

NATGUG News January February 2007

Editorial

The first thing I have to publish is the date of the next Swindon Meeting, that will be on the 9th 10th & 11th March 2007.

Well I'm sorry I have been busy again and not until now had time to write the editorial and produce a Natgug News, any one want to take on the job of editor???

Two blasts from the past to report firstly I had a call from Tony Evetts last evening, he found a video he took of the auction we held at the Wiltshire Hotel to help fund a gift for Neil Hams wife on his sudden death, this video will be on our web site in the near future.

Secondly I had a call from Roger Storrs, he wonders if there are any sharp eyed TRS80 fans around, the latest Egg advert right at the end has a TRS80 3 or 4 on screen, have you spotted it? It's great to think it's still being used if only as a decoration or prop in an advert.

Understanding USB

by Vinny La Bash
vlabash@home.com
Sarasota Personal Computer Users Group, Inc.

[This article is reprinted from the 2005 February issue of "SYDTRUG News", newsletter of SYDTRUG Inc., PO Box 75, PANANIA NSW 2213, AUSTRALIA, where it was brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organisation to which SYDTRUG Inc. belongs. There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author.]

Hail USB! Until a few years ago if you wanted to add an external device to your computer, such as a

scanner or a Zip drive, it needed your one and only parallel port. The trouble with this was that your printer had already staked out that territory. One way of getting around the problem was installing an A/B switch. However, if you needed more than one device, you had to install an A/B/C/D switch. Sometimes moving among these devices meant having to turn one off before you could use another, and often you had to reboot before your machine would recognise another device on the switch.

Early Palm Pilots and digital cameras sought your serial port. Computers had, and most still have two serial ports, but they were slow and almost always involved installation of controlling software.

There were also devices that came with their own controller cards. This meant you had to open the case and install the card in an expansion slot, provided you had one available. Things could get crazy quickly, and you had to handle IRQ conflicts, more cables, and additional power cords.

Rescue arrived with the introduction of the USB port (Universal Serial Bus) that lets you attach almost anything to your computer quickly and easily. Windows XP is designed to support USB so device conflicts are gone. The standard allows up to 127 devices on a single USB port. In practice, no one uses that many devices. USB connectors let you attach everything from TV tuners to modems. It's an amazingly flexible technology. If you had a toaster with a USB connection you could hook it up, but it's doubtful you

NATGUG News January February 2007

could watch bread turn brown on the screen.

Installing a USB device is incredibly simple. Windows XP senses it through a process called auto-detection, and asks for the driver disk if it's needed. If you have previously installed the device, XP activates it, and it's ready for use. Part of the beauty of USB is that you can connect and disconnect devices at any time without having to reboot your machine or change any options. If a cable is built-in to a USB device it will connect to your computer with its own "A" connector. Otherwise it will connect with a "B" connector. "A" and "B" connectors are of different sizes and shapes so there is never a question of getting them mixed up.

Today, most desktop computers are built with least four USB ports. That is inadequate, but there are relatively inexpensive USB hubs available that act as expansion devices. The number of ports available on an expansion hub can vary from as few as two to as many as seven, depending on your needs and how much you care to spend. Plug the hub into your computer, and then plug your devices into the hub. You can chain hubs together, and build dozens of available USB ports on a single computer.

The USB standard lets USB connected devices draw their power from their USB connection to the PC. This works well for mice, digital cameras, web cams, and other devices that use small amounts of power. Printers, scanners, and other high power accessories require their own

power supply, and they can be plugged into hubs that do not have their own power supply. If you run out of USB sockets and you have a lot of low power devices, get a powered hub so you don't overwhelm the PC bus.

Inside your computer the USB bus lets the computer act as a host to all USB devices attached to it. If you have the up-to-date USB 2.0 standard, data can be transferred at up to 480 megabits per second. If you were moving text, that works out to about 30,000 pages of documents per second. That's a maximum rate, not typical of actual use. Nevertheless, it's impressive.

USB has other advantages. You can plug in or remove USB devices without having to reboot your machine, and the computer can put USB devices into an inactive state when conserving power. XP queries all USB devices when your machine powers on, assigns each one an address, and determines what kind of data it needs to send or receive. XP keeps track of the total bandwidth of all the attached USB devices. If the combined devices reach 90% of the 480 megabit maximum, XP denies access to any additional devices. The remaining 10% is reserved for transmitting control characters, stop and start transmission codes, error checking, and other overhead.

USB 2.0 encourages the development of innovative products that would be impossible to develop with the older standards. It's the solution for all PC users who want an instant, no-hassle way to connect new hardware like digital joysticks, scanners, digital

NATGUG News January February 2007

speakers, digital cameras or a PC telephone to their computer. Plug and Pray has truly become Plug and Play.

Do You Know How Safe Your Credit Card Number Is ?

by S. Jack Lewtschuk
Monterey Bay Users Group -- PC
November 2004 mbug-pc
newsletter

[This article is reprinted from the 2005 February issue of "SYDTRUG News", newsletter of SYDTRUG Inc., PO Box 75, PANANIA NSW 2213, AUSTRALIA, where it was brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organisation to which SYDTRUG Inc. belongs. There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author.]

How many times have you typed your credit card number or password into your computer ? Any idea what happens to it ?

When you type in a password, it is stored in random access memory (RAM), where it is held temporarily until other data overwrites it or the computer is turned off. But every so often, the computer copies the contents of its RAM onto hard disk, where it is easy prey for a hacker, who can read it directly or design a worm to e-mail it back. The longer sensitive data is in RAM, the more likely it is to be copied onto the disk, where it stays until it is overwritten -- which might not happen for years.

On the other hand, do you know what happens to your credit card number after you hand your card to a clerk in a store or server in a restaurant ? He/she has your number and your signature.

Are you paranoid yet ?

****Securing Your Credit Card Before You Lose It****

Keep a record of your credit cards and other contents of your wallet. Place the contents of your wallet on a photocopy machine or scanner; copy both sides of each license, credit card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to call to report the theft and cancel the cards. Keep the photocopy in a safe place.

If you do lose your wallet, don't forget to call these numbers to report it:

Equifax 800.525.6285
Experian (formerly TRW)
888.397.3742
Trans Union 800.680.7289
Social Administration Fraud Line:
800.269.0271
Your local police department to file a theft report

****Myths VIII -- To Sign Or Not To Sign The Back Of Your Credit Card****

By the way, have you heard the idea that it is best not to sign the back of your credit cards ? That instead of signing, you can print the words: "SEE ID" or "ASK FOR PHOTO ID?"

Here is what major credit card fraud departments had to say:

MasterCard -- To not sign your card is an urban legend that sounds sensible, but is not a good idea.

American Express -- We have warned merchants not to accept

NATGUG News January February 2007

your credit cards if they aren't signed.

VISA -- They agree with the other credit card companies and said that merchants are instructed not to finish the transaction until you sign the back of your card.

So, the idea of not signing the back of your credit card is an example of a very popular urban legend that is false. Sign your credit cards immediately when you receive them.

Computer Essentials

by Pim Borman
SW Indiana PC Users Group

[This article is reprinted from the 2005 February issue of "SYDTRUG News", newsletter of SYDTRUG Inc., PO Box 75, PANANIA NSW 2213, AUSTRALIA, where it was brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organisation to which SYDTRUG Inc. belongs. There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author.]

What can be done to make computers true household appliances, intuitive and simple to use even by technophobes ? Computers capable of e-mail and word processing, Internet browsing, audio and video editing and storage, simple data processing such as checkbook and genealogy tree maintenance, and entertainment in the form of games and puzzles. After all, modern cars have highly complex, powerful engines under the hood, but turn on with a simple ignition switch and only need a steering wheel, accelerator and brakes for operation. Computers should be just as simple to use. Here are some suggestions.

A simple on/off switch for instant-on computing, with a reset button for the rare occasions the system goes haywire and needs to reboot. The hibernate feature in Windows XP is the nearest thing to it, but for shutting your system down you must first click on Start (!), then hold the shift key down to change the Standby option to Hibernate, and click on Hibernate. Stupidly unobvious, and it should be easy to replace the whole rigmarole by reprogramming the current on/off switch.

Security and privacy, built-in virus and spyware protection, automatically updated. Upgraded Internet/e-mail protocols to thwart sender address spoofing.

Fortunately, the need for improved security is now widely recognised, and the search for solutions is on.

Application programs. As my former boss used to say, "Be reasonable, do it my way." That should go double for computer applications that satisfy the users' needs without extraneous bells and whistles and with simple menus to access special features and built-in security provisions. Most common menu items should be available by using clearly labelled, standard, special purpose keyboard keys; read on.

Special purpose keys on the keyboard to perform common operations in most programs. There already are Insert, Delete, Backspace, Home, End, Page Up and Down, and Arrow keys; why not have more of that kind ? To start with, the function keys (F1 -- F12) could be reassigned, standardised, and clearly labelled

NATGUG News January February 2007

to make them more useful. F1 might always provide context-sensitive help and be relabelled as such. F2 could Save current work while shift-F2 would Save as.... F3 might do Find and Find / Replace operations, and so on. Many current programs, such as Microsoft Office, already make extensive use of the F-keys, but usage is non-standard and few users are familiar with them for lack of labelling. The same holds for the Windows and Menu keys on most keyboards; they provide handy shortcuts but are mostly underused.

Wireless Connections, high-speed, self-configuring, to peripherals such as a mouse, printer, scanner, sound system, and router for connections to Internet and a local computer network. That rat's nest of wires under and behind our computers has to go!

Broadband connection to the Internet, essential for regular updates of security programs and desirable for other Internet activities.

You may be able to think of more simplifications. Let me know about them.

Pim Borman
(swipcug@sigecom.net) is Web Editor and APCUG representative for the SW Indiana PC Users Group, Inc
(<http://swipcug.apcug.org>).

An Alternative Approach to Computer Security: Reduce Your Risk of Being a Target

by Pim Borman
Southwest Indiana PC Users
Group

[Reprinted from the 2005 February issue of "SYDTRUG News", newsletter of SYDTRUG Inc., PO Box 75, PANANIA NSW 2213, AUSTRALIA, where it was reprinted from the 2004 December issue of "Monitor", magazine of the Capital PC User Group, Inc., 19209 Mt. Airey Road, Brookeville MD 20833, U S of A, where it was brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organisation to which SYDTRUG Inc. belongs. It was reprinted from an unspecified issue of the newsletter of the Southwest Indiana PC Users Group, U S of A. There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author.]

As we all know, Microsoft software is used on 90% of the world's desktop computers. Over the years Microsoft has managed to include Internet Explorer with the Windows OS sold with almost every new computer. Microsoft Works or the more expensive Microsoft Office programs are bundled with most systems, at extra cost, but hidden in the total cost of a new computer. As a result, earlier successful programs such as Netscape, Word Star, WordPerfect, dBase II, and Lotus 1-2-3 are still only used by a few dedicated fans. To this date it is almost impossible to buy a computer from a major manufacturer without pre-installed MS software. Most recently Dell has started to sell some computers with Linux based Linspire pre-installed, but only in Europe. Dell is also offering some computers without any operating system in the US, allowing the buyer to install the OS of his or her choice. Some smaller, lesser known manufacturers also sell Microsoft-free computers. Still, it will take

NATGUG News January February 2007

years, if it is ever possible, to overcome the domination of Microsoft in the desktop computer market.

Microsoft has historically emphasised ease of use (with varying degrees of success) and addition of new features to program updates to keep the customers coming back for more. Now that it has become painfully obvious that the programs should also be resistant to tampering by malicious individuals, it is probably too late to correct the many vulnerabilities, given that there are millions of lines of code to be critically reviewed.

Microsoft recently released Service Pack 2 (SP2), a major security update for Windows XP, to address those vulnerabilities. Reviewers describe it as a major security improvement for Windows XP and Internet Explorer 6, but the virus and worm kiddies will undoubtedly find new ways to bring down the system. SP2 reportedly introduces dozens of potential incompatibilities with your hardware and software. Also, the size of the update is between 100 and 300 MB, depending on the updates already installed on your computer. Such a download is not feasible for those with a telephone modem. Microsoft has made the update available on CD, but the question remains: how many users will go to the trouble to get the update and install it? And how long will it take before most of us are up-to-date?

Alternatives

Since MS Windows and its programs are the fat and juicy sitting ducks preferred as targets for attack by virus artists, a good

way to protect yourself is to get away from it and to choose alternative software, not susceptible to common worms and viruses, and not targeted by script kiddies. The following are some possible choices.

Since most of the nastiness enters your computer through Internet Explorer and Outlook Express, choose alternative programs. Many users are changing to the free Mozilla Firefox (<http://www.mozilla.org/products/foxfire/>), an open source browser and e-mail program for Windows, Linux, or the MAC OS. The browser is quite similar to Netscape and receives high praise from most users, who prefer it to Internet explorer. Version 1.0, now available for download, also performs pop-up blocking and protection from spyware.

Another popular choice is Opera for Windows or Linux (www.opera.com), also a free download, although you must pay \$29 to get rid of an advertising banner at the top of the page. I prefer Mozilla in Linux because it is less cluttered.

MS Office programs, especially Outlook, Word and Excel, have also been targets of hackers, making use of their macro features to cause haywire. WordPerfect Office 12 from Corel (www.corel.com) includes a word processor, the Quattro Pro spreadsheet, and the presentations multimedia slideshows similar to MS PowerPoint. It costs \$300 and is almost fully compatible with MS Word documents.

NATGUG News January February 2007

StarOffice 6.0 Office Suite from Sun Microsystems (www.sun.com/software/star/staroffice/6.0/) includes word processing, spreadsheet, graphics, presentation, and database programs. It claims full compatibility with MS Office and costs \$75. It is available for Windows, Solaris, and Linux operating systems. I tried it several years ago, when it was still free, and didn't like the way it took over my computer, including rearrangement of my desktop.

Finally, a promising newcomer is the free, open-source OpenOffice.org, currently at version 1.1.2., and also from Sun Microsystems (www.openoffice.org/). It is derived from StarOffice, with omission of the code licensed by Sun from third-party sources. It is available for Windows, Mac OS, Linux and Solaris operating systems. In addition to the MS Word compatible OpenOffice Writer, it includes spreadsheet, database, and presentation programs. I have been using the word processor in Linux and find the compatibility with MS Word formats quite good. It also supports saving and mailing documents in PDF format and supports mobile device formats like AportisDoc (Palm) Pocket Word, and Pocket Excel.

The best way to avoid Microsoft targeted worms and spyware altogether is not to use any Microsoft products at all. Apple Computer's Mac Operating System is based on Unix and the Macs are therefore immune to PC viruses. The exceptions are MS Office for the Mac programs that are susceptible to the same malicious

macros aimed at PCs. The Mac OS does not run on Intel or AMD cpu-based PC clones, so you will have to buy a new expensive Apple computer to achieve trouble free on-line communications. You may still need your PC for programs that are not available on the Mac,

A better alternative is to install one of the new, inexpensive, user-friendly Linux distributions on a separate partition of your hard drive, or on an older computer if you have one. I have used Linspire (www.linspire.com) now for a year on an old laptop. It connects by Wi-Fi wireless via my router to the Internet and to my printer. I use the Mozilla browser and OpenOffice.org Write for browsing and correspondence, and everything works flawlessly. I have transferred genealogy and checkbook data to corresponding Linux programs. I can play more solitaire programs than I know how to, including two versions of FreeCell. Many other games are available, including the addictive arcade games BreakOut II and Frozen Bubble. I even managed to install a free version of the antivirus program f-prot (www.f-prot.com/) that protects Linux systems as well as Windows, but for lack of Linux viruses, I have no idea if it works or not. There is a harmless virus-like test file on the f-prot Web site that I downloaded to test f prot. It worked as advertised. A longer discussion of my experiences with Linspire can be found in the July-August issue of the P-See UrGent (<http://swipcug.apcug.org/archive/pdfs/.pdf>)

So there you have it. Maybe it is better to switch than fight!

Is There a Legal Remedy for Software Bugs and Other Things That Go Bump in the Night?

by John Brewer
Computer Club of Oklahoma City
October 2004 eMonitor

[This article is reprinted from the 2005 February issue of "SYDTRUG News", newsletter of SYDTRUG Inc., PO Box 75, PANANIA NSW 2213, AUSTRALIA, where it was brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organisation to which SYDTRUG Inc. belongs. There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author.]

How does one practice "safe computing" when one considers software bugs, adware and spyware, viruses, worms and other bits and bytes of malicious code? There is a concept in law called "product liability". Product liability means that a manufacturer can incur liability for marketing a product with defects. Does this concept apply to software? Probably not ... due to the EULA. EULA is an acronym for "end user license agreement," sometimes called the "shrink-wrap license". The term shrink wrap is used because the license is usually contained within the shrink-wrapped box containing the software and is contained in a read-me type file within the software itself. When one installs software, there is generally a license that appears in a small window that one must "accept" before the software can be installed. The small window contains a small portion of the license agreement.

In order to read the entire agreement, one must either scroll through the text or print it out. Very few people actually read the license agreement.

End user license agreements generally contain very broad waivers as a condition to use the software and such agreements have been consistently upheld by the courts. In recent years, the trend has been to broaden protection to software companies. A new controversy is over the issue of embedded software. For example, if you purchase a new automobile, and it has software that controls certain of the automobile components, do different legal rules apply to the embedded software?

Everyone is familiar with the Microsoft patches that seek to plug holes in their operating systems and applications. Nefarious people stay awake nights searching for vulnerabilities to exploit. These attacks, in the form of malicious code, often cause damages of staggering proportions. Is Microsoft at fault or is this simply a price for "doing business"? Would software companies do a better job if they had less legal protection for vulnerabilities in their software? That is an interesting question. Perhaps broad EULAs are nothing more than protection for negligent work in many instances.

The opposite side of the issue is that software programs are difficult to finish in a manner that is completely error free and plugged from malicious exploitation. Programmers have more issues to contend with than security.

NATGUG News January February 2007

Richard Fromo, an author and security consultant, is very outspoken in his criticism of the protection that software companies possess. He said recently, "Unfortunately, the only way to effect change in the software makers' philosophy of doing business is to hit them where it hurts, namely, in the pocketbook. All it takes is a few (large) customers to say 'enough is enough' and move to an alternative operating environment, and it'll be all the incentive Microsoft needs to revamp its products quickly and effectively."

Recently there was a large and complicated law called the Uniform Computer Information Transaction Act (UCITA) that was considered by many State legislatures. UCITA is very pro-industry in so far as it gives a green light to shrink-wrap licenses and allows software manufacturers to virtually sell their products on an "as-is" basis and to disclaim liability for defects. Fortunately, UCITA has encountered a skeptical reception at the State level and only Virginia has enacted the law.

The following is extracted from the licensing agreement for a well known software application:

DISCLAIMER OF WARRANTY. The software (including without limitation, the related documentation) is provided on an "as is" basis, without warranty of any kind, including without limitation the warranties that it is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the software is borne by licensee.

Should the software prove defective in any respect, licensee and not [name omitted] or its suppliers or resellers assumes the entire cost of any service and repair. This disclaimer of warranty constitutes an essential part of this agreement. No use of the software is authorized hereunder except under this disclaimer. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, so the above limitations may not apply to you.

LIMITATION OF LIABILITY. To the maximum extent permitted by applicable law, in no event will [name omitted] or its suppliers or resellers be liable for any indirect, special, incidental or consequential damages arising out of the use of or inability to use the software, including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if advised of the possibility thereof, and regardless of the legal or equitable theory (contract, tort or otherwise) upon which the claim is based. In any case, [name omitted] the entire liability under any provision of this agreement shall not exceed in the aggregate the sum of the fees licensee paid for this license (if any), with the exception or death or personal injury caused by the negligence of [name omitted] to the extent applicable law prohibits the limitation of damages in such cases. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not be applicable.

NATGUG News January February 2007

It might be prudent to read the licensing agreement the next time one installs software. It is doubtful if one can do anything about these one-sided terms but it is an issue worthy of notice.

John Brewer practices law in Oklahoma City, is a member of the Governor's and Legislative Task Force for E-Commerce, and enjoys issues relating to eBusiness and cyberspace.

Computers of the Future

by Pim Borman
SW Indiana PC Users Group

[This article is reprinted from the 2005 February issue of "SYDTRUG News", newsletter of SYDTRUG Inc., PO Box 75, PANANIA NSW 2213, AUSTRALIA, where it was brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organisation to which SYDTRUG Inc. belongs. There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author.]

For the last 40 years or so computer chips have closely followed Moore's Law, which states that the number of transistors doubles every 18 months. The corresponding increase in computing performance has been enormous, but chip manufacturers are beginning to reach the physical limit of miniaturisation. Intel's latest chip, "Prescott," with 125 million transistors an improved version of the 55-million transistor Pentium 4, was delayed by production difficulties and proved to be only marginally faster. Cramming more transistors in a certain area by reducing their size leads to increasing electrical leakage problems and crosstalk; it also increases heat generation.

Some recent microprocessors consume over 100 watts, generating more heat per square centimeter than a laundry iron on the cotton setting (W. Wayt Gibbs, writing in Scientific American, November 2004, pp.96-101). Increased computation speeds have to a large extent also been the result of clever changes in computer architecture that allow the chip to execute multiple instructions for each clock tick. We are finally reaching the inevitable end of Moore's Law.

Intel has already announced that it will no longer distinguish its microprocessors by clock speed, which is after all only part of the system's performance characteristic. In addition, starting next year, all Intel chips will have not one but two "cores" that allow higher computation speeds through parallel processing. AMD already has such chips. There is nothing new about fast computing with parallel processing computers; the fastest computers in the world are now built using thousands of processors that operate in parallel to perform specific operations, such as playing world champion chess. But all current software for home and office use will have to be rewritten.

Many users, as well as software companies, may decide it is not worth the hassle. If you have an up-to-date computer it probably responds faster to your inputs than you can provide them, unless you are a game freak or use industrial-strength graphics or database programs. Customers will be better served by improved security and simplified operations.

NATGUG News January February 2007

Not by coincidence, W. Wayt Gibbs also wrote an article in the same issue of Scientific American (Nov. 2004, pp. 80-87) about future computers using photons (light) instead of electrons (electricity) to perform computations and connections between the CPU and memory storage. There are many technical problems to be solved as yet, including the challenge to bring the cost down, but it seems likely to be the computer technology of the future. Photons move many times faster than electrons and do not significantly generate heat. All the rest is engineering detail!

Pim Borman
(swipcug@sigecon.net) is Web Editor and APCUG representative for the SW Indiana PC Users Group, Inc
(<http://swipcug.apcug.org>). This article appeared in the November 2004 issue of the P-SEE URGENT, newsletter of SWIPCUG

Why Can't I Open This File?

by Brian K. Lewis, Ph.D.
Sarasota Personal Computer Users Group, Inc.

[This article is reprinted from the 2005 March issue of "SYDTRUG News", newsletter of SYDTRUG Inc., PO Box 75, PANANIA NSW 2213, AUSTRALIA, where it was brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organisation to which SYDTRUG Inc. belongs. There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author.]

There are times in every computer user's life when the computer seems to be deliberately trying to increase your level of frustration.

One of these little moments is when you receive a file from an associate and no matter what you do, you can't open it. The file can be a document, a picture, a spreadsheet or any number of other types. So why does this happen? And what does it have to do with these things called extensions or suffixes?

Believe it or not, every file name on your computer has a three digit suffix. I know if you have never used any OS other than Windows you may never have seen this suffix or file extension. But they really do exist. If you open "My Computer" or Windows Explorer, select "Tools" from the menu. Then click on "Folder Options" and in that window click on "View". In this list some items are checked and some are not. If there is a check mark in the item "hide extensions for known file types", remove it. Then click on "apply to all folders". You will get a message telling you that the change will occur the next time you open a folder. Now open up any folder and look at the array of file extensions. Go from folder to folder and see how many different extensions you can find.

So now you see that the number of different extensions seems to be limitless. Or at least enough to bring on some confusion. Why is there such a proliferation of these three figure suffixes? Let's look again at the "Tools" menu and "Folder Options". This time click on the tab for "File Types". The upper window lists "Registered file types". Now scroll through the list until you find "Adobe Acrobat Plug-in file".

NATGUG News January February 2007

This has an extension of API and in the lower window you find a short explanation as to which program can open this file. In this case, Adobe Acrobat. Keep scrolling down through the list. You will probably find the BMP suffix. This is a picture file and usually opens with Microsoft Paint. However, on my computer it has been associated with IrfanView, a graphics viewer. Keep scrolling to get an idea of all the different file types and their extensions.

If you click on enough different file types you will notice that each type is generally, but not always, associated with an application. When you click on the change button, the preferred application is listed at the top. You can change this to another application but then double-clicking a file of that type may result in a error and it won't open. Applications such as Microsoft Word, Word Perfect, Microsoft Works, Excel, etc., can only open files that were created by them unless they have the appropriate translator for the document.

This goes back to the reasons for the file suffixes. The suffix tells Windows what application is needed to open a particular file. Every application capable of creating files uses a different format for the file header and body information. This formatting allows Word, for example, to open a document that has specific margins, type face, printer assignment, etc. The same is true for other applications.

Let's take a look at some of the definitions associated with the file structure of a Word file.

"FIB (File Information Block): The header of a Word file. Begins at offset 0 in the file. Gives the beginning offset and lengths of the document's text stream and subsidiary data structures within the file. Also stores other file status information." "DocFile: A Word docfile consists of a main stream, a summary information stream, a table stream, a data stream, and 0 or more object streams which contain private data for OLE 2.0 objects embedded within the Word document."

"Document: A named, multi-linked list of data structures, representing an ordered stream of text with properties that was produced by a user of Microsoft Word."

"Datastream: The stream within a Word docfile containing various data that hang off of characters in the main stream. For example, binary data describing @ pictures and/or form fields."

From these descriptions you can see that a Word document has a very specific structure that has to be read and interpreted in a specific way. Other applications can't read a Word file unless they have a translator for it. Even then, the translation may not accurately reflect the content and format of the original file.

NATGUG News January February 2007

Another file format is that of database files. In a dBASE file, or a FoxPro file, the first byte identifies the version that created the file. Consequently, older versions can't read files created with newer versions of the program. For a number of years Microsoft created similar problems in Word documents by changing the file format every time a new version of Word was released.

Another application that has its own file formats is Microsoft Works. This application can create text documents, database files and spreadsheets. None of these files can be opened by other programs. The interesting thing is that Works can save files in Word format, WordPerfect format or RTF (rich text file). It can even open most of these formats. But Word and WordPerfect are unable to read files in the native Works format.

Another problem exists with picture (graphic) files. Although your web browser should be able to read the most common formats, they have to be associated with the browser. If they are not, you will get an error when you attempt to open the file. Every graphic format has a different structure and may not always open in your photo software.

The most common formats used on the web are GIF and JPG (jpeg). However, these are two very different formats.

GIF

GIF is a compressed format that is referred to as a "lossless" compression. In other words, you don't lose any detail in the process of compression/decompression. However, GIF can not use more than 256 colors. That makes it less usable for color photos than other formats. However, for web page logos and other small graphics, GIF is ideal. The file size is small, so transmission time over the Internet is quite short.

JPG

Photographs can be sent by e-mail using the JPG format which is very compressible. Jpegs can be compressed to 10% of their original size which greatly reduces transmission time. However, the greater the compression, the greater the loss of detail. Jpegs are a "lossy" format. The detail that is lost by compression can never be recovered. If the picture is important, you should always keep an uncompressed master in a safe location.

TIF

Another "lossless" graphic format is TIF or TIFF (tagged image file format). This is the best format for color pictures and should be used to save the master copy of important photographs.

NATGUG News January February 2007

The major problem with TIF files is that they are very large. Much larger than jpegs. For example, a file from a digital camera was 526 KB in its native format. When converted to TIF and compressed, it took up over 6 MB on the hard drive. However, not every graphics program can read TIFF files. If yours can't, then you need something like IrfanView, a free file viewer.

So the answer to the original question is: you either don't have the application installed on your computer or you don't have the application associated with the file you are trying to open. Now, if you know the application that created the file and if you have it on your computer, you can solve the problem. You only need to associate the file with application. To do this open "My Computer" and select the "Tools" menu and "File Options". Click on the "File Types" tab and then scroll to the file extension for the file you want to open. Click on "Change" and select the application you want to use to open the file.

All of this discussion assumes that the file has not been corrupted. Even minor damage to the header of file can keep it from being opened. Transmission of files between computers is always subject to possible damage. Now maybe those undamaged files can be opened with a little less frustration.

Dr. Lewis is a former university and medical school professor. He has been working with personal computers for more than 30 years. He can be reached via e-mail at bwsail@yahoo.com.

Index

Editorial	Page 3
Understanding USB	Page 3
Do You Know How safe your Credit Card Number is?	Page 5
Computer Essentials	Page 6
An Alternative Approach to Computer Security: Reduce your risk of being a target	Page 7
Is there a legal remedy for Software Bugs and other things that go bump in the night	Page 10
Computers of the future	Page 12
Why can't I Open this File?	Page 13