



# The Fall 2006 Spam Explosion – How Postini is Responding

December 2006

**Presenters:**

**Dan Druker, Executive VP**

**Kevin Lund, Principal Systems Architect**

**Barry Schmell, Senior Trainer/Curriculum Developer**

# Agenda



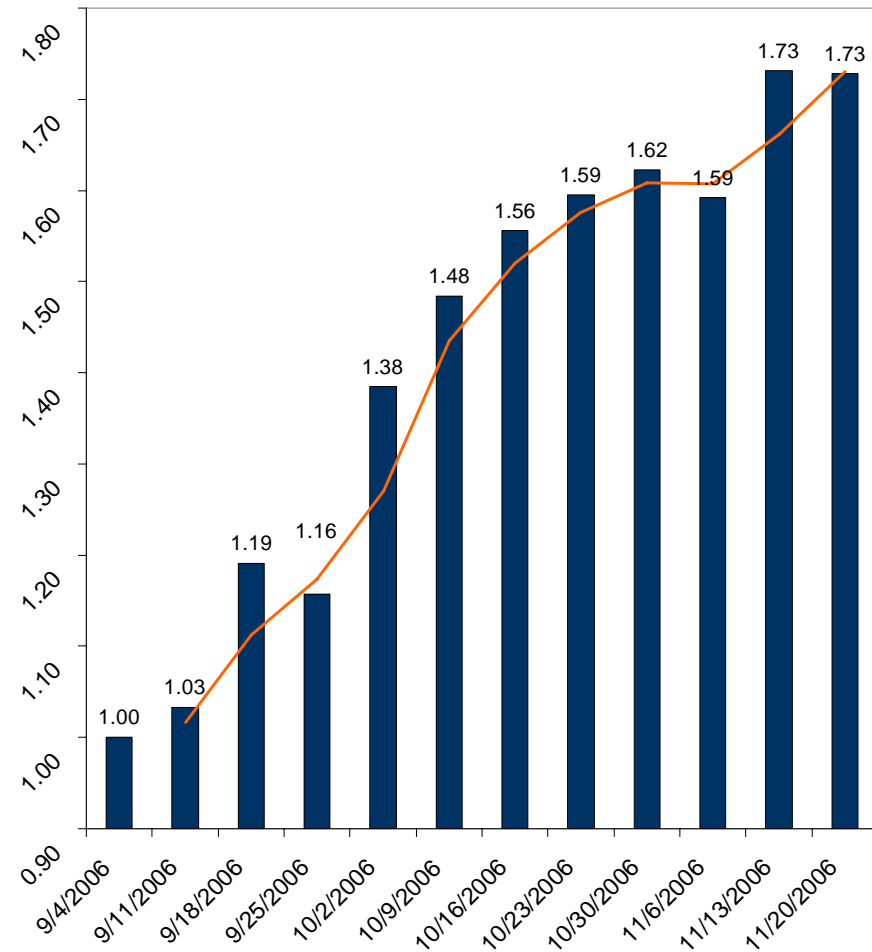
- The Fall 2006 Spam Explosion
- Spam Trends and Postini Response
- Best Practices

# Securing email from spam has become a front-burner issue again



- Total email spam volumes are up 147% in the last twelve months
  - Nearly 93% of all email is now spam
- Email spam has exploded, up 73% from September through November 2006
  - Postini blocks twelve spams for every good Internet email
  - Postini blocks more than 80 spams per day for the average user
- Image and office document spam now average 30% of all junk messages, up from minimal in 2005
  - Driving 334% annual increase in bandwidth, processing and storage requirements

73% Growth in Spams Blocked by Postini  
September - November 2006



Weekly data, normalized to September 1, 2006 = 1.00, source: Postini

# Spammers are increasingly aggressive and sophisticated



- Spam has evolved from a tool for annoying marketers to one for criminal enterprises
  - Criminals favor phishing, fraud and stock manipulation schemes
- Spammers now use massive networks of hijacked computers - “bot-nets” - to initiate attacks
  - More than one million IP addresses are now coordinating spam and virus attacks each day
  - More than 50,000 infected computers are attacking at any particular point in time
  - Spammers are constantly changing IP addresses to evade detection
- Virus outbreaks precede and are typically predictive of spam storms
  - October / November “Warezov” aka “Stration” Worm most recent example



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.

To resolve this problem please visit link below and re-enter your account information:

[https://signin.ebay.com/ws/eBay/SAPI.dll?SignIn&sid=verify&co\\_partnerId=2&siteId=0](https://signin.ebay.com/ws/eBay/SAPI.dll?SignIn&sid=verify&co_partnerId=2&siteId=0)

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,  
Safeharbor Department eBay, Inc  
The eBay team

This is an automatic message, please do not reply

Copyright © 1995-2005 eBay Inc. All Rights Reserved.

# Agenda



- The Fall 2006 Spam Explosion
- Spam Trends and Postini Response
- Best Practices

# The Basics



- Update DNS MX Records
  - Mail flows through Postini
- Add Users
  - Filters user email messages
- Secure firewall
  - Limit Port 25 to Postini IP Addresses and any other significant IP Addresses
  - IP address range is identified in the Administration Guide

# Recommended Settings



- Virus Blocking
  - Non-account Virus Blocking - On
  - Virus Disposition – Delete
- Attachment Manager (Additional virus protection)
  - System Threats – Quarantine
    - Executables: exe, ini, ins, iw, class, js, scr, vbs, com, pif
    - Compressed: hex, hqx, sea, sit, tar, zip, zoo, lzh, bz, bz2, gz, tgz
- Blatant Spam Blocking
  - Blackhole or Bounce
- General Settings
  - Support Contact
  - Non-account Bouncing – On (After adding all users)
- User Access to the Message Center
  - Spam Filtering - Read
  - Virus Settings - None
- Default User Settings
  - Spam filtering – Moderate settings
  - Virus blocking – Enabled and Organization Default

Spam filtering and virus protection

Have a question? Submit it via the WebEx Console

# Best Practices



- Configure Email Server Config settings
  - Connection Manager server protections
  - Automatic Spooling and Unspooling
  - Configure Alerts
- Lock down firewall
  - Limit access to port 25
- Add users, user aliases, and mailing lists
  - Default User spam filtering and virus settings
  - Non-account bouncing
  - Methodologies to manage users
- Consider Directory Sync and enable Non-account bouncing

Protect server and add users

# Commonly Overlooked



- Adding additional domains and domain aliases
  - Update DNS MX records, as well
- The Approved/Blocked Sender lists
  - Minimize the number of approved senders
  - User's approved/blocked sender list takes precedence over Organization's
  - Consider not allowing users to modify approved/blocked sender list via the Message Center
- Locking down the firewall

# Header Analyzer

- Easy to use user interface
- Interprets message headers
- Easy to read and understand display format
- Available at the Support Portal

**postini**  
PREEMPTIVE EMAIL PROTECTION

MESSAGE CENTER +

## Message Header Analyzer

Perimeter Manager inserts custom tags into the message headers of processed email. The Message Header Analyzer uses these tags to determine why a message was quarantined or allowed through. To analyze your message, copy and paste the message header into the window and press Analyze Header.

**Important:** Be sure to copy the *full message headers* into the window. The full headers are not normally visible when you view a message.

See the instructions below:

- Outlook Headers
- Notes Headers
- Administrative
- Self-Paced

**Header Analysis Summary**

- This message went through the Postini System
- This message was filtered

**Copy and paste message header here**

Analyze Header

```
Microsoft Mail Internet Header
Received: from exchsrvr3.postini.com [10.10.10.10]
Received: from thor.postini.com [10.10.10.10]
Received: from psmtmp.com [10.10.10.10]
Received: from source [206.105.100.10]
Received: (qmail 38528 invoked by SMTP)
DomainKey-Signature: a=rsa-sha1, s=1024, d=yahoo.com,
h=Message-ID:Received:Date:From:Subject:RSS:IE blog
b=GMSz7A051aYp+KsU
IU9gsecY= :
Message-ID: <2005071819500...>
Received: from [12.158.40.254]
Date: Mon, 18 Jul 2005 12:50:00 -0700
From: Jim Rambo <hello_rambo@yahoo.com>
Subject: RSS: IE blog
To: Jim Rambo <jrambo@postini.com>
MIME-Version: 1.0
Content-Type: multipart/alternative;
Content-Transfer-Encoding: 8bit
X-pstn-levels: (S:83.56696/S:100)
X-pstn-settings: 3 (1.0000:1.0000)
X-pstn-addresses: from <hello_rambo@yahoo.com>
Return-Path: hello_rambo@yahoo.com
X-OriginalArrivalTime: 18 Jul 2005 12:50:00 -0700
```

Overall Evaluation	Result	Note
Passed Virus Detection	Yes	
Content Manager	Filter off	Filter Name: n/a
Approved/Blocked Senders	Approved	Sender=hello_rambo@yahoo.com Trigger=user good
Scored as Legitimate Mail	Yes	See spam scores below for more information.

Spam Filtering Scores	Score	Note
Spam Threshold	1.0000	= Bulk Filter Value X Category Filter Value Higher score is greater sensitivity to spam
Spam Score	83.56696	Calculated by Perimeter Manager Range: 0(Spam) - 100(Legitimate)
Spam score is above the threshold?	Yes	Message is not considered spam.

Copy and paste message header here

# Summary / Q&A



- Spam volume and sophistication are dramatically on the rise
- Postini services are unmatched and we are continually investing to improve them
- Clients should leverage best practices and review them on a frequent basis
  - If spam is getting through, use Header Analyzer
- Resources and Information available at the Support Portal:
  - Best Practices
  - Webinars
  - eLearning Tools
  - Threat Advisories

