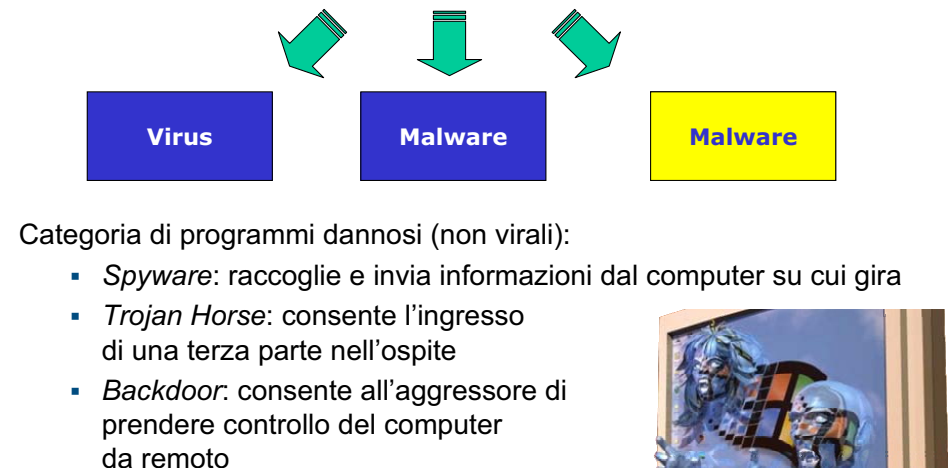
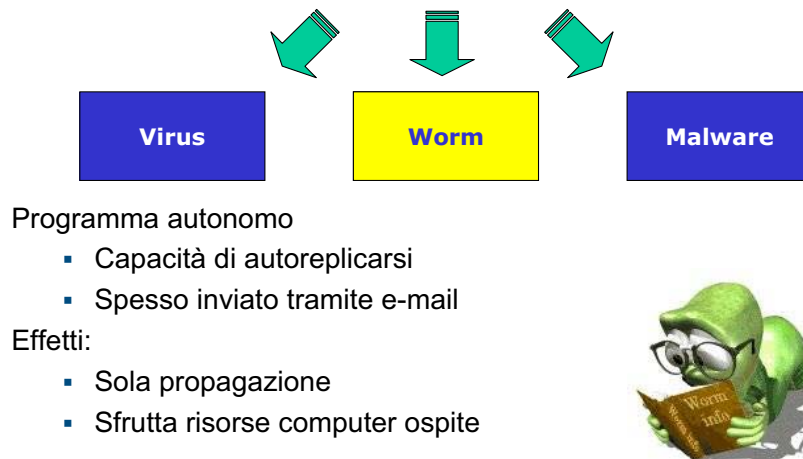
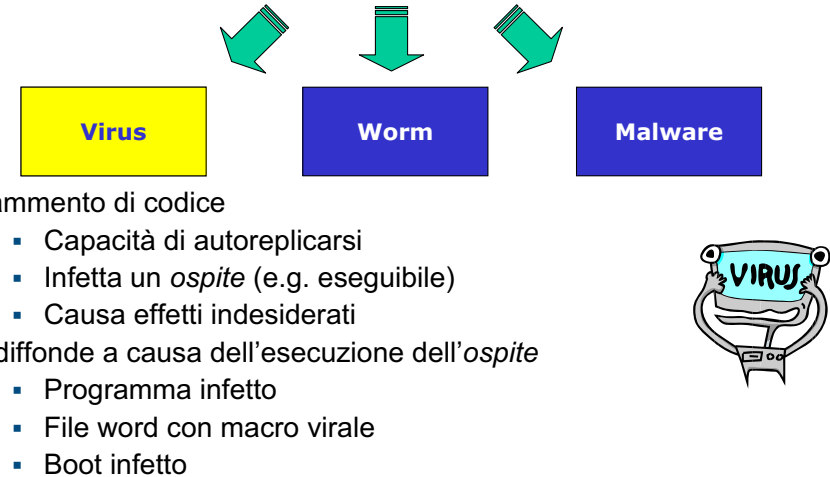
Try us and you will NOT BE DISAPPOINNTEd.

Have a Nice Day.

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

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

Corpo del messaggio





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



Spam



Spam: tecniche di contenimento

Spam



Accordi tra:
Utenti
Amministratori
Legislatori

Filtraggio in ricezione:
Blacklist e blocking list
Content Filtering



Blacklist

Insieme di indirizzi IP potenziali sorgenti di spam.

- Open relay
- Proxy aperti

Modalità di creazione:

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



Insieme di indirizzi IP potenziali sorgenti di spam

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



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



Messaggio considerato spam

- Respinto da una lista
 - Delivery Status Notification (DSN)
- Il mittente riceve una comunicazione
 - 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.isn.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.



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

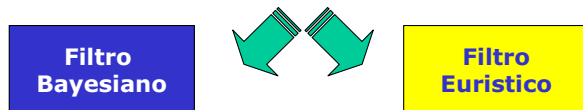
Conseguenze del filtraggio:

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



Content filtering: filtri

37



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

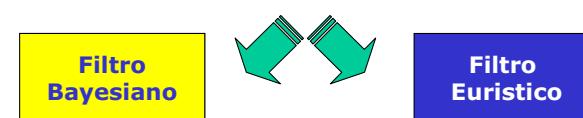
Alto costo manutenzione:

- Il database necessita di aggiornamenti continui



Content filtering: filtri

38



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

39

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 bessel...
```

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](#)



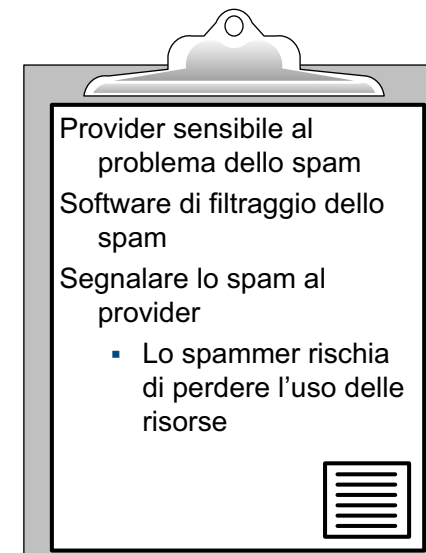
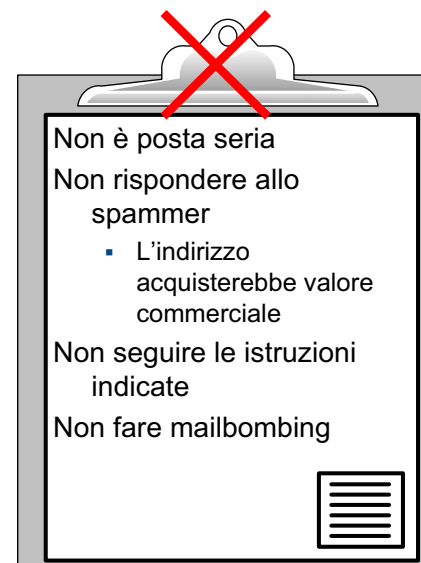
Carattere bianco
su sfondo bianco


Carattere
minuscolo



Spam: cosa fare e cosa non fare

40





Antivirus

- Mantenerlo aggiornato

Target dei virus:

- Software diffuso
- Sistemi operativi diffusi

Firewall

- Aggiornare S.O.

Diffidare degli allegati

- Diffidare del mittente indicato

