Email Marketing vs. SPAM

ANACOM 2009
Workshop CNSA-LAP
“SPAM fighting”

Ricardo Oliveira

Out/2009

ANACOM

eurotux

Eurotux, SA

Remote managed services, professional hosting services, edge security technologies, email security solution.

Managing a free webmail service (400k mailboxes) since 2003, several thousand mailboxes worldwide.

Protect customer's infra-structures with ETMX - an email security service (filtering in-the-cloud).

SPAM

- “Online statistics estimate that about 94% of all email sent, is spam. The only way we can ever really stop this trend is to do everything we can to block it, ignore it, or stop clicking the darn things.”
  www.hardathosting.com, 2009
- “More than half of all spam either uses either uses domain names registered in China, is sent from computers in China, or uses computers in China to host their web pages.” www.thewhir.com, June 2009

Hosting companies perspective

Email marketing hosting draws an interesting return to hosting companies:

- increasing bandwidth needs;
- server and storage requirements (reports; opt-in/out mechanisms);
- possibility of additional services;
- service draws immediate return to the customer;

Hosting companies perspective

SPAM solutions hosting ***also*** draws an interesting return to hosting companies:

- huge and increasing bandwidth needs;
- distributed server needs;
- return to customer;
- additional services are ***mandatory***: manage complaints; blackholes from neighbour ISPs; blacklisting; etc
- deal with reputation issues;
- no control over customer's internet access;

Hosting companies perspective

Spam filtering (in-the-cloud) is ***yet another*** service which makes hosting companies happy:

- immediate customer satisfaction and growing customer base;
- primary concern: protect customer from SPAM sources;
- deal with SPAM attacks and address complaint requests from customers;
- day-to-day management is hard: create / update heuristic rules, static block known SPAM sources; unblock inactive sources;

Three sides of the same coin...

One can't promote and protect at the same time (at least, efficiently)!

- promote the migration of legacy / spam-alike solutions to modern, opt-in / opt-out technologies;
- police suspicious behaviours (network health);
- classify known sources of email-marketing, and create custom rules to influence the message analysis process in the filtering tier;
- create local spamtraps / honeypots;

Three sides of the same coin...

...

- promote services to help customers protect from typical SPAM attacks (form abuse, email server misconfiguration, email harvesting, etc);
- investigate foreign complaints as if they were your own;
- publicly publish known spammers;
- ensure AUP violations result in breach of contract;

Questions?

Thank you for listening!