



approaches to dealing with spam

speech for the Association of Digital Information and Industry
Tokyo, Japan

Christopher R. Keener
adi2@duck.mailshell.com
July 16, 2003

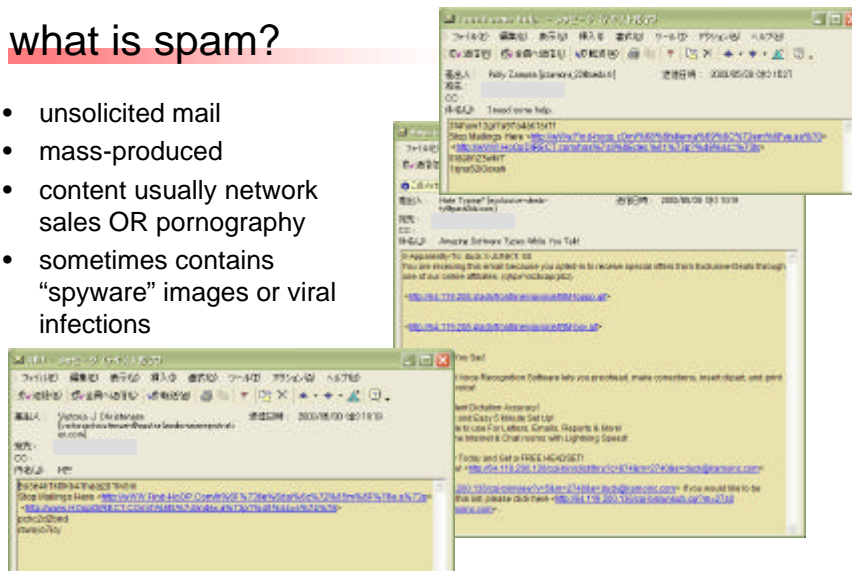
www.spamradio.com

www.venture-web.or.jp/adi2/

www.kamoinc.com

what is spam?

- unsolicited mail
- mass-produced
- content usually network sales OR pornography
- sometimes contains "spyware" images or viral infections



from where does it derive it's name?



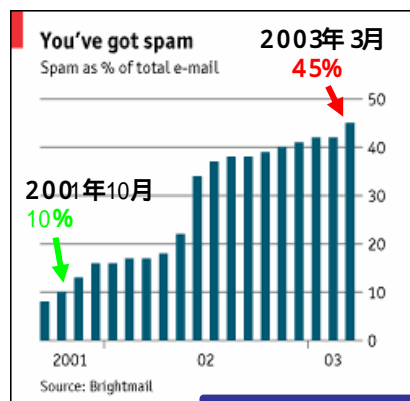
www.spam.com

- SPAM™ is the name of a canned ham manufactured by Hormel Foods (USA)
- “spam” as junk mail apparently derives its name from a skit on Monty Python (a BBC TV program from the early 70s)



www.ironworks.com/comedy/python/spam.htm

recent explosion of spam

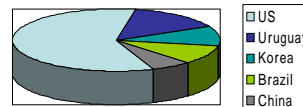


www.brightmail.com



www.jmm.com

Top-5 spamming countries by volume



www.mailarmory.com/resources/stats/

my personal experience

- over 20 years experience using e-mail on daily basis for work
- very little negative experience with spam until early this year
- began to receive 40-50 spam messages every day in January

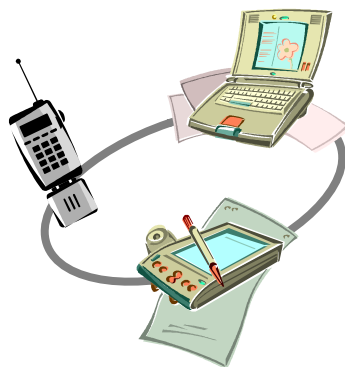


approaches to dealing with spam
Christopher R. Keener

July 16, 2003
Copyright © 2003 by kamo, inc.

5

my use of e-mail



- predominantly use a PC
- often access Internet via a slow, expensive connection (i.e. from a cell phone or from an Internet cafe)
- use cell phone & PDA for urgent short mail messages
- preservation of permanent e-mail address is important
- "end-user" solution should not involve programming or maintenance of server

approaches to dealing with spam
Christopher R. Keener

July 16, 2003
Copyright © 2003 by kamo, inc.

6

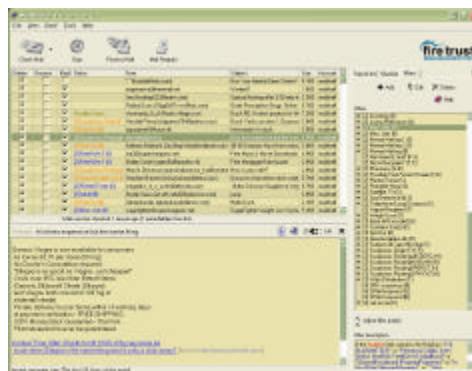
three solutions I have tried

company name; location; URL	service content	background of company
① FireTrust New Zealand www.firetrust.com	"MailWasher PRO" stand-alone application.	Small independent start-up. Founded 2000. Good personalized support by developers; cadre of dedicated personal users.
② BrightMail California USA www.brightmail.com	Filter service based on "honey pot" concept.	Small startup with financial backing from Symantec. Founded 1998. Used by large US corporations and ISPs (ATT, EarthLink, MSN).
③ MailShell California USA www.mailshell.com	Web-based service which employs multiple proprietary filtering approaches.	Small independent start-up. Founded 1999. Has adopted several industry standards such as TRUSTe's Postiva Trusted Sender technology.


MailWasher: overview



- stand-alone application that you invoke *before* you read mail using your e-mail client
- checks mail against
 - "friends" white list
 - black-list spammers (learns from previous mail)
 - filter rules



MailWasher: pros & cons




<h3>STRENGTHS</h3> <ul style="list-style-type: none">catches 95% spameasy to initially populate and maintain white and black listsallows use of powerful regular expressions in white/black lists and filter rulesworks with any POP e-mail client	<h3>WEAKNESSES</h3> <ul style="list-style-type: none">complicated setupthe manual work involved in reading mail increases with use of this toolaggressive filters generate false positives
---	--

approaches to dealing with spam
Christopher R. Keener

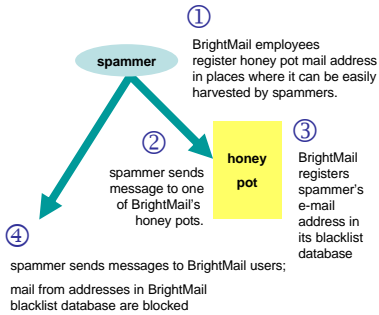
July 16, 2003
Copyright © 2003 by kamo, inc.

9

BrightMail: overview



- service which filters your e-mail before it is placed in your POP mailbox (no software included)
- BrightMail employees leave "honey pots" for spammers to find (e-mail addresses left on web pages, news groups, subscription to mailing lists, etc.)
- BrightMail filters trap any mail bound for its clients that has also been sent to its "honey pots"



The diagram illustrates the BrightMail honey pot process in four steps:

- 1** BrightMail employees register honey pot mail address in places where it can be easily harvested by spammers.
- 2** spammer sends message to one of BrightMail's honey pots.
- 3** BrightMail registers spammer's e-mail address in its blacklist database.
- 4** spammer sends messages to BrightMail users; mail from addresses in BrightMail blacklist database are blocked.

approaches to dealing with spam
Christopher R. Keener

July 16, 2003
Copyright © 2003 by kamo, inc.

10

BrightMail: pros & cons



STRENGTHS

- does not complicate use of e-mail client and reading of e-mail
- simple setup procedures

WEAKNESSES

- catches only 50% - 75% of spam
- poor interface for deletion and manipulation of spam items in *junk mail* folder
- not configurable

MailShell: overview



- web-based filtering service
- provides IMAP/POP mail box with 50Mb storage
- allows user to specify delivery locations for "clean" mail and junk mail
- allows user to set up disposable e-mail addresses




MailShell: pros & cons

STRENGTHS	WEAKNESSES
<ul style="list-style-type: none">• catches 99% spam• easy to set up• flexible interface allows setting of forwarding options, filter strength• allows user to set up white and black lists and other simple filter rules	<ul style="list-style-type: none">• unscheduled server downtime• lack of regular expressions• lack of Bayesian filters• relatively expensive (\$35/year)

approaches to dealing with spam
Christopher R. Keener July 16, 2003
Copyright © 2003 by kamo, inc. 13

recommendations

- avoid using a permanent e-mail address if possible
- never reply to spam or follow opt-out instructions
- use multiple levels of spam filtering



approaches to dealing with spam
Christopher R. Keener July 16, 2003
Copyright © 2003 by kamo, inc. 14

