



Welcome to “The spam problem” computer-based training module.

There are links to additional information throughout this module.
Click on graphics and all listed URLs in the slides to find out more.

Navigate through this Adobe Acrobat PDF by clicking on the titles in the
“Bookmark” menu.



Module content

SOPHOS

This short module provides an introduction to the spam problem:


- What is spam?
- Spam techniques
- Anti-spam techniques
- Sophos PureMessage

SOPHOS

The spam problem

What is spam?

www.sophos.com



What is spam?

SOPHOS

- Unsolicited commercial email – UCE
- Offensive content
- Malicious email (identity theft, fraud)

- Annual losses:*

 - Theft of information ~\$US170 million
 - Fraud ~\$US115 million

*source: FBI

<http://www.sophos.com/spaminfo/explained/>

Spam

Typically, spam is defined as unsolicited commercial email (UCE), often sent in bulk:

- Unsolicited in that the recipients have in no way requested, subscribed or invited the email
- Commercial in that the message is intended to motivate you to spend your money.

Put simply, spam is uninvited email attempting to get money from you.

Spam comes in many forms from offers to provide low-cost pharmaceuticals or ink jet cartridges to invitations to pay for subscription-based pornography sites, and sometimes even fraudulent money scams.

Spam means different things to different people. What one person may consider junk mail, another may classify as essential information. Any company policy designed to deal with spam may need to recognise these distinctions.

There is always a “call to action” in spam emails – without it, the spam is as worthless to the spammer as it is to the target.

Why spammers spam

SOPHOS

- To make MONEY
- 3-5% response rate beats the 1-2% of direct mail
- No postage, paper or printing costs
- Spammers can send hundreds of thousands of unsolicited messages at the click of a mouse



How do they find you? **SOPHOS**

- Address harvesting
- “Free” software downloads
- Online greetings cards
- Chain letters
- Purchase from list sellers




Spammers use dictionary attacks to harvest email addresses. They will work through all possible email address permutations – relying on the target server to provide “user unknown” responses to the ones that do not exist and “recipient OK” responses to the ones that are valid.


Many free software downloads that request email addresses are also in the business of selling valid email address lists. They will even deliver the software via email to validate the addresses given to them.

Some online greetings cards services also sell email address lists. Have you ever wondered how they fund “free” greetings card services? The services, bandwidth and the software all cost money.

Another simple technique spammers use to collect email addresses is the chain letter. Most chain letters ask you to forward the email to a set number of your friends and in doing so you add to the growing list of valid recipients that the spammer will target.



Spam statistics




- *eMarketer* predicted the volume of spam messages would reach 76 billion in 2003
- Costs of resources, lost productivity and time
- 30% of employees' email time wasted managing spam
- Estimated that spam management requires one full-time administrator for every 10,000 users

eMarketer, a leading provider of internet statistics, estimated that nearly 76 billion spam messages would be delivered over the internet in 2003.


According to Ferris Research, the overall cost to US organisations for 2003 was estimated at over \$10 billion, measured in lost productivity, time and resources such as additional servers, network capacity and software.

Gartner Inc. estimates that ridding a business of spam would result in a 30% savings in the time that employees spend managing email.

Meta Group expected most companies to spend \$7-\$10 per user during 2003 buying spam-blocking software, and to dedicate one full-time employee per 10,000 users to spam-blocking operations.



Impact of spam



- Total impact of spam is difficult to calculate:
 - Most spam is unreported
 - People have varying levels of tolerance
 - People receive different amounts of spam
- Many organisations report that more than 50% of inbound email is spam

Spam has a variety of impacts on an organisation, but the total impact is generally recognised because most spam goes unreported.

Offensive spam is often unreported, as users are embarrassed about having such content in their inboxes and are often afraid they will be blamed for receiving it.

Depending on their level of tolerance of spam and the amount they receive, some people may tolerate it rather than report it.

Many people believe nothing can be done and as a result do not bother to report spam.

Organisations should be encouraged to determine the collective impact of spam to assess their protection needs.

Organisations that have evaluated Sophos PureMessage consistently identified more than 50% of their inbound mail volume as spam.

Costs of spam



- Not just a nuisance
- Email is an essential business tool
- Prevalence of spam is rising dramatically
- Spam is a cost to end users and their organisations




Ferris Research estimates that managers will spend four hours per day on email this year.

Direct marketing through spam is growing at an exponential rate. Part of the reason for this is that spam shifts the cost of marketing to the receiving company, making it a very cost-effective method of reaching potential customers.

Worse still, the flood of spam shows no sign of abating. Internet resource company Jupiter Media Metrix claims the average American received 571 spam messages in 2001 and predicts that, by 2006, the annual figure will be 1,479.

Spam is an increasingly pervasive problem costing money, time, and valuable IT resources. According to a recent study, spam costs consumers worldwide approximately \$8.8 billion a year in connection expenses alone.



Costs of handling spam **SOPHOS**

- Lost productivity of email users
- Lost productivity of system administrators
- Extra mail system resources required
- Consumption of bandwidth
- Example of productivity costs:

Wages \$30/hour = \$0.025/email
10,000 users x 9 spam / day x \$0.025
= \$2,250 / day or \$495,000 annually
(assuming 220 working days)

Costs of spam to the organisation

One of the largest organisational costs is lost productivity.

If it takes three seconds to identify and delete an unsolicited email, at an average employee cost of \$30/hour, that represents a cost of \$0.025 per email. While the figure may seem insignificant, multiply it by the amount of spam received each day for each employee (say, 30% of 30 messages = 9), and the cost quickly becomes substantial for a large organisation.

Lost productivity also occurs among email administrators and IT helpdesks because of the increasing amount of time spent responding to spam complaints from frustrated users.

Stanford University reported that, before the installation of Sophos PureMessage, they were receiving 800 helpdesk calls a day about spam.

Other organisational effects include:

- Network resource drain, including internet bandwidth, mail server processing cycles and storage capacity
- Potential legal issues resulting from creating a “hostile environment” if some employees receive spam they consider to be offensive

SOPHOS

The spam problem

Spam techniques

www.sophos.com



Typical spam content

SOPHOS

- Vulgar, lewd or offensive words
- Contains alphanumeric identifiers
- References to money or similar themes
- Offers:
 - Pharmaceutical and “personal” products
 - Insurance
 - Low interest rate loans




Spam characteristics

SOPHOS

- Same (or similar) message sent in bulk
- Designed to solicit a commercial response
- Typically has a “call to action”, money solicitation
- Contains tracking tools to validate recipients
- Attempts to make message appear unique
- Uses vague subject tags, e.g. “Hi it’s me...”

Evolving spam techniques



- Using HTML tricks to hide content
 - This can be a combination of HTML formatting, vowel substitution and other tricks:

T	H	I	S	I	S
@		5	P	A	M

- Using HTML image-based spam
 - Including a link to an HTML image which is automatically downloaded from a website

<http://www.sophos.com/spaminfo/explained/fieldguide.html>

With the advent of anti-spam solutions, spam has begun to evolve in an effort to circumvent filtering. This leads to spammers attempting to present their message to the recipient effectively, while sneaking past anti-spam systems. This evolution has also included the development of techniques so that spammers can validate recipients' address information and verify that recipients have actually seen the message.

Examples are:

LOST IN SPACE

What it is: Insertion of spaces and other non-alphabetic characters between letters to make words unrecognisable to a word filter.

Example:

```
M O R T G A G E
F * R * E * E V ' I ' A ' G ' R ' A O * N * L * I * N * E
* O - N - L - I - N - E * P - O - R - N *
```

Hypertextus interruptus

What it is: Splitting of words using HTML comments, pairs of zero-width tags, or bogus tags.

Example:

```
milli<!-- xe64 -->onaire: the recipient sees "millionaire"
Fi</n>nd N</n>ew </n>Fri</n>end</n>s: the recipient sees "Find New Friends"
Vi<b></b>agra: the recipient sees "Viagra"
F<XYZ>r<XXYA>ee: the recipient sees "Free"
```



Spam is a moving target.

There is now a stronger link between virus writers, hackers and spammers. Certain worms and Trojans are designed to allow hackers to take over innocent users' servers and use them to generate millions of spam messages. Thus hiding the true identity of the spammer and enabling them to generate spam for free.

LOMBODI: In a historical occasion for the Hindu community in Britain, Dewal has been celebrated inside the House of Commons, with Prime Minister Tony Blair lighting the traditional lamp to mark the festivities. Presiding over the function, attended by more than 100 MPs and 400 guests, Blair said the visit "demonstrated the unity, warmth and the festival brings each year and the spirit with which it is celebrated. It is a great privilege and pleasure for me to share in the joy of celebrating Dewal with the Hindu community in the House of Commons. Dewal is now celebrated by different communities across the UK and its growing popularity helps to strengthen the bonds between them." The speech the prime minister's celebration of Dewal in the House of Commons is a unique achievement in the history of the British Parliament. "Dewal has 19 million Indians, who organised support for an other parliamentarians for holding the event, said. The major difference this year is that we have introduced an interfaith element to the celebrations," said Ramesh Kaldas, general secretary of the Hindu Centre for Consciousness and coordinator for the event. "Members of all the religions and all the public of various faiths came together at the House of Commons to celebrate and share the universal message of Dewal." JALANDEHARI: Gurabhai Singh Malik, Canadian Member of Parliament, has termed as "unfortunate" the invitations of the ex-tennis star in prison during Prime Minister Jean Charest's visit to India in 2004. Malik was a part of the delegation but stayed back to meet relatives and friends and pay a visit to his village near Nagabhatoli told THE news that the Canadian MP wanted to extend business relations with the government of India and with Punjab. There are over 1.1 billion Punjabis in Canada out of which 70 per cent are from Doha. The Punjabi population cannot be ignored. Punjab is facing a lot of problems there. Even the legal assignments don't get filed," said the MP. "Knowing that geographic boundaries were changing and that soon the map of the world would have to be re-drawn, Malik said it was probably the first time that the Prime Minister of a country had made such a trip.



Latest spammer innovation - 'hashbusting' example

New frontier
Spam sent 'in the clear'

No attempts to disguise the message

Early adaptation
Text disguised content

- * Randomised content (subject)
- * Word obfuscations (o=0, l=1)
- * Source relocation (IP to IP)
- * Dictionary attacks (a@, b@)

Adv obfuscation
HTML disguised content

- * Randomised content (body)
- * Content in images (jpgs, other)
- * HTML tags obfuscate text (**)
- * Use of web bugs to clean lists

Threat convergence
Spam and viruses converge


- * Viruses building a spam network
- * Dynamic sources and destinations
- * Hashbusting techniques, eg 'textbook' content in body

SOPHOS


The spam problem

Anti-spam techniques

www.sophos.com



Detecting spam



- Domain Name System blackhole list (DNSBL)
 - List of known spammers
 - Updated by the public
 - Limited effectiveness


There are many anti-spam techniques, the first of which was listing known sources of spam and refusing to accept mail from them. The listing technique evolved into a consolidated public effort known as DNSBL (Domain Name System Blackhole List).

A DNSBL maintains a list of known spammers, updated by spam complaints from the general public. Mail systems receiving mail could query those lists to see if the sender of a message transaction was listed on the DNSBL as a spammer, and refuse an email transaction if they were.


However, DNSBLs suffered from some limitations. They could be late in adding new entries because users could receive numerous spam messages before they complained about a specific spammer. Although domain name information used to take some time to register, it is now very quick. However, spammers are equally quick to change their internet identity once they are blacklisted. Additionally DNSBLs have a habit of punishing the innocent with the guilty.

Some legitimate domain names, such as Yahoo, have been in the past listed on DNSBLs as some of their users were indeed responsible for spamming. Unfortunately, the entire domain gets listed thus punishing the innocent users as well. Several DNSBLs have emerged on the internet, including Spamcop, Dorkslayer and MAPS. Although some DNSBLs are run on a pay-to-subscribe basis, others are free.

Spammers have sought to circumvent DNSBLs, so other anti-spam techniques have evolved too.



Detecting spam



- Whitelisting
- DNS checks
- Header analysis
- Keyword filters
- Signature check
- Heuristic analysis

Whitelisting: The listing of trusted or 'known good' senders

DNS checks: Checking the sender information to ensure its validity

Header analysis: Analysing the header to look for bogus or spoofed information as well as other spammer like addressing characteristics

Keyword filters: Filtering messages with spam-like subject

Signature check: Comparing the incoming message body's signature against a database of known spam signatures

Heuristic analysis: Analysing the message for known spam characteristics and patterns. Not looking for specific examples of things like a keyword filter might do, but, actually looking more at characteristics, like obfuscated words.

SOPHOS

The spam problem

 puremessage

www.sophos.com



- Gateway email filtering software
 - Consolidated protection against viruses, spam and other email-borne security threats
 - Subscription software with inclusive 24/7 live support and automated anti-spam and anti-virus updates
- Sophos PureMessage solutions
 - PureMessage for Unix
 - PureMessage for Windows/Exchange
 - PureMessage Small Business Edition

Detailed training is available for the Sophos PureMessage product range. Please contact your Sophos account manager for further information on the following training modules:

PureMessage for Unix:

- Computer-based training
- Classroom technical training (two days)

PureMessage for Exchange:*

- Enterprise solutions computer-based training
- Classroom Enterprise solutions technical training (two days)

PureMessage Small Business Edition:

- Computer based training
- Classroom technical training (one day)

* PureMessage for Exchange is covered as part of a two day training course on Sophos Enterprise solutions.

Thank you for taking "The spam problem" computer-based training module.