

## INSIDE THIS ISSUE:

<i>Committee details</i>	Page 2
<i>OPEN News</i>	Pages 3-8
<i>PC Security after XP's Official End of Life</i>	Pages 9-14
<i>Computer Joke</i>	Page 14

## FEBRUARY MEETINGS

**OPEN's ANNUAL GENERAL MEETING will be held on Wednesday, February 5th, 2014 at 1.00pm. The main items of business will be the presentation of the annual financial reports and the election of office-bearers.**

**A short monthly meeting will follow the AGM At 7:00 pm on February 5th the AGM for the Launceston Computer Group will be held, with a similar agenda to the OPEN AGM. Time permitting a short monthly meeting will be held at the conclusion of the AGM.**

### Newstream Articles

Deadline : 10 Days before Meeting

Editors Contacts:

Address: 8 Cadorna Street Mowbray Heights 7248 Phone 6326 5824

email address [editor@lcg.org.au](mailto:editor@lcg.org.au)

### Correspondence

Address all Correspondence to:  
Launceston 7250

Launceston Computer Group Inc

PO Box 548

### Membership

**Single \$20, Family \$30 (Includes Email edition Newstream)**

**Printed & Posted Newsletter \$20 extra**

**Disclaimer:** The articles in this newsletter may be reprinted as long as credit is given to the original author. Opinions expressed are those of the author & not necessarily the views of the Editor or the Group. Unless otherwise noted material is copyright 2011 for the Launceston Computer Group Inc.

## LCG Committee 2013/14

President: Bruce Dineen

Vice President: Ivan Turmine

Secretary: Treasurer: Dennis Murray

Ass. Treasurer: Laraine Rist

Newstream Editor: Ron Baker

[<mailto:editor@lcg.org.au>](mailto:editor@lcg.org.au)

Public Officer: Judy Hall

O.P.E.N. Co-ordinator: Robert Tierney

Webmaster/Content: Tom Olsen

[<mailto:webmaster@lcg.org.au>](mailto:webmaster@lcg.org.au)

Auditor: Ron Baker

Publicity Officer: Iris Meek

"V.I.C.T.O.R." Co-Ordinator: Robert Tierney

LCG Committee: Glenn Gilpin, Reinhard von Samorzewski, June Hazzlewood, Janet Headlam, Julie Hjort

## OPEN Committee 2013/14

**O.P.E.N. Co-ordinator:** Robert Tierney. *Responsible for the smooth running of the Centre on a daily basis*

**O.P.E.N. Chairperson:** Laraine Rist. *Chair all meetings of OPEN and ensure that they run smoothly*

**O.P.E.N. Vice Chairperson:** Robert Tierney. *Chair meeting when the Chairperson is unavailable.*

**O.P.E.N. Minute Secretary:** Heather Loffel. *Handles all incoming and outgoing communications Responsible for the documentation and distribution of all meeting minutes*

**Assistant Secretary:** - open -. *Help the Secretary where necessary*

**Treasurer:** Dennis Murray. *Responsible for all monies and banking*

**Assistant Treasurer:** Laraine Rist. *Help the Treasurer where necessary.*

**Newsletter Editor:** Dennis Murray.

**Publicity Officer:** Iris Meek. *Responsible for all advertising*

**Membership Co-ordinator:** Eleanor Horder. *Keep Membership database up to date.*

**Tutor Co-ordinator:** Bruce Dineen. *Keep regular contact with Tutors to bring ideas and concerns to meetings*

**Maintenance Co-ordinators:** Dennis Murray. *Responsible for the maintenance and repairs to all computer equipment*

**"V.I.C.T.O.R." Co-ordinator:** Robert Tierney.

**Webmaster/Content:** Tom Olsen. [<mailto:webmaster@lcg.org.au>](mailto:webmaster@lcg.org.au)

**OPEN Committee:** June Hazzlewood, Judy Hall, Janet Headlam, Sandra Viney, Kay Dawson, Karia Wicks.

## OPEN NEWSLETTER — FEBRUARY 2014

### SO LONG BRUCE ... AND THANKS!

It isn't what I would call the best of starts to the New Year at OPEN but unfortunately I have to advise members that our multi-talented tutor and 'volunteer-at-large' Bruce Dineen will not be a part of our team in 2014.

For health-related and family reasons Bruce has decided to step down from all his duties effective immediately.

How do we best describe Bruce? Extremely knowledgeable and widely experienced in the technical and tutorial aspects of computing, with an ability to impart his knowledge to members on computer subjects ranging from the most basic to the more complex, and the versatility to take on the challenge of the ever-changing technological environment that OPEN and its members operate in.

In the last twelve months Bruce has served in the positions of Launceston Computer Group President and as OPEN's Tutor Coordinator, and is the person who can be credited with setting up a formal instruction and education program for our growing 'Android Community'.

Although I'm not an Android fan I think I can speak for the many Android-owning members who found that individually they may have been 'stumbling through the wilderness' until Bruce convened special sessions that allowed members to learn about the most useful 'apps' to install, and how to navigate their way around their tablets.

From a personal perspective I will miss Bruce's invaluable assistance on the technical side, particularly with the installation and implementation of our upgraded wireless network, while a glance inside our storeroom will reveal the work that Bruce put into installing new shelving to improve and re-organise our storage facilities.

I'm sure that all members who have had contact with Bruce during his three years at OPEN will agree that our club's knowledge base has been enriched as a result of his considerable input, and will join me in wishing him better health in the coming months and years.

**All the best, Bruce!**

**Dennis Murray**

### FEBRUARY MEETINGS

**OPEN's ANNUAL GENERAL MEETING will be held on Wednesday, February 5th, 2014 at 1.00pm. The main items of business will be the presentation of the annual financial reports and the election of office-bearers.**

**A short monthly meeting will follow the AGM**

**At 7:00 pm on February 5th the AGM for the Launceston Computer Group will be held, with a similar agenda to the OPEN AGM.**

**Time permitting a short monthly meeting will be held at the conclusion of the AGM.**

**VICTOR PHONE NUMBER 0408 174 235**

**Contact the Coordinator Rob Tierney for assistance with computer problems at home**

**(Bookings are subject to availability of tutors.)**

### VENUE TELEPHONE NUMBER

Don't forget that the club telephone is available during class hours.

**\*\*\*\*\* 6343 4928 \*\*\*\*\***

Members and tutors can be contacted at the clubrooms **during class hours** by telephoning the number shown above.

Monday to Friday 10am – 3pm

Tuesday evenings 7pm—9 pm

### CO-ORDINATORS REPORT FOR 2013.

A big thank you to all the committee members and volunteers for making 2013 another successful year. Without you and our students there would be no O.P.E.N.

In 2013 we welcomed 99 new members

**From April to December** – Dennis ran a beginners class for Windows 8.

**June** - V.I.C.T.O.R again sponsored Australia's biggest morning tea for Cancer Council. An incredible \$413 dollars was raised.

#### Guest Speakers:

July - Natalie Sankey from Hearing Australia

August - Nigel Jessup from Telstra gave a talk on the NBN

**October - Seniors Week:** This year there had been a delay with the publishers meaning organisations received their Seniors Week supplement so that we only had about 2 weeks to receive any bookings. Also the sign-up form to register was very hard to navigate. After Seniors Week an email was sent to participating organisations to give their feedback and I well and truly expressed my frustrations and from subsequent correspondence other organisations were also expressing their views on the issue.

#### Special Workshops:

Music Conversion

Free Rip

Android

Computer maintenance

Scanning

Internet Security

#### Grants:

We were successful in acquiring a \$2,000 grant from Community Capacity Building Grants program for volunteer travelling expenses, a one-off small gift to say thank you to our tutors.

#### Christmas Lunch:

The Christmas lunch was held at the Commercial hotel—it was our biggest turn out with 80 people. The venue was still not adequate as we filled nearly the whole function room, so for 2014 we will need to find a bigger venue if that is possible.

**Rob Tierney**

## LOOKING AHEAD INTO 2014

Many of you will have already received a copy of our 'Wednesday' Specials' program for the first few months of 2014.

Based on the results of that often-mentioned survey we've introduced some new subjects for this year while continuing the popular topics from previous years.

With Bruce Dineen not being available there have been some changes to the initial program so please make sure you have the latest copy. The February classes are covered in the boxes to the right, so I'll just comment on a few of the sessions March and April.

I'll be kicking off with an **'Introduction to Excel Spreadsheets'** on the morning of March 5th with a follow-up session on April 3. Spreadsheets can be useful for tasks other than 'number-crunching' but for many of our members spreadsheets faded from view after completion of e-Learn and O-Learn courses.

For Android users we are hoping to keep you up-to-date with the recruitment of one or two new tutors. We'll keep you informed of progress in that regard.

**Dennis**

## SCREEN-PRINTS IN WINDOWS XP (AND EARLIER OPERATING SYSTEMS)

Those computer users who don't have the Snipping Tool available to them often use the Print Screen function to capture the contents of the screen in front of them.

Usually we have to hold down the Shift key and press the PrtSc key located somewhere near the top of the keyboard, and then we paste the captured image into some sort of file.

But did you know that there is a variation of this function that will copy just the contents of an open window?

Try holding down the ALT key and then PrtSc and see what happens when you paste it.

You should see just the window contents so you won't need to crop the image.

**Dennis**

## OPEN NEWSLETTER – FEBRUARY 2014

### FAMILY HISTORY 2014

**Wednesday February 12**

**1:00 pm to 3:00 pm**

**Wednesday February 26**

**10:00 am to 12:00 noon**

New information is being added to our resources on an on-going basis to help you trace your family's origins. Contact the club for more information.

**Classes limited to 8 people.**

Join Judy, Margaret G and the other tutors for these informative sessions.

### STAYING SAFE ON THE INTERNET

**Wednesday February 19th, 2014**

**10:00 am to 12:00 noon**

In our post-Seniors Week survey Internet Security ranked highly as one of the topics that members wanted to know more about.

Technology can only provide a certain amount of protection so it is up to the computer user to be aware of the pitfalls that may be encountered.

Even reputable web-sites may set traps for the unwary e.g. which of the three DOWNLOAD buttons shown is the one that is going to give you the program you require.

Rob Tierney's session aims to provide you with information on what security products are safe and reliable, what pitfalls you may encounter, how to spot a fraudulent invitation and more.

Motto ??? It's best to know what a bear-trap is **before** you put your foot in it!

### LEVEL 2 & 3 GRAPHICS

**With Paint Shop Pro 7 and 8**

**Wednesday February 12**

**10:00 am to 12:00 noon**

### ADVANCED GRAPHICS

**Incorporating Paint Shop Pro XI**

**Beginners**

**Wednesday February 26**

**1:00 pm to 3:00 pm**

**(re-introduced after 3 years)**

These classes are designed for people who have completed the Basic Graphics classes, and involves more advanced features of the Paint Shop Pro graphics programs.

### PASSWORD MANAGEMENT

**WEDNESDAY February 19th at 1:00 pm**

Almost every aspect of our computer operations requires a password—from logging in to your computer, checking your e-mail, social networking, updating your software, on-line banking and so on.

Being able to access all your services with the correct passwords, (whether you are at home, at OPEN or on holiday) makes life so much easier and adds flexibility to your computing adventures.

Learn how to keep on top of all those passwords.

## OPEN Session Times

At Studioworks, 1 Pipeworks Rd, L'ton

**Standard Sessions \$6.00**

[Some special tutorial materials may incur additional charges]

Monday	10 am –12	General & Beginners
	1 pm – 3 pm	<b>Basics and Beyond</b>
	<b>3:30 pm – 5:30 pm</b>	<b>Beginners Class</b>
Tuesday	10 am –12	O-Learn & Beginners [all day]
	1 pm – 3 pm	<b>Mac [all day]</b>
	7 pm–9 pm	Basics (Night Class)
Wednesday		Special sessions or Meetings
		As for mornings (see rosters)
Thursday	10 am –12	General & Beginners
	1 pm – 3 pm	General &
Friday	10 am –12	General & Beginners
	1 pm – 3 pm	Beginners Class

## OPEN NEWSLETTER – FEBRUARY 2014

### SPECIAL WEDNESDAY SESSIONS

Please register on the sheets – numbers may be limited

Date	Time	Topic	Details
February 5	10 am—12 noon	Windows 8 Introduction and Review	What has been the impact of Windows 8 so far and how will it affect computer users in the future?
	1 pm onwards	<b>OPEN AGM and Monthly Meeting</b>	Presentation of 2013 Financial Report and Election of Office-bearers for the coming year
	7:15 pm onwards	<b>Launceston Computer Group AGM</b>	<b>Presentation of 2013 Financial Report and Election of Office-bearers for the coming year</b>
February 12	10 am—12 noon	Level 2 and 3 Graphics Class	Advanced graphics using Paint Shop Pro 7 and 8
	1 pm—3.00 pm	<b>Family History</b>	<b>Judy, Margaret G and the team will help you trace your ancestors.</b>
February 19	10 am—12 noon	Internet Security	This was one of the most-requested topics in our recent survey. Rob Tierney will explain on-line pitfalls.
	1 pm—3.00 pm	<b>The Importance of Password Management</b>	<b>As more of our computer life is being lived 'on-line' learn how to keep on top of all your passwords.</b>
February 26	10 am—12 noon	Family History	Use our extensive range of resources or use Ancestry.com on-line to research your Family History.
	1 pm—3.00 pm	<b>Graphics Beginners PSP XI</b>	<b>Re-introduced after 3 years this course will take our 'Basics graduates' to the next level.</b>

**Members are reminded that subscriptions for 2014 were due on December 1st, 2013. if you haven't yet paid your subs please do so on your next visit to the club. Single Membership \$20, Couples \$30 per year**



## OPEN NEWSLETTER FEBRUARY 2014

### RECYCLING OLD IDEAS

It occurred to me recently that the computer industry has been 'borrowing' ideas from the entertainment industry for about 30 years.

If you cast your mind quite a few years you may remember that the music-cassette arrived on the scene around the late 1960s. Most of us have had some sort of love-hate relationship with the cassette ranging from the 'highs' of still having treasured music memories from way back to the 'lows' of having the tape inside the case decide to go 'free range' and wind up somewhere in the innards of the cassette player. Who can forget the curious sight of yards and yards of thin brown tape tangled on road-side fences – I wonder if these were the first instances of 'streaming media'?

Moving ahead to the early 1980s we found that the first publicly-affordable computers including Tandy TRS, Commodore 64 and the Amstrad CPC often used cassette-based 'disk drives' to load and run programs. Some smartie had worked out that the magnetic tape that held musical data in music cassettes could be used to hold program data that controlled computers. In that era the concept of holding information on hard-disk drives was reserved for governments and large businesses with equally large budgets.

Fast-forward to the mid 1990s and we found that the computer industry again borrowed an idea from the music industry by using CDs to hold data for installing operating systems and large programs. I can recall that to install Windows 95 required around 20-plus floppy disks for the installation process but with the advent of the data CD a single disc was all one needed to set up an entire operating system.

*(continued in next column)*

### RECYCLING OLD IDEAS (*continued*)

And so it continued with the conscription of DVDs that could hold more than six (6) times the amount of data of a CD, and then to dual-layer DVDs and finally now to BluRay disks with theoretical capacities of 25GB and 50GB. These capacities are staggering when I think back to the **30 MEGABYTE** hard-drive that was in the first PC that I used in my job as an accounts clerk in the mid-1980s.

Digital cameras have been around for quite a few years and most of you will be aware that the photos you take are usually stored on internal magnetic cards. The most popular type is the Secure Digital or SD card, but some manufacturers opt for the XD or CF style cards. The possibility of using these cards for data storage may not have been in the forefront of your mind but in the last couple of years there has been a major development in computer technology that driven the need for a small high-capacity storage device.

That development is the invention of the tablet computer, a lightweight device that doesn't have room for hard-drives or DVD readers so we are now seeing the MicroSD card gaining popularity as a method of increasing the storage capacity of tablet computers.

Ten years ago the notion that something the size of a finger-nail could hold 32 GB of data or more might have been considered 'science fiction' – now it is a fact of technology.

**Dennis Murray**

### NOT ALL TABLETS ARE THE SAME!

It might sound obvious but from time to time a member will come to OPEN and assume that all our tutors are conversant with the use of Android tablets and iPads.

In reality these devices are quite different from 'mainstream' PCs and laptops in regard to their operating systems. Arrange a booking with an experienced tutor.

### INCREASING TABLET STORAGE CAPACITY WITH MicroSD CARDS.

Depending on the type of tablet computer you purchase the amount of storage 'on board' will be limited.

For example the top of the range **iPads** have a storage capacity of 32 Gigabytes and you'll probably need to spend around \$700 - \$800 to acquire one with that capacity.

**Android tablets** will typically have capacities ranging from 8GB to 16GB.

**Windows 8 tablets** can have as little as 16GB and as much as 128GB but for the latter you will be paying a premium price – possibly \$1400-plus.

As far as I am aware iPads still don't have any in-built USB or MicroSD card slots but you can buy an adaptor that enables external memory devices to be attached.

The majority of budget Android tablets and phones have a MicroSD slot included, and the same applies to Windows 8 tablets and Windows Phones. Insert the MicroSD card and it will be recognised as an extra storage device.



However as I have found from personal experience with my new Nokia Lumia 520 phone there may be some issues in getting the phone to recognise the SD card.

So what would you need the extra storage for?

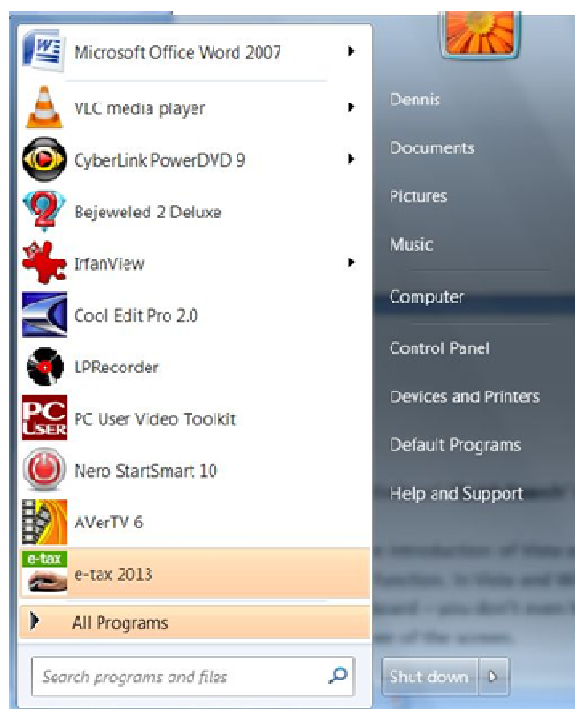
With tablets of all 'breeds' being used as entertainment devices you will obviously need somewhere to store those 100s of songs, YouTube music clips and perhaps even a movie or three.

In my own case I have two 16GB MicroSD cards, one that holds several hundred MP3 songs and some Flash Video music videos, while the other has some movies that I can watch while laying in bed taking it easy after a hard day's work trying to tame computers. Your own storage requirements may be quite different to mine but an extra 16GB or 32GB will give added flexibility when using your tablet.

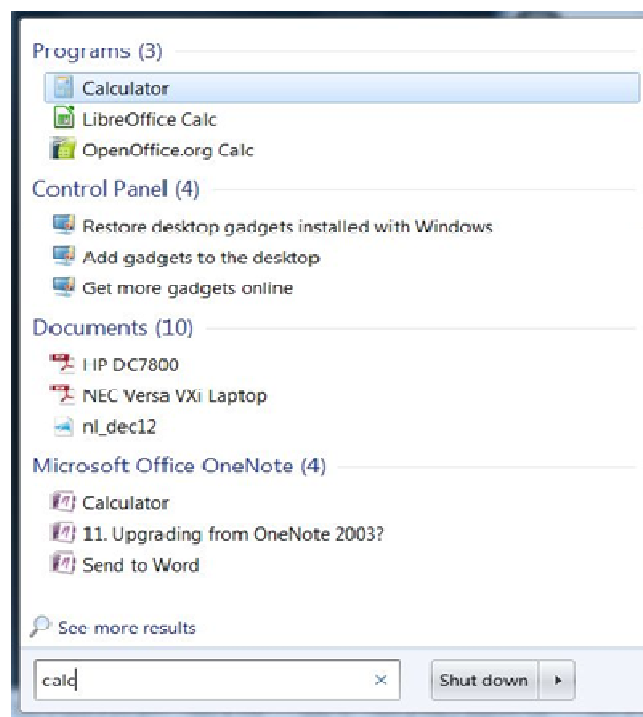
**Dennis**

## USING WINDOWS' 'QUICK SEARCH' FUNCTION WINDOWS VISTA AND WINDOWS 7

Since the introduction of Vista around 2006 the Windows operating system has included a 'quick search' function. In Vista and Windows 7 it is easily accessed by tapping the Windows/Start key on the keyboard – you don't even have to pick up your mouse and click the Start symbol in the bottom left corner of the screen.



## OPEN NEWSLETTER – FEBRUARY 2014



Please turn to the next page to see how to do a Quick Search in Windows 8.

## CONVERT VHS TAPES TO DVD

Reprinted from May 2013

Since the beginning of this year quite a few of our members have become involved with 'capturing' music from their old cassette tapes on to their computers in order to transfer the digital music to CDs or some other music-playing device such as an MP3 player or an iPod.

Similar principles can be applied to capturing video footage from your old VHS tapes so that the resulting digital files can be burned to DVDs.

So what do you need in order to undertake this process?

1. A Video Cassette Recorder to play your tape/tapes.
2. A **capture device** that provides the interface between the VCR and your computer.
3. The correct **video and audio cables** to connect the two together.
4. **Software** that enables the video files to be recorded on to your computer.
5. **TIME!** In most cases VHS Tapes can only be played and recorded in **real time** i.e. a 2-hour tape will take 2 hours to play and record.
6. **Plenty of space** on your computer's hard-drive—**every second** of video you record will occupy **1 Megabyte** on your computer.
7. A suitable **DVD-burning program** to transfer the footage to DVDs
8. In the case of long-running VHS tapes you may need **double-density blank DVDs** to burn the video files. These have a capacity of 8.5 GB
9. **MORE TIME!** The DVD-burning process can be quite time-consuming but the end product is something that easily duplicated for your family and friends.

If sufficient interest is shown we might conduct a special session on this subject later in 2014.

**Dennis**

## OPEN NEWSLETTER FEBRUARY 2014

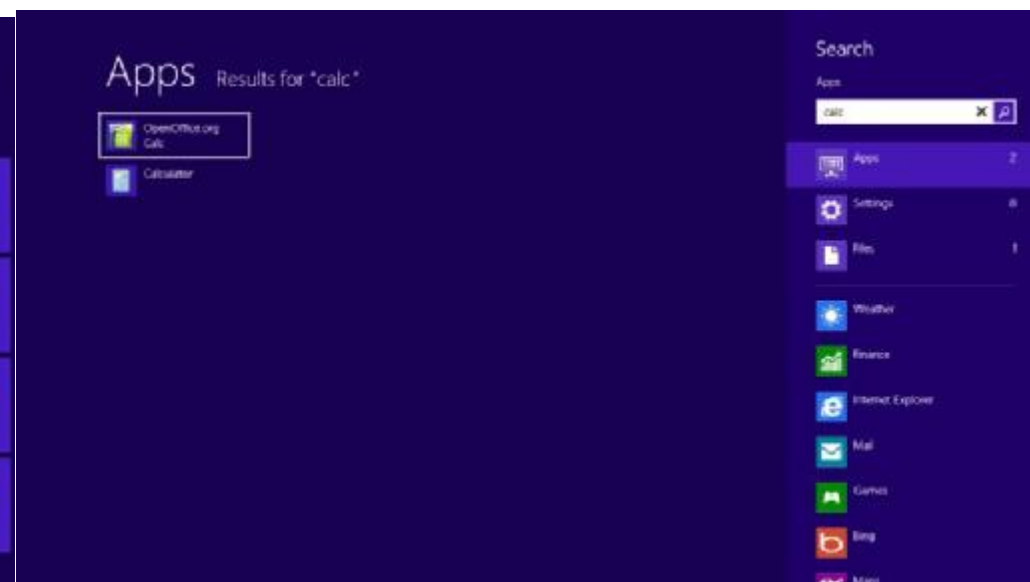
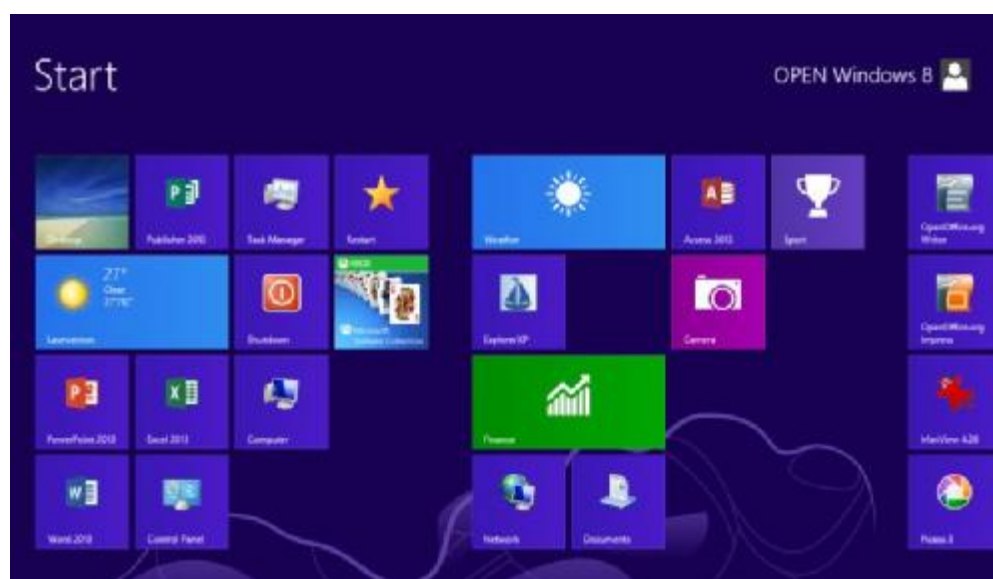
### USING WINDOWS' 'QUICK SEARCH' FUNCTION WINDOWS 8

For Windows 8 it is a little different for keyboard users. Firstly you need to return to the Modern Interface – the screen with those square Tiles on it, shown below :

Then just start typing ... I know it may sound confusing but there isn't a 'search box' to type the letters in to. I've typed those same four letters **calc** with the result being the the right-hand screen-shot shown below :

Clicking on the icon for Calculator would open that program.

If you look really closely at the 'Search' area on the right-hand picture you may note that as well as 'Apps' (i.e. Programs) the Quick Search function also looks for Settings and Files - eagle-eyed readers may see that one File is shown and if we were to click on that area of the screen the name of that file would be displayed ... and it could then be opened.





## PC security after XP's official end of life

On April 8, 2014, Microsoft officially drops support for its venerable operating system. John Foster is undoubtedly one of many Windows Secrets readers thinking through the ramifications of XP's rapidly approaching end of life (EOL).

"After reading all of the articles on XP's EOL, I wonder how vulnerable XP will really be after next April.

"If we keep our browsers up to date, are careful about the websites we visit, and have current anti-malware software running, will we be safe using XP?"

Sorry, no — even with all those precautions, XP still won't be safe. Here's why:

In Microsoft's parlance, "end of life" means that the company will no longer write and issue security patches for XP. Many of those patches fix newly revealed vulnerabilities within the operating system itself. But after XP's EOL, any unpatched security holes will go unfixed. (See Microsoft's explanation; the April EOL also applies to Office 2003.)

You might think that all the major holes in XP have surely been found and patched by now! After all, XP's been out for 12 years.

Sadly, that's purely wishful thinking. As of September's Patch Tuesday, Microsoft had released, just in 2013, more than 80 system-level patches and updates specifically for XP — plus dozens of additional patches for XP-related ancillary software such as Microsoft Security Essentials!

You can see for yourself. Open Windows Update on your XP system and click the Review your update history link (in the window's left column, typically under Options). Note how many new patches there are — even 12 years into the game!

Despite extensive patching, XP is still far from perfect. Given its age and the number of XP systems still in use, the OS will remain an attractive target, possibly for years to come. In other words, when Microsoft stops writing patches for XP, it'll be open season for hackers.

Using good third-party apps and tools such as fully current browsers and anti-malware software will help keep you safe — but only up to a point. They'll do little or nothing to correct fundamental vulnerabilities in the base operating system.

There's also declining third-party support for XP. Few mainstream software vendors will continue investing in a dying market — even if that market is still huge. Moreover, the quantity of tools designed for XP is in sharp decline, a trend that will only accelerate.

There's no way to avoid the inevitable: after next April, XP will be far less safe than any of the more modern Windows versions. XP was truly great, but its day is done.

OK to run multiple always-on security tools?

A comment in the April 4 Top Story, "Microsoft's six free desktop security tools," prompted John to ask this question:

"In the article, you say, '... a PC should run only one real-time, anti-malware/anti-spyware tool at a time.' "I have been using Microsoft Security Essentials (MSE) since you first recommended it. I also use Malwarebytes

(paid version) and SUPERAntiSpyware.

"Is it okay to have those three running together?"

Like MSE, Malwarebytes Pro (site; paid) provides real-time protection. But as a Malwarebytes Product Support Questions page states, the product should be used to supplement other full-time AV tools — it should coexist without conflicts. The free version of Malwarebytes will also run alongside other AV products, but it's active only when you manually launch it.

SUPERAntiSpyware is a whole other thing. I know it's hugely popular, and I recently test-drove it again on multiple versions of Windows for last week's Top Story, "A dozen tools for removing almost any malware." But for several reasons, I decided to omit the product from the article.

For one thing, parts of its nomenclature seemed misleading. For example, the "SUPERAntiSpyware Portable Scanner Personal Edition" doesn't really fit the common definition of a portable app. It's a renamed .exe file that must be installed and run like other common Windows programs. I quickly lose confidence in products that claim something (e.g., portability) they don't have. (The SUPERAntiSpyware site suggests the app is "portable" because it has all the latest virus definitions when you download it. So you don't need an active Internet connection to run it.)

SUPERAntiSpyware also didn't uninstall cleanly. This is 2013! Surely any decent Windows-based app or utility ought to remove itself fully when you uninstall it.

I can't speak to SUPERAntiSpyware's effectiveness. The red flags mentioned above caused me to put it aside. The anti-malware product category has many great tools — some mentioned in last week's Top Story. So why

waste time on apps that seem to have obvious flaws and/or drawbacks?

That said, if the three AV tools you're using appear to be working, then great! You're probably well protected. (But I'm guessing that Microsoft Security Essentials and Malwarebytes are doing most of the heavy lifting.)

Bottom line: You can run a second full-time scanner (such as Malwarebytes Pro) if it's specifically designed to work with other full-time scanners.

Using multiple layers of security — an update Bob, a long-time reader, sent in this plea:

"Over the years, you've commented on the use of multiple layers of security. But I often see news stories about computer crackers recovering data and emails from computers. Once, when I was sick, anyone could have entered my office and snooped for days.

"What can I use to protect against snoops accessing my programs and data? Help!"

Good timing, Bob; I was thinking about this just the other day! It was back in the 1990s that I first recommended using multilayered defenses for PC security. I updated that advice in the early 2000s and again a few years later. It's time to revisit the concept — and to update the advice.

Today, complete PC protection means guarding against two different types of attacks: remote and local. Let's discuss each in turn.

Protecting your PC against outside threats: The vast majority of computer breaches now occur over the Internet. There are stories every day about

*(Continued from page 10)*

hackers successfully compromising some company's computers. But everyone using the Net should be concerned about remote attacks, most of which are launched by malware (a virus, worm, Trojan, etc.) delivered to PCs via malicious sites or emails.

Protection from these threats requires four primary layers of defense:

**Firewalls:** No firewall is perfect, but a good one prevents external snoops from finding and accessing your PC via the Web. (See the March 11, 2010, LangaList Plus, "Let's put your firewall to the test.")

The firewalls built into Win7 and Win8 are effective; I run them on my systems, using their default settings with no special tweaks. Both are, however, highly customizable and configurable, as described in the March 17, 2011, LangaList Plus, "Outbound blocking for Windows Firewall."

Vista's built-in firewall is somewhat inferior to Win7's, but it's still adequate. Windows XP's firewall is based on decade-old technology and is relatively weak — able to defeat only the most blatant kinds of external attacks. For that reason, I recommend using a third-party firewall with XP (and with Vista, too, if you need strong security). There are many good third-party firewalls — any Web search will turn up a dozen or more — but a favorite among Windows Secrets readers is Comodo (site; free and pro versions available).

**Always-on anti-malware apps:** The better anti-malware tools constantly guard against the delivery and activation of malicious software, regardless of the attack vector — browser, email, infected document, or whatnot.

You'll find some anti-malware-tool comparisons in the Feb. 16, 2012, Top Story, "Is your free AV tool a 'resource pig?'" I use the free Microsoft Secu-

rity Essentials (MSE; site), but it's not for everyone and there's some debate over its effectiveness. (For more on this, look up the Dec. 20, 2012, LangaList Plus.)

**On-demand anti-malware scans:** Because even the best firewall/anti-malware software defenses can fail, it's good practice to verify that your system is infection-free by routinely running one or more standalone security tools — for example, ESET's Online Scanner (site), Microsoft's Safety Scanner (site), or Trend Micro's HouseCall (site).

**Common sense:** Malware doesn't teleport itself into your PC; most Windows infections are allowed in when users are enticed or tricked into clicking phony links in websites or phishing email — or fall for a bogus "You're infected!" popup. You can avoid all these infection vectors with a little care, common sense, and skepticism. For more on this, see the Dec. 20, 2012, LangaList Plus.

**Protecting against local/physical treats:** Obviously, stealing your data is easier if someone has direct access to your PC. They can, for example, download sensitive information to a thumbdrive by simply using your keyboard — or walk off with the entire system (or at least the hard drive)! And if they possess your PC, they can take all the time they need to methodically analyze and access your data. (If your office is not secure, consider buying cable locks for your systems.)

By the way, if your defenses against external attacks fail and the hacker installs remote-control malware, it's effectively the same as if they're sitting at your keyboard.

The best defenses against local attacks are these:

**User-account passwords:** Windows' user-account passwords don't provide

*(Continued on page 12)*

heavy-duty security, but they're better than nothing. Your user password will at least foil casual snoops and nosy coworkers. Every version of Windows allows the use of sign-in passwords; use them — even at home.

**Hardware-level passwords:** PCs often provide stronger, hardware-level password protection that's independent of the operating system and managed typically with the PC's BIOS or Unified Extensible Firmware Interface (UEFI) settings. This type of password protects the entire system (not just the OS) from unauthorized use by anyone who has physical access to your machine.

Almost all PCs let you set a primary, hardware-level, system password. You're asked for this password when your PC first powers on (or resumes after hibernation or deep-sleep mode) and before any OS loads — whether it's installed on the hard drive or booted via external media. You must enter the correct password before the system lets the OS boot or resume. Not only will system-level passwords foil casual or hurried snoops, they can impede even professional data thieves.

Some systems — especially portable PCs — also provide a secondary, hardware-level, power-on password for the hard drive(s). If a hacker gets past the primary password and boots the system from a floppy, CD, or USB drive, he still won't be able to access data on the hard drive. When this password is handled by the hard drive itself, a thief is (in theory) locked out of the drive, even if it's physically removed from your PC and placed into another system. This type of password is extremely difficult to bypass, even for pros.

The simplest way to tell which hardware-level password options your PC supports is to explore its BIOS/UEFI settings. Reboot and watch the screen for a line of text that says something like Press to enter BIOS setup. (Instead of "F2," it might say F1, DEL, ESC, F10, or some other key.) Press whatever key is indicated, and you'll enter the system setup pages.

Look for a page or tab labeled Security — or for something similar. Select it, and you should see options for setting a master Administrator or Supervisor password plus a separate User password. The Administrator or Supervisor password is more secure because it locks the entire PC (including BIOS access).

If your system supports hard-drive locking, you'll also see an option for setting passwords for the system's hard drives — often referred to as HDD0, HDD1, and so on.

Figure 5 shows a fairly typical system BIOS that lets you set Administrator/Supervisor or User passwords, set separate passwords for accessing either of two hard drives, and enable a "Password on boot" option, which prevents startup if an incorrect password is entered. Figure 6 shows a typical system-level, startup-password dialog box.

BIOS password settings Figure 5. Settings like these (circled in yellow) add hardware-level password protection to your PC and its hard drives.

Hardware-based password sign-in Figure 6. Once the BIOS-level password(s) is/are set, the correct password(s) must be entered into a power-on dialog box similar to this one — otherwise the PC won't boot, you can't enter the BIOS, and no software will run.

Encryption: Scrambling all the data on your hard drive (or at least scrambling your most sensitive data) offers excellent protection against even the most determined, professional-level snoops, no matter how they access your system — via local access, remote hacking, or malware.

On my systems, for example, I compress and scramble all my tax, financial, health-related, and similarly sensitive folders with the 256-bit Advanced

*(Continued on page 13)*

Encryption Standard (AES) option built into the free 7-Zip tool (site). AES-256 is currently regarded as uncrackable — in any practical sense of the word. (For more on AES, see the related Wikipedia article.)

I protect those encrypted folders with different, complex, non-obvious passwords. I don't try to remember all the passwords myself. Instead, I safely store all my passwords (including those used by 7-Zip) in RoboForm (U.S. \$9.95 the first year, \$20 thereafter; site), which uses its own 256-bit AES encryption. I just have to remember only one long, complex password (my RoboForm master password); the utility remembers all the rest for me. It also automatically fills in saved passwords on demand.

Thus, in the unlikely event someone stole my PC or its hard drive and managed to get past all the aforementioned security layers, they'd still have to crack my encryption to access my most personal, sensitive data.

There are other tools besides 7-Zip and RoboForm, of course; those just happen to be the ones I use. Two popular — and free — alternatives are TrueCrypt (site) and KeePass Password Safe (site), but a Web search will turn up many others. For more information and alternatives, including whole-disk encryption options, see the section of the Sept. 13, 2012, Top Story, titled "SAFE, step one: Encrypting all sensitive data."

Some versions of Windows offer built-in file and folder encryption; others support Microsoft's BitLocker whole-disk encryption. But there are limitations and problems with these, as explained in that same Sept. 13 Top Story — see the sections titled "Windows' built-in encryption-tool limitations" and "Windows' BitLocker offers whole-disk encryption."

As safe as can reasonably be achieved: And there you have it: an up-to-date, highly secure, multilayered approach to PC security that will protect

you against just about any form of attack, whether it's remote or local, electronic or physical.

Bottom line: No single security strategy can protect you from today's sophisticated threats. Safe computing requires the combined efforts of a fire-wall, always-on anti-malware, on-demand anti-malware scans, and some common sense in how you use your PC. A truly secure PC also requires multiple layers of passwords and data encryption. You have a lot of security options. Protecting your data is really up to you.



**"There are better ways to log off."**