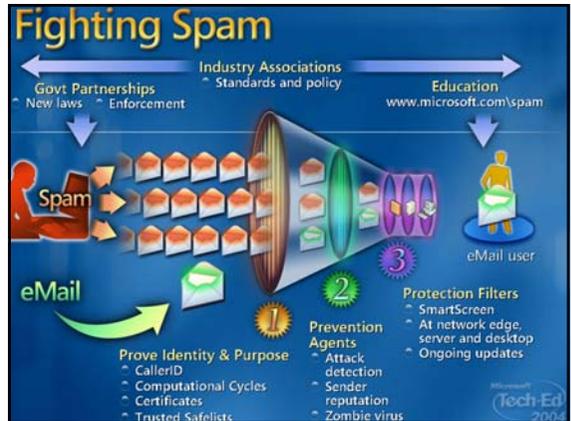


Microsoft's AntiSpam Strategy and Solutions

Microsoft Schweiz GmbH
Enterprise & Partner Group
Senior Technology Specialist
Andre Hagmann
ahagmann@microsoft.com



Anti-Spam Technologies

- Outlook 2003
 - Safe and Block lists, SmartScreen Technology
- Exchange 2003
 - Connection Filtering (IP based)
 - Recipient filtering
 - Sender filtering
 - ISV Support - Per Message Spam Rating (SCL) tagging
 - Microsoft Exchange Intelligent Message Filter
 - Server-side
 - Managed via ESM

How to Fight Spam

What Its About Classification

↑ Desirability	Critical legitimate mail	Business Personal Order confirmations	Easily classified at Gateway
	Non-critical legitimate mail	Subscriptions Listserv	
	Legitimate commercial mail	Amazon.com promotions Expedia fare tracker Mail from companies with a pre-existing business relationship	Gray area, best classified by end user
	Spam	Unsolicited product promotions Health & "pharmaceutical" Real estate & financial Scams & chain letters Pornography	Easily classified at Gateway
	Destructive	Viruses	

* External communication only. All internal communication is assumed to be legitimate

Where From (Connection Filtering)

- Global Allow and Deny lists
 - Configure individual IP or ranges by subnet mask
 - Allow overrides Deny by design
- Support for subscribing to 3rd party "real-time block list (RBL)" services
 - Support for multiple RBL providers
 - Customizable NDR response per configured provider
 - Override exception email address
- Integrated IP features

Who From (Sender Filtering)

- Filter messages sent from particular email addresses or domains
- Filter messages with blank senders
- Optionally drop connection
- Enhanced spoof detection – message submission method is persisted
- Don't resolve anonymous sender by default
- Blocking own domain will break list services

Who To (Recipient filtering)

- Filter messages sent to nonexistent recipients
 - No NDR – message rejected at protocol
 - Address book mining
- Filter messages sent to particular email recipients (valid or invalid)
- Restricted Distribution Lists
 - Allow only authenticated users to send to a DL
 - Reduces impact of unsolicited email sent to internal only DLs

Microsoft Exchange Intelligent Message Filter

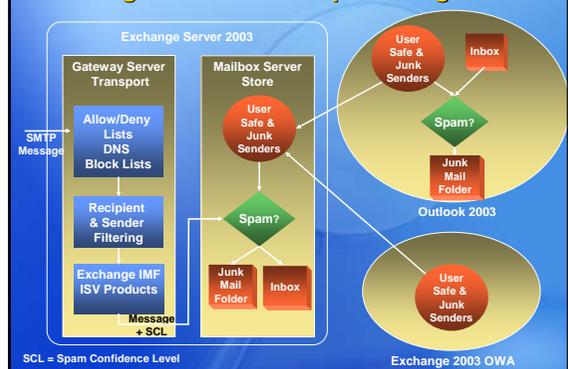
- Leverages SmartScreen Technology
 - Developed by Microsoft Research
 - Based on Heuristics-Based Message Analysis
 - Free available for Exchange Server 2003
 - Shipped in Outlook 2003, Updated with SP1
 - Deployed at Hotmail since January 2004
 - Deployed at Microsoft IT since July/August 2004
- Extension to Exchange 2003 Server, deployed on Internet Bridgeheads
- Leverages the SCL infrastructure
- Coexistence with 3rd party solutions
 - Compliments not compete

Outlook 2003 and OWA Client Features

Outlook 2003 and OWA 2003 Enhancements

- User specified Safe & Blocked Senders lists
 - Safe Senders, Safe Recipients, Blocked Senders
 - Can optionally include Contacts and GAL
 - Supports Safe Senders Only mode
- User Lists shared by Outlook 2003 and Exchange 2003 OWA, stored on the server
- Move to junk folder determined by:
 - Exchange 2003 Mailbox Store based on user lists
 - Per message SCL
 - Client Side based on Microsoft SmartScreen Technology
- Block all external content by default (Web beacons)

Exchange/Outlook Anti-Spam Integration



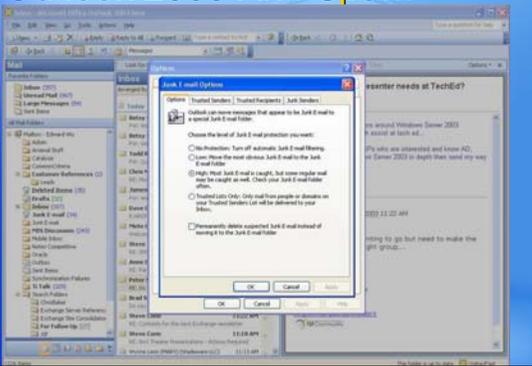
Outlook 2003 External HTML Content Blocking



OLK2003 Blocked Content



Outlook 2003 Anti-Spam



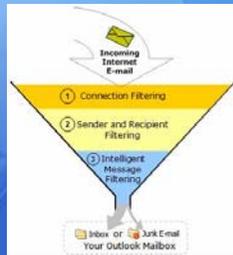
Trusted And Blocked Senders

- Safe Senders
- Safe Recipients
- Blocked Senders
- Can optionally include Contacts
- User Lists shared by Outlook 2003 and Exchange 2003 OWA
- User Lists are stored on the server
- Move to junk folder determined by store based on user lists and per message SCL

MS Exchange IT Showcase

<http://www.microsoft.com/itshowcase>

- IMF Deployed in 2004
- Real-time block lists
- Connection filtering
- Sender / Recipient filtering
- Microsoft Exchange Intelligent Message Filter
- Outlook Junk-E-Mail
- No longer 3rd Party Products in place
- 85% of 6-9M Mail's per Day filtered



AntiSpam Enhancements in Exchange Server 2003 Service Pack 2

Intelligent Message Filter v2 Benefits in SP2

- Updated SmartScreen Filter
 - Pre-SP2: update to IMF in Feb 2005
 - Includes additional data from MSN
 - SP2 will further include the latest updates
- Identify and block "phishing" mail
 - Anti-"Phishing" technology
- Tools to validate sender legitimacy
 - Computational Puzzle Validation
 - Anti-spoofing with Sender ID

Anti-"Phishing" Technology

- Determine if mail contains a "phishing" scam for gathering confidential data
- Integrated into SmartScreen engine - no additional configuration required
- More info:
<http://www.microsoft.com/athome/security/email/phishing.mspx>

From: [\[redacted\]](#)
To: [\[redacted\]](#)
Subject: PayPal® Account Review Department

Dear valued PayPal® member:

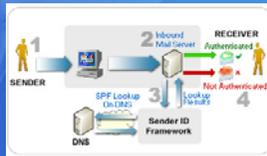
PayPal® is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account, PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

Recently, our Account Review Team identified some unusual activity in your account. In accordance with PayPal's User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved. This is a fraud prevention measure meant to ensure that your account is not compromised.

To update your Paypal records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login

Anti-Spoofing with Sender ID

- Sender sets mail servers' IP addresses in DNS
- Receiving e-mail server checks IP Address against DNS record, sets Sender ID status on message
- Exchange 2003 SP2 can be configured to check SPF records, take action against mail from spoofed domains
- Sender ID property used by Smartscreen for SCL
- Assists against "phishing"
- More info:
<http://www.microsoft.com/senderid>



Microsoft
Your potential. Our passion.™

© 2004 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.