Computers and Stuff.

Sam Houliston.

New computer virus causes havoc.

A powerful new computer virus has been causing havoc with e-mail systems on computers running Microsoft Windows – right across the world.

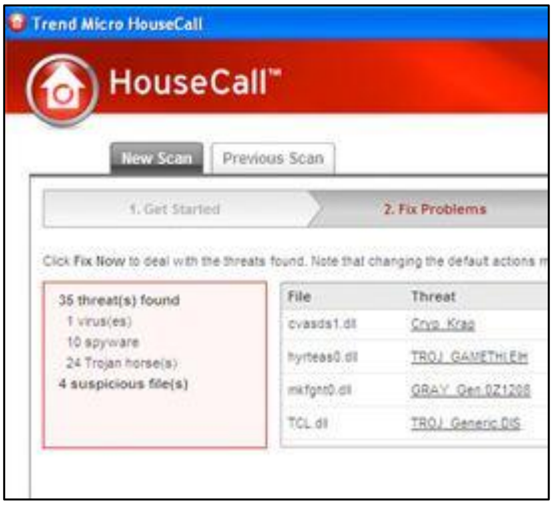
Experts described the virus, called Goner, as one of the fastest-spreading they had yet seen and warned computer users (Windows) to immediately delete it if they received it. It spreads with tremendous speed and thousands of users across the world have already been infected.

The virus mass mails itself out through e-mail by grabbing all your addresses in your address book and re-sends the mail in which you received the virus to all those addresses. These processes are repeated over and over again very swiftly and before long millions of computers are infected. It also attempts to destroy any anti-virus software on your computer.

The infected e-mail has the word "Hi" as its subject and the body text reads something like "You won't believe this" followed by a link.

It was first detected a few weeks ago in the US but experts believe it was created somewhere in Europe. The US, the UK and France were the worst hit but it caused havoc in Australia as well.

A criminal investigation has been launched in an effort to track down the person responsible for the virus – good luck we say!!.



Click Fix Now to deal with the threats found. Note that changing the default actions m

35 threat(s) found
1 virus(es)
10 spyware
24 Trojan horse(s)
4 suspicious file(s)

File	Threat
cvasds1.dll	Cryp_Krag
hyrteas0.dll	TROJ_GAMETHI.EH
mkfgnt0.dll	GRAY_Gen.0Z1208
TCL.dll	TROJ_Generic.DIS

Unfortunately, the Radschool computers got mixed up in it too and a lot of you were sent an infected email before we realized what was happening and pulled the computers off line. We keep our anti-virus software up to date but it still got through, probably before the anti-virus people has time to write a 'block' for it - though you can bet they all have now.

Once our machines were cleaned up we sent out an email advising you of the problem and suggesting you use our favourite "fix" – Trend HouseCall. If/when you receive a virus or Trojan, it is no good running your anti-virus software to try and get rid of it – this is because if the virus has got though, you can bet the bank it has also negated your software which will look at the virus and think it is a legit file. An up to date anti-virus program will normally stop most viruses getting through, but for those that do, you need to use an independent un-affected program.

We've been using Trend HouseCall for some years and find it an excellent fix. It is not an anti-virus program, it doesn't sit in the background and check each file coming in but instead will check every file already on your computer and remove those that are infected. The big difference with these programs and the anti-virus program that sits on your computer is this: to use them, you have to download or run them from the developer's site which means they are clean and unaffected.

There are a number of these free to use programs around, such as Microsoft's "Malicious Software Removal Tool" but HouseCall is good, it is quick and it too is FREE to use.

It's probably a good idea to run it every now and then – you will find a link to it on our Links page.

Paddy took 2 stuffed dogs to Antiques Roadshow " Ooh!" said the presenter, "This is a very rare set, produced by the celebrated Johns Brothers taxidermists who operated in London at the turn of the last century. Do you have any idea what they would fetch if they were in good condition?"

"Sticks?" said Paddy.

Anti-Virus software.

Anyone who has a Windows PC and who uses the internet will have some sort of anti-virus software on their machine, if they don't, well, they are just asking for trouble – big big trouble.

But!! How does Anti-virus software work??

There are two types of antivirus program. These programs are powerful pieces of software and are essential on any computer running Windows.

On-Access Scanning.

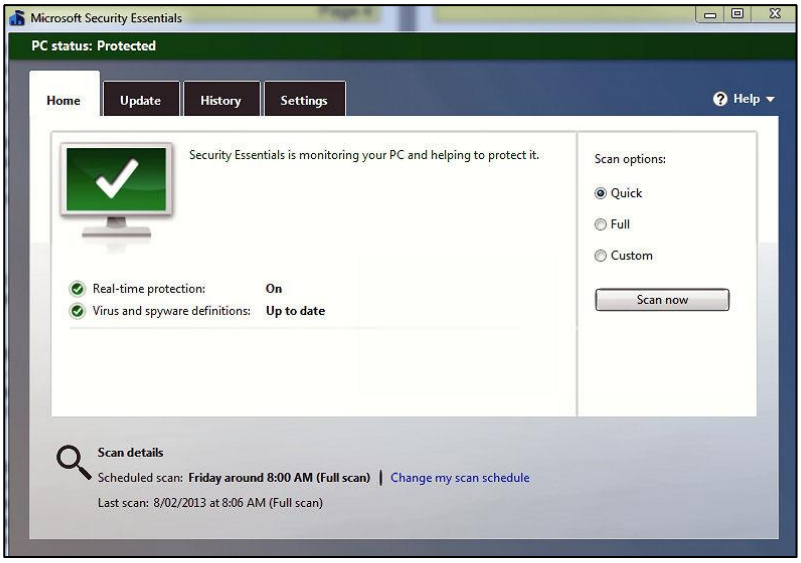
This type runs in the background on your computer, checking every file you open and is also called background scanning, resident scanning, real-time protection, or something else, depending on your antivirus program. When you double-click an EXE file, it may seem like the program launches immediately – but it doesn't. Your antivirus software checks the program first, comparing it to known viruses, worms, and other types of malware. Your antivirus software also does "heuristic" checking, checking programs for types of bad behaviour that may indicate a new, unknown virus.

Antivirus programs also scan other types of files that can contain viruses. For example, a .zip archive file may contain compressed viruses, or a Word document can contain a malicious macro. Files are scanned whenever they're used, if you download an EXE file, it will be scanned immediately, before you even open it.

It's possible to use an antivirus program without on-access scanning, but this generally isn't a good idea as viruses that exploit security holes in programs wouldn't be caught by the scanner. After a virus has infected your system, it's much harder to remove. (It's also hard to be sure that the malware has ever been completely removed.)

Full System Scans.

Because of the on-access scanning, it isn't usually necessary to run full-system scans. If you download a virus to your computer, your antivirus program will notice immediately – you don't have to manually initiate a scan first.



PC status: Protected

Security Essentials is monitoring your PC and helping to protect it.

Real-time protection: On

Virus and spyware definitions: Up to date

Scan options:

● Quick

○ Full

○ Custom

Scan details

Scheduled scan: Friday around 8:00 AM (Full scan) | Change my scan schedule

Last scan: 8/02/2013 at 8:06 AM (Full scan)

Full-system scans can be useful for some things, however. A full system scan is helpful when you've just installed an antivirus program – it ensures there are no viruses lying dormant on your computer. Most antivirus programs set up scheduled full system scans, often once a week. This ensures that the latest virus definition files are used to scan your system for dormant viruses.

Full disk scans can also be helpful when repairing a computer. If you want to repair an already-infected computer, inserting its hard drive in another computer and performing a full-system scan for viruses (if not doing a complete reinstall of Windows) is useful. However, you don't usually have to run full system scans yourself when an antivirus program is already protecting you – it's always scanning in the background and doing its own, regular, full-system scans.

Virus Definitions.

Your antivirus software relies on virus definitions to detect malware. That's why it automatically downloads new, updated definition files – once a day or even more often. The definition files contain signatures for viruses and other malware that have been encountered in the wild. When an antivirus program scans a file and notices that the file matches a known piece of malware, the antivirus program stops the file from running, putting it into "quarantine." Depending on your antivirus program's settings, the antivirus program may automatically delete the file or you may be able to allow the file to run anyway, if you're confident that it's a false-positive.

Antivirus companies have to continually keep up-to-date with the latest pieces of malware, releasing definition updates that ensure the malware is caught by their programs. Antivirus labs use a variety of tools to disassemble viruses, run them in sandboxes, and release timely updates that ensure users are protected from the new piece of malware.

Heuristics.

Antivirus programs also employ heuristics. Heuristics allow an antivirus program to identify new or modified types of malware, even without virus definition files. For example, if an antivirus program notices that a program running on your system is trying to open every EXE file on your system, infecting it by writing a copy of the original program into it, the antivirus program can detect this program as a new, unknown type of virus.

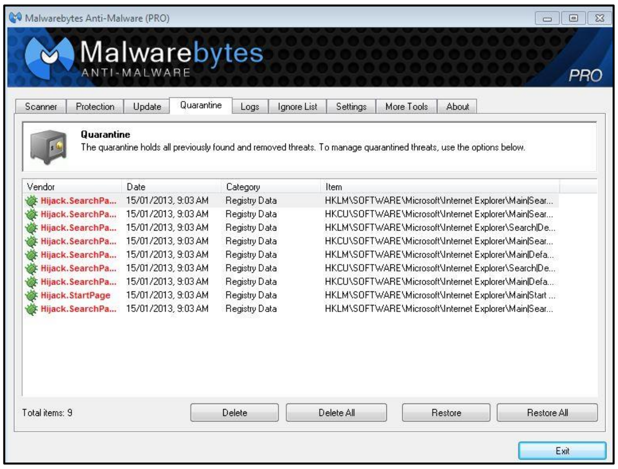
No antivirus program is perfect. Heuristics can't be too aggressive or they'll flag legitimate software as viruses.

False Positives.

Because of the large amount of software out there, it's possible that antivirus programs may occasionally say a file is a virus when it's actually a completely safe file. This is known as a "false positive." Occasionally, antivirus companies even make mistakes such as identifying Windows system files, popular third-party programs, or their own antivirus program files as viruses. These false positives can damage users' systems – such mistakes generally end up in the news, as when Microsoft Security Essentials identified Google Chrome as a virus, AVG damaged 64-bit versions of Windows 7, or Sophos identified itself as malware. Heuristics can also increase the rate of false positives. An antivirus may notice that a program is behaving similarly to a malicious program and identify it as a virus.

Despite this, false positives are fairly rare in normal use. If your antivirus says a file is malicious, you should generally believe it. If you're not sure whether a file is actually a virus, you can try uploading it to VirusTotal (which is now owned by Google). VirusTotal scans the file with a variety of different antivirus products and tells you what each one says about it.

Detection Rates.



Quarantine
The quarantine holds all previously found and removed threats. To manage quarantined threats, use the options below.

Vendor	Date	Category	Item
Hijack.SearchPa...	15/01/2013, 9:03 AM	Registry Data	HKLM\SOFTWARE\Microsoft\Internet Explorer\Main|Sear...
Hijack.SearchPa...	15/01/2013, 9:03 AM	Registry Data	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main|Sear...
Hijack.SearchPa...	15/01/2013, 9:03 AM	Registry Data	HKLM\SOFTWARE\Microsoft\Internet Explorer\Search|De...
Hijack.SearchPa...	15/01/2013, 9:03 AM	Registry Data	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main|Sear...
Hijack.SearchPa...	15/01/2013, 9:03 AM	Registry Data	HKLM\SOFTWARE\Microsoft\Internet Explorer\Main|Defa...
Hijack.SearchPa...	15/01/2013, 9:03 AM	Registry Data	HKCU\SOFTWARE\Microsoft\Internet Explorer\Search|De...
Hijack.SearchPa...	15/01/2013, 9:03 AM	Registry Data	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main|Defa...
Hijack.StartPage	15/01/2013, 9:03 AM	Registry Data	HKLM\SOFTWARE\Microsoft\Internet Explorer\Main|Start ...
Hijack.SearchPa...	15/01/2013, 9:03 AM	Registry Data	HKLM\SOFTWARE\Microsoft\Internet Explorer\Main|Sear...

Total items: 9

Different antivirus programs have different detection rates, which both virus definitions and heuristics are involved in. Some antivirus companies may have more effective heuristics and release more virus definitions than their competitors, resulting in a higher detection rate.

Some organizations do regular tests of antivirus programs in comparison to each other, comparing their detection rates in real-world use. AV-Comparitives regularly releases studies that compare the current state of antivirus detection rates. The detection rates tend to fluctuate over time – there's no one best product that's consistently on top. If you're really looking to see just how effective an antivirus program is and which are the best out there, detection rate studies are the place to look.

Testing an Antivirus Program.

If you ever want to test whether an antivirus program is working properly, you can use the EICAR test file. The EICAR file is a standard way to test antivirus programs – it isn't actually dangerous, but antivirus programs behave as if it's dangerous, identifying it as a virus. This allows you to test antivirus program responses without using a live virus.

Torrents.

These days millions of people are downloading music and movies "illegally" using a Torrent, (also called a BitTorrent) - but what is a Torrent?

A Torrent is a "system" that allows you to very quickly copy large files, via the internet, from someone else's computer to yours. It does it by copying bits of the file from as many computers as it can, crunching all the bits together and putting the completed file on your machine. It's called "swarming and tracking".

It works like this.

Let's assume you want to get a copy of a movie. You open your search Torrent (there are lots of them, THIS one is good) and in the search window you type the name of the movie (or song) you want. The Torrent then searches all the computers on the Internet that also have a Torrent installed and shows you a list of possible copies. Some could be DVD quality, some Blue Ray, some copies taken from the TV, you select the one you want. You then tell the Torrent to download the movie (or song) and it grabs chunks of the file from as many computers as it can and a 'torrent' of data starts coming into your machine. When all the data has been downloaded, the Torrent puts it all together and voila, you have your movie.

It all started back in 2001 when a bloke named Bram Cohen wrote and released the first Torrent program. Today, it has been estimated that the at least a quarter of a billion people are using a Torrent each month – and at any given moment, there are more people using a Torrent than are using YouTube and Facebook combined. It's called P2P (peer to peer) file sharing.

It is now the primary means to trade software, music, movies, and digital books online and although Torrents are extremely unpopular with the film, music and other media producers they are much loved by millions of people across the planet.

Because torrents strive to screen out dummy and corrupt files, are mostly free of adware/spyware and achieve amazing download speeds, torrent popularity is still growing fast and by straight gigabytes of bandwidth used, Torrent networking is the most popular activity on the Internet today.

However, you have to be careful, there is an extremely good chance that by downloading a file form someone else's computer you could be downloading a nasty virus – if you do use a Torrent – be very very careful.

And – as you could be violating a copyright law, you could be sued for downloading a movie or song - be very very careful.

HDMI Cables.

CNET

HDMI cables are an excellent way to connect your TV to a media source, with HDMI you get sound and picture all in the one cable and as everyone knows, wives hate cables so using the one HDMI cable instead of separate RCA cables makes for a happy household – and what more could you ask for. But!! - as anyone who has bought a HDMI cable recently knows, there are huge differences in price out there, with a typical 2 metre cable ranging in price from $15 at the bottom of the range to $200 at the top.

So, what's the difference??

We don't reckon there is one – a cheap $15 cable will produce the exact same picture and sound quality as a $200 one.

HDMI cables come in 4 different varieties,

- High speed with Ethernet
- High speed without Ethernet
- Standard speed with Ethernet
- Standard speed without Ethernet

Forget standard speed cables as they cannot handle the definition you want, but today, the vast majority of cables sold are high-speed anyway and very few "black boxes" have Ethernet-over-HDMI compatibility, so you don't need to pay extra for that feature in the cable either.

And you can forget all that mumbo jumbo the sales people will tell you, there is no such thing as an "HDMI 1.4" cable, nor do you need a special cable for 3D, 120 or 240Hz, or Audio Return Channel (ARC) but cable length is a bit of a killer, you shouldn't use an HDMI cable much longer than 3 metres. If you need to go longer you should use an active cable, these (obviously) cost a bit more than a 3 metre cable but if length is your thing, go active.

If you’re happy buying stuff on the Internet, you could try this site http://www.monoprice.com/, apart from a lot of other things, they have an excellent range of cables, are cheap and as the dollar is high, are good value.

Buy inexpensive high-speed HDMI cables. Online is cheaper by far and will be available in whatever length you need. Only buy from a physical store if you absolutely have to, and if you do, certain stores do better than others. At the very least, if you're in a bind, check the Web sites of the various stores in your area. They'll at least give you an idea which store offers the best in-store price.

The things that come to those who wait, may be the things left by those, who got there first.

Computer.

A Spanish Teacher was explaining to her class that in Spanish, unlike English, nouns are designated as either masculine or feminine. 'House' for instance, is feminine: 'la casa.' 'Pencil,' however, is masculine: 'el lapiz.'

A student asked, 'What gender is 'computer'?'

Instead of giving the answer, the teacher split the class into two groups, male and female, and asked them to decide for themselves whether computer' should be a masculine or a feminine noun. Each group was asked to give four reasons for its recommendation.

The men's group decided that 'computer' should definitely be of the feminine gender ('la computadora'), because:

1. No one but their creator understands their internal logic;
2. The native language they use to communicate with other computers is incomprehensible to everyone else;
3. Even the smallest mistakes are stored in long term memory for possible later retrieval; and
4. As soon as you make a commitment to one, you find yourself spending half your pay on accessories for it.

The women's group, however, concluded that computers should be Masculine ('el computador'), because:

1. In order to do anything with them, you have to turn them on;
2. They have a lot of data but still can't think for themselves;
3. They are supposed to help you solve problems, but half the time they ARE the problem; and

4. As soon as you commit to one, you realize that if you had waited a little longer, you could have gotten a better model.

The women won.

Let your PC start the New Year right!

A little time spent now on preventive maintenance can save hours of PC troubleshooting later — and provide better computing all year long.

Windows Secrets
Everything Microsoft forgot to mention.

Use the following steps to give your PC (running Windows) an annual check-up — and ensure it starts 2013 as healthy as possible.

Consider what your PC has been through in the past 12 months: Windows Update added dozens of patches to your operating system; you've likely installed some new third-party software, uninstalled other programs and upgraded or patched apps and utilities. You've probably altered, tuned, and tweaked various aspects of your system's user interface and software settings and you've undoubtedly created and deleted myriad new emails, documents, photos, MP3s, videos, spread sheets, and such.

All during that time, your hard drive spun hundreds of millions of revolutions and the system fans rotated for hundreds of hours. Heat, dust, and chemical degradation did their inevitable damage, reducing the remaining physical life of your system's components. In short, just as we're a year older, our PCs are not the same machines they were a year ago.

To ensure your system runs smoothly for another year, now's a good time to perform some extra maintenance. It'll help prevent new errors from piling on old ones and keep your system fundamentally sound.

Preserve and protect system data.

As with all significant changes to a PC, start any serious system maintenance with a full system backup — if anything goes bung, you can recover quickly. (You should regularly back up anyway, it is good insurance against all manner of ills that might bring down a PC, power spikes, hard-drive crashes, malware infestations, cockpit error, and many other calamities.)

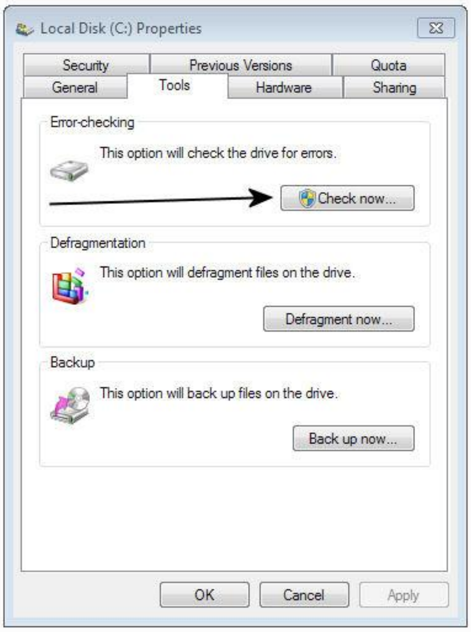
All current versions of Windows provide the means to make reliable backups, though each new generation of the OS has added enhancements to its archiving capabilities

Check the hard drive's physical/logical health.

Traditional hard drives are possibly the hardest-working components in PCs. Their spinning platters can rack up hundreds of millions of rotations per year, and their read/write heads chatter back and forth millions of times, moving chunks of files in astronomical quantities. It's a testament to hard-drive technology that they work as well, as long, and as reliably as they do. But as sure as death and taxes, all drives eventually wear out. Take a few minutes to check your drive's physical health via the Self-Monitoring, Analysis, and Reporting Technology (aka SMART) subsystem built into most current hard drives. You can do that HERE.

Although SMART tools monitor the ***physical*** health of drives, Windows' built-in tools check on the ***logical*** health of the files on the drive.

Every version of Windows, from XP on, has **CHKDSK** (as in "check disk") for exactly that purpose. The basic version of **CHKDSK** is a simple point-and-click operation. In Windows Explorer, right-click the drive that you want to check and select Properties.



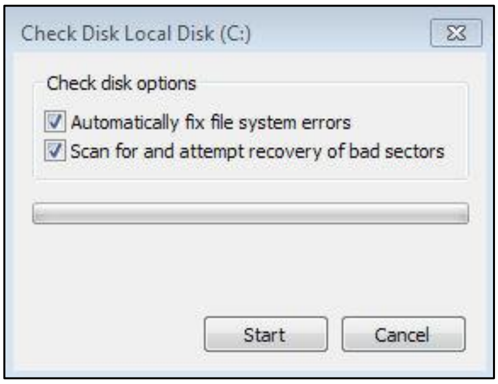
This option will check the drive for errors.

This option will defragment files on the drive.

This option will back up files on the drive.

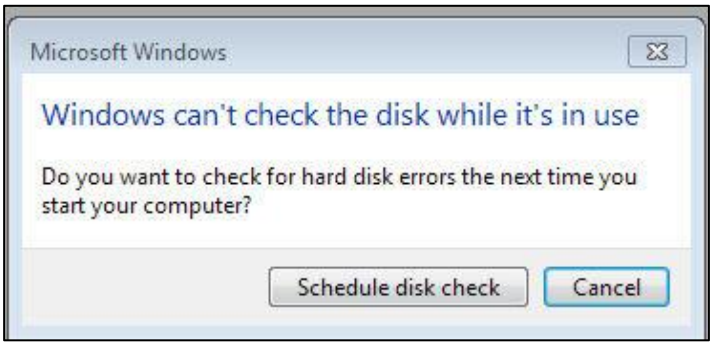
Click the Tools tab and then, under Error-checking, click the **Check now** button (arrow right).

You will then be offered the option (left) of selecting whether to fix any errors and/or to try and recover any bad sectors, select both.



☑ Automatically fix file system errors
☑ Scan for and attempt recovery of bad sectors

If the drive you wish to check is the one which you are using, **CHKDSK** will not be able to do its magic until you log off, it will offer you the opportunity to schedule a check next time you start your computer, if it does, click **Schedule disk check.** Then next time you start your computer, Windows will run CHKDSK before starting up.



Windows can't check the disk while it's in use

Do you want to check for hard disk errors the next time you start your computer?

If you've got two hard drives on your machine, (say Drive C [main] and Drive D) and you want to do a check on drive D, Windows will go straight into **CHKDSK** and check drive D without requiring a restart.

Patch and update all software and the OS.

Next step is to make sure all software updates are installed — especially security-related patches! Start by opening Windows Update and clicking **Check for updates,** then review the list of patches Microsoft wants installed. (Not all Windows patches are necessary.)

If you're using XP, Vista and Win7, start by opening the Control Panel, in XP, click on ***Automatic Updates***, in Vista and Win7, click ***Windows Update***.

If you need help with Windows Update, Microsoft has more info for XP, Vista/Win7, and Win8.

With Windows fully up to date, it's time to check your other software. Most applications let you check for updates manually via menu options such as Help, Help/About, or Help/Update.

Do a thorough review of your PC's defences.

Passwords: As PCs have become more powerful, passwords that were once virtually uncrackable might now fall to various free, easily used, and surprisingly fast hacker tools. Verify that your most important passwords are still secure by testing them (or a variant of them) on any of the many good password-checking sites, such as:

- How secure is my password?
- Gibson Research Corporation's How big is your haystack?
- Password Meter
- Microsoft PC Security page

Firewall: Put your firewall through its paces to ensure that your PC is not visible or potentially accessible to Internet-based hackers. The following sites offer free, easy-to-use, firewall-testing tools and services.

- HackerWatch Probe
- SecurityMetrics' Port Scan
- Gibson Research Corporation's ShieldsUP

Antivirus: As we've discussed earlier, your anti-virus software is very important if you use the internet – but it's no good if it is not regularly updated, you should check it every day. Verify that your system is free of worms, viruses, Trojans, and other malware by running a full scan with a standalone security tool such as Trend Micro's HouseCall (site), ESET's Online Scanner (site) or Microsoft's Safety Scanner (site).

Wi-Fi Router: Many current Wi-Fi routers contain a flaw in their implementation of ***Wi-Fi Protected Setup*** (WPS). Hackers might easily breach your Wi-Fi defences, regardless of what encryption and password you use. Click HERE to see how to check if your router is affected and and what to do if it is.

Take out *all* the rubbish accumulated in Windows.

Windows is something of a packrat (as are most PC users when it comes to their systems), it can accumulate truly astounding amounts of digital debris, including temporary files that sometimes become all too permanent. Fortunately, there are many excellent disk-clean-up tools available. Windows' own **cleanmgr** is one — if you know how to access its hidden settings. If you want to know how it use it, see HERE.

One clean-up tool that we use and which we've spoken about previously is CCleaner. There are 3 versions of CCleaner available these days, one of which is still free and we think it takes a lot of beating. You can get a copy HERE.

Defrag (or optimize) data on hard disks.

A major hard-drive clean-up often results in ***fragmentation*** — files and pieces of files scattered across the hard drive that can waste drive space. Defragmenting can improve drive performance on all spinning-platter drives, but it's not needed (or wanted) on solid-state drives. Microsoft has online instructions for using the Windows disk defragmenter tool in XP, Vista, and Win7 though if you're using Windows 7 or 8, you needed bother and these systems schedule their own defrag.

Once your system is updated, cleaned, defragged, and otherwise optimized, make a new full backup or system image to preserve your new setup. This way, if anything goes wrong in the coming months, you'll be able to return your PC to its fully cleaned and optimized condition in just a few clicks.

Physical clean up.

We think of our PCs as electronic devices — and they are — but they're also mechanical systems. Most PCs have cooling fans that constantly draw in room air. Over time, the inside of your PC can become astonishingly choked with dust, resulting in poor air flow, higher temperatures, and shorter component life.

Most motherboards, CPUs, and hard drives have temperature sensors built in, but oddly, most operating systems largely ignore them. However, there is a handy little program that you can download for free that will keep an eye on things and let you know if the temps inside your computer are a bit high, It's called SpeedFan and you can get it HERE. Look under the Download section and click the Speedfan (x.xx) link.

The 50-50-90 rule:
Anytime you have a 50-50 chance of getting something right, there's a 90% probability you'll get it wrong.

The "cheap" iPhone.

It has been reported that apple will release a cheap iPhone in the second half of 2013. It isn't the first time this report has surfaced as speculation has been rampant for months that Apple would soon roll out a low-cost iPhone aimed primarily at the emerging markets. The iPhone market is very volatile and very robust, Google gives away its Android operating system for free and lets many hardware makers use it to power their devices which means there are many different Android handsets available at a variety of price points.

The cheaper Android-powered phones have appealed to consumers in emerging markets, who simply lack the purchasing power to afford Apple's iPhone. Even though the iPhone is wildly popular in the U.S., it has a paltry share of the global market, with Android commanding a solid 70+ percent.

Like the mini iPad, a cheaper iPhone might simply be a strategy Apple undertakes to protect its operating system. The more people use iOS, the more attractive it is for app developers to code for it. The more apps iOS has, the more attractive the devices are to users – elementary!!

Despite the lower price point, it is also claimed that the cheaper iPhone will have a larger screen, following the trend pioneered by Samsung and other Android makers. For Apple investors, the question will be one of margin: How much, if at all, will a cheap iPhone reduce Apple's margins?

For Apple consumers, it will be of availability: Will this cheaper iPhone make its way to Australia, perhaps as an option for those who stay on prepaid mobile plans? And, if the device is sporting a larger screen, does this mean that the next version of the flagship iPhone will as well?

Time will tell!!

If you want to test your memory,
try to recall what you were worrying about one year ago today…

Some tips!

A while ago my work PC was running very slowly. The problem was a large amount of data in the form of big zip files which I was using as point-in-time backups. My antivirus program was scanning these files, which is a lot of effort since it was effectively unzipping them before scanning. End result was that by the time it finished the scheduled scan that I couldn't avoid, it was just about time for the next one. Moving these big zip files (at least the ones I still wanted) to an external hard drive and then removing the external drive from the computer made a huge difference.

So – if you have large zip files on your computer, it is a good idea to move them onto a removal drive and then disconnect it from your computer, that way your anti-virus program can and will do its scan more quickly and your computer will not bog now and will run faster.

MS-WORD

One of the annoying things about MS-Word is that when you reopen a document you've been working on, it opens at the top of the document. Unlike Excel, which takes you to the spot where you left off last time, Word's short-term memory always wants to start you off at the beginning again. You can work around this if you press [Shift][F5] as soon as the document opens. [Shift][F5] is the Go Back shortcut, which cycles you between your four most recent edits during a Word session. But if you can remember to hit it immediately after opening a document, Word will jump to the last thing you changed before saving and closing that doc.