SOUTHERN DISTRICTS COMPUTER USERS CLUB INC.

March 2011

Club Web Site   http://sdcuci.com/

**MEETINGS are held on the third Wednesday of the Month, in the Hall at the rear of
St Mary's Catholic Church
Morphett Vale.
(Corner Bains Road and Main South Road)
Visitors most welcome**.
Cost $2 per person, which includes the Newsletter, plus coffee/tea and biscuits.
Subscriptions for twelve months Single $18
Family membership $24
Novice and experienced computer users will be warmly welcomed

---

Southern Districts Computer Users Club Inc.
For further information about S.D.C.U.C.Inc.

Contact The Club President, Jim Greenfield 83824912
Or
The Secretary
Correspondence to
The Secretary
S.D.C.U.C.I.
Box 991
Morphett Vale 5162

Email to
secretary@sdcuci.com

ROUGE EMAIL TARGETS UNWARY

Scammers already are trying to take advantage of the outpouring of compassion after the tsunami disaster.

One fraudulent scheme involves an email claiming to be from the British Red Cross and that asks recipients to make Japan aid donations via wire transfer, FBI spokeswoman Jenny Shearer said yesterday.

Roughly 350 internet addresses related to Japan were registered in a 24-hour period from Sunday to Monday, according to internet security expert John Bambenek.

The names reference Japan and such terms as "earthquake relief" and "aid".

Another con artist used search engine optimization techniques to make a bonus site appear at the top of Google search results for Japan quake information. The site pretended to be advertising anti-virus software but was actually malicious.

To prevent being scammed, experts say be very wary of online solicitations, do your homework, watch out for phony names, examine web address, check with the charity and resist pushy demands.

Spam from charities claiming to be linked to relief groups are common after natural disasters.

*This article was taken from The Adelaide Advertiser Wednesday March 16 2011
www.adelaidenow.com.au*

Never let a computer know you're in a hurry. ~Author Unknown

Fleurieu Peninsula Family History Group

Meet regularly on the third Saturday of each month at 1.30 p.m.
(i.e.- 3 days after our own monthly meeting)

Access available to large resource centre for research;
Access to special interest groups:
(eg English: Scottish; Irish: Brick Walls)

Visitors most welcome:

Contact: Vanessa Catterall on   catterallvg@bigpond.com
8384 7918

or Keith Jones   kjones2011@optusnet.com.au
7288 0192

How do I get rid of Nero Scout?

Nero 7 installs some rubbish called Nero Scout.
 If you installed Nero7, upon reboot you will find a search bar within your Task Bar.   Nero does not include an option to disable this or not to install this pest. So here is the quick way to disable this once installed.
Click Start Run and paste this whole entry and press enter
regsvr32 /u "%COMMONPROGRAMFILES%\Ahead\Lib\MediaLibraryNSE.dll"
For more information go to this web page
http://www.help2go.com/Tutorials/Software_Utilities/Disable_Nero_Scout_in_Nero_7.html

---

Location of msconfig
If msconfig will not start from the "run" command. (Due to a virus or file corruption) try running msconfig from its location

C:\WINDOWS\PCHealth\HelpCtr\Binaries\MSConfig.exe.
This should allow you to run msconfig

MEETING RULES

We are allowed to use the facilities at Hall at the rear of St Mary's Catholic Church Morphett Vale. (Corner Bains Road and Main South Road) in return of a small fee plus respect for their property. We ask for your co-operation in respect to the above. While we can not control what our members do away from our club meetings, Piracy of copyright material can not be condoned at our meetings.

Out of Memory error in Works

To work around this issue, delete any templates in the Template folder that you do not want to keep. To do this, follow these steps:

1. Quit Works if it is running.
2. Click **Start**, and then click **Run**.
In the **Open** box, type the following line (with quotation marks), and then click **OK**
    "<drive>:\Program Files\Msworks\Template"
    where <drive> is the letter of the hard disk on which Works is installed.
4. Right-click a template file you want to delete, and then click **Delete**.
Repeat step 4 for each template file you want to delete.
When you finish deleting files, close Windows Explorer and then start Works

Member profile
HEATHER LINEHAN

Joined	2010
Computer	Dell Inspiron 1525 laptop, 2 GB Memory RAM, Operating system Windows Vista. ADSL2+ wireless modem.
Main Usage	Writing letters (WordPad and Open Office). Emails – especially to my 2 brothers who live in Brisbane and Ceduna. Recently purchased new digital camera – waiting to participate in photography lessons. Have photo studio installed on computer.
Working Life	Stenographer (shorthand/typist) at Pope Products. Company bought out by Simpsons. I then transferred to Simpsons to be teleprinter operator. Shorthand typist/Book-keeper for an accountant in Savings Bank building, King William Street. Student nurse training in country hospital for 18months before traveling to Normanton in Gulf of Carpentaria with friends . Worked as semi-trained nurse in Normanton Base Hospital for 12 months. Back home some more work as typist (by this time electric typewriters were in use) before starting my training again as student nurse at The Queen Elizabeth Hospital. Midwifery training followed and a career in nursing at the hospital for 31 years, working in most areas of the hospital. Retired approximately 10 years ago.
Interests	Married to Peter who recently joined SDCUC and is taking Basic 1 and computer classes at the club. He has recently acquired a laptop and is a new user.
	Volunteer at the Save The Children shop in Blackwood. Member of VIEW, a service club for women. View assist The Smith Family sponsoring disadvantaged school children through their `learning for life` program. I am enjoying being a member of SDCUC and help with the bookings of computer courses. I find the speakers at meetings very interesting and worthwhile helping me update my computer skills.

My thanks to Evacom Computers Pty Ltd for this article

Evacom Hepful Hints and Customer Support

Thousands fleeced in 'Microsoft' scam but police powerless to act

With many thanks to optusnet.com.au for the article on 9 December 2010

Thousands of Australians have been taken for hundreds of dollars each by cold call scammers pretending to be Microsoft /Windows but police, regulators and the software company are powerless to fight the growing problem.

The scammers, typically based in Indian call centres, cold call people claiming to be Microsoft staff informing them that their computer has a virus on it. They provide bogus evidence of a virus infection and after winning over the victim, convince them to allow the scammer remote access to their computer through an internet website.

The scammers then pretend to fix the machine and ask for a fee that is up to $400. They use a combination of high pressure sales tactics and social engineering to scare the victim into paying the fee and because victims willingly hand over their credit card details, there is little legal recourse.

But the head of the NSW Police fraud squad, Detective Superintendent Col Dyson, said in a phone interview that in addition to taking payment the scammers also stole money and planted viruses on the victims' computers.

"We've had quite a few people report this to us and it's increasing all the time ... you're basically opening the door to your bank accounts to a criminal," he said.

"We have strong indications that they're looking at activity logs so they can pick up things like passwords and bank account details; some people's computers have also been infected with viruses and keyloggers.

"People have had money taken from bank accounts, only because of that, it's the only common denominator."

This website first reported on the scam in June but since then a plethora of readers have written in to say they have been targeted.

Stuart Strathdee, Microsoft Australia's chief security advisor, admitted the problem had grown in scale in recent months and Microsoft was receiving anywhere from two to 50 complaints a day from consumers.

"There's a number of different organisations doing this and they're changing their names almost constantly - we hear new names every week," said Strathdee, who himself has been cold called by the scammers three times.

"We've had a number of situations where they seem to be targeting one region or one country town; I've got a number of examples where they've targeted one small town or one mining village in far north Queensland or Western Australia and things like that."

As is common with internet crimes, Supt. Dyson said there was little police or local regulators could do to shut down the scams because the perpetrators are based overseas.

"All we can do is take the reports and liaise as closely as we can with the Indian authorities, but it's very much up to them to investigate," he said.

"These offenders when they do this don't leave a very obvious trail, it takes a lot of investigation to track them down."

Supt. Dyson said instead the police strategy was to alert the public to the scam and stress that under no circumstances should people give anyone remote access to their computer.

"People go to the trouble of having strong passwords, they have good virus protection and firewalls on their computer, but then allow remote access to someone - they're basically allowing them into their computer without really knowing who they are," he said.

Supt. Dyson said anyone who has allowed remote access into their computer should immediately change all of their passwords, scan their computer for viruses and, ideally, get a professional company to scan the computer as well.

Communications Minister Stephen Conroy would not comment, instead pointing to a joint statement put out by the Australian Competition and Consumer Commission and the Australian Communications and Media Authority in October this year.

When contacted, the ACCC and ACMA would not provide any new details on how they would beat the fraudsters,
instead also pointing to their old statement that warned consumers to be wary about unsolicited phone calls.

The October statement said over the previous two months complaints about scam telephone calls to the ACCC and ACMA had increased significantly from 200 per month to around 2000 across the two agencies.

In September, Queensland Police also issued a warning to the public following a "dramatic increase in reports" of the fake Microsoft scam.

But the problem seems far from abating due to the scale of the problem and the inability of Australian police and regulators to charge or take action against overseas fraudsters.

Strathdee said Microsoft had reached out to one of the sites the scammers use for remote access, logmein123, which had implemented IP address filtering and examined misuse of their test accounts to prevent scammers from using the service.

"We were hoping to push them a little bit to put messaging up on their front page or their home page but they were concerned about impact on their real customers, so that's ultimately their decision," he said.

Asked whether Microsoft's Indian office could take legal action against the call centres perpetrating the scams, he said "there's a whole range of reasons why that's much easier said than done".

"I know that we worked with our legal teams up there quite extensively but actually proving who it is that's doing it
is extremely difficult and the way that some of these companies have set themselves up and they way they operate the scam makes it very difficult," he said.

"There are a range of consent issues - the customer is consenting to allow the person to connect to their machine and the customer is also agreeing to a charge and providing their credit card details."

Strathdee said any prosecution would be difficult as victims would need to have recorded the calls for use as evidence. Some have published recordings of the scam calls on YouTube.

The International Consumer Protection and Enforcement Network (ICPEN), which coordinates responses to global scams such as this, said in an emailed statement that "both ICPEN and other national enforcement agencies are aware of the scam that you refer to".

SELF PUBLISHING

This months speaker will explain the key points in transforming your passion and reminiscences into book form. When one "gets involved" and starts gathering information on a topic close one's heart it can be a never ending story, with months, even years of recording your information. Eventually the thought of producing a book on your passion may surface.

KEY POINTS
> Research
> Organising
> Import/Exporting data between primary programs (for Family History)
> Selecting program to publish in (e.g. Word or Publisher or other)
> Formatting
> Inserting images
> Page numbering
> Indexing and Table of Contents
> Saving
> Creating pdf files
> Publisher

Family History Focus

Importing / Exporting is achieved between (pretty well) all programs set up to organise family history data.

Usually found under "File" in the main menu bar. Export to a "gedcom" file. Programs that allow export will usually have a "gedcom" option to export to.

Ensure also that the genealogy program selected to export to has a capability of converting your information into a Word document . (ie .doc: .docx or .rtf) Some genealogy programs may have options to convert to Publisher or other such programs.

> Select your desired export options:
> Select your desired Import options:
> Create a new file.

Creating your Word document for publishing

Should your passions be in some other discipline, (eg Trains: Crochering: Egyptian Mythology: Fungi: Music: Geology etc. etc,. etc,), the following parameters will be a good start in setting up Word as your operating document.

Page Set-up options

I have found the following page set up options for Word work well if you are contemplating and A4 size document. (Both Windows XP and Windows 7):

Page	(for A4 portrait)				
Margins	(cms)	**Top**	2.2	**Bottom**	1.8
		Inside	1.8	**Outside**	2.2
Gutter	1.7				
Select	"Mirror Margins"				
Select	Apply to whole document				

Evacom
COMPUTERS

Evacom provides the following services:

Purpose Built Up-Market Computer Systems for Home and Business

Repairs & Upgrades to Computers and Laptops

Various types of computer hardware

Acer, ASUS, Compaq, HP, Leader, Lenovo and Samsung Laptops

Computer Preventative Maintenance

Canon, Epson, HP and Brother Inks and Accessories

Internet Services and Software

Backup & Antivirus solutions

Evacom built Computer Systems are C-Tick Compliant
as required under The Radio Communications Act

We provide Local After Sales Service to all our Customers and
Technical Support to all Evacom Built Computer Systems

Contact: Helen, Mark or John
Tel: (08)83223390
Fax: (08) 8322 2109
sales@evacom.com.au

Trading Hours
Monday 9.00am to 5.30pm
Tuesday 9.00am to 5.30pm
Wednesday 9.00am to 5.30pm
Thursday 9.00am to 8.00pm
Friday 9.00am to 5.30pm
Saturday 9.00am to 4.00pm
Closed on Sunday's and Public Holiday's