

Theft of Services

By Bob Osgoodby

Theft of Services

Bob Osgoodby
bob@adv-marketing.com

Advanced Marketing <http://adv-marketing.com>

Spammers will use many tricks in their effort to "ply their wares". One of the most common is to use someone else's email address as their return address. Another is to link to images contained in their email, which are on your web site, illegally using your bandwidth.

Using a stolen email address as their return address, is becoming quite common, as some Internet Service Providers are checking to ensure that the sending address is valid before relaying the message. They have started doing this due to the "raft of complaints" received about mail going out with a phony return address.

The consequences of this can be quite far reaching for the person whose address has been stolen. This happened to me late last year. It was a porno ad that was sent out bearing my return address. I got over 7,000 requests to remove their name from my mailing list in a 3 day period. Many were quite nasty, threatening all sorts of things. I called "At Home", who provides my cable service, to see if there was anything I could do about it. Their advice was to use a different email address.

Fortunately it was an address that I don't use for business, and if it was, it would have been far more serious. The real problem here is not that your ISP will shut you down for spamming, as it is fairly simple to find out that you didn't send it, regardless of the return address.

There are three potential problems however, that you may have to deal with.

The first is the number of "bounces" (bad email addresses that cannot be delivered). Many ISP's program their servers to shut down an email account that is getting a large number of bounces, as it is one of the symptoms of a denial of service attack. If your bounces exceed a certain number - usually around 500, your web server may automatically go into a "self protect" mode and shut down your email address.

If you start receiving many bounce notifications, immediately notify your ISP of the problem, telling them that someone has illegally used your return address. If it was an email address that you use for business, the bad press that you get can be devastating. You should write a short email explaining what had happened, and send it to everyone who sends you a complaint. While this sounds like a Herculean Task if you are getting thousands, you can use an email package such as Eudora to do this automatically. You can download this software from our web site at:

<http://adv-marketing.com/business/freebie.htm>

Another problem is that you can be quite sure that someone will report you to "Spam Cop", who in

turn places a complaint with your ISP. Spam Cop may not check the validity of a complaint prior to notifying your ISP, which I feel is unconscionable on their part. Unfortunately, if they do forward the complaint to your ISP, you will have to defend yourself. That is why you should immediately notify your ISP if this happens. If you have a copy of the spam, be sure to send it along with your notification, and also save a copy in case it is needed later.

The second major problem a spammer can cause, is to steal an image from your web site that they use in their email. If they send their email in HTML format, and many do, they can actually link to an image on your web site. They are in effect stealing your bandwidth. Many web servers have bandwidth limits, which limit the amount of information you can send and receive each month. If you exceed that limit, you could be liable for additional charges from your web space provider.

If they do this to you, your only recourse is to change the name of the image, displayed on your web site that they are stealing. Another effective step is to replace the original image that they are using. Replace it with a notification that the sender of the email has stolen the image from you, and advise anyone who receives it not to do business with them. Once you do this, anyone who receives their spam will receive your warning.

When you get down to the bottom line, even people who send out emails with forged addresses are stealing. If you receive hundreds of spam emails a day with no way to have your name removed from their list, they are using your resources without your permission. You then have to sort through all this "junk mail" to find your legitimate email.

Theft of services is a serious problem. Unfortunately, it appears that the only solution will be through legislation making it illegal, and provide severe punishments for the guilty parties.

Did you know that subscribers to Bob Osgoodby's Free Ezine the "Tip of the Day" get a Free Ad for their Business at his Web Site? Great Business and Computer Tips - Monday thru Friday. Instructions on how to place your ad are in the Newsletter. Subscribe at:

<http://adv-marketing.com/business/subscribe2.htm>

[Get-Articles.com : 1000's of reprintable business and internet marketing-related articles.](#)

[Submit your article for reprint.](#)