Why You Should Never Use an ISP Email Address for Business

By Chris Wright
chris.wright@cwic-solutions.co.uk

Table of Contents

1 Why you should never use an ISP Mail address for Business

As a member and contributor to various Anti-"spam" forums, this is a subject that often appears. Now unless you have some technical understanding of how mail works, it is not surprising that many people are not aware of the pitfalls surrounding email.

This document will discuss the issue of using any ISP for email, and examine the various other options available.

The title was intended to be contentious in order to provoke the reader into understanding the concept of why it is potentially harmful to your business not to understand the effects of not controlling your email. It must also be made clear that there are good ISP's out there with which you could have no problems what so ever, but the points raised below still hold true for ANY ISP.

1.1 What do I mean by an ISP Business address?

There are many small businesses in the world that rely on a fairly small web site for their income and most often these come bundled with their ISP.

Along with your ISP you often get a number of email addresses to use any many people will create an address such as "sales@business.isp.net"

Where business would be replaced by the company name.

Many people will claim that they have had no problems in sending and receiving mail to addresses such as these.

When I present to them that they wouldn't necessarily know that there are problems it quite clearly shows that they don't fully understand how their email works.
Unless you physically check your mail server periodically, the chances are that you would never realise that any problems exist. And just how often do people check their email servers? As far as most people are concerned, they write a mail, hit send and that is the end of it.

1.2 Contact Email Addresses on your Web Site.

Most companies will provide an email address on their web site as a means of contact.
There are a couple of main reasons why this can lead to problems.

- Masses of "spam".
- Users unable to send mail to the address.
- User sends mail, but it's not received by you.

1.2.1 The Incoming "spam" Problem.

By including a mail address on your web site, you are asking that email account to be "spammed" out of existence. There is no bullet proof method of avoiding this, but you can reduce the effects which I shall cover in another article.

1.2.2 Users Unable to Send Mail

A user comes to your web page, decides they want to contact you and clicks on the email address link on your web page.
This opens up their mail application (what ever it may be).
They write and then send their mail.

The chances are that your customers could be using their own ISP to send mail, or they could be using Hotmail, Gmail or Yahoo or a similar service.

Later on they ***might***[1] get a message from their own mail server called a 'bounce message'.
When users receive a bounce message back, they will not likely understand the reason and just go to another site.
If they see the word “spam” in the bounce message, they are likely to leave with a bad opinion of your site, despite the fact it was their 'ISP' that was the result of the “spam” message.

1.2.3 User sends mail but it's not received by you.

An even worse scenario is when the user sends a mail which gets rejected by your mail server, but they do not get a 'bounce' message back. When this happens, they won't actually know that their mail was never received by you.
As far as the user is concerned they have sent you a mail but you could not be bothered to respond or they assume you are no longer in business.

In this case, they are likely to leave and not come back to your site again.

1.2.4 Solving the User Contacting You via Your web site Problem.

Rather than provide an email address on your web site, it would be much better to use a web form.

There could still be a problem with "spam" being entered on the form, but there are ways to prevent or reduce this.

Your web form application can email you the contents of the form, or write it into a local database from which you can retrieve the messages.
What this method does do is take the end users mail server out of the equation.

- What you should also do on your web form is inform the user of the email address from which they will be getting a reply to their inquiry.
- Remind them to add the address to their 'white list'[2] or exclude it from their "spam" filtering.
- Inform them that if they receive no reply, to check their "spam" folders and if still no luck, contact you via the web form once again to let you know of the problem and ask them to provide an alternate contact method.
- Just in case a user has a phobia about using web forms, provide a back up email address to be used a last resort and give them a message to let them know that.

1 I say “might” and the reasons are discussed later on.
2 “white list” - a list of known good email addresses or domains that your "spam" filter will not flag as "spam" regardless of whether they fail "spam" tests.

1.3 Getting No Replies to your Mail?

Having now provided a more reliable method for your customers to contact you, imagine you have received an inquiry from a customer.
You send a reply, but never hear anything back.
You send a further reply, but still nothing back.

Or imagine you send out a newsletter from your own ISP mail account.
But you have a really low return rate.

Does this mean that your customers are just not interested in you now?
(Then why would they contact you in the first place).

The chances are that the customer never received your mail in the first place.

For us to understand why, we must look briefly at how mail filters work.

1.3.1 Mail Filters – Brief Introduction

With the massive increase in “spam”, many email servers now incorporate filtering of your mail.
Some ISP's give you total control over the level of filtering, many give you known.
Some ISP's will have their own filtering that overrides your own settings.

It should be said that many ISP's do this with the best intention, but fail to realise that losing any mail can cost you money.

Filtering is performed using a number of methods and the following is a summary intended to show you the workings of it rather than a full technical description.

The following is a very basic example of how mail is sent and is for informational purposes only.

When you send an email, it leaves your machine and arrives at your outgoing mail server.
(As it leaves your PC, it gets stamped with your IP address of your machine and your IP address given to you by your ISP).

The message then leaves the sending email server and finally arrives at the recipients email server.

Your PC --> ISP Sending Server --> Recipients Mail Server --> Recipients PC

Before the recipient’s mail server accepts the mail it checks the IP address of where the mail came from against a list of blocked IP’s.
If it finds the IP your mail will be rejected and a bounce message sent back to you.

1.3.1.1 RBL's (Real Time Blackholes)

(Again, the following is a very simplistic description aimed at the very non-technical).

The RBL is nothing but a list of IP addresses.

- RBL's are the most widely used method of filtering mail.
- You can filter mail based on a geographic location, such as blocking all mail from China if you so wish.
- You can block mail that comes from ADSL customers, (to reduce the amount of mail from infected PC's on the network).

Two examples of RBL's are SPAMCOP and UCEPROTECT.

A mail filter will check the incoming mail and look through the list of IP's to see if yours is listed. If it's listed, then the mail server will bounce the mail.

1.3.2 How does an IP get listed on an RBL?

An IP can get listed on an RBL in a number of different ways. (The following is not a comprehensive list).

- Infected PC being used to send “spam” without the user’s knowledge.
- Compromised Email accounts being used without the user’s knowledge.
- Infected Mail Server
- Badly configured mail server.

By far the worst offender from the above are the Infected PC's being used as mail servers.
When “spam” first became a problem, the emails were coming from a handful of known mail servers used by spammers. It became easy to block them since there were very few IP's being used. A single mail server would send many millions of “spam” but by blocking the IP of that machine, you would wipe out the effectiveness of the “spammer”.

So the spammers needed a new method and this involved a *botnet*[3] of *Zombie*[4] machines.
Rather than have one machine sending a million emails, they can have a million machines sending a few each. If one IP becomes blacklisted, then they only lose a small proportion of their “spam” run.

1.3.3 How does that affect your ISP Business Email Account

Because so many home users PC's are infected with badaware/trojans/virus/trojans, many of them are being used as part of networks to send out masses of “spam”.
Ultimately these PC's and the networks they belong to end up on a RBL.

It won't necessarily be your IP that end up on the RBL, but the IP address of your ISP's mail server. Even though your ISP is likely to have many mail servers, each one handles possibly millions of message per day for thousands of users. It only takes one user to send one spam mail to a 'spamtrap'[5] and that whole server and everyone who uses it will be affected.

3 In this context, a Botnet is a collection of machines on a network that can be tasked to perform various tasks under the control of the “Botnet controller”. Sending spam via email is just one use of a “botnet”.

4 A “Zombie” machine is one that has been compromised by a security cracker, a computer virus, or a trojan horse. A “botnet” is usually made up of “zombie” machines.

5 A “spamtrap” is an email address that is created to trap spammers. It usually hides on a web page and is not visible to normal users. A spammer will use a tool to trawl web pages, find the email address and add it to his list. Since no human would ever send a mail to the address, the sending mail server is assumed to be spam friendly.

When you now send out your mail using your ISP's mail server, the chances are that it will get blocked by the recipient's mail server.
At the very best, the message might get tagged with a "spam" tag, and filtered into the users "spam" folder, but that now relies upon the user to check their "spam" folder on a regular basis.

Another problem that became apparent with some UK ISP's during 2006 was that they were effectively deleting the rejection messages that are sent by the recipient's mail server.
If you send a message to someone and it is rejected, usually a message is sent back to the sender informing the sender of the reason for rejection. These rejection messages were being deleted, so the sender had no clue that their message was being rejected at any stage.

There have been several discussions as to whether this was an intentional act on the part of the ISP's, with some claiming that it was easier for the ISP's to deny there was a problem with their servers than fix the problem itself.

It is also worth noting that rejection messages are not always sent, but for the majority they are.

1.4 Improving your mail reliability

If you don't use your ISP mail servers, there are two possible options:

a. Using the mail server on your Web Server

b. Dedicated Mail Server Account.

Most often small businesses will change the From: or Return Address fields in their mail client to their company domain (sales@mycompany.com).

Nearly all spam uses faked "From:" and "Reply To:" fields.
If you reply to spam, you are not replying to the sender themselves, just an innocent bystander, if indeed the faked address actually exists.

So when the recipient receives the mail, it appears to have come from "mycompany.com".
It is only when someone looks at the headers that they can see which mail server it really came from. (That someone can also be your "spam" detection software rather than just a real person).

1.4.1 Using "Faked" From: and Reply To: Fields

If you use your ISP to send the mail and just change the From: or Return Address: fields, then the IP's will differ and this can raise flags and cause mail to be rejected.

By using the same server for mail and web services, then the sending IP will match the domain name and this reduces some problems.
Some spam filters will check to see if the sending mail address domain matches that of the IP in the header.
Nearly all spam uses faked "From:" and "Reply To:" fields. If you reply to spam, you are not replying to the sender themselves, just an innocent bystander, if indeed the faked address actually exists.

It should be noted that the method of changing the From: and Reply To: fields is an acceptable practice and has been in use since the early days of email. It is only down to the abuse of this method by spammers that causes potential problems.

1.4.2 Using the Mail Server on your Web Server.

Many businesses will have their own web pages on a web server . More often or not, these web servers also come with their own mail server and a number of accounts.

Although this is a massive improvement over using your ISP, there are also pitfalls associated with this method.

Unless you have your own dedicated server, the chances are your web site is hosted on a machine along with hundreds and sometimes thousands of other users.

So although your mail server has its own unique IP address which can be matched to your domain, that same mail server and IP address is potentially being used by thousands of other users.

If the web or mail server get misused either intentionally by a user or becomes 'hacked' and is used to send "spam", that IP address could be flagged and end up on a RBL.
Web servers themselves have access to email functions, (for example when using forms), and it is most often compromised web pages that lead to these machines been listed on RBL's.

If you have a good web host, the chances are that the IP address will not be listed on the RBL for too long, but conversely, there are many bad web hosting companies out there that are either slow to respond, or don't care what happens on their machines so long as they get paid.

1.4.3 Dedicated Mail Server Account

When you buy a domain name you probably realize that you can host your web site anywhere you like. And you can move it around as often as you like whenever you like. Provided you keep renewing your domain name it is yours for life.
This is one benefit of using your domain name for email rather than an ISP address.

"sales@mycompanyname.ispname.co.uk"

"sales@mycompanyname.co.uk"

If you change your ISP, then you have to change your email address, notify existing customers and update literature and web site pages.

What few people don't realize is that you can have your web server on one machine, and your mail server on a different machine. They don't even have to be in the same country, or with the same company.

By using a company that solely than has dedicated mail servers, they are more likely to keep control of the users that use them. They will do everything they can to keep their servers from being listed in RBL's, since that will harm their business.
Email is their business; therefore it is in their best interests to keep their service free from problems.

This is not to say there are any bad email companies out there, but you stand a much better chance of getting a first rate mail service from a company that has mail services as a central part of its business plan, and not just an 'extra' (as you would get with your ISP, or your web hosting provider).

And the final thing that most people don't realize is the cost.
You don't have to go the whole way and get your own dedicated machine just to host your own mail

server.
You can do a similar thing with your mail server as you would with a mail server and get a shared mail server. Provided it is with a company who deals primarily with mail, the risks of suffering from abuse by other users should be considerably less.

1.5 Conclusions

Email forms a vital part of communicating with your customers whether it be from you to them or vice versa.

- Ensuring that your email server you use to send your email does not get listed on black lists is essential. (Whether that be your ISP or your own email server hosted elsewhere)
- Providing a reliable method for your customers to contact you is essential.
  Relying on their own email to reach you will lead to lost emails.
- Using your own domain name gives a more professional look to your email.
  Including your ISP name in your email address should be avoided if only for the image it portrays. If a company can't afford £9.99 for its own domain name, what sort of company image does that project?
- Relying on your ISP to keep its email servers off of black lists is dangerous.

1.5.1 Why do the problem exist?

I have long argued that ISP's should rename themselves as ICPs (Internet Connection Providers). These days ISP's main aim is to provide a connection to the internet and all its other features are 'bonuses', (email, web space, phone provider etc).

Consider a few years ago when cheap (and even free) internet connections became possible; it led to a massive boom in people connecting to the internet. If you take Freeserve for example, all you had to do was walk into any Dixons or Curry's store, and pick up a CD, plug it in your PC at home and you were connected.
Almost overnight there was a massive increase in the number of people connecting to the internet that had little or no knowledge of PC security or how their internet connection worked. (I am not saying that this is their fault. There are arguments that Windows contributed to this, but that is another argument totally). Ultimately this led to a massive increase in the number of infected PC's on the Freeserve network. Even today, France has the highest proportion of infected PC's in Europe and Wanadoo being a French company (that coincidently owns most of the large UK ISP's), has nearly every one of its mail servers listed on nearly all of the black lists available.
No sooner than a Wanadoo email server leaves a black list, it gets listed almost immediately.

ISP's do not have the money to invest in customer support to deal with email problems related to spam. It is not cost effective for them to handle it at a customer level. With this in mind, many tend to incorporate spam filtering at a higher level.
Spam reports to abuse desks can run to millions per day, and that only takes into consideration the spam that is actually reported. (90% of all the email sent in December 2006 was spam and that is predicted to rise to 97% in 2007 - http://m-net.net.nz/1321/security/news/the-security-forecast-for-2007-yet-more-spam.php)

1.5.2 How to check if your mail server is listed on a RBL?

You can check quite easily if your domain name is present on any spam database by using the tool at DNS Stuff (http://www.dnsstuff.com/).

Using DNS Stuff will also give you an idea of just
But simply testing for your domain name isn't a good enough test if you use a forged From: and Reply To: fields, or a different mail server to your domain name (i.e. Your ISP mail server).
In this case, you need to search the spam database by IP, and determining your IP of your sending mail can be tricky since in theory it can vary each time you send a mail.
I will detail the exact procedure in a different article at later date.