



GET MORE INFO

rpinfo@returnpath.net

1-866-362-4577

Return Path Q2 2008 Reputation Benchmark Report

Executive Summary

The Return Path Reputation Benchmark Report describes actual email performance data for a sample of IP addresses pulled from our cooperative reputation database. We created this report to help quantify the volume of email sent, the quality of the servers sending those messages and how that quality influences deliverability performance.

What we found is that the email universe is a big, ugly, scary place. The volume of email sent everyday is overwhelming, and most of it is spam. Consumers hate spam because it ruins their inbox experience and can cause them harm. Marketers hate spam because it clogs the inbox and gets in the way of their messages. Internet Service Providers (ISPs) and other receivers really hate spam because the process of sorting, routing, filtering and blocking this email is expensive. What's more, they bear the entire burden of this expense.

The good news for commercial senders is that they tend to perform better than the rest. Why? Their attention to email best practices is paying off. The bad news is that lots of good email gets blocked along with the spam and phishing scams. Continued vigilance is essential to ensure that permission email is easily identified as legitimate.

Keeping the world safe for email is a big job. We need all the help we can get. ISPs are stuck sorting the mail so commercial senders need to focus on building and maintaining strong sending reputations. This will help ISPs identify them as good guys and will help their shared customers get the email they want.

Methodology

The Return Path Reputation Data Network processes hundreds of millions of unique IPs from a wide range of volume senders each month. To generate an accurate sample of IPs for this report, a random sample of approximately 2.3 million unique IPs was pulled from our reputation database. This report covers activity on our network from April 1, 2008 through June 30, 2008.

For the purposes of this report we only included data for IPs that generated at least one complaint over the 90 day period. This was done to minimize any complaint rate bias because the rate at which consumers complain varies by ISP. IPs deemed unclassifiable with no reverse DNS were dropped from the analysis.

Definition of Terms

Return Path Reputation Data Network: A cooperative data network that collects and analyzes data from ISPs and other receivers of large volume email. Our network processes more than two terabytes of data every day from receivers representing more than 100 million mailboxes.

Legitimate email server: A valid, static and properly configured email server. This designation does not mean the email coming from this server is good, by any definition of good. The email that comes from legitimate servers runs the full spectrum in terms of permission, content and value.

Illegitimate email server: Hosts that are clearly not intended to be mail servers. Many of these are dynamic IPs.

Unknown email servers: There is not enough data to determine if these servers are legitimate or not.

Delivered rate: The number of messages that the receiving machine accepted (either to the end recipient's inbox or junk folder) divided by the number of messages seen by our receiving sources.

Filtered rate: The percentage of messages reviewed by the receiving machine's filtering system. These messages are ultimately blocked by the receiver, though they get further along in the system than message which are rejected (see next definition).

Rejected rate: The number of messages that the receiving machine blocked from entering their network.

Complaint Rate: Complaint rates are calculated as spam complaints reported by our network divided by delivered mail.

Unknown User Rate: Dead addresses are reported to our network as "unknown user," "no such user" or "invalid address." The unknown user rate is calculated by dividing the number of these dead addresses by the attempted volume of email sent through the Return Path reporting network.

Spam Trap Hits: Number of times an email server attempts to send to a spam trap address, as defined by our reporting network.

Blacklists: Our network tracks IP inclusion on blacklists that we have identified as closely correlating to poor delivery rates. Note that the correlation here is not necessarily because the blacklist is used by many receivers. These blacklists are indicative of reputation problems that cause blocking.

For this report the blacklists included are:

xbl.spamhaus.org
combined.njabl.org
sbl.spamhaus.org
ubl.unsubscore.com
bl.spamcop.net
bogons.cymru.com
dnsbl.sorbs.net
pbl.spamhaus.org
psbl.surriel.com

Analysis

There is a lot of email being sent, and most of it is bad. We don't mean bad as in irrelevant, though there is surely plenty of that too. No, we mean really bad – spam, phishing attacks and other scams.

In our study of email traffic, we found that 46% of email came from hosts which should not be sending mail at all. This includes compromised hosts, dynamic IPs and a variety of other “non-mail servers.”

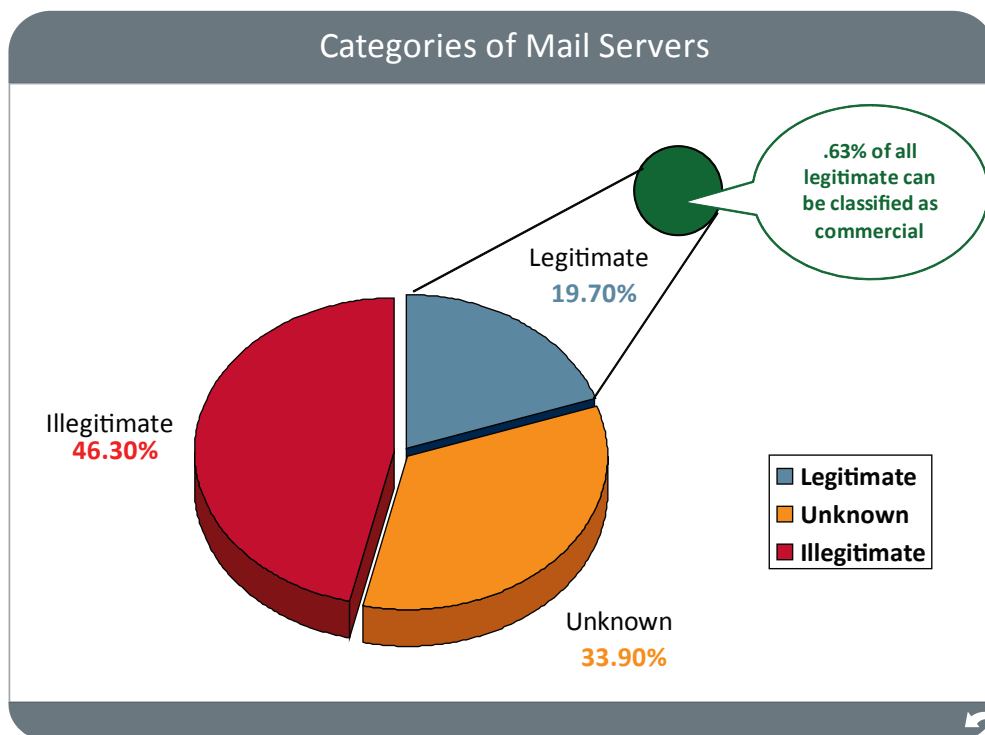
Another 34% of IPs studied were what we call “unknown” – meaning they are not directly classifiable given available data. These hosts do not act like well configured mail servers; so, either they are not legitimate mail servers or they are mail servers with enough problems that leave them in the unknown category due to their behavior. These servers present the biggest problems for ISPs and other receivers because it is difficult to know whether or not to deliver email that comes from them. For commercial senders, deploying email from an unidentifiable server is a recipe for, at best, erratic inbox deliverability.

The final 20% of the email seen came from servers that we can categorize as legitimate, meaning they are real, static, well-configured email servers. These are servers dedicated to sending commercial messages (transactional, content and promotional) as well as person-to-person and corporate communication. But there is still spam in this bucket as well. For example, this category includes known spammers who send mail from these types of static mail servers.

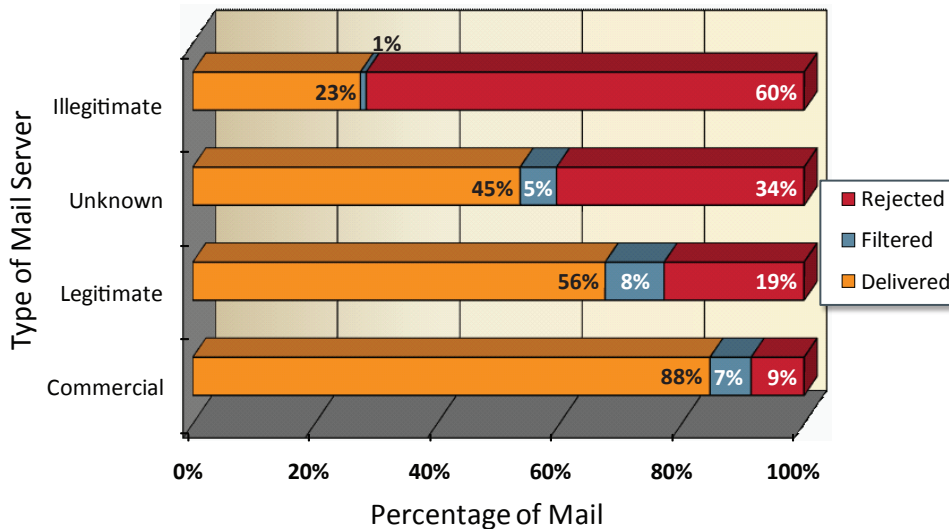
It's worth noting that the email universe as a whole is even worse. For the purposes of this study, we took out data from servers that do not have reverse DNS and are clearly not supposed to be sending email. This bucket represented 35% of the total email seen in our network. Adding this bucket to the illegitimate and unknowns shows that 87% of all IPs sending mail almost certainly should not be.

Not surprisingly, email streams from illegitimate or unknown IPs were far more likely to be rejected or filtered than email coming from legitimate IPs. We found that email coming from illegitimate hosts had average rejection rates of 60% and delivered rates of 23%. Illegitimate hosts actually had low filtered rates – slightly less than 1% on average. This is because this email is easy to identify and reject.

For email coming from unknown hosts, the picture is different. Here we see average delivered rates of 45%, filtered rates of 5% and rejected rates of 35%. This is where the ISPs need to do some heavy lifting by running this email through their filters.



Mail Server Performance by Category



As for legitimate email servers, the averages are 56% delivered, 20% rejected and 8% filtered. Again, ISPs need to scrutinize messages coming from these servers more closely, though here we see a more favorable outcome.

Legitimate email is also less likely to be complained about, with the average complaint rate for these messages being 2.1%. For the unknown category it was 2.6% and for the illegitimate category it was a whopping 3.6%.

Very likely, the reason why complaint rates are not higher for the dynamic hosts is because of complaint rate thresholds at the ISPs; beyond

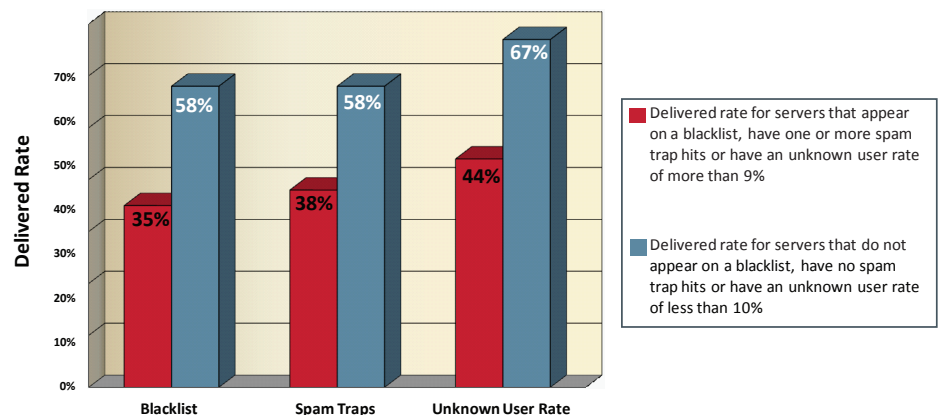
which, ISPs tend to block all email. Blocked email, of course, doesn't generate consumer complaints.

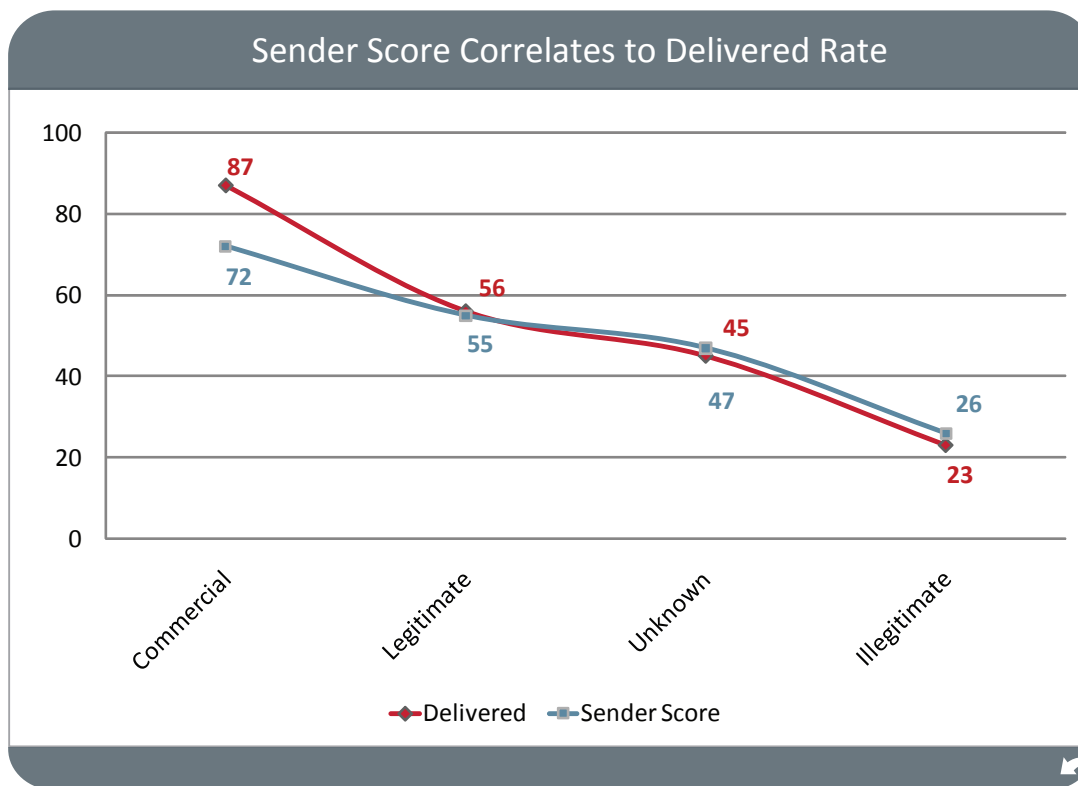
The good news is that commercial mailers who apply best practices and pay attention to reputation metrics enjoy delivery rates that are much higher than average. In fact, we found that for commercial email servers, which is a very small subset of the legitimate stream, the average delivery rates were 88% delivered, 9% rejected and .71% filtered. They also had a much lower average complaint rate of 1.1%.

But it's important to note that seemingly small infractions can doom an email program to junk folder purgatory, or worse, send it into the black hole we all call "missing."

Our study found that IPs categorized as legitimate servers with even one spam trap hit saw their delivered rate plunge to 38% versus 58% for mailers with no spam trap hits. Similarly, IPs that appeared on even one of the top 12 public blacklists had a delivered rate of 35% versus 58% for mailers not listed on any of these blacklists. This pattern held true for unknown user rates as well. IPs with an unknown user rate below 10% had 67% of their email delivered, on average, versus 44% for senders with dead email address rates greater than or equal to 10%.

Spam Traps, Blacklists & Unknown User Rates Impact Delivered Rates





What's more, our data revealed that our Sender Score reputation score closely correlates to delivered rates. Senders with a Sender Score of 72 had, on average, delivered rates of 87%. Compare that to senders with a Sender Score of 26 who average a delivered rate of 23%.

Sender Score: The Reputation Measure from Return Path

Our Sender Score reputation measure levels the playing field for all email senders. It offers senders and receivers a simple score based entirely on the metrics that distinguish legitimate email from spam: volume, complaint rates, unknown user rates, infrastructure, spam trap hits and content. The Sender Score reputation measure is based on data contributed by ISPs and other receivers of large volume email. Return Path consolidates and analyzes this data to provide all stakeholders with a complete view of email activity across all networks. Based on this data we are able to provide any email sender with a reputation measure or Sender Score, host our accurate real-time Sender Score Blacklist and run our Sender Score Certified whitelist program.

We offer free access to our Sender Score to any sender, receiver or consumer of email at our reputation portal: www.senderscore.org. Senders and receivers can register with senderscore.org – also for free – to gain access to detailed reports on the metrics that drive their sending reputation.