Southern Districts Computer Users Club Inc

Supporting inexperienced users with local expertise

September 2017

Vol. 17
No. 09

Club Web Site   http://sdcuci.com
Email Address: sdcucinc@gmail.com

SDCUCI

**MEETINGS are held on the third Wednesday of the month at 7.30 pm, in the Hall at the rear of
St Mary's Catholic Church
Morphett Vale.
(Corner Bains Rd and Main South Rd)**

Visitors most welcome.
After three visits, visitors will be requested to become members.

Cost $3 per person, which includes the Newsletter, plus coffee/tea and biscuits.
Subscriptions for twelve months
Single $20
Family membership $30

Novice and experienced computer users will be warmly welcomed

---

CLAYTON'S PRESIDENT REPORT

As you know, our esteemed Yardbroom and his lovely wife are hotfooting, sailing and railroading across Canada and Alaska, so no awesome report for you this month.

Again, just a reminder of our AGM next month.

Happy Computing

Our next meeting is scheduled for

Wednesday 18th October, 2017

Topic: it will be our AGM!

**Committee Members
Southern Districts Computer Users Club, 2017**

L-R: Dean Howard: Trevor Francis (Secretary): Linda Kirby:
Anne Leddra: June Harman: Jim Greenfield: Wanda McDonald:
Jo Berkin: Cheryl McDonald (Treasurer): Lindsay Chuck:
John KIrby (Vice President): Lionel Leddra (President): Lorraine Loader.

SEPTEMBER BIRTHDAYS

A very Happy Birthday to you all

September
SAPPHIRE

Trevor Francis

Wanda McDonald

Colin Hornby

Ken Rowley

Editors: Our apologies if we missed your birthday this month. If you haven't given us your birthday month, please see Bib or Bub or someone at the desk.

THIS MONTH'S MEETING

Email, for many people, is one of the main reasons for having a computer.

Trevor's presentation continues on from his previous session on Web & ISP emailing, and if you need to download email to your computer to access it offline, then consider coming along.

Thunderbird is a free program.

How to find WiFi Hotspots using Facebook.

The Facebook app on your device can help you locate available hotspots at nearby businesses. Here's how:

Tap on your *Facebook app* to open.
Tap on the *More* tab (3 dots in top right corner)
Under the Apps section, tap *See All*
Scroll down and tap on *Find WiFi*
Tap on *Enable Find WiFi*
A list of businesses will appear
Or you can tap on *Map* to see a map of WiFi hotspots.

You can tap on a business name and Facebook will provide information about the business via their Facebook page, or give you directions to their location.

Please note: you do not need an internet connection to use this feature, and you can use WiFi when you get to the location.

LAST MONTH'S MEETING

A wild, wet and windy night saw many (including 1 visitor) be brave enough to come listen to Jason from IT&C Computers give a talk on what's new in the live-streaming world of movie watching.

Some choices are:

Netflix. This is a US company which has been around since 1998 and used to deliver DVD's in the mail (postal, that is). Internet streaming began in the US first in 2007 and now operates in nearly every country. It has the largest library with over 1200 TV shows and 2700 movies. Cost can be $10 per month for 1 person on standard HD or $14 per month for 2 people to watch at the same time.

Stan.   Is Australian based company which offers subscriptions to selected movies and TV shows/series. It has a choice of over 350 TV shows and 1000 movies. Was a bit slow to take off but now has 1.5m users after 6 months. Cost is slightly cheaper than Netflix.

Jason says NBN is great for Netflix: 2 things to look for -

1. Resolution - HD etc
2. Bit rate - quality videos.

Movies can get quite large to download. Netflix, for example:

       0.7 GB (gigabyte) per hour of standard definition video
       3 GB per hour for HD video (most popular)
       7 GB per hour for Ultra HD

So, a 2 hour movie in HD (the most common subscription) will take up to 6 GB of data.

Catchup TV

Is free. Every major network has a different name and different apps and they can be watched on all devices. Shows are usually kept on-line for up to a month.

Con't

ABC	iview
Ch 7	Seven Plus
Ch 9	Nine Now
Ch 10	Ten Play
SBS	SBS On Demand

Fetch TV. Launched in 2010, Australian access to all other apps and can get a mixture of movies, shows, free-to-air and catchup TV. Does cost about $6 per month and have just added HD. Will cost $399 to buy the Fetch black box.

Foxtel. Is an Australian PayTV company which is a bit more pricey than the others - $104 per month for all packages. Does have the best choice of live sport, new shows, blockbuster movies and catchup TV.

YouTube Red will allow streaming and do have some exclusive shows.

Facebook is starting a streaming service soon (Jason not sure when) and will possibly be free as it could be "ad" supported.

Spotify is a music streaming service which recently added off-line watching.

Google Music is merging with YouTube. Can upload your own music to their service.

Radio Stations have their own website services. Go into the website, click and it will play music.

Jason warned us to be careful of scrupulous streamers as these could be riddled with ads and popups which contain viruses. Best go to the relevant website instead of the app.

Jason then showed us his new "toy". **Google Assist!** There is just so much these little gadgets can do - tell jokes, set timers, play songs etc.

Lionel thanked Jason for this wonderful insight into live-streaming and then reminded all about our AGM in October and asked us to consider joining the committee.

Why Browser Extensions are So Dangerous

Jim Greenfield said "over the last 3 weeks, I have repaired 4 computers that I believe were corrupted by malicious extensions". This has prompted him to request this article be put in the newsletter. So Jim, here it is!!

Browser extensions are much more dangerous than most people realise. These small tools often have access to everything you do online, so they can capture your passwords, track your web browsing, insert advertisements into web pages you visit and more. Popular browser extensions are often sold to shady companies or hijacked, and automatic updates can turn them into malware.

If an extension has access to all the web pages you visit, it can do practically anything. That doesn't mean that every extension **is** doing these things, but they **can** - and that should make you **very, very wary!**

Modern web browsers like Google Chrome and Microsoft Edge have a permission system for extensions, but many extensions require access to everything so they can work properly. Even an extension that just requires access to one website could be dangerous, however. For example, an extension that modifies Google.com in some way will require access to everything on Google.com and therefore have access to your Google account (including email).

These aren't just cute, harmless little tools. They are tiny programs with a huge level of access to your web browser, and that makes them dangerous.

How safe extensions can transform into malware

Modern web browsers like Google Chrome automatically update your installed browser extensions. If an extension requires new permissions, it will temporarily be deactivated until you allow it. But, otherwise, the new version of the extension will run with all the same permissions the previous version did. This leads to problems.

In August 2017, the very popular and widely recommended Web Developer extension for Chrome was hijacked. The developer fell for a phishing attack, and the attacker uploaded a new version of the extension that inserted more ads into web pages. Over a million people who trusted the developer of this popular extension ended up getting the infected extension.

In many other situations, someone develops an extension that gains a large amount of users, but doesn't necessarily make any money. That Developer is approached by a company that will pay a large amount of money to purchase the extension. If the developer accepts the purchase the new company modifies the extension to insert ads and tracking, uploads it to the Chrome Web Store as an

update and all the existing users are now using the new company's extension - with no warning.

This happened to Particle for Youtube, a popular extension for customizing YouTube, in July 2017. The same thing has happened to many other extensions in the past. Chrome extension developers have claimed they constantly receive offers to buy their extensions. In addition to the hijacking and sale of extensions, it is also possible that an extension is just bad news, and secretly tracks you when you install it in the first place.

Chrome has been under attack due to its popularity, but this problem affects all browsers. Firefox is arguably even more at risk, since it doesn't use a permission system at all - every extension you install gets full access to everything.

How to minimize the risk.

Here's how to stay safe: Use as few extensions as possible. If you don't get much use out of an extension, uninstall it. Try to pare down your list of installed extensions to just the essentials.

It is also important to only use extensions from companies you trust. For example, an extension for customizing YouTube created by a random person you have never heard of is a prime candidate for becoming malware. However, the official **Gmail Notifier** created by Google, **OneNote** note taking extension created by Microsoft, or **LastPass** password manager extension created by LastPass will almost certainly not be sold to a shady company for a few thousand bucks.

You should also pay attention to the permissions extensions require, when possible. For example, an extension that only claims to modify one website should only have access to that website. However, many extensions need access to everything or access to a very sensitive website you want ot keep secure (like your email). Permissions are a nice idea, but they are not too useful when most things need access to everything.

It's a fine line to walk. In the past we might have said the Web Developer extension was safe because it was legitimate. However, the developer fell for a phishing attack and the extension became malicious.

More on Browser extension security at: http://www.popularmechanics.com/technology/security/a16741/browser-extension-security/

Thank you to Jim Greenfield for this article.

SANDS COMPUTER GROUP
& BROADBAND FOR SENIORS

ESTABLISHED JANUARY 2011

Coordinator and Editor: Lindsay Chuck

E: Lindsay.chuck@gmail.com

W: http://sandslifestylebfs.wix.com/scgbfs

Laptop Issues

Have you had any of these problems recently?

* turned computer on and the Lock screen is black (no picture, date, time and cursor are displayed.)
* Backgrounds in settings are black with white writing
* Some settings would not change
* Computer is slow

After being told of recent Windows Updates, I suspected a Microsoft patch may be the problem.

In settings, Windows Update indicated more updates were available, so we proceeded to download and install the updates then rebooted the computer. This didn't resolve all the issues, but it did allow the default settings to be reset.

Changed the default for the Lock screen, and changed the background screens setting from dark to light. Rebooted the computer.

Computer was still slow, but the visual issues were corrected.

Several days later, the computer was operating normally.

When you update Windows, ensure computer finishes updating before turning off.

Clear space on your Android

Smartphone or tablet, there is nothing worse than not being able to install a new app or update older ones. The following suggestions may overcome this problem.

* *Cached app data* - check your app storage setting screen and tap an individual app. Its amazing how much data apps store, the possible saving can be in the hundreds of megs. Tap settings > Storage > Cached data, then tap OK in confirmation window.
* *Download folder* - as with your laptop or desktop, the downloads folder is a place often forgotten about, and should be cleaned out on a regular basis.
* *Remove photos already backed up* - the Google photos app will let you know how many pictures it can delete from local storage. Open Photo app > tap three line menu button (top left corner of the screen) > tap free up device storage > tap OK to pull trigger.

New Windows Flaw

A new flaw has been found in Windows which could allow a WannaCry like attack. Microsoft is urging users to update and install the issued patch (Click *check for updates* in Windows to check your system is up to date).

Windows Search in Windows Server 2008 SP2, R2, SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold, R2, Windows 10 Gold, 1511, 1607, 1703 and Windows server 2016 are all affected.

Instapaper
https://www.instapaper.com

Save anything. Read anywhere.
Available for iPhone/iPad and Android.
Allows you to save articles, videos, cooking recipes, song lyrics while you are browsing. One click to save, read and manage interesting things you find on the internet.
Instapaper syncs articles and videos across iPhone/iPad, Android phones/ tablets and Kindle to read and view at a later time.
It also creates notes.

.

I
Instapaper

Lindsay's tips.

Block WiFi Thief, is an Android app available in Play Store. When opened, it scans all devices on your network. Check & remove any device.

. . . .

Photopea Free Online Photo Editor, nicknamed Photoshop online, you can save your work as PSD, JPG, PNG and SVG. Creates a new image or an image from existing files on your computer.

. . . .

...SO THEN I HIT 'ANY KEY'!

Stegangraphic Technique stacks on the rise.

You are not alone if you haven't heard of this terminology before. Kaspersky Labs researchers have noted and comment on the rise of these attacks, and are spreading the word on this technique.
What is it?
Code concealed in pictures.
Malware including updated trojans like Zerp, ZeusVM, Kins, Triton and others. The attacks are difficult to detect as the file size remains the same, and the aim is to steal financial information.

.

SCAM ALERT

Watch out for NBN scams

The ACCC is warning the community that scammers are pretending to be from NBN to con victims out of their money and personal information.

Scamwatch has received 316 complaints this year about scammers impersonating NBN with nearly $28,000 reported lost.

The three common scams reported that involve scammers impersonating NBN are:

* Signing victims up to fake accounts - scammers will ring victims to 'connect' them to the NBN for a low price. They will often demand payment be made through itunes gift cards.
* Gaining remote access to computers - scammers pretending to be from NBN will call a victim with claims there are problems with their computer.
* Phishing - scammers impersonating NBN will call victims to steal valuable personal information like their name, address, Medicare number etc. The scammer may tell them they are entitled to a new router, for example, and say they need these personal details to confirm the victim's identity.

"NBN will never phone you out of the blue to try to sign you up to a service over its network. NBN will also never call you to remotely 'fix' a problem with your computer or request personal information. Finally, if someone asks you to pay using an iTunes card, it is 100% a scam" NBN spokesperson said.

People can protect themselves by following some tips.

* If in doubt, hang up the phone then call your retailer direct to check if the person calling is a fraud.
* You can only connect to the NBN network by purchasing a plan through a phone and internet service provider.
* Never give your personal, credit card or online account details over the phone unless you have made the call.
* Never give an unsolicited caller remote access to your computer.

If you think you have provided bank or credit card details to a scammer, contact your bank or financial institution immediately.

TIPS TO PROLONG YOUR SMARTPHONE'S BATTERY LIFE

Are you lamenting over the short lifespan of your smartphone battery?   For some people, keeping your phone up and running for a whole day when it is open 24/7 is a lost cause. However, there are a number of things to keep in mind that do help preserve your battery life.

1. **Quit your apps.** Even when you have closed out of your apps, they are still running in the background. This drains a good deal of your battery life. Here's how to 'quit' your app that hasn't been used in a while.
   a) Have your phone unlocked and open
   b) Double push your menu button. You will see a screen displaying each of the apps that you currently have running in the background. Swipe to the right to see them all.
   c) Once your app is in the middle of the screen, swipe upwards. This will drag your app up until it disappears past the top of your screen. You have now quit out of the app.

2. **Lower the Brightness.**   The brighter your screen, the more battery is drained. Adjust your brightness settings to the lowest possible brightness for maximum efficiency and comfortable for you.

3. **The 40-80 per cent rule.**   Some people think that keeping their phones charged at 100% for a long time will mean that their battery will last longer once unplugged. This is false! It is actually bad for your phone, because you are putting your battery under stress by not allowing it to discharge. The rule of thumb is to charge your phone to around 80% and then take it off the charger. It is also bad for your phone if you let it drain to 0%, instead recharge prior to reaching 40%.

4. **Avoid exposing your phone to direct sunlight.**   Letting your phone have a sunbath is bad for its battery! The heat from the sun causes the battery to overheat, which depletes its life. Furthermore, for those of you with an auto-brightness setting on, the brightness from the sun will amp up the brightness setting on your phone display. As we know, this drains battery life.

5. **Get a new battery!**   If all else fails, and you have noticed that your battery life has worsened noticeably since you first purchased your phone, this means it is time to change your battery. Batteries will depreciate over time, so if it is gotten to the point where you can't even go a few hours without charging, you need your battery replaced.

Reproduced (in part) from Over60 Facebook page

COMMITTEE CAPERS

This month's meeting was held at the Kirby's with 9 members (and a dog) in attendance.
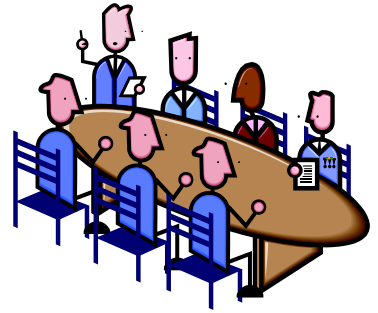
Points discussed:

* Letter received from Amanda Rishworth offering an award for outstanding volunteer in our group.
* Lorraine Rosenberg has agreed to chair and give a talk at our AGM.
* Suggested we show a 5 minute video about hacking at a future meeting.
* Trevor to check if we can connect a smartphone/tablet to our projector for future meetings as this seems to be the way technology is going.
* We will be sending emails to members for nominations to join our committee. We have 3 members retiring after our AGM.
* An assessment on a Thunderbird workshop will be made after this month's meeting.

TEST YOUR COMPUTER KNOWLEDGE

This month's puzzle

1. An internet terminology IP means?
2. The first page of a website is called?
3. Which Company is nicknamed "big blue"?
4. What was the first web based email service?
5. Who designed the first Apple Computer (Apple 1)?
6. The first movie (released in 1982) with terrific computer animation and graphics was?
7. One byte is equivalent to how many bits?
8. What does ISDN stand for?
9. What command at File Menu to you use to create a document?
10. What kind of files have .mpg extension?
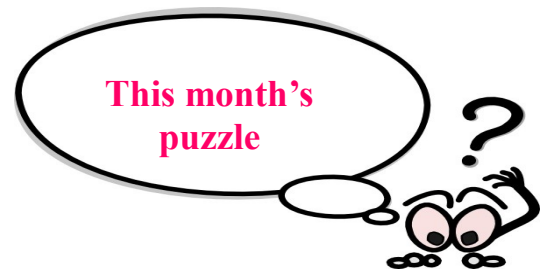
From the Editors

To ensure the standard of the newsletter is maintained, and the articles remain of interest, contributions from all members will be welcomed. Forward to Bib or Bub.

NOTICE BOARD

∗ Another reminder about our AGM which is coming up in October. As we have 3 current committee members retiring, please consider nominating yourself or someone you know who will enjoy being part of our committee.

∗ If you hear of any special event or move or illness or birthday or anniversary etc, please let the editors know so we can acknowledge it in this noticeboard. Thankyou in advance.

5 Things Hackers Love to see You Share on Social Media

Chances are you have shared what you've been up to on social media. Communication channels like Facebook, Twitter and Instagram make sharing easy. Here's a list of things you should never share on social media.

Your phone number - Social media hackers want phone numbers because they are unique identifiers that typically last a long time.

Your home address - To avoid burglars showing up at your home would be one reason not to share your address, however, social media hackers are out to get everything you are worth via phishing.

Hashtags - These make it easy to follow conversations for hackers as they provide another avenue for attackers to obtain information about you.

Where you have checked in - Hackers now know where you are or where you're not, and where you are using your credit card making it easier to post transactions that would otherwise be unusual.

From OverSixty Facebook page

Disclaimer: The information contained herein is of a general nature. Always do your own research and seek advice before proceeding on information you don't understand.

Smith climbs to the top of Mt Sinai to get close enough to talk to God. Looking up he asks the Lord, "God, what does a million years mean to you?"

The Lord replies, "A minute."

Smith asks, "And what does a million dollars mean to you?"

The Lord replies, "A penny."

Smith asks, "Can I have a penny?"

The Lord replies, "In a minute".

Answers—from page 12

1. Internet Protocol
2. Home page
3. IBM
4. Hotmail
5. Steve Wozniak
6. Star Wars
7. 8 bits
8. Integrated Service Digital Network
9. New
10. Video

NOTES