Address Munging Considered Harmful

Matt Curtin
<cmcurtin@interhack.net>

Date: 1998/12/08 02:34:45

Abstract

Many solutions have been suggested to manage the problem of Internet abuse. These methods have varying degrees of success and utility. I argue that the practice of address munging is in itself a problem. Those who mine the Internet in search of a quick buck without regard to their negative effect are akin to terrorists, and rather than close our eyes, we netizens must fight them, intelligently and effectively. We must not allow those who abuse the Internet to destroy it, or to push us to destroy it.

1 Introduction

The problem of net abuse is a relatively new one in the history of what is now known as the Internet community. However, it has now been more than four years since our first sightings of massive Internet abuse, and in that time, we have learned a number of things about it and how to deal with it. Unfortunately, some of these methods are themselves problematic.

1.1 What is Address Munging?

"Munging" (sometimes also inappropriately called "spam blocking") is the practice of turning email addresses into a form that humans can understand, but that is unreadable by computers. For example, `<foo@example.com.no-spam>` is a munged version of the address `<foo@example.com>`. A human can easily determine the correct address, but software designed to read email addresses will read the address incorrectly.

1.2 Why Do People Munge Addresses?

A number of self-serving, money-hungry, socially irresponsible, and otherwise obnoxious people have become Internet users in recent years. Many of these people who fancy themselves "marketers" have mined various Internet sources for email addresses to whom to send advertisements via email. An increasing number of users who are becoming desperate for and end to the endless parade advertisements for pyramid schemes, miracle cures, and "bulk email services" have taken to preventing the "publication" of their email addresses.

Some users who resist publication of their email addresses no longer participate in any sort of public online message exchange, such as Usenet and mailing lists. Others have begun to munge their addresses to prevent spammers from harvesting them for use in their lists of spam targets.

There is even a Usenet FAQ that discusses how to effectively munge addresses at `http://members.aol.com/emailfaq/mungfaq.html` .

2 Dealing With Terrorism

To understand the reasoning behind this document, it is useful to know something about how spamming is akin to terrorist activity.

2.1 Why "Terrorism" is an Appropriate Term

Terrorism is the practice of using fear to accomplish an objective, probably one that is unpopular. In general, this is best done by breaking the rules of society in such a way—such as hijacking passenger airplanes and planting bombs in busy metropolitan areas—that people will be motivated to give into the demands of the terrorist.

Spamming, as well as other practices which can be more abstractly called "Internet abuse", are similar to terrorism in that during the course of accomplishing their objectives—often making a lot of money with comparatively little work, the rules of society are broken. Historically, an overwhelming theme of the Internet has been one of respect for the resource, as well as the time and resources of other members of the Internet community. Spammers wantonly disregard the Internet's unique culture, using a number of arguments in an attempt to justify their own selfish, disrespectful behavior. No matter how you look at it, the issue of spam takes the time, money, and resources of millions of Internet users and administrators, without their consent, and even against their will. This is in every way contrary to the Internet's culture.

2.2 Goals of the Terrorist

A terrorist can be motivated by a number of things. Perhaps he is part of a group of people who have been subjected to a foreign government's authority without representation. In that case, he might be using fear of attack as a tool to gain representation in the government over him. Perhaps he is hoping to overthrow a government in power. In that case, he could be hoping to effectively break the operational ability of the government by eliminating some number of its leaders, using fear to prevent them from working against the terrorist's agenda, or both.

2.3 Why Terrorists Have an Inherent Advantage

By the very nature of the ideological battle between terrorists and societies, the playing field is not level. That is, societies, in some form or another, agree to abide by some set of rules. These typically include limitations of the government's power, requiring some sort of process for guilt to be established, and a framework for sentencing criminals.

Terrorists, on the other hand, have no rules, or at least they allow themselves more freedom in action than do the societies against which they fight. If a terrorist's goal is to subvert a government or to overturn a society, he succeeds if he is able to make the government ineffective or if he succeeds in making the society break its own rules, even if dealing with him.

The society itself can only win if the terrorist is stopped. It can be argued that any changes in the society's rules in order to stop the terrorist are, in some sense, a loss.

2.4 How Munging is Letting Terrorists Win

Address munging, by definition, is breaking some of the Internet's functionality. As such, some of its value is lost. Rather than allow the Internet to be broken, piece by piece, by those who show no respect for it, we netizens should stand our ground and fight those who do not wish to become part of our society, but rather want only to make a quick buck from it at the expense and to the detriment of others.

3 Eliminating Spam

Those who munge their addresses are generally not interested in decreasing the value of the Internet, or breaking any of its functionality. They simply want spam to stop.

3.1 Economics of Spam

People send spam because it's cheap enough that even if it does not work as advertised, the loss to the spammer is not significant. This issue has been covered in greater detail in many other documents about network abuse, so it's not necessary to cover that here.

3.2 Making Spam Ineffective

The best way to eliminate spam is to eliminate its effectiveness. That is, by having the accounts from which the spam originates canceled quickly—before the spam is finished being sent—and taking down web sites and email drop boxes advertised with spam before any replies can be accumulated, we can make spam a completely ineffective method of promoting a service or product on the Internet.

As noted above, however, this is only the first step. The cost of spamming must be made higher. Some are doing this through legislation, others through private litigation, and some ISPs through expensive "clean-up" charges applied to the spammers through the terms-of-service agreement. However, in order for any of these to take place, it is necessary to catch and then complain about the spam.

3.3 Catching the Spam

You might say "Yeah, but if I don't munge my address, the spammers will get me!" That, to some extent, is true. But neither will you get them. That is, you can close your eyes to the problem, but it doesn't go away, and you will suffer the effects, in the form of higher costs from ISPs who have to employ staff to deal with network abuse, degraded quality of service in the form of legitimate mail relays bogged down with spam and wasted bandwidth, and other unpleasant side-effects.

Sending mail to your munged address costs the spammer nothing. It brings his accounts no closer to elimination. However, if you are effective at complaining about spam, you can actually increase the spammers' costs and make his business model even less effective by having his accounts deleted and his feeds eliminated.

4 How Address Munging Hurts

As noted earlier, address munging does not hurt the spammer in any way, or bring the problem any closer to elimination. It merely provides a way for you to usually close your eyes to the problem.

4.1 Spammers Do Not See Bounces

Some have munged their address in hopes of creating more bounces for the spammer to handle. In practice, this simply does not work, since the origin is forged, almost without exception.

4.2 Violating Standards

The standards upon which Usenet is built, that is, the specification for the system's operation, requires that the poster use a legitimate email address. Making exceptions to standards simply for short-term convenience is unwise at best. At worst, it jeopardizes the Internet's long-term viability to continue the same level of utility that it has enjoyed.

Allowing standards to be broken is contradictory to the philosophy behind the Internet, that is, of specific, published standards for system operation. It is this philosophy that has allowed the Internet to grow to meet the tremendous demands placed on it, not only in total volume, but in growth, during this decade. Systems built on other philosophies have not been able to approach the Internet's level of scalability or longevity. This suggests that the Internet's way of doing things is right.

4.3 More Hassle for Innocent Third Parties

Those who manage the systems whose addresses have been forged or whose hosts have been used for relaying will need to deal with even more bounces than usual.

4.4 Additional Hassle for You

In addition, you will have some hassle trying to juggle your munged and non-munged addresses, trying to remember which to use for each occasion, and having to set it back and forth. And if you forget to switch to your munged address and post to Usenet, all of the effort you've put forth to protect your address will have gone to waste.

4.5 There Is No Silver Bullet

Even someone who perfectly manages their munged addresses will receive spam at some point. The battle between spammers and other netizens is essentially an arms race. Each measure that one takes eventually has a countermeasure from the other group. You might find that as spammers and those who sell lists of targets become more sophisticated, those lists will be "de-munged" by increasingly intelligent harvesting software.

The end result is that all of the effort you put in to hiding your address goes to waste.

Rather than spending that precious energy trying in vain to protect your address, why not invest that energy into learning how to use effective tools for complaining about net abuse, thereby actually working to solve the problem (by making spam less effective) rather than just closing your eyes to it?

5 Complaining About Spam

Section four of the Email Abuse FAQ at `http://members.aol.com/emailfaq/emailfaq.html#4a` covers how to effectively complain about spam.

I personally use *adcomplain.pl* (periodically posted to `alt.sources` and elsewhere) and the abuse.net service[1] Such tools have reduced the amount of time for complaining about spam to just a second or two longer than necessary to delete the message. Additionally, my mail server is protected with the MAPS (Mail Abuse Prevention System) RBL (Realtime Black List)[2], which prevents it from accepting mail from mail servers known to send spam and not work to prevent it.

6 Conclusion

Though active in many Usenet newsgroups, mailing lists, and being listed in numerous directories for various projects around the Internet, I spend less than 10 minutes of each day dealing with spam. This isn't to say I do not get any spam, but rather that using the tools available, I can effectively fight spam without breaking the Internet or spending huge amounts of time.

I urge all netizens to play their part—however great or small—in stopping spam, by standing their ground against spam, neither by "learning to accept it" nor by reducing the quality and functionality of the Internet.

[1] More information available from `http://www.abuse.net/` .
[2] More information available from `http://maps.vix.com/rbl/` .