News & info from...

Executive Stress OFFICE SUPPORT

Newsletter: Vol. 8, Issue 2 - June 2008

Quote: "What do I want to be when I grow up? I want to be old - really, really old."

- Laurie A. Gray, Socratic Parenting

In this Issue

WELCOME!

Dear [subscriber-firstname],

This last three months has just flown by! We've had another successful OIVAC - and now the steering committee is in for some well-earned rest! I'm SO tired ... as I'm sure the rest of the committee are!

We're at mid-year already and tax time again. Time to get your tax info together and clear out all the clutter. That's what I use end of financial year for ... I've managed to do my accounting "on the fly" so that's all up to date. That means end of year is time to get rid of all those old records hanging around so my shredder does double duty. That meant I was faced with two problems: finding the spare time to do the actual shredding, and mountains of shredded paper to deal with. The solution to the first problem was to enlist the help of my daughter - she gets $5 a pile to shred the paper for me. We then bag up the paper and take it to our local pet store for use in their kitten/puppy cages.

Don't forget, **June 18** is the **Year End Tax Planning** webinar at AVBN - Robert Carius of Carthills is going to tell us all we need to know so make sure you **stop by and register** for what should be a great webinar - and only $15!

You might remember from last newsletter my New Year's Resolution was to keep my inbox under control. I'm happy to report that so far so good! I've been dealing with mail as soon as it comes in which means my inbox has only 2 messages in it. Yay me! :)

We took a trip down to Tasmania for a week during April and had a great time visiting a number of wildlife parks as well as the wonderful people at University of Tasmania and Department of Primary Industries and Water who are working on the Save the Tassie Devil Project. **Ceilidh's site** has now raised over $1200 and her "Little Devils Day" has been held at her school and is proposed for a Forest Lake school later in the year. It's also heading over to the US when she was contacted by a school student in Idaho who wants to help her cause. She's also set up a Cafe Press store with some great merchandise so when you're looking for gifts check out **The Tassie Devil Diner** - you'll be

giving twice!

In this issue we have a tip on how to save your dictionary file when you've filled it with all those jargon words you use regularly, an eye-opening article on Facebook, information on malware in Flash advertisements, and some tips on ***really*** deleting those confidential files.

Till next quarter!

Virtually yours

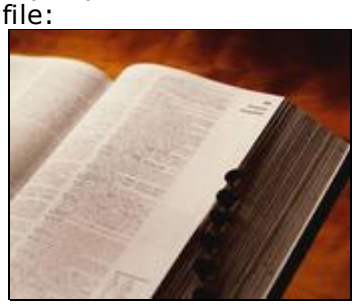
Lyn PB

PS: Don't forget: click here if you want to be unsubscribed. If you have a friend/colleague who may be interested in the content of our newsletter share the love and forward the newsletter to them.

WORD TIP: Saving Your Dictionary File

(Thank you to Terence Kierans, CAVB, of Cyberspace Virtual Services)

If you're like me you're adding words to the in-built dictionary in Word all the time! Especially if you use lots of legal or medical terminology. Is there a way to save the dictionary so you don't lose those words you've added if you have a system crash? Well according to one of my most highly-respected colleagues and fellow Thomas Leonard International VA of Distinction Award nominee Terence Kierans, yes you can! Here is Terence's steps for finding and saving that precious dictionary file:



1. Using Windows Explorer locate the file "custom.dic', or "whatever I named it.dic" - It is usually located in Program Files\Microsoft Office\Office.
2. Right click on the file; select "Copy".
3. Select your backup CD, drive, or removable drive, Right click on it and select "Paste".

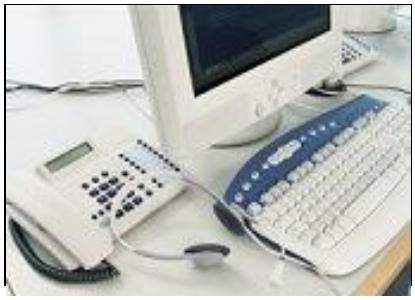
Too easy! Thanks Terence!

AVBN WEBINAR SERIES 2008

The **Australian Virtual Business Network Webinar Series for 2008** has gotten off to a great start with over 1/3 of attendees voting the speakers and content exceptional with the remainder voting Very Good.

Don't forget our **Year End Tax Planning Session which is scheduled for June 18** with Robert Carius of Carthills!

If you're interested in any of the sessions but have missed them, you can still get copies of the recorded presentations. Simply register in the usual way and we will send you access codes for the recordings. Topics again are:



- Business Plans
- IP/Trademarks
- Search Engine Optimisation
- Year End Tax Planning
- Time Management
- Writing Press Releases
- Responding to Requests for Proposal

- Subcontracting Made Simple
- Scams
- Goal Setting for the New year

(Note: There is no session in May as this is when OIVAC will be taking place.)

Presenters are from around the world and are experts in their field. If you go to the AVBN Webinar Schedule you'll find more information on who and when!

Given the quality of information, sessions have been incredibly priced at just **$15 per session** - the price is the same for the recordings.

Is FACEBOOK All It's Cracked Up To Be?

Recently I was sent a link to an alarming article about Facebook that appeared in the Guardian. Having read it I decided to delete my account, but soon discovered that what Tom Hodgkinson alleges in his article is indeed correct: Once you're in, you're in. You can only de-activate you account - not delete it - and whilst your info is not accessible on search, all that private info you signed up with IS available to the owners of the site and their affiliates. Have a read by clicking the link above and decide for yourself.

For me, best bet is to sign up with some of the more legitimate Web 2.0 networking sites like Ecademy, LinkedIn or Cagora.

AUSTRALIAN ACHIEVER AWARDS 2008

BIG NEWS for Executive Stress Support this quarter is we won a **2008 Australian Achiever Award** for Queensland's Office Services & Supplies category - achieving **98.52%** for customer relations and service and a Highly Recommended ranking!

We received 100% rankings in Customer Care and Attention; Value; Attitude; and Referral. I'm very excited about this achievement! The overall category winner for 2008 will be announced 10 December 2008. Thanks to those clients who agreed to be interviewed!

HANDLING CONFIDENTIAL FILES

If you are worried about protecting files on your computer - particularly if you have a lot of confidential documentation - you might be surprised to know that deleting these files and emptying the Trash folder - or reformatting your hard drive - doesn't actually really ***delete*** them. Here's an interesting article by Gabriel Torres reprinted from **Hardware Secrets** that you may find enlightening.

A lot of people don't know, but when we delete a file from a computer in fact it isn't really deleted. The operating system simply removes it from the file list and makes the space the file was using available for new data to be written. In other words, the operating system doesn't "zero" (ie doesn't clean) the space the file was using.

The operating system acts like that in order to save time. Imagine a large file that occupies lots of sectors on the hard drive. To really delete this file from the disk the operating system would have to fill with zeros (or any other value) all sectors occupied by this file. This could take a lot of time. Instead, it simply removes the file name from


the directory where the file is located and marks the sectors the file used as available space.

This means that it is possible to recover a deleted file, since its data wasn't really removed from the disk. Recovery data software works by looking for sectors with data in them that are not currently used by any file listed.

This leads us to a very important security question: if you have really confidential files, that cannot be read by anyone else, deleting them from the disk simply by hitting the Del key and then removing the recycle bin contents isn't enough: they can be recovered by an advanced data recovery tool.

There is software called SuperShredder that solves this problem. Deleting your files using this program really "zeroes" all sectors that the file was using. This program can be freely downloaded at http://www.analogx.com/contents/download/system/shred.htm.

With disk formatting it isn't different. When we format a hard drive, the data that was there isn't deleted, making it possible to recover data with an advanced data recovery tool even after formatting your hard drive.

When you format a disk, the operating system only "zeros" the root directory and the tables containing the list of sectors on the disk that are occupied by files (this table is called FAT). Pay attention when you format a hard drive - a message "Verifying x%" is shown. The hard drive isn't being formatted; the format command is only testing the hard disk magnetic surface in order to see if there is any error and, in case an error is found, marks the defective area as bad (the famous "bad blocks" or "bad sectors").

So, in the same way it happens when we delete files, the hard drive isn't really "zeroed" when we format it. In order to really "zero" your hard drive, use utilities like **Zero Fill** from Quantum. This utility fills all sectors from your hard drive with zeros, making it impossible to recover any data after this utility is run. You can also use the so-called "low-level format utilities". These programs fill all sectors with zeros as well. You must download the software according to your hard drive manufacturer. **In our download section** you will find low level format utilities for the most common hard disk drive manufacturers.

MALWARE IN FLASH ADVERTISEMENTS

According to Scott Dunn of Windows Secrets, Flash-based advertisements on the USA Today site download malicious code to users' computers, generating false warnings of a malware infestation and offering a fake solution.

The Flash vulnerability is so widespread that such "malvertisements" may be present on thousands of sites, but there are measures you can take to reduce your exposure.

Just opening the page puts you at risk

Visitors to USAToday.com got more than they bargained for. A hacked Flash advertisement meant that merely viewing a page in your browser was capable of triggering a malware attack on your PC. Apparently, the ad can take control of the browser without any user interaction at all.

Two days after the ad appeared on the USA Today site, two prominent Utah-based news sites, DeseretNews.com and SLTrib.com, were found to have similarly dire banner ads. These ads directed users to various unexpected locations, including the site for AntiSpywareMaster. This destination has been called a "corrupt anti-spyware parasite" and a "fake program" by the RDV Group, a safe-computing organization.

News sites aren't the only victims. Even Microsoft-sponsored sites have had problems serving up malvertisements though they denied it at first. And advertisements are not

the only source of the problem. The principal conveyors of this malicious code are Flash animations (or **.swf files**), which are commonly used to create intro screens, online video, and other Internet content in addition to Web ads.

Of particular concern are Flash files that are vulnerable to insertion of malicious code using a technique called cross-site scripting, or XSS.

This vulnerability was widely publicized earlier this year by Google researcher Rich Cannings and his co-authors in their book *Hacking Exposed Web 2.0: Web 2.0 Security Secrets and Solutions.*

What you can do to protect yourself

Even though the long-term solution is for the providers of Flash-based content to create more secure versions of their files, there are some measures users can take to protect themselves. These protections are not foolproof, but they at least reduce the risk of exposure to malware via compromised Flash files.

Some of these tips come from Andre Gironda, Secure SDLC Consultant and author of the ts/sci security blog.

The no-Flash option

The most effective - albeit drastic - way to protect yourself from malware-bearing Flash files is to uninstall Flash entirely. Adobe provides a special tool for doing this; you can find instructions and a link for downloading this file in a Technote published on the Adobe site.

The part-time-Flash option

If going without Flash entirely is too extreme, you can limit the sites that use this and other risky plug-ins by installing free browser add-ons that let you manage active Web content more granularly:

For **Internet Explorer**, TurnFlash lets you toggle between blocking Flash files and allowing them to run. A tray icon lets you turn Flash on or off, but the setting takes effect only in any new IE windows that you launch, not in the existing browser window.

A similar utility called No! Flash also switches Flash on and off, but it also gives you the ability to turn off several other elements, such as Java applets and other scripts. As with TurnFlash, the changes take effect in the next IE window you open

Installing IE7Pro add-on requires you to restart Internet Explorer 7 when it's first installed, but you can turn Flash animations on and off thereafter without launching a new instance of the browser. Moreover, the program lets you selectively unblock individual Flash animations on a single Web page.

This free add-on for IE7 adds a number of other useful features to the browser, including tab management, spell checking, and crash recovery.

For **Mozilla Firefox**, a plug-in called Flashblock disables all Flash content on Web sites and replaces it with a round Flash logo. You can selectively enable Flash files by clicking their icons.

For more comprehensive security, the plug-in NoScript not only disables Flash but also turns off Java, Silverlight, and other active Web elements. A NoScript icon in the Firefox status bar provides a pop-up menu for adding a site you trust to the add-on's "whitelist," which enables all scripts and animations on the site (but not necessarily those on the site's pages that are served up by ad networks). You can also right-click a link in Firefox to set its NoScript options via the context menu.

The minimal option

At the very least, update the Flash Player software on your system to the latest version (9.0.124.0 or higher). In the last three months, Adobe has patched a number of security

holes in this product. The update won't protect you from all buggy Flash files on the Web, but it will make your browsing much safer.

You can download the latest Adobe Flash Player from the Adobe Website.

After you install the update, run the free Secunia Software Inspector online malware scanner to find old versions of the Flash Player that may have been left behind on your system. Secunia's on-screen report will show the path and filename of the old files you need to delete. You may have to run the inspector more than once to make sure all the old files are deleted. If you delete a needed file by mistake, simply run the newest Flash Player installer again to correct the problem.

When it comes to removing an old version of the Flash Player, Rick Austin has some advice:

- "As a fan of Secunia's Software Inspector, I frequently have been notified to install the latest up-to-date version of the Flash Player and get rid of the old one. But I have found that getting rid of the old version as you describe doesn't work. The only way I know to do it is as follows:

  Step 1. Download the Adobe Uninstaller found on Adobe's Web Players page and save it for future use. (It only needs to be downloaded one time, because it is not version-sensitive.)

  Step 2. Create a desktop shortcut linking back to the same Web Player page.

  Step 3. Close the browser.

  Step 4. Run the "Uninstaller."

  Step 5. Click the link to the Web Players page to open your browser, and then run the appropriate installer.

  Step 6. Run Secunia to confirm.

  Step 7. Rejoice!

  "This works every time for me."

Thanks, Rick. Some users may also need to uninstall other applications that come with Flash components __ such as older versions of Adobe Photoshop Elements __ and then upgrade to newer versions.

One danger posed by Flash bugs is the ability of hackers to get your login credentials for a given site. Andre Gironda recommends creating multiple Firefox profiles, each with its own NoScript (or, if you prefer, Flashblock) settings. He uses his Flash-enabled profile to browse sites such as YouTube, but he exits that browser and launches his Flash- and script-blocked copy of Firefox when he conducts online banking and visits other sites that require logins.

To set up a Firefox profile, do the following:

Step 1. Choose Start, Run. Type **cmd.exe** and press Enter.

Step 2. At the command prompt, type:

"C:\Program Files\Mozilla Firefox\firefox.exe" -profilemanager

Then press Enter. (Note that the quotation marks are required and that your path may differ.)

Step 3. If you want Firefox to prompt you for a profile each time you launch it, uncheck the option **Don't ask at startup** in the Firefox __ Choose User Profile dialog box.

Step 4. Click Create Profile and follow the steps in the wizard to name your new profile. Repeat the

steps to create a second profile. For example, you might name one profile **Flash-Yes** and another **Flash-No.** When you're done, click Exit.

Step 5. Rather than being prompted for a profile each time you open Firefox, create separate shortcuts to launch each profile. For example, if you have a shortcut to Firefox in your QuickLaunch toolbar or on the desktop, drag the shortcut with the right mouse button pressed, drop it, and choose Create Shortcuts Here.

Step 6. Right-click one of your Firefox shortcuts and choose Properties. Click the Shortcut tab and edit the command line so it ends in with **-p** followed by a space and the name of one profile. For example, the entire command line might read:

"C:\Program Files\Mozilla Firefox\firefox.exe" -p Flash-Yes.

Repeat these steps for a second shortcut to launch your other Firefox profile.

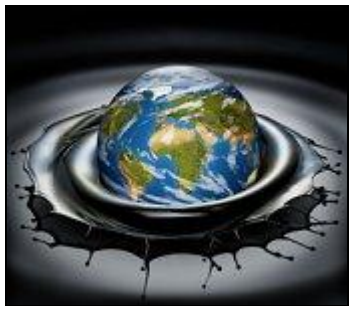
Step 7. You may need to download and install one of the plug-ins described above for these profiles and configure each profile's browser differently. However, any changes you make should be saved with that profile, so they will be in effect the next time you launch it.

If you don't want to create separate profiles for Firefox you can install two browsers - for example Firefox with Flashblock, and IE for when you need Flash to view some content.

A complete solution to high-risk Flash files may not come any time soon. Until the creators and managers of these files can ensure a high degree of safety, users have to be extra cautious to avoid the risks of Flash-borne malware.

A Poem by Joe Miller

This poem was sent to me as part of a Care2.com ecard. I thought I would share it here:



If the earth were only a few feet in diameter,
Floating a few feet above a field somewhere,
People would come from everywhere to marvel at it.
People would walk around it marvelling at its big pools of water, its little pools and the water flowing between.
People would marvel at the bumps on it and the holes in it.
They would marvel at the very thin layer of gas surrounding it and the water suspended in the gas.
The people would marvel at all the creatures walking around the surface of the ball and at the creatures in the water.
The people would declare it as sacred, because it was the only one, and they would protect it so that it would not be hurt. The ball would be the greatest wonder known, and people would come to pray to it, to be healed, to gain knowledge, to know beauty and to wonder how it could be.
People would love it and defend it with their lives because they would somehow know that their lives could be nothing without it.
If the earth were only a few feet in diameter.

-Joe Miller

CONTACT US

Mail:

PO Box 1036
Oxley Qld 4075
Australia

Email:

lyn@execstress.com

Phone:
+61-7-3375-5613

Fax:
+61-7-3009-0452

Web:
www.execstress.com