

Executive Stress

OFFICE SUPPORT

Newsletter — September 2003

Welcome!

Volume 3, Issue 3

With this quarter came the anniversary of my dad's death (10 July) and 9/11 - the passing of this 12 months, unlike any other, really hit me like running into a brick wall. I think when we lose someone - particularly someone who is close to you - one single fact eventually becomes blazingly obvious, especially on anniversaries such as this: and that is, life just goes on. The world continues to turn without us; there is still music, laughter.

The sun rises and sets; the seasons come and go. All without us. I sat in amazement for the longest time on 10 July wondering what I'd done in my life in that last 12 months - but moreso, wondering what difference has it made to the world or my place in it? Then into the office bounded my little girl, and I knew that my existence makes a difference in the life of at least one person ... And I guess that's really what this life is about.

I have many friends who lament "What's it all about?" or "Surely there's more to life than this?" And then I think of the nanno second it took for the passing of that 12 months and realise that we are the authors of our own lives. If things are not the way you want them ... MAKE THEM SO.

No-one else will do it for you and we only get one shot to make life all that it can be.

The meaning of life for me is simple: the laughter of your child and knowing you can help them be all that they can be. In the end what more is there?

On a more positive note, this quarter eSOS was a finalist in the 2003 Quest Business Achievers Awards. I'd like

"Slow down and enjoy life. It's not only the scenery you miss by going too fast - you also miss the sense of where you are going and why."

Eddie Cantor

to thank those clients who have supported and encouraged me over the last 3½ years - without you there'd be no "me"! :) The industry still struggles to gain recognition and respect, but we're getting there!

As many of you now know, I'm off with my family to New Zealand for a holiday in Oct/Nov - our first together in over 10 years, and my first away from the PC since I started the practice. Thanks to all clients for your willingness and flexibility in working with the arrangements in place for your continuing support needs during that time.

Inside this issue:

Announcements	2
New Clients	2
Hopi Prayer	3
Spamming the Spammers	3
Swen	4

Additional news this quarter is the inclusion of a private chat space on our site - which will be useful (and cheaper than phone calls) for those distant clients who need to communicate securely with me from time to time. And new credit card facilities for overseas clients and other payment options for domestic clients.

Till next quarter.

Virtually yours

Lyn P-B ✓

"At the end of our lives we will not remember how much money we made, how many ball games we watched, or how many things we possessed. What will come back to us in a brilliant and blinding light will be ... the quality of the relationships we formed with those we loved: our family, our spouse, our children, our friends."

Lilly - www.whispy.com

Disclaimer: Articles in this newsletter are for information purposes only. Readers should make their own enquiries before implementing any of the information contained herein. Neither eSOS nor Lyn Prowse-Bishop shall be held responsible for any loss or damage caused by following the information in any article contained herein.

Copyright © 2003 Executive Stress Office Support. All rights reserved

ANNOUNCEMENTS!

This quarter a couple of new and exciting things happened!

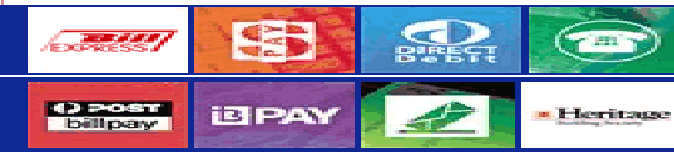
More ways to pay!



From your August invoice, clients would have noticed additional ways to pay. eSOS now have a merchant account with Stratapay, which offers clients a few ways to pay their bill.

Our preferred method of payment is still direct credit to our account. At this stage we've made available:

- BPAY – direct from your bank account to ours by quoting the reference number and biller code on your invoice.*
- Credit Card payment: *for overseas clients only*. By advising us of your credit card details, we can process your payment and the exchange is done for you. (This is not available to domestic clients at this time.)*
- Clients can also still pay by cheque if they do not have internet banking.



Stratapay actually offers eight ways to pay - though all are not available to eSOS clients at this time. If you would like a merchant account to give your own clients more ways to pay, Stratapay is a great option, with no monthly fees and lower rates per transaction than the banks. Visit

www.stratapay.com.au for more information. Contact us for an application form - you can save \$20 on the joining fee.

eSOS Recognised!

During September, Quest Community Newspapers held the Business Achievers Awards, where businesses across Brisbane were recognised for contributions, efforts or achievements. Executive Stress Office Support was a **finalist** in the IT category! Thank you to all our clients and supporters - without you, we wouldn't be here!



New Private Chat Room!

The eSOS site now has its own private chat room. This will be particularly useful for remote clients - or for other clients who may need to communicate needs to us whilst interstate or overseas. The chat room is secure and you will require a username and password to access it.

Should you require the use of this facility, simply schedule an appointment with us in Outlook, and ask us to make it online. We'll book the chat space for you and advise the URL, username and password.

FTP Those Audio Files!

We can now offer clients a dedicated FTP folder on our site allowing you the option of uploading audio files there and avoiding the problems of bounced email. If you would like to utilise this service, please contact us and we will arrange for a folder to be set up for you.

* Fees apply. See your invoice for details.

New Clients

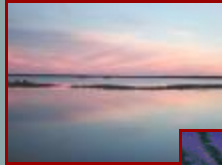
The following new clients benefited from partnering with eSOS during the last three months, and we welcome them!

🏢 International Infrastructure Management Ltd - Mr Graham Mulligan, Qld (Virtual Assistance)

Don't forget our **Referral Policy**: when you refer a new paying client to eSOS you will receive 10% off your next invoice of \$100 or over.

In Memory of Dad ... Hopi Prayer

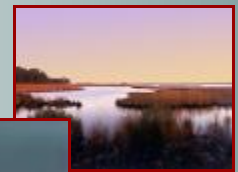
I found the following Hopi Prayer (author unknown), which really helped me explain this aspect of life to my daughter. I hope it helps those of you who have recently lost loved ones.



Do not stand at my grave and weep.
I am not there, I do not sleep.
I am the thousand winds that blow.
I am the diamond glint in the snow.
I am the sunlight on the ripened grain.
I am the autumn's gentle rain.

When you awaken in the morning hush,
I am the swift uplifting rush
Of quiet birds in circled flight.
I am the soft stars that shine at night.

Do not stand at my grave and cry,
I am not there,
I did not die.



Spamming Spammers: Fighting Spam - the Lighter Side!

The following (edited) article by Stewart Kirkpatrick gives a lighter view on fighting incessant spam.
(<http://www.news.scotsman.com/scitech.cfm?id=694642003>)

First, a word of comfort: it's not just you. Your friends have not been talking about you. There is not a hidden camera in your bedroom. Your email box may be stuffed with offers to make the male regenerative organ larger, but it's nothing personal. Everyone in the world with an email account has been offered a larger penis at some point. Even women. And, more worryingly, children.

The person sending the email does not know anything about its recipients because it's being sent to millions of people. Spam (mass unsolicited email) now accounts for half of all email. And a recent study by Symantec, an internet security firm, found that 80 per cent of children get adult-oriented spam - offering them drugs, dating services and financial offers along the lines of "send me your life savings and I'll give you millions of dollars. Honest."

And of course, there's the sexual spam. I get it by the bucketload. I get dozens of messages each day offering me "intimate enhancement", cures for impotence, Russian brides and, bizarrely, cheap printer ink cartridges.

This doesn't happen because I spend my time trawling dodgy sites looking for Slavic ladies with a thing for office supplies. I get so much spam because my email addresses regularly appear on the web.

Top tip: It's all a con. And if you fall for it A) you're an idiot and B) you're encouraging more spam.

Spammers use automatic programs called bots to crawl across the internet looking for emails. When they find one they pass it back to the spammer and he or she sends you his junk mail.

There is a way to defeat this. If you post your email on the web don't write it like this: skirkpatrick@scotsman.com, write it in words (skirkpatrick at scotsman dot com). The bots are looking for the magic "@" sign and don't understand "at".

Most people fight spam by ignoring it. However, it's getting harder to do this as a lot of spam tries to look like

(Continued on page 4)

Spamming Spammers (contd)

(Continued from page 3)

legitimate messages. Thus it is that you open an email like "Re: that thing you asked me" and find yourself faced with lurid text promising significant increases in length and firmness - usually when you're talking to your boss, mother or a party of vicars being shown round the office.

Top tip: If you open such an email and see an "unsubscribe" link at the bottom saying something like "click here to stop receiving emails like this", ignore it. All that will happen is that the spammer will be notified that your email address is used regularly and he or she will then sell it on to others. For this reason you should never reply to spam. In the rare event of your message getting through, you will only succeed in verifying that your email account is active.

Along with everyone else in the world, I've had enough of this. When I got my latest tranche of spam I decided to track down the person responsible.

I chose a message that purported to come from "Gertrude Godwin" because the name sounded like one of Dickens' less successful heroines. I was intrigued to find out why a minor character from the *Mystery of Edwin Drood* was offering me girth-increasing unguents.

I went to the site named in the email. I did a "whois" search on the URL (web address) through DNSstuff.com. This provided me with contact details for the person who owned that address. They appeared to be based in Mexico, but the information looked like it might be bogus. Lo and behold, the email address turned out to be false.

I then did a "traceroute" search on the URL, which showed me the connections that led my PC to the site. I followed this up with a whois search on the last IP address in the list. This gave me the name and address of an internet service provider in Pakistan.

However, just because the trail ended with that ISP, it did not mean that I had found "Gertrude". The original spammer was probably just routing his or her stuff through that ISP. I still had no concrete information on who they were.

At this point I realised I was floundering around and should stick to watching how the expert anti-spammers do it.



The first to catch my eye was Francis Uy. He successfully traced down a spammer and posted the man's name, address and contact details on a website - a practice that is becoming increasingly popular.

The spammer, George Alan Moore Jr, then sued, claiming that as a result he had received numerous threatening phone calls and hundreds of unsolicited magazines and catalogues.

Needless to say, his case was thrown out. But he did succeed in making himself very well known and now Mr Moore's contact details are very popular on the internet. This comment from a visitor to geek.com is typical:

"Don't anyone harass this guy: Maryland Internet Marketing LLC, George Alan Moore Jr, 300 Twin Oaks Rd, Linthicum MD, 21090-2154, 877-655-3438, 410-963-8226. Clearly he has suffered enough already at the hands of that cruel, cruel Francis Uy!"

Another anti-spammer trick is particularly fiendish. Spammers' email addresses are tracked and then collated on a website like Spamerang.net. Remember I mentioned that the spammers use bots to search for email addresses on the web? When they search Spamerang they pick up all those lovely email addresses and add them to spam lists. The spammers then spam each other.

But the anti-spam crown goes to "Man in the wilderness". His site, belps.freewebsites.com was being used by a spammer to mask her activities. He asked her to stop. She didn't. Big mistake.

"Man in the wilderness" is a computer security consultant, which means he knows a lot about hacking. He not only found the spammer, he hacked into her PC. He got a screenshot of her forging his domain. And he went through it with a fine-tooth comb digging out all sorts of personal information, secrets and details of scams. He discovered that the spammer had accomplices so he did the same to them.

He then anonymously turned over all the information to the authorities and posted it on his site. He even found a topless picture of the main spammer that she had stored on her hard drive. It's online too.

Of course, this kind of hacking is illegal, but then again so is flaying spammers alive and dousing them with lemon juice - and I don't think we should rule out any punishment for these scumbags. ✓

Swen - the newest offering from the hackers

Another day, another security scare! The latest offering is **W32.Swen.A@mm** and was covered in a special *Woody's Windows Watch*. The issue is reproduced here. Subscribe to *Woody's Windows Watch* by emailing WWW@woodyswatch.com.

Swen (contd)

About Swen / Avoiding Swen

W32.Swen.A@mm isn't that clever but, like many of these variants the reason they spread is because of the ways they are disguised.

It appears to come from Microsoft and while the software itself isn't anything particularly new, the format of delivery is.

But it does have some points of interest. If it runs on a computer it will try to protect itself by disabling some anti-virus programs that might be running. Swen also disables access to the Registry Editor.

If infected you may also see a fake MAPI error message that asks for various email details.

But there's nothing technically new. The standard precautions that we and everyone else have been recommending will protect you, in short:

- Have an **up-to-date** antivirus package. Set it to scan regularly and also monitor what happens on your computer. In this case 'up-to-date' means get the most recent update now - they've probably been revised in the last 24 hours due to Swen.
- Don't open email attachments unless you're very sure what they are and who they come from. This is a no brainer for most people because recent versions of Outlook stop you. While this can be annoying it does have advantages.

Getting Swen

What's attracted so much attention and questions is the way this virus arrives. It generally comes disguised as a message purporting to be from Microsoft. Unlike previous attempts (which were plain text and primitive), this one is HTML formatted to look like the MS web site design right down to links to the real Microsoft web site. It's similar in concept to the 'phishing' messages apparently from Paypal or banks.

The trick is that there's a phoney patch attached to the message. We've warned readers about this before but based on questions we've been getting the word hasn't got through:

Microsoft does NOT send software updates via email!!!

No reputable company would do it these days if

for no other reason than you can't tell the difference between real and fake patches. Companies may send out warnings and suggestions that you update your computer but the updates themselves are separately downloaded from the company's web site. In Microsoft's case it's via the Windows Update system.

However it is done it is NEVER by sending a patch as an email attachment. Any email you get, however sincere it might look, is bogus if it has an attachment.

As well as the fake Microsoft notice, Swen can also arrive as a fake mail delivery notice with a message like "I'm sorry I wasn't able to deliver your message to one or more destinations" plus an infected attachment.

The exact wording of the From and Subject lines does vary.

It can also be distributed via Kazza shared folders (using a variety of file names), IRC, network shares and some newsgroups.

If you get such a message - delete it.

Simple as that - hit the DEL key and get on with your life.

The FROM: address is faked so there's no point warning the sender. Don't waste your time notifying Microsoft, they know already; in any event there's little they can do.

More information

As usual Symantec has done a good job of going into the details of the attack. Much more information than most people will ever need is here:

<http://securityresponse.symantec.com/avcenter/venc/data/w32.swen.a@mm.html>.

There's some suggestions for blocking ports using a firewall to prevent future attacks and that's tempting to do in the heat of the moment. However those ports can be necessary for you to do your work so make sure you know what you're doing. ✓

Executive Stress

OFFICE SUPPORT

"Professional Assistance for the 21st Century Professional!"

Phone: +61-7-3271-6668
Fax: +61-7-3271-6668
Email: lyn@execstress.com

PO Box 1036
Oxley Qld 4075
Australia

Newsletter — September 2003

Volume 3, Issue 3
