

# Zero Spam

## Email hints for users and mail server operators

### Introduction

Email spam seems to be a new curse of our times that is as tough to eradicate as a new virus or superbug. After many years in a corporate environment I have seen my fair share of unwanted emails and probably many times more than that have ended up in spam filters and blacklists.

For a few years now I have been running my own mail servers and still haven't quite gotten over the amazement that I don't get any spam any more, even though many people around me still do. No doubt, as soon as some malicious persons read this, I might get attacked with new vigor.

However, most recently I experienced that several people I know and with whom I have been communicating for some time didn't get my emails any more. Some spam filtering, however inadequately set up, managed to intermingle my perfectly valid emails with spam, which got then deleted. That's when I thought it's time to write down how I do it, because there seem to be many who aren't doing it quite right.

# Zero Spam

## Email hints for users and mail server operators

### First Principle

The ‘first principle’ as I coin it, is a philosophical one. We need to ask ourselves a very high-level question:

*“A. Should I consider all email as bad and reject it, unless somebody or something tells me it’s good?”*

Or,

*“B. Should I consider all email as good and accept it, unless somebody or something tells me that it’s bad?”*

This is a very important deliberation, because it is fundamental for our choice of tools. If we go for option A then we basically say, reject everything, unless we explicitly say that it’s OK to let in. This kind of principle might be appropriate for high-level executives, who could easily get swamped with email, or, the President of the United States, whose Blackberry address is only known to a very small circle of people.

This principle is also used with mail authorization servers, who want you explicitly acknowledge that you are the sender before they will forward the email to the proper recipient.

You might also be applying the same principle if you have a mail client that lets you configure which email addresses you accept mail from. All others will end up in a spam folder.

I must say that I am not in favor of option A, probably because I am neither the President, nor a high-level executive. Furthermore, it would prevent me from getting emails from strangers, such as far-away relatives, childhood friends, etc. that would be very beneficial to receive.

So, I am obviously in favor of option B, however, with a proviso. My mandate is that absolutely everything that can be done should be done, so that I am not deluged with unknown email. In order to achieve this we need to do several things at different levels. And here I have to admit that some of the recommendations listed may not be within the reach of most email recipients. However, if they get to know about them they may simply ask for them or demand them from their email server providers.

# Zero Spam

## Email hints for users and mail server operators

### Approach

As amazed as I am at the success I have had so far in avoiding spam I have to warn that it is possible that others may most likely fail if they only partially follow these recommended steps or substitute some for similar approaches. As I have not tried alternate approaches I cannot vouch for any of them.

There is also a time element here. Something that works today may not work tomorrow. I used to use a blacklist that's no longer working. When such things happen they do have an effect on the efficacy of our spam filtering.

The following steps can be divided into user or client-side steps and steps that need to be taken at the mail server side. Each one is as important as the other.

### User or client-side approach

Who knows your email address? I know many people who complain to me that they get too much spam. Well, actually, a lot of it is their fault. The solution is quite simple,

**User Rule 1:**            *“Change your email address.”*

In these times where many mail providers give each user more than one email address we should all be getting used to using different email addresses for different purposes. For example, if your name is John Smith and your friends know you as Johnny, what's stopping you from using,

[Johnnys6789@yahoo.com](mailto:Johnnys6789@yahoo.com),

unless the name has been taken already. If it gets compromised, tell your friends that in a week's time your email address will be

Johnnys\*5432@yahoo.com

Likewise, if your job is accounts clerk, then communicate with your colleagues only as

[John\\_Smith\\_AC01@company.com](mailto:John_Smith_AC01@company.com)

If this account gets compromised by some bozo in your company, then simply change it to

[John\\_Smith\\_AC02@company.com](mailto:John_Smith_AC02@company.com)

## Zero Spam

### Email hints for users and mail server operators

Do not use simple first name/last name combinations as email addresses, because they can so easily be guessed.

As I have my own mail server and several companies I can literally have hundreds of email addresses. If, for example, I am asked to register at some company, such as Amazon, etc. I use a name that hints to that company. If it should ever get compromised I can go back to that company and tick them off. Under no circumstances would I register with an outside company with my email addresses that I use for my friends and business emails.

#### **User Rule 2:**            *“Don’t publish your email address.”*

How often have I seen email addresses embedded in blog entries, forum contributions, websites, etc.?

DON’T DO IT!

Putting your email address on a web page that is readable by the whole world is the equivalent of attracting one hundred spam emails a day. Nobody deserves any spam, but doing such a stupid thing makes it just too easy for spammers.

Even if you think of putting your email address onto business cards, or any other printed matter, such as white papers, etc., remember that eventually they either end up on a website or get scanned into somebody’s address book. Sooner or later that somebody will then include you on an open distribution list or gets his address book or email account hacked into.

#### **User Rule 3:**            *“Be careful about your client-server link.”*

Unfortunately, many people don’t understand yet the distinction between their client-side mail program, such as MS Outlook, Mozilla Thunderbird, various web-based mail clients, and mail servers, such as MS Exchange, Yahoo Mail, Postfix, etc.

There are a couple of reasons why this is important.

1. Only read your mail, after you are satisfied that you have established a secure link between client and server.
2. Make sure that nobody can imitate your mail client and read your mail.

Neither one of these two points are very easy to satisfy. But here are the reasons why they are important.

## Zero Spam

### Email hints for users and mail server operators

When establishing a link between a mail client and a mail server we may be asked to enter a username and password. Ideally, the password should not be requested while there is an un-encrypted link between client and server. The correct sequence should be:

- a. Enter username or mail server location
- b. Server establishes encrypted handshake with client
- c. Then enter password or username/password combination

This may not be necessary if both client and server are on a protected local area network that is shielded from the outside world via a firewall, and doesn't go any further than the local office. In my setup, for example, I have denied myself access to my own email over the Internet. I can only read it from within my own office.

This will help towards point #2 above. It is unfortunately very easy, over the Internet, for anybody to imitate you and read your email, if Internet access is allowed. For the majority of mail users who utilize free Internet email, this is unfortunately the case. If you have the benefit of an office email system, then use that instead, whenever you can, but be careful not to inter-mingle private and office email, as this is most likely an abuse of your terms of employment.

# Zero Spam

Email hints for users and mail server operators

## Server-side approach

This is where it gets boring and tedious and any non-technical person will probably stop reading. However, the server-side configuration is actually where the majority of the work should be happening that prevents you from receiving spam email. Nevertheless, from all of the client-side steps mentioned above, changing your email address after an abuse has been detected is the most important one. This implies that you tell your email service provider to remove your old email, or you will continue to get spam.

### **Server Rule 1:**        *“Only maintain valid email addresses”*

There is no point in keeping email addresses that are no longer used. It is amazing how long spammers keep sending to old email addresses. The email server will simply reject those if they have been properly removed. Based on my experience, this makes up the largest amount of spam hitting a mail server. But it will never be seen by the users.

### **Server Rule 2:**        *“Don’t allow relaying of emails.”*

Any email server that allows relaying of emails basically applies no security at all. It doesn’t care where the emails are coming from nor where they are going to. That’s very bad. Indeed, some of these relaying mail servers are blacklisted by some spam databases. If you don’t configure your mail server properly and it relays for any amount of time it is quite possible that it will be blacklisted and then you are likely to be excluded from receiving emails from reputable mail servers.

Email that’s being received should only be going to a known address within your domain. Email that’s being sent should only be sent from an address within your domain.

### **Server Rule 3:**        *“Do header checks.”*

This may be as simple as checking the subject line for ‘I love you’, which was associated with a computer virus some time ago, etc.

### **Server Rule 4:**        *“Do contents checks.”*

This is similarly a scan of the message body for known virus markers, etc.

## Zero Spam

Email hints for users and mail server operators

### **Server Rule 5:**        *“Do address checks.”*

First of all there should be a syntax check that the from address and sender domain matches. This requires a DNS lookup, which might slow down the mail processing a little, but it's worth it. Then there should be a check against any current spam database that checks if the address or domain is listed as an origin of spam.

Currently I know of only two reliable spam databases:

Sbl-xbl.spamhaus.org and  
Bl.spamcop.net

There used to be a third, [dsn.rfc-ignorant.org](http://dsn.rfc-ignorant.org), but that's no longer functional. It still seems to be available though, but I can only recommend not to use it, because the result, as it happened to me once, can be that it screens out perfectly legitimate companies that may in the past have done something wrong to get onto their list, but are OK now.

### **Server Rule 6:**        *“Build up your own blacklists.”*

Check your Email logs regularly. If you see certain abuses repeating frequently or perhaps even a denial of service attack, block out those IP addresses either at your firewall or within the mail server configuration. This means that the mail processor will be kept free to deal with the actual mail.

### **Server Rule 7:**        *“Restrict the size of mailing lists.”*

Users don't necessarily consider the impact on the server if they plan to send a 10 MB attachment to 100 users. Don't let it happen. Limit the number of recipients on a distribution list to what is acceptable for your users. In my setup this number is very low. It also means that an external attack cannot abuse this feature.

The same applies to the size of individual emails. Set it to the minimum acceptable.

### **Server Rule 8:**        *“Apply any other prudent mail server configuration.”*

Mail servers, such as Postfix, have over 200 parameters that can be configured. I am not going to publish my precise mail server configuration, as that would be rather foolish. Rest assured that I have tuned my configuration over several years, with the end result of having no unwanted emails at all.

This does not mean that no unwanted emails reach the server. That is unfortunately not possible, based on today's email interoperability architecture. I get several hundred

## Zero Spam

Email hints for users and mail server operators

emails an hour. But most of them get either rejected or bounced for any one of many reasons, based on all of the checks that I apply, as stated above. The net result is that as an email user, I see none of it in my email client inbox.