

2008 Leadership
Series Webinars



Email Deliverability and Its Impact On Your Bottom Line



Featuring Mark DiMaio
Deliverability Expert





Agenda

- **What is Deliverability?**
- **Why should I care about Deliverability?**
- **How does Deliverability impact my results?**
- **What can be done to improve Deliverability?**
- **Q&A**



A photograph of a person's hands using a computer mouse and keyboard. The image is slightly blurred and has a light blue border. A semi-transparent orange horizontal band is overlaid across the center, containing the text "What is Deliverability?".

What is Deliverability?



Deliverability – What is it?

- **Deliverability = percent of communications that actually deliver to the recipient's inbox**
- **Why is deliverability important to non-profits?**
 - Email is a primary and cost effective medium for online donor and marketing communications

Acceptance by Domain + Placement in Inbox =

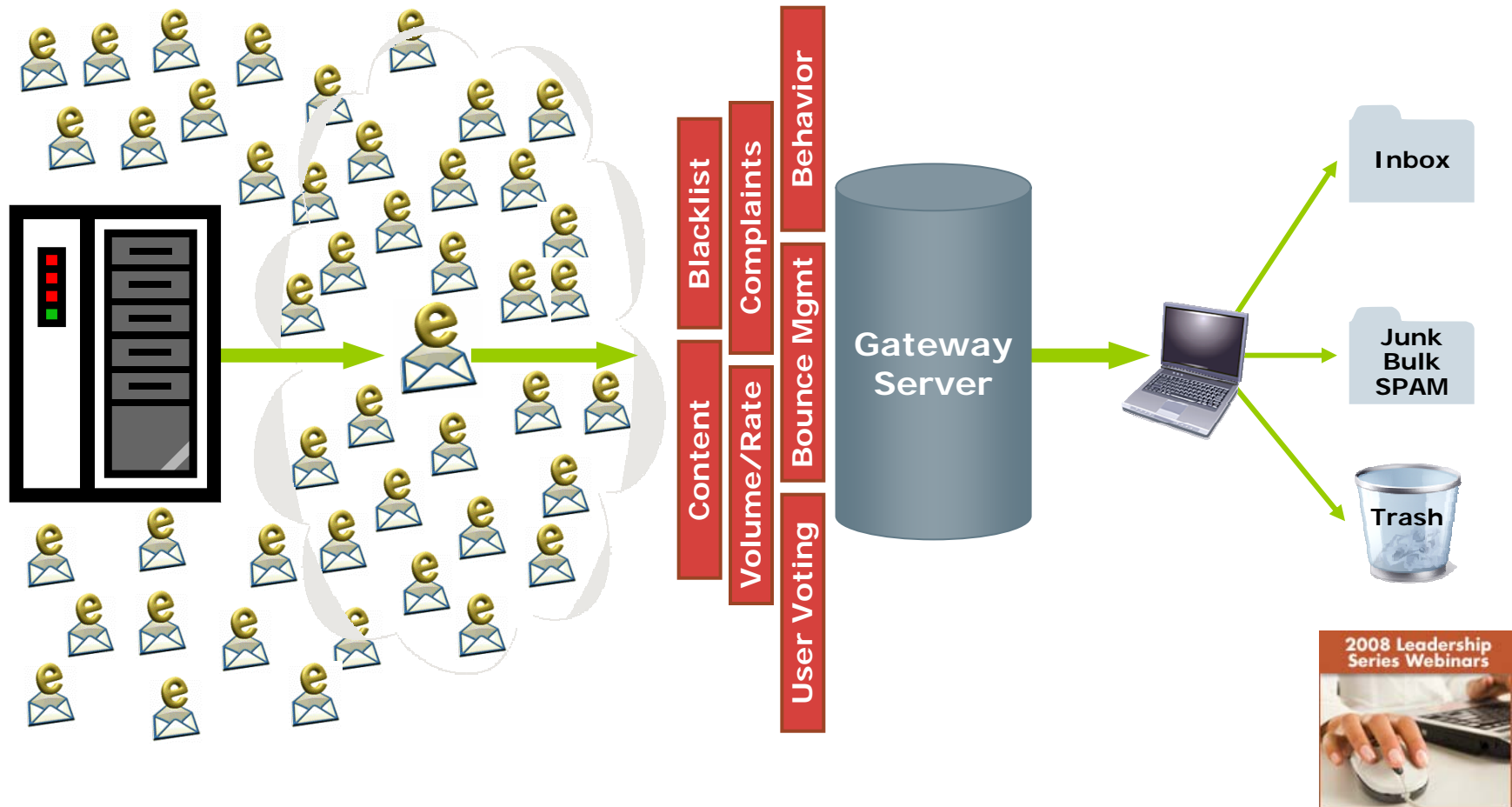
- Implied legitimacy
- Images and links render on screen
- Higher response and results





The Good, the Bad – It All Gets Ugly!

- Receiving domains and members have to distinguish the “good” from the “bad”





Is 100% Deliverability Achievable?

Spam
Software

Address Churn
(33-40% per yr)

Internet
Traffic
& Outages

NO.

But why?

Authentication

Multiple
Addresses

Real-Time Blackhole Lists

User-Specified
Filters

ISP Filtering:
Volume
Bounce
Complaints
Trap Addresses

Domain
Policy

2008 Leadership
Series Webinars





What is a Whitelist vs. Blacklist?

WHITELIST

vs.

BLACKLIST

Only certain ISPs:
Yahoo!, AOL, NetZero, Juno,
RoadRunner, etc.

Unregulated list of perceived spam
sources: include IP addresses,
domains, URLs

Guidelines that a sender must
follow for preferential acceptance
and placement

Listings/blocks happen without
investigation; Membership is open
to everyone

Helps, but does not guarantee
Inbox placement; ***Not a silver
bullet for Deliverability***

Automated Monitoring & Human
Intervention needed to unblock in
most cases

Other ISPs have certain protocols that
help when followed...

2008 Leadership
Series Webinars



A photograph of a person's hands using a computer mouse and keyboard. The image is slightly blurred and has a semi-transparent orange banner overlaid across the middle. The banner contains the text "Questions?".

Questions?



Why Should I Care?



Why Is All This Necessary?



90% of all
email on
the web
is SPAM

Who decides what is Spam?

Domains:

- Unsolicited
- Inappropriate
- High bounces
- Too much
- Complaints

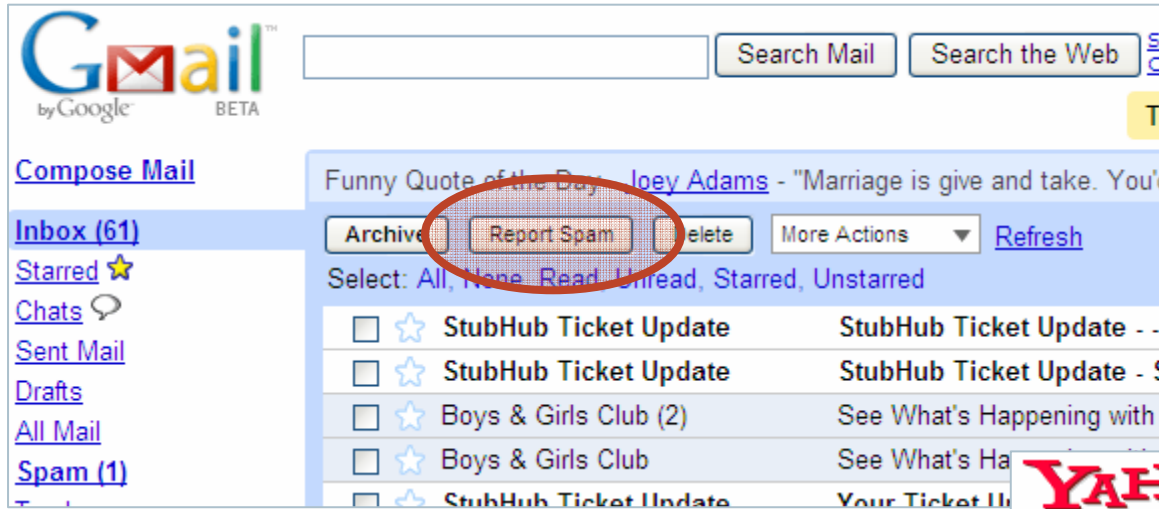
Email Account Owner:

- Unsolicited
- Inappropriate
- Too much from one sender
- Fast way to unsubscribe

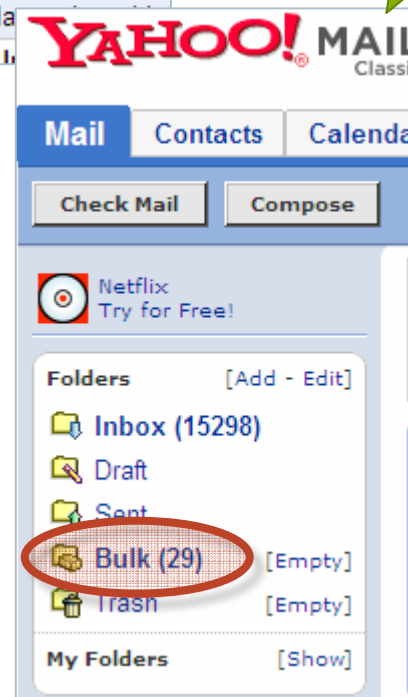
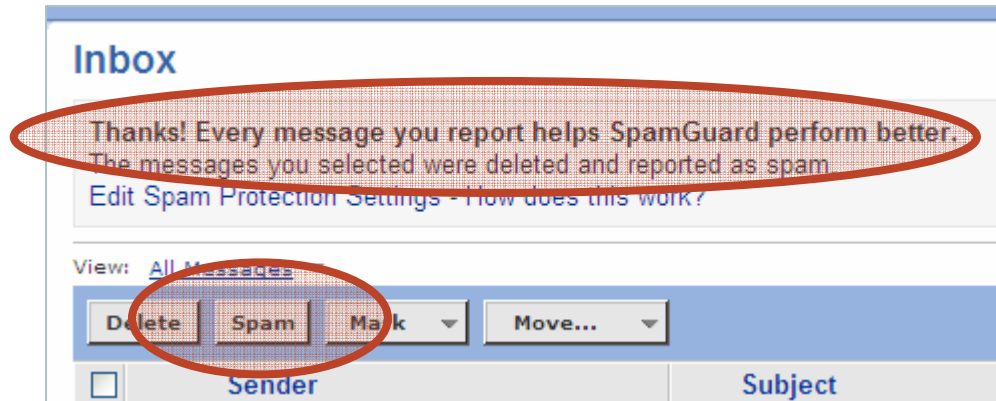





ISPs Make It Easy to Cry "Spam!"



25% simply want to unsubscribe



A photograph of a person's hands using a computer mouse and keyboard. The image is overlaid with a semi-transparent orange banner in the center containing the text "How does it impact my results?". The background is a blurred office setting.

**How does it impact
my results?**



How does Deliverability Impact My Results?

Deliverability has a direct monetary impact on both **revenue** and **cost**.





Sample Email ROI: Inbox vs. ?

- Let's take a simple example...

	Good Deliverability	Poor Deliverability
Sent	20,000	20,000
Delivery Rate	97%	80%
Delivered	19,400	16,000
Click-through Rate	4%	4%
Conversion Rate	0.28%	0.28%
Avg Gift Amount	\$500	\$500
Donations	\$27,160	\$22,400

The difference for this one campaign is \$5,000





Cost per Acquisition Must Be Considered

- **The loss financially is staggering...**

Original List Amount	20,000
Permanently Undeliverable/Hard Bounces	2%
Remaining Addresses	19,600
Average Conversion	0.28%
Average Gift Amount	\$500
Lost Donations for One Campaign	\$560
Cost of Acquisition - \$20/address	\$8,000
Total Lost for One Campaign	\$8,560
Lost Opportunity for One Year (2x/mo)	\$205,440





Over Time, What Does That Mean?

Lost donors

More work

Lost prospects

Missed donations

Missed goals

Diminished advocacy

Wasted employee
time (lost \$\$\$)

Lost lifetime
donations



(Profit)





Polling Question #1

- **In a recent survey of one of Papilia's clients, donors who engaged online as well as offline, gave on average:**
 - Just as much as those who only interacted offline
 - Twice as much
 - Five times as much
 - Half as much





Polling Question #1

- **In a recent survey of one of Papilia's clients, donors who received email gave on average:**
 - Five times as much as those who only receive offline communication

“Donors who donate offline but receive communication online tend to give **twice as much** as those who only receive communication offline.”

- Integrating Online Fundraising with Direct Marketing, Convio & StrategicOne
-January 18, 2007





Questions?

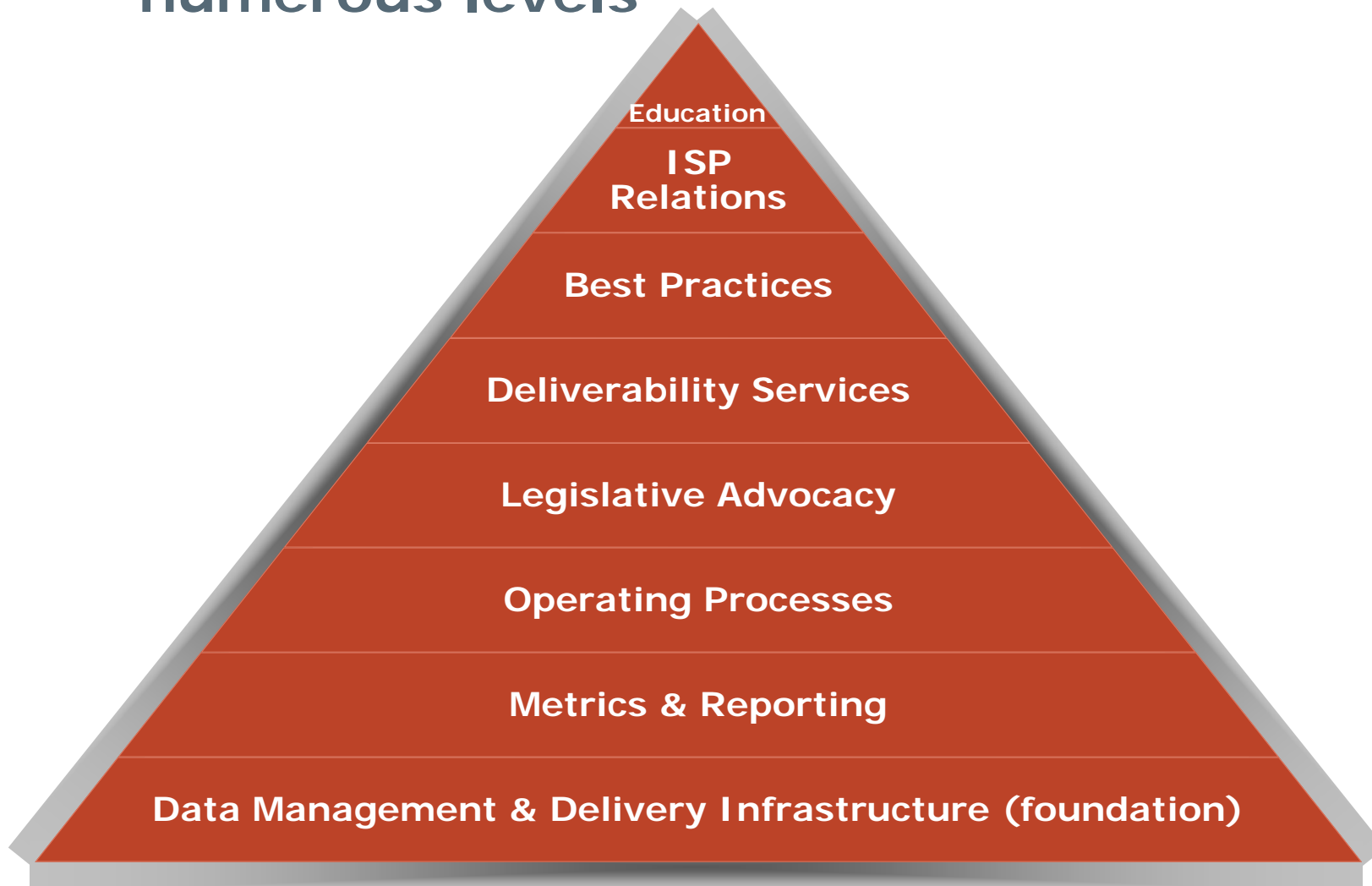


What can be done?



A Holistic Approach to Deliverability

- **Deliverability must be addressed on numerous levels**





Practice Good Data

Data
Capture

Hygiene
Rules

Source

Permission

Expectations

Opt-outs

Address
Updates

Data	Single entry, verification, syntax (@, .)
Source	Rented Lists, Website, Partner Sites
Permission	"Yes! I want to receive updates about the great work you're doing!"
Expectations	Set what content and frequency should be expected, and follow them
Opt-outs	2 options (snail mail address & "click here") and completed within 10 days
Address Updates	Auto-replies, Services (National Change of Address, Return Path, etc.)

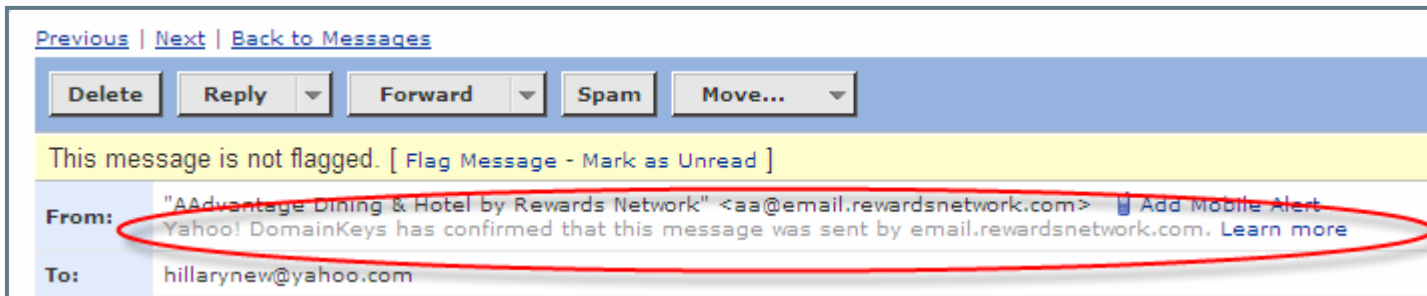
2008 Leadership
Series Webinars





Authentication: Prove Who You Are

- Authentication was first created to help combat “spoofing” or “phishing”
- Spammers could pretend they were a legitimate company



- Includes:
 - Domain Keys: Yahoo!, Gmail, AOL
 - Sender ID: Hotmail/MSN
 - SPF: AOL, Gmail





What Can Be Done: Partnership

Action	Client	Vendor
Ensure Good Data Management	X	
Authentication: Sender ID, SPF, Domain Keys		X
Build and maintain a Good Reputation with the receiving community and recipients	X	X
ISPs technical guidelines		X
Spam Complaint Feedback Loop with ISPs		X





Polling Question #2

- **If someone provides you with their business card containing their email address, the suggested best practice is:**
 - Mail them whenever you want
 - Send them a welcome email inviting them to opt in to future communications
 - Send them only one-to-one (personal) emails
 - Not contact them via email since they haven't given you permission





Polling Question #2

- **If someone provides you with their business card containing their email address, the suggested best practice is:**
 - Mail them whenever you want
 - *Send them a welcome email inviting them to opt in to future communications*
 - Send them only one-to-one (personal) emails
 - Not contact them via email since they haven't given you permission
 - **All of the above, but we recommend #2**





CAN-SPAM Defined

The screenshot shows an email from ODC (Older Driver's Center) with the following content:

From: ODC [oldfeedback@my-websites.org]
To: Barbara Perry
Cc:
Subject: Make ODC Your Own!

Check out the latest from ODC! [Get Started Now](#)

Dear Friend of ODC,

ODC's impact in the community can be felt in a variety of ways; we are a dance company, a school and a theater. As a friend and supporter of ODC, we want to keep you informed about all our programs and special events, as well as offer you exclusive opportunities to participate, according to your interests.

How does this NEW service work?

First, you answer one question:
- Of all we do what interests you most?

Then, we provide you with regular updates and news according to your particular interests.

Also included, is a special area of our website, personalized specifically for you, called **MY ODC**.
Here you can:
• Get more information and give us feedback
• Make secure online donations and track your giving history
• ... and more!

Your password is: CYDJWX
Please change your password in the MY Profile section upon first login.

MyODC
▶ Get news you care about
▶ See your gifts at work
▶ Tell a friend

[Click here](#) to access MY ODC

We hope you enjoy the experience and look forward to hearing your feedback.

Sincerely,

Brenda Way
Founder and Artistic Director

© 2006 ODC. All rights reserved.
351 Shotwell Street, San Francisco CA 94110 Ph: 415.863.6606

A note about privacy: We assure you that we will never sell or give your information to anyone else. We assure that all your data is kept private and secure. The occasional email messages we send are an important benefit of the program but anytime if you would like to unsubscribe, you can simply click on the link that appears in the footer of each message or email oldfeedback@my-websites.org. Follow this link to read our full [privacy policy](#).

PAPILIA

1) "From" line clearly represents the NPO

2) Subject line clearly represents the content of the body of the email

3) Message includes NPO's valid street address as a means for the supporter to contact the NPO. Best practice is to use the NPO's physical address.

4) Message includes an email address to which supporters can send requests to opt out of further emails. A link to an opt-out page is also acceptable.

5) Message includes a link to the NPO's privacy policy.

- **CAN-SPAM (2003) = Controlling the Assault of Non-Solicited Pornography & Marketing**
- **Regulates the form of commercial and non-profit email**
 - <http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm>
 - <http://www.fcc.gov/cgb/consumerfacts/canspam.html>
- **Please consult your attorney for all legal advice**





Common Monitoring Tools

Inbox Tracking	Where does the email go when sent (inbox vs. junk)
Spam Scoring	Scores content and coding in HTML to predict spam triggers
Blacklist Monitor	Identifies appearance on numerous blacklists
Inbox Viewing (multiple ISPs)	Shows various email views at a number of ISPs
ISP Status	Identifies typical arrival time and uptime of ISPs





What You Can Do Today

The Good Deliverability Partnership

- Practice Good Data Management
- Set correct expectations when capturing email address
- Subscription management – let people sign up for what they want
- Process unsubscribes and changes of address asap
- Analyze opt-out data
- Analyze and possibly remove non-responders
- Send snail mail to recapture invalid/ unsubbed addresses



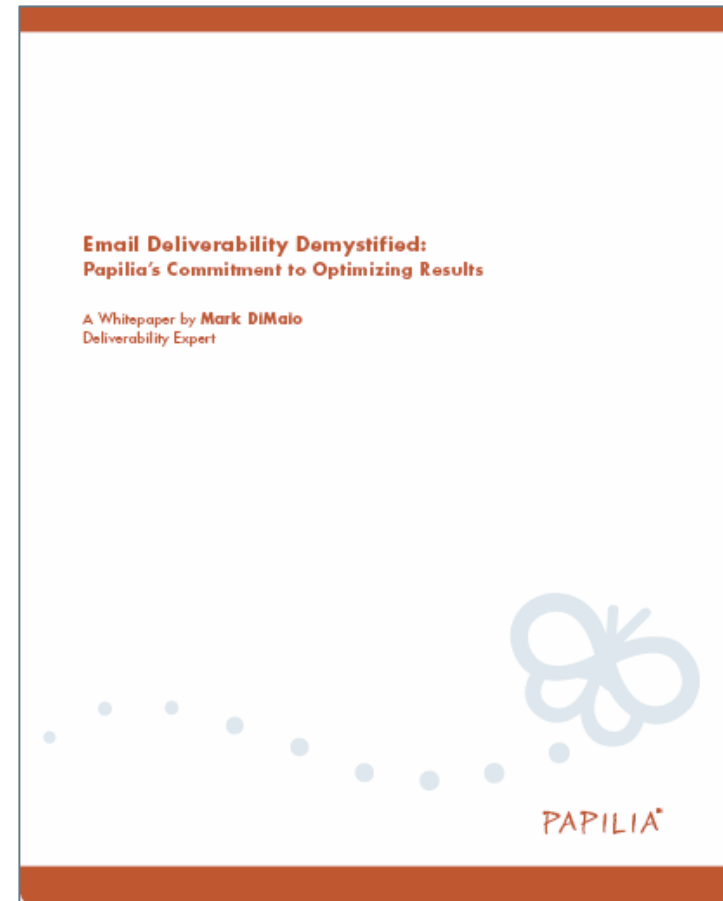
A photograph of a person's hands using a computer mouse and keyboard. The image is slightly blurred and has a semi-transparent orange banner overlaid across the middle. The banner contains the text "Questions?".

Questions?



Additional Resources

- **Email Deliverability Whitepaper**
 - www.papilia.com
- **FREE Papilia Service – Online Tax Receipts**
 - www.papilia.com/receipts
- **Papilia Integrated Direct Mail**
 - <http://www.papilia.com/web-mkt/addon-mailer.php>





Additional Resources

- **Microsoft Junk Email Filter Readme**
 - <http://office.microsoft.com/en-us/help/HA010450051033.aspx>
- **Email Marketing Resources**
 - MarketingSherpa
 - eMarketer
 - Forrester
 - Direct Marketing Association
 - TowerData – email list hygiene





Glossary of Terms

- **Block**

- Mechanism or determination by receiving domain or recipient not to accept email based on predefined criteria, such as abuse complaints, volume, message content, etc. Blocks can be dynamic or permanent in nature.

- **Challenge Response (C/R)**

- One method which may be used by internet service providers (or by specialized services) and end users to combat spam is to require unknown senders to pass various tests before their messages are delivered. These strategies are termed challenge/response systems or C/R.

- **Complaint**

- Member determination that email is SPAM which sends a formal notification to hosting domain or ISP and, in some cases, the sender (frequently in the form of a feedback loop-see Feedback Loop).

- **DNS (Domain Name System)**

- The Domain Name System is the system that translates Internet domain names into IP numbers. A "DNS Server" is a server that performs this kind of translation.

- **Domain Keys/Domain Keys Identified Mail (DK/DKIM)**

- An e-mail authentication method that computes a digital signature which is added to the message header. The receiving mail server obtains the sender's public key from the DNS system to validate the signature. In 2004, Yahoo! began to sign all outgoing mail with DomainKeys headers.

- **Domain Keys Identified Mail (DKIM)**

- Yahoo!'s DomainKeys was combined with Cisco's Identified Internet Mail system, which maintains signature consistency, to become DomainKeys Identified Mail (DKIM). DKIM is backward compatible with the DomainKeys system.





Glossary of Terms

- **Domain Name**

- The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general. A given machine may have more than one Domain Name but a given Domain Name points to only one machine.

- **Feedback Loop (FBL)**

- Mechanism by which ISPs route member complaints back to the sender for member removal from lists.

- **Gateway**

- The technical meaning is a hardware or software set-up that translates between two dissimilar protocols, for example America Online has a gateway that translates between its internal, proprietary e-mail format and Internet e-mail format.

- **IP Number (or Address) (Internet Protocol Number)**

- Sometimes called a dotted quad. A unique number consisting of 4 parts separated by dots. Every machine that is on the Internet has a unique IP number - if a machine does not have an IP number, it is not really on the Internet. Many machines (especially servers) also have one or more Domain Names that are easier for people to remember.

- **ISP (Internet Service Provider)**

- An institution that provides access to the Internet in some form, usually for money.

- **Permission**

- Recipients consent to receive email from a company or other sender. There are many levels of permission ranging from implied to double opt-in.

- **Seed list**

- Set or defined list of email addresses in various domains, deployed alone or with actual production email used to help determine rendering, acceptance, and placement of email.





Glossary of Terms

- **Sender Policy Framework – (SPF)**

- Sender Policy Framework (SPF) is an anti-spam approach in which the Internet domain of an e-mail sender can be authenticated for that sender, thereby discouraging spam mailers, who routinely disguise the origin of their e-mail, a practice known as e-mail spoofing.

- **SenderID – (SID)**

- The Sender ID Framework is an e-mail authentication technology protocol that helps address the problem of spoofing and phishing by verifying the domain name from which e-mail is sent. Sender ID validates the origin of e-mail by verifying the IP address of the sender against the purported owner of the sending domain.

- **Server**

- A computer, or a software package, that provides a specific kind of service to client software running on other computers.

- **SMTP -- (Simple Mail Transfer Protocol)**

- The main protocol used to send electronic mail from server to server on the Internet.

- **Spam (or Spamming)**

- An inappropriate attempt to use a mailing list, or other networked communications facility as if it was a broadcast medium (which it is not) by sending the same message to a large number of people who didn't ask for it. The term probably comes from a famous Monty Python skit which featured the word spam repeated over and over. The term may also have come from someone's low opinion of the food product with the same name, which is generally perceived as a generic content-free waste of resources.

- **Trap address – (SPAM trap, honey pot, bait account)**

- Non-opted in address used by RBLs and ISPs to "catch" spammers. If a sender mails to one of these addresses, the receiver considers the mail SPAM since they never gave permission for the mailing.





Permissions - Defined

- **Double Opt-in**
 - Double opt-in (aka confirmed opt-in) is considered the industry gold standard. Subscribers receive a confirmation email after sign up which requires further action on their part prior to being added to a list.
- **Notified Opt-In**
 - Notified opt-in is very similar to single opt-in with the addition of one extra step. In the notified opt-in scenario, a confirmation or welcome email is sent to the subscriber allowing them the opportunity to opt-out. If there was a malicious or errant sign up, or if the requester simply changed their mind, they would be able to take action in order to avoid future mailings.
- **Single Opt-in**
 - Subscribers indicate interest in receiving mail and are added to a specific list. This permission may be given via an Internet or off-line sign up. No other steps are required either from the requestor or the sender prior to mailings.
- **Implied**
 - Assumes the recipient wants to receive email since they did not take any action upon sign up to opt-out (i.e. uncheck pre-selected box, etc.). Generally not considered an industry best practice since this is the weakest method of "permission".
- **Generic/General**
 - Subscribers indicate interests on a partner or co-registration site, however they might not necessarily know who might be sending them email. Since the sign up might be unmemorable and mail non-relevant, often time recipients think they are receiving unsolicited email.

*Single, Implied, and Generic/General Opt-in have a number of potential issues since email address verification is not performed by the sender, which may allow malicious or unintended sign ups. Data entry errors may also cause malformed email addresses resulting in undeliverable email, or email being sent to an unintended recipient. These methods may also result in mailing to spam traps; addresses maintained by ISPs, domains, and realtime blackhole lists (RBLs) who have not signed up to receive email. If these traps are hit, they automatically consider the mail spam and act accordingly. Old lists, poor data sources, malicious sign up may contribute to the introduction or spam trap addresses to a list.

