

Collateral SPAM

Dr Henry O'Keefe
Computer Centre
U.C.C.

What is it?

- E-mail has a forged “from:” field with an address in your domain.
- Your institution is usually not the direct/intended recipient of the original SPAM.
 - The recipients and real senders are often in a different country or continent to you!

What can the consequences be?

- Denial-of-service
 - Individual
 - Organisation-wide.
- Large volumes of “SPAM” complaints.
- E-mail blocking of your institution’s name by naïve system administrators
 - Most blacklist providers are smart enough not to be fooled.
- Loss of “good name”.

How can DOS occur?

- SPAMs of this type can have LARGE numbers of e-mails – much larger than your system may be designed to handle.
- Many of the e-mails sent may generate e-mails to your site
 - Delivery failures
 - Deliver notifications
 - Virus warnings
- E-mailed complaints from end users or administrators

Individual DOS

- If the forged address is a genuine e-mail address in your domain
 - That user's mailbox will fill up!
 - The overhead of delivery or “mailbox full” handling will impact the overall system.

“Social” Aspects

- Willingness to take the “from:” field at face value....and
-E-mail headers are not always checked/understood leads to.....
 - Irate complaints (degree depends on material)
 - Naïve blocking
 - Reputation suffers.

Symptoms

- Large amount of individual e-mails
 - from many different legitimate e-mail addresses
 - from many different relays and IP addresses
- Often relatively small numbers of different “Subject:” fields
- Reduced e-mail performance

Coping strategies

- Scalable mail delivery system
 - Extra hardware “horsepower” quickly in crisis
 - Stateless software
- Configurable software
 - Subtle identification
 - Controllable behaviour
- “Early” rejection
 - Avoid “expensive” processing

Educational

- Provide “first stop” web info so that complainants can verify if the SPAM actually came from you (Headers etc.)
- Provide a dedicated e-mail address to handle complaints as politely and efficiently as possible.
- Some advice from JANET (relatively old)
<http://www.ja.net/CERT/JANET-CERT/mail/junk/collateral.html>

Emerging solution?

- SPF (<http://spf.pobox.com/>)
 - Sender Policy Framework
 - was Sender Permitted From
- DNS based information (your DNS)
- Says what relays can send e-mail with from: fields in your domain(s)
- Recipient will block forged e-mails if it examines you DNS.