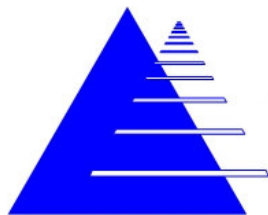


The '7 secrets' to eliminate sp@m

This is the full article written by our chosen associate Rob from Unite Innovations part one was published in our February newsletter. I do hope you find this useful.

Anita Jones – Altered Ego Design Ltd

PO Box 24367
Manners St
Wellington
Aotearoa NZ



Unite Innovations Ltd
*Unlimited
IT Engineering*

Overview

90% of all internet traffic is now estimated to be sp@m; Never mind that this means 90% of our multi-trillion dollar global infrastructure is effectively going to waste; Never mind that Internet Service Providers and businesses are spending additional multi-billion dollars a year on fighting sp@m. The REAL problem is the massive list of useless email messages in your inbox on Monday morning or, worse, after a long weekend or a holiday. The time you waste sifting through them is one thing; the message you accidentally delete that WAS a genuine message (probably the one with the biggest order of the year, or the one from your boss/wife/ex-girlfriend) is yet another.

Sp@m is the biggest threat to the internet today. And although one day we'll think of sp@m as a thing of the past, that day is still a wee while off and until then we'll have to live with it and protect ourselves (and our businesses) from it as best as we can.

For the uninitiated: what is sp@m?

Sp@m is unsolicited email. And the way internet-based email was designed, it has proven to be the perfect vehicle for it. Sending an email message to millions of addresses is as simple and

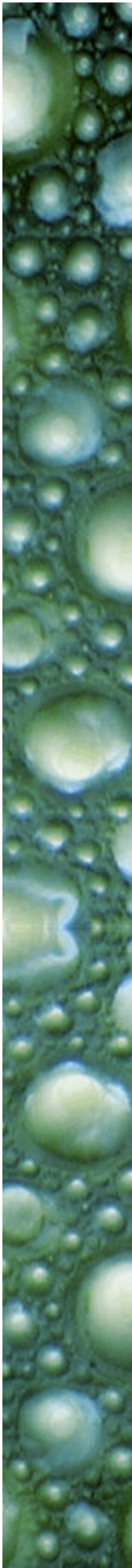
Altered Ego Design Ltd

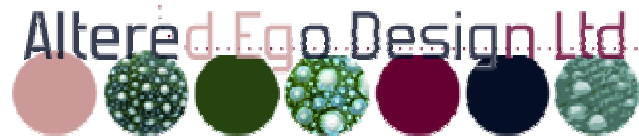
- We create websites that improve your business bottom line-

PO Box 24 367 | Manners St | Wellington | New Zealand

T: 04 473 6588 M: 021 779 303 E: anita@alteredego.co.nz WWW.alteredegodesign.co.nz

All information contained in this document is subject to our intellectual property, subject to copyright and intended only for the person or entity to which it is addressed. It may contain confidential or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you receive this in error, please contact Altered Ego Design and delete the material from your records.





cheap as sending one to your colleague in the next door office. And this 'opportunity' has been taken up by large quantities of people selling anything and everything, although given the reputation of this type of 'marketing', usually of a questionable nature.

So, do people actually respond to this type of marketing? Apparently! It is estimated that if 0.00001% of actual recipients reply by ordering the offered product (and they do!) then you can have a viable 'business'.

What is NOT sp@m?

Viruses often replicate via 'mass email'. However, this is relatively easily caught by virus scanners. Spyware is often 'distributed' through sp@mming mechanisms. Adequate Spyware filtering (incorporated in good virus scanners (you get what you pay for! (off-topic.....))) will deal to this though.

But even though these nasties use mass-mailing/sp@m as a distribution method, sp@m 'as such' is neither a virus nor Spyware.

Allow yourself to be confused; you're in good company. But the bottom line is: your virus scanner is not going to protect you from sp@m, which is a very common misunderstanding.

So, what CAN we do about sp@m?

For a start, accept that sp@m is now a 'fact of life' (at least for the foreseeable future), and you'll never get rid of it completely. What you can get rid of however, is the quantities that some organizations receive which irrefutably cost them time, money and headaches.

Much of the work is done by your Internet Service Provider (ISP) if you let them (more on the 'if' later). The ISPs as the 'crossroads' of most email are ideal places where costly software ('sp@m filter') is utilized to scan messages for what is undeniably unsolicited nuisance mail. However, your ISP has an obligation to you to provide you with reliable email. And every time a messages is filtering out, this remains a judgment call which no ISP is prepared to make on your behalf if that means running the risk of one day accidentally filtering out that one message that was important enough for you to sue them for \$\$\$-million dollars in lost revenue. Therefore, these filters have to stay on the conservative side of what might be considered 'sp@m'. The result is that a significant portion of unwanted mail still makes it through the filters onto and into your inbox.

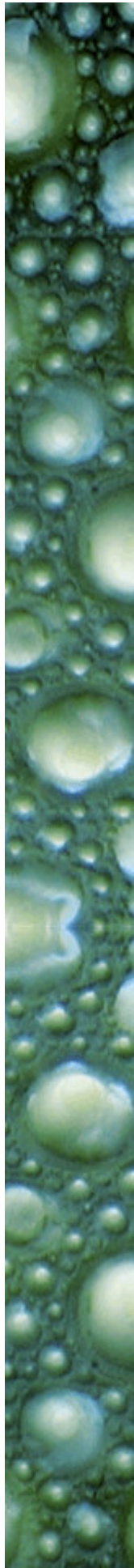
Altered Ego Design Ltd

- We create websites that improve your business bottom line-

PO Box 24 367 | Manners St | Wellington | New Zealand

T: 04 473 6588 M: 021 779 303 E: anita@alteredego.co.nz WWW.alteredegodesign.co.nz

All information contained in this document is subject to our intellectual property, subject to copyright and intended only for the person or entity to which it is addressed. It may contain confidential or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you receive this in error, please contact Altered Ego Design and delete the material from your records.



PO Box 24367
Manners St
Wellington
Aotearoa NZ



What's worse, most sp@m filters operate on a number of factors, one of the most important one being 'key words'; messages with the occurrence of certain words are more likely to be sp@m. Recently, however, a new form of messages has flooded the internet whereby the 'message' (including 'keywords') is actually presented as a 'graphic picture' rather than as normal text, effectively bypassing most sp@m filtering.

So, leaving it all up to your ISP is not going to do the job adequately. But there are a number of things you can do too!

PO Box 24367
Manners St
Wellington
Aotearoa NZ

For a start, let's see how sp@m mail 'finds' you. Or rather, how did they find out about your email address in the first place? Chances are: 'you told them'. You may have entered your email address at some website one day, requesting a complimentary copy of a gardening magazine you had never heard of. Or signed an 'online petition' to better the world, or anything else to trick the unwary internet user into surrendering their email address. Since then, your email address has been sold (yes: sold) together with millions of other addresses to whomever wants to presents you the 'opportunity' to buy something you didn't ask for, you don't need, and which probably doesn't exist in the first place.

Therefore:

Tip 1: Use caution giving out your email address to unknown parties (online or otherwise); preferably stick to known, reputable companies only.

Many sp@m messages contain a section that says: 'if you no longer wish to receive these messages, click here....or reply with in the subject line ' or something along those lines. As soon as you do this, you have acknowledged that your address is actually an address of a 'real' person assuring a secure place on the lists of the sp@mmers fraternity for good.

Tip 2: Never respond to a sp@m message, not even (or particularly not) in an attempt to stop receiving it or to (tempting) abuse the crap out of the sender (which won't be an actual address anyway).

Some mail programs ('clients') have a built-in sp@m filter. Suspected messages are automatically moved to a dedicated folder or deleted. Because you are in charge of whether this filtering is turned on, and what happens to suspected messages, the vendor is much more comfortable to apply more stringent 'rules' than your ISP ever will. It is important however to

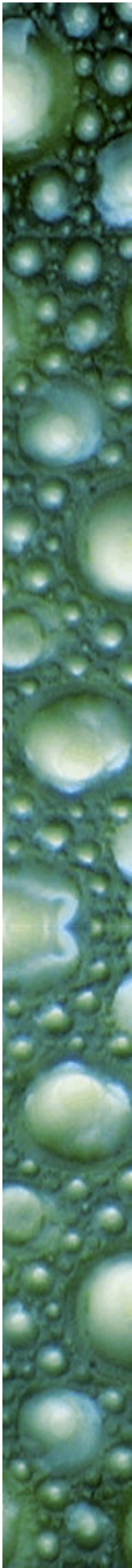
Altered Ego Design Ltd

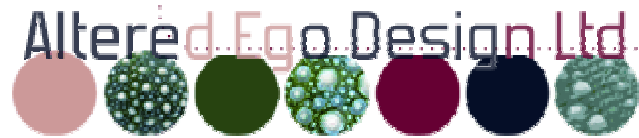
- We create websites that improve your business bottom line-

PO Box 24 367 | Manners St | Wellington | New Zealand

T: 04 473 6588 M: 021 779 303 E: anita@alteredego.co.nz WWW.alteredegodesign.co.nz

All information contained in this document is subject to our intellectual property, subject to copyright and intended only for the person or entity to which it is addressed. It may contain confidential or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you receive this in error, please contact Altered Ego Design and delete the material from your records.





keep your mail client up to date with its latest 'patches', 'fixes' and 'enhancements' in order for the sp@m filter to keep working efficiently.

For example, if you use MS Outlook, make sure your 'Automatic Updates' are configured to download the latest updates periodically and make sure that they are actually installed.

Tip 3: Keep your mail client's sp@m filter up to date.

But apart from these somewhat 'general guidelines' regarding sp@m, there are actually more active approaches as well.

Much sp@m is targeted at 'random addresses'. In other words, if your domain name is 'mycompany.com' then typical addresses attractive for spammers to assume are: 'info@mycompany.com', 'sales@....', 'support@....' etc.

What's more, it's easy for a spammer to automatically generate 'random' addresses, like: qwadfaewr@mycompany.com, or any letter combination 1% of which might resemble an actual address of a real person.

Historically, email systems were configured to have a 'catch all' account or to have all 'incorrectly addressed' mail forwarded to a 'postmaster'. E.g. if mail for matthew@mycompany.com was accidentally sent to mathew@mycompany.com (one 't' missing), the 'postmaster' (whoever the lucky one is that didn't attend the meeting....) would receive the message, spot the error, and forward it to the intended recipient.

However in this sp@m-age, poor postmaster by now will have either quit his job, asked for a raise, been taken to an asylum, or all of the above.

Matthew's error-prone name aside, 'catch-all accounts' and '(real person) postmasters' must be a thing of the past.

(In the example of 'Matthew' an 'alias' could be added to the mailbox called 'Mathew' so messages to the incorrectly spelled name would still appear in Matthew's inbox)

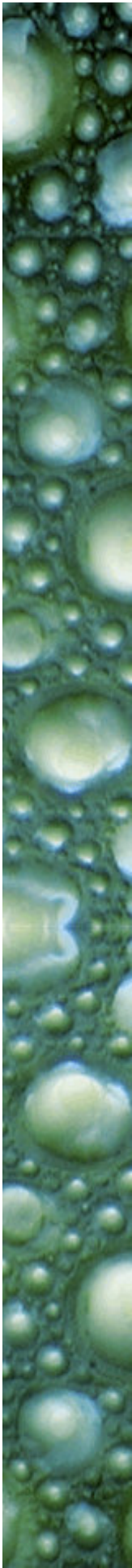
Altered Ego Design Ltd

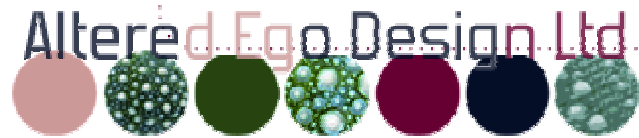
- We create websites that improve your business bottom line-

PO Box 24 367 | Manners St | Wellington | New Zealand

T: 04 473 6588 M: 021 779 303 E: anita@alteredego.co.nz WWW.alteredegodesign.co.nz

All information contained in this document is subject to our intellectual property, subject to copyright and intended only for the person or entity to which it is addressed. It may contain confidential or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you receive this in error, please contact Altered Ego Design and delete the material from your records.





Tip 4: 'Incorrectly addressed' mail must not be accepted by your email system or in any mailbox.

Depending on your setup, this may require configuration changes at your ISP, or (if you have one) on your own mail server.

Tip 5: Get rid of 'common' addresses like 'info@...', 'sales@...', etc.

Doing away with your 'info@mydomain.com', 'sales@...' etc. is a bit more painful. You like those addresses and your customers use them all the time. But if this is what it takes, tell your regular customers that the address has changed, and choose something less 'guessable' such as: 'mycompany_orders@...' you'll be amazed how much improvement there might be, to the point where you might actually find and read their orders from now on!

If you're dealing with larger quantities of (less regular) customers, chances are you solicit their custom via a website. Typically, there will be a link on the website for customers to order, or make an enquiry, or for whatever reason to contact you in some way or another, etc.

Such contact can be established in different ways. Typically, clicking the link will bring up an online form to fill in your order or request. Or it may bring up the email client on the (prospective) customer's screen with your email address in the 'To' field.

Additionally, many sites simply show the email address in readable written format:

'For enquiries, contact ilovesp@m@mycompany.com'. We will give you an answer in 6 months, IF we can find your message at all.

Tip 6: Never have your email address published on your (or any!) website.

You may have to get your web designer to follow this 'best practice':

Online inquiries, orders, etc. must only be handled through 'online forms'. Using the right technology the result of the form (the inquiry or order) is forwarded to you (the vendor/supplier) via email using a hard to guess email address.

Your customer never gets to see the email address their query or order is sent to. Nor can the address be extracted by anyone for addition to a sp@m list.

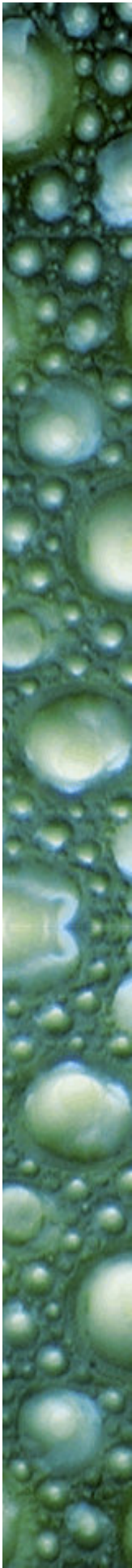
Altered Ego Design Ltd

- We create websites that improve your business bottom line-

PO Box 24 367 | Manners St | Wellington | New Zealand

T: 04 473 6588 M: 021 779 303 E: anita@alteredego.co.nz WWW.alteredegodesign.co.nz

All information contained in this document is subject to our intellectual property, subject to copyright and intended only for the person or entity to which it is addressed. It may contain confidential or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you receive this in error, please contact Altered Ego Design and delete the material from your records.





If you have to 'print' your email address, do so in a format which is not easily 'automatically' detectible, e.g.:

Our email address is:

d*o*w*n*w*i*t*h*s*p*a*m @ m*y*c*o*m*p*a*n*y*.c*o*m (without the '*'-s)

Last but not least, if you have your own email server (common ones are Microsoft Exchange, Microsoft Small Business Server', Mdaemon, (but there are many many others)), email can reach your server using one of two methods, both with their own advantages and disadvantages:

1. Messages are sent directly to your server, which forwards it to the end-users.

Advantage:

Mail is received 'instantly' without delay. You can receive a message from your friend/customer/business contact in Timbuktu while you have them on the phone, hearing them click the 'send' button.

Disadvantage:

Your mail server must be equipped with its own sp@m filtering software. This is not only expensive; sp@m filtering software also requires ongoing 'administration': the tighter the filter rules are (less sp@m getting through), the more genuine messages will be filtered out for examination and release by an administrator.

2. Messages are sent to your ISP. Your server collects messages periodically from the ISP and forwards them to the end-user.

Advantage:

Generally no need for sp@m filtering software on your own server. Your ISP's filter does (most of) the job, unless you have very specific needs for a much tighter filtering regime (see disadvantage above).

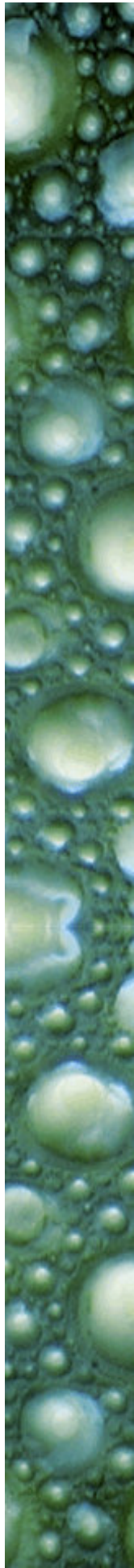
Altered Ego Design Ltd

- We create websites that improve your business bottom line-

PO Box 24 367 | Manners St | Wellington | New Zealand

T: 04 473 6588 M: 021 779 303 E: anita@alteredego.co.nz WWW.alteredegodesign.co.nz

All information contained in this document is subject to our intellectual property, subject to copyright and intended only for the person or entity to which it is addressed. It may contain confidential or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you receive this in error, please contact Altered Ego Design and delete the material from your records.





Disadvantage:

Due to the interval between subsequent collections, there is a delay in receiving mail. Also, all ISPs have limitations to the size of a mailbox and to the maximum size of each message. If you receive large messages (attachments) or don't 'collect' frequently enough, your mailbox might end up 'full', bouncing messages back to the sender.

(NB. Most ISPs have very(!) liberal limits to the mailbox and message size. Also, with current ADSL plans and prices, it is not uncommon to collect mail very frequently like every 10 or even 5 minutes).

Tip 7: Configure mail server to collect mail using POP instead of accept mail via SMTP.

With sp@m in the mix, in most cases the balance of advantages and disadvantages has tipped in favour of mail collection (technical term: POP-ing) rather than receiving directly (tech: SMTP). Configuration changes to your email sever and on your ISP side are required to change from SMTP to POP.

(NB: 'Microsoft Exchange 2003' requires third party software to POP mail. See:

<http://www.msexchange.org/software/POP3-Downloaders/>)

About the writer:

Rob Leenheer has been an IT consultant for over 10 years. He currently owns and manages a business providing innovative IT Solutions to the wider Nelson region.

For more information, contact:

Unite Innovations Ltd.

Ph. 0275 755416

Fax 03 526 8579

Email (without the stars and spaces): r*o*b @ u*n*i*t*e*.c*o*.n*z

Altered Ego Design Ltd

- We create websites that improve your business bottom line-

PO Box 24 367 | Manners St | Wellington | New Zealand

T: 04 473 6588 M: 021 779 303 E: anita@alteredego.co.nz WWW.alteredegodesign.co.nz

All information contained in this document is subject to our intellectual property, subject to copyright and intended only for the person or entity to which it is addressed. It may contain confidential or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you receive this in error, please contact Altered Ego Design and delete the material from your records.

