AfriNIC 11

November 2009

Mail Abuse

S. Moonesamy

Eland Systems

sm+afrinic@elandsys.com

How do we stop spam

- No instant solution
- Social problem

How we read an email message depends on the context

- If I send an email to all the people attending this meeting, is it spam?
- If If I send a personal email to each of you, is it spam?
- If a person I do not know read these slides on a web site and sends me an invitation to join a social network, is it spam?

Senders

- Is your network sending out spam?
- Can you identify the computer sending out spam?

What makes a good sender

- Accurate information in WHOIS to identify the point of contact
- Accurate information in AfriNIC Whois database if the IP address block has been delegated to your organisation
- Forward and reverse DNS match
- Correct hostname (FQDN) for the SMTP EHLO

What makes a good sender

- Respond to abuse complaints
- My email is important. Why do you block me?
- Opt-In v/s Opt-Out

Receivers

- Spam
- Backscatter
- Too many SMTP connections

Mail abuse

- Unsolicited commercial mail (UCE)
- Malware
- Phishing

Antispam Techniques

- DNS Blacklist (DNSBL)
- Reverse DNS checks
- Greylisting
- RFC compliance
- Content filtering
- Callback verification
- Challenge/response systems

Thank you