GETTING YOUR EMAIL DELIVERED

By Landon Ray, Founder/CEO

ONTRAPORT
PLUG IN YOUR BUSINESS

Getting Your Email Delivered

Everything you need to know about why some emails go to the inbox while others don't, and what to do about it.

by Landon Ray, Founder/CEO

If getting your email to your leads' inboxes is important – in other words, if having it trashed costs you money – then it's important for you to understand how the email world works. Unfortunately, there's a ton of incomplete, inaccurate or outdated information out there (often written by some blogger regurgitating something they read somewhere else like "using the word 'free' gets your email trashed so use 'f.ree' instead" or some other nonsense).

This report is going to be as brief and as simple as I can make it, but it's my goal to give you the information you need to understand what's happening to your email. This information will enable you to make good decisions about your email delivery, and what you, as a mailer, need to know to make sure you don't end up in email delivery hell.

Part of this story is going to be a bit technical, because that's just the nature of the information. I'll explain everything as we go so you don't need any technical background to understand anything here.

Much of what you're about to read will sound like a non-fiction war history, because that's exactly what it is.

Let me explain...

Part 1

The War for Your Inbox

There's an ongoing war being waged for the control of your inbox. Think about why: many people spend more time with their email now than with television. That level of attention is extraordinarily valuable.

On television, the networks create great shows in order to entice you to watch the advertisements they jam in there, which they sell to advertisers (like you). That's the business model and it's a very big business. They're selling your attention for profit.

Now imagine for a moment what would happen if some high-tech geeks figured out a way to actually TAKE OVER the airwaves and start showing their own programming.

What would happen?

Well, first you'd probably see some really nerdy nonsense – geeks playing practical jokes on the populace, right?

But pretty quickly, those geeks would realize the massive power of what they'd done. They've stolen the attention of millions of people.

Pretty soon, those geeks would figure out how to use their newfound skills and the attention they stole to...

GET MONEY.

They'd start selling stuff like Viagra, wouldn't they? Or they'd start scamming people, telling them to call special numbers and hand over their bank account information, right?

“54% of emails sent by businesses are marketing messages”

Source: Epsilon (2013)

I mean, I believe in the goodness of the human spirit as much as the next guy… but isn’t this the way it would go down?

It is, and I’ll prove it in a second. But first, consider what the networks who owned those stolen airwaves would do in this situation.

Well, they’d be hopping mad, of course. They’d hire lawyers and lobbyists and they’d get laws passed. They’d amass armies of their own tech-geeks to thwart the hijackers.

YOUR INBOX HAS BEEN HIJACKED.

The little story we just told is, of course, the story of the war that’s going on for your inbox today. The players are a little bit different, but the stakes are the same.

Instead of television networks, it’s ISPs (Internet Service Providers) like AOL, Yahoo!, Gmail, MSN and zillions of smaller mailbox providers that have their clients’ attention being stolen.

The techno-geeks are the same, but instead of stealing airwaves and playing their own programming, they’re stealing attention by filling your inbox with offers for Viagra and invitations to send money to Zimbabwe.

WE CALL THEM SPAMMERS.

Did you know that 91% of all email sent in the world is spam?

91%! That represents a giant, seething, massive horde of attackers charging at your inbox day in and day out, battling for your attention.

What would happen if, say, AOL or Gmail didn't protect you from the onslaught of spam that's thundering for your inbox everyday?

Well, 9 out of 10 emails you'd get would be spam.

And what would you do about it? Well, you'd just close that email account and move on and AOL or Gmail would lose a client. Pretty quick they'd lose ALL their clients, and they'd have to pack it in and go home.

If you couldn't find another mailbox that was any better, email as a media would be dead.

THE PLAYERS

To finish setting the stage here, let's recap who the players are:

1. **The "ISPs"**: These are the folks that run your mailbox and are concerned with keeping spam out of your inbox. And ISP could be a public service like Yahoo, AOL, or Gmail or it could be a corporate filtering system. Either way, if your spam gets out of control, these guys lose you as a client.

   Their job is seriously complicated by the fact that most of us, particularly in business, are intolerant of 'good' emails mistakenly going to our spam folders because that could mean missing a sale or worse. ISPs have to walk a fine line: keep the spam out and keep the real mail in. Tough job.

2. **The Spammers**: These are the guys sending the email that you don't want to get.
3. **The Recipients**: That's you and recipients of the other 200+ BILLION emails sent each day. (For reference, the current population of Earth: over 7 billion people)
4. **The ESPs**: ISPs, ESPs, DNS, SPF... why so many initials? Sorry, nature of the beast.

We haven't mentioned the ESPs yet. ESP is short for 'Email Service Provider'. That's us, the companies responsible for delivering many of those 200 billion emails on behalf of individuals and companies like yours. Our job is pretty complicated too, as you'll soon see.

[1] (According to Ironport, a top provider of spam protection worldwide)

Part 2

The Arms Race

The history of spam is like the other histories of war: each side moves as quickly as possible to build more powerful and effective weaponry while creating tools, systems, or strategies to render the enemy's weaponry powerless. They build a missile; you build a missile defense shield, right?

An understanding of the brief history of the war between ISPs and spammers will help you understand why things are the way they are today, how to navigate today's email climate and even to predict where the industry is headed.

IN THE BEGINNING...

... there was an awful lot of spam. How many email addresses did you have to abandon because they just became overrun by spam? (Hotmail anyone?)

Early attempts (that is, circa 2000) at curbing spam depended on content filters. That is, if the content of the email had 'Viagra' (or a giant list of other suspicious words or phrases) in it, it went to the spam folder.

Even today, content filters play a limited role. For clear reasons, filtering emails based on content is a pretty blunt tool. Not only are content filters easy to circumvent (with images, for example) or avoid (just don't say 'Viagra') they're also very likely to filter emails that aren't spam, which is

a serious no-no for ISPs. For example, 'free' would be a good word to use for content filtering but would obviously also put a lot of 'permission-based' emails in the trash.

The onslaught of spam was only temporarily slowed.

“Both marketers (76%) and consumers (69%) favor email as their first online “check” of the day.”

Source: ExactTarget “Marketers from Mars” (2013)

The ISPs, intent on stemming the tide, said to themselves, “Well, if we can’t filter based on the content of the email alone, maybe we can filter based on who’s sending the email!”

That was a good idea, and the ISPs quickly banded together and started communicating between themselves (and with other 3rd party organizations) about where the bad emails were coming from.

I’m going to introduce another abbreviation here: IP Address which is short for Internet Protocol Address. This is not to be confused with ISP (internet service provider – the mailbox providers).

IP Address is a unique number assigned to virtually every single computer on the internet. Think of IP Addresses like your driver’s license number.

The big mailbox providers (ISPs) started keeping lists. Giant lists of all the IP addresses that were sending them mail. If the mail looked spammy, they’d block email coming from that IP address and tell all their ISP buddies that they’d identified a bad address. Pretty soon, if that bad address was yours, you were hosed.

This was a cool new tool for keeping spam out, and led to the first dramatic drop in spam that we all experienced around 2002. Unfortunately, of course, spammers don’t quit so easily.

There were two problems with the new system. First, it was a giant hassle for the ISPs to figure out what was spam and what wasn’t and to mark it accordingly. Early on, it must have been a fairly manual process for them and for those 3rd party organizations, like Spamhaus. Imagine trying to mark 90% of 200 billion emails. ‘Giant hassle’ is putting it mildly, I’d say.

Second, the Spammers are wily critters. As soon as their IP addresses were blocked, they'd just jump ship to a new one and fire away. To this day, professional spamming services (yes, you can actually hire them!) boast about how they use 47 new IP addresses a week.

So pretty quick, the ISPs got buried by the task of manually blocking IP addresses, and the spammers discovered that the IP address tracking was really a minor annoyance.

ISPs had one other nagging challenge that we haven't talked about yet, and that's the issue of 'spoofing'.

ISPS HAUL OUT THE BIG GUNS

Spammers may be wily critters, but the ISPs were not screwing around either. The state of spam at that time was threatening the core of their businesses.

Microsoft's Hotmail, for example, once the clear leader in hosted email, experienced a mass exodus because they couldn't keep spam out of their client's inboxes. Today, they're lagging in second place to the webmail giant Gmail.com.

It was around this time that ISPs got serious and hauled out the heavy artillery. Starting around 2003, they outlined the systems that have kept your email inbox pretty darn clean these last years... and which have frustrated countless 'legitimate' email marketers to no end.

THE FOUR PRONG DEFENSE

Here's what they came up with.

1. Sender Authentication
2. User reporting for spam
3. IP reputation filtering
4. Linked domain filtering

Let's look at each.

Sender Authentication actually describes several systems by which email recipients (ISPs) can determine whether the sender of an email is actually authorized to send on behalf of the domain in the FROM line. Authentication has been likened to requiring license plates on cars. It doesn't stop speeding, but at least you can identify the car.

Yahoo's Domain Keys (now DKIM) and Sender Policy Framework (SPF) are the two most widely used authentication systems today. If the IP addresses your email is being sent from doesn't have registered SPF and DKIM records, you're gonna feel it.

User reporting for spam is a big, big, biggie. Remember ISPs had this giant issue with the sheer volume of spam coming through and figuring out how to mark it all, and for that matter, how to figure out what's spam and what isn't!

Then they realized 'hey, spam is anything our clients don't want in their inboxes!' That is, the ISPs gave the job of deciding what spam is and reporting it right to their users in the form of a 'This Is Spam' button. Now the mob rules. If the messages from a certain sender start getting reported as spam by lots of users, then it's spam and that's all there is to it.

This changed everything. Now your success as a sender lives and dies by a click of your recipient's spam button. They know who you are (because of authentication and IP address tracking) and they'll punish you, quickly and severely.

IP reputation filtering is the same system we talked about earlier. Basically, the IP address you send from carries to a large degree your reputation. If your IP has a bad reputation (that is, users have been clicking the emails sent from it as spam too much), your emails don't get delivered.

In fact, this system has gotten very sophisticated over the years. Information is quickly shared between ISPs and 3rd party reputation

> **"80% of email delivery problems are directly attributable to a poor sender reputation."**
>
> Source: DMA "Email Deliverability Review" (2012)

monitors. In fact, whole IP 'neighborhoods' can have their reputations tarnished by the poor behavior of a few IPs using nearby numbers.

This is a huge problem for many ESPs (email service providers) that send email on behalf of many clients from one or a few IP addresses (which accounts for virtually all of us).

Imagine the problem: we ESPs have hundreds or thousands of clients all using our services and sending out email every day. We've got terms of service and rules about not importing bad addresses, but at the end of the day the truth of the matter is that we all take our clients' words that their lists are clean and opt-in.

Of course, as soon as a new client emails their list, we can see if the list was clean or not. If it's a bad list, complaint rates go right through the roof. The good ESPs take fast action and find out the problem, clean up the list, educate the client on better email practices or even remove the list and fire the client.

But the damage is done. Every time that happens, the reputation of the IP address suffers. And over time, the delivery rates for ALL clients using that IP will suffer.

It doesn't matter what your ESPs marketing and sales pitch says: **if you're sending from a shared IP address you're placing yourself at a disadvantage**. Your reputation will roughly equal that of the worst sender on your IP.

That said, it's not quite as bad as all that. See, ISPs (Google, Yahoo, etc.) understand the problem. They don't WANT to punish all of an ESPs

> **"For every $1 marketers spend on email, the average ROI is $40"**
>
> Source: Direct Marketing Association (2011)

clients for the bad behavior of one. So there's some play in there. The good ESPs have relationships with the mailbox providers and when we've been burned by a bad client, we'll literally call up the ISP and fess up, tell them what happened, tell them what we've done to remedy the problem, and beg forgiveness. And that works pretty good.

But more and more ISPs are turning to a new tactic to take on bad senders one by one...

Linked domain filtering is the newest trick to be introduced. This is where ISPs keep track of not just the IP address that's sending the mail (ours) but they actually keep track of the domains linked to IN THE CONTENT OF THE EMAIL!

The idea here is this: Joe's Dog Food Company buys a big list of dog owners' emails. (That's a spammy thing to do, by the way. Never buy a list of emails!) He comes to us and we say 'No way, Joe. Can't send that list here.'

So, Joe goes and hires a spam company who happily sends out 12 million emails a day for him. If you're quiet, you can almost hear the clicking of a million 'this is spam' buttons by dog owners everywhere.

The IP the spammers were sending from is shot. The spam company doesn't care, they'll just get a new one.

But, because Joe was advertising his shiny new website in all those emails and had links pointing to www.joesdogfood.com, Joe's now shot too, permanently and forever.

Now, Joe comes back to us with the opt-in list he would have inevitably built from his spam campaign and says 'Ok! I've got a squeaky clean list of folks who opted-in right on my website, let's rock!" We say, "Great! Let's do this!" and fire off an email to his list. What happens? Nothing happens because all Joe's email go right to the spam folder. Not because WE have a bad reputation, but because Joe's website does!

If you sit and think about it for a minute, you'll see that in the next few years, as ISPs perfect this system, it's going to put the wood to many marketers, some of whom may think they're doing the right things but really aren't.

THE FIFTH PRONG

At about the same time, another strategy was developed. Not by the ISPs themselves, but by enterprising young companies out to save the world spam and make a buck along the way. These are 3rd party white-listers.

Basically, a few companies got the idea that if they set some standards about how to be a good sender and then monitored company's mail practices to make sure they met those standards, they could 'vouch for' these companies as good senders. They'd put them on a 'white-list'. And

then they'd go out and talk the big mailbox providers into checking their list of whitelisted IP addresses on a regular basis, and automatically accepting mail that came from them.

The ISPs were happy to do this because frankly they could use all the help they could get separating good email from bad.

The white-listers sell their services to companies. The service is basically to continually monitor your mailings and, if you fail to meet their standards, to make sure you get back up to speed quickly or get out.

Over time, the white-listers consolidated and now one organization is the clear and undisputed leader of them all, virtually to the exclusion of all others: SenderScore.org.

If you mail enough (over roughly 40k emails a month) and have good email practices and low complaint rates, you can get SenderScore certified and you will see a boost in your delivery.

THE ISPS WIN. SPAMMERS LOSE. (AND MARKETERS FOOT THE BILL.)

At the end of the day, it's clear to see that in the War for Your Inbox, the Spammers are getting their butts kicked. These days in Gmail you may get a spam email every day or so. More with other services... maybe. But with spam accounting for 9 out of 10 of all emails sent, I'd say that's pretty impressive.

Unfortunately, it's folks like you and me – the legitimate senders of marketing emails – who have to work and jump through hoops and manage our lists impeccably to make sure we're not marked with the Scarlet S.

Part 3

How to Get Your Email Delivered

Now that you've got a solid background of the problem and the current state of affairs, it's pretty clear what you've got to do, isn't it?

1. Don't get marked as a spammer by users.
2. Don't get marked as a spammer by users.
3. Don't get marked as a spammer by users.
4. Don't let affiliate marketers whose messages get marked as spam send mail on your behalf.

It's that easy.

Ok... there's actually a touch more to it than that.

First, though, you should understand that 100% inbox delivery is an impossible to reach goal. Getting darn close isn't actually too hard, but get comfortable with the fact that some of your marketing emails are going to get filtered. Don't freak out; it's just the nature of the beast.

With that said, let's look at how to get the best possible inbox delivery rates.

Don't get marked as a spammer by users.

Your reputation lives and dies by the click of a 'this is spam' button. The ideal number of complaints is less than .1 percent... that's 1 in a thousand. Not a lot of wiggle room.

So, how do you avoid getting marked as a spammer?

"Roughly 18% of all commercial email in North America never reached the inbox in 3Q12: 5% landed in spam traps and 13% was blocked or went missing"

Source: Return Path "The Email Intelligence Report Q3 2012" (2012)

1. **Don't EVER, EVER, EVER buy a list.** Don't put email addresses in your system that didn't SPECIFICALLY ask to be there. Importing an old list of emails that you haven't mailed in a year is a recipe for disaster. Adding people who dropped their card in your fishbowl at a tradeshow because they wanted to win a free iPod is going to get you in trouble. The bottom line here: **ONLY** email folks who **specifically** requested to get email from you, and...
2. **ONLY send them what they requested.** That is, be relevant and set expectations. Just because someone signed up for your monthly newsletter does NOT give you permission to add them to your daily e-course sequence, your product launch promotions, or anything else.
3. **Don't write like a spammer.** If it walks and sounds like a duck... you know. Although content filters are declining in importance, they're still very much a part of the picture. Starting an email with 'CONGRATULATIONS! You've WON!' is going to get your email trashed. Your subject and FROM lines should identify you and accurately describe the contents of the email. It's not only important for the delivery rates of your emails but also legally required by the CAN-SPAM act. A surprised or confused recipient is likely to complain.

   Let them know, at the top of your message, why they're getting your email and how they can unsubscribe.

BUILD YOUR OWN REPUTATION

Without a doubt, the best thing you can do for your long-term success with email is to **get a private IP address**. As long as you're mailing from a

shared IP address, part of your reputation is out of your hands... and your reputation determines how well you get delivered.

If you're mailing over 300,000 emails a month, it's time to start thinking about striking out on your own IP.

There's one downside you should know about: in the email world, no reputation is a bad reputation. When you launch a new IP, you're starting out with no reputation. Some ISPs will reject your messages without looking twice for the first several weeks. There are strategies for minimizing this problem that your email provider should know about and use. We call the process 'warming up an IP' and we have a guide on how to do that if you're curious. Just ask.

Once you've built your reputation on your new IP over the course of a few weeks, you'll finally be in control of your own email delivery destiny: keep your list clean and your practices tight and **you'll enjoy the highest delivery rates available to any mailer anywhere**.

CAN'T GET A PRIVATE IP?

There are only two reasons not to get a private IP: your email service provider doesn't offer it or you don't mail enough to warrant getting one.

The first is easy to fix and a no-brainer. If you are an even moderately heavy mailer, you should get on your own IP. Change to a service that offers them. Of course we do, but there are several other higher-end email service providers who offer the service.

If you don't mail enough to warrant getting a private IP, there are still some things you can do to make sure you're getting the best delivery rates possible.

1. **Check out your provider.** Make sure the domains you're sending from have valid SPF and DKIM records.

Hard bounces are errors that can't be remedied. For example, "user doesn't exist" is a hard bounce.

Soft bounces are fixable and not permanent: ex. "mailbox full"

2. **Send from your own domain.** Send from your own domain. Often, especially with the lower-end email services, the email you send will show your name in the FROM: line of the email. It may even show your own URL. But look at the actual email headers (you may have to dig a little to find the code) and you'll see that the email is actually coming from the address of the ESP. Something like noreply@spcd1.myesp.com.

   The problem with this is that your 'reputation' is partially determined by that FROM: address and if you're sharing it with thousands of other clients... well, it's a lot like sharing a toothbrush. You could, but do you want to?

   Much better to send at least from a subdomain all your own (noreply@yourcompany.myesp.com) or better a URL all your own. This could be done in one of two ways: noreply@mail.yourdomain.com or noreply@yourdomainmail.com. There are benefits and drawbacks to either of these options, but both are MUCH BETTER than sending from a shared address. Your email service provider should be able to set something like this up for you.

3. **Test delivery rates yourself.** You should know: the 'delivery rates' that your email service provider gives you is not 'how many emails reached the inbox'. It's simply 'total emails sent minus total bounced'.

   That number completely ignores how many actually make it to the inbox versus the spam folder. Why? Because there's no way of knowing. The only way to know if your mail is making it to the inbox or not is to periodically test with a delivery monitoring service. You can use services like Email Reach or Delivery Watch to check your inbox delivery rates and get information about block lists your IP addresses may be on.

These services aren't free, but they're both under a hundred bucks a month. Email Reach has a free trial (www.emailreach.com).

MANAGE YOUR BOUNCES

If you're using an email service provider, ask them how they manage bounces. The thing is, if you keep mailing to bad email addresses (or hard bounces) at Yahoo, they start getting testy and wonder about your email practices. If they tell you an address is no good, stop sending to it! Of course, that's a giant pain in the rear for you to do manually… and something your email service should handle for you. Ask what their bounce policies are.

Do they remove or disable email addresses after a certain number of bounces? Hard bounces only, or soft bounces? Soft bounces are when you try to send an email to an inbox that is full or temporarily unavailable.

If your provider has answers for these questions and reasons that make sense, you're probably in good shape. If not, run.

HANDLE YOUR COMPLAINTS

Another core service that your Email Service Provider should be handling is complaint management. You need to quickly remove any complainers from your list; once someone's peeved enough to complain, they're likely to click spam on every subsequent message you send. Those add up all too quickly. Get rid of them!

GET THEM TO 'WHITE LIST' YOU

In the same way that ISPs will blacklist you for getting spam complaints, when recipients purposefully white list you (that is, add you to their safe senders list or to their address book) you're building credibility. Like, you know, good Karma. So, ask people to whitelist you! Tell them exactly how to do it.

> **"People spend 13 hours per week reading their email - 28% of our workweek."**
>
> Source: McKinsey Global Institute (July 2012)

LINK RIGHT

Turns out that even the way you create links in your email affects your delivery rates, when you're using an email service provider that tracks click-through rates for you.

Let's say you write a link like this: http://www.mysite.com. The email service provider has to add their tracking code to track the click, so the link actually points to http://www.mysite.com?id=1398vh981323890

In this case, some ISPs and spam filters think you're trying to pull a fast one, sending people to places other than advertised. Seems pretty dull on their part, and it is. But it's the state of the union right now, so here's how to avoid it: make your links have real anchor text that isn't a URL. So, instead of linking a domain name like http://www.mysite.com, use words like 'Visit my site' and link those. It looks less suspicious to filters AND it looks more pro to your recipients. A double whammy.

CODE RIGHT

The first mortal sin of email coding is to copy and paste from Microsoft Word. **Just don't do it.**

There are two reasons. First, there are all kinds of special characters in Word that don't exist in Internet Land such as the apostrophes that curve

toward the center of the word they surround, ellipses (which are the three periods in a row… Word actually changes those three dots into one character), dashes and other characters.

Some email editors, including our own, will actually show the Word characters properly. And some recipients will see it properly. BUT the majority of recipients will see all those unique-to-Word characters replaced with question marks and weird characters.

Not very pro.

The other issue with Word is that when you copy and paste, you're also copying and pasting a bunch of Word-code that makes no sense to email systems.

In the worst case, that code can break your email completely. In the best case, it's just a mess asking to get spam-filtered.

Some email programs, like ours, have a 'copy from Word' feature that will handle the grossest parts of the problem. Still, it's best to avoid Word all together.

Write your emails directly in the email editor, or else in a simple text editor like Notepad.

Also, check your links.

Broken links are no good for anyone. Finally, if you're using HTML, make sure it's well-coded and looks right in all the major email readers, even with the images turned off. You can check this with services like Email Reach (www.emailreach.com) or Litmus (www.litmus.com) for those on a tighter budget.

AFFILIATE MANAGEMENT

What you don't know can hurt you. Affiliates are a great way to grow your business, however they can also be a huge detriment to your deliverability rates. Did you know that the behavior of one rogue affiliate could cause ALL messages promoting your website to end up in the spam box? That's the last thing you want to happen.

To veer away from this dismal scenario, hand-pick your affiliates before you let them promote your goodies: put all incoming affiliates through a screening process. Confirm that they have an existing brand that stays consistent from time of opt in to the mail they send their customers. This is accomplished by having a basic affiliate sign-up form that asks for their website URL. Then when someone applies to be your affiliate it's a cinch for you to go to their website, sign up to be on their list and see what types of messages they're sending. Once you're sure they're an ethical marketer you can approve them with a clear mind.

In Conclusion...

Hey, nice work slogging through this paper. That shows that you're serious about email and up to the task of managing your list and your reputation.

The bottom line is that there's no real secret to email delivery. You've just learned everything you need to know to get the best delivery rates available. It's work, and it takes some patience. Like most good things in life, I guess.

If you have any questions that we didn't address here, don't hesitate to send them to support@ONTRAPORT.com.If you have any questions that we didn't address here, don't hesitate to send them to support@ONTRAPORT.com.

Landon Ray *is Founder/CEO of ONTRAPORT, Inc.*

ONTRAPORT is a business management platform that consolidates sales, marketing and business automation software. While other products create frustration, ONTRAPORT streamlines, enabling businesses to harness the power of technology with one simple solution.

ONTRAPORT.com
2040 Alameda Padre Serra #220, Santa Barbara, CA 93103
855 - ONTRAPORT