Twenty Computer Myths That CPA's Should Know

Alexander McLeod, Ph.D. – Assistant Professor University of Nevada Reno
E-mail: amcleod@unr.edu; Phone: 775-784-6897

Sonja Pippin(*), Ph.D. – Assistant Professor University of Nevada Reno
E-mail: sonjap@unr.edu; Phone: 775-784-1337

Mark Simkin, Ph.D. – Professor, University of Nevada Reno
E-mail: simkin@unr.edu; Phone: 775-784-4840

Department of Accounting & Information Systems
College of Business Administration
University of Nevada Reno
1664 N. Virginia Street
Reno, NV 89557

Short Biographical Information:

Alexander McLeod is an assistant professor of Information Systems at the University of Nevada, Reno. He earned his Ph.D. in Information Technology from the University of Texas San Antonio. His research is practical in nature covering information systems security, healthcare and system performance. He currently teaches introduction to management information systems and business process management.

(*) *Sonja Pippin* is an assistant professor in the accounting and information systems department at the University of Nevada Reno. She received her master's in accounting and her Ph.D. in business administration from Texas Tech University in Lubbock, TX. She currently teaches undergraduate and graduate tax courses. Her research combines her interests in public finance, information systems, and tax law.

Mark G. Simkin is a professor of Information Systems at the University of Nevada. His research interests include man-machine interfaces, computer testing, and end-user programming. He is also the coauthor of Core Concepts of Accounting Information Systems (John Wiley and Sons). His Ph.D. and his M.B.A. Degree are from the University of California Berkeley.

(*) Corresponding author

Twenty Computer Myths That CPA's Should Know About

It doesn't matter how computer myths start. For CPAs, separating fact from fiction might matter a lot in terms of saving money for themselves or providing useful advice to clients. Here, we present, and hopefully dispel, 20 common computer myths we found circulating today.

1. **Claim:** I need a dual-core processor in my computer because I need the speed.

   Reality: The idea behind dual-core processing is to split the computations between two processors, thereby doubling the internal computational speed of a computer. But most accounting applications do not need such speeds because they do things in linear fashion. A possible exception is if you use software specifically written for two processors and your operating system can exploit this, but most accounting software does not fall into this category.

   In addition, most computers today are input/output bound, which means that what keeps them from going faster are the limits imposed by peripheral equipment in providing data to or outputting data from a computer. Your inability to type faster is one example of such limitations. Another constraint is the limit on transfer speeds over the Internet.

2. **Claim:** I need a new computer with a 64-bit operating system.

   Reality: Until recently, most application software was written for 32-bit operating systems such as Windows XP. If you are using software such as ProSystems, Gosystems, Excel, QuickBooks, or TurboTax and things are working well, there is probably no immediate need to upgrade because processing speed or primary memory space is not likely to be an issue.

   The biggest problem with 32-bit operating systems is their inability to address massive amounts of primary memory used to store and run applications. This is analogous to five-digit zip codes. The maximum number of different codes possible using a five-digit zip code is 100,000 (i.e., the zip codes 00,000 to 99,999). Similarly, the maximum number of addressable bytes of memory possible with 32-bits is 2^{32} = 4,294,967,296 —i.e., 4 gigabytes of memory. As computer manufacturers continue to increase the amounts of primary memory, a 64-bit operating system can address them while a 32-bit system cannot.

   Even now, however, a standard feature of all Windows operating systems is their ability to use hard-disk memory to augment the primary memory of your computer. This "virtual memory" overcomes most RAM space deficiencies and allows computers with small RAM capacities to run programs requiring larger amounts of primary memory.

   Having said this, we also note that the relentless expansion of RAM in today's personal computers continues and generally speaking, more of it is a good idea. Someday soon, personal computers will need massive amounts of primary memory to function efficiently. But that day is not here yet.

3. **Claim:** I need two monitors to work efficiently.

   Reality: It is true that two monitors allow you to see more area than a single monitor—for example, to simultaneously view an accounting application on one monitor and an Excel application on the other. In this sense "more" is always better. But is it necessary? For some individuals, it's true that the ability to see more will help them perform better. For most people, "more thinking" is preferable to "more viewing." If you install two (or more) monitors on your desktop, make sure you and your employees know how to use them efficiently. For example if you use Excel or Excel-based engagement software, you can configure the program to open a new instance with each document instead of just opening the document. This will allow you to move one document to the other monitor and, for example, copy and paste information from one Excel file to another more easily. For review tasks, having two monitors is especially helpful when references/tickmarks are in different documents/files.

   User note: If you do install two (or more) monitors on your desktop, make sure you and your employees know how to use them efficiently. For example if you use Excel or Excel-based engagement software, you can configure the program to open a new instance with each document instead of just opening the document. This will allow you to move one document to the other monitor and copy information from one Excel file to another more easily. For review tasks, having two monitors is especially helpful when references or tick marks are in different documents/files.

4. **Claim:** I need a duplex printer that can print on both sides of a page.

   Reality: In today's ecologically-sensitive arena, two-sided printing saves paper and perhaps storage costs, and therefore conserves resources. But do you really need an expensive printer to achieve these goals? When creating multiple copies of a document, a duplicating machine set to "two-sided copy" can usually do the job faster and cheaper. The fact that many people prefer one-sided manuscripts is also worth noting here. Exactly who is going to be happy with two-sided copy? Finally, the storage-cost argument is worth a second look. If storage is important, why not avoid hard-copy storage entirely and save documents electronically? Using dual monitors efficiently (see myth #3 above) can eliminate the need of printing documents for review.

5. **Claim:** If you don't eject or remove your USB storage device correctly, you will damage or lose the data stored on it.

   Reality: This is rarely true. An occasional error when removing your USB storage device doesn't damage the device. If you unplug your USB drive while your computer is writing data to the USB, it is possible to corrupt the data or files. Most USB storage devices now have a small LED that indicates write activity. Waiting until the computer has saved your data is best. If you unplug too early, simply reinsert your USB device and try to open your file. If your computer doesn't recognize your USB drive, remove it, wait a few

seconds and reinsert it. Other options include rebooting or running the "Add Hardware" wizard.

6. **Claim:** You need to defragment your hard drive regularly to keep it from slowing down.

   Reality: In this context, it may help to liken the storage space on your hard drive to a series of postal mail boxes—i.e., discrete locations where your computer stores data. Now imagine that you are a postal patron who rents several mail boxes from the same post office station. Just as you would find it more convenient to retrieve the mail from all your mail boxes if those mailboxes were physically close to one another, a computer operating system finds it convenient to retrieve the data from a single file if the separate file "fragments" or pieces are near to one another on a hard disk. Defragmenting a hard disk means rewriting file segments so that they are closer to one another and therefore more accessible.

   The question isn't whether defragging a disk drive makes things more "convenient," but whether it makes the reading or writing rates of the disk faster. In this matter, things are less clear. It is possible to achieve faster access, but many other items are also at play a role here, including the size of the file to read or write, the read/write speeds of the disk drive itself, and what other actions are competing for operating system resources at the time a disk read or write request occurs. Defragmenting your hard drive might help, but in most cases it won't.

7. **Claim:** Keeping your email open at all times makes you more efficient.

   Reality: While having your e-mail open all the time may be viewed as useful, time management experts suggest only checking email periodically at prescribed times. This removes the distraction and urgency factors associated with keeping your mail client active at all times.

8. **Claim:** Leaving my computer on all night saves me time when I access my emails in the morning.

   Reality: This is not a myth, but it's not necessarily a good idea either. Let's begin by conceding that leaving a computer on all night *does* save boot-up time in the morning. We also acknowledge that a machine that is "always-on" facilitates system updates, which can be disruptive and are therefore better performed when you're not using your computer for other things. Finally, we admit that no one likes to wait while a computer boots up, and that leaving a computer on all night does hasten access to email and the other applications you left running from the day before.

   The reason leaving your computer on over night is not a good idea is because a machine with constant access to the Internet is also a computer that is continuously exposed to hackers. Connected computers also increase their potential use as "zombie" devices for denial-of-service attacks on others. Finally, "always-on" computers are always available to anyone walking in the door. It is for these reasons that many companies expressly

require employees to shut down their computers at night. Last but not least, turning them off also saves small amounts of power and wear and tear.

9. **Claim:** To get less SPAM, you should click on the "opt out" links provided in the sender's emails.

   Reality: Many legitimate companies follow opt-out rules and will remove you from their email lists if you ask them. But what illegal spammers do isn't so clear. The problem is "How will you know whether you are dealing with a legitimate company or an illegal spammer?" For this reason, many experts advise against replying to opt-out invitations because doing so (1) validates your email address, and (2) indicates to the spammer that you read questionable emails. Why trust someone who is spamming you in the first place?

   There are better methods for weeding out junk mail. The large amount of spam email has spawned a market for spam filters: additional software that you can acquire to reject unwanted email. Many of these work well but may also filter out legitimate email. Another solution to this problem is to adopt a "policy of inclusion" for your email system—i.e., a system that only accepts email from listed senders and rejects all others.

   Our best advice for controlling email spam is to use caution when *providing* your email address to anyone. No law says you must give out your email address in data-entry applications, and the best "opt-out rule" is leaving that box for your email address blank. If you must provide an email address, consider using one of the free services such as Gmail, Hotmail, MSN or Yahoo.

10. **Claim:** Social networks are fun, safe ways to "get your information out there."

    Reality: Social networks can be dangerous with regard to information privacy. One downside is the potential for third parties to post information about others. Also, many employers now search the more popular social networks such as Facebook, MySpace, Twitter, and LinkedIn to see if potential hires have posted anything derogatory. Obviously risqué photos, talk of drug use, rants, etc., may affect an employer's decision to hire.

    While it may be potentially useful for your business to "be connected" in order to attract clients and employees, people need to use discretion and think long term before posting private information. Once you post something online, you can't take it back. For CPAs, instead of using a social network, you may want to consider creating a very good company website that provides useful information to potential clients and employees. Try to keep the website current and interesting – possibly by adding one or several blogs about tax and accounting-related issues. This is also a fun way to involve employees in the upkeep of the website. If the blog is interesting and well-written, it will attract traffic to the website and could help in retaining more business.

User Note: Instead of using a social network, CPA's may want to consider using their own company website to provide useful information to clients and employees. You should try to keep the website current and interesting—for example, by adding blogs about accounting-related issues or current, local events. This is also a fun way to involve employees in the upkeep of the website. If the blog is interesting and well-written, it will attract traffic to the website and could also help in retaining business.

11. **Claim:** You can damage files or the Windows operating system if you don't properly shut down your computer.

    Reality: While it is true that turning off your computer without shutting down Windows might corrupt data files or fragment your hard drive, you shouldn't be too concerned about making this mistake. Tests show that the files from multiple applications on Windows XP-based systems rarely incur damage when you do not shut down correctly—at least up to the last time files were saved. Application recovery systems work well, as they should. In this sense, data losses are similar to those suffered during power outages or fluctuations. Most operating systems can handle such occurrences but you might lose data that was not saved prior to the outage.

12. **Claim:** To maximize the life of your laptop battery you must let it drain down to zero charge before recharging or it will create a charge level memory.

    Reality: While draining laptop batteries was a good idea for older, nickel-cadmium batteries, modern lithium batteries do not suffer from this problem. At one time, nickel-cadmium battery performance degraded if the batteries were not discharged completely every few months. This problem was solved with battery conditioners. Lithium batteries should be drained occasionally so that system calibrations concerning the desktop fuel gauge remain accurate. But frequent battery draining is not necessary.

13. **Claim:** Turning your computer off every day shortens its life.

    Reality: The jury is still out on this question. Some argue that the daily cycling of the computer power supply stresses many of the computer components. There is some truth to this but most processors function for many years without difficulty in both scenarios. The central processor does not appear to be harmed by turning off the power supply daily. There was some debate concerning stopping and starting hard drives, but most concerns were for older drives, not modern ones. Software shouldn't have a problem with daily startups and it might be helpful to the operating system. As we know, most operating systems benefit from a reboot when they are having difficulties. Restarting occasionally has the added benefit of clearing "memory leaks" (unreleased or improperly released memory). So a daily restart probably is not a serious issue.

14. **Claim:** If I own a Mac, I don't have to run virus scanner software because Macs are immune to viruses.

Reality: All brands of computers are subject to viral attacks. The reason most people don't get viruses when using a Mac is that the "bad guys" know that the majority of personal computer users in the world are running Windows-based operating systems. This means that there is less opportunity to execute code against specific vulnerabilities. As of June 2008, it was estimated that one billion personal computers were operating. About 15 million of these are thought to be Apple computers. If you own a personal computer, use a virus scanner. Keeping the virus definitions up to date will ensure that your files and data are not damaged and that your computer is less likely to become a "zombie."

15. **Claim:** The cookies written on my computer track everything I do on the Internet.

Reality: Cookies are very small files that some web applications write on the hard drive of your computer. First, not all of the websites you visit write such files. Even when they do, however, not all such files are necessarily "bad." Some can actually improve your web experience. For example, one cookie can keep you from viewing the same advertisement more than once, while another can remember the information in an order form in the event that you accidentally lose connection to the Internet before completing a transaction. Finally, some cookies remember important passwords or login names for you, sparing you the trouble of entering such data repeatedly. While it is true that cookies can indirectly track your website visits, most merely serve to customize your interaction with Internet websites.

A final point to remember is that you can easily delete your stash of cookies or turn off the cookie-writing feature of your web browser. To do so using Internet Explorer 8, for example, select "Tools" from the Main menu, and then "Internet Options." About half way down on the General tab of this menu, you will find "Browsing History" and a "Delete" button within this section. Clicking on this Delete button allows you to selectively pick what items you want your browser to delete, including temporary Internet files, cookies, website visit history, or passwords. You can also view (and delete) selected temporary Internet files by first clicking on the "Settings" button in this Browsing History portion of the Internet Options menu and then click on View Files button on the subsequent dialog screen.

User note: We suggest you use caution before disabling the cookie-writing or password-saving features of your browser. Many sites are unusable if you turn off cookies, and of course, your computer will no longer remember viable passwords for you if you do.

16. **Claim**: Accessing files on your computer(s) remotely is dangerous because your computer is more vulnerable to an attack.

Reality: Remote desktop access allows users to connect to another networked computer. Most modern operating systems such as Windows, Mac OS X, and Linux/Unix include a remote desktop client. While logging on to your computer remotely can be quite useful for various reasons, there are still two major issues to consider:

- Security: Make sure that your remote-access application is secure and does not allow third parties to hack your system. Most remote desktop systems use 128-bit encryption for this task, although a few older systems are less secure.
- Speed: Remotely accessing files can be computationally cumbersome because of the significant decrease in speed. If this is the case, accessing your files remotely from a client's office may not be a feasible option. If remote access is important to you, you may need a connection with more bandwidth.

17. **Claim**: You should not use VoIP because it is not secure and cannot guarantee the same quality that regular phone services can.

Reality: There are two separate issues here:

- Security: Neither VoIP (voice over Internet protocol) nor regular phone service can guarantee absolute security because both are subject to packet-sniffing intrusions when using wireless transmission. Compared to regular phone service, however, VoIP is more secure due to its encryption capabilities.
- Quality: This can be an issue because of the complexity of VoIP. This is akin to a bicycle being more reliable than a car because the car is a more complex vehicle than the bike. However, it is usually the "voice" portion of VoIP quality loss that matters not the data-transmission portion. Voice quality may suffer because of technical issues like network contention and latency, which basically create a voice "traffic jam" on the network. Generally, these are no longer an issue because of smarter and better networking gear that is supporting packet prioritization technologies. VoIP technology is usually more efficient than a regular phone because multiple calls can pass down the same wire at the same time (traditional phone lines have dedicated wires). For example, an old system using a CAT5 cable can support four simultaneous calls. With a VoIP system the same eight wires in the CAT5 cable can support thousands of simultaneous calls.

In addition to these issues, it should be noted that VoIP can provide powerful tools to enhance productivity such as unity messaging, a feature that allows you to pickup your voice mails in your email inbox, "roaming" landlines where your phone network follows your physical location, or geographically dispersed private (and "local") phone systems.

18. **Claim:** You should use a screen saver to keep your monitor from "burning in" whatever stays on the screen.

Reality: While modern screen savers are entertaining, they do not protect most monitors from "phosphor burn." A better way to protect your monitor is through the Power Management module in the Control Panel. This directs your monitor to go into Standby mode after a specified time period instead of starting a screen saver.

As a side note, screen savers can perform a security function by requiring users to enter their system passwords when returning to a computer after a screen-saver display begins. To require a password on return from screen saver using Windows XP, for example, go to the Control Panel, click on the "Display" icon, and then select the "Screen Saver" tab.

Select a screen saver from the drop down box and set your wait time (the idle time before your screen saver kicks in). Then, check the box that states "On Resume, Display the Logon Screen." Your system will be more secure, requiring the entry of the password before allowing access to the other components of your computer.

19. **Claim:** Most computer viruses are created by teenagers having fun.

Reality: This may have been true in the early days of computing when hackers were people who liked to tinker with computer systems. Today, most viruses and Trojans are created to hijack an individual's identity or steal credit card information for use by organized crime rings located around the world. The black market for stolen identities, which are used to illegally acquire goods or services, is big business, not idle entertainment. So, don't think you are trying to protect your computer systems from prankster teenagers.

You want the best security protection you can afford to protect from the criminal element. At the time this article was written, the top ten anti-virus software packages, as rated by TopTenReviews.com, were, in rank order: (1) Bit Defender, (2) Kaspersky Anti-Virus, (3) Webroot, (4) Eset Nod32, (5) F-Secure, (6) AVG Antivirus, (7) McAfee, (8) G-Data, (9) Norton, and (10) Trend Micro. Given that (1) virus attacks have been the number one problem reported by the Computer Security Institute annual computer crime survey for the last several years and (2) none of these anti-virus software packages costs more than $40 acquiring and using anti-virus programs is imperative for CPAs. As an added bonus, many of these packages indirectly protect individual privacy by blocking Trojan horses from compromising computers or transmitting personal data to the criminals behind them.

20. **Claim:** Fake websites and spam are easy to spot and avoid.

Reality: The Internet today is a dangerous place for those lacking protection. Sophisticated programming tools allow people with criminal intent to create believable "phishing sites" and spam. They take advantage of vulnerabilities on websites and add programming to hack your computer. This type of inserted coding on websites facilitates "drive by" attack code. You visit a legitimate site, get attacked and don't even know it. Spam email is just as susceptible. It is therefore imperative to keep your security and firewall software current and to make sure that you have Windows update keeping your operating system up to date.

Conclusion

Marketers and retailers sometimes exploit the ignorance of shoppers by convincing them to buy hardware or software they don't need. After all, sellers are in the business of selling, not consulting, and they don't make any money by convincing you that you *don't* need new merchandise.

Misconceptions about computer systems would not be a big problem if they were not so widespread. To us, not buying a dual core processor makes sense while acquiring anti-virus software is vital to protect against systems against unwanted software bugs. Understanding why some claims are myths while others can be true can make CPAs more informed shoppers as well as more helpful consultants.