Federal Trade Commission

July 11-12, 2007

Spam Summit

The Next Generation of Threats and Solutions

Keeping it Out of the Inbox

Moderator:

Sana Coleman Chriss, Attorney and Spam Coordinator, *Division of Marketing Practices, FTC*

- During the FTC's 2004 E-mail Authentication Summit, co-hosted with the Department of Commerce's National Institute of Standards and Technology, the FTC initiated efforts to spur the development and wide- scale adoption of domain level e-mail authentication. Where does the implementation of e-mail authentication stand? What are other key spam-reducing tools?

SPAM SUMMIT July 11-12, 2007

Keeping it Out of the Inbox

- **Des Cahill**, Chief Executive Officer, Habeas, Inc.
- **Jim Fenton,** Distinguished Engineer, Cisco
- **Richard L. Gingras,** Chairman, CEO and CoFounder, Goodmail Systems
- **Martha K. Landesberg,** Director of Policy and Counsel, TRUSTe
- **Margot Koschier Romary**, Senior Manager, Anti-Spam Operations, AOL
- **Craig Spiezle**, Director, Online Safety Strategies and Technologies, Microsoft Corporation

Craig Spiezle

- Director, Online Safety Strategies and Technologies, *Microsoft Corporation*

Returning control of the inbox to the consumer

empowering users to confidently interact, communicate & conduct business online

Craig Spiezle
Director, Online Safety Technologies
Trustworthy Computing Group
Microsoft Corporation

© 2007. All Rights Reserved. Microsoft Corporation

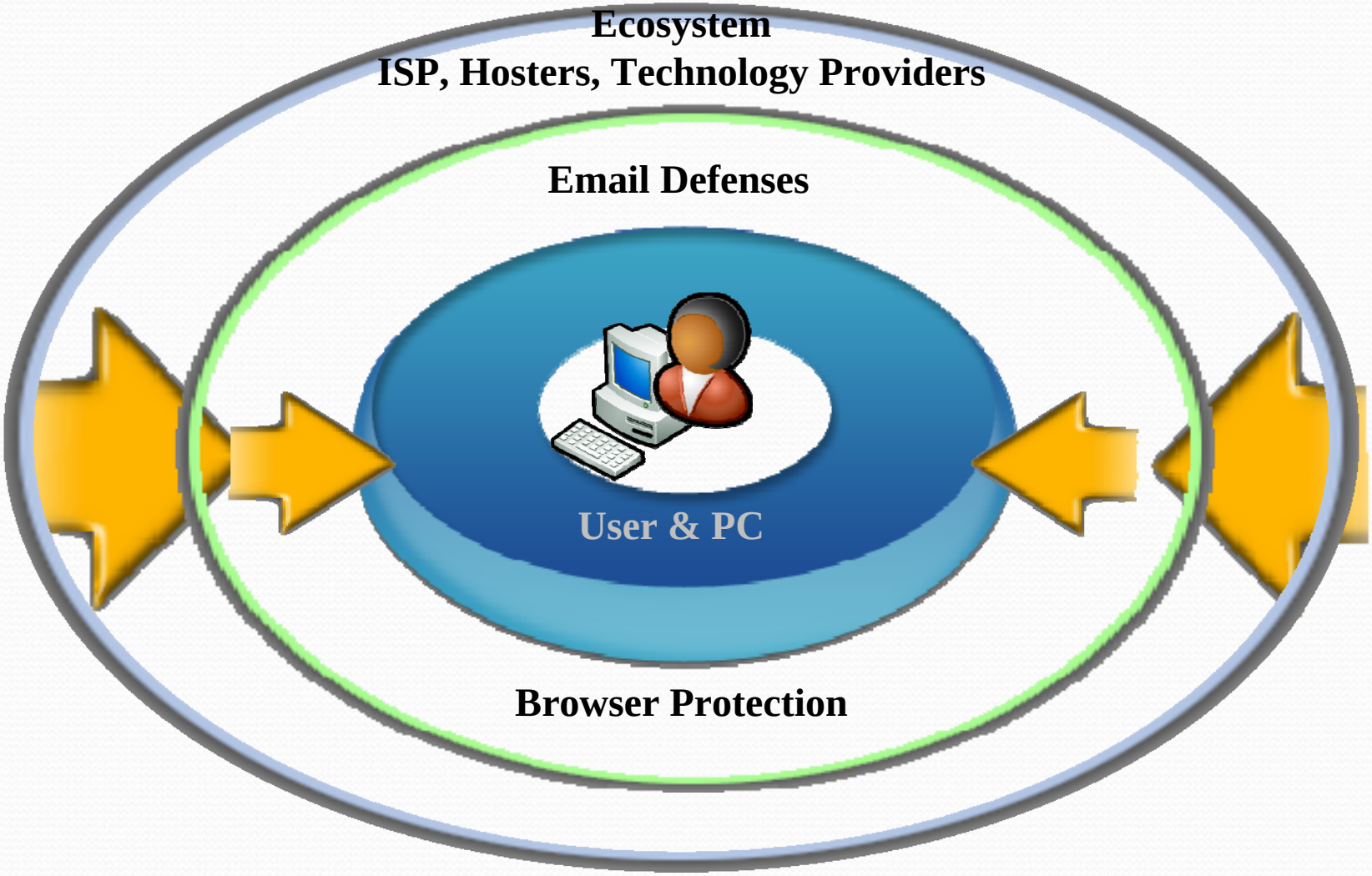
Agenda

- Shifting control of the inbox back to the user
  - Email, Instant Messaging, Mobile Phones…..
- Intrusion & protection from harm & data abuse
  - Time, privacy, productivity & infrastructure
- Counter Measures & Investments
  - Technology investments
    - Sender ID, Reputation & Postmarks
    - Microsoft Phishing Filter
    - Family Safety Settings & Parental Controls
  - Industry & business best practices
    - Education & prescriptive advice
    - Collaboration – Industry, Business and Enforcement

© 2007. All Rights Reserved. Microsoft Corporation

Requires a holistic defense strategy

Volumes, Vectors & Velocity



Why Authenticate with Sender ID?

Broad spoofing of top domains

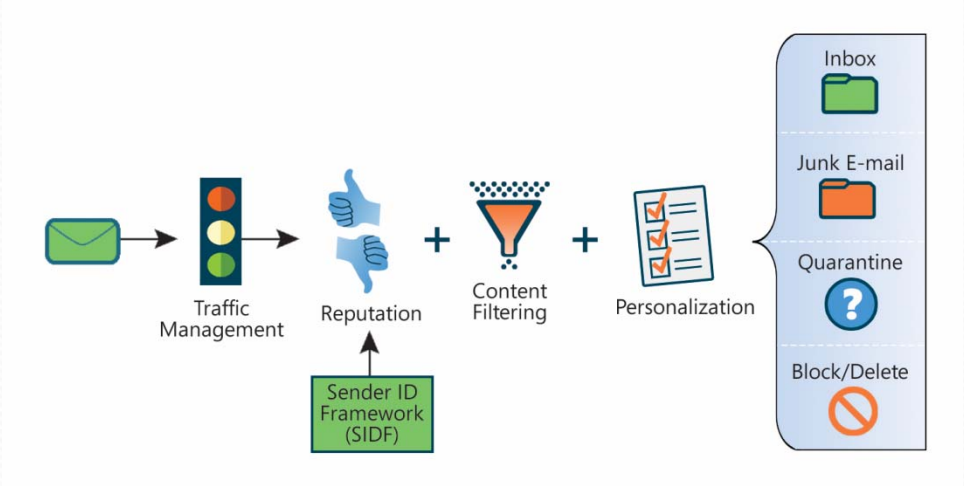
- Worldwide
  - ISPs
  - Carriers
  - Financial Institutions
  - Government Agencies
  - ecommerce sites

- **Enhanced brand and user protection by SIDF*

Domain	Rate
yahoo.com	81.0%
bankofamerica.com	61.3%
*	47.3%
verizon.com *	45.7%
irs.gov	41.2%
telefonica.net *	40.4%
paypal.com *	37.6%
hotmail.com *	33.3%
comcast.net	33.0%
prodigy.net	29.2%
ebay.com *	27.9%
aol.com *	26.1%
amazon.com *	10.4%

Why Authenticate with Sender ID?

- Benefits
  - A tool for more accurate filtering & mail delivery
  - Reduction of deceptive email in the inbox
  - Protect their brands & domain names
- Results
  - 85% fewer false positives
  - Blocks 95% of phishing exploits
  - Over 20 million exploits blocked daily
- Adoption
  - 45% of legitimate email
  - Over 10 million compliant domains
  - 39% of F500 banks & 85% of marketers



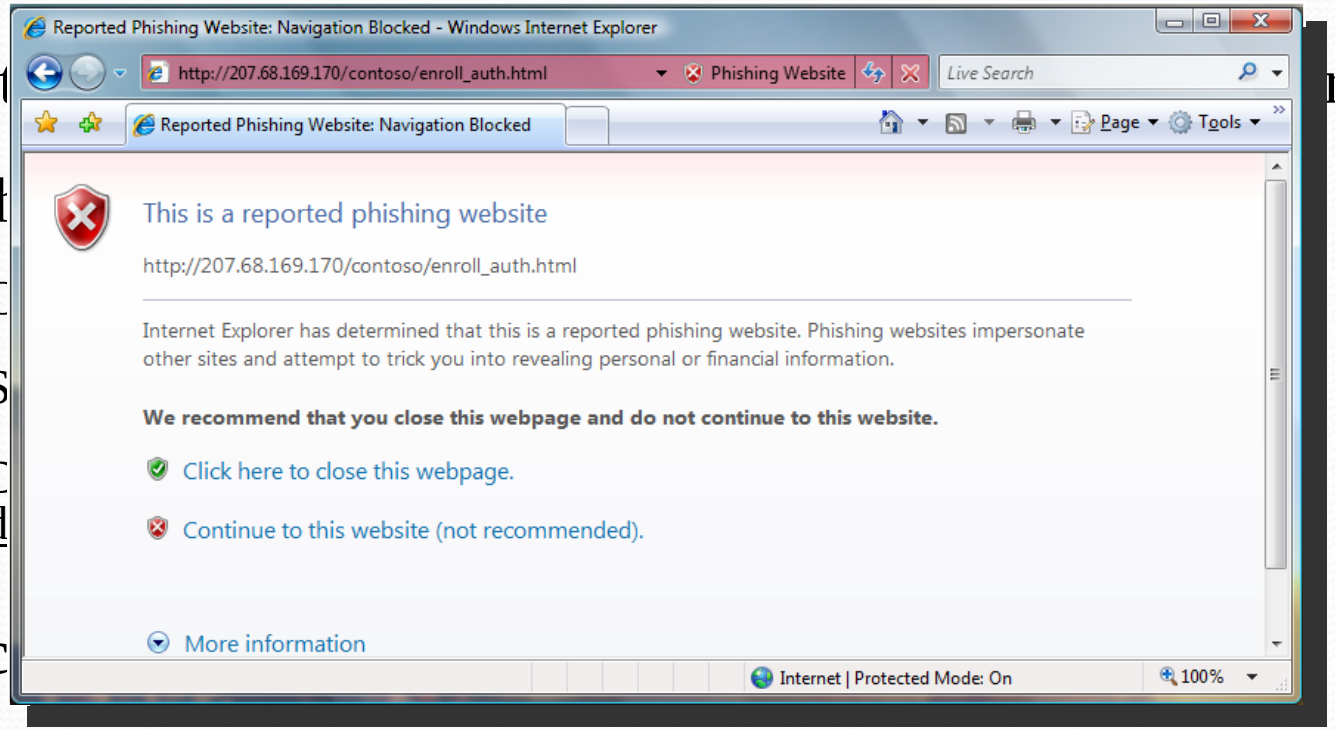
- Authenticate your domain and email today with SIDF
  - Consider DKIM as a complementary solution
- Implement inbound checking and reputation

© 2007. All Rights Reserved. Microsoft Corporation

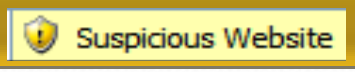
Microsoft Phishing Filter

Dynamic protection against fraudulent websites

- Built r
- 3 "cl
  - ✓ C
  - ✓ S
  - ✓ D sites
    d
- Bloc
- Two levels of warning and protection



Level 1: Warn Suspicious Website

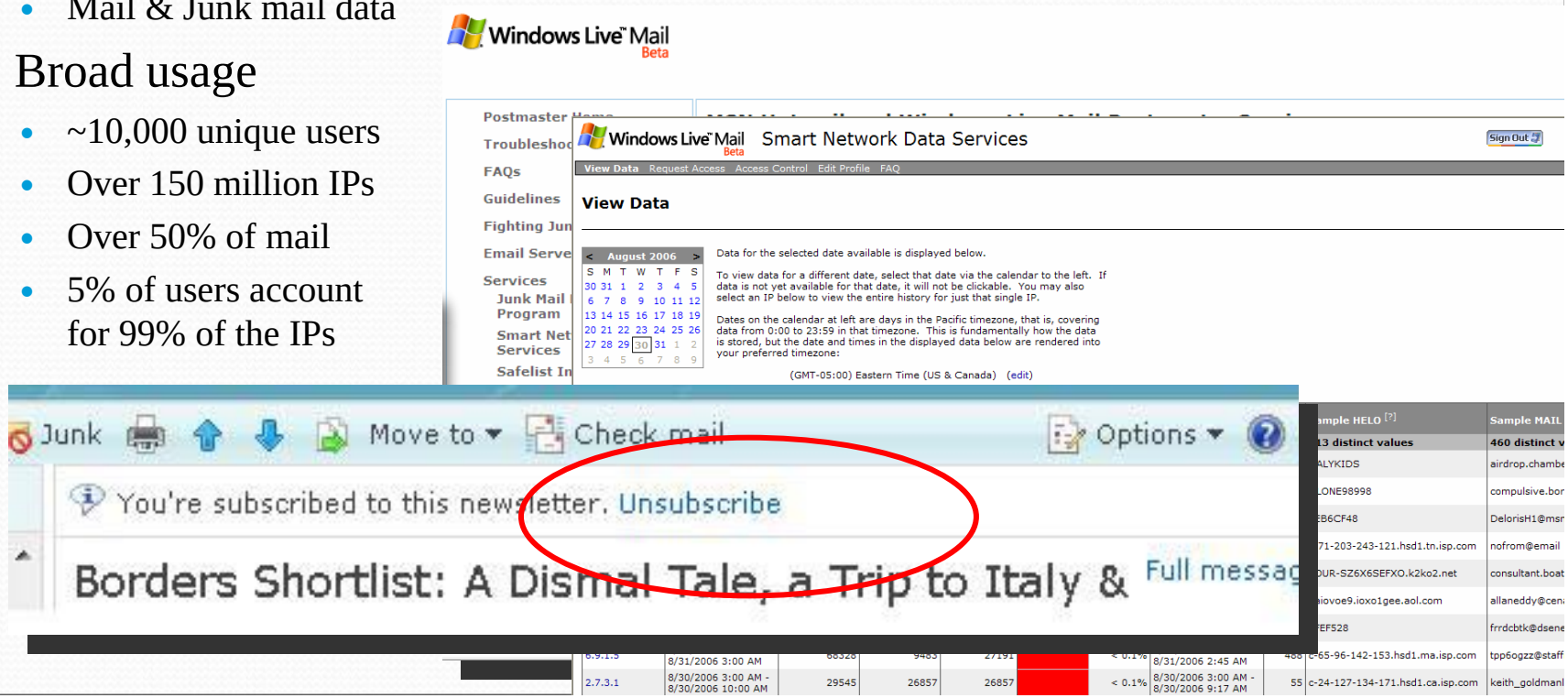


Windows Internet Explorer 7

Best Practices

http://www.microsoft.com/postmaster

- ISPs
  - Port 25 management, throttling, reputation, SIDF
  - Unsubscribe increased user control
- Junk Email Reporting Program (JMR) maintenance, reporting & reputation
- Smart Network Data Services (SNDS)
  - Detect unexpected or suspicious mail activity – spammers, botnets, malware
  - Mail & Junk mail data
- Broad usage
  - ~10,000 unique users
  - Over 150 million IPs
  - Over 50% of mail
  - 5% of users account for 99% of the IPs



Next Steps

SIDF Authentication & Reputation is extremely effective

- Counterweight to rapidly changing spammer tactics
- SIDF and DKIM are complementary

Marketers have taken a great first step now they need to commit to

- Corporate and brand domain protection
- Stem gray mail and honor user expectations

ISPs need to move from watching from the sidelines and invest

- Outbound spam management

Industry - collaboration investment and speed to implementation

Resources - www.microsoft.com/safety

- Sender ID - www.microsoft.com/senderid
- Senders & Marketers - www.microsoft.com/postmaster
- Security - www.microsoft.com/security
- Consumers - www.microsoft.com/protect

Microsoft®

Your potential. Our passion.™

© 2007. All Rights Reserved. Microsoft Corporation

Additional Data & References

© 2007. All Rights Reserved. Microsoft Corporation

Microsoft's security & safety strategy

Secure platforms, products and services strengthened by safety innovations, user guidance and industry cooperation efforts to help keep customers safe

- **Excellence in fundamentals across platforms, products and services**
- **Other security-enabling innovation**

- **Educational content and tools**
- **Authoritative incident response**
- **Safety in user experience**

- **Ecosystem**
- **Awareness and education**
- **Collaboration and partnership**
- **Public policy and enforcement**

Vectors, Volumes & Velocity

- **Spam – a plague of biblical proportions**
  - **Redefined from unsolicited email to malicious**
  - **Volume up 40% since June 2006, 80% from Bots**
  - **1/3 is image based, diminishing content filtering impact**
  - **Receiving networks are under attack**
- **Criminals do not recognize international boundaries or law**
- **Growing level of sophistication & precision**
  - **Anti-virus to remove "competing" malware**
  - **Spyware, keystroke loggers**
  - **Thriving black market for data**
- **67% of users don't have current A/V, but 80% think they do**
- **Marketers understanding consumer expectations**
  - **Frequency & Relevancy**
- **Consumer, Government and Business at risk**
  - **Control over the Inbox**
  - **Impact to critical infrastructure & commerce**

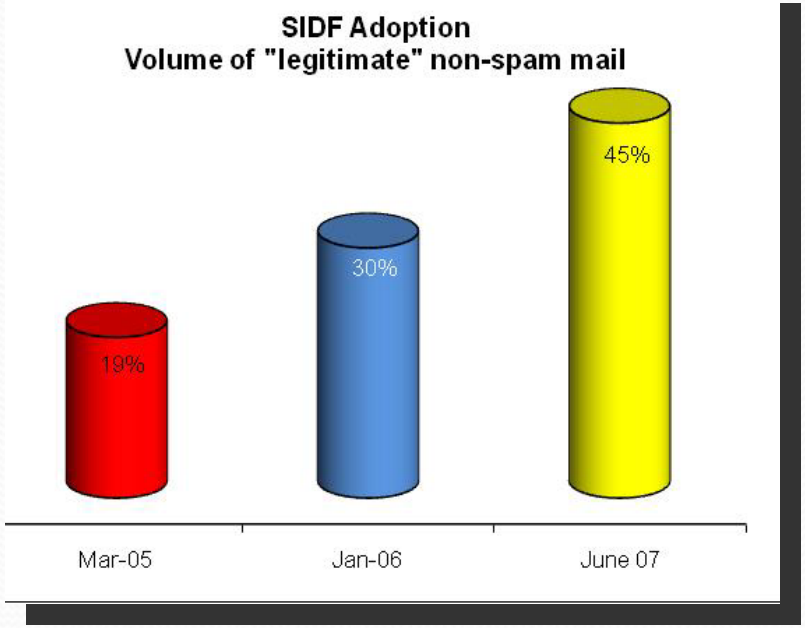
Spam Selling Trends

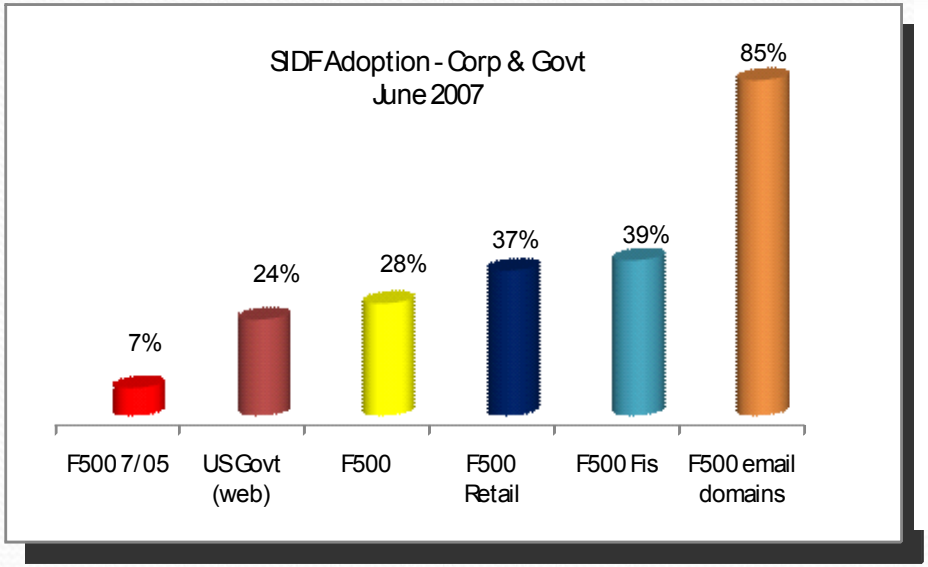
- Opportunistic seasonality and quick to “market”
- Market segmentation and “agewave”
- Varying tactics to targeted network / users
- Consumer vs Corporate mail boxes
- Image spam
  - 33% of Hotmail spam has images
  - 17% at Exchange Hosted Filtering

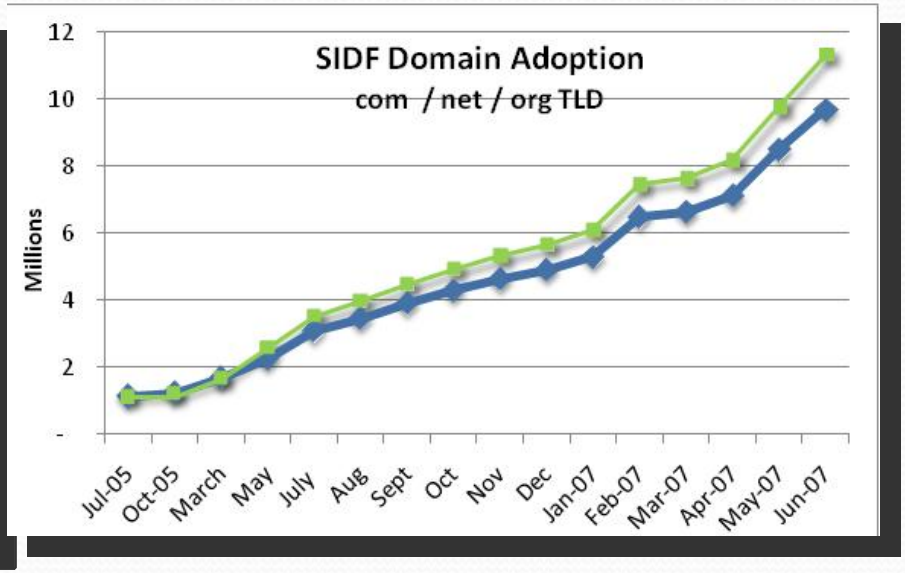
© 2007. All Rights Reserved. Microsoft Corporation

SIDF Adoption

- **Over 45% of legitimate email**
- **Growing support by F500**
- **Over 12 million domains**
- **Leading ISPs & Mail Providers**
  - **Windows Live Hotmail**
  - **Qwest, Bell Canada**
  - **Go Daddy, Gmail ….**
  - **……..**



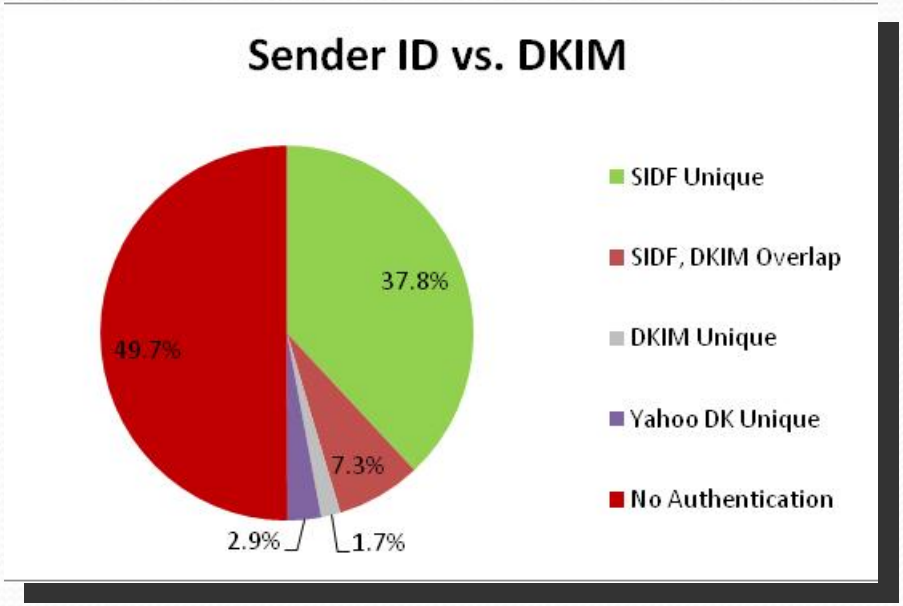




Sources: Microsoft research 7/2/07 (2) Mark Monitor Report 7/2/07

Adoption Scorecard

- **SIDF now over 45% of legitimate email**
- **SIDF & DKIM are complimentary**
- **50% of all legitimate email is authenticated by one or more!**
- **Needs of volume mailers vs domain holders & SMBs**
- **Spam detection & Deliverability vs Fraud & Phishing**
- **Operational, infrastructure & legacy systems**



Source: Analysis of non-spam email being sent into Windows Live Hotmail, sampling of ~300 million mailboxes. Note while not documented it is possible signed mail may be understated due to senders only signing mail sent into specific ISPs. © 2007 Microsoft Corporation. All rights reserved.

Sender ID + Reputation Example

Current Content Filtering & Scoring

Spam Features		Non-Spam Features	
Feature	Weight	Feature	Weight
Free	- 0.0413	Document	+ 0.0084
Free (Subject)	- 0.2397	Record	+ 0.0402
Hot	- 0.0453	Confidential	+ 0.0925
Sexy	- 0.0756	Job	+ 0.1323
Diploma	- 0.1776	Pen	+ 0.0234
Viagggra	- 0.3222	Apple	+ 0.1196

Sender ID with Reputation

Spam Reputation	Good / Non-Spam Reputation
- 1.7203	+ 3.1642

Example - Email about investments, interest rates, and other financial data

- **Content score = -.9103, → mail delivered to junk folder.**
- **Mail is from legitimate bank, passes SIDF, reputation score = +3.1642**
- **Net score = 2.2539, → mail delivered to Inbox**

- **Note: Weights change frequently. Values shown are for illustration only.**

IE7 Security Status Bar

Improving Online Trust & confidence

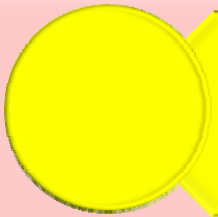
Verified Identity, Strong Encryption

- Provides most protection for transacting online

Unknown Verification, Strong Encryption (SSL)

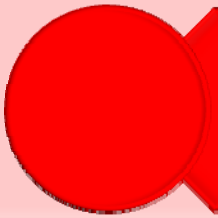
- Protects from eavesdropping

EV SSL



Suspicious Identity, Possible Encryption

- Caution! Proceed at own risk!



False Identity, Possible Encryption

- Stop! Known phishing site!

Phishing Filter

Personal Reputation – Identity

Outlook 2007 Email Postmark

Problem

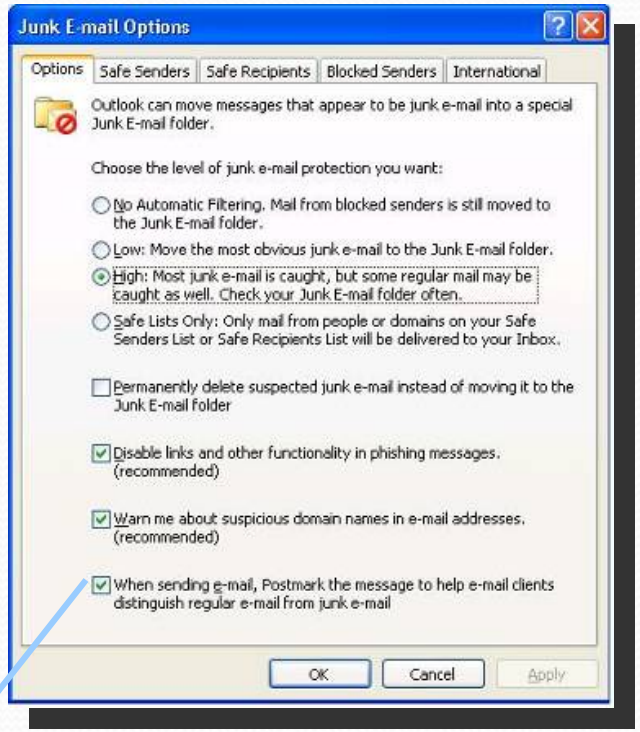
- Individual users mail may appear like spam to filters but are legitimate causing their mail to blocked
- Improving deliverability & legitimacy, reducing the risk of being junked

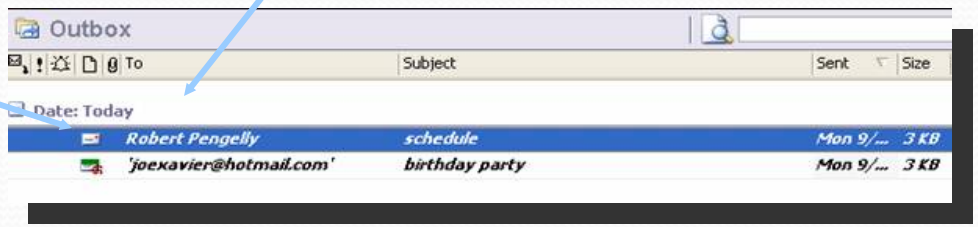
Solution – Outlook Email Postmark

- Microsoft SmartScreen analyzes the mail for content that might trigger heuristics on receiving networks
- Outlook attaches a Postmark or computational puzzle on the mail before being sent, (takes 8-10 seconds of computing time), transparent to the user.
- Receiving networks validate the token and apply a score to the Spam Confidence Level (SCL)

Support

- Windows Live Hotmail
- Exchange 2007
- Outlook 2007





© 2007. All Rights Reserved. Microsoft Corporation

Keeping it Out of the Inbox

- **Des Cahill**, Chief Executive Officer, Habeas, Inc.
- **Jim Fenton,** Distinguished Engineer, Cisco
- **Richard L. Gingras,** Chairman, CEO and CoFounder, Goodmail Systems
- **Martha K. Landesberg,** Director of Policy and Counsel, TRUSTe
- **Margot Koschier Romary**, Senior Manager, Anti-Spam Operations, AOL
- **Craig Spiezle**, Director, Online Safety Strategies and Technologies, Microsoft Corporation

Jim Fenton

- Distinguished Engineer, *Cisco*

The Role of Email Authentication in Keeping Spam Out of the Inbox

Jim Fenton

 © 2007 Cisco Systems, Inc. All rights reserved.

DKIM Status

- DomainKeys Identified Mail (DKIM) approved by IETF as a standards-track protocol (RFC 4871)
  - Provides signature-based authentication of email messages
  - Supports transparent forwarding of messages (“alumni” domains, etc.)
  - Complementary to path-based techniques (SPF, SenderID)
- DKIM currently available or soon to be available in a wide variety of vendor email products
- Already deployed by Google Mail; expected soon from other consumer-oriented mail service providers
- Enterprise deployments underway, with financial institutions leading the way

 © 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

Cisco's DKIM Deployment

- Cisco has been deploying DKIM over the past year
  - 7 major data centers worldwide
  - Interim deployment of dedicated signer/verifiers
  - Transition to integrated DKIM support as it becomes available
- Valid signatures received from over 20,000 domains
- Computational overhead low

 © 2007 Cisco Systems, Inc. All rights reserved.

How Does Email Authentication Help?

- Can be used in conjunction with whitelists to ensure delivery of messages from known correspondents
  - May permit more aggressive filtering of unknown messages
- Supports the creation of domain-based reputation systems
  - Current IP-based reputation services suffer from issues associated with IP address reuse
- Supports accreditation/certification services
- Deters use of well-known, phished domains by cybercriminals

 © 2007 Cisco Systems, Inc. All rights reserved.

What About Unauthenticated Messages?

- Some messages will always be unauthenticated
  - Some applications require anonymity
  - Deployment will never reach 100%
- Visibility into use of authentication by domains is helpful in evaluating messages
- Sender Signing Practices specification, currently under development in IETF, will provide this capability
- Particularly useful for phished domains
  - Domains that sign all of their messages can cause unsigned messages to appear much more suspicious

 © 2007 Cisco Systems, Inc. All rights reserved.

Won’t Cybercriminals Use Authentication?

- They will, and probably already are
  - Strong circumstantial evidence based on Cisco deployment
- Authentication limits the addresses available for use by cybercriminals
- Throw-away domains are still a problem
  - Accreditation and reputation address this
- Authenticated messages aren’t necessarily desirable

 © 2007 Cisco Systems, Inc. All rights reserved.

Conclusion

- Authentication provides a way to recognize the sender of email
- Like a peephole in a door, provides a way to decide:
  - It's a friend, so open it (whitelist)
  - It's someone with a valid looking ID (e.g., utility worker), so open it (accreditation)
  - It's someone you don't know, so ask more questions (authenticated, unknown sender)
  - It's someone who won't say who they are, so ask many more questions (unauthenticated)

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

 © 2007 Cisco Systems, Inc. All rights reserved.

CISCO

Keeping it Out of the Inbox

- **Des Cahill**, Chief Executive Officer, Habeas, Inc.
- **Jim Fenton,** Distinguished Engineer, Cisco
- **Richard L. Gingras,** Chairman, CEO and CoFounder, Goodmail Systems
- **Martha K. Landesberg,** Director of Policy and Counsel, TRUSTe
- **Margot Koschier Romary**, Senior Manager, Anti-Spam Operations, AOL
- **Craig Spiezle**, Director, Online Safety Strategies and Technologies, Microsoft Corporation

Des Cahill

- Chief Executive Officer, *Habeas*, *Inc.*

The Email Trust Authority

FTC Spam Summit: Keeping It Out of the Inbox

July 12, 2007

Agenda

- Reputation today
- Evolution of reputation
- Reputation statistics
- Conclusions

HABEAS

Reputation Definition 2007

- General industry view of reputation
  - Historical data applied to a known entity
  - Observed/objective sender behavior
  - **End user feedback** is key
  - Granular score
  - Legitimate, bad and grey mailers
  - IPs, domains, business
  - Important component in minimizing impact of spam

HABEAS

Authentication and Reputation work together

- (SIDF or DKIM) + Reputation improves:
  - identification of legitimate email
  - identification of spoofed/phish email
- The 2007 industry analogy:
  - Authentication is driver's license (who?)
  - Reputation is driving record (how good?)
- Working model for receivers
  - Known bad reputation = block email
  - Known good reputation + authentication = deliver email
  - Unknown reputation or no authentication = filter email

HABEAS

Reputation evolution

- 1999 - Negative reputation services (blocklist)
  - Receiver pays to block bad stuff
  - MAPS/Trend, Spamhaus, SenderBase, Symantec, TrustedSource
- 2002 - Sender accreditation (whitelist)
  - Sender pays for improved delivery
  - Bonded Sender, Haiku Habeas
- 2006 – Reputation Services
  - Legitimate, bad and grey senders rated
  - Covers > # of senders than whitelists
  - Rating on observed sender behavior
  - Habeas, ReturnPath, Lashback (RSPs)
  - AOL, Yahoo!, Hotmail (Private systems – Tier 1 ISPs)

HABEAS

Reputation and email ecosystem

Bringing transparency and accountability to email

- ISP
  - Additional data sources on sender trustworthiness
- Commercial Senders
  - “Rating” drives decisions on email investment, practices
- Email Service Providers
  - Ensure prospects/customers are reputable
- Consumers
  - Empowered to make email choices (opt-in, unsubscribe)

HABEAS

Reputation Data Context

- Habeas analyzing email traffic data for last 18 months
  - 5M reporting email networks in....
  - 190 countries and territories querying....
  - Habeas 600M-800M times a day....
- Habeas tests volume email senders in these areas:
  - Identity: whois/domain, authentication
  - Reputation: DNSBL, 3rd party tests
  - Infrastructure: RDNS, MX record, static-dynamic IP
  - Practices: unsubscribe, CAN SPAM compliance

HABEAS

Reputation Data from June 07

- Observed/tested 750M distinct senders
  - 450M dynamic IPs
  - 300M static IPs
- 99.8% of senders classified as “spammers”
- Of the “non-spammer” senders (1.5M, .2%)
  - 40,000 classified as “good practices” (<3%)
  - 1.46M classified as “questionable practices” (~97%)
  - 27% use SIDF/SPF
    - But 13% have record misconfigured
  - 40% have RDNS issues

HABEAS

Reputation conclusions

- There are a *lot* of spammers out there
- Legitimate senders must work hard to stand out
  - authentication adoption and email best practices
- Reputation systems complement authentication and anti-spam filtering approaches
- Likely that multiple reputation systems will be used by email receivers
  - HabeasBL (320M) has < 8% overlap with SBL
- Still early days of reputation; expect lots of innovation in next few years

HABEAS

Thank You

Des Cahill

CEO, Habeas

650 694-3312

des@habeas.com

www.habeas.com

RED HERRING 100 WINNER N. AMERICA

THE STEVIES

THE AMERICAN BUSINESS AWARDS™

2007 Winner

HABEAS

Keeping it Out of the Inbox

- **Des Cahill**, Chief Executive Officer, Habeas, Inc.
- **Jim Fenton,** Distinguished Engineer, Cisco
- **Richard L. Gingras,** Chairman, CEO and CoFounder, Goodmail Systems
- **Martha K. Landesberg,** Director of Policy and Counsel, TRUSTe
- **Margot Koschier Romary**, Senior Manager, Anti-Spam Operations, AOL
- **Craig Spiezle**, Director, Online Safety Strategies and Technologies, Microsoft Corporation

Richard L. Gingras

- Chairman, CEO and CoFounder, *Goodmail Systems*

Will Email Become the Medium We Want It To Be?

Richard Gingras (presented by Ken Hirschman)
Chairman, CEO & Co-Founder
Goodmail Systems

July 12, 2007

GoodmailSystems™
Bringing Safety and Reliability to Email

Confidential & Proprietary - Goodmail Systems, Inc. - 2007

An Email Inbox of Risk

Fear, uncertainty, doubt

93% of email users say phishing and identity theft are a major concern

96% of email users think adding a symbol confirming authenticity is important

55% delete any and all bank messages

As much as **30%** of legitimate email does not get to the inbox

InternetEmail

possibly, maybe, sometimes.™

Reliability and Trust are in Tatters

Key question:

Can email achieve its full potential or maintain its value without clear attributes of reliability and trust?

Confidential & Proprietary - Goodmail Systems, Inc. - 2007

Do we <u>want</u> to reduce email to plain text?

No images & links?

No secure forms?

No future for advanced functionality?

Do we <u>want</u> email only for casual communications?

No "official" use?

No legal standing?

No future for paper suppression?

CertifiedEmail Creates a New Dynamic

- Deterministic email processing rather than “ad hoc” and probabilistic
- Advanced delivery services for qualified senders with service-level commitments (SLA)
- Protect recipients and support structured business relationships with senders

Confidential & Proprietary - Goodmail Systems, Inc. - 2007

Advanced Services for Qualified Senders

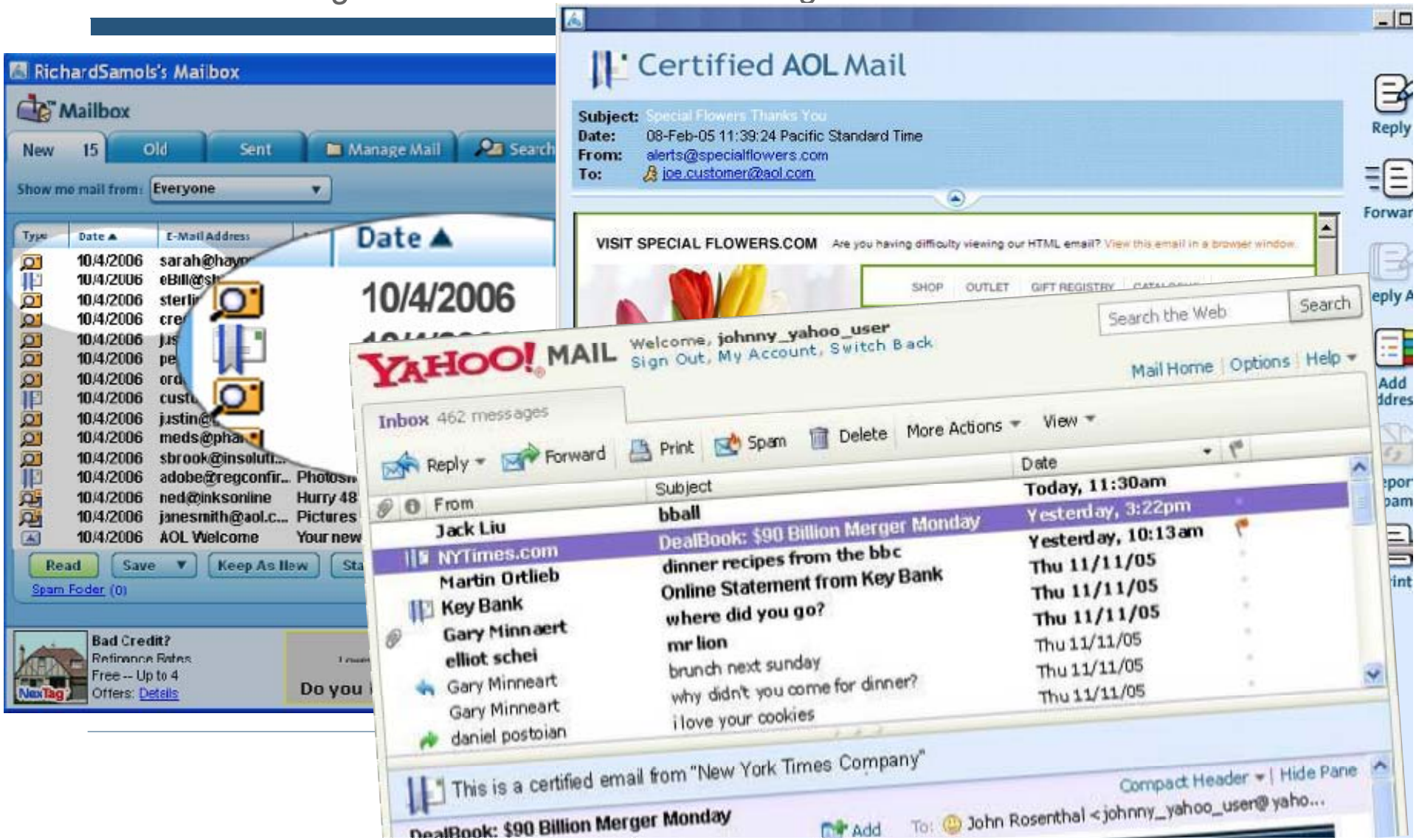
CertifiedEmail: assured delivery, message presentation, reporting

- Assured inbox delivery
  - Bypass volume filters
  - Bypass content filters
  - Does not bypass complaint mechanisms
  - Confirmation receipt by message
- CertifiedEmail inbox labeling
  - Non-spoofable
  - Conveys trust
- Full message functionality
  - Images, enabled links
  - No restrictions on copy

Confidential & Proprietary - Goodmail Systems, Inc. - 2007

Restore Trust Through Visual Certification

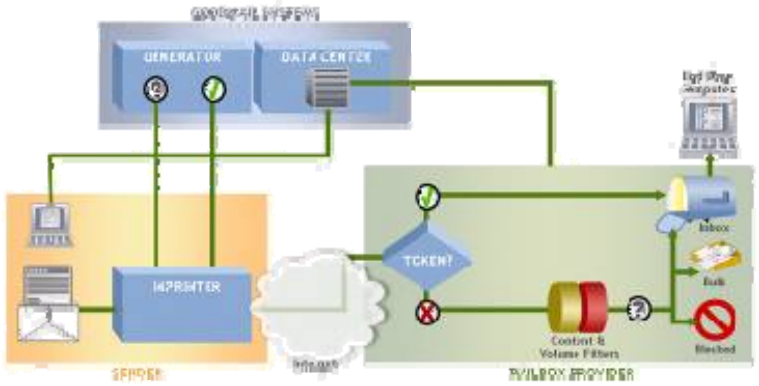
Visual marking restores trust & encourages interaction



What makes CertifiedEmail secure?

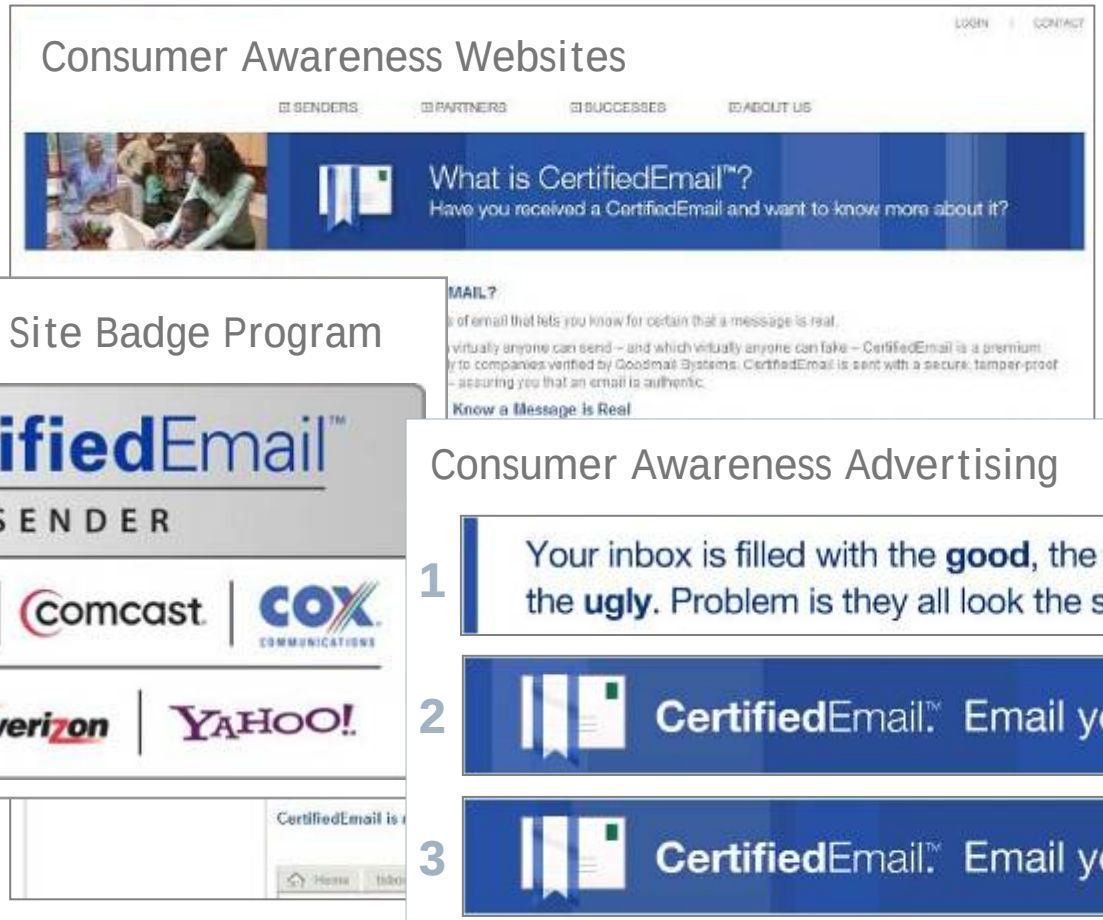
Message-specific tokenization, multi-dimensional anomaly detection

- Thorough process of accreditation and qualification
  - Have rejected 72% of applications
- Unique cryptographic token embedded in each message and signed by Goodmail
- Ongoing complaint monitoring to enforce AUP
- Message tokenization allows:
  - Quota management
  - Accurate complaint monitoring
  - Anomalistic behavior detection
  - Complaint spike detection
  - Dynamic privilege revocation



Driving Consumer Knowledge & Trust

Consumer Awareness Websites



Consumer Awareness Site Badge Program

Consumer Awareness Advertising

1

2

3

4

Making Email the Medium It Needs To Be

- Email is becoming central to our lives
  - 146 million adult email users in the US
- Restoration of reliability and trust is critical
- Email's future rests on our ability to secure its trust and advance its capability and potential

CertifiedEmail

Email you want. Email you trust.

Confidential & Proprietary - Goodmail Systems, Inc. - 2007

Will Email Become the Medium We Want It To Be?

Richard Gingras (presented by Ken Hirschman)
Chairman, CEO & Co-Founder
Goodmail Systems

July 12, 2007

GoodmailSystems™
Bringing Safety and Reliability to Email

Confidential & Proprietary - Goodmail Systems, Inc. - 2007

Keeping it Out of the Inbox

- **Des Cahill**, Chief Executive Officer, Habeas, Inc.
- **Jim Fenton,** Distinguished Engineer, Cisco
- **Richard L. Gingras,** Chairman, CEO and CoFounder, Goodmail Systems
- **Martha K. Landesberg,** Director of Policy and Counsel, TRUSTe
- **Margot Koschier Romary**, Senior Manager, Anti-Spam Operations, AOL
- **Craig Spiezle**, Director, Online Safety Strategies and Technologies, Microsoft Corporation

Martha K. Landesberg

- Director of Policy and Counsel, *TRUSTe*

Best Practices in Email and Downloadable Software:

Set High Standards, Elevate Good Actors, Protect Consumers

FTC Spam Summit 2007

Martha K. Landesberg
Director of Policy and Counsel
TRUSTe

TRUSTe: 10 Years of Impact

1997

reviewed by TRUSTe site privacy statement

2007

TRUSTe EU SAFE HARBOR | TRUSTe CERTIFIED WEBSITE PRIVACY | TRUSTe KIDS PRIVACY | TRUSTe CERTIFIED EMAIL

- **Web Privacy Seal**
  - 2,400 Websites
  - 1,500 companies
  - 22 of Top 50 most visited websites
  - 1 Million "click-to-verify" pageviews monthly
  - Thousands of consumer complaints resolved annually

- **EU Safe Harbor** Seal by authority of the US Department of Commerce
- **Children's Online Privacy Protection Act Safe Harbor** by authority of the FTC
- **Email Privacy Seal** beyond legal requirements for legitimate mail
- **Trusted Download Program** (beta)
  - Certifying consumer downloadable software (not Spyware)

TRUSTe

EMAIL PRIVACY SEAL PROGRAM

Leading permission-based standards:

- Consumer-facing seal linked to verification page
- Clear notice & consent at point of collection
- No 3rd party sharing without explicit permission
- Easy to use, responsive, persistent unsubscribe
- Third party oversight – audit & certification
- ISP and abuse network complaint monitoring
- Proprietary list seed notification system
- Dispute resolution
- Malicious sources fail verification

Email Privacy Seal
Point of Collection Disclosures

- **Credit.com** does not share your email address with third parties unrelated to this transaction. You may receive email from Credit.com for identity verification, our newsletter and customer support. You can opt out at any time.
- **3riversarchery.com** – Your privacy is important to us. We never share your email information with third parties. We collect your email address so we can send you order confirmation and our newsletter with sales and new products. For more information please review our privacy policy.

TRUSTe

Why Seals Work

- Consumers use them
  - 1 million clicks per month on TRUSTe “click to verify” validation seals
- Consumers trust them
  - 73% say they are more likely to provide an email address where seal is present
- Identify trustworthy companies
- Provide consumer education
  - About program, verification process
- Provide dispute channel: recourse at time of need
- Provide monitoring mechanism
  - Consumers enlisted to help us track fraud

Trusted Download Program (Beta):
The First Industry Standards for Downloadable Software

- Provides meaningful notice and control for consumers
- Establishes industry-wide standards for software developers
- Marginalizes malware
- Creates marketplace incentives for the development of good software
- Identifies trustworthy applications via whitelist for distributors, marketers and anti-spyware vendors
- Helps advertisers protect their brands through spyware-free advertising
- Whitelist first published on February 16, 2007 on www.truste.org

TRUSTe

TDP Program Elements

- Strict standards:
  - Notice
  - Consent
  - Easy uninstall
  - Collection & use of PII
- Prohibits fraudulent software behavior
- Imposes affiliate controls
- Rigorous certification process
  - Disclosure reviews by TRUSTe
  - Software evaluation by independent testing lab
- Ongoing monitoring and enforcement by TRUSTe
- Partners: AOL, Computer Associates , CNet, Microsoft, Verizon, and Yahoo!

TRUSTe

To Combat Spam & Malware: Fit the Pieces Together

TRUSTe

Contact Information

Martha Landesberg
Director of Policy and Counsel
TRUSTe
1750 K Street, NW, Suite 1218
Washington, DC 20006
+1.202.835.9751
mlandesberg@truste.org

www.truste.org

Fran Maier
Executive Director & President
685 Market Street, Suite 270
San Francisco, CA 94105
+1.415.520.3418
fran@truste.org

TRUSTe

Keeping it Out of the Inbox

- **Des Cahill**, Chief Executive Officer, Habeas, Inc.
- **Jim Fenton,** Distinguished Engineer, Cisco
- **Richard L. Gingras,** Chairman, CEO and CoFounder, Goodmail Systems
- **Martha K. Landesberg,** Director of Policy and Counsel, TRUSTe
- **Margot Koschier Romary**, Senior Manager, Anti-Spam Operations, AOL
- **Craig Spiezle**, Director, Online Safety Strategies and Technologies, Microsoft Corporation

Margot Koschier Romary

- Senior Manager, Anti-Spam Operations, *AOL*

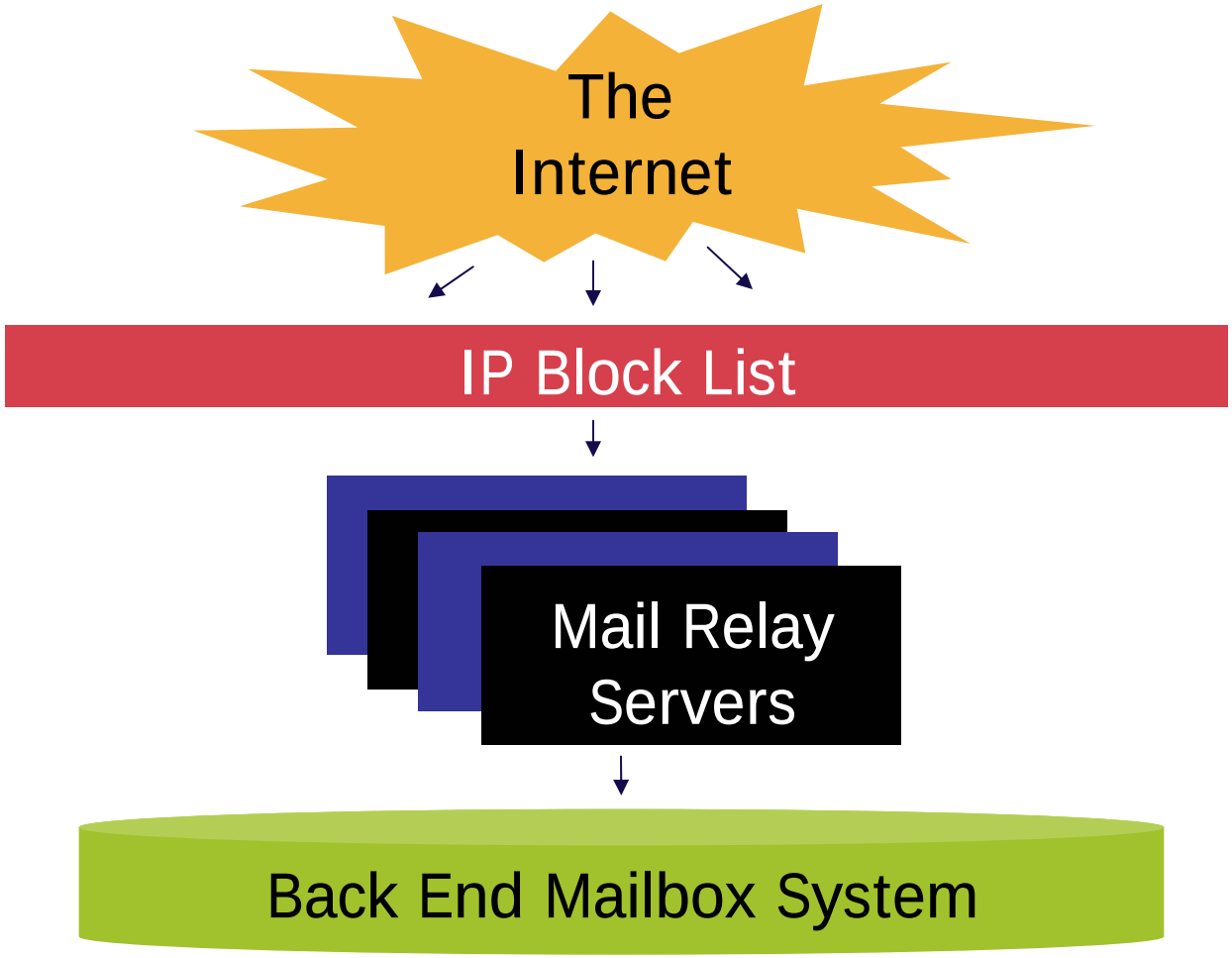
Keeping it Out of the Inbox

Authentication, Reputation and Other Technologies

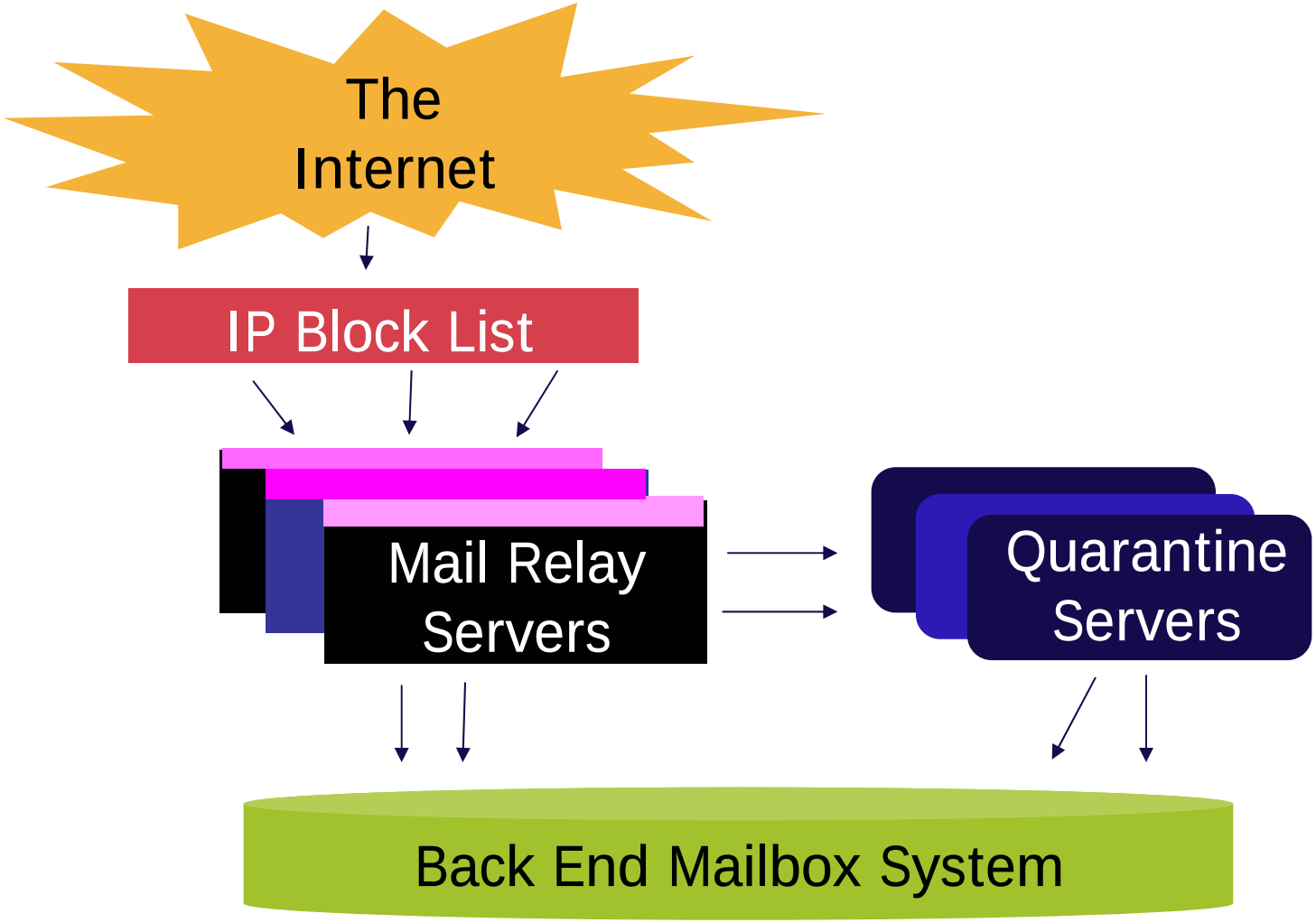
Margot Koschier Romary

July 12, 2007

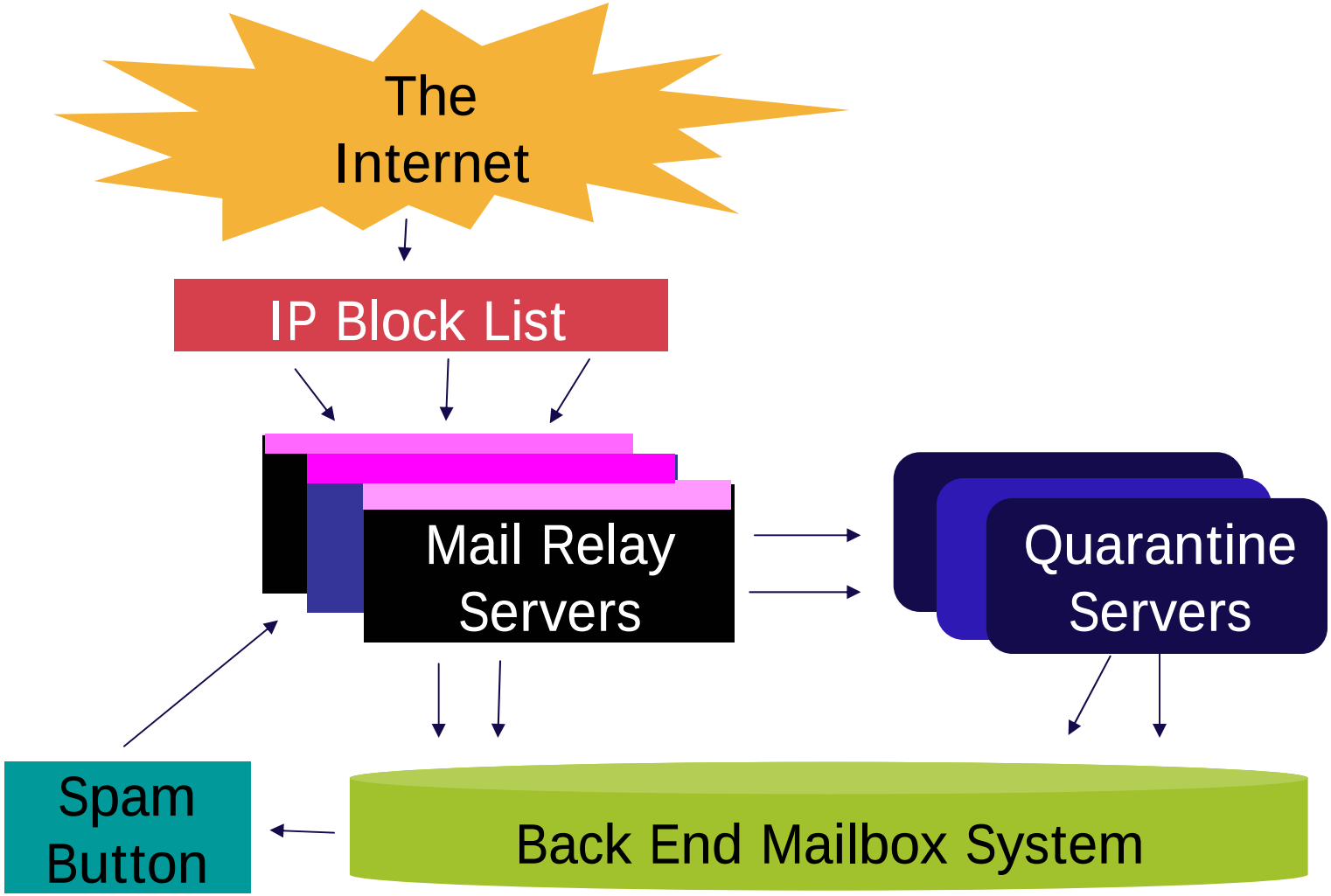
AOL Anti-Spam Infrastructure (c. 1997)



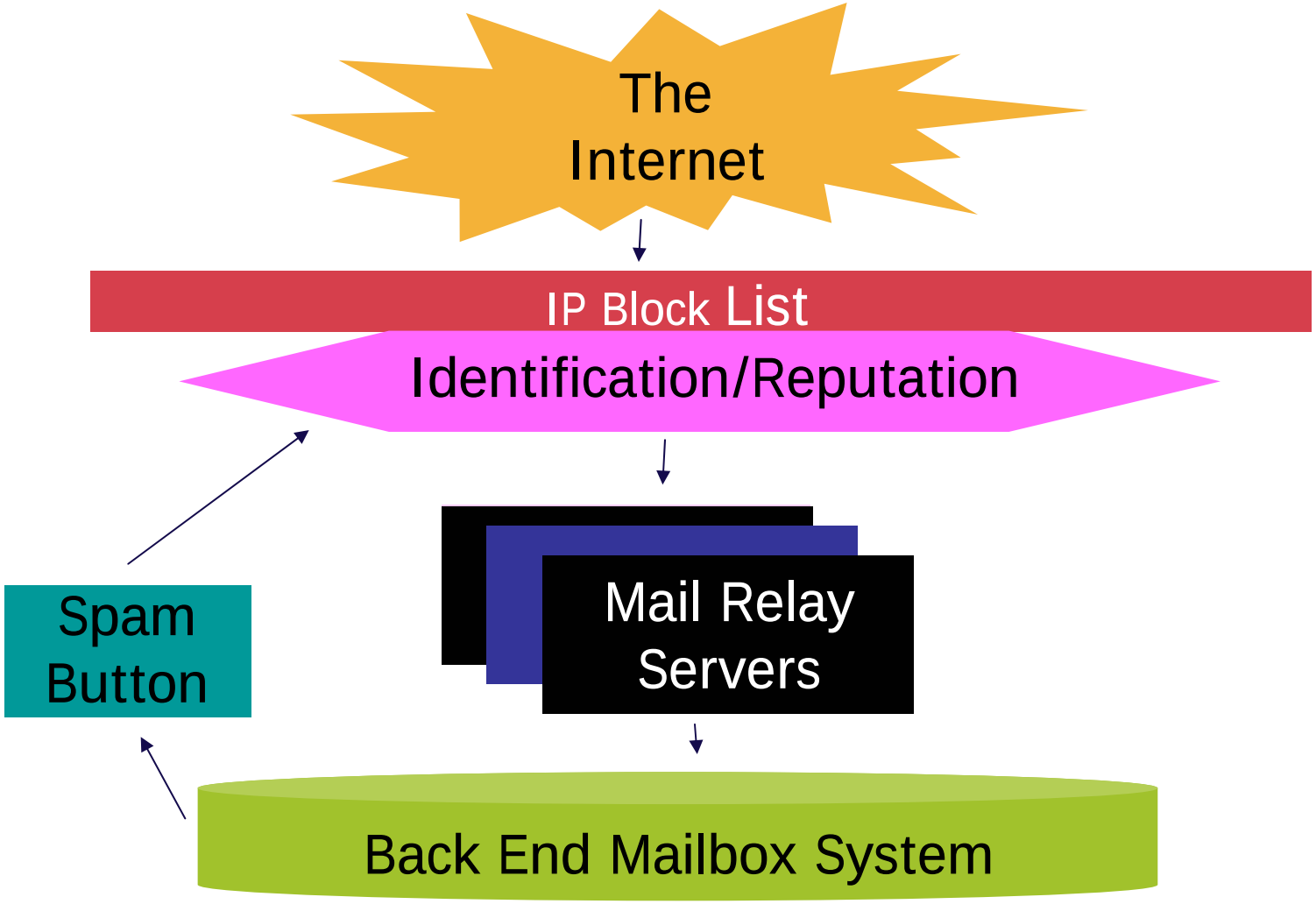
AOL Anti-Spam Infrastructure (c. 2000)



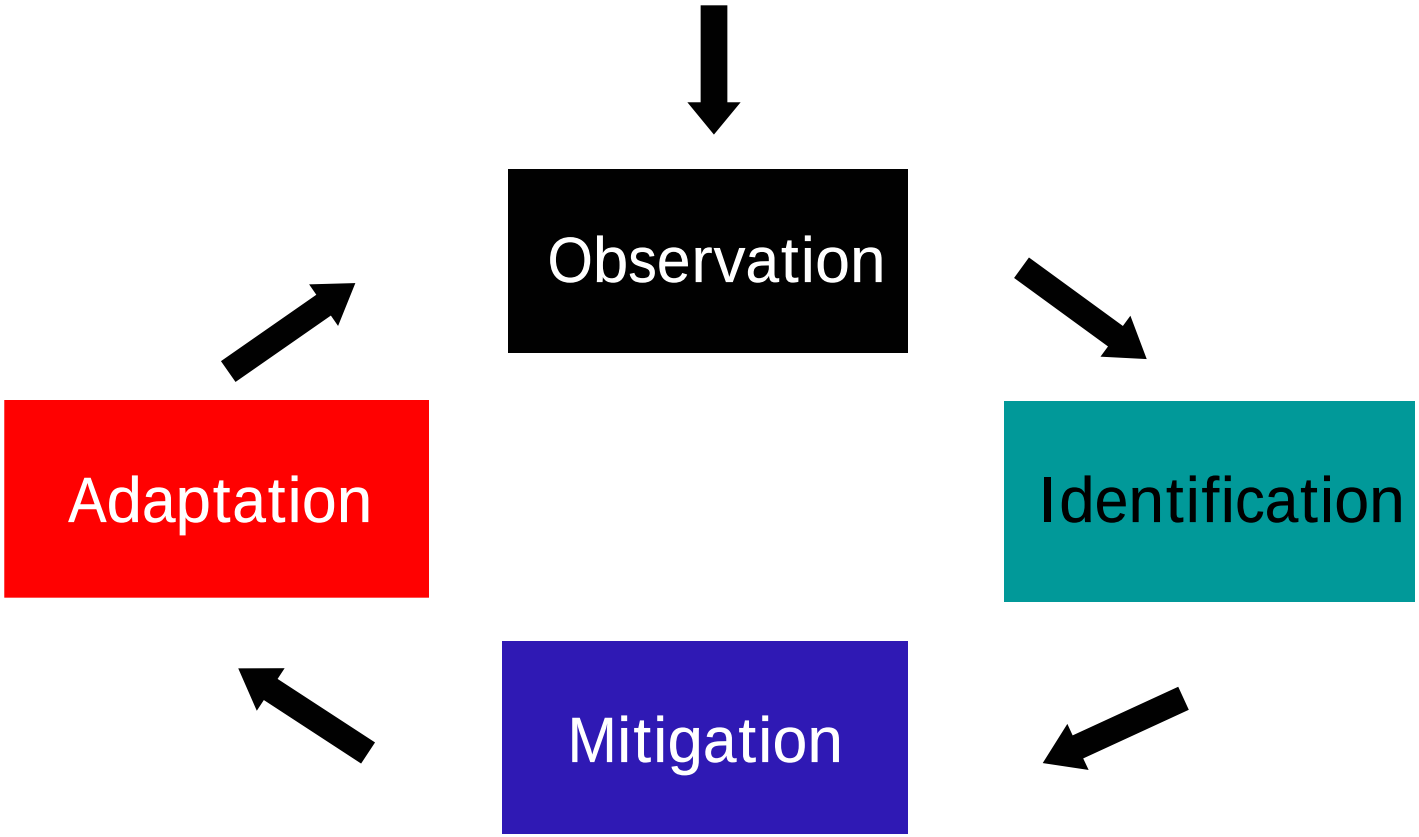
AOL Anti-Spam Infrastructure (c. 2003)



AOL Anti-Spam Infrastructure (c. 2007)



Anti-Spam Technology Evolution



The Current Cycle…

In Summary…

- There is no silver bullet
- Successful anti-spam efforts evolve
- ISPs are present and accountable

Identity/Authentication + Reputation = Success?

Keeping it Out of the Inbox

- **Des Cahill**, Chief Executive Officer, Habeas, Inc.
- **Jim Fenton,** Distinguished Engineer, Cisco
- **Richard L. Gingras,** Chairman, CEO and CoFounder, Goodmail Systems
- **Martha K. Landesberg,** Director of Policy and Counsel, TRUSTe
- **Margot Koschier Romary**, Senior Manager, Anti-Spam Operations, AOL
- **Craig Spiezle**, Director, Online Safety Strategies and Technologies, Microsoft Corporation

LUNCH

Lunch (On your Own):

12:30 PM - 1:30 PM