Controlling spam

Devdas Bhagat
devdas.b@gmail.com

SANOG

Defining spam

Unsolicited
Bulk
Email

Devdas Bhagat
devdas.b@gmail.com

The main problem?

Spam is a **social** problem, not a technical one. Using technology to stop spam is using the wrong tool for the job.

Devdas Bhagat
devdas.b@gmail.com

Inbound spam

Devdas Bhagat
devdas.b@gmail.com

SANOG

HOWTO

- Defense in depth
  - At the border router
  - At the MX
  - At point of delivery
  - At the customer MUA

Devdas Bhagat
devdas.b@gmail.com

At the border router

- ACL off IP space involved in ROKSO listings.
  - CAVEAT: You have to maintain this yourself.

Devdas Bhagat
devdas.b@gmail.com

At the MX

- Accept mail only for valid recipients
- Use DNSBLs.
  - I recommend using zen.spamhaus.org
  - Check what the listing policy of the DNSBL is and whether it agrees with your policy.
  - DNSBLs have been known to shut down. Check your DNSBL rules.
- Use local sender/IP blocking rules.

Devdas Bhagat
devdas.b@gmail.com

At point of delivery

- Spamassassin or other content filtering system
  - Especially a well trained Bayesian system
- Antivirus (ClamAV has been known to work well).

At the customer's MUA

- Thunderbird and Outlook have reasonable spam detection. So do other MUAs.
- Help your customers learn to use the tools on their desktop.

Devdas Bhagat
devdas.b@gmail.com

Outbound spam

Devdas Bhagat
devdas.b@gmail.com

SANOG

Benefits

- Reputation
- Save helpdesk costs on debugging customer message delivery issues.
- Happier customers AND peers.

Devdas Bhagat
devdas.b@gmail.com

Active approach

- Block port 25 outbound at the border router or firewall for all dynamic IP blocks
- Require all mail to go via your mail servers
  - Use SMTP AUTH.
  - Use DKIM
- Scan outbound mail for spam signs and viruses
- Rate limit your customers when sending email

Devdas Bhagat
devdas.b@gmail.com

Passive approach

- Run a well supported abuse desk
  - This needs serious management support.
  - The abuse desk needs to be able to suspend customer accounts directly.
  - The abuse desk must respond quickly. As in, a matter of minutes.
- Subscribe to Feed Back Loops run by various ISPs.

Devdas Bhagat
devdas.b@gmail.com

Further reading

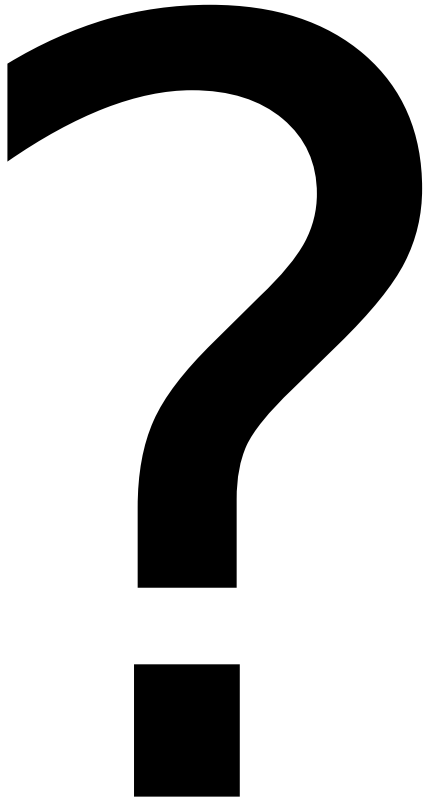
Policy help:
http://www.maawg.org/published-documents
http://blogs.msdn.com/b/tzink/

FBLs:
http://wiki.wordtothewise.com/ISP_Summary_Information

Technology:
http://spamassassin.apache.org/
http://www.ijs.si/software/amavisd/
http://www.clamav.net/lang/en/
http://www.dkim.org/

Lists:
http://spam-l.com/mailman/listinfo/spam-l

Devdas Bhagat
devdas.b@gmail.com



Devdas Bhagat
devdas.b@gmail.com

SANOG