

# Stakeholder Best Practices

What best practices should stakeholders adopt to reduce malicious spam and minimize its impact?

**Mike O'Reirdan**

**Distinguished Engineer**

**National Engineering and Technical Operations**

**7/12/2007**



**Comcast.**

# Agenda

---

- **What we're doing now**
- **What we're doing next**
- **What needs to be done in the future**
- **We need to harden networks... and PCs... some ideas**
- **Pushing the envelope: more approaches to consider**

# What Comcast does now: focus on technology

---

- **Inbound email traffic management**
  - Active control of inbound connections
  - Management of simultaneous connections
- **Reputation**
  - Use of multiple reputation services.
  - Suppression of bad IPs based on observed behaviors and customer and 3<sup>rd</sup> party ISP complaints.
- **Content and virus filtering**
- **Users**
  - Targeted Port 25 blocking
    - Management of Port 25 is currently key to suppressing outbound spam following industry best practices
    - Apply boot files, very little customer complaint, not noticed as majority of users using webmail
    - Redirect POP users to port 587. Ensures authenticated users
  - McAfee Security Products
  - Anti-phishing protection via Comcast toolbar
  - Comcast Security Channel
    - Extensive Customer Security education
- **Bot / Botnets**
  - Measurement
  - Detection
  - Suppression

# What Comcast plans to do next

---

- **Introduce authentication by EOY 2007**
  - DKIM
  - SPF
- **New anti-abuse technology**
  - Based on advanced signature detection capabilities
  - Users engaged in the anti-spam process
    - Able to report false positive and negative messages
- **Advanced outbound spam mitigation techniques**

# What needs to be done in the future

---

- **Need to move from reactive approach to a proactive approach**
- **Network and PC hygiene is key. It is a collaborative process with input from all industry partners**
- **Without breeding grounds, viruses / bots cannot flourish**
- **No matter how hardened the network is, the PC is often the weakest link. We can only educate users, not control them.**
- **We protect the power grid, it is something we all rely on – for the same reason, we must do more to keep “malicious devices” from connecting to the Internet.**

# Addressing the “PC portion” of the problem

---

- **Further emphasis on the unbreakable PC**
- **Work with industry partners – PCs are sold as “easy to use,” they must be “safe to use” as well**
- **Need to be able clean a PC totally and reliably. At present, impossible to clean a PC without “nuking” it – customers will lose data.**
- **Need PC vendors to make it possible to keep data safe.**

# Other possible approaches

---

- **Trusted mail network**
  - Trusted mail transit network between trusted ISPs
    - Mail to have passed through ISP MTAs, passed through anti-abuse platform
    - Membership earned by cleanliness of mail
  - Highly trusted connections
  - Much more aggressive filtering on inbound mail from country domains known to be badly managed, which reinforces efforts of government and law enforcement to bring pressure to bear on those countries to shut down spammers operating there
- **Real time abuse data sharing between major ISPs**
  - Very rapid identification of spam sources
  - More rapid take down of phishing sites
  - Share honeypot data
- **Working with Domain Registrars to control spammers' access to domains**
- **Better education on cyber issues for the legal profession. Still seen as a maze for them to navigate:**

**In May, the magistrate overseeing the trial, Justice Peter Openshaw, interrupted the proceedings with a statement that observers said stunned prosecutors for the Crown. "The trouble is I don't understand the language. I don't really understand what a Web site is."**