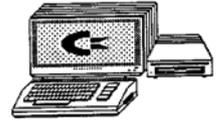


SOUTHERN DISTRICTS COMPUTER USERS CLUB INC.



June 2009

Club Web Site <http://videocam.net.au/sdcuci/indexhtml>

Editor Jim Greenfield

MEETINGS are held on the third Wednesday of the Month, at Christ Church O'Halloran Hill 1708 Main South Road O'Halloran Hill at 7.30pm

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

Correspondence to
The Secretary
S.D.C.U.C.I.

Box 991

Morphett Vale 5162

Email to

ronald.stephens1@three.com.au



Jim Bandt	4 th June
George Cettl	8 th June
Ed Uden	14 th June
Allan Norton	14 th June
Robert Zeugofsge	22 nd June

The President's Page

Windows XP by default enables all visual effects if it thinks your PC can handle it, even PCs with 256mb of ram it enables it, some of these features are pointless and can be turned off without any noticeable visual effect

Right click my computer

Properties

Advanced

Click on settings under performance

Disable all the visual effects except the last 3

Click apply and OK

OK again

Right click your desktop

Properties

Appearance

Effects

Untick the first two boxes.

You should now notice a great speed up in your PC without losing the visual effects of windows XP, of course you can disable them completely and notice an even greater speed up but some of you might want the blue and green look of windows XP.

Jim Greenfield

President

It's better to attempt to do something and fail than to attempt to do nothing and succeed.

From the Editor
E-MAIL TRACKING

Here is something everyone should read and take the advice. If you don't, you're hurting yourself and your email contacts.

By now, I suspect everyone is familiar with www.snopes.com <<http://www.snopes.com>> and/or www.truthorfiction.com <<http://www.truthorfiction.com>> for determining whether information received via email is just that: true/false or fact/fiction. Both are excellent sites.

Advice from Snopes.com Very important!

1) Any time you see an E-Mail that says forward this on to '10' (or however many) of your friends, sign this petition, or you'll get bad luck, good luck, you'll see something funny on your screen after you send it, or whatever, it almost always has an **E-Mail tracker program** attached that tracks the cookies and E-Mails of those folks you forward to.

The host sender is getting a copy each time it gets forwarded and then is able to get lists of 'active' E-Mail addresses to use in SPAM E-Mails, or sell to other spammers. Even when you get emails that demand you send the email on if you're not ashamed of God/Jesusthat's E-mail tracking and they're playing on your conscience. These people don't care how they get your email addresses - just as long as they get them. Also, emails that talk about a missing child or a child with an incurable disease - "how would you feel if that was your child"....**E-mail Tracking!!!**

Ignore them and don't participate!

2) Almost all E-Mails that ask you to add your name and forward on to others are similar to that mass letter years ago that asked people to send business cards to the little kid in Florida who wanted to break the Guinness Book of Records for the most cards. All it was, and all any of this type of E-Mail is, is a way to get names and 'cookie' tracking information for telemarketers and spammers - - to validate active E-Mail accounts for their own profitable purposes.

You can do your friends and family members a GREAT favour by sending this information to them; you will be providing a service to your friends, and will be rewarded by not getting thousands of spam E-Mails in the future!

If you have been sending out (FORWARDING) the above kinds of E-Mail, now you know why you get so much SPAM!

Do yourself a favour and STOP adding your name(s) to those types of listings regardless how inviting they might sound!...or make you feel guilty if you don't!...it's all about getting email addresses - nothing more!

You may think you are supporting a GREAT cause, but you are NOT! Instead, you will be getting tons of junk mail later and very possibly a virus attached! Plus, you are helping the spammers get rich! Let's stop making it easy for them!

Also: E-Mail petitions are NOT acceptable to Government, or any other organization - i.e. social security, etc. To be acceptable, petitions must have a signed signature and full address of the person signing the petition, so this is a waste of time and you're just helping the Email trackers.

Please read the full story here:

<http://www.snopes.com/inboxer/petition/internet.asp>

QUEEN ELIZABETH II was born on 21st April 1926
at 26 Bruton Street, Mayfair, London. England

Marked by a parade and a military ceremony known
as Trooping the Color, the celebration this year fell
on June 13.

Since the 18th century, British monarchs have been
publicly celebrating their birthdays in June, no matter
when they were actually born, in hope of good
weather for public events.



Opinions expressed in this newsletter do not necessarily represent those of the Southern Districts Computer Users Club Inc. nor does publication of an advertisement imply endorsement by the Southern Districts Computer Users Club Inc.

While every attempt has been made to verify that the information in this newsletter is correct, the Southern Districts Computer Users Club Inc accept no responsibility for any inaccuracies.

Likewise no member of the committee or member of the Southern Districts Computer Users Club will accept any liability for any damage occurring to a computer, to any computer system and/or data from following instructions given in this newsletter.

Let **Evacom** Fix it Professionally

Minimum charge applies

FOR UP MARKET & UPGRADEABLE
COMPUTERS,
PROFESSIONAL REPAIRS AND UP-GRADES
AT SENSIBLE PRICES

—!! Go To !!—

Evacom **YOUR LOCAL COMPUTER SHOP**

"WE ARE A GROWING FAMILY BUSINESS, LOCAL AND PROUD OF IT"

Shop 4, Woodcroft Market Plaza
217 Pimpala Road, Woodcroft
PH: 8322 3390 or Fax: 8322 2109
E-Mail: sales@evacom.com.au



MEMBER PROFILE

GEORGE STEFFE.

Member	George Steffe
Joined	2007
Computer	NEC Pentium ® 4 CPU 3.00 GHz Windows xp Professional Version 2002
Main Usage	Microsoft Office: Picasa 3 for Photos: Searching Web for News and Subjects of interest: Music and Films: Letter Writing to friends and relatives: Skype to see and talk to friends and relatives in U.K.
Marital status	Married – 4 children with 12 grandchildren.
Pre- retirement	Worked for the South Australian Government mainly on Security until the reorganization when I transferred to Occupational Health and Safety as a Safety Consultant to the Construction Department.
Post-retirement	Left paid employment in 1994. Spent most of my time traveling around Australia with the caravan and trips to Europe and Asia.
Interests	Mainly photography, playing cards, visiting the children and spending time with friends on various get together's. I spend most of my time looking after the house and garden and following the grandchildren's sporting activities. This includes, Football (McLaren Vale Footy Club), Sturt Lacrosse Club, Pony riding and finally Basket Ball at Willunga. All of this takes plenty of our time .

The only club that I am a member of is our club SDCUCI so I have not been active in any other club since leaving the Christies Beach Football Club several years ago.

I hope this gives other members the incentive to follow this up with their own profiles .

Have you recently acquired, or do you just want to learn more about operating, your computer?

The Club conducts classes on a wide range of subjects, at a very moderate charge.

The maximum number in class is five.

(Our aim is to conduct the classes in a friendly non-threatening atmosphere)

Some of the classes that are available:-

1. Basic Computing (Stage One and / or Stage Two)
2. Advanced Word
3. Internet workshops
4. Digital Cameras

For more information contact a committee member.

South Australia Dates

1884.

Fort at Large Bay opened.
56 Afghans and 293 camels arrived at Port Augusta on the Bengal.
Railway reached Marree.
Jack Hester pioneered first mail service on the Birdsville Track.
Hans Heysen arrived in South Australia.

1904

First community-run hotel in the British Empire established at Renmark.
School opened at Innamincka.
South Australia first State to make road laws for cars. They must carry a disc with name of owner and make of car.

1908

We of the Never Never published by Jeannie Gunn.
The Outer Harbor opened.
Jack Oakes took up Merty Merty station.
First secondary school, Adelaide High School opened.
RM Williams born on 24 May 1908.

Dynamic Mechanix

Automotive Repairs

ALL GENERAL MECHANICAL REPAIRS

Brakes, Suspension, Clutch,
Auto Trans Service,
Wheel Balance & Repairs,
New & S/Hand Tyres.

SERVICE, TUNE & SAFETY CHECK
(most 4 & 6 cyl. cars) - Includes plugs,
points, oil, filter.

**Pensioner
& Seniors
Discount**

U4/2 Somerset Circuit
Lonsdale S.A. 5160

 8186 0081

MEETING RULES

NO SMOKING NO DRINKING NO SWEARING

We are allowed to use the facilities at Christ Church, O'Halloran Hill 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.

Avoid being caught by fraudulent email

As the Internet has grown in popularity and convenience it is increasingly being used by people to shop, bank and carry out business online. The Internet provides access to resources and services that would be far more time-consuming and difficult to reach in person.

Unfortunately, there have been cases of the Internet and email being used for fraud - to trick people into revealing personal information in order to commit a crime. This information sheet contains information about a kind of online fraud called “phishing” and will give you some pointers on how to avoid being caught out by it.

What is “phishing”?

An early form of computer hacking was used to gain illicit access to people’s phone accounts and use them for illegal or expensive calls. This was called “phreaking”, using the first two letters of the word “phone”. It became fairly common hacker practice to replace the letter “f” with “ph” when talking about online or phone-based activities.

“Phishing” is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses, most commonly banks. These authentic-looking messages are designed to lure recipients into divulging personal data such as account numbers and passwords and credit card numbers.

How to identify a Phish

Phishing emails often look authentic. They pretend to come from a financial institution or other company and have a believable email address. They often copy that institution’s logo and message format. It is common for phishing emails to contain links to a website that is a convincing replica of the company’s home page .

Phishing emails give themselves away by telling you that there is some reason why you must provide personal details such as your Internet banking logon, password, credit card card number or PIN by reply mail or through a website.

Phishing emails often try to instil a feeling of urgency by saying things like:

your account will be closed down unless you log on;
a recent security upgrade means that you have to log on to be protected; or
a large sum has been debited to your account and you need to provide your account details to confirm that the charge is incorrect.

Got a phishy email? Here’s what to do:

Frustrate the phishers

You can avoid most phishing scams by being alert and employing sound practices for Internet use. If you receive a dubious email,

1. Pause and think

Phishing emails may seem plausible when first read and attempt to force the recipient to urgently reply or logon to a website before they have time to think about what they are doing.

When you receive emails asking for personal details, take your time to think about what you are being asked to do.

Is it a message that you would expect to receive?

Is it one that you have received from the financial institution or company before?

Are there related announcements on the financial institution’s or company’s website?

Most phishing emails are sent as spam, where the sender has no knowledge of the recipient. But even if you receive a message that is addressed to you alone, read it carefully. If you are suspicious about an email, double check before responding.

Avoid being caught by fraudulent email

2. Follow your own path to the site you choose

It is possible to create a link on a web page or in an email and make it look as if it is taking you to a bona fide website when it is actually sending you somewhere else. Your safest course is to check that you have the correct address (URL) and then type it each time into your address bar.

If you want to check the message by telephone, use the contact number that is in the phonebook, not a number listed in the email. Often the numbers provided in phishing emails are false or can lead to you incurring costs.

3. Report it

If you think you've been taken in by a phishing scam, you should report it to the institution concerned as soon as possible. Also report the crime to the police in your State or Territory.

4. Delete the phishing mail

Some phishing emails include more than fraudulent information - they can also carry viruses. If you identify that an email is 'phishy' immediately and permanently delete it.

Banking online safely

Be careful

Whether or not you receive a phishing email, there are some simple steps that you can follow to make your online transactions much more secure. These are set out below.

Secure your system

Some criminals try to use computer viruses to harvest people's account details, so you should make sure your computer is not an easy target.

- Run and maintain an anti-virus product on your computer

- Do not run or install programs of unknown origin

- Use a personal firewall

If using a local area network, contact your administrator and seek information on the availability of email gateway filtering for specific file attachments.

Secure your passwords

If you bank online, you have a logon and password or a personal identification number (PIN) so that only you can access your own account. Don't let this personal information fall into other people's hands.

- Don't give your PIN or password to anyone else

- Change your Internet banking passwords on a regular basis

- Avoid using your birth date or name as your PIN or password

- Avoid storing your passwords on your computer

- Don't set up your computer so it "autocompletes" or saves your password.

Don't use links in emails or web pages - follow your own path to the financial institution

It is possible to create a link on a web page, or in an email that looks as if it is going to a bona fide website of a company or financial institution but actually sends you somewhere else. If you want to go to the website of a financial institution, your safest course is to check that you have the correct address from your financial institution and type it into your browser's address bar. If you use the site on a regular basis, you can type in the address, bookmark it and access it from your browser's "favourites" list.

Any doubts? Report it

If you had anything stolen, you would report it as soon as possible. The same principle applies to your account details. If there's a chance that someone could use your account details to illicitly access your money, you should report it immediately to your financial institution and the police in your State or Territory.

From the Editor:- I have been taught to be cautious. Have you?

