

SPAM ... SPAM SPAM ... Why does it keep coming back?

Internet users, irrespective of what they already know, will be well aware of 'SPAM' - an annoying element discovered in e-mail in-boxes. Considered as a nightmare for the e-marketer (and the e-mail user), 'SPAM' keeps coming back despite our best efforts. Why is it so? Let's look into what exactly spam is and its various facets.

'Spam' is defined as unsolicited e-mail on the Internet. From the sender's point-of-view, it's a form of bulk-mail, often sent to a list culled from subscribers to a Usenet discussion group or obtained by companies that specialize in creating e-mail distribution lists. In general, it's not considered good netiquette to send spam. It's generally equivalent to unsolicited phone marketing calls except that the user pays for part of the message since everyone shares the cost of maintaining the Internet.

Also referred to as junk e-mail, the term 'spam' may have its origin in the Monty Python song "*Spam spam spam spam, spam spam spam spam, lovely spam, wonderful spam...*" Like the song, unsolicited e-mail is endlessly repetitious. Another theory is that the term originated from a computer group lab at the University of Southern California, which postulated that unwanted e-mail has the same characteristics as canned meat.

What is 'SPAM'?

Spam is the act of flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam mail is commercial advertising, often for dubious products, get-rich-quick schemes or quasi-legal services. SPAM' costs the sender very little to send - most of the costs are paid for by the recipient or the carriers rather than by the sender.

There are two main types of spam, and they have different effects on Internet users. Cancelable Usenet Spam is a single message sent to 20 or more Usenet newsgroups. Usenet Spam is aimed at "lurkers", people who read newsgroups but rarely or never post and give their address away. Usenet Spam robs users of the utility of the newsgroups by overwhelming them with a barrage of advertising or other irrelevant posts. Furthermore, Usenet Spam subverts the ability of system administrators and owners to manage the topics they accept on their systems.

E-mail Spam targets individual users with direct mail messages. E-mail Spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses. E-mail Spam typically costs recipients money, out-of-pocket. Spam is an additional cost for anyone with a measured phone service who reads or receives their mail while the meter is running, so to speak. On top of that, it costs money for ISPs and online services to transmit spam and these costs are transmitted directly to subscribers.

One particularly nasty variant of E-Mail Spam exploits mailing lists (public or private e-mail discussion forums). Because many mailing lists limit activity to their subscribers, spammers will use automated tools to subscribe to as many mailing lists as possible, so that they

can grab address lists to sell to other spammers or use the mailing lists themselves as a direct target for their own attacks.

Why 'SPAM' Survives

It's always been a baffling question. Why - when everyone is inclined to hate spam so much - does so much of it keep piling-up and coming back in our e-mail inboxes? A study done by the Robert H. Smith School of Business at the University of Maryland found that on average Americans receive nearly 20 spam messages a day.

Amount of Spam Received Daily according to US Adult Internet Users, November 2004 (as a % of respondents)	
0*	22%
1-4	18%
5-9	16%
10-19	13%
20-39	12%
40 or more	11%
Not sure how many	8%
Median per day	5 spam e-mails
Mean per day	18.5 spam e-mails
<small>Note: n=418; *A user who reports "0" spam e-mails per day may still receive spam occasionally</small>	
<small>Source: Center for Excellence in Service at the Robert H. Smith School of Business, University of Maryland; Rockbridge Associates, Inc., February 2005</small>	
<small>062867 ©2005 eMarketer, Inc. www.eMarketer.com</small>	

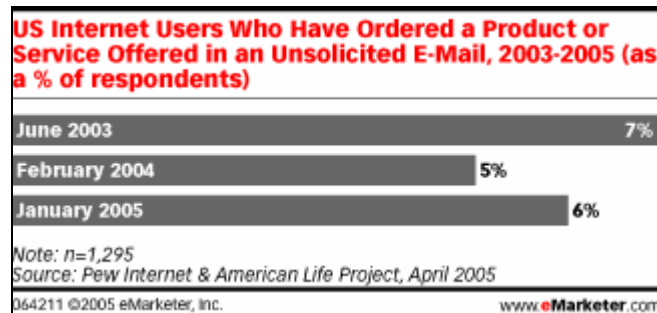
No one wants spam. In fact, there are people willing to pay handsomely to avoid it. IDC, a premier global provider of market intelligence, advisory services and information technology events, projects that Anti-Spam product and service revenues will climb close to \$2 Billion by 2008.

Worldwide Anti-Spam Solution Revenues, 2003 & 2008 (in billions)	
2003	\$0.3
2008	\$1.7
<small>Note: CAGR=42%</small>	
<small>Source: International Data Corporation (IDC), February 2005</small>	
<small>063133 ©2005 eMarketer, Inc. www.eMarketer.com</small>	

Nevertheless, the spam still keeps coming back. According to a new survey of nearly 800 end users, comprising 34% corporate business users and 66% consumers, by Mirapoint and the Radicati Group, the answer is simple: Many of the people who claim to hate spam are supporting the practice by buying products from spammers. The survey found that 11% of users purchase products and services from Email Spam - even though 9% of users have lost money through fraud, orchestrated by e-mail scammers.

Even if they don't buy the products, 39% of users admit to clicking on embedded links within a spam message, other than the unsubscribe link. Clicking links within a spam e-mail not only alerts the spammer that the e-mail address is active, it also directs users to websites that install viruses, spyware and other malicious code. Not surprisingly, 57% of respondents who click on spam links were found to receive more spam than average.

The findings are even more perplexing than a study conducted this year by the Pew Internet and American Life Project, which found that 6% of Americans online buy from spammers.



How to stop SPAM?

Unfortunately, many of us spend so much time filtering and deleting spam that our biggest concern has become that we do not lose messages we really want. Many opt-in e-mail newsletters are being incorrectly filtered, so recipients who sign-up never receive them. And even personal communication and one-on-one e-mail is now regularly being filtered at the server level.

In fact, according to an article in Time Magazine, 40% to 70% of all e-mails are currently getting blocked by spam filters, preventing them from being received. Ironically, the cure has become as bad as the disease. This is especially true of some filtering solutions with over-zealous criteria. Nevertheless, here are seven good tips that will help you dramatically reduce the amount of spam you receive. We have noted that implementing these tips and resources, has reduced the amount of spam we receive by over 55%.

Seven tips that could help you reduce or stop spam:

Tip-1: Use a separate e-mail address when you post messages to any public forum, such as newsgroups and mailing lists. Never use your personal e-mail address for this purpose -- or you'll be flooded with spam. You can then quickly go through the e-mail in this account to check for emails that aren't spam. This ensures that your main personal e-mail address won't be as clogged with spam. *For Example:* AOL users can set up a special user name for free to use for postings. They can then just discontinue that account if they start to get too much spam.

Tip-2: Consider acquiring multiple e-mail addresses for different purposes. This helps you to identify different sources and senders, and lets you filter more effectively. For instance, you may have one for personal use only by friends, family or colleagues that is never used to request information or to subscribe to newsletters, discussion lists, etc. Another might be used just for sales inquiries or orders, or for making online purchases. This can be arranged through your ISP, web-host or through any number of online e-mail service providers. Even free mail services like Yahoo Mail and Gmail can be used for this purpose.

Tip-3: You can subscribe to services online that provide you with disposable addresses that can be deleted if they begin to attract spam messages. You can create a unique address for each e-mail newsletter or forum you subscribe to. Then, when an e-mail address starts receiving spam, you 'throw it away' and start using another e-mail address. This works because the disposable e-mail addresses actually forward to your real e-mail address. The software lets you track which addresses are receiving spam, and you can just re-subscribe using a new, spam-free address.

For information on disposable addresses, visit:
<http://email.about.com/library/weekly/aa072002a.htm>
A company that offers free disposable e-mail accounts is Sneakemail.
<http://sneakemail.com>

Tip-4: Remove your e-mail address from your website. If you list or link to your e-mail address, you can expect to be spammed. Automatic address-harvesting programs can scan your website and extract email addresses. So remove them wherever possible and use web-based forms instead. This will drastically cut down the amount of spam you receive if you have a website.

Tip-5: NEVER buy anything from a company that spams. Don't visit their sites or ask for more information. Responding to their spam mail only encourages them to continue spamming - they only need a tiny fraction of responses to be profitable. Here's another reason not to buy anything from a company that spam; over 95% of spam offers are scams! In fact, not responding to spam is the single most effective way to avoid getting scammed on the Internet.

Tip-6: Filter your e-mail. Using filters is key to managing your e-mail effectively. It may take a short time to figure out how to do this, but it's definitely worthwhile. For more Anti-Spam filtering information visit: <http://email.about.com/cs/spamfiltering>. For more on negative spam filtering, visit: <http://email.about.com/library/howto/htnegativespamfilter.htm>

Tip-7: Consider subscribing to a spam prevention service. We're not enthusiastic about these services ourselves, but many people find them invaluable. They range from the good to the bad to the downright ugly, free or fee-based. Many of these services are "challenge response" services. This means they require potential spammers to make responses by clicking, visiting a website, and/or typing in a code that only a human (not a spam bot) could do correctly.

Unfortunately, many people -- and most newsletter publishers -- simply refuse to participate. That's because it requires people who are sending you legitimate e-mail to take THEIR time to ensure YOU get e-mail.

Tip to Implement: Make sure that any software or system you select gives YOU control of which e-mail you get, without automatically erasing your messages. On a related note, safeguard your newsletter and discussion list subscriptions. If you, your ISP or web-host use spam filters or white lists, be sure to let them know that you want to receive messages from any newsletters or discussion lists that you subscribe to. Do it as soon as you sign-up, otherwise it's very easy not to notice that you're not receiving them.

While these seven tips may not actually stop spam, they will certainly help you drastically reduce the amount of spam you get.

ANTI-SPAM ~ How to Efficiently Complain about 'SPAM' Mail

Listed here are eight steps that have proved to be helpful in efficiently carrying out a complaint:

Step-1: Identify the Spammer

To find out to whom to complain, first you must find out who sent the e-mail. Look at the header (see at the end of page) of the e-mail you received and locate the "Received by:" line. Just below that, find the "From:" line, which contains an e-mail address, e.g.

useless@spam.com. Be aware that some spammers mask their location by using one or more relays, so you may have several "Received by:" lines.

Step-2: Find the Spammer's Provider

Next we have to find out who provides the spammer with his/her services, like the domain host, web-host and ISP. Start by performing a WHOIS lookup of the domain name you located in Step-1. This can be done at several sites, such as <http://resellers.tucows.com/opensrs/whois>

Here you want to find the DNS or NAME SERVERS, often being something like: NS1.PROVIDER.COM.

If the DNS or NAME SERVER is different from the domain name located in Step-1, e.g. NS1.SPAMMERSHOST.COM, then proceed to Step-3.

If DNS or NAME SERVER is the same domain name as the one located in Step-1, e.g. NS1.SPAM.COM then proceed to Step-4.

Step-3: Filing the Complaint

Most DNS/WEB/ISP providers have an e-mail address set up for abuse called abuse@provider.com. Send an e-mail to the DNS or NAMESERVER host located in Step-2 (NS1.PROVIDER.COM), e.g. abuse@spammershost.com. Be sure to include the COMPLETE header located in Step-1.

Below is a standard complaint mail you can use or you can write your own. Just remember, more often than not, the provider has no previous knowledge of the spamming, so be firm but also be polite (After all, you want the provider to take action against the spammer)

Dear Sir/Madam,

I have received unsolicited spam mail from what appears to be one of your customers.

Please investigate and take action against your customer to prevent recurrence of this incident.

Find below headers of the offending spam mail:

(insert headers located in Step-1)

Sincerely,

Your name

You may also include (forward) the offending spam mail you received, but most providers will require the headers of the e-mail before they'll react. This address may not always be valid, in which case you should proceed to Step-7

Step-4: Finding the Spammer's Alternate Providers

Sometimes the DNS or NAME SERVER listed on a WHOIS lookup will be the same as the offending domain. In this case you have to do a TRACEROUTE to locate alternate providers for the spammer. Many sites offer TRACEROUTE services such as: <http://www.opus1.com/www/traceroute.html>

Enter the domain name located in Step-1, and check the box "Round-up the usual suspects", then hit the trace button. The last entry on the TRACEROUTE list will often be either the spammer's domain or spammer's host's domain. If the last entry is the same as the spammer's domain, e.g. HOST-123.456.789.0.SPAM.COM, then proceed to Step-5

If last entry is different from spammer's domain, e.g. HOST-123.456.789.9.SPAMMERSHOST.COM, then proceed to Step-7

Step-5: Traceroute Result same as Spammer

If the last entry is the same as the spammer's domain then an e-mail address is listed to the right of the hostname, e.g. client@spam.spammershost.com. Send the email from Step-3 to abuse@spammershost.com. This address may not always be valid, in which case you should proceed to Step-7

Step-6: Traceroute Result Different from Spammer

If the last entry is different from the spammer's domain, you should see something like HOST-123.456.789.9.SPAMMERSHOST.COM. Send the e-mail from Step-3 to abuse@spammershost.com. This address may not always be valid, in which case you should proceed to Step-7

Step-7: Invalid E-mail Address

If you get an e-mail back stating that abuse@spammershost.com does not exist, you can try and visit their website, which will often be <http://www.spammershost.com>, and see if they have listed any spam-complaint procedures. If not, you can always try and locate an e-mail address to the domain-host from their web-pages (often listed under "Contact" or "Who are we" sections). If you still get no result, you should proceed to Step-8.

Step-8: No Response from Spammer's Provider

If you do not get a response from the spammer's provider or if they refuse to take action on the spam complaint you can try and file a complaint with the provider's provider. In Step-4 you performed a TRACEROUTE, which showed the route of providers to the spammer. The last entry is often either the spammer or the spammer's provider. The second-last entry will often be spammer's provider's provider. Now follow Step 5 or 6, but use the second-last entry instead of the last entry.

Additional Options: Filing a complaint with the spammer's provider is the most important step to stop spam, but it is not the only one. Most spam mails promote some product from a third party merchant, who likes spam about as much as you do, and quite often directly prohibits the use of spam by affiliates. Click the link in the e-mail (yes, the one the spammer wants you to click), this action will often lead you to an address called something like <http://www.merchant.com/signup.php?refID=9999> or something similar. Just take out everything after the .com, making it <http://www.merchant.com> and then locate an e-mail address to the merchant (most often found in the "Contact" or "Who are we" sections). If they don't have these sections just look around some more, almost all merchants will have a contact e-mail listed somewhere. Then, send a complaint e-mail to that address.

Here, you will often benefit from forwarding the entire spam mail which you received. Many merchants will immediately cancel the affiliate account, especially because they get to keep the money this affiliate had otherwise earned; money that is now "tainted" by spam.

CONCLUSION: Most ISPs dislike spam as much as the rest of us, some even more. An ISP risks being placed on a "black-list" if they are reported as not following up on spam complaints. Other ISPs block these black-listed ISPs, resulting in all kinds of unpleasant things for the offending/non-responsive ISP, such as having their mail blocked. Thus, normal, non-spamming customers of that ISP will see their normal, harmless e-mails blocked and have their customers

complain that they are not delivering a satisfactory service. In the end, the ISP risks losing good customers, which is something they would like to actively prevent. And they can, by reacting to spam complaints.

As for the merchants, when they keep the money, the spammers lose the benefits from their spamming activities and thus have no reason left to spam. If you are consistent and report most if not every spam incident, you will see results. First, the offending spammers will lose their services such as domains, hosting accounts and even Internet access in some cases. Secondly, for the long term, you're sending a message to spammers that you will no longer tolerate this invasion of your Internet experience and the rate of spamming activity will decrease.

Many people buy spam protection in the form of various software - this shouldn't be necessary, and WON'T be necessary if you take an active part in combating spammers. There is only one effective way to stop spam. As Marcel Nienhuis of the Radicati Group says, "*If people stop buying products from spam, it would probably go away.*"

REMEMBER: Spammers can only exist as long as we allow them to spam without complaining! Don't let Spammers exist - Complain! It's your Internet!

For more information on 'SPAM' check out:

- The superb spamFAQ maintained by rocket scientist Ken Hollis at digital.net/~gandalf/spamfaq.html
- The ominous-sounding 'Death to Spam' page by Steven Rimmer at Alchemy Mindworks www.mindworkshop.com/alchemy/nospam.html

For information on CAN-SPAM-ACT 2003 visit:

- <http://www.spamlaws.com/federal/can-spam.shtml>
- <http://www.ftc.gov/bcp/online/pubs/buspubs/canspam.htm>
- http://en.wikipedia.org/wiki/Can_Spam_Act_of_2003

Source/Reference URLs:

- www.spam.abuse.net
- www.antispam.radio-showtime.com
- www.scambusters.org/stopspam

- www.iptv.org/digital/dictionary_internet.cfm
- www.emarketer.com/Article.aspx?1003490
- www.faculty.valencia.cc.fl.us/jdelisle/lis2004/glossary.htm