

## WHY YOUR BANK'S EMAIL BLASTS MAY NOT GET THROUGH

Some issues make messages look like spam

By Steve Cocheo, executive editor and digital content mgr.

Have you ever wondered why your bank's e-mail campaigns don't pull better? It may be that something you're doing makes your messages look like spam, resulting in an email reputation that results in your messages being blocked by recipients' internet service providers (ISPs).

Indeed, according to a new study, banks' campaign emails, as a group, fall into the same reputation ranking as gaming sites. Other mainstream companies suffer from the same affliction, but for a business that relies on trust, online reputation troubles are poison.

Major study finds issues for banks

Return Path, Inc., which works with large-volume email senders, recently completed a study by monitoring data from its Reputation Network over all of 2011. The network is a large group of ISPs who cooperate with the company. The study, 2012 Sender Reputation Benchmark Report: The Power To Be Heard, found that banks were among outliers in the "Sender Score" index that Return Path uses to measure the likelihood that an ISP will permit an email to be delivered, making it past spam filters and other hurdles designed to protect ISPs' customers--the people and businesses that emailers are attempting to reach.

Return Path points out in its report that every ISP uses its own selection of criteria to screen out spam, but that the firm's Sender Score represents a metric with high predictability regarding whether a message will make it to the recipient's inbox. (Once it makes it there, it's up to the recipient to open it or not, of course.)

The firm's study looked at nearly 20 trillion emails sent from 130 million IP addresses. (IP addresses are those of devices connected to the internet.) Over 85% of the messages were classified as spam by ISPs. Return Path defines these not as the "junk" marketing email we often receive, but messages delivered, frequently by anonymous senders, frequently with evil intent.

Return Path notes that most spam comes from botnets, groups of computers hijacked by spammers to use for sending spam in bulk. Such senders often display other telltale signs

to ISPs.

Return Path's Sender Score is an index where the best rating is 100. The average IP address in the study had a score of 25.96. The company likes to compare it to a "FICO score" for email.

Three main factors pull down scores, according to the study:

- &bull; Sending emails to unknown users and email addresses no longer in active use. A managed email list culls such junk, but spammers are going for volume.

- &bull; Complaint rates that go up as more email recipients mark messages as spam, which is recorded by the ISP. This is an issue for banks, as we'll look at further in a minute.

- &bull; Sending emails to "spam traps." These are email addresses set up as decoys by ISPs. They never belonged to anyone but the ISP and so anyone attempting to reach them is suspected of being a spammer.

As noted, many of the "bad guys" show common characteristics that make them obvious spammers. But legitimate senders may fall into a borderline category. "A good percentage of these are spammers," the report states, "but others are legitimate senders who fail to implement deliverability best practices. Inevitably, ISPs will mistakenly identify some of the latter as spammers."

#### Avoiding the borderline

Businesses that find themselves in the space between definite spam and clearly legitimate messages may rank between 60 and 80 on the 100-point scale. Return Path says that when a company's emails fall below 80 points on the scale, as much as 80% of their email messages may fail to make it into targets' inboxes.

"ISPs are understandably eager to protect their users," the report states. "But, in doing so, they may be blocking or filtering emails from legitimate senders. While ISPs continually work to improve their filtering algorithms, the onus is on businesses to improve their deliverability best practices."

Complaints represent the metric that will most likely pull down a sender's score, according to Return Path. After all, it indicates a conscious decision on the part of the ISP's customer to brand a sender as a spammer. Return Path states that its data "show that email senders need to keep their complaint rates at one-tenth of one percent or below in order to avoid negatively impacting inbox placement." (Emphasis added.)

Where do banks rank in this regard? Return Path reports a complaint rate of 3.2% on average--32 times the threshold just mentioned.

Also, banks have a high average "unknown user rate," at 4%. Only gaming and social networking emails hit higher levels. ISPs prefer to see levels less than 2%.

Compounding the matter, for banks, is that recipients, naturally, are very sensitive to issues with email concerning their financial affairs. If a banking email lands in a spam folder at the recipient level, subscribers to the ISP's email service are not likely to mark them as "not spam."

Tips to avoiding spam destiny

Tom Sather, senior director of email research, met with ABA BJ to discuss the report's findings and recommendations. These tips come from the report and from Sather.



from popular bulk emailing websites--can look suspicious.

Bounces that happen over and over don't look good. Return Path suggests setting a limit to the number of times a sender sends to an unknown user hard bounce. One to three such hard bounces at most and then remove the name. And the company recommends reconsidering acquiring email lists from vendors. Their lists frequently contain many inactive email accounts.

Sather says email authentication is important, as well. A key method is DMARC, which stands for Domain-based Message Authentication, Reporting, and Conformance. In brief, it is a means of informing ISPs that the sender uses two mechanisms--Sender Policy Framework and Domain Keys Identified Mail--to verify that its messages are legitimate. For a bank that takes this step, any messages from it not using those mechanisms will be blocked.

Sather says the idea is to make it harder for phishers and other frauds to game the bank's email. They are interested in easy targets.

Another step to take doesn't involve technology at all, simply messaging. The report advises periodically analyzing patterns of subscriber unhappiness. If particular offers or subject lines are driving problems, adjust accordingly.

And in similar vein, Sather warned banks that are aggressive marketers that a heavy email volume to recipients can be annoying and can trigger complaints.

Free online help available

The company also suggests accessing its free service, at [www.senderscore.org](http://www.senderscore.org), which can help a bank determine how their campaigns rank with Return Path and thus with ISPs.