



E-mail Whitelists

Andrew Cormack
Chief Regulatory Adviser, UKERNA
A.Cormack@ukerna.ac.uk



How to do Spam Filtering

- Recipient site can rate messages based on
 - Characteristics of individual message (default “score”)
 - Bad words, bad headers, hyperlinks, etc., etc.
 - List of domains to treat less favourably, because historically
 - High proportion of spam, low proportion of important messages
 - Don’t respond to complaints⇒ **Blacklists** (e.g. MAPS)
 - List of domains to treat more favourably, because historically
 - High proportion of important (to me) messages
 - Do respond to complaints⇒ **Whitelists** (e.g. perhaps, domains on my and other NRENS?)
- Can use these exclusively, or (better) combine scores
- Aim: increase ratio of (important messages):(spam)



About Whitelists

- Need some policy for who is on it
 - Informal policy
 - Friends, partners, ‘big ISPs’, etc.
 - You choose who to list
 - List only useful to those who agree with you
 - Formal policy
 - Define rules for whitelisted sites/domains
 - They ask to be on it, you check they satisfy rules
 - List useful to anyone who finds rules valuable



Formal Policy Example

(discussed extensively on e-COAT tools list)

Applicant for whitelist agrees to

- Provide up-to-date details for reporting e-mail abuse
- Respond promptly and effectively to reports
- Provide up-to-date list of mailhubs covered by agreement
- Ensure those mailhubs implement good practice
 - Consistent forward/reverse DNS records
 - Timestamps from an authoritative standard source
 - Provide accurate submitter details in “Received” headers
 - Do not generate delivery failures for detected spam/virus
 - Confirm requests to subscribe external addresses to mail lists



Use of Whitelist

- Recipients volunteer to use Whitelist
 - Configure lookups into your MX
 - If rules give you greater comfort ⁽¹⁾
- Senders volunteer to join Whitelist
 - If you can satisfy the rules ⁽²⁾
 - Not on Whitelist => 'default' treatment
- Do the proposed Rules satisfy (1) & (2)?



Policy Enforcement

- Abuse/IR Team provides oversight
 - Of reports
 - Receives and forwards reports
 - Tracks them till problem resolved
 - Of Whitelist membership
 - Adds domains that sign up to the Policy
 - Removes domains who fail to abide by Policy
 - Maybe temporarily, till they prove they've fixed problem
- Whitelists change slower than blacklists



Exchanging Whitelists

- If two Whitelists implement same Policy
 - Could treat them as equivalent
 - Exchange Whitelists between ISPs/NRENs?
 - Batch transfer probably best
 - Out-of-dateness a minor issue for Whitelists
- Need a central authority (?TERENA)
 - To manage Policy
 - To maintain list of compliant Whitelists
 - Server details and preferred transfer method
- Note that servers may be attacked by spammers



Technical issues

- Publishing whitelists
 - (could follow blacklists), and use
 - Interactive DNS query, and/or
 - Batch DNS Zone transfer, and/or
 - Other (secure) network synchronisation
- Using whitelists
 - Support in MX software is variable
- Exchanging whitelists
 - Batch methods probably adequate
 - Bi-lateral exchange avoids single point of failure