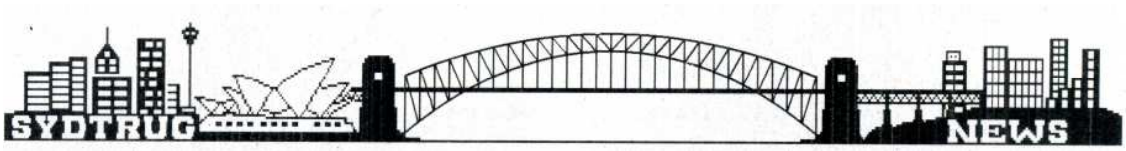


Newsletter of Sydtrug Inc.

Sydney TRS-80/MS-DOS Users' Group

C/- Peter Wignell PO Box 95 NARWEE NSW 2209
AUSTRALIA
Website : www.sydtrug.org

Volume 36 Issue 01 January 2016 Price $2.00

Contents

Who's Who	
President	Peter Wignell (02) 9759 8024 pres@sydtrug.org
Vice-President	Denis J Pagett (02) 9772 4848 den119@optushome.com.au
Secretary	Alex Zui (02) 9726-3594 sec@sydtrug.org
Treasurer	Debbie Lord (02) 9796 1185 treas@sydtrug.org
Membership Secretary	Peter Wignell (02) 9759 8024 memsec@sydtrug.org
Hardware Co-ordinator	Errol Rosser (02) 9796 1185 hwcoord@sydtrug.org
Newsletter Editor	Peter Wignell (02) 9759 8024 newsletter@sydtrug.org
Web Editor	Alex Zui (02) 9726-3594 ax@axlecomp.com
Public Officer	Alex Zui (02) 9726-3594 ax@axlecomp.com

Meeting Arrangements

Meetings will be held on the
SECOND Saturday of the following months @ 1pm

Regents Park Community Centre
1 Amy Street Regents Park NSW 2143

2016 12th March
11th June
10th September

Closing date for the Newsletter contributions is at the monthly meetings

SYDTRUG Inc. INFORMATION

MEMBERSHIP FEES

For **single membership**. $45 per standard financial year (July to June). Or for a **family membership** (which includes all family members living at the same address $55 per standard financial year (as above). These **Fees fall due 1st July each year**. They cover the costs of the newsletter, admission to Sydtrug meetings and access to the group's library.

Our newsletter "SYDTRUG News"

Distributed on a regular basis, it includes the Groups business information and contact details along with articles and information on software and hardware from local and overseas sources. Contributions are always welcome

COST: Included in your membership fee. **Printed Back Issues** (where available) are $2.00 an issue, plus postage ($1 in Australia). However you should first check our WebPages for available newsletters at **www.sydtrug.org**

Other Newsletters

We receive numerous exchange newsletters from similar groups, both local and overseas.

ADVERTISEMENTS

Financial members may place "For Sale", "Exchange" or "Wanted" advertisements in SYDTRUG News. There is no charge, but inclusion is dependant upon space being available. The Editor reserves the right to edit the advertisements as thought fit.

DISCLAIMER

SYDTRUG Inc Members contact details
As at 13th December 2015

Members please note that if no internet address is shown on your membership form or renewal, then none will be shown in this listing.

NAME	Internet address	Phone
Cooper, Mary	oakfordrespnse@virginbroadband.com.au	
Edmonds, Owen	edmonds@spin.net.au	(02) 9451 5758 (H)
Evans, David	davidevans412@gmail.com	(02) 9771 4119 (H)
Jarrett, Robert	gizmomaker@bigpond.com.au	(02) 9371 8539 (H)
Keegan, Brian L	bkeegan@zeta.org.au	(02) 9890 8180 (H)
Kennedy, Ivan R	Ivan.kennedy@sydney.edu.au	(02) 8065 5756 (H)
Lin, Yao (Jenny)	jen@axlecomp.com	
Lumb, George	georgelumb@hotmail.com	(02) 9804-0708 (H)
Mackaway, Julie	Jm2907@hotmail.com	0421-445-299
Ian Mavric	ianmav@netspace.net.au	03-9390-0797
May, Colleen	colleenmay@unseen.is	0410-562-499
O'Connor, Graham	coggoc@hotmail.com	0498 -653 -903
Pagett, Denis J	den119@optushome.com.au	(02) 9772 4848 (H)
Randall, John	marykate@axlecomp.com	(02) 4774 1566 (H)
Randall, Mary	marykate@axlecomp.com	(02) 4774 1566 (H)
Rosser, Errol G	errol@lan-mind.com.au	(02) 9796 1185
Sijnstra, Egbert	sijnstra1@bigpond.com	(02) 4751 3941 (H)
Wignell, Peter	pwignell@bigpond.net.au	(02) 9759 8024 (H)
Zui Alex	ax@axlecomp.com	(02) 9726-3594 (H)

Please check your entry to confirm that there are no errors
For any changes to this listing please advise the **MEMBERSHIP Secretary**

AGM 2015 – Committee Report

Peter Wignell, SYDTRUG Committee
Chairman and President

All the monthly Sydtrug meetings last year were held in the Regents Park Community hall.

The membership of the committee has not changed during the year. They are the following members: Peter Wignell (President, Editor and Membership Secretary), Denis Pagett (Vice President), Alex Zui (Secretary, Webb Site Editor and Public Officer), Debbie Lord (Treasurer) and Errol Rosser (Hardware Coordinator and Librarian). The three Ordinary Member positions on the committee have not been filled.

Original articles for the Sydtrug News magazine have been provided during the last twelve to eighteen months by Sydtrug members including Ivan Kennedy and Errol Rosser. The main source of the articles are articles which we receive via APCUG (Association of PC User Groups in the USA). Each three months Judy Taylour of APCUG bundles twenty to thirty articles together that she receives from various groups who are members of APCUG and emails them to member groups for use in their newsletters. Thanks to all members who have contributed articles for Sydtrug News.

The NSW Dept. of Fair Trading has announced that a statutory review of the Associations Incorporation Act 2009 (the Act) has been completed. The review was undertaken to determine whether the policy objectives of the Act remain valid and whether the terms of the Act remain appropriate for securing those objectives. It is intended to make the proposed amendments in 2016. Any changes to the Act could probably affect the Sydtrug Constitution.

The Sydtrug membership is currently 18 primary members and 7 family members for a total of 25 members being financial for 2015-2016. Three members have decided not to renew their membership for this 2015-2016 year.

The Committee wishes all members of Sydtrug to have a Happy New Year and best wishes for 2016.

Peter Wignell
SYDTRUG Committee Chairman
December 2015

Cloud Computing - An Ephemeral Concept

By Phil Sorrentino, Member of The Computer Club, Florida

http://scccomputerclub.org

Philsorr.wordpress.com
philsorr (at) yahoo.com

Cloud computing has been around for quite some time. It just wasn't called Cloud computing until recently. Although, the term "Cloud Computing" is relatively new, references to "Cloud Computing" can be found as early as the mid-90s. But the term seems to have become popularized sometime in the mid-2000s. In 2008, Steve Jobs of Apple fame, developed his vision of the cloud as a "digital hub for all your digital content". His idea was that a person's digital content (pictures, documents, videos, music) would be stored on a remote server, managed by a trusted company, making that content available for that person to use on any device, anywhere, anytime.

The "cloud" is really just a metaphor for the Internet. It goes back to the days when engineers made presentations that referred to the internet, they pictured the large amorphous infrastructure of the Internet as a puffy, white cloud. This cloud would accept requests for data and provide information and answers. If you are wondering if you ever use Cloud Computing, think about this. If you have ever searched for a gift on-line, ordered it from Amazon, and tracked its progress using the supplied tracking information, you were doing Cloud Computing. You were using applications hosted on someone else's server to accomplish your task.

In the simplest terms, cloud computing just means storing and accessing data and programs over the Internet instead of using only your computer's hard drive or local storage. When you run programs from your local hard drive and store the data on your local hard drive you are doing local computing. Everything you need is physically close by. Local computing is how we have functioned for many years and it has some obvious benefits, like speed, but cloud computing expands your computing reach beyond your local resources.

So, if the cloud is really the internet, let's look at a brief history of the internet. The internet had its beginnings in the development the ARPAnet network that was funded, in the late 1960s, by an agency of the Department of

Defence, Defence Advanced Research Projects Agency. DARPA is responsible for the development of new technologies for use by the military, but in this case non-military commerce has greatly benefited. Some brief technical considerations shows that the internet has no real structure, there are no plans or schematics that define the internet, only the implementation of packet switching and an agreed-upon set of communications protocols, called TCP/IP. Packet switching is a digital networking communications method that groups all data messages, regardless of content, type, or structure, into uniformly sized packages or packets. TCP/IP provides the protocols that specify how data should be formatted, addressed, transmitted, routed and received at the destination. Packet switching and the use of TCP/IP is what makes the internet so amorphous and yet extremely resilient. Amorphous in that you do not know what path a packet will take to get to its destination, and resilient in that if part of the network is unusable, the packets will go via alternate routes. A complete message will consist of from one to many packets. A complete message can be reconstructed when all the packets are received because the packets include the address of the intended receiver, the address of the sender, the body of information, and a set of check characters used to prove the correctness of the received data.

So because the cloud is really the internet, we all have been doing cloud computing for quite some time and we didn't even know it. Google searches, email, Netflix movie streaming, Carbonite backup, Pandora music, YouTube videos, Facebook sharing, Twitter tweeting, and Google Earth mapping, are all examples of cloud computing.

Once the internet was established as a communications pathway to anyone who could operate a personal computer, commerce began to take advantage of its reach. Think about the reach of the highway system in the 60s and 70s. The highway system brought people and commerce together. Shopping malls were easy to get to and they became the place to purchase goods. Now with the internet, people can visit (cyber) stores without even having to use the transportation highways (though the products do have to be delivered and that must be done over the highways). Commercial establishments have built large websites to accommodate the large number of people attempting to use the internet for these commercial activities. Some websites were set up just to search out information that was available from other websites. Does Google come to mind? Other websites were developed to provide the communications capability that has become email. What would we do without email? Still others like Facebook and Twitter provide a forum for social interactions. Many websites were developed to provide the news that would normally be sent to people by the newspapers, and so news websites and news readers became available. Financial institutions realized that they could interact with their customers via the internet and so they created financial websites. Financial websites give the user instant access to their financial information and allow them to buy and sell financial instruments from their home computer. I'm sure you could come up with many more types of internet websites. The last time I looked, there were over 800 million websites connected to the internet. That's a pretty big cloud.

The point of all this is that websites are hosted on computers.

Website computers provide the Server portion of the Client –Server operation. (Your browser provides the "Client" side.) Large websites are not hosted by a single computer. Large websites may employ a network of hundreds of computers. So the bigger the website, the more computers are needed to host that website. The need for these networks of computer servers has evolved into website companies building large "Server Farms". These server farms may have hundreds, if not thousands, of computers networked to act as website servers. Many of the companies with large server farms have set aside a portion, of their cloud, for use by the public. Typically, the first small amount of storage (3 – 7 GB) is free, with larger amounts at a cost. Think, iCloud, OneDrive, Google Drive, and Dropbox.

Creating Your Own Template in Word 2013

By Nancy DeMarte, 1st Vice President,
Sarasota Technology User Group, FL

June 2015 issue, Sarasota Technology Monitor

www.thestug.org

ndemarte (at) Verizon.net

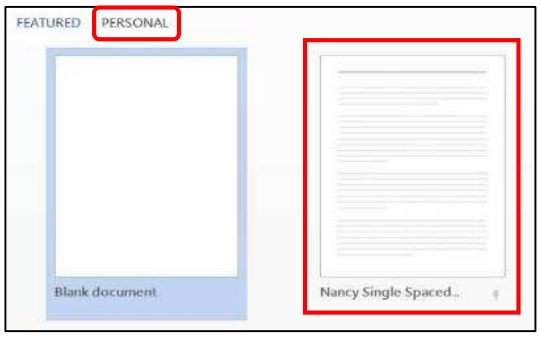
For many years, Microsoft Office has included templates. These are preformatted Word documents, PowerPoint presentations, or Excel spreadsheets, all ready for you to fill in the

content. Using templates saves time and adds a professional look to a project. Office 2013 has changed a few things that make it easier for you to create your own templates.

Since installing Office 2013, I had used the Blank document template, which is the first one displayed in the gallery. Soon I had realized that I was not satisfied with some of the features of this template. I had wasted time by manually changing the line spacing and font too often. So I decided to create my own basic Word template. It was a lot simpler than I expected.
I didn't begin with Blank document template because it contains the Normal style. I knew that some of my previously saved documents might be adversely affected if I did. Instead, I started by choosing the "Single spaced (blank)" template located near the Blank one in the gallery. It opened a box that showed its properties: Font: Calibri 11 point; Paragraph spacing: Single Space; Margins: 1" (on all sides). I clicked Create, and the template opened as a Document. Now I could make my changes. I kept Single Spacing, but chose the font, Calibri Light, in 14 point. To get slightly smaller margins, I clicked Page Layout – Margins, then Custom Margins. I adjusted the 1" margins to .8" on all sides and clicked "Set as Default" to save the margins setting.

Then it was time to save this modified blank document as a template. I clicked File – Save As, opened the Documents folder, named the template "Nancy Single spaced Template,"

changed the file type to "Word Template," and clicked Save. When I opened the Documents folder, surprise! A "Custom Office Templates" folder had been created for me, and it held my new template. I later learned that this folder is created the first time you save any template in Word, Excel, or PowerPoint 2013 applications.



Even though I knew that this new template was stored in the Custom Office Templates folder, I was happy to see that it was also automatically listed in my PERSONAL templates area above Blank Document. And, when I restarted Word, it was also sitting next to the Blank document template, where I could easily choose it any time I opened Word.

You can create a template by modifying an existing one as I did. If you have a document that you use regularly, another option is to start with one of these documents and save it as a Word Template (.dotx). I currently have saved two customized Word templates and a custom PowerPoint template. I always name my personal templates to include the word "Template" so I can easily distinguish them from documents or presentations.

More Security Vulnerabilities Disclosed For Phones, Carriers

Ira Wilsker, *Assoc. Professor, Lamar Institute of Technology; technology columnist for The Examiner newspaper www.theexaminer.com; deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.*

If you are like me, I carry my cell phone everywhere, carrying on voice conversations, sending and receiving text messages, utilizing countless apps, and surfing the Web. Until recently, I gave very little heed to the security of these external communications as our smart devices are supposed to be somewhat secure. GSM carriers like AT&T and T-Mobile utilize encryption to make communications secure; CDMA carriers like Sprint and Verizon also claim to have secure networks. Yes, I do have a major security app on my Android phone that scans new apps and text messages for malware, as well as protects from hazardous websites. Google created Android to be secure, with apps running in a somewhat closed memory space, called by some a "sandbox," which is supposed to prevent purloined apps from talking over the phone. IPhone fanatics, along with many Apple fans in general, believe that their devices are immune to attack, as Apple would not dare to allow any threats to harm their beloved devices.

Now welcome to the world of stark reality. In a recent column, I wrote about two newly revealed vulnerabilities, known as "Stagefright" and "Certifi-gate," that may threaten the security, safety and privacy of nearly a billion smart phones and tablets. Since then, others have come forward demonstrating previously

unannounced security vulnerabilities that threaten the security of our smart phones, often including both iPhones and Android devices in their threat assessments.

One of these newly disclosed threats explicitly targets the most technology innocent and uninformed among us. Appropriately called "grandma malware," this clever piece of malware sneaks onto Granny's phone using a compound method of infection designed to defeat many of the simplest security precautions. While recently updated Web browsers and desktop security software, as well as updated phone operating systems, have likely patched the vulnerabilities, Granny's often older and unpatched computer and phone may be vulnerable. The first step in the infection sequence occurs when the victim downloads an innocent looking app, often a game or simple photo utility, onto their computer using any one of the older versions of most of the common Internet browsers, which are still in wide use. This small utility, explicitly designed to appeal to a "grandma," does not itself contain any malware, and will pass the scrutiny of many of the less sophisticated desktop security products. This utility sits quietly and apparently innocently on the victim's computer, often performing its intended tasks. The app surreptitiously monitors Web surfing until Granny logs on to an app store, such as the Google Play Store. The malicious utility captures the logon and connection information from the app store; with this information, the malware is invisibly downloaded wirelessly to the smart device, installing itself on Granny's phone. Once installed, this malicious app immediately gathers personal data from the phone and sends it to parties unknown. Even if this malware is detected and removed in a subsequent security scan by a third party security utility, it is too late; all of the personal information was stolen within seconds of the app being installed on granny's phone. Granny's private information has just been stolen, and she might very well become an identity theft victim; as is common in criminal enterprises, the most vulnerable among us are more likely to be victimized.

Despite the travesty of purposely going after Granny, it is not one of the most insidious of the newly announced threats imperiling our smart phone usage. In recent days, a pair of IBM cyber security analysts, Or Peles and Roee Hay, uncovered a flaw in the Android operating system still being used in over a half-billion Android smart phones. This vulnerability, not yet formally named but referred to as a type of "masque" attack, could allow hackers to take over and remotely control vulnerable Android phones. According to these researchers, "Masque attacks are defined as malicious apps uploaded, say, from e-mails directing victims to fake Web links." According to Peles and Roee, Google has issued patches for devices running Android 5.1, 5.0, 4.4, and Android M, but as often the case for many Android devices (except some Nexus phones), it is up to the phone manufacturer or cell phone carrier to push these patches to their users, meaning that although the patches are available, over half of Android phones do not yet have the patches installed.

This "masque" attack vulnerability allows hackers to control the security privileges that are a part of the Android operating system, allowing compromised or counterfeit apps to access information on the phone that would otherwise be unavailable to the hacker. According to the researchers, this vulnerability allows the data thieves to steal personal information, capture banking information including logins and passwords, access the phone's cameras, download contact lists, and pilfer stored files and e-mails, sending the stolen information to a remote server. While this particular Android vulnerability was recently discovered by IBM cyber security experts, it is very similar to one discovered several months ago by FireEye that explicitly targets Apple's iPhones. The mechanism and modus operandi, as well as the data thefts, are almost identical between the Android and iPhone vulnerabilities.

A "masque" attack can occur when smart phone users download any of 11 authentic looking but counterfeit or contaminated apps that also appear to work properly when downloaded and

installed. Among the most commonly downloaded iPhone and Android apps that enable this vulnerability are modified copies of Facebook, Twitter and WhatsApp. According to FireEye, iPhones are as vulnerable to these masque attacks as Android devices. According to Zhaofeng Chen, a senior research engineer and scientist at FireEye, the 10 tainted apps that most threaten Apple devices are "WhatsApp, Twitter, Facebook, Facebook Messenger, Google Chrome, Blackberry Messenger, Skype, WeChat, Viber, Telegram and VK." These apps are often downloaded from genuine-appearing links in e-mails or SMS text messages, and mimic the functionality of the genuine app, but allow for the remote access to this valuable personal content. FireEye was quoted as stating that this iPhone vulnerability can steal or access a variety of information from compromised phones. Among the dastardly deeds that this masque vulnerability can perform include recording and forwarding phone calls placed on Skype, Wechat and other voice apps; intercept text and SMS messages from iMessage, WhatsApp, Facebook Messenger, Skype and other SMS apps; send real-time and historical GPS locations; access website histories; steal contact information and lists; and download photos from the phone. Apple has created patches and upgrades closing this vulnerability, and pushed these patches to many of its users, but there are inevitably iOS device users who have not received or installed these patches.

In recent days, on the Australian version of the "60 Minutes" news magazine, another cell phone vulnerability was demonstrated where hackers in Germany were easily able to listen in on a cell phone chat between individuals in Australia and the UK. This ability to readily capture live calls is known as the "SS7 Vulnerability." SS7 technology is widely used, legitimate and necessary for cell phone carriers to properly direct calls and text messages to their intended recipients. ComputerWeekly.com said, "Like any protocol, SS7 is vulnerable to exploitation by sophisticated and well-funded third parties with criminal intentions." In another ComputerWeekly.com story titled "Security flaw exposes billions of mobile phone users to eavesdropping," the online magazine says, "Hackers, fraudsters, rogue governments and unscrupulous commercial operators are exploiting flaws in the architecture of the mobile phone signalling system known as SS7. ... Billions of mobile phone users around the world are at risk from covert theft of data, interception of their voice calls and tracking of their location." SS7 is not a vulnerability in the phones themselves, as the vulnerability is not brand or operating system dependent, impacting Android, iPhone, Blackberry and other systems equally, but is in reality a vulnerability in the switching system utilized by the cell carriers themselves.

For those of us who routinely use Android, iOS or Blackberry devices without much thought about the inherent security vulnerabilities of the phones and cellular carriers, keep at least a spark of consideration in mind. While I am fully cognizant of the risks, I will continue to use my smart devices pretty much as I have in the past.

The Times They Are A-Chargin'

By Greg Skalka, President, Under the Computer Hood User Group, CA

February 2015 issue, Drive Light

www.uchug.org

president (at) uchug.org

I just want to say one word to you. Batteries.

In the 1967 movie "The Graduate", Dustin Hoffman's character was advised that plastics would be the future hot field. Today, I think the hot field to go into may be batteries. Modern technology is dominated by mobile and cordless electronics, which need batteries to supply their power. Cameras, smart phones, tablets, laptops, quadcopters, cordless tools and electric cars all depend on batteries for their primary power source. We probably don't realize, until the batteries go dead, how many of the products we use every day depend on batteries to run. That television on your wall (try using it for any length of time without a remote control), noise-cancelling headphones on your head, wireless mouse in your hand, electronic safe in your closet, electronic safety light on your bike and Fitbit on your wrist all need batteries to run. So many other products, like your alarm clock, electronic thermostat and sprinkler timer, require batteries for backing up settings and timekeeping. We are awash in battery-powered products. Keeping all these batteries charged or changed presents a big challenge. And like plastics, they have the potential for harming our environment if not handled and disposed of properly.

Before we mastered electricity, our devices had to be human, animal, water or combustion-powered. Batteries actually predate the electrical grid; Alessandro Volta invented the first true battery in 1800. Early electrical

innovations like the telegraph and electric lights were initially powered by batteries. It wasn't until the early 1900's that widespread commercial electrical power generation and distribution displaced batteries in most uses for electricity. Now with our thirst for mobile electronic devices and need for better energy storage, batteries are making a big comeback.

Battery technology has changed and improved over the years. Volta's zinc-copper voltaic pile has spawned zinc-carbon and alkaline single-use battery technologies, as well as many rechargeable battery types. New materials have increased the energy density and battery lifetimes for rechargeables. Nickel-cadmium (NiCd), nickel-metal hydride (NiMH), lithium, lithium ion (Li-ion) and lithium ion polymer batteries have allowed our portable devices to shrink in size and increase in capabilities. Batteries now come in many shapes and sizes, from tiny watch batteries to huge electric car battery packs. The standard AAA, AA, C, D and 9V cells have been supplemented with a multitude of custom sizes to suit new product applications, from large, high-capacity removable laptop batteries to super-thin, non-removable smart phone batteries.

Battery charging has become an important part of the life of every technology user. How long it takes dictates the time you and your cell phone must remain tethered to a wall outlet and determines when you may continue your electric car road trip. Higher capacity and the ability to swap batteries can help users, but eventually everyone must recharge. The most popular place in the airport terminal has become the seating next to the wall outlets. Unfortunately, every new electronic device adds another charging cable to your collection. The 5V USB socket has become the new charging standard for many devices. New upscale homes come with USB charging sockets built into the kitchen outlets; plug-in versions, like the Vivitar Home Charging Station, are also available.

No battery lasts forever. After many charge and discharge cycles, every rechargeable battery begins to lose its ability to hold a charge. Eventually it can hold so little energy that it is useless and must be replaced. For many products, battery replacement is very easy. Laptops and digital cameras have batteries that are easy to remove, and replacements are usually easy to find on the Internet. For other devices like tablets, smart phones and electric razors, changing the battery is much more difficult. Opening the device to get to the battery may be difficult and require special tools, and the battery is sometimes soldered in. Special knowledge is usually required to open the device without damaging it. Sometimes the product can continue to be operated by using it with power cord (like my electric razor), or with an external battery (like my wife's iPhone with a Patriot Memory Fuel+ portable charger). Eventually it may get to the point where either the battery or the device must be replaced.

Fortunately, the Internet comes to the rescue again, not only to help locate a replacement battery, but also to provide the knowledge required to make the change. Lots of step by step instructions and how-to videos are available on YouTube and other sites to help disassemble almost any battery-powered device. Replacing the battery saves the consumer money, avoiding the purchase of a new product, while continued use of the device keeps it out of our landfills.

I recently had the batteries in two of my electronic devices go bad, requiring a change to continue using them. By doing some research on the web and spending around US$20 total on replacement batteries, I gave new life to these items while postponing having to spend the approximately US$120 in total to replace them.

An uninterruptible power supply, or UPS, is an almost essential accessory for a desktop computer. While a laptop's data is protected by a charged battery should line power fail while running with the ac adapter, you can lose data and risk hard drive corruption if a blackout occurs when using a desktop computer. A UPS contains a battery which is charged off the wall output and allows the computer and anything else plugged into it to run for a time if the ac is interrupted. The UPS typically monitors the battery's health and emits a loud tone when the battery is failing.

My desktop computer's UPS recently sounded its battery's death-call, so I shut it down and plugged the computer into a power so I could still run it while working on the UPS. I'd changed the battery before, and planned ahead by placing a label with the battery part number on the outside of the case. I found a replacement battery on Amazon for US$12; a new UPS of this capacity would cost US$40 to US$50. Once I'd received the new battery, I removed a couple screws on the back to release the cover and reveal the battery. The battery is connectorized, so changing it is easy, as long as you observe the polarity of the battery

connections. Once it was reassembled, it worked as good as new.

My second battery change was a bit more difficult. My Braun Oral-B electric toothbrush had been having charging difficulties for quite some time. The internal battery had developed a memory from going through repeated short charge-discharge cycles, and no longer held much of a charge. Fully discharging it and recharging helped for a time, but it was finally getting to the point where it was essentially unusable. Since it charges inductively from its wall unit, there was no way to use it in a "corded" manner.

I searched the web and found www.fixit1stop.com had a repair video for my toothbrush. It showed how to disassemble the toothbrush and change the battery. This was considerably more involved than the UPS. The case had to be opened to expose the plastic frame containing the motor, circuit board, battery and inductive charging coil. The NiCd battery was soldered to the internal circuit board. Fortunately, I am an electrical engineer and have the skills and tools to perform the transplant. For those that don't, this web site not only sells replacement batteries (US$10 for my model's) but also provides a repair service (US$25 for mine). I couldn't find the correct battery anywhere else, so ordered it from this site. When it arrived, I performed the replacement per their web instructions and, after a night of charging, the toothbrush worked great.

Batteries contain hazardous materials and must be recycled or disposed of properly. In many places it may be illegal to send old batteries to the landfill. Once again the Internet can provide information on battery recycling in your area. It turns out rechargeable batteries are accepted for recycling for free at many Best Buy stores, including the ones near me. They have a bin just inside the entrance, where I was able to deposit my two old batteries. There were a lot of recycling options for rechargeable batteries in San Diego, but I didn't find any place that accepted single-use batteries without a fee.

Batteries will continue to be an important part of our technology. To save money and the environment, consider changing the batteries in your electronic devices when they fail, rather than toss out the whole thing, and be sure to dispose of the old batteries properly.

The Rankin File

What is Medical Identity Theft?

Bob Rankin, bob@rankin.org
September 22, 2015 Column

Medical Identity Theft on the Rise

Your credit and bank account balance are not the only valuables that identity thieves are after. As health care costs have soared, so have incidents of "medical identity theft" in which crooks steal the credentials that enable one to obtain health care and sell them to other crooks. Here's what you need to know...

Medical identity theft is on the rise. And sadly, it is much more difficult to guard against this type of ID theft, and much harder to clean up the havoc it can create for a victim.

The Medical Identity Theft Alliance estimates that over 2.3 million Americans have been victims of medical ID theft, and 2014 saw 500,000 more cases than the previous year. That bad news is sure to get much worse. The MITA's latest survey was conducted in November, 2014, before the disastrous leak of 80 million patients' personal health information from Anthem. And just yesterday, I read that an "error" on Amazon's Web Services platform exposed 1.5 million people's private medical records.

Criminals can use victims' birth dates, Social Security Numbers, and the ID numbers found on insurance cards to obtain medical services and prescriptions at hospitals, clinics, and doctors' offices. While medical providers today routinely scan your driver's license, you may notice that they aren't very diligent about verifying its authenticity.

Medical Identity Theft

A fake license that wouldn't fool a liquor store clerk can be used to rack up thousands of dollars in health care costs very easily. Insurance cards, generally, don't bear photos or signatures. Using stolen medical credentials, a crook may visit multiple hospitals, pharmacies, and doctors to obtain services and drugs – often narcotics.

The records of these transactions are added to victims' health care records, and should be visible on your Explanation of Benefits letters, but bogus healthcare transactions often go undetected for months or even years.

The MITA's survey found that the average victim did not learn of medical ID theft until three months after it happened, and 30 percent victims could not determine when their health care credentials were improperly used. Health care privacy laws force victims to be intensely involved in investigations of medical fraud.

Can't Get No Satisfaction

If you've ever challenged a hospital bill, you know how hard it can be to prove that you did not authorize or receive the treatment claimed. Only 10 percent of victims in MITA's survey indicated they were "completely satisfied" with the resolutions of their cases. About 65 percent of respondents said they ended up paying an average of over $13,000 to resolve disputed claims.

MITA estimates that medical ID theft crimes are a $5.6 billion industry. Larry Ponemon, head of The Ponemon Institute that conducts MITA's annual surveys, believes that "a medical record is considered more valuable than everything else" to cybercrooks. Credit cards expire and are replaced frequently, rendering them useless to fraudsters after a short time. But Social Security numbers and personal health information don't change; a crook can use them practically forever.

There is no way to "freeze" health care credentials as one can freeze a credit card account. There are no centralized reporting agencies analogous to Experian, TransUnion, and Equifax that collect health care activity and can monitor it for suspicious patterns. Health care providers are trained to be helpful to patients, not sceptical of their identities.

In short, there are very few protections against medical ID theft and little help resolving its consequences. My 10 Tips to Avoid Identity Theft will help you safeguard your personal and financial records.

Aside from that, the most important thing you can do to guard against medical ID theft is reactive: read all of those "explanation of benefits" letters that come from your health care providers and insurance company as soon as they arrive. If you see anything suspicious, do not delay in challenging it.

Are you concerned about other forms of identity theft? Your best defence is knowledge and a proactive stance. See my articles *Free Credit Reports Online* and *10 TIPS: Identity Theft Protection* to learn what steps you can take, both online and offline, to protect yourself.

SYDTRUG AGM 2015 Results

Peter Wignell, President of Sydtrug
Email: pres(at)Sydtrug.org

The Sydtrug Annual General Meeting (AGM) was held in the Regents Park Community Centre on 12th December 2015 with seven members present including one family member.

A Christmas party followed the AGM.

All ordinary business items were passed by the members attending the AGM with the exception of the motion to 'Suspend Monthly Meetings' which was passed by all members present with an amendment from Ivan Kennedy. The motion was amended to change the meeting times from monthly to quarterly which means only four meetings will be held each year. The meetings will occur on the second Saturday of January (2016 only), March, June, September and December. Even though January is not on the new schedule, this month's meeting will still go ahead because the date was within the one month's notice period that Auburn Council requires for a cancellation.

Proxy votes were received from two members.

There was no changes to the SYDTRUG office bearers as the Secretary did not receive any other nominations. The following positions have been filled.

President	Peter Wignell
Vice President	Denis Pagett
Secretary	Alex Zui
Treasurer	Debbie Lord
Membership Secretary	Peter Wignell
Hardware Co-ordinator	Errol Rosser
Newsletter Editor	Peter Wignell
Webb Editor	Alex Zui
Librarian	Errol Rosser
Public Officer	Alex Zui

Check the front page of this newsletter for contact details for the above committee members.

To all members I wish you and your family a HAPPY NEW YEAR for 2016.

SYDTRUG Meeting News for Saturday 12th December 2015, Christmas & AGM

By Errol Rosser, SYDTRUG Librarian

(Photos courtesy of Ivan Kennedy and Errol Rosser)

Signs of Christmas at the meeting


Welcome signs at the car park and front door

Committee meeting

Present :-

President, Secretary, Hardware CoOrdinator, Membership Secretary, Public Officer, Treasurer, Librarian, Web Editor and Newsletter Editor

Meeting Details :-

Started at 13:04, minutes of the previous meeting were accepted, correspondence noted and various committee reports were given. Debbie noted there was $0.01 income (bank interest) and $0.00 expenses for the previous month.
Discussion was started on the committee meeting dates and venues for 2016, but couldn't be completed until results of voting on the motion to suspend meetings in known (at the AGM)

General meeting

The usual three non-committee members attended today - Jenny (arrived with Alex), Colleen May, and Ivan Kennedy.
I delivered some Model I floppy drives for Ivan to test on his Model I and MISE (Model I System Expander) from Peter Bartlett and Ivan set up his Model I while the committee meeting was in progress

Model I floppy drives ready for testing

2015 AGM

Meeting Details :-

Started after the committee meeting finished, the minutes of the previous AGM were accepted. The committee report and president's "Thank You" speech were given by Peter. The treasurer's report was given by Debbie, noting the Nett result for 2014/2015 year was $295 negative.
The election of office bearers didn't require voting as the only nominations were from the incumbents to continue in their office.
The motion to suspend meetings was then put to the meeting & much discussion ensued. The motion was eventually amended to reduce the meeting frequency to quarterly, instead of a total suspension. It was suggested that December be one of the quarterly meetings, so we can continue to have the AGM and Christmas meetings on the same day.

Christmas lunch followed the AGM

All members had brought food & drinks to share.
Armed with good food and drink, we all sat down to a convivial social get together.

Alex and Jenny getting some Christmas lunch

Ivan suggested having a "Reunion" style meeting in 2016. After some discussion, it was decided to have the reunion at the September meeting. Ivan will try to get in contact with previous club members to invite them to attend

By the time the AGM and Christmas lunch were over, it was time to pack up, so very little testing of floppy drives was done

The meeting was closed, at 17:05

Top 10 Reasons to Upgrade to Windows 10

Sandy Berger, COMPUkiss
www.compukiss.com
sandy (at) compukiss.com

If you are still on the fence about upgrading to Windows 10, it is everything that Windows 8 should have been, but wasn't. Here are 10 reasons why you should upgrade.

1. Windows 10 is a free upgrade for anyone using Windows 7 or Windows 8.1. This offer is good until July 28, 2016. After that time it will cost US$119.
2. When Windows 10 starts, you are dropped immediately into the Windows 7- type desktop. Although there will be some new things to learn, end users will find that the transition to Windows 10 will be much smoother than the transition to Windows 8.
3. Windows 10 is faster and more secure than Windows 7 or Windows 8.
4. Windows 10 is easy to use with a keyboard and mouse and just as easy to use with a touch screen. If your computer has a touch screen as well as a keyboard and mouse, you get the best of both worlds.
5. As a service, Windows 10 will be constantly updated to keep it more secure and more capable.
6. The new Edge web browser that comes with Windows 10 is faster and more secure than Internet Explorer. It also offers useful new features like the ability to make notes on a web page and send them to a friend and the ability to save a web page to read later.
7. Several apps like Mail and Photos have been dramatically improved.
8. Although the Start Menu is back, it is larger and more distracting than it was in Windows 7. Fortunately, it is customizable so you may want to spend some time getting it to suite your taste.
9. Cortana, a voice assistant like Apple's Siri is built into Windows 10. You can ask her questions and she can even help you find your files.
10. The new File Explorer is much improved. It now shows a list of useful Quick Access locations and folders you use frequently in addition to Recent Places.

Ian Mavric collects and repairs TRS80 machines, he will provide a home to any unwanted TRS80's complete or otherwise.
He is trying to stimulate interest in the TRS machines, not so much as a useful alternative to a current Win7 or MAC computer, but as collectors and restorers of old hardware for posterity.
Ian repairs, upgrades, purchases and re-sells TRS stuff... following is the address of his website to give you more of an idea of what he does.

http://ianmav.customer.netspace.net.au/trs80/