

BY IRENE CHERKASSKY

CERTIFIED DELIVERY

AUTHENTICATION HELPS GET YOUR E-MAIL CAMPAIGNS TO INBOXES



It's no secret. Every e-mail marketer knows spam and phishing pose the biggest challenge to getting legitimate e-mail into recipients' inboxes today.

In a recent report released by Austin, Texas e-mail service provider, Skylist, 72 percent of e-mail marketers responding to the company's survey cited deliverability as their greatest challenge. According to New York City e-mail service provider Return Path's Mailbox Monitor service, in 2004 an average 22 percent of permission-based commercial e-mail did not reach inboxes, by virtue of being blocked or filtered to the recipients' junk/spam folders by ISPs.

The truth is, there are no magic bullets that will get you delivered. However, most direct marketers are learning that implementation of the emerging authentication protocols is a vital step in boosting deliverability, now and in the long term.

"Authentication protocols are the key innovation in the last year to year and a half," says Quinn Jalli, director of privacy and ISP relations for digital marketing solutions provider Digital Impact, in San Mateo, Calif. "They're the first major step in ending the spam crisis, because once you're able to identify positively who a sender is, you're then able, as the next step, to attach a reputation to that sender."

Simply put, authentication helps ISPs verify that a sender of an e-mail is indeed who it claims to be, thereby facilitating the delivery of legitimate

e-mails and reduction of fraudulent and unwanted mail.

The ABCs of SPF and SIDF

Several technological options recently have emerged to help ISPs verify the identity of e-mail senders. The easiest of these protocols to implement is the Sender Policy Framework (SPF). Used by ISPs such as AOL and Earthlink, this is an open-source solution, free from licensing requirements. SPF requires e-mail senders to publish their SPF records in the Domain Name Service (DNS). DNS specifies which computers are authorized to send e-mail from a specific domain. When the e-mail passes through the DNS server, it's compared to the SPF record for that domain to verify that the IP addresses listed as authorized to send e-mail from that domain match those listed in the e-mail header.

"SPF is the leader in that it has the widest adoption and it was the first one in the marketplace," says Bill Nussey, president and CEO of e-mail service provider Silverpop, in Atlanta, Ga. Marketers can publish their SPF records by having either their e-mail service provider or internal IT staff go to a site such as www.spf.pobox.com, which takes them through the process.

The second of the IP-based authentication solutions is Sender ID Framework (SIDF), which combines SPF with Microsoft's proprietary Caller ID solution. Microsoft implemented SIDF earlier this year for Hotmail

and MSN. This solution also requires senders to publish their SPF records and adds an extra layer of protection by authenticating the Purported Responsible Address (PRA) of the e-mail, which essentially is the visible "FROM" portion of an e-mail header.

Because they are cost-effective and easy to implement, SPF and SIDF have made inroads to wider adoption by ISPs and marketers alike. According to Bigfoot Interactive's chief marketing officer, Michael Della Penna, at the New York City e-mail service provider's recent PROfile E-mail Summit, Microsoft reported that approximately 10 percent of all e-mail sending domains are compliant with SPF/Sender ID, and that these domains represent approximately 25 percent of all incoming e-mail volume at Hotmail.

"Sender ID has the blessing of the major ISPs because it's the accumulation of both SPF and Caller ID," points out Tricia Robinson, chief marketing officer for e-mail marketing solutions provider Socketware Inc., in Atlanta, Ga. "In terms of adoption by the ISPs, Sender ID is going to have a much more positive impact than SPF."

Mastering DomainKeys

In comparison to SPF and SIDF, cryptographic, signature-based solutions, such as Yahoo!'s DomainKeys or Cisco's Identified Internet Mail (IIM) are viewed as more robust authentication options both by the ISPs and many ESPs. "We view IP-based solutions

continued on page 55...

like SPF and Sender ID as critical foundational authentication layers, with cryptographic solutions like DomainKeys as a stronger complementary layer,” says Della Penna. Yahoo!’s DomainKeys requires e-mail senders to generate public/private key pairs, and to publish the public keys in their DNS records. Matching, private keys are stored in a sender’s outbound e-mail servers. When these servers send out an e-mail, the private keys generate a digital signature of the message that is pre-pended as a header to the e-mail. ISPs then can check if an incoming message’s private key matches the public key published in the DNS records. This, according to Yahoo!, not only ensures the message was sent by an authorized sender, but also that the headers and content were not altered during the mailing process, something protocols such as SPF and SIDF cannot guarantee.

The IIM system works much the same way, except the public key is stored in the e-mail sender’s outbound

e-mail servers, while the private keys are stored in the DNS record. According to Cisco, storing the generic public key in the e-mail header instead of producing private key-based signatures each time a message is sent would take fewer computing resources from e-mail senders, compared to DomainKeys.

Yahoo! and Cisco currently are

working to merge the two protocols to create an even more effective cryptographic solution. Although more effective, these solutions do require greater investment in e-mail delivery infrastructure, which, in part, has slowed their implementation by marketers. “When you’re looking at an overtaxed IT

continued on page 56...

The Path to Authentication

Learn more about authentication protocols by visiting the following sources online:

www.spf.pobox.com/forsysadmins.html—for a description of Sender Policy Framework and a step-by-step guide to becoming SPF compliant.

www.microsoft.com/mscorp/safety/technologies/senderid/overview.mspx—for further information on Microsoft’s Sender ID Framework.

<http://antispam.yahoo.com/domainkeys>—to learn more about Yahoo’s DomainKeys.

www.identifiedmail.com—to learn more about Cisco System’s Identified Internet Mail.

www.postmaster.aol.com—for the latest information on AOL’s authentication requirements and policies.

www.truste.org—to learn more about authentication issues from this independent, nonprofit privacy advocacy organization.

department, it's easier for them to implement Sender ID than it is to implement domain keys," describes Robinson.

Word on the Street

Not surprisingly, marketers may be wary of investing in an infrastructure that is still a work in progress and are likely to wait for a more definitive solution to emerge. Tim Kiss, director of one-to-one marketing for Atlanta, Ga.-based catalog and online food marketer HoneyBaked Hams, offers a pragmatic perspective on the evolving state of authentication. HoneyBaked Hams began e-mailing its customers in 2000. Its first efforts were primarily discount-based. The marketer since has developed more actionable and personalized e-mail campaigns. Although its e-mail budget has grown to represent 10 percent to 11 percent of its total mail-order sales, the marketer has experienced a decline in response rates. Kiss attributes this in part to spam filters.

"We're starting to see that there is

not going to be a one-fix technology that's going to separate us from the spammers," says Kiss. "But we've also started to see that if we don't start to do some of these things, we're going to be blocked out." The marketer therefore has implemented Sender ID

"Authentication protocols are the key innovation in the last year to year and a half."

—QUINN JALLI, DIGITAL IMPACT

and is SPF compliant.

Kiss is more reticent about DomainKey implementation. "Sooner or later technology will come up, but we're just preparing for the long haul, and until we find something that's 100 percent flawless, we're not ready to invest," he says.

However, the other side of the deliverability equation for HoneyBaked Hams is relevancy. "We started to focus our efforts on making our e-mails

as compelling as possible," says Kiss. "Consumers have to understand that there's some value in there for them."

Dawn Bronkema, senior CRM specialist for retail and grocery marketer Meijer Inc., in Grand Rapids, Mich., offers her perspective: "E-mail deliverability issues are quickly becoming a roadblock to maximizing the use of e-mail." She does not, however, see the current, available authentication options as a cure-all. "All good ideas, but in the end there are always programmers that can program around what others have done," she says.

Bronkema suggests education is vital, as is getting decision makers behind any anti-spam/deliverability protocol for any solution to work in the long term.

Incentive to Authenticate

Whether you choose SPF, SIDF or take the plunge into DomainKeys or IIM, implementing any kind of authentication protocol is no longer an option. Rather, these technologies

continued on page 80...

E-MAIL...continued from page 56

quickly are becoming the first steps in the legitimate e-mail marketer's set of best practices.

In a white paper titled "E-mail Authentication: Actions You Need to Take Today," Return Path describes the basic steps to authentication:

1. Perform an audit of all domains and subdomains used by your company.
2. Have your IT team publish the appropriate record.
3. Validate your SPF and/or SIND record.
4. Check your log files for problems.
5. Update records as your environment or the authentication requirements change.

"Definitely, at the very least, ensure accurate SPF publication today. It's simple, low-cost and actually remarkably low-tech to do so," advises Bigfoot Interactive's Della Penna. "Moreover, there's now the very real possibility that not being compliant or publishing your SPF records the wrong way, can result in blocking or 'junk' folder placement at Hotmail and MSN. This

will become the case elsewhere as more and more ISPs implement these solutions."

He cites reduction in false positives and better delivery assurance as additional incentives for marketer authentication compliance, especially as authentication gets tied to white listing requirements. "Marketers need to understand the value proposition and benefits of compliance," says Della Penna. "We believe accountability will increasingly be tied to authentication, with nonauthenticated e-mail being subjected to additional filtering hurdles compared to authenticated e-mail. Therefore, there may be significant ROI and relationship ramifications for those companies that haven't authenticated."

E-dialogue's director of privacy and ISP relations, Rick Buck notes, "At some point in time, some subset of them needs to be defined as the defacto standard across marketers and ISPs, literally around the world, that says this is going to be the baseline of information we use to say this is authenticated. When that is able to happen,

you'll see a lot less fraudulent e-mail and, in fact, potentially, no fraudulent e-mail in our mailboxes."

While authentication remains in flux, however, there's every incentive to take advantage of the benefits each option affords.

"Most people are coming around to the view that there is no reason to have just one [authentication protocol] and that multiple authentication standards are as good, or better than, having one dominant one," suggests Silverpop's Nussey. David Daniels, research director at JupiterResearch in New York City, agrees: "The best solution is for the ISPs to use all of them, or for these standards to be blended into one protocol."

Della Penna concludes, "Authentication is not the silver bullet, but it is a critical aspect of the ongoing multifaceted approach to combatting spam and e-mail fraud. Perhaps most importantly, authentication will play a vital role in helping marketers and ISPs preserve consumers' trust in the e-mail medium."