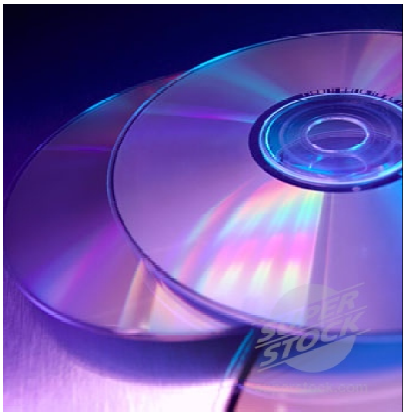
TOGGLE

THE MICROCOMPUTER TURN (ON)

MONTHLY NEWSLETTER FOR TACOMA-SEATTLE AREA MICROCOMPUTER USERS

Volume 33 Number 8 February 2013 Issue #357

IN THIS ISSUE



UPDATE

Communucations

In *What Is Online Behavioral Advertsing?* .the author says: ''Online Behavioral Advertising (OBA) uses information collected across multiple websites that you visit to predict your preferences or infer interests and to show you ads that are more likely to be of interest to you.

That's the short answer. And now for more detail.'' Read on.

In *What are cookies?* the author notes that cookies keep track of your surfing behavior and may tie in with behavioral advertising.

In *Interesting Internet Finds* the author lists some Internet sites that he found interesting.

In *Setting up hosting for your website* the author gives some advice on exactly how to do that.

In *How to get good social network security* the author gives a fairly detailed suggestions on what to post on sicial networks and what not to.

In *How to avoid the Google Redirect Virus* the author gives some advice and also several websites where antivirus tools may be downloaded.

In *Smartphone Users Should be Aware of Malware Targeting Mobile Devices* the author notes that it is not surprising that the ubiquitous communcation devices have now come under attack from viruses.

Operating System

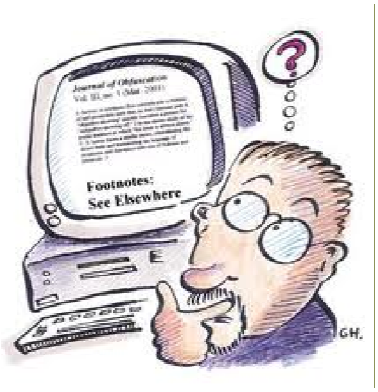
In *The Page File* the author notes that: ''Windows uses a page file to store data that can't be held by your computer's random-access memory when it fills up. Windows manages the page file fine on its own unless you specifically tinker with the size which you can do. '' He then goes on to discuss this in more detail.

In *Upgrading to Windows 8* the author, our own Carl Tenning, analyses what new features Windows 8 brings to computing and the resources needed to support this. He concludes that Windows 8 probably shouldn't be installed on a computer more than three years old.

In *Building a Better System and Data Backup Strategy* the author gives a fairly detailed list of data management tasks and disaster avoidance. Is your data valuable? If so, you should read this.

Hardware

In *Tablet PC vs. Traditional PC - Which one to buy?* the author deals with the problem we all face when it comes time to upgrade our system. This may be a very timely article for many of our members, including your editor.



COMMUNICATIONS NOTES & TIPS

What Is Online Behavioral Advertsing?

Big Bear Computer Club Bearly Bytes November, 2012

Online Behavioral Advertising (OBA) uses information collected across multiple websites that you visit to predict your preferences or infer interests and to show you ads that are more likely to be of interest to you.

That's the short answer. And now for more detail. The goal of online behavioral advertising is to make the ads you see more relevant to you based on the types of sites you visit on the Web. NAI members don't match advertisements to you as an individual, but to data categories such as books, fine arts, movies, minivans, dogs, cats, aquariums, theme parks, spas, cruises, or hundreds of other similar categories. This helps companies connect their advertisements with the right audience. Think about it this way. If you prefer to stay in bed & breakfasts when you travel, wouldn't you rather receive advertisements from websites that list those venues (maybe with discounts and specials) rather than from large hotel chains? The large hotel chains don't want to spend their valuable advertising dollars chasing after you either. And there are dozens of categories around sports and entertainment. If you like hockey, wouldn't you rather receive advertisements for NHL games than be bombarded with ads for yachting, figure skating or fishing? Most of the content on the Internet, like TV, is supported by advertising. As long as there are going to be ads on the websites you visit, wouldn't you prefer that those ads be relevant and interesting to you? Relevant advertising, customized to your perceived interests, can actually be informative to you and give you a better online experience.

What is ''personally identifiable information''?

Personally Identifiable Information (PII) includes name, address, telephone number, email address, financial account number, government-issued identifier, and any other data used or intended to be used to identify, contact or precisely locate a person.

What is ''non-personally identifiable information''?

Non-Personally Identifiable Information (Non-PII) is information that is not used to identify, contact or precisely locate a particular individual. Used for OBA by NAI member companies, this data consists primarily of click-stream information (sites you have visited or links you have clicked) that is tied to a randomly generated anonymous user identifier.

Is PII used for OBA?

While it is possible to use PII for OBA, NAI member companies primarily use only non-PII. The NAI Code would require member companies to provide notice and to obtain consent prior to using PII for OBA. In sum, online behavioral advertising does not depend on information that may be personally identifiable to you, such as your name, e-mail address, your phone number, photographs, etc. Rather than using PII, most OBA uses cookies for collecting data and creating interest-based profiles.

What are cookies?

Big Bear Computer Club Bearly Bytes November, 2012

A cookie is information (a small text file) that a site saves to your computer using your web browser. Cookies make the personalization of your web experiences possible. For example, a cookie may allow sites to record your browsing activities - like what pages and content you've looked at, when you visited, and whether you clicked on an ad. Cookies can help sites remember items in your shopping cart, your log-in name, your preferences such as always showing the weather in your home town, or your high game scores. Other cookies may be placed in your browser by third-party advertising companies to help deliver the ads you see online. These ''third-party cookies'' may be used to ''remember'' parts of your online activities in order to deliver ads tailored to your interests. For example, if you read an article online about running, a cookie may be used to note your interest in running. As you continue to surf the web, you may see coupons to save money on running shoes. Learn more about cookies by reviewing our educational resources on cookies. Frequently Asked Questions | NAI: Network Advertising Initiative

What are ''third-party'' cookies?

Cookies set by the websites you visit are typically ''first-party'' cookies. The sites you visit may work with ad networks or other service providers to help provide content or services, including advertising. Those partners also use cookies. But because these partners can only place cookies using their own web domains, they are called ''third-party'' cookies.

What is Online Behavioral Advertising?

What choices do I have regarding online behavioral advertising? Consumers have a variety of options available to customize their web experience regarding OBA, ranging from browser controls and add-on utilities to opt-out tools. Learn more about those options by checking out our educational resources here .

What are web beacons (sometimes called ''pixels'' or ''web bugs'')?

Generally, a web beacon consists of a small string of software code that represents a graphic image request on a web page or email. There may or may not be a visible graphic image associated with the web beacon and often the image is designed to blend into the background of a web page or email. Web beacons can be used for many purposes - including site traffic reporting, unique visitor counts, advertising auditing and report-ing, and personalization.

Does the NAI opt-out stop spam, junk mail, or pop-ups?

No. The NAI Opt-out covers only member companies' use of cookies to target advertising based on users' web brows-

ing. We do not maintain opt-out programs for postal or electronic mail, text messages, or for pop-ups.

Can my browser settings interfere with the use of the NAI opt-out tool?

Yes. Your browser must be set to accept third-party cookies in order for the NAI opt-out tool to work. Simply go to the opt-out page to check your system.

Will I ever need to renew my opt-out choices or opt out again?

If you opt out of OBA by one or more NAI member company, that choice will be stored in ''opt-out cookies.'' The NAI requires that such opt-out cookies have a ''lifespan'' of at least 5 years. However, if you ever delete opt-out cookies from your browser (such as by clearing all cookies), buy a new computer, or change web browsers, you'll need to renew your opt-out choices.

Interesting Internet Finds

by Steve Costello, President/Editor editor (at) brcs.org
Boca Raton Computer Society, Inc., FL Nov '12 Boca Bits
www.brcs.org http://about.me/sefcug

In the course of going through the more than 200 news feeds in my Google Reader, I often run across things that I think might be of interest to other user group members.

The following are some items I found interesting during the month of October 2012.

(Long URLs shortened with the Google URL shortener http://goo.gl/)

The Best Three Public Domain Clipart Galleries
http://goo.gl/DGNMQ

5 Best FeedBurner Alternatives For Your WordPress Blog
http://goo.gl/dP5Da

HTG Explains: How Antivirus Software Works
http://goo.gl/Yjp38

Why I bought my wife a Mac
http://goo.gl/FDzmM

How To Get Free Movies Online - Legally
http://goo.gl/jc8Nw

Secrets for successfully narrating a presentation
http://goo.gl/USl4m

Setting up hosting for your website

WWW tip By Bill Armstrong, Treasurer,
Lehigh Valley Computer Group, PA
www.lvcg.org - armstrong_bill (at) yahoo.com

Web addresses (URLs) are not just for businesses. Many individuals prefer to have their own family address, such as armstrongfamily.org (I made that up). Here are some things to think about when considering this approach.

There are two phases that both have to be completed:
- Get your own web address (a yearly charge)
- Get some business/ISP to host your address (a yearly charge)

Getting your own web address is accomplished by searching on the web for a web address vendor, such as ***http://www.networksolutions.com***. They are the original authorized vendor (many others are now available). Here you may do a search to discover what addresses are available. Many URL extensions are now available, in addition to .com, .org, and .net.

Finding a business to host your site is easy also. Try Googling ''web hosting'' to find many. You might also consider local Internet Service Providers (ISPs).

You will have to inquire about the hosting costs. Most companies offer a low-cost hosting that includes basic services, such as email accounts, limited disk space for storage, etc.

In many cases, these two items merge into one, by companies that specialize in doing both and charging you one fee. This website reviews hosting companies: ***http://www.top10hostinglist.com***.

Most of these all-in-one sites offer ways for you to create a website for yourself. Their scripting services will assist you.

If, however, you want the ease of using Google Sites, as we do in the LVCG, that can also be done. Our website is ***www.lvcg.org***, hosted by PAETEC (formerly Fast.net) and on it we have a ''redirect script'' that sends every visitor to our Google Sites website. We can have many people able to add and edit stuff, and customize it easily. You may find that it is easier to work in Google Sites than in the tools offered by the hosting site.

However, redirecting to Google Sites does not give you email services. You could check with the hosting companies to see if there is a way to redirect web-based traffic to another address (your Google Sites website), and still give you the ability to have, access and manage email services using your own web address.

Be careful of limited time offers. I saw one that was $3.50 per month for the initial period, and then jumped to $7-8 per month. It did include a free web address (URL), so that's probably still a good deal. Also review their ''uptime'' and ''speed'' statistics for the various sites.

Having your own website address is a nice feature, and many consider it well worth the expense. It is a little work to do the maintenance needed, but that is minimal.

This article appeared in the July 2012 issue of LVCG Journal.

How to get good social network security

By Penny Cano, member and instructor,
Cajun Clickers Computer Club, LA
www.clickers.org - ccnewsletter (at) cox.net

Facebook, Twitter, Google+, YouTube, Pinterest, LinkedIn and other social networks have become an integral part of online lives. Social networks are a great way to stay connected with others, but you should be wary about how much personal information you post. Have your family follow these tips to safely enjoy social networking:

- Privacy and security settings exist for a reason: Learn about and use the privacy and security settings on social net works. They are there to help you control who sees what you post and manage your online experience in a positive way.

- Once posted, always posted: Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research (http://www.microsoft.com/privacy/dpd/research.aspx) found that 70% of job recruiters rejected candidates based on information they found online.

- Your online reputation can be a good thing: Recent research (http://www.microsoft.com/privacy/dpd/research.aspx) also found that recruiters respond to a strong, positive personal brand online. So show your smarts, thoughtfulness, and mastery of the environment. ??Keep personal info personal: Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data, or commit other crimes such as stalking.

- Know and manage your friends: Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. Use tools to manage the information you share with friends in different groups or even have multiple online pages. If you're trying to create a public persona as a blogger or expert, create an open profile or a ''fan'' page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know and trust) more synced up with your daily life.

- Be honest if you're uncomfortable: If a friend posts some thing about you that makes you uncomfortable or you think is inappropriate, let them know. Likewise, stay open-minded if a friend approaches you because something you've posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them; respect those differences.

- Know what action to take: If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator. Protect Yourself with these Stop. Think. Connect. Tips:

- Keep a clean machine: Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.

- Own your online presence: When applicable, set the privacy and security settings on websites to your comfort level for information sharing. It's OK to limit how you share information.

- Make passwords long and strong: Combine capital and lowercase letters with numbers and symbols to create a more secure password.

- Unique account, unique password: Separate passwords for every account helps to thwart cybercriminals.

- When in doubt, throw it out: Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.

- Post only about others as you would have them post about you.

How to avoid the Google Redirect Virus

by Penny Cano, member and instructor, Cajun Clickers
Computer Club, LA
www.clickers.org - ccnewsletter (at) cox.net

You search Google for something that interests you and get a series of Google web pages with links to websites with pertinent information. But this time, no matter which link you click on, it takes you to a website selling something that has absolutely nothing to do with the topic of your search.

Suspecting something, you do a full scan with your virus program and don't find any infection. Then you may try some of the other malware removal programs like Malwarebytes, Spybot, or SuperAntiSpyware; they don't find anything either. But you know something is wrong. I ran into this when one of our club members became infected and came to me seeking help. Since most of us use Google search with some frequency, I thought it a good time to discuss how this Trojan and other similar Trojans work.

Incentive for infection

Some of the other names for this Trojan are Bac-door.Tidserv, Win32.TDSS, and Alureon. It's not new; it was first discovered in 2008 and additional variations have been created since then.

Its purpose is primarily profit-making. The person or enterprise that infects your computer actually gets paid for doing so. To go undetected, it hides itself using stealth techniques, including a rootkit.

Once it is on the computer, it installs itself where it cannot be detected, then deletes the original files to eliminate traces of itself. The payload then causes the user to be redirected to web sites associated with malicious schemes or ones that download and install software that is not needed or wanted. So the infector gets a kickback for each user who succumbs.

How you get infected

Social networking opens up a myriad of opportunities for these attackers. It can be spread by means of the KoobFace Trojan specific to FaceBook. Forums and Blogs are another source. A typical scenario involves some sensational topic with an associated link to what appears to be a video or pictures.

When the user clicks one of these links, the attacker has the opportunity to deliver the infection. The same attacker may place these links on many sites on the Web. Links in e-mail provide another opportunity.

When people see something they think is funny or interesting on the Internet, they feel compelled to forward the website or link to all their friends. This in turn gets forwarded and re-forwarded. You may not know the original sender or many of the other people it was sent to. (Of course you've never received these - right?) And then there's spam with all sorts of links. If the link points to an infected site, the infection gets spread to anyone clicking on it.

Peer-to-Peer networking for the downloading of pirated software (music, movies, and programs) and shared files is another source of infection. The supplier of the illegal software (or files) is often anonymous. Who's to say the name of the malware file was not changed to that of a popular song, for example. When the pirated ''song'' is downloaded the user is really downloading the Trojan. It is much safer to pay for legitimate content.

Hacked websites can actually be legitimate or well-known sites that have malicious software unknowingly installed on them. Web forms are particularly vulnerable if the system they are on is not properly secured. Those crazy looking letters that you are asked to type into the box below (don't you just hate them?) are a security measure to keep attackers from gaining access to the forms.

Avoiding infection

Be careful about clicking on links on Web sites and in e-mail. Sometimes, if you pause your cursor on a link, you can see where the link actually leads. Be cautious clicking on links in e-mail, particularly spam and those that have been forwarded multiple times to multiple people.

Some virus programs have link-checking as a built-in function and rate links on Web pages. This is particularly useful when following search engine results. If advertisements occur in pop-ups, do not click on them or follow the links they offer.

Buy your downloaded software from known sources. Pirated software is often booby-trapped with malware. Keep your Windows Operating System up-to-date. Windows Update provides patches that can lessen the risk of the system being compromised.

Removal

I found three removal tools online:

- Symantec: go to ***http://symantec.com/security_response*** and search the site for ''Tidserv''.

- Kaspersky provides TDSSKiller.exe ***http://bit.ly/h4FjC8***

- McAfee offers Stinger.exe ***http://bit.ly/dJTzpJ***

However, since this Trojan hides in areas outside the operating system and makes itself undetectable by normal means, I highly recommend that you take your computer to someone familiar with its removal if you experience these symptoms.

This article originally appeared in the July 2012 issue of the Cajun Clickers Computer News

Smartphone Users Should be Aware of Malware Targeting Mobile Devices

Big Bear Computer Club Bearly Bytes November, 2012

The IC3 has been made aware of various malware attacking Android operating systems for mobile devices. Some of the latest known versions of this type of malware are Loozfon and FinFisher.

Loozfon is an information-stealing piece of malware. Criminals use different variants to lure the victims. One version is a work-at-home opportunity that promises a profitable payday just for sending out e-mail. A link within these advertisements leads to a website that is designed to push Loozfon on the users device. The malicious application steals contact details from the users address book and the infected devices phone number.

FinFisher is a spyware capable of taking over the components of a mobile device. When installed the mobile device can be remotely controlled and monitored no matter where the Target is located. FinFisher can be easily transmitted to a smartphone when the user visits a specific web link or opens a text message masquer-ading as a system update.

Loozfon and FinFisher are just two examples of malware used by criminals to lure users into compromising their devices.

Safety tips to protect your mobile device:

When purchasing a smartphone, know the features of the device, including the default settings. Turn off features of the device not needed to minimize the attack surface of the device. Depending on the type of phone, the operating system may have encryption available. This can be used to protect the users personal data in the case of loss or theft.

With the growth of the application market for mobile devices, users should look at the reviews of the devel-oper/ company who published the application.
Review and understand the permissions you are giving when you download applications.

Passcode protect your mobile device. This is the first layer of physical security to protect the contents of the device. In conjunction with the passcode, enable the screen lock feature after a few minutes of inactivity.

Obtain malware protection for your mobile device. Look for applications that specialize in antivirus or file integrity that helps protect your device from rogue applications and malware. Be aware of applications that enable geo-location. The application will track the users location anywhere. This application can be used for marketing, but can also be used by malicious actors, raising concerns of as-sisting a possible stalker and/ or burglaries.

Jailbreak or rooting is used to remove certain restrictions imposed by the device manufacturer or cell phone carrier. This allows the user nearly unregulated control over what programs can be installed and how the device can be used. However, this procedure often involves exploiting significant security vulnerabilities and increases the attack surface of the device. Anytime an application or service runs in unrestricted or system level within an operation system, it allows any compromise to take full control of the device.

Do not allow your device to connect to unknown wireless networks. These networks could be rogue access points that capture information passed between your device and a legitimate server.

If you decide to sell your device or trade it in, make sure you wipe the device (reset it to factory default) to avoid leaving personal data on the device.

Smartphones require updates to run applications and firmware. If users neglect this, it increases the risk of having their device hacked or compromised.

Avoid clicking on or otherwise downloading software or links from unknown sources.

Use the same precautions on your mobile phone as you would on your computer when using the Internet.

If you have been a victim of an Internet scam or have received an e-mail that you believe was an attempted scam, please file a complaint at ***www.IC3.gov*** 10/12/12

OPERRATING SYSTEM NOTES & TIPS

The Page File

by F. Verano,
Computer Club of Menifee Valley Newsletter, January 2013

Windows uses a page file to store data that can't be held by your computer's random-access memory when it fills up. Windows manages the page file fine on its own unless you specifically tinker with the size which you can do.

How does the page file work? The page file is also known as the swap file, pagefile, or paging file. It is a place on your hard drive. And because it is on the hard drive, it takes longer for the processor to have access to data in the file because the hard drive is much slower than the RAM. This may be gobblygook to you so let me give you an example.

Pretend that the RAM is the physical desk that you, an office worker, are doing work on, like opening mail, writing checks making notes or writing letters, reading letters or reports, etc. You get the idea; it's the stuff you are working with. You pulled all that stuff you are working with out of a big 5 drawer file cabinet the first thing when you sat down at the desk. But everything on your desk is immediately accessible to you to work with and you don't have to pull it out of the file cabinet. However, ... let's make it HOWEVER, if you if your desk isn't big enough, stuff may fall off on the floor or in the waste basket or get mixed up with other papers on the desk. And your work can come to a screeching halt.

But if you are orderly, you'll temporarily put it in the file cabinet so as to not lose it. (You have lots of room there.) And when you need it you have to go the file cabinet to get it and perhaps move some of the junk on the desk to the file cabinet. You know that gets too inefficient and work slows down.

Above I said to pretend the RAM (Random Access Memory) is your desk. Just for the heck of it pretend that it is small like a cutting board. You ain't going to get much done. You'll have keep running back and forth to the cabinet to get your stuff and put stuff back there. On the other hand (I jokingly tell people, you have a thumb and four fingers) if your desk was 20 feet square, you couldn't use all of it and it would be wasted, unless . and I'll come back to this shortly. Meanwhile think about it. Your file cabinets are like your hard drives. You can put a lot of stuff in there. And providing that you put it there in an organized way to begin with, it is easily retrievable.

It seems like a logical way for a computer to be designed organized: Have a fast work space like the RAM and a big storage place like the hard drives.

That is as far as I want to go on describing how things work. Now let us think ahead but continue using these analogies.

Most of you have thumb drives. I often referred to them in the past few years in this newsletter. I've also mentioned the evolution of solid state memories (SSDs) similar to the thumb drives but on a bigger scale. These are intended to replace the hard drives.

So in my analogy I picture the SSD as another big desktop, really, really big desktop with no drawers to pull. This big desktop is right there with the working desktop (RAM analogy.) Using the file cabinets as an analogy to the hard drives is easy to understand but it is not easy to see what the SSD analogy would be. I think it best to think of rows and rows of shelves with each shelf occupying a data storage unit.

My analogy does make the work of the processor more complicated. If we think of you as the processor then you'd have to be on roller skates to quickly access files in the SSD. But then the work in the RAM was be halted. Well the solution is to have two (or more) processors One would be doing the work in the RAM and the other controlling the SSD, accessing, storing, rearranging for maximum efficiency.

The analogy breaks down as far as the physics is concerned. SSDs are much lighter than the Hard Drives and they use much less power. They are being used in some laptops where weight is a problem. They will be ultimately be the standard in desktops too, if they survive. Right now there are two problems with the SSDs. They are still expensive and we can expect them to become price competitive eventually. The other problem is that unlike the hard drives, when a hard drive fails, in many cases data can be retrieved but it is an expensive matter.

On the other hand (so far) when a SSD fails there is no hope of retrieving your data. For that reason redundancy must be used to reduce the probability of data loss. Redundancy is used extensively in military equipment and I suspect that the military will lead the way.

A final note: Laptops sales equal or by now exceed the sales of desktops. We are seeing a convergence of the SSD and the laptop.

I keep thinking of the huge differential analyzer I worked on in 1952 at the Lincoln Labs.

Upgrading to Windows 8

by Carl Tenning
Tacoma Open Group For Microcomputers

I had a notebook that came with Windows Vista pre-installed. Later when Windows 7 was released, I upgraded the notebook to Windows 7. That upgrade was without much difficulty. But just recently I received an offer from Microsoft for an upgrade to Windows 8 Pro for $39.95, so I went for it. This was the download-only price. Receiving the media by mail was an extra $14.95, but I opted for the download only.

The download is about 2.5 GB and is an image file for burning your own DVD. I used the free image burning application ''ImgBurn''. The whole process of downloading and DVD burning was without problems. The problems started when Windows 8 failed to install. But at least it reverted back to the Windows 7 operating system. I was able to make a phone call to the Microsoft Store that I made the purchase from and they were very helpful. They actually took control of my laptop and proceeded to make the installation. There were two options for installing Windows 8; the first option was to retain the applications that were currently installed and the second was to delete all applications for a clean install.

I had selected the first option when I first attempted to install Windows 8, which was the installation that failed. When the Microsoft helper took control, there was no longer the option of saving the current applications, so the installation proceeded with a clean install, which was successful.

At least Windows 8 was now running. But there were still some problems. Not all of the drivers for Windows 8 were compatible with this particular notebook, probably because of the age of this notebook (it was originally designed for Windows Vista). One was that the coprocessor driver would not install, apparently leaving the coprocessor inoperative. Another was that the video driver would not support an external monitor. This was only discovered at the January computer club meeting when we couldn't get the notebook to display on the external projector. Well, enough is enough! I decided to go back to Windows 7. Now the original installation of Windows 7 was the 32-bit version. But since I originally made that installation, I learned that this notebook was capable of x64 bit operation, so I opted for installing the x64 bit version. The Windows 7 package I had was an upgrade version that came with two DVD's, one for a 32-bit installation and another for a 64-bit installation. Now since this edition of Windows 7 was for upgrade-only installation, I wasn't sure that it would install over Windows 8. But I tried it and it did install. Of course I had to re-install all my applications, but at least it was successful. One advantage of the whole process was that it eliminated all of the junk files and applications that had accumulated over seven years of usage.

Conclusion: It's probably not worth installing operating system upgrades to computers over three years old.

Building a Better System and Data Backup Strategy

by Gabe Goldberg, APCUG Advisor Region 2,
Destination.z@gabegold.com

Because operating without reliable backup risks corporate health and can be a profoundly career-limiting move, the most fundamental resolution for mainframe professionals is ''backup, backup, backup.'' But beyond that, some may ask where to start and what to do? Challenges and opportunities to better preserve critical software and data resources divide - though not precisely - between technology and human issues.

Let's address backup - and its indispensable partner, restore - which are separate from more complex issues of business continuity (BC), formerly called disaster planning/recovery. While critical for BC, backup/restore are hardly a complete solution for it. Consider these tips and best practices:

Subhead: Technology/Logistics Tasks

1. Remember why you're doing this. Let business reasons for backup govern your decisions. Consider disaster recovery, user errors, audit/disclosure/preservation requirements.

2.. Back up everything that matters. Do you know where your data is? It's no longer just nicely boxed in server rooms. Besides servers, desktop and laptop computers, tablets and smartphones can contain essential nowhere-else data. If you'd miss it, back it up. Remember Hardware Management Console (HMC) data, and back it up regularly to a USB drive, DVD, via FTP, etc.

3. Integrate backup processing and data as much as possible. No matter why you're restoring data, it's messy and risky to have to use too many tools to recover varying format/location data.

4. Ensure backups are complete. Some utilities won't include expired files in full-volume backups, or won't write them to tape. After backup procedures are created, verify file inventories are complete.

5. Plan ahead for restoring data in a recovery center. Require vendors to provide emergency keys/codes/passwords for using their products away from home.

6. Automate. As much as possible, avoid manual steps in backing up data, documenting ''what's where'' for each backup and how to restore it.

7. Create duplicate/redundant/separate backups. Single backup volumes have huge capacity, so losing or damaging one can be a catastrophe. Data Facility Storage Management Subsystem's (DFSMS) duplex option simplifies this. Don't let one bad tape volume spoil a disaster-recovery drill - or a real disaster recovery.

8. Be secure. Maintain strict control of backup media to avoid a massive data breach appearing in the other media.

9. Use offsite storage. You won't win an award for stellar backup if all data copies are destroyed at once by fire, earthquake, hurricane, flood, or tornado. Use enterprise-worthy shipping, perhaps not local delivery services, and don't send duplicates together!

10. Encrypt whatever leaves your local facility. No matter how it's shipped or where it's sent, don't let ''out of sight'' mean ''out of control.''

11. Remember stored backup media when changing IT technology. Especially if you're subject to longterm retention (and retrieval) requirements, don't let older backup generations become unreadable. Include backup migration in equipment-upgrade planning.

12. Automate failure notification. Don't rely on manual detection and alerting; it's too easy for processing oddities to become routine without appropriate people knowing.

Subhead: Human/Management Challenges

1. Ensure BC. Meaningful disaster planning/drill/recovery requires using standard live backup files to recreate enough production operation to remain in business. To avoid unpleasant surprises, restore and verify ''everything that matters'' working properly.

2. Understand varying backups. Full, incremental and differential backups have different purposes, strengths and weaknesses, as do tape, DASD, virtual tape and FlashCopy technologies. Apply them appropriately to data with special requirements such as DB2 databases, which benefit from DS6800 FlashCopy consistency groups, creating consistent point-in-time copies across multiple volumes.

3. Back up critical files especially carefully and often. What would you do without VM's system directory, TSO's user attributes data set (UADS), or a Resource Access Control Facility (RACF) database? Most directory management tools allow backing up directory files; it's useful and comforting to have a few copies, just in case. Always know which copy is authoritative and protect these files as critical, high-exposure data.

4. Plan backup cycles to match business needs. No backup plan or technology fits all situations. High volatility or transaction rates processing missioncritical or customer-sensitive data might need realtime offsite mirroring; ensure that it's far enough away to prevent both data centers being affected by the same incident. More leisurely environments handling fewer or more-easily reconstructed transactions might only require daily backups.

5. Test backup/restore periodically. Appearances can be deceiving; backups seeming to run normally might not be

doing anything useful. Occasionally - but reliably - test all backup aspects by restoring and verifying data. This also ensures that restore processes aren't used for the first time in a crisis situation. Even if backups have worked flawlessly, that's not the time to learn how to restore data.

6. Document everything. This includes automatic and manual processes, tools used, file formats, data placements, error recovery, etc. Ensure information is current; don't let ''small'' changes creep in via oral tradition updates. Keep documentation duplicates onsite, at BC site, perhaps at operations or system programmers' homes, or on keychain USB drives. Write processes as non-technical, simple checklists that someone can handle cold when seeing them for the first time.

7. Train operations and other staff on backup technologies and processes. Ensure that everyone understands not just backup's critical nature but also how data is being protected, so they're not robotically following mysterious procedures.

8. Train operators to notice and notify on oddities as well as failure/warning alarms. It's too easy for minor glitches to be ignored and grow into major problems.

9. Educate users and management in what's done and what's possible. Help them be realistic in expectations and demands. Ensure they have a voice in designing and planning backup protections.

10. Provide user-initiated restore. Within reasonable and announced constraints, allow users to automatically restore files without technical support. Of course, ensure that only original data owners can do this.

11. Backup is not archive. Be clear that backups are not forever and that arbitrarily old data cannot be restored. If desired, provide file archiving - userdriven or automated - separate from backup.

12. Consider risks of human error or malicious behavior. Online-only backup might be vulnerable to simultaneous destruction of original data and all adds reliability, as does separation of duties requiring multiple people to perform sensitive tasks.

As mundane as managing backup is, no ''Backup Professional'' certification is available. It's a foundation of data center survival. It's best when never needed but potentially catastrophic when missing. Once established and verified, backup processing needn't be burdensome, as long as it's remembered and integrated into change management. Backup/restore/BC are not purely technical issues; they're fundamental corporate and line-of-business decisions.

Gabe Goldberg has developed, worked with and written about technology for decades.

HARDWARE NOTES & TIPS

Tablet PC vs. Traditional PC - Which one to buy?

Phil Sorrentino, Member, Sarasota PCUG, FL,
October 2012 issue, PC Monitor,
www.spcug.org, pcugedit (at) verizon.net

This is a really great question or contest. So, first let's define the two contenders. We'll consider a notebook, or laptop, as the traditional PC. (The contest between laptop and desktop has already been had and for most users, the laptop seems to have come out on top.) And as to the tablet, let's consider only the 10 inch variety. Currently, tablets are available in two sizes, 7 and 10 inches, but as a replacement for a notebook (with screen sized between 14 and 17 inches), a 10 inch tablet seems to be the only real contender. Actually, we could even consider a smartphone as a very small tablet, but in this contest, size counts.

If you need a quick answer to the question, that answer might be: if you are only going to ''consume'' data, then the tablet will work fine; but if you intend to ''produce'' data, then the laptop with its keyboard and large hard drive is the better choice. Consuming data implies playing music, showing pictures, watching videos, checking email, light game playing, and maybe minimal web surfing. Producing data is more like creating well formatted text documents, developing spreadsheets, editing pictures and videos, creating lengthy emails, heavy game playing, and spending a good deal of time navigating the internet.

Tablets are similar to notebooks in many ways, because they are both built for mobility. They both are small and light weight (especially the newer Ultrabooks), and they both are battery powered. But that's about where the similarities end and the differences begin. Tablets have no moving parts, no hard drive or optical (CD/DVD) drive; whereas notebooks typically have a hard drive and an optical drive. Tablets, with their smaller screens, are typically smaller and thinner than laptops. Tablets, typically, do not have a keyboard or a mouse; data input comes from touching the display screen. (Today's improved touchscreens employ a capacitive effect, which responds to fingers, as opposed to yesterday's touchscreens, that used a resistive effect, and required a stylus for operation.) Laptops and tablets both have USB connections. However, on the Laptop the USB is used to connect peripheral devices, but on the tablet the USB is used to connect the tablet to a laptop (or desktop) as a peripheral device. Laptops and tablets both have video output connections. Typically, on the tablet the connection will be a micro-HDMI connector, while on the laptop it will be probably be either VGA or HDMI.

Today's tablets use a different Operating System than traditional computers, although this may change with the

advent of Windows 8, which is being advertised as able to run on tablets and traditional computers. Windows 8 is scheduled to be released October 26th, so for today, practically speaking, the choices for Operating System are iOS from Apple, and Android from Google. iOS will be found on all Apple iPad tablets (and iPhones), and Android will be found on all Android style tablets, from manufacturers such as Motorola, LG, Samsung, Sony, Toshiba, HTC, Acer, etc.

Advantages and disadvantages of tablets vs. traditional computers are highly subjective. An ''advantage'' that appeals to one user may be exactly what disappoints another, but here are some commonly cited advantages and disadvantages. Some of the tablet's advantages may be: smaller size, lower weight, lower power usage, and the use of the touch environment. While some of the tablet's disadvantages may be: smaller screen size, and slower input speed due to the use of the touch environment.

The Touch environment is a basic difference, until Touch comes to the laptop. Touch on a tablet is similar to the mouse environment on a traditional computer. If one is familiar with using a mouse, the Touch motions needed for computer input are very intuitive. A Tap on a touchscreen is similar to a click on a mouse. A ''Touch and Hold'' on a touchscreen is similar to a Double-click using a mouse. Drag and Drop is done with a finger on a touchscreen similar to that done with a mouse. A ''Finger Scroll'' on a touchscreen is similar to a Mouse scroll with a scroll bar on a computer screen. A Pinch (using two fingers), on a touchscreen is similar to a Zoom on a computer screen. As far as text data input goes, typically, a virtual keyboard is presented on the touchscreen whenever text data entry is required. The virtual keyboard is large enough to be comfortable on a 10 inch screen, but it lacks mechanical movement and feedback. (Typically there is audible feedback and some provide haptic feedback, which is a brief, gentle vibration.)

So, after you've seen the obvious size, weight, and cost differences and appreciate the different input techniques, it all comes down to what you want to accomplish with this piece of technology. After all, you're buying this device to accomplish something, aren't you? Or, is this just another toy?

Assuming it is not just another toy, then let's look at what it might be used for. A tablet is ideal for showing pictures to your family and friends, listening to your favorite music, and watching relatively short videos, like Youtube videos. (Probably best to leave the full length movies for your big screen TV in the living room). (When it comes to listening to music, the smaller the device the better, because listening to music doesn't require much of a display, so an MP3 player (iPod) is probably the best device for listening to music; but if you have a laptop or tablet around it can certainly do the job.) A tablet is also good for casual internet access where there is a minimum of data entry and easy web page navigation. A tablet is fine for getting your email, as long as you don't have to create any lengthy replies. A tablet is great for quickly checking into your social networking sites to keep up with your family and friends, as long as you intend to leave only short messages. (A tablet would probably not be good for you if you intend to ''blog'' a lot.)

For those familiar with the Windows File and Folder organization, a laptop with Windows provides a familiar interface. The tablet's interface is similar but not the same. There is no ''Windows Explorer'' that is common to all the tablets, although there are some good file management Apps available. So, file management is easier on a laptop, making it a better choice if you are going to create and organize many files, be they text, pictures, or videos. The laptop is probably a better choice if you intend to do anything that requires a lot of data entry (keyboarding) such as preparing lengthy spreadsheets. The laptop is better for producing slideshows combining pictures and videos, or creating any digital video. (In fact, video projects are probably better performed on a desktop where you have a larger display screen, lots of hard drive space, a very fast processor and a lot of memory.)

Networking can be a major consideration. If you have a home network, the laptop (running Windows) will be able to become a Workgroup or Homegroup member and it will be able to transfer files to and from the other network members, once the proper sharing parameters and permissions are set up. The tablet (running Android or iOS) will not be able to participate in the home network without a good amount of effort and special Apps running on the tablet. So if you intend to share files on the network, the laptop would probably be a better choice.

Even after you appreciate the advantages and disadvantages of each, specifically to you, and you have struggled with all the differences, it is still a difficult decision. So, maybe it is not really a contest at all, but rather just a separation of capabilities, needs and/or desires. There are probably many good reasons for having both. It is just a matter of what you want to accomplish and how soon you can justify the additional cost of having both. (Good luck with that justification and decision.) Have both and leave the tablet on the coffee table for easy access and bring out the laptop only when needed.

Help Lines

HARDWAREHELP	Advisor No.
Reformat Hard Disk, FDISK	2,4,5
Install Hard Drive, CD-ROM/RW	2,4,5
Install Video Card	7
Partitioning Hard Drives	2
Internet/Intranet	6,7
Audio Cards	4
MPs Files, WMA Files, WAV Files	3,4
Burning CD's	3,5
Homesite	7
Net Objects	7

SOFTWAREHELP	Advisor No.
Win 95/98/ME/2K/NT/XP	2,3,4,7
Win 7	4,7
Microsoft Word	2,7
Microsoft Excel	4
Microsoft PowerPoint	4
WordPerfect	1,7
Norton/Symantec AntiVirus	2,3,6,7
Norton System Works	2,7
CompuPic / CompuPic Pro	3,7
Winzip, WinRAR	6
Ccleaner	3,4
Outlook, Outlook Express	2
Internet Explorer	2,7
RegSeeker	3,5
Instant Messaging	2
Installing Software after Reformatting	5
Deleting Files; Wiping	6

ADVISORS

Name	Phone	Hours
[1] Fred Shelton	(253)752-0120	Variable
[2] Bob Henkel	(253)537-6732	8A-8P any day
[3] Tom Stepanek	(253)922-7939	7-9P Mon-Fri
[4] Carl Tenning	(206)824-3843	6-9P Mon-Fri
[5] Oclad Wesley	(253)212-0352	6-9P
[6] Bob Thomson	(253)752-5582	Variable
[7] Ray Mills	(360)692-7568	6-9P Mon-Sat

Tacoma Open Group for Microcomputers (TOG)
New Member Application/Existing Member Change of Address Form

For **Tacoma Open Group** annual membership, send form (if needed) & **$25** to Bob Henkel., 10613 25th Avenue E., Tacoma, WA 98445.
Make checks payable to TOG

Please print or type. Date:_____ Sponsored by:_____

Member's Name:_____

Address: _____

City:_____ State:_____ Zipcode:_____Plus Four _____ Country: _____

Home Phone: (____) _____ Work phone: (____) _____ E-Mail Address _____

TACOMA MEETING

When: **Mon 9 Dec 2012 -7:00 PM**
Where: SE Tacoma Community Centre
1614 99th Street E.
Tacoma, Washington

From I-5 take Exit 127 (Hwy 512) to Portland Ave., north on Portland to 99th, left over tracks. Building is on south side.

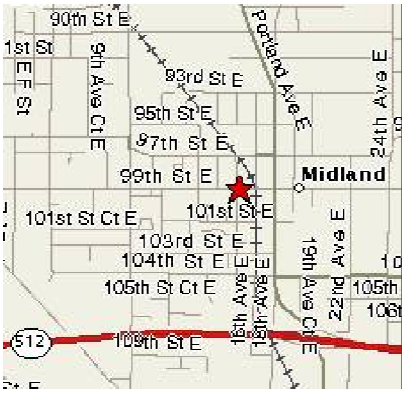
Future Dates: 2nd Monday of Month

TOG BOARD MEMBERS

Deadline: 15th of this month to appear in next months' issue, if room

How To get To The Meeting

For those readers still unfamiliar with how to find our meeting place we have reproduced the map showing its relationship in Tacoma to Portland Ave S. and the 512 Freeway. The 512 Freeway can be entered from I-5 in Tacoma on the west or from Hwy 167 in Puyallup on the east. Proceed to Portland off-ramp and turn north to 99th Street. Some folks in the middle of Tacoma may prefer to take Portland southbound to 99th. At 99th turn west over the tracks and there you are!



Tacoma OPEN Group for Micros
1808 Lenore Drive
Tacoma, WA 98406-1920

Change Service Requested

PROGRAMS

This Month's Meeting

This will be a regular monthly meeting. Meeting discussions are always interesting and the ever-popular Q&A (Question & Answer) period is sure to pique your interest, come up to your expectations and tickle your fancy. Come and share your own experiences, problems and discoveries.

No Formal Program is scheduled at press time. Come and bring your questions and discoveries.