East SIG Report – June 2017

The June meeting commenced with **Frank Maher** welcomed members followed by Q&A conducted by **George Skarbek**.

Q: One of my old portable backup drives failed and I replaced it with a new one. The old one was connected to the power but the new one is powered through the USB port. Is there any difference and does it matter how they are powered?

A: Usually the ones powered through the 240 volts power socket are faster because they are running 12 volts and have a bigger motor. However they are only slightly faster than those powered through the USB. USB2 ports delivers up to 500 milliamps (mA) while USB 3 ports delivers up to 900 mA.

For around $35 to $40 you can buy an adapter that takes a normal laptop drive that fits into a cradle which is powered through a USB port. That's a good way to use drives from an old PC for backups. Some of the earlier backup drives may require 2 USB cables to be connected to a PC, one for power and the other for data.

Q: Would the drives that get their power through the USB port use a USB3 port and would that drive be a solid state drive (SSD), as I believe they use less power?

A: No it would not necessarily need to be a USB3 port or SSD drive. A SSD would run on USB3 and be very fast, but an SSD would be overkill for a backup drive. To buy a terabyte SSD for backups would very expensive compared with a common 1 terabyte mechanical drive costing $80 or less. USB 3 has more power and will give greater transfer rates than USB2.

As an alternative to backing up to a hard drive you might consider purchasing a 120 GB USB3 stick which I've seen for as low as $40. You can fit a lot of data in 120GB. E.g. your mail, Word documents, Excel files, photos etc. I carry with me on my keyring a full Acronis backup of all my important data, but not videos, on a 120GB USB3 stick in case the worst happens.

Q: How do you tell if a port is USB 3?

A: To identify a USB port, USB3 will have a blue bar. If it's not blue it's most likely USB2.

Q: You mentioned you have a full Acronis backup on a 120GB USB3 stick, how big would that backup be?

A: Acronis will compress the data to about half the original size and mine is around 32GB at present. I backup all My Documents folder and mail. I don't backup the Swap file or Hibernate file as these are on the RAM drive and aren't included.

Q: You mentioned earlier that only a very small percentage of members are reading PCUpdate. The current download method is messy by requiring logging in to the MelbPC website. Why can't PCUpdate be emailed out to everyone instead?

A: It can certainly be done. However some members have a small data allowance or small mailbox so historically that is the reason we don't mail PCUpdate out. PCUpdate runs to around 5MB and if people are away their mail will accumulate and could easily fill the mailbox. If photos from the photo completion I mentioned earlier are included in PCUpdate, the size may more than double.

In next month's mail out to members we may introduce an "opt in" option for members who would like to have PCUpdate mailed directly to them. A recently installed system at the office in Moorabbin should make that option possible.

Q: How often should I change my passwords? Various institutions advise me to change my passwords regularly. Based on probability, I believe changing my password daily would only give me low security from brute force algorithms or keystroke logger. If someone steals my banking password from a utility company, my bank account would be cleaned out within an hour. What is your opinion?

A: I change my passwords very infrequently. Some of my passwords for trivial sites such as an online magazine are only 3 characters. I don't want to sit there typing long passwords for these sites. For banking and other more important passwords I use at least 8 characters or longer with upper and lower case letters and include numbers and symbols. If someone steals your computer and tries to log on to a site requiring a password, most sites will only allow between 3 and 10 tries before shutting down. Sites that require passwords will generally limit the time between entries so they can't be bombarded with a million tries a second.

However if someone steals your computer, an Excel file with a password can be attacked using brute force techniques as the file is read into RAM unlike a website login. If you store passwords in an Excel file, I recommend you encrypt the file and change the files extension to, for example .dll (Authors note – In Excel saving with a password varies depending on the version. For Excel 2010 click on the File tab then Select Save. In the Save dialogue box, name the file and in the Tools dropdown box bottom right select the General option. You can add two passwords, one to open the workbook and one to modify the workbook. If Advanced options are available you can set encryption options for added security.)

You shouldn't use the same password for everything. My suggestion when choosing passwords is to start with open square brackets. I use a square bracket rather than a round bracket as it's a character and is quicker to enter as you don't need to use the shift key. The square bracket is followed by 1 or 2 spaces The space key is a character and like the square bracket doesn't require the use of the Shift key. I use spaces as most people don't use spaces in passwords. (A show of hands from the audience revealed no one used spaces in their passwords). Next enter a name with 1 capital letter (e.g. freD) followed by 1 or 2 numbers. Currently the password above is 8 or 9 characters long (eg [freD11). I use this as the basis of all my other passwords. The final part of the password is based on the name of the organisation where the password is to be used, but not the first part of the organisations name. I use the first and last letters, for example I would use Ck for Commonwealth Bank and Tn for Transurban. Using a constant beginning for all passwords makes them much easier to remember as not much thinking is required to remember them.

If you are one of those people who write your passwords down, I suggest you leave off the end of the password by following the method above. Alternatively a written password can include one character that represents something else. For example, if the written password contains a capital A, when entering the real password wherever a capital A appears you replace it with a comma.

After Q&A the first presentation was by **Dave Botherway** on the "**WannaCry Ransomware**". Dave presented the trends in malware, starting from hackers just desiring notoriety to the latest thieves' targeting individuals and businesses for financial gain using Crypo locking ransomware.

The WannaCryTP ransomware exploits social engineering concepts. It requires a user to activate the program usually via an email. The virus encrypts all documents, pictures, music, videos and other data files on the host PC. Other PCs on a network, including those not normally accessible will also have their data encrypted. There is often a "progress" message displayed while file are being encrypted, purporting to be a normal Windows activity such as file or drive checking.

The Windows operating system remains operable as only data files are encrypted. The hackers need the PC to be able to access the internet otherwise the user wouldn't be able to pay the ransom.

Data can be retrieved using a decryption key provided by the hackers when payment in Bitcoins is made. The hackers give the user 3 days to pay around $300 for the decryption key. If not paid within the 3 days, the user is given a total of 7 days from encryption to pay and the price doubles to $600. There is no guarantee a decryption key will be provided and even if it is the virus still needs to be removed from the PC. The best option is to keep a PC up to date and have an image backup and restore your files from that.

Dave explained that the WannaCry ransomware uses a backdoor in Windows to encrypt data and is thought to have originated from the USA National Security Agency (NSA). After the backdoor was made public, MicroSoft issued Windows updates for PCs running Windows 7, 8.1 and 10. Those PCs running Windows 8, Visa and XP are exposed as they are out of support. Updates are no longer available for those older operation systems however MicroSoft has since issued a patch for 8, Vista and XP due to the potential flow on effect of the malware. These OS's can be protected using a simple registry setting to turn off SMB (Server Message Blocks).

After a short break **Stuart Bedford** gave a presentation which touched on a variety of subjects titled "**Humour and More**".

Six degrees of separation. The theory is that anyone in the world is only 6 degrees of separation from anyone else in the world. Eg In Google type a name *Person A* followed by *Person B* a space followed by *number,* Google will tell you how many degrees of separation *Person A* is from *Person B.*

Viewing photos and media files. Stuart revealed that it's not necessary to open a dedicated photo viewer or media player if you already have your web browser open. Stuart demonstrated how dragging photos, videos or music files into a web browser window will play or display these files without the need to open any other programs. For small viewing or listening tasks, a web browser may be a quicker and adequate alternative.

Office Programs. Libre Office was highlighted as a fully functioning alternative to MS Office. The major comparisons are: *Write* is equivalent to *MS Word*, *Calc* is equivalent to *MS Excel*, and *Impress* is equivalent to *MS PowerPoint*. There are other programs included with Libre Office but those mentioned are the main ones most people will use. Libre Office is free with versions available for Windows and Linux. Libre Office opens MS Word, Excel and PowerPoint files and saves in a variety of formats including current MS formats. On occasions Stuart has found that when saving Impress files in PowerPoint format, they don't always play quite the same.

Video Editing. For anyone wanting a free video editing program Kdenlive is worth considering. Kdenlive is a professional quality video editing program developed for Linux and currently ported to Windows. Although the Windows version is still in beta it is very stable and more than usable. Windows and Linux versions of Kdenlive were compared in a Christopher Barnatt YouTube video Stuart played. There was little noticeable difference between the 2 versions as both operated flawlessly in testing in the video.

Downloading YouTube Videos. Stuart demonstrated how he downloaded YouTube videos for his presentation using the Base Terminal in Linux. This was demonstrated in Linux but Stuart has been told the same technique should work in Windows. Stuart demonstrated using a small

Linux program called *YouTube Downloader.* Firstly go to YouTube and copy the URL from the address bar of the video you wish to download then paste this into the terminal. The video is then downloaded.

Passwords. If you need to check how strong your password is go to www.checkmypassword.info/ This site gives an estimate of how many years it would take to break the password. Obviously you don't check with your actual password but with one that's similar in length and with similar characters to the one you finally plan to use.

Humour. The presentation concluded with 3 humorous videos. All were well received by the audience.

Neil Muller