



Email Marketing Solutions by Marketers, for Marketers

Is Your IP Address **Whitelisted**?

By **Neil Anuskiewicz**

Whitelist your IP Address & Increase Email Deliverability

You play by the rules. Your list is confirmed opt-in. You have spent time writing a compelling message and an inspiring call to action. Your graphic designers have designed a stunning custom email.

You then send the email to your list but find that deliverability rates are lower than you planned—mostly because none of your recipients at a major Internet service provider (ISP) received your email. This is a disappointing outcome to say the least, and you decide to look into the matter further in order to avoid low email delivery rates in the future.

Why did this ISP block your emails? You learn that the ISP has blacklisted the IP address that you share with numerous other customers of your email service provider (ESP). Another email marketing customer sharing your IP address sent out an email blast and got too many spam complaints. As a result, the ISP blacklisted the IP address from which the email blast came.

Your email delivery rates were lower than normal because of the actions of someone else. This problem was caused by factors completely out of your control.

Problem and Solution:

You may be surprised to learn that most ESPs have a very small pool of IP addresses that nearly all of their customers share. Their large customers, however, do get a private IP address. Small businesses and nonprofits typically have to share them or pay extra for a private one. Consider requesting a private IP address from your current ESP or even switching to an ESP that offers a private IP as a standard feature.

Alternatively, if your deliverability numbers are consistently high, it probably means that your ESP is already offering private IP addresses or is doing a good job of managing relationships with the major ISPs. If they offer mostly shared IP addresses, good delivery rates mean they are doing a good job of ensuring CAN-SPAM compliance among their customers and—when

your shared IP address blacklisting happens—they are able to get it removed relatively quickly. This is where good relationships with the ISPs is important.

What Is an IP Address and Why Should I Care?

Every machine connected to the Internet has a unique number called an IP address. A good analogy would be cell phone numbers.

The big difference is that you do not share your cell phone number with a large group of people. You have a unique cell phone number through which people can reliably reach you and only you. They know it is you calling, and not some prank caller who happens to share your phone number.

With a shared IP address, you share your IP address with other customers of the ISP. With some ESPs, each customer shares an IP address with thousands of other customers.

When you send out an email campaign, your emails are stamped as coming from a specific IP address, similar to how caller ID shows who is calling you—but, for emails, you are lumped together with everyone else who shares your IP address.

As a result, ESPs are fighting a constant battle to keep their pool of IP addresses in the good graces of the ISPs, corporate networks, etc. Though high-quality ESPs make sure that their customers are CAN-SPAM compliant, recipients still can and will file spam complaints. If above a certain threshold of your recipients file spam complaints (the level varies by the ISP or corporate network), the ISP or network administrator adds the IP address to a blacklist and blocks all email originating from that IP address.

continued . . .

It is worth mentioning again that the better ESPs have relationships with the ISPs and do a good job of keeping their IP addresses off the blacklists. If the IP address does get blacklisted, they are usually fairly effective at getting the IP address removed from the blacklist. This process does not always go smoothly though.

The Next Step: Whitelisting Your IP Address:

If you decide to get a private IP address, follow guidelines to avoid the spam filters, and stay CAN-SPAM compliant... your deliverability rates should be excellent.

You could achieve even better deliverability by getting on the whitelists of the major ISPs and even some corporate networks to which you send a lot of email. If you do this, you will enter the realm of email senders the ISPs trust to send permission-based emails that will not annoy their customers.

A whitelist is a list of IP addresses that have proven to be used for permission-based email only. The ISP lets emails from that IP through, and they are much less likely to be blocked by spam filters.

To get your IP address on a whitelist you have to establish a track record through a couple of months of sending legitimate email. Once you have done that, you apply for whitelisting and the ISP adds you to its whitelist. Since nobody else shares your IP address, nobody else can cause you to be removed from this whitelist or cause the ISP to add your IP to their blacklist.

How Specifically Do I Whitelist My IP Address?

To be whitelisted, you just have to establish a track record as a permission-based email marketer. This is essentially complying with the CAN-SPAM regulations, meaning that you do things like include a valid From address, send to confirmed opt-in email lists, and provide your recipients a clear opt-out link; you do not do things like write deceptive subject lines or try to hide the intent of your emails. There is more to CAN-SPAM, and I recommend doing a Google search and reading the summary of CAN-SPAM. You can read it in a few minutes, and it will help you make sure your email campaigns comply. The rules are simple.

To qualify for whitelisting status, you have to have a good, not perfect, track record in terms of spam complaints. As all who do email marketing know, sending email to an opt-in list can still result in some spam complaints. People forget that they opted in originally or they grow irritated with the emails and file a quick spam complaint rather than finding the opt-out link at the bottom of the email. The ISPs recognize that there will always be some spam complaints with permission-based email marketing. However, as long as the complaints fall below a certain threshold, you can pass the criteria for whitelisting. The ISPs know that real spammers receive a higher level of complaints than permission-based email marketers.

Each major ISP maintains its own whitelist, so you will need to visit the respective websites and submit their forms. Your ESP should be able to provide you links to the whitelist application forms for the major ISPs and email address providers. They should also be able to provide you assistance, if needed.

For additional ISPs and corporate whitelists, you will have to do a Web search or contact them directly for more information. It might be worth it to request whitelisting on selected corporate networks if a large-enough number of your list members have email addresses on those corporate networks.

The important point to remember is that deliverability is key to email marketing success, so watch your email deliverability like a hawk. If your ESP is not performing for you, then find out why and remedy the situation quickly. Try to make changes using your current ESP first. If nothing changes, then it might be time to consider a change.

continued . . .

About StreamSend

StreamSend is an award winning email marketing solution created by marketers, for marketers.

Thousands of companies have already discovered that StreamSend is the ideal e-mail marketing partner. It is the most affordable permission-based ESP on the market, and the only one that provides every account with a private IP address at no additional cost.

With enterprise level features such as trigger-based messaging, A/B testing, transactional emails and in-depth reporting, StreamSend enables customers to increase the ROI on every campaign and pinpoint what successfully drives sales.

For more information on StreamSend, please visit www.StreamSend.com, or call 877-439-4678, extension 819 and speak to Neil Anuskiewicz.

StreamSend Partners and Affiliations:

