

WHITE PAPER

A User's Guide to SPAM Prevention

By Steve Glass, Site Tuneups

<http://www.sitetuneups.com>

Introduction

SPAM, we all know what it is; that horrible email from people we don't know selling product we don't want, filling our in baskets day after day. If we are unfortunate, we get tons of it, while they guy at the desk next to us gets maybe two a day. Why does this happen? Why can't anybody stop it? Can we make it go away forever?

In this paper we'll take a close look at SPAM; what it is (and is not), why some of us get more than others, and what can be done about it. We will look past simply filtering or white-listing to examine more proactive methods of dealing with SPAM by preventing or inhibiting address acquisition. This discussion is fairly comprehensive, so not all solutions will fit all situations. However, it is hoped that in general we might be able to ease the burden if we can't eliminate it.

A Few Rules

Here are few important things to remember during this discussion:

- Individuals who are getting a lot of SPAM will not eliminate it in the near term. The goal is to reduce the flow for those who get a lot of SPAM.
- In general, the purveyors of SPAM value email addresses in the following hierarchy, worst to best:
 - Generic addresses such as info@domain.com or webmaster@domain.com
 - Personal addresses such as david0102@yahoo.com or janet@holidaygiftbaskets.com
 - Personal addresses where the recipient has allowed something to happen that proves he/she really monitors that email address
 - Personal addresses where the recipient has clicked on a link
 - Personal addresses where the recipient spent time on the target web site
 - Personal addresses where the recipient made a purchase

Spammers generally get paid for results. So, the Spammer will work with Clients to track the behavior of anyone who clicks a link right through to purchase. If the individual buys something, the Spammer knows and records this, and that Individual's address becomes more valuable on the SPAM market.

- Many Spammers try to maintain the quality of their lists, so they are always re-verifying their information. If an address disappears from the Web, or someone who has previously clicked through has not done so in a very long time, the address loses value.
- Every email address exposed in some way on the Internet will eventually be targeted by a Spammer. Special programs called Harvester Bots search for and download web page files. A Bot then searches each file for strings of characters that look like email addresses, which the Bot saves. There are many, many Bots, and they do not miss very much.

Armed with these rules, let's talk about some of the ways that Spammers obtain addresses, and what the individual can do about it.

How Spammers Find New Targets, and How to Prevent It

Email Addresses on Web Sites

The Problem—It is very easy to place an address on a web site for visitors to use as contact information. Unfortunately this also makes an address available to Bots.

Solutions

1. Remove personal addresses from the web site, substitute generic addresses such as info@domain.com. The generic address will still receive spam, but will not be as highly valued as the personal address. Also, the generic address can be checked occasionally with an online email system usually provided as a service by the ISP, so the SPAM email does not appear on the desktop.
2. Use a form. An online form passes the form data to a program running on the web server. That program is responsible for checking the form data and either saving it or sending an email to a designated address with the form data enclosed. Because the target email address is in a server-side program, it is not exposed on a web page. NOTE: many ISP's provide access to a third party form processing program such as the ubiquitous Formmail. These require that the form pass an email address as a "hidden" value, which means the address is actually exposed in the HTML. While form processors can be convenient and versatile, they have little value in reducing SPAM.

Some Visitors find forms offensive and impersonal. A possible follow-on solution is to provide a drop-down list with employees names that the visitor can select. A key for the selected name is then passed to the server-side program, which selects the appropriate email address. The drawback is that both the form and the program must be changed whenever there is a personnel change. This could be overcome with a simple Content Management System (CMS) which maintains a list of employee names in a database. The online form is then built dynamically from the current list, so that the Visitor can select an individual he/she wants to send a message to without exposing any email addresses.

Email Addresses in Domain Registry Listings

The Problem—When a domain is registered, an email address must be provided for Administrative and Technical contact. These addresses are published, and easy for Harvester Bots to access.

Solutions

1. Most registrars provide a service that takes the contact data private. There may be a fee for this.
2. A generic address can be supplied for administrative contact. Often the Host ISP will supply an address that may be used for technical contact. NOTE: Domain Holders are REQUIRED by their agreement with the Registrar to keep contact information current, to include an email address that is real and monitored. This address may be the only method a Registrar uses to contact the Domain Holder when the domain registration is about to expire.

Indiscriminate Use of Email Address on the Web

The Problem—Many victims of excessive SPAM are guilty of some or all of the following behaviors:

- Using personal email address for blog comments, or Facebook or other social networking site
- Using a personal email address in an online advertising/marketing site such as Craigslist
- Posting a personal email address on any public profile

- Participating in an event such as a trade show or conference, and allowing a personal email address to be posted on the conference/trade show web site

Solutions

1. Many blogs and other sites will accept a Gravatar (globally recognized avatar) in lieu of an email address for posting. The blog (or other) site software check with the Gravatar issuer to see if the Gravatar is legitimate. The Gravatar issuer uses encryption to hide the user's email address.
2. Create a "throw-away" address. Something associated with a personal brand (thespeakingcoach@domain.com for example) can be used. Use this address for registering for conferences etc., migrating any real contacts from this address to the permanent address. Retire the throw-away when it becomes saturated with SPAM. Some users may wish to check the throw-away a few times after retiring for anything useful.

Buying ANYTHING as the result of a SPAM Solicitation

The Problem—The SPAM email offered something the Individual really wanted, the individual went to the Client's site and made a purchase.

Solutions—**There aren't any.** The Spammer considers buyers to be premium list material, and charges accordingly for those email addresses. The Merchant also targets the address, and may sell the address to non-competitors. Individuals should consider retiring the email address, and re-evaluating their online habits.

Buying from a Legitimate Online Retailer and Not-Opting Out

The Problem—Any good online retailer will ask if they can send email to the buyer. Often the request comes right at the point of decision, where the Buyer is otherwise distracted, and fails to uncheck the box. Legitimate vendors will also supply a link to a Privacy Declaration when they request permission. Buyers rarely read these, as they are distracted by the online purchase they are trying to make..

Solutions—First, this is not SPAM. Buyer had an opportunity to opt-out. Buyer will also have an opportunity to opt-out with every email they get from the Retailer. The issue is when the Retailer has the right to sell Buyer's address or provide it to affiliates in accordance with the Privacy Declaration the Buyer did not read. Online buyers must deal only with legitimate online merchants, read Privacy Declarations, and opt-out when necessary.

You Gave Your Business Card to This Person Who....

The Problem—People collect business cards at networking events, and put them in their database

Solutions—This one is the subject of spirited debate, if you give your business card to someone you meet at a networking event, and they put you in their email database, are they spamming you? Online services such as AWeber say yes it is, if they did not ask you "Can I send you email"? If their content is not interesting, and a clear opt-out works, is the question not moot? There is no clear consensus on this, so any opinion is valid. Some selective diligence should probably be employed in passing out cards, as well as the occasional lie "Sorry, I ran out".

Goldfish Bowl Syndrome

The Problem—Some individuals drop a business card in every goldfish bowl they see, sincere in the belief that they will win lunch, or possibly a new car.

Solutions—The free lunch still is not free, someone paid for it and expects consideration, in this case contact information they can use. This method is traditionally grist for the telemarketing mill, but is increasingly used in email marketing also. Whether or not this is SPAM is a subject for debate (did the individual Opt-in or not?). In either event, a legitimate marketer will be happy to reveal how the contact

information will be used, often in writing on request. If they cannot or will not, it might be better to pass on this golden opportunity.

Dictionary Harvest Attacks

The Problem—Many Spammers target an ISP's mail servers, bombarding them with random email addresses and recording all of the ones that don't bounce.

Solutions—This is the ISP's issue, and most are very diligent about detecting and thwarting these attacks. Many email servers are now delivered with protection built in. Some attacks still get through, and if the problem persists, it may be time to change ISP's and email addresses.

Conclusion

Most of the solutions in this paper simply call for good habits and diligence. Consistency is all, even one slip will be recorded, and move an email address higher up the hierarchy. Spammers can't sell an address to a Client when the Client does not make money from that transaction. The goal for individuals is a permanent spot on the "dead address" list. With help from a competent and diligent Service Provider who protects against Dictionary attacks and filters the obvious SPAM, it is possible to bring the amount of SPAM down to a minimum.