# Spam ju-jitsu – disposable email addresses

### *Jon Jermey - 1524 words*

*Take advantage of this wonderful offer right now! Just enter your email address and we will add you to our mailing list!*

How many times have you read this? And what do you do about it? Most ‘wonderful offers’ are spam bait, of course, but now and then an opportunity comes along that you want to take up. It could be a shareware application that you are keen to trial, for instance, or a mailing list that you want to examine before you commit yourself. Do you sigh with resignation and submit your email address, or lose out on the opportunity? Now there is a third option: you can use a disposable email address for each new subscription. Check the response via your disposable address and if it’s what you need, then transfer the subscription across to a real address: if not then just leave it alone and it will disappear into cyber-limbo, along with all the follow-up spam emails despatched to that same address. Like ju-jitsu, disposable email addresses use the spammers’ own strengths against them; without the time to check thousands of addresses, they are unable to stop their junk email plunging into a electronic black hole.

Disposable email systems come in three strengths: free basic, free standard and commercial. This article looks at each in turn, starting with…

## *Mailinator – when forgetting is a virtue*

The free Mailinator site (**www.mailinator.com**), developed in the US by Paul Tyma, has the simplicity of genius. It works like a vast net, catching thousands of emails every minute – but only for an hour or two. New recipient accounts are generated on the spot: as soon as a message arrives addressed to, say, *jon26September@mailinator.com*, that account springs into existence and the intended recipient – or anyone else with Internet access – can point a web browser to the Mailinator site and see what that account has received. Messages stick around for ‘a couple of hours’ according to the site documentation, then disappear. No message is ever stored on disk; they exist, briefly, only in electronic memory – a handy feature, Tyma notes, which reduces the incidence of subpoenas for messages with legal implications. Once all the messages for a particular account are gone, the account goes too. Some account names – like *bob@mailinator.com* – are used so often they exist more or less permanently, but these are the exception.

Tyma explains the elegant reasoning behind his site and its implementation on his blog at **paultyma.blogspot.com**. Since email transmission is virtually instantaneous these days, and since most spammers aren’t willing to take the time to check whether the addresses you give them are ‘real’, why not generate a temporary new address to receive each response as and when it is needed? Every spam message sent to a non-existent address at Mailinator is one less spam message sent to a real person.

Of course, spammers don't like having their mail consigned to limbo in this way, and nor do some other legitimate businesses that want to maintain a valid contact address for their current or potential customers. A minority of sites have set up filtering rules on the email addresses they will accept, with the intention of screening out disposable email sites like Mailinator. Tyma's response has been to register a number of other domain names which act as alternatives to *mailinator.com*: demonstrating his sense of humour, these include *spamherelots.com* and *thisisnotmyrealemail.com*.

A recent development on Mailinator has been the addition of aliases. Each valid Mailinator address now has an unguessable alias which redirects mail into that account. For instance, the alias of *jon26september@mailinator.com* is *M8R-3mq5x3@mailinator.com*. If I give only the second address to someone then they can write to me, but they can't log on to the Mailinator site as 'jon26september' and read other messages that I may be getting at that address.

And that's Mailinator: a very elegant solution to a pervasive problem. Its funding appears to come from a deal Tyma has struck with a local web hosting system, though there is an address on the site for sales enquiries, so he may be planning to expand his sponsorship. Meanwhile he has recently applied the same clear thinking to the chat system and developed Talkinator, a free open access chat system that allows a single chat channel to be shared between many websites and/or blogs. Let's hope he continues to come up with many such good ideas.

## *Disposable plus: Spamgourmet*

A similarly devastating combination of altruism and ruthlessness can be seen on the Spamgourmet site (**www.spamgourmet.com**). This also provides disposable email addresses, but unlike Mailinator these are private and have a medium-term existence. Spamgourmet requires its users to login with a username and password, and provide a *real* email address, in order to use its services. This is called the 'protected address', and the email Spamgourmet receives for you is automatically redirected on to your protected address.

Like Mailinator, Spamgourmet automatically accepts all incoming mail addressed to *...@spamgourmet.com*. How does it know which mail is meant for me? Because my 'fake' addresses all incorporate my Spamgourmet username. Say for instance my Spamgourmet username is *harryw* and my real address is *hwayne@bigpond.com*. If I subscribe to a mailing list using the disposable address *ebooklist.**harryw**@spamgourmet.com*, then when email arrives from that list Spamgourmet will use the fake address to identify my username, and use my username to look up my real address. The email is then forwarded to that address with some additional text in the header to indicate that it has come via Spamgourmet. Thus Spamgourmet acts as a barrier between the world and my real email address, in the same way that my PayPal identity acts as a barrier between the world and my real credit card number.

What makes Spamgourmet more than a simple redirecting site, however, is the fact that – unless I specify otherwise – any Spamgourmet address automatically expires after a set number of emails have been received. The default is three; so in the example given above, the first three emails to *ebooklist.harryw@spamgourmet.com* would be passed through to me, and any subsequent emails will be bounced. This will give me a chance to evaluate whether the mailing list is worth pursuing, and if so I can then join with my real address or tweak my Spamgourmet settings to let more emails through – see how below.

One quick way to specify the number of emails Spamgourmet will allow is to include the number in the address – for instance, *manymails.20.harryw@spamgourmet.com* will let through the first twenty mails sent to that address, whereas *onlyone.1.harryw@spamgourmet.com* will let through the first email received only.

More advanced settings allow the Spamgourmet service to be extensively tweaked. Users can change the default number of emails they want to receive at their disposable addresses. They can add 'trusted senders', whose mail is sent on regardless of how many items that address has already received. They can define secret 'watchwords', to prevent other people coining new addresses on their behalf: for instance, if harryw defined the watchword 'potato', only mail to addresses including the word 'potato' would be accepted, and all others would be blocked. Mail to onepotato.harryw@spamgourmet.com would get through but mail to twoyams.harryw@spamgourmet.com would not. And the reply-to addresses in the forwarded messages you send can be modified to pass back through Spamgourmet, where your real reply address is replaced with the Spamgourmet address. Finally, like Mailinator, Spamgourmet has also registered several other domains which can be used when registration sites are unhappy with the ...*@spamgourmet.com* extension.

Spamgourmet is free, although grateful users are supplied with a link which allows them to donate via PayPal or credit card. Like Paul Tyma's blog, the Spamgourmet FAQ page indicates the extent to which the development team have thought about their customers' needs and how to best address them. Both sites pay tribute to the advantages of running an unpaid service: it releases them from the responsibility of having to meet legal requirements and contractual obligations, and allows them to get on with the job of making fast effective code. But do commercial spam blocking services offer more?

Spamex (www.spamex.com) is a typical commercial system disposal email system. For $US9.95 per year it makes the same features available as the advanced Spamgourmet settings, with one important addition: Spamex will also store and pass on attachments, which neither of the free systems will. As you might expect, Spamex also has customer support and a customer discussion forum. It also offers an enterprise edition for businesses. MailMoat (www.mailmoat.com) is a similar system charging $US20 per year.

So if the option to receive unsolicited attachments at an anonymous address is worth a dollar a month to you, then Spamex may be your system: otherwise Mailinator or Spamgourmet should give you all you need. Next time you get an offer you can't refuse, use the potential spammer's strengths against him with some disposable email ju-jitsu.

But don't forget: you'll still need an email add-on system like ThunderBayes and some spam protection set up in your anti-virus program to catch any lowlifes who have somehow managed to get hold of your real address.