15 Trade Secrets
Of Email Service Providers

Secrets Your ESP Won't Tell You...
But You Need To Know

by Andrew Lutts, CEO Net Atlantic, Inc.

Email Servers Require Active Management

What you need to know before choosing an ESP

Definitions:

- An ESP is an Email Service Provider, a company that helps its customers send out email newsletters and automatically manage mailing lists.
- An ISP is an Internet Service Provider, a company that provides Internet access and email accounts to customers.
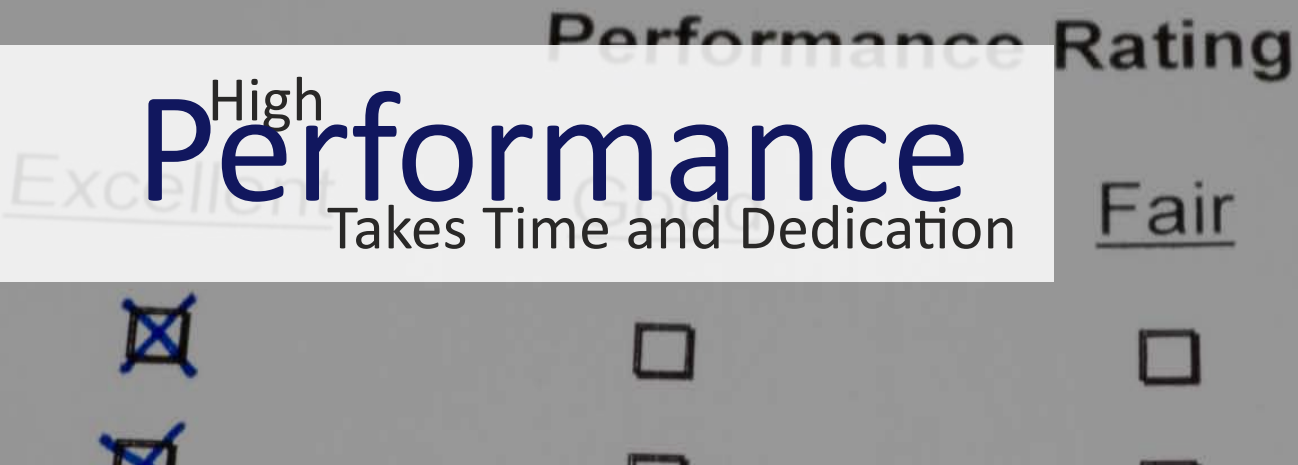
Secret #1:
Email servers require active management

A well designed, high volume outbound email mail server has a significant impact on the Internet, and specifically ISPs that receive your email. In contrast to a static web server that serves up web pages, a mail server is a dynamic entity that needs to be actively managed. Although many people try to set up their own mail servers in an attempt to save money, they soon find out how much more oversight it requires when compared to other types of servers on the Internet.

Why you need to know:
When you hire an ESP to send your email, you are paying for the active management of everything in relation to your email, in addition to reporting, storage, backup and uptime. Mail servers are unique, compared to other kinds of servers on the Internet.

High Performance
Takes Time and Dedication

Secret #2:

High performance takes time and dedication

Whitelists, feedback loops, sender authentication, and good reputations are some of the most valuable things an ESP can offer you. All ESPs can send your email out. Not all ESPs can do so capably and professionally, with high deliverability.

Why you need to know:

Unless your ESP has invested a significant amount of time and effort establishing relationships with ISPs, your delivery will likely be poor. Ask your ESP what whitelists and feedback loops they have in place. If you decide to go it alone and set up your own email server, you will need to spend the time on these issues with all ISPs.

Not every ESP is equal when it comes to performance. Deliverability is often based on relationships built over time.

Compliance
Suffers First in a Crisis

Secret #3:
Abuse desks suffer first in a crisis

Most major ISP operations are very well run with capable abuse staff, monitoring, oversight, escalation, and more. Many of their abuse staff are knowledgeable email veterans that may have worked at non-profit anti-spam organizations like MAPS, CAUCE, Habeas, SpamCop, and others. However, if an ISP is failing or suffering financial difficulty, abuse desks and support desks are often the first to suffer cutbacks.

Why you need to know:
The relationship between sender (ESP) and receiver (ISP) is a critical one. Unless you have done your work in advance and set up whitelists and feedback loops, it can be difficult to work with and get support from a struggling ISP.

Split Testing helps you know which message and value propositions generate the best response.

Security
is Always a Priority

Secret #4:
Zombies hurt everybody

One of the biggest challenges for all ISPs, especially cable and DSL providers, is customer "zombie" machines that have been remotely hacked to spew out spam, ping requests, DNS attacks, and other unsavory activity. As a result, many DSL and cable provider's residential networks (Verizon, Comcast, Cox, RCN) are automatically blacklisted with Spamhaus and various RBLs (Realtime Blackhole Lists). This means that you will have a hard time sending mail out through these networks.

Why you need to know:
ISPs have plenty to worry about and work on. ESPs that manage their business well can make life easier for ISPs.

Secret #5:
Anti-SPAM practices help, not hinder

Outblaze.net is probably the best spam-fighting company on the internet, and provides a critical role as a model for anti-spammers worldwide. Thanks to efforts like Outblaze.net, AOL, Spamhaus, and others, legitimate mailers can reach their subscribers.

Why you need to know:
The anti-spammers work selflessly for the greater good of the internet. Email marketing is an industry that becomes more mainstream and legitimate with each passing year, and owes a great deal to the anti-SPAM community.

Security is a top priority for ISPs because reduced security means reduced deliverability and reduced business.

Customer Interests Vary, And That's Okay

Secret #6:

Open rates vary wildly

Email Open rates can vary from 5% to 80% depending on many factors. The average is 20% - 40%. Open rates are almost always understated.

When your ESP reports a certain open rate for your mailing, realize that this technology is somewhat inherently flawed. Some ISPs do not correctly report "opens" in an effort to block malware and protect the customer's privacy. This can be especially true on mobile phones.

Why you need to know:

Don't despair if you are experiencing low open rates. Email is still king when it comes to return on investment, compared to all other methods available today. Pay special attention to both your subject line and your (mail from) sender's name and email address to improve open rates. Also, avoid list fatigue by using a regular schedule for your mailings.

Probably the largest factor in open rates is relevance. If your email is relevant, people will open and read it. Also, actual response is more important than opens. Instead of comparing your clickthroughs to opens, look for your rate of clickthroughs to messages sent.

Your customers vary, which is why open rates swing all over the map. It doesn't mean they aren't getting your message.

Email Servers Improve With Time

Secret #7:
Email servers improve with time

As the years pass, an IP address normally improves with age. Companies like Senderscore and others will assign you a more favorable weighting for operating on the same set of IP addresses and IP space. In fact, some ESPs will even attempt to "warm up" new IP addresses to help them deliver favorable ratings.

Why you need to know:
Choose an ESP with history (a good one, of course!). Everything else being equal, the longer the history the better.

ESPs that have been around, and have developed a strong reputation, have greater ability to get your email messages delivered consistently.

Get
Personal

love

Secret #8:
Make it personal

Curious fact: People rarely complain about opt-in adult-oriented email marketing. Why? Fear of embarrassment.

Why you need to know:
If you are selling something that is personal, you will likely experience fewer complaints about your emails, as people will be embarrassed that they "somehow" got onto your list.

Marketers who offer their customers a more personal message experience higher open rates and clickthroughs.

Secret #9:
Different email formats provide different results

Plain text email can sometimes outperform HTML email in terms of both delivery and response.

Why you need to know:
ESPs will try to sell you the moon with templates, tracking, video, and other technologies. However, realize that when ISPs receive your email bound for their customers, many of them have methods of "stripping out" potentially harmful elements of email messages, such as opens tracking, forms, and various "big brother" sleuthing technologies embedded within the email message. Try some clean and simple plain text email campaigns mixed in with your other campaigns. It is much more likely to reach your subscribers intact, and your response may improve dramatically.

One good rule is to make your email 60% images (with Alt Tags) and 40% text, for best response.

Good Fences Make Great Neighbors

Secret #10:
Good fences make great neighbors

You are only as good as your neighbors on your ESPs shared server, IP space, and data center. If your ESP uses a good data center that keeps a clean network by promptly terminating services to abusive customers, your will have much better success. These data centers may charge more, but they are worth it.

Trying to save money by going to a "discount" datacenter and ESP may look smart in the short term, but when delivery suffers you will probably lose more business and sales in dollars than you saved by going with an inexpensive solution.

Why you need to know:
If you change ESPs, your IP addresses, or other aspects of your sending operations, it may affect the delivery of your messages.

Secret #11:
You may be categorized by your ESP

Some ESPs keep certain servers reserved for poor reputation lower-quality customers, and certain other servers for their highest reputation customers with the best delivery.

Why you need to know:
Ask your ESP what kind of server they are putting you on. Know what kind of environment you are in.

Which box are you in? Your ESP knows.
You should, too.

Dedicated IPs Cut Both Ways

Secret #12:
Dedicated IPs cut both ways

A dedicated IP address can be a double edged sword. If you are squeaky clean with both your mailing list new subscriber policies and your mailing practices, a dedicated IP address is the best option. However, if you have not always used best practices with your email marketing in the past, a dedicated IP address can hurt you, and your delivery, if you do not properly adjust your mailing practices as you warm it up.

Why you need to know:
Send your newsletters under a dedicated IP address when you feel confident about the integrity of your email marketing. While you work towards best practices, choose a shared server option where your mail is mixed up with other client email on the same IP address.

Secret #13:
Bounces count

Outbound mail servers from an ESP not only need to send out a large amount of email, they need to receive it too! It's easy enough to write software to blast out email one-way; it is much harder to properly manage the bounces, retries, tracking data, temporary failures, unsubscribes, and more.

Why you need to know:
Choose an ESP with a proven fully-developed hosted solution, with a large array of incoming (mail-in) servers, to quickly and accurately manage incoming mail. Very few things will hurt proper delivery of your email more than an ESP that does not quickly manage the return mail and messages from ISPs. For example, if an ESP can't handle returned mail bounces in real time, the ISP will simply refuse all outbound mail from that ESP.

Best practices are now well-developed, and email marketers should use them at all times, and keep up with the most recent email marketing trends.

Reputation
Matters

Secret #14:
Reputation matters

If you are squeaky clean with a great reputation, you may not need a reputation company like SenderScore, ReturnPath, Habeas, or others.

Why you need to know:
Don't spend your money unless you have to. Of course you will get *slightly* better delivery with some of these reputation companies vouching for your email. However, for many mailers, the price of the service may not be worth the incremental improvement in delivery.

Secret #15:
ISPs are active behind the scenes

Large webmail companies like Yahoo!, Gmail, Hotmail, will filter, categorize, and deliver email based on a number of things completely out of your control. For example, if several of your subscribers didn't like your latest newsletter and did not open your email or sent it to trash, it will negatively affect the delivery of your email to other subscribers at the same webmail company.

Why you need to know:
You need to make every message count by sending high quality content to engaged recipients every time.

About Net Atlantic

Founded in 1995, Net Atlantic, Inc. is a global email service provider (ESP) offering email marketing solutions, branded reseller programs and dedicated email marketing servers. Net Atlantic's goal is to help businesses maximize ROI with email tools like A/B/N split testing, triggered and sequential mailings, custom surveys, click streaming, spam analysis tools, open database connectivity, and an open API (application program interface for even further customization). Net Atlantic was one of the first email marketing companies.

Visit **www.netatlantic.com**, or contact an account executive toll-free at **877-263-8285**.