East SIG Report – December 2016

Being the last meeting for 2016 we commenced with the now traditional BBQ followed by a shortened meeting. Normal meetings will resume on the second Thursday in February 2017.

The meeting commenced as usual with Q&A conducted by President **George Skarbek**.

Q: When overseas recently I took my ASUS T100 (Transformer PC) with me. When I first connected to Wi-Fi at the airport the T100 asked do I want to connect to the firewall. This seemed a good idea so I said yes. Now that I'm home it continues to ask me to connect to a firewall. I would have thought that it would now know that I'm home on a safe home network. How can I stop the firewall nagging me?
A: When at home you can go into the network settings and tick that you are on a "Trusted Network". This should stop the firewall nagging you. Alternatively you would do no harm to disable the T100's firewall. The silicone firewall in your router is far better than the software firewall on your PC. When at the airport I would turn the firewall back on, but at home it is safe to turn it off.

Q: I've been trying to install Windows XP on an old PC and near the end of the install I get the blue screen of death (BSOD) and the install fails. When I try to reboot I'm told the NTLDR etc. is missing. When I search for the missing files I find they are there. Can you suggest a solution?
A: If the BSOD stays up long enough record the 8 digit hexadecimal code that is displayed. Use another computer to search the code and the result are usually quite explicit and helpful. Failing that use Hirens boot loader (https://www.**hiren**.info/pages/**boot**cd) to fix your corrupted NT loader. The Hiren's boot CD contains a stripped down version of XP.

After Q&A **Dave Botherway** alerted members to the latest version of the Petya ransomware. This is similar to cryptolocker in that it encrypts your files but also overwrites the MBR, leaving the computer unbootable. The latest Petya ransomware is mostly delivered by fake emails and will do its work without requiring administrative privileges. Even when the MBR is repaired files are encrypted via the Master File Table (MFT) making them invisible to the operating system. When the infection starts, a fake BSOD is displayed and then a fake chkdsk scan runs which is actually encrypting the MFT. Refer http://www.briteccomputers.co.uk/posts/petya-ransomware-overwrites-mbr-encrypts-hard-drive/ for information and video. Melbourne PC has a Yammer group that alerts members to current threats including this one so it is worth signing up to.

Following this **Dave Botherway** gave an excellent presentation on how to setup and use a Home Network. A typical home network comprises a modem, which connects to the internet and then the modem connects to other devices on your network. The majority of modems incorporate a router and have wireless capability. From the modem, devices are either connected via Ethernet cable or by wireless to the network. If you have multiple computers and devices a home network will make life much easier with the ability of share or synchronise files between PC's or to share a printer. Dave's presentation was aimed at Windows users and he discussed the two options available in Windows. The most commonly used is Windows HomeGroup. It is easy to setup and can be enabled with a single password. The alternate option is Selective File Sharing where single files, folders or peripherals can be selected for sharing between PCs.

Neil Muller