Welcome!
Best Current Practices on spam prevention

Champika Wijayatunga, APNIC
champika@apnic.net

2 August 2006, Karachi, Pakistan

In conjunction with SANOG8

1

Overview

- Background: spam
- Problems and prevention
  - Consumers, Businesses and ISPs
- Spam filtering and anti spam techniques
- Handling spam
- Spam laws
- APNIC involvement

2

Background - spam

3

Quick quiz! :-)

- When you hear the word ‘spam’ which one of these would you be thinking of?
  a) A salty, pink meat that comes in a blue can?
  b) A British comedy troupe’s skit with singing Viking warriors?
  c) Annoying junk mail and other advertisements you never asked for that are sent to you via the internet?
  d) All of the above

4

Who is responsible for spam?

- Advertisers
  - Technical experts who do their own spamming
  - Businesses who hire a third party to do the spamming
- Spam service providers (most common)
  - Build up hardware, software & expertise need to send spam
  - Advertise their services to distributors
- Spam support services
  - ISPs/web hosting services that take any customer
    - no matter what kind of activity they are involved in

5

Statistics – how critical?

- Nearly 75% of email traffic is spam
  - Over 1 billion unsolicited messages sent per month
  - Amount is doubling every 5 months
- AOL & Hotmail block around 2 billion spam each day & still more slipping through
  - Now the figure is 10 times higher than that of 5 years ago

Source: http://www.postini.com/stats

6

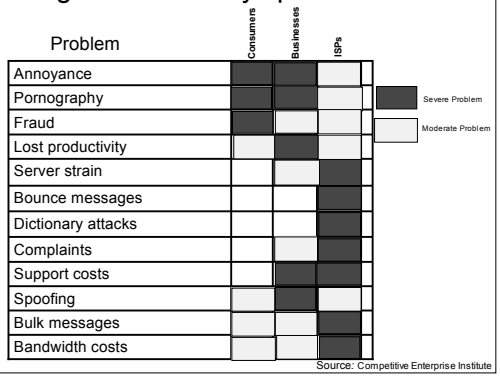
Statistics – how critical?

- Spam volume grows at 37% per month
  - an annual growth of 400%
- Lots of spam appears to use foreign relay
  - Countries may need to work on spam legislations
- Court cases between spammers & innocent victims
  - Only major corporations can afford such court cases

Source*: InformationWeek* Survey

7

Who gets affected by spam?



Source: Competitive Enterprise Institute

8

Problems & Prevention:
Consumers

9

Problems for consumers

- Privacy
- Concern about children receiving pornographic spam
- Mobile internet devices are getting popular
  - Charges based on contents or time to download
- How the attack works
  - Victims give away their own addresses

10

Email validation process

- Spammers are interested in only active accounts
  - Not only valid address but also active ones
- Once the spammer has a list of email addresses
  - it is easy to take out the invalid and inactive addresses
    - See whether any bounce backs

11

Email validation process

- Spammer can determine validity based on the response
  - Ex: “This account does not exist”, “Account could not be found” , “The recipients inbox is full” etc.
- Once the invalid addresses are deleted spammer use lower resources to send emails
  - Or even to sell the list

12

Email validation process

- By sending a series of messages, attackers can determine
  - What time of day the user reads email
  - How often the user checks mail
  - What email program user uses
  - What operating system is being used
  - Whether user uses HTML or plain text email
  - Whether user always use the same computer to check mail etc.

13

Prevention

- Use caution when choosing sites
- Avoid giveaways & other “too good to be true” sites
- Avoid signing up for sites that use an opt-out policy
- Read sign-up screens carefully
- Read privacy statement carefully

14

Prevention

- Know where your email can be found
- Guard your primary email address
- Never click reply to unknown senders
- Be careful with your browser
- Choose an ISP that actively blocks spam
- Find out how to filter your own email

15

Problems & Prevention:
Businesses

16

Problems for businesses

- Technical support costs
- Spoofing (use of legitimate name)
- Harvesting e-mail ids of staff
- Phishing attacks
- Sexual harassment
- Marketing difficulties

17

Web crawlers, robots

- Robots or spambots are used for email harvesting
- These tools work like browsers and catalog information found
  - Robot makes a request for a particular URL
- After the HTML page has been returned, the robot parses the HTML
  - Then locates all the links on the page
  - Loads each of these pages, and again continue parsing

18

Web crawlers, robots

- The robot also performs tasks with HTML on each page
  - eg: count pages for statistical analysis, index pages for search engines, mirror the content of web pages, etc.
- List of common robots
  - http://www.robotstxt.org/wc/active/html/index.html

19

Web crawlers, robots

- This technology can be used to find and extract email addresses
  - email addresses follow a particular pattern or regular expression (ex: "@" symbol)
- A robot can be configured to parse each page
  - look for email addresses
  - store them in a database

20

Email patterns

- It can be easy for a spammer to guess email patterns for most companies
  - eg: first initial and last name are used to form an email address
  - A simple run through the alphabet with common last names yields many valid hits
- Two guessing categories
  - Common email addresses or patterns
  - Blind guessing

21

User exposure

- Friends
  - Forwarding emails
  - New users who haven't faced bad experiences may be less cautious than more seasoned users
    - Parsing of lists
    - Address books
  - Help these users

22

Tracking emails to gather information

- Many scams and hoaxes
- HTML mail
  - Email messages can contain colours, fonts and embedded graphics
  - Image isn't actually sent but connects to the website when the email program loads
- Web bugs
  - Track the emails
  - How many times the mail program access the contents etc.

23

Hyperlinks

- Similar to web bugs
  - But require some interaction from users
- Instead of simply viewing or opening an email message, the user needs to click a link or button
  - So the spammer knows the email account is active
- As with web bugs, hyperlinks can be coded to indicate what user clicked the link
  - The user may also be asked to supply additional information

24

Vacation auto responders

- Spammer determines that the email address is active
  - More information can be retrieved (time of the email message read, IP address, email program etc)
  - Some times the vacation responses can provide more info for spammers

25

Vacation auto responders

I will be out of the office from August 15 through 28, attending a conference in Singapore. If you need to contact me, you can leave me a message at the Oasis, or you can send an email to my *abc* account at jbright_test@abc.com. I will be checking that account remotely throughout the conference.

If there is an emergency, please contact Cindy Jones at 617-234-1234 or at cindy_jones_test@mycompany.com.

Jeff

26

Vacation auto responders

I will be out of the office from August 15 through 28, attending a conference in Singapore. If you need to contact me, you can leave me a message at the Oasis, or you can send an email to my *abc* account at jbright_test@yahoo.com. I will be checking that account remotely throughout the conference.

If there is an emergency, please contact Cindy Jones at 617-234-1234 or at cindy_jones_test@mycompany.com.

Jeff

27

Spoofing email identities

•

```
Return-Path: <test-user@company.com>
Received: from [66.38.203.132] by e-hostzz.comIP with HTTP;
          Sun, : 31:55 +0400
From: "Tim" <test-user@company.com>
To: someuser@country.com
Subject: Re: CYXS, Contact !
Mime-Version: 1.0
X-mailer: mPOP Web-Mail 2.19
X-Originating-IP: [e-hostzz.comIP]
Date : Sun, 16 Jun 2006 11:37:55 -0700
Reply-To: "Tim Wright" <test-user@company.com>
```

28

Phishing

- Starts as an email message to get users to go to a web site
  - To enter personal details for use in an identity scam
- Web site looks similar to the real site

29

Using email addresses for other purposes

- Web applications routinely store email address as data and as user ID
  - Any vulnerability in a web application's security can reveal this sensitive information
  - Need to use unique IDs

30

Error message reasoning

- Error messages from web applications can expose email addresses
  - Login pages, forgotten password, registration are focus points for these type of attacks
  - The attacker can keep trying email IDs until the error message gives a clue

31

SQL injection

- Ex: web site that displays job listings can have a link such as
  - **http://www.mycompany.com/Jobs.asp?id=6236**
- A hacker can add a single quote or an apostrophe (') to the end of the URL and the following error message appears

Microsoft OLE DB Provider for SQL Server error '80040el4' Unclosed quotation mark before the character string ' AND published=1'.
/Jobs.asp , line 20

- The hacker now knows the page is vulnerable to SQL injection and can determine the DB schema

32

Prevention

- Robot exclusion standards
  - Tags direct a robot to ignore the document and not follow any hyperlinks contained on the page
    - <META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">
- Confuse the robots
  - Obfuscate
    - Allow email address to appear in web page but make it difficult for spambots to retrieve
  - html tagging
    - Encoding the address in such a way that it no longer matches the email pattern
      - **jbright@test.com**
  - email ids as images

33

Prevention

- Spam poison (sending fake email ids)
  - Doesn't prevent email addresses from being harvested but attempt to taint the results
- Choose hard to guess email addresses that doesn't follow a standard pattern
- Organizational policies that set standards for creating email addresses
  - Standards can also aid an spammer who is focusing on your company
  - Don't let the spammers make educated and higher probability guess

34

Prevention

- Maintain the privacy
  - Secondary addresses
  - Not to forward hoax messages
    - http://hoaxbusters.ciac.org
  - BCC fields
- Text mails over HTML
  - Tracking systems are ineffective
  - Speed up your email access

35

Prevention

- Be careful when using vacation auto responders
  - Restrict auto responder to certain people or those that matches particular rules
- Check for spoofing: IP lookups to verify the hostname
  - If the machine name on a received line doesn't match the IP address:
    - It is likely to be a forgery
    - All lines that follow should not be trusted
    - Do an IP lookup in whois

36

Prevention

- Web application security
  - Fix the web applications
  - Applications need to return general errors
  - Ensure that the site can't be used to mine email addresses from the database
  - Every input value to the application needs to be carefully checked and validated
- Filters and spam reporting
- Challenge responses
  - Server holds all email from unrecognized addresses and sends an automated message

37

Problems & Prevention: ISPs

38

Problems: Costs

- Sending or receiving massive amounts of email in a short period of time
  - uses large bandwidth and storage space
- Upsets the customers
  - Adds to technical support costs
- ISPs must build enormous overcapacity into their systems
  - Excessive email traffic can crash the systems
- Rising costs of spam can shut down the business

39

Problems: Costs

- Bounce messages
  - Spammers usually put a fake email address in the Reply-To header to avoid bounces
  - Another ISP or user ends up getting thousands of bounce messages, clogging the servers

40

Problems: Costs

- Dictionary attacks
  - Try multiple combinations of letters, at a popular domain name
    - This puts a huge drain on ISP's servers
- Customer complaints
  - Consumes a lot of helpdesk and customer service time
  - Large amounts of objectionable email can drive customers away

41

SMTP

- SMTP is simple
  - No mechanism to verify the sending server or the accuracy of the from address
  - SMTP server has no way to verify messages such as "This message is from your bank and concerns your account" etc.
- But SMTP is reliable and pretty much universally implemented

42

Prevention

- Contractual and cooperative solutions
  - Acceptable Use Policy (AUP)
    - Spammers try to operate through open relays or by hijacking ISPs other than their own
    - ISPs need to have strong anti-spam policies
    - Prohibit these customers from sending spam through ISP servers

43

Prevention

- Contractual and cooperative solutions contd.
  - Pay-to-send and pay-to-transmit models
    - Charge customers to send bulk email
      - Internet community view
      - Spammers still bypass their ISP servers
        - » Install their own SMTP servers and use open relays in foreign countries
        - » Hijack open proxies run by users with home networks

44

Prevention

- Contractual and cooperative solutions contd
  - E-stamps
    - Sender agree to pay money per message if the message is reported as spam
  - Bonded Sender Programs (BSP)
    - Sender deposits a sum of money with a bonding company per mailing
      - Noted in the headers of the emails to ensure that they are not blocked by ISPs
      - If a recipient decides that the message is spam
        - » It can be reported through a spam program
        - » Recipient's ISP collects the money

45

Prevention

- Software solutions
  - Software can partially stop the spam problem at several levels
    - Efficient tools for end users to control spam
    - Blocking techniques for ISPs
    - Sender authentication programs

46

Prevention

- Whitelists
  - Lists of servers known to be sending valid, legitimate emails
  - The address of the sending server can be compared to a whitelist
- Blacklist filtering
  - Opposite of whitelists; lists of servers known to be operated by spammers
  - Block all incoming mail from the blacklisted addresses
    - Many blacklists block all IP addresses from specific countries

47

Prevention

- Multiparty solutions
  - Need collaboration between ISPs, bulk mailers, and consumers
    - Options of redesigning the SMTP
      - Probably based on security certificates
      - Should be a secure, verified protocol like HTTPS

48

Prevention

- Force accountability by identifying who is sending the message (e.g. spam, phishing & viruses)
  - Email authentication systems
    - SPF (Sender Policy Framework or Sender Permitted From)
    - Caller ID
    - Sender ID

49

Prevention

- SPF (Sender Policy Framework for email address spoofing)
  - Patch the security weakness of SMTP
  - Modify DNS to declare which servers can send mail from a particular Internet domain
- Once widely deployed, SPF records could be consulted by Mail Transfer Agents
  - They can check records for particular domains
    - Determine an email message's source is legitimate or spoofed

50

Prevention

- SPF only checks for spoofing at the message transport level
  - Verifying the "bounce back" address for an email, which is sent before the body of a message is received
  - Tells the receiving email server where to send rejection notices
- SPF itself will not stop spam
  - It will help other anti-spam technologies
    - Enabling ISPs to track spam back to specific domains and forcing spammers to move to new domains more frequently

51

Prevention

- Caller ID
  - Use sender authentication technology
    - Tries to validate source address associated with an email message
  - Asks email senders to publish the IP address of their outgoing email servers
    - Part of an XML format email "policy" in the DNS record for their domain

52

Prevention

- Caller ID contd.
  - Email servers & clients that receive messages check the DNS record
  - Match the “From" address in the message header to the published address of the approved sending servers
  - Email messages that don't match the source address can be discarded

53

Prevention

- SPF and Caller ID (merged)
  - Possible to check for spoofing at the message body as well
  - With the merger, companies can use the SPF to reject spam messages before they are sent
    - if spoofing is detected at the message envelope
  - For messages that require a deeper inspection, the Caller ID method can be used

54

Prevention

- Domain keys
  - Uses public key encryption technology at the domain level
    - To verify an email message's sender
  - Uses a set of private and public encryption keys to validate the IP address (or domain) of the sender
  - Verify that the message's contents haven't been altered
  - ISPs can allow authenticated email messages to bypass spam filters
    - Free the resources to interrogate unauthenticated messages

55

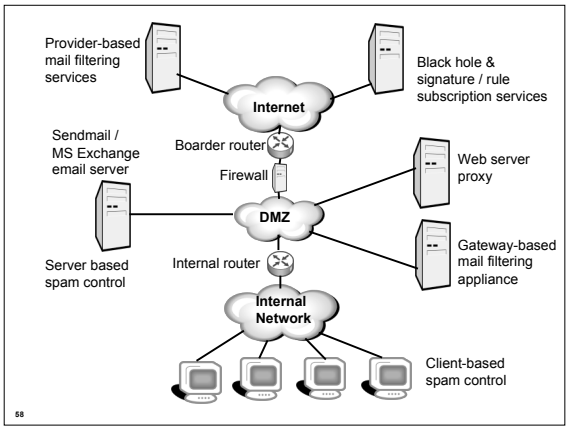
Prevention

- Legal solutions
  - Legislation that targets fraudulent or destructive conduct
  - Forged headers can be made illegal
  - Illegal to send emails with falsified routing information
  - Labeling (ex: [ADV:] or [ADV:ADLT])
  - Mandatory unsubscribe or opt-out (options to reject emails) requirements
  - Restrictions on email harvesting
  - Opt-in (options to receive email)

56

Spam filtering & anti-spam services

57



Mailbox filtering in email programs

- Use mail folders
  - Spam can go into the trash folder
- Create filters which tell the email program to sort incoming messages into the folders
  - Most email programs include filters

59

Using filters

- Create a filter telling the email program
  - Which message to move
    - To address, From address, Subject line, or the body of the message
  - Where to move the message
    - Specify the name of the mail folder to move the message to
- Good to create multiple filters as there are different kinds of spam

60

Spammer's tricks to evade filters

- Capitalisation
  - eg: filter may look for spammersrus.com but spammers can use SpammersRus.com
- No text
  - Many spam messages contain only graphical image of text
- Wrods Speled w.r.o.n.g
- Hidden bogus codes
  - Ex: instead of make money it says ma<m>ke mon<n>ey
  - Filter can get confused with the HTML tags

61

Server-side spam filtering

- If you run a mail server, recommend running spam filtering software for users
- Server filters can do a better job than user filters
  - Server has access to the entire stream of incoming mail
- Spam and virus filtering can be done at the same time

62

Server-side spam filtering

- Users don't have to download the spam
  - Filters can reject mail or divert to separate mail box in the server
- Users don't need to install their own filtering software
- No need to try to support different random filtering programs that users download from the web

63

Server-side filtering techniques

- DNSBL filtering
  - Most filters let you set IP address ranges or domains to blacklist or whitelist directly
  - Using shared blacklists and whitelists distributed via DNS is common

64

Server-side filtering techniques : Bulk counting

- One of the most effective approaches
  - These filters look at incoming mail to try to recognize when many similar messages are arriving
- Each time a message arrives, the filter makes a *hash* (compressed) code representing the contents of the message
- Looks in the database to see how many other messages arrived recently with the same hash code
- If it's several, the message is probably a spam

65

Server-side filtering techniques: Bulk counting

- Spammers tend to change their messages to avoid bulk counting filters
- Effective bulk counting filters should have "fuzzy" hash codes
  - Designed to disregard minor differences between one copy of the message and another
- Any bulk counting system needs to be configured to whitelists

66

Server-side filtering techniques: Bulk counting

- Bulk counting doesn't need to be restricted to a single mail server
  - Can exchange hash code information among many servers
- Distributed Checksum Clearinghouses
  - www.dcc-servers.net
  - Networks that handle small amounts of mail (fewer than about 50K messages a day) can use public DCC servers
  - Larger mail users should arrange to run their own DCC server

67

Server-side filtering techniques: Timing and greylists

- Timing techniques and greylists
  - Filters can often detect spam by looking at peculiarities of the rate at which it arrives
- Body filters
  - These filters look at the contents of spam
  - As the server filter can see all incoming mail, Bayesian and other adaptive techniques can use a larger sample base

68

Server-side filtering techniques: Timing and greylists

- Most spam is sent by *spamware*
- As there are no error checkings, viruses and worms can get away
- These spamware and viruses can be detected by looking for timing peculiarities caused by the lack of error checking

69

Server-side filtering techniques: Timing and greylists

- During mail exchange, the sequence of commands & status messages are predictable for successful message delivery
  - Spamware sends all the commands without waiting for replies
- Server can check to see whether the sending machine is getting ahead of the replies
  - Conclude that the mail is coming from spamware or a virus than a real mail client

70

Server-side filtering techniques: Timing and greylists

- A mail server can be short of disk space or other problem that temporarily keep it from receiving mail
  - It returns temporary error status codes
    - Real mail programs retry the message
    - But spamware and viruses don't bother

71

Server-side filtering techniques: Timing and greylists

- With greylisting when a server sees an incoming message from an unknown server:
  - The server returns a temporary rejection message and keep track of the IP addresses
- If the sender retries the same message reasonably soon (by the same IP)
  - Server accepts the future mail from that IP without delays
  - If not continue to send temporary rejections to mail from that IP

72

Server-side filtering techniques: Timing and greylists

- This process might create delays
  - Rejects nearly all mail sent by spamware
- Both these timing and greylists have to be implemented in mail server software
  - Only the server knows the timing of incoming mail

73

Server-side filtering techniques: Combination filtering

- Sequentially filtering
  - Apply multiple tests sequentially
  - Do the IP tests first as the remote host connects
    - Then the bulk tests
    - And the body tests
  - If any of the tests identify a message as spam, the filter stops and doesn't do any more testing on that message

74

Server-side filtering techniques : Combination filtering

- Scoring filters
  - Run all their tests, assign a weight to each test and add the weights of the tests that the message passed
  - If the score is above a threshold level, the message is considered to be spam
- Sequential filters can be much faster because they often don't need to run the full set of tests
  - But harder to tune than scoring filters

75

Filtering on UNIX/LINUX servers

- Most of the email software and filtering add-ons for UNIX are open source or freeware
- Most widely used UNIX mail server is sendmail
  - Provisions to plug in many mail filters with direct support for DNSBLs and a *milter* (mail filter)
- Other popular mail servers (Exim, postfix, qmail etc) also supports DNSBLs

76

Filtering on UNIX/LINUX servers

- UNIX/Linux mail servers also use procmail filtering package
  - Procmail has its own pattern matching language
- Most popular UNIX/Linux filter is SpamAssassin
  - www.spamassassin.org
  - Can use DNSBLs, DCC etc along with fixed, heuristic, and Bayesian filters

77

Anti-spam programs

- Most of the email programs may not have truly effective spam filters
- Install extra spam-filtering software & signing up for spam filtering service
  - These programs act as proxy servers
  - Extra step but lots of spam can disappear along the way

78

Anti-spam services

- Spam filtering is a complex and CPU-intensive application
- Better to dedicate a separate server
- Many vendors offer anti-spam devices
  - Already configured with anti-spam software that logically sits between the Internet and the existing mail server
- Network mail configuration is adjusted
  - Incoming mail goes to the appliance which examines the mails
  - Then re-emails the filtered mail to the existing mail server

79

Checklist for server spam filters

- Regular updates to handle improvements in spam recognition & latest spammer tricks
- Multiple filtering techniques
  - Fixed body filters, adaptive (Bayesian) body filters, bulk counting and greylists etc. etc.
- System-wide and per-user configuration to deal with individual preferences, false positives and new spam variants

80

Handling spam

81

Email headers

```
Return-Path: hptimeline@yahoo.com
Received: from ns.isoutsider.com (unknown
[210.109.171.2]) by receiving.my-isp.com
(8.9.3/8.9.3) with ESMTP id FSW930923; Sun, 31 Aug
2003 22:59:28 -700 (PDT)
Received: from adventures (CPE –
65-31-127-1.wi.rr.com [65.31.127.1]) by
ns.ioutsider.com (8.11.6/8.11.6) with ESMTP id
h7JFLKK09863; Sun, 31 Aug 2003 22:56:22 +0900
Message – Id:
200308191.h7JK09867@ns.isoutsider.com
Received: from billclinton.whitehouse.gov
([184.325.23.124]) by mailout.yahoo.com (Postfix)
With SMTP id 7600A32641; Sun, 31 Aug 2003 11:40:44
-0700 (PDT)
From: hptimeline@yahoo.com
To: <undisclosed.Recipients>
Subject: Look Great for the Spring with Discounts
on HGH (human Growth hormone)!!!!
Date: Sat, 30 Aug 2003 02:10:21 -0800
MIME-Version: 1.0
Reply-To: hptimeline@yahoo.com
Errors-To: pow@163.com
```

82

Following the flow of email headers

- Every time an email message passes through a mail server, that system adds a received line
- Most recent one should be the one that says who delivered to your ISP

```
Received: from ns.isoutsider.com (unknown
[210.109.171.2]) by receiving.my-isp.com
(8.9.3/8.9.3) with ESMTP id FSW930923; Sun, 31 Aug
2003 22:59:28 -700 (PDT)
```

83

Following the flow of email headers

- As you are sure that your ISP may not be sending you spam, you can look for ns.isoutsider.com

-

```
Received: from adventures (CPE –
65-31-127-1.wi.rr.com [65.31.127.1]) by
ns.ioutsider.com (8.11.6/8.11.6) with ESMTP id
h7JFLKK09863; Sun, 31 Aug 2003 22:56:22 +0900
```

84

Following the flow of email headers

```
Received: from billclinton.whitehouse.gov
([184.325.23.124]) by mailout.yahoo.com (Postfix)
With SMTP id 7600A32641; Sun, 31 Aug 2003 11:40:44
-0700 (PDT)
```

- Suspicions about the legitimacy of this Received line
- Seems you have reached a deadend
  - Leaves with adventures or CPE-65-31-127-1.wi.rr.com as the end of the trail

85

Looking at the last verifiable mail handling server

- Use a tool which enables you to find out whether these computer names and IP addresses match each other
  - Forward and reverse lookups

```
Ns.isoutsider.com resolves to 210.109.171.2
CPE-65-31-127-1.wi.rr.com resolves to 65.31.127.1
Error – billclinton.whitehouse.gove doesn't exist
```

86

Investigating contents of spam

- Example

```
Wholesale Prescription Medications
DISCREET OVERNIGHT PHARMACY !

Now get HGH, Vicodin, Sex Organ Enhancements,
Prozac, Viagr@, BustPro, Zoloft, Propecia. And
many, many more!
Just e-mail doctorfeelgood328@yahoo.com, or visit
our website at http://1024349897/HGH_13/specialoffer.html
```

- Web page address looks a bit strange
  - 1024349897 translates into 61.14.86.201
    - URL tool www.samspade.org/t
  - Translates to c201.h061014086.is.net.tw

87

Address the complaints

- Most of the ISPs have their terms of service on their websites
  - Prohibits any form of spam-related activity
  - Provide an address for filing the complaints
  - Most commonly abuse@followed by the domain name

88

Sending complaints

- Nicely :-)
  - Don't transfer your anger at spammer to the ISP
  - Spamming isn't really ISP's fault

Dear Administrator,

I received a piece of spam that I have attached below.
The headers appear to have originated at RoadRunner
and been relayed via ns.isoutsider.com, and it advertises
both a mailbox at Yahoo.com and a webpage at is.net.tw.
Please take appropriate action to stop this spammer.

Thanks!

89

Sending complaints

- Make sure you attach a complete copy of the spam
  - Including all headers
  - Turn off any HTML or RTF formatting
    - Bold, colored stuff, embedded pictures etc
  - Send the message in plain text
- Some ISPs send acknowledgements but some do not
  - Most departments handling abuse are overworked and understaffed
  - Let them kill a few more spammers instead of responding to you :-)

90

Sending complaints

- Sometimes the complaints can bounce back as undeliverable
- Try some whois inquiries
  - You can find more addresses to send the complaints
- Use traceroute
  - Find out where the spammer is getting the internet connection
- Sometimes the ISP doesn't care much about the problems caused by spammers
  - However the upstream ISPs may be able to help you

91

Sending complaints

- Sometimes the results of traceroute can go cold after a private IP address
- So find the upstreams using whois
- Don't complain to IANA :-)
- If everything fails:
  - send documentation of your efforts to your ISP and ask it to block the spamming sites at their routers
    - If ISP is not responsive, it's time to look for an ISP who offers better services

92

Fighting spam with spam

- Not a good idea
- One of the common tricks of the spammer is to relay their messages via an innocent third party mail server
  - So don't flood the innocent site with your complaints
- A common trick is to forge mail headers
  - Looks like the mail originated elsewhere
- So if ISP claims innocence don't fight back!
  - They may really be innocent

93

If blacklisted – What ISPs should do?

- Contact the blacklist directly
- Need to requests the blacklists to quickly de-list you
  - Submit a request to retest your "repaired" mail server
  - Propagation time after you are de-listed (may be ~ a week or so)
  - Destination mail server administrators pull the updated lists at times they prefer
- After that
  - Update your anti-virus software
  - Make sure your network is secured
- Don't send any more spam from your network

94

Spam laws

95

Characteristics of spam

- Solicited or unsolicited
  - Was the message sent to someone who specifically asked to receive it?
- Permission and relationship
  - Did the recipient of the email address give permission, either expressed or in some sort of implied fashion?
- Commercial or noncommercial
  - Does the email message advertise the commercial availability of a product or service offered for sale or lease? etc

96

Characteristics of spam

- Bulk or not bulk
  - Was the email sent in bulk to hundreds or thousands or millions of recipients?
- Email or something else?
  - Is the message coming via email or popup window etc?
- Forged headers
  - Does the email message contain any forged information such as a false From address or non-existent Reply-To address

97

Characteristics of spam

- Misleading subject lines
  - Does the email message try to mislead the recipient?
- Fraudulent content
  - Is the email message advertising an illegal get-rich scheme or a bogus work from home? etc
- Bogus opt-out
  - Does the message offer to remove you from its mailing list, but when you click the link the removal web page doesn't exist?

98

Spam laws

- Opt-in or opt-out options
  - Commercial emails to contain some type of instructions telling recipients how to get off future mailings by that company
- ADV or ADLT labels
  - Commercial email to be labeled with some variation of the letters ADV or ADLT

99

Spam laws

- Contact info
  - email to contain the company's name and a physical address or other contact information
- No using third party's domain name
  - Using anybody else's domain name to send spam without their permission

100

Spam laws - a comparison

101

Australian Spam Act

• The Spam Act refers to spam as "unsolicited commercial electronic messaging".

•The Spam Act mandates that such messages must not be sent

102

Messages covered by the Act

The Spam Act covers commercial electronic messages that are sent by applications such as:

- Email
- Short message service (SMS)
- Multimedia messages service (MMS)
- Instant messaging (iM)

103

What is considered as spam?

- Electronic messaging (emails, SMS, etc.)
- Commercial in nature
- Unsolicited – sent without prior consent
- The Spam Act makes no reference to bulk messaging
  - A single unsolicited commercial electronic message could be a spam

104

The penalties

- A business found to be in breach of the Spam Act may be subjected to a penalty of up to AU$220,000 for a single day's contraventions
- Repeated breaches may result in penalty of up to AU$1.1 million

105

3 steps to ensure compliance

Step 1 - Consent

Your commercial messages should only be sent when you have consent

üexpress consent üinfer consent

Step 2 - Identify

Your commercial messages should always contain clear and accurate sender identification and how they can be contacted

Step 3 - Unsubscribe

I5 working days

Your commercial messages should contain an unsubscribe facility, allowing recipient to opt-out from receiving future messages

106

Coverage of Australia's Spam Act

- The provisions of the Spam Act cover commercial electronic messages:
  - Originating in Australia that are sent to any destination
  - Originating overseas that are sent to an address accessed in Australia

107

International laws

- Enforcement of penalties relating to spam coming from overseas can be problematic until international arrangements are in place
- Often these laws vary subtly from country to country

108

APNIC's involvement

109

Detecting the spam/abuse

- Software to detect network abuse
  - Mostly designed to search the ARIN Whois database
  - May refer to APNIC
- Many websites with whois lookup functions has the same limitations
- However the IP addresses are registered by five RIRs on a regional basis

110

Detecting the spam/abuse

- If a standard search refers you to APNIC
  - Means only that the network in question is registered in the AP region
  - Does not mean that APNIC is responsible or that the hacker/spammer is using APNIC network

111

Investigation of complaints

- APNIC is not able to investigate these complaints
- Can use the APNIC Whois database to find out where to take your complaint
- APNIC does not regulate the conduct of Internet activity (legally or in practice)

112

Investigation of complaints

- Laws relating to network abuse vary from country to country
- Investigation possibilities
  - Cooperation of the network administrators
  - law enforcement agencies
    - Local jurisdiction
    - Jurisdiction where the problem originates

113

How can APNIC help you?

- The APNIC Whois Database
  - Holds IP address records within the AP region
  - Can use this database to track down the source of the network abuse
  - Can find contact details of the relevant network administrators
    - Not the individual users
    - Use administrators log files to contact the individual involved

114

How can APNIC help you?

- Education of network operators in the Asia Pacific community
  - Address policies and the importance of registration of resources
- Community discussions can be raised in the APNIC open policy meetings, mailing lists, etc.
- Spam BOFs

115

Summary

- Background: spam
- Problems & prevention
  - Consumers, Businesses, ISPs
- Spam filtering and anti spam techniques
- Handling spam
- Spam Laws
- APNIC involvement

116

Questions?

117