The Rochester Computer Society, Inc.
Since 1982

MONITOR

Vol. 31, No. 4 April 2013

Contents

Do You Still Need a Landline? Bob Rankin 1
Ten Tips: Identity Theft Protection Bob Rankin 2
Phone Scammers Want to Hijack Your Computer Ira Wilsker 5
Extending the Life of Your XP PC Dick Maybach 10
Speccy: Another Useful Utility Phil Sorrentino 12
Ask Mr. Modem 15
Living in the Past? Computing in a Software Museum John Davey 17
How Do Viruses Spread? Bob Rankin 20
Gizmo's Freeware 20
Society News 22
The Lighter Side 23

apcug Member of the Association of Personal Computer User Groups

Do You Still Need a Landline?

by Bob Rankin
askbobrankin.com

Between mobile phone service and free VoIP options such as Skype, does anyone really need to keep paying for a traditional landline? Many families have decided they don't. But before you cut that cord, there are some things you'll need to consider...

Is a Phone Company Landline Still Necessary?

As you look for ways to trim your household budget, your gaze may fall on that dusty landline telephone languishing in the corner of the kitchen. The bill continues to arrive each month, even though it's rarely used. Mobile phones are ubiquitous, and free internet calling options abound. (See my article about Free Internet Phone Calls.) So do you really need to keep that old-school landline active?

Overall, about a quarter of Americans have ditched landlines. Landline-only households fell from 34 per cent to 13 per cent between 2005 and 2010. About 29 per cent of children live in homes without landline service. About 40 per cent of poverty-level households rely on wireless phones alone. Nearly 18 per cent of households receive nearly all of their calls on wireless phones despite having landlines. Still, there are some good reasons to maintain a home landline.

RELIABILITY: Landlines provide redundant protection against service interruptions. They don't depend on household power or batteries (except for cordless phones). Internet service and cellular towers may be knocked out by natural disasters or power failures, while landlines are more likely to continue functioning.

Given the popularity of mobile phones and carriers' reluctance to invest in adequate infrastructure, it is not surprising to see network overloads during natural disasters or power outages. In the aftermath of Hurricane Sandy, cellular phone service was knocked out for several days along the eastern U.S. coast. The well established landline network's capacity is not as strained during emergencies, and is more resilient to damage, as much of the copper wire infrastructure is underground.

EMERGENCY SERVICES: When you call 911, a landline automatically provides your physical address directly to dispatchers, speeding the arrival of police, fire, or medical assistance. Commercial VoIP (internet phone) services such as Vonage may have emergency service, but it may not be available in some areas. If you use a free VoIP service such as Skype or Google Voice, forget about E-911.

Cellular services may not precisely pinpoint a caller's location; they may be off by a dozen blocks. Emergency dispatchers then have to get location data from panicked, error-prone callers; in certain cases, callers are not even capable of speaking.

Want to learn about free phone calls? See my ebook *How To Make Free Phone Calls on Amazon.*

WARNING, DANGER! Another consideration is alarm and monitoring systems. If you have a system that automatically calls police, fire, or other emergency services, it probably relies on landline service. Some systems can work with VoIP phone service, but that assumes you've got power and a working Internet connection.

It's best to think of a landline as optional insurance. Evaluate the risks in your own household. Do power outages happen often? Do you get "network busy" errors or dropped wireless calls frequently? What is your VoIP provider's emergency service provision? What is your tolerance for risk? Having a nearby neighbor with a landline may be a mitigating factor. And of course, if you keep a landline, you should also have a corded phone that doesn't require an electrical outlet or battery.

Weigh these factors against the cost of a landline carefully. And remember that mobile phone service is not necessarily cheaper, especially if you have multiple phones in the household. (See my related article Five Cheap Mobile Phone Plans, if you want to explore low-cost options.)

TEN TIPS: Identity Theft Protection

by Bob Rankin

askbobrankin.com

A new study shows that identity fraud increased in both 2011 and 2012, affecting over 5% of U.S. adults. Big spikes were noted in 'new account fraud' and 'account takeover fraud' – two of the most damaging types of ID theft. And those damages amount to about twenty billion dollars a year, reason enough for any consumer to be on guard. Read on for my tips on avoiding fraud and identity theft...

Ten Ways to Protect Yourself From Identity Theft

Identity theft is one of the most traumatic non-violent crimes to which one can fall victim. When a crook uses your good name to commit fraud or robbery, the impact on your reputation, employability, and credit is severe and can last for years. It's even possible to find yourself arrested for crimes you did not commit. So it's important to protect yourself against identity thieves.

The telltale signs that your identity has been stolen can be subtle and go unnoticed for months, even years. Inexplicable charges on your credit card bill may be chalked up to clerical errors. Letters from creditors you've never heard of and certainly never did business with may be ignored. But eventually, an enormous credit card bill, legal papers or police show up at your door. You are denied a mortgage or a job. Then the real nightmare of proving "I didn't do it" begins.

Prevent Identity Theft

It can be maddeningly difficult to clear your name, costing hundreds of hours and thousands of dollars. That's why it's important to take steps NOW to make it as difficult as possible for a scammer to victimize you. Take action on these ten tips as soon as possible, and you'll tips the scales in your favor:

Check your credit report on a regular basis, to see if there is any incorrect information, or accounts you don't recognize. My article Free Credit Reports Online explains how U.S. citizens can get three free credit reports per year.

Shred your sensitive personal documents before throwing them away. A battery-powered cross-cut shredder can render your banking and credit card information unreadable and costs less than $30. "Dumpster diving" is a favorite, low-tech way by which ID thieves collect bank statements, credit card numbers, Social Security Numbers, and other bits of your identity from your trash.

Be wary of telephone solicitors asking for personal or financial information to "verify your identity." Common scams involve someone who claims to be from your bank or credit card company, claiming that there is a problem with your account. If you did not initiate the call, hang up and call the toll-free number on your statement, then ask for the security department.

Keep important documents, such as tax returns, birth certificates, social security cards, passports, life insurance policies, and financial statements secure in your home. A fireproof safe is a good idea, but remember to bolt it to the floor or hide it well.

Make sure no one is looking over your shoulder when you enter your debit card's PIN at an ATM or point-of-sale terminal. I recommend the "two finger method" where you point two fingers at the ATM keypad, but only press with one. This makes it nearly impossible for someone nearby to discern your PIN while you're entering it.

Memorize PINs, account numbers, and passwords; do not write them down. And for heaven's sake, do not put such data on scraps of paper kept in your wallet, purse, or laptop case!

Get blank checks delivered to your bank branch, not to your home mailbox from which they may be stolen. On a similar note, eliminate junk mail which may contain "convenience checks" and credit card offers that can also be intercepted from your mailbox. Visit the Privacy Rights Clearinghouse and OptOut Prescreen for help eliminating these dangerous nuisances.

When you order a new credit or debit card, mark the calendar and follow up promptly if it does not arrive within 10 business days. Ask the card issuer if a change of address request was filed, and if you didn't do it, hit the panic button.

Don't give your Social Security Number to any business just because they need a "unique identifier" for you. Instead, ask if you can provide alternate proofs of identity, such as your driver's license or birth certificate.

Consider placing Fraud Alerts with the major credit bureaus, so new accounts cannot be opened without your knowledge. Call Equifax (800-525-6285), and they will pass along the request to both Experian and Trans Union. Fraud alerts expire after 90 days, so you can repeat the process quarterly, or lock down your credit file with a Credit Freeze. A freeze is permanent and free (in most U.S. states) but it may interfere with loans applications, employment screening, signing up for utility or phone service, new insurance policies, and other transactions. You'll also need to contact each credit bureau (Equifax, Experian, and Trans Union) to request the credit freeze.

There are plenty of common sense things you can do to protect against identity theft, but sometimes it's beyond the control of even the most vigilant. The Javelin Research 2013 Identity Fraud Report found that data breaches perpetrated

on large companies proved to be a "treasure trove" of data that could be used to commit identity theft and fraud. And before you put too much blame on those big corporations, check yourself. Security firm McAfee says that when a relationship ends, it's quite common for an angry ex to engage in revenge tactics, which may involve exposing your personal data or passwords. So be careful what you share via email, text and social media. And keep passwords close to the vest.

What About LifeLock?

You may be considering LifeLock or a similar identity theft protection service. Although this can be helpful, no company can guarantee that identity theft will never happen. These services monitor your bank account, and look for suspicious online activity done in your name. They'll alert you if they spot any red flags and promise to help you repair the damage. But because of lawsuits filed by the credit bureaus, Lifelock can no longer place fraud alerts on your behalf. Also, all identity protection services are barred from offering Identity theft insurance coverage to residents of New York state.

It can be a nuisance to manage fraud alerts manually. But given the recent focus by scammers on new account fraud and account takeover fraud, a service such as LifeLock, Identity Guard or Trusted ID may still be useful. Most cost about $10/month, which isn't much for the additional peace of mind they offer.

Back Again - Phone Scammers Want to Hijack Your Computer

by Ira Wilsker

Early last year, I wrote a column here warning that telephone scammers, claiming to be from Microsoft, were calling local people, informing them that their computers were infected with malware. The rip-off had seemed to be somewhat dormant for several months, with only occasional inquiries from people asking about a phone call from Microsoft, Norton-Symantec, McAfee, or their ISP alleging that their computers were infected, and that for a fee and with remote access, they could repair the computer. During a few week period in late 2011, I heard from many people that they had received such calls, but for the last 15 months, I only received an occasional inquiry. Now, in just the last few days, I have received several such calls and emails indicating that either by plan or coincidence, local computer users are again receiving those calls in quantity.

Last Friday evening, I received a frantic phone call from an acquaintance indicating that he and his wife had received a half-dozen calls over the past few hours, many irate, from foreign accented individuals claiming to be from Microsoft. These "Microsoft employees" needed immediate remote access to stop the victim's computer from spreading malware, and that Microsoft had detected hundreds of viruses and other malware coming from their PC! Demanding that they, the crooks, needed to take immediate remote control of the victims' computer, in order to prevent the spread of computer viruses. The first polite request was denied, followed a short time later by a second telephone request, also denied. The third

telephone request was somewhat irate, demanding immediate access to the victims' computer. A fourth, fifth, and sixth call over a period of a few hours became much more irate and belligerent, demanding immediate access. The distraught victim then phoned me, asking if Microsoft really needed to take control of his computer in order to clean off viruses; I told him no, that this was a well documented scam, and to simply hang up on them if they called again.

Later Friday evening, I received an email from another friend, "Is there a scam going on with someone calling on the phone to notify us that there has been a problem on my computer, and that they can directly connect into all Windows users?" I replied promptly, that this was also a scam. Saturday afternoon, I received a phone call on one of my digital phone lines that has an unpublished number that I had never given to anyone outside of my immediate family. This call showed no name on the caller ID, but appeared to be from the 559 area code (Fresno area of California). The caller had an unusual accent, and the voice quality sounded like it was a foreign call. A quick check indicated that the call was possibly a VoIP (internet relayed digital call) coming through a node near Fresno, and then on to the domestic phone network. While I have no empirical evidence to prove it, I would make an educated guess that the call originated from Nigeria, a common source of this and many other internet scams. Similar scams have been traced to India, Pakistan, the Philippines, China, Vietnam, Russia, and other south Asian countries.

Being fully cognizant of the nature of the scam, I decided to play along with it. This very polite gentleman, with the foreign accent, informed me that he worked for Microsoft, and that Microsoft had detected that my computer was responsible for infecting other computers with several viruses. Very kindly, he offered to perform a remote security scan on my computer if I would only allow him to remotely access it. Trying hard to sound somewhat cyber illiterate, I asked him how he could remotely perform a scan, and he told me that all I had to do was click on my Windows 7 icon (orb) on the bottom left of my screen, or click on the "Microsoft Menu" key on the bottom left of my keyboard, and then follow his instructions. Pretending to be somewhat unsure of myself, I had him walk me through the process; open my menu, and then click on Control Panel, then System, then click on "Remote Settings" on the left side of the window. When the next window opened, he instructed me to click on the remote tab, and then to check the box "Allow remote assistance connections to this computer." I hesitated, telling him that I was not comfortable doing this, and in a reassuring voice akin to the classical "Trust Me" ruse, he assured me that all that he was going to do was a comprehensive virus scan on my computer to verify that it really was my computer that was broadcasting viruses to other computers. Knowing what would be coming next, I asked him if his virus scan would remove the viruses for me. Very politely he responded no, that this was just a virus scan, but for a "nominal fee" he could remove any viruses that he found from my computer. A follow up inquiry disclosed that this "nominal fee" was $69.95 charged to a credit card number that I would give him over the phone. I told him "no thanks," but before I could hang up the phone, he pleaded with me to trust him, and allow him remote access to my computer. With a stern "NO!" I hung up the phone.

This was not just some isolated or random event; in the past few days another co-worker received a series of similar phone calls in his office from a very persistent caller who would not take "no" for an answer. Shortly after hanging up on him, he called back again, with the same response. A few minutes later, he called back very angry, demanding remote access to his work computer, which was duly refused. Moments later, someone claiming to be a "supervisor" demanded access "right now" to his computer; he called me over to talk to the scammer. The "supervisor" said that he was with Microsoft in India, and that it was mandatory that I give him remote access to this computer immediately. My curt refusal was met with a somewhat threatening reply that I would be in trouble for refusing him remote access to this computer, and that I would regret it.

According to those that have fallen victim to this crude scam, the repeated scenario is the crook asks the victim to allow him remote access to the victim's computer by clicking on some Window's commands, allowing the crook complete remote access and control of the computer. Once the crook has control of the victim's computer, he regretfully informs the victim that his computer is heavily infested with malware, and that for a fee, typically $69.95 (but it may vary greatly), he can clean the computer and return control to the victim. What the cyber-thief does not say is that while he is performing the security scan on the computer, he is likely to download (steal) documents, spreadsheets, personal information, emails, address books, password files, and other valuable data from the computer. It is also not uncommon for the bad guys to install malware such as keyloggers and screen capture utilities to steal usernames and passwords for the purpose of identity theft. If a credit card number, expiration date, and CVV security code are given to clean the computer, not just is the card charged for the service (often for much more than the agreed upon price), but the credit card information also often appears for sale on the illicit websites selling credit card numbers.

The number of people victimized by this scam may be much larger than previously known. According to a report on this scam, published June 16, 2011 in "The Register" (UK), "The software giant (Microsoft) surveyed 7,000 computer users in the UK, Ireland, US and Canada and found an average of 16 per cent of people had received such calls. In Ireland this rose to a staggering 26 per cent." Personal losses can be quite dramatic for those victimized by this and similar scams. In this same report, "(Microsoft) said 79 per cent of those tricked suffered financial loss – the average loss was $875 (£542). Losses ranged from just $82 (£51) in Ireland to a whopping $1,560 (£967) in Canada." (Source: theregister.co.uk/2011/06/16/tech_support_scam_calls)

Scams such as these have been around for several years, and reputable organizations, news services, and blogs have been warning about them. In several locations, Microsoft has emphatically stated, "Neither Microsoft nor our partners make unsolicited phone calls (also known as cold calls) to charge you for computer security or software fixes." (Source: www.microsoft.com/security/online-privacy/avoid-phone-scams.aspx). Be especially aware if a person over the phone offers to remotely install "genuine" Microsoft security software for a fee, since Microsoft makes this same software available to anyone for free.

If you are one of the many victims of this scam, Microsoft and others have published a series of recommendations to follow. First, if you gave the crook your credit card number, immediately contact you credit card company using the 800 number on the back of your card, and cancel your card, requesting a new one. Over the phone, the customer service representative can list your recent charges, and may give you an opportunity to question them right away. Look carefully at any recent charges on your online or paper statement, and challenge any illicit or unknown charges with the credit card company. Next, perform a complete security scan of your computer using security scanners other than the security software already installed on your computer. Since your current security scanner and protective software may have been neutralized by the cyber crook, perform a scan with one of the major third party security scanners; my personal favorites are the free versions of SuperAntiSpyware (superantispyware.com) and MalwareBytes (malwarebytes.org). Once your computer has been satisfactorily cleaned of any malware that the scammer may have installed, it may be necessary to reinstall your security software. Change the password that you use to logon to your computer, and any other passwords that you use to access your email, financial accounts (including banks and credit cards, as well as such services as PayPal), online retailers (including eBay), and any other passwords that you may have used. After doing what you can to mitigate the damage done, consider filing a complaint with the Federal Trade Commission using the "Complaint Assistant" at www.ftccomplaintassistant.gov.

Please, do not fall victim to this scam which is again targeting mainly local residents. If "Knowledge is Power," then now you have the power to protect yourself from this and similar scams.

WEBSITES:

http://www.microsoft.com/security/online-privacy/avoid-phone-scams.aspx

http://answers.microsoft.com/en-us/windows/forum/windows_vista-security/scam-phone-call-claiming-to-be-from-windows/193f0a33-4ad9-4a07-96eb-9a7e3debb269

http://answers.microsoft.com/en-us/windows/forum/windows_xp-security/phone-call-scam-received-call-from-a-technician/6ed2b99c-20ff-468b-a69b-aec78b93f287

http://www.theregister.co.uk/2011/06/16/tech_support_scam_calls/

http://windowssecrets.com/top-story/watch-out-for-microsoft-tech-support-scams/

https://www.ftccomplaintassistant.gov/FTC_Wizard.aspx?lang=en

Websites to Broaden Your Computer Horizons

by Jim Fromm

Editor, MOAA Computer User Group, HI

Because a number of you (I mean us) fall in the senior age group, and because some of you (I mean us) may be thought to lead a sheltered life, I thought it was time to offer to broaden your computer horizons.

So, I'm providing you with a laundry list of websites that you can visit and decide yourself if you want to bookmark them. It's never a disadvantage to be informed of what is happening in the world. News, opinions, human interest, goofy and technical sites are included.

There are innumerable websites on the internet covering every topic imaginable. Some are toxic to the sensibilities. Some are dedicated to historic events. Many are opinion sites that cover all topics from art, to comedy, to topical news, anything you can think of, you can find on the internet. All have their own interesting element.

I must admit, I have become addicted to visiting numerous sites every evening. I can't remember the last time I watched TV after 7 PM. I'm usually at the computer after dinner surfing through a favorite list of blogs, news and feel good sites. It's my way of taking a break from the dismal news events of the day but still keeping current.

At many of the blogs you can read the headline without clicking on through to a link. If the topic does not interest you, scroll down to the next entry. With the talking heads on TV you have to suffer through the narrative and the frequent commercials or press the mute button. At a blog you don't have that problem.

Many of the opinion sites report news items and then give you opinions from one, or more, contributors, whereas the TV news casts spend mere seconds on a topic before breaking for commercial and oftentimes have a one-sided slant to the item.

The really fun part of these is the comments section. Which, I must warn you, can get pretty salty, so be cautious. If profanity offends you, be especially careful. F-bombs are strewn throughout some of the comments. A few blog hosts prohibit foul language and you'll learn which ones if you check out the listings.

I've categorized them so you can see the genre and pass on those that you know won't interest you.

Opinions – Far Right; Left and Far Left

www.instapundit.com
www.politico.com
www.slate.com
www.rightwingnews.com
www.maggiesfarm.anotherdotcom. com
www.huffingtonpost.com
www.twitchy.com—a compilation of tweets, and responses to them, from around the world.

Fun stuff— Animals and satire

www.cuteoverload.com
www.rumfordmeteor.com
www.flixxy.com
www.top20sites.com/

Tech stuff— Computers mostly

www.docmercury.com
www.pcworld.com
www.cnet.com

Arts and Music

www.classical.net
www.classical.com
http://www.deviantart.com/
http://www.fineartsites.org/

Novels and manuscript

http://tinyurl.com/c4x5vpm— Cincinnati Library list of books

http://manuscriptsonline.wordp ress.com/ (Research site)

http://www.bl.uk/manuscripts/ - British Library

A few of the sites listed require registration but no membership fee unless you sign up for their "premium" offerings. Quite a bit of the content is free to browse.

From the January 2013 issue of The TUG*, newsletter of the MOAA Computer User Group, HI.*

Speccy: Another Useful Utility

by Phil Sorrentino

Member, Sarasota PCUG, FL

Way back in November 2009, in the heydays of XP, shortly after the release of Windows 7, I started reviewing useful utilities. Along the way I reviewed some very useful utilities such as Stickies, MP3Tag, CKRename, and UltraFileSearch. Just as a matter of review, Utilities are usually small programs that are intended to do a specific task or a small range of tasks, they are small software application. Today, after the release of the Apple iPad and in the current Tablet environment, we would call these Utilities "Apps."

These Utilities (or Apps) are usually designed to help manage the computer hardware, Operating System (OS), or assist a particular software application. Just as a matter of history, sometimes a utility becomes so popular that the functionality of the utility is included in newer versions of the OS. The functionality of one long-time popular utility, Snagit, which allows a user to capture a piece of the display into a graphics file, is now included in Windows as the Snipping Tool. The functionality in Windows may not be as complete as the commercial version of Snagit, but it is a part of Windows, which means it is integrated into the OS, and therefore available at no additional cost.

Useful Utilities can be found in a variety of places such as computer stores (internet or brick & mortar), Google searches, and The Computer Buffet, edited by our own Monitor editor, Herb Goldstein. The Computer Buffet is a treasure trove of useful software, some of which can be considered Utilities, like Speccy, and some of which are full-blown application, like Open Office. Speccy was originally discussed in a Monitor article in the December 2012 issue. Speccy was developed by Piriform, the same company that brings us Ccleaner and Recuva, two other useful utilities that many SPCUG members have used. You can download Speccy at www.piriform.com/speccy. When you download it, be sure to uncheck the boxes for other things like the Google Toolbar, unless you want them to come along with the Speccy download.

Speccy is a Utility used to provide information about your computer hardware and Operating System. Speccy is very similar to Belarc, a Utility that is fairly well known and often used at the Refurbishing Facility. Belarc goes a little further and additionally provides information about the software and the software versions, installed on the computer. Just remember "I have not come to bury Belarc, I have come to praise Speccy." There is probably more information provided by Belarc, but what I like about Speccy is the visual organization and presentation. The initial results are presented in a two window-pane format, much like

Windows Explorer. Highlight an item in the left pane and you get detailed results in the right pane. The left pane includes the Summary and all the major computer subsystems; Operating System, CPU, RAM, Motherboard, Graphics, Hard drives, Optical drives, Audio, Peripherals, and Network. The Summary that is shown on the right pane after the program completes its initial analysis phase has the answers to many of the basic questions regarding this specific computer. Immediately you know the Operating System name and the Service Pack (if applicable), and whether it is a 32 or 64 bit OS, and the type of computer CPU. Other basics in the Summary are the amount of RAM, the size of the Hard drive, along with the drive connection type, and the Optical drive and its connection type. From the main menu you can Print any of the results or you can choose "Save as a Text file" and save the results for future review.

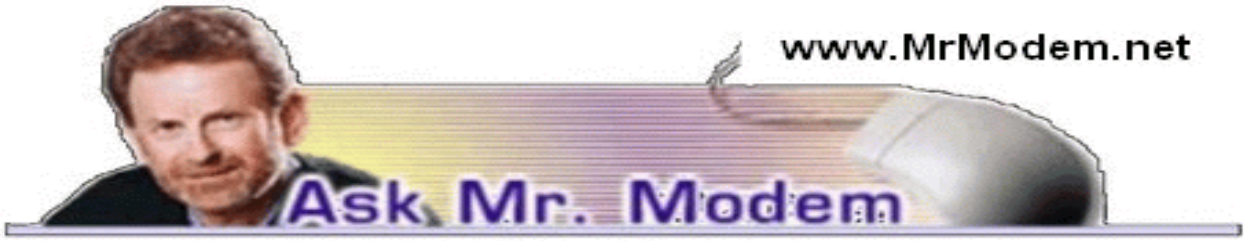
Details of the major subsystems, shown on the left, can be obtained by selecting the appropriate subsystem. Click on any of the major subsystems, and the details will be shown in the right pane. The details are very extensive, probably much more than the average computer user needs to know, but may be useful to someone trying to help solve a problem. Some of the detailed information provided by these subsystems is as follows:

- The Operating System subsystem shows the OS type (Windows 7, XP), 32 or 64 bit OS, the serial number, the Windows Update schedule, the Antivirus software installed and the age of its Virus Signature Database.
- The CPU subsystem indicates the number of Cores (today most modern CPUs are multi-core), the Bus speed, the Cache configuration, and the Average Temperature the CPU has been experiencing (if this is approaching 60 degrees C you may be in for some trouble, although the Critical Temperature depends on the specific CPU).
- The RAM subsystem shows the amount of RAM installed as well as the number of memory slots and the number of free memory slots (nice to know if you are thinking of increasing your memory).
- The Motherboard subsystem shows the motherboard manufacturer, the chipset (CPU and glue chips) vendor, and the BIOS brand and version number (things that you probably will never need to know).
- The Graphics subsystem provides information about your Monitor such as the Resolution, and the Graphics chipset (again probably never needed by the average user).
- The Hard Drives subsystem shows the Drive size, the File System type (FAT or NTFS), and the Partition information (nice to know if you think you will ever re-partition the drive).
- The Optical Drive subsystem indicates the Media type (CD or DVD), and whether or not you can write to the drive (Writer or Read-only).
- The Audio subsystem just shows the Sound Card and the Playback Device (usually speakers).
- The Peripherals subsystem indicates the type of keyboard and mouse, the Printers that are currently in use, and any external disk drives or USB memory devices attached.

- The Network subsystem provides all the IP addresses, DHCP status (enabled or not), the Computer Name and Workgroup (if it belongs to one), the Wi-Fi SSID (network name) and channel number (good to know if you are experiencing slow operation caused by interference on the network). Surprisingly, I didn't find the MAC (or physical) address of the communications adapters.

As you can see, Speccy provides a lot of information and is definitely a very useful utility. Download it and pin it to the task bar so it will be available and easily accessible when you need it. By the way, a printed version of the results might be nice to have for reference if the computer is down for any reason.

From the February 2013 issue, The Monitor*, newsletter of the Sarasota PCUG, FL. Courtesy of APCUG.*



What Causes >>> Marks in Email?

Q. I probably should not even bother you with this silly questions, but I'm curious: What causes all those >> marks that appear in the body of email? They can be very irritating and sometimes they even overshadow the text.

A. Those angle brackets are there by design, and depending on the email program involved, you may see >> marks or vertical lines, both of which designate replies or forwards. The number of marks or lines allows you to track the "depth" of a reply or forward. One >, for example, indicates it's the first reply or forward; >> indicates it's the second round of replies or forwards, etc. That's why when you receive a joke or hoax message that's been forwarded a bazillion times, you will often see >>>>>>>>>>> in front of each line. People deal with these marks in a variety of ways: Most simply ignore them; others delete them using their software's Find and Replace feature (CTRL + F in some applications). There are also programs that can be installed, such as PaperCut's eMail Stripper at www.papercut.com/emailStripper.htm or easy-to-use Web-based appli-cations such as the similarly named Mr. Ed's Email Stripper at www.mistered.us/stripper/index.shtml.

Q. When I want to go back and look at old email I received in Gmail, only the first 50 emails will come up and I cannot figure out how to access the next 50. While I'm at it, I can't seem to locate Gmail's Help, either. Can you help me with these issues, Mr. M?A. When viewing the Sent Mail folder, if you look in the top right of your Gmail screen, you will see numbers such as 1-50 of 214 with < and > arrows. That refers to messages 1 through 50. If you click the > arrow, you can view the next 50, messages 51 through 100, etc. To access Gmail's excellent Help, click the little gear icon to the far right, then select Help from the drop-down menu that

appears. Gmail's Help is one of the best there is, so any time you need to learn how to do something with Gmail, be sure to search its Help section.

Q. Please help me stop the very annoying Yahoo! Messenger from popping up when I boot the computer or receive email. It's driving me crazy!

A. Open Yahoo! Messenger when it appears, then click Messenger > Preferences or press CTRL + SHIFT + P. Under Category, click Alerts and Sounds. In the "Alert me when" box, click "I receive email in Yahoo! Mail." Next, uncheck the boxes next to "Display a dialog box," "Show an icon in the system tray," and "Show a message in the bottom right corner of my screen." Just to clarify these three options, "Display a dialog box" refers to the dialog box that pops up to notify you of new mail. "Show an icon in the system tray" references the little envelope that appears when new mail arrives. "Show a message in the bottom right corner of my screen," is the box that displays the subject of the message or how many messages are present. If you prefer not hearing the "Pow!" audible alert – and heaven knows why anybody wouldn't want that jolting the bejeepers out of them – uncheck "Play a sound." Lastly, click OK and you're done.

Mr. Modem's DME (Don't Miss 'Em) Sites of the Month

Behind the Name

Learn the history behind more than 18,000 first names. Search the diverse database of English, German, Spanish, Arabic, Mythological, Biblical, and African names. By gender, there are 9600 male names, 8000 female names, and 750 that could be either. Also included is a list of the most popular names in the world. The most popular name in the Netherlands? Daan. Good to know.

www.behindthename.com

Google Flights

Google has entered the flight-planning business (what aren't they into?) with Google Flights, which you can use in two ways: Using the Google.com search engine, type search parameters such as "flights from Phoenix to Dallas" and flight information will appear at the top of the search results. If you really want to dive into flight information, go directly to Google Flights and get precise results by using the filtering options, such as your preferred airline, desired number of stops, maximum number of screaming babies, etc.

http://google.com/flights

Rentometer

If you're a renter or if you have rental property, use this site to comparison shop and find the price of other rental properties in your area. Type in the address of the rental property, the amount you pay or charge for rent and how many bedrooms. When you're finished, click the Analyze My Property button. Results are displayed in two ways: A graph that shows rent on a scale with other area rents and segregated into Low, Medium and High categories. There is also a Google map that is bulleted to display other rentals in your immediate area. You can zoom in and out with the slider + and – navigation in the top right corner of the map.

www.rentometer.com

Use Promo Code GIZMO when entering your six-month subscription to Mr. Modem's award-winning weekly computer-help newsletter and receive one month for free! Visit www.MrModem.com.

Living in the Past?

Computing in a Software Museum

by John Davey

Workshop Leader, Cascading Style Sheets Workshop, Philadelphia Area Computer Society

It was at a recent meeting of my computer user group that it hit me – I do my computing in a museum.

It's not my hardware. My printers from several presidential administrations ago, and parts from 286 and 386 laptops, have all been delivered to the local recycler. Ditto that 19-inch CRT monster. (Though I did keep the Leading Edge Model D that started me off – you never know when you will need a fallback.)

No, I'm talking about software.

It was at the PHP session. The topic was email, and the session leader was talking about scripting an HTML email message. He threw in the suggestion to include a fallback version in case a subscriber was using an email client that did not display HTML. It was as if he was talking about writing a webpage for someone who might be using Netscape Navigator 4 – but I actually use an email program that does not display HTML pages, at least not with my setup. Not surprisingly, I was the only one in the group. And that got me thinking about how many software relics that I use at home, and even at work, and that I actually reinstall every time I buy a new computer.

Mail from Another Era

The email client goes back to the 90's. Java was a hot new platform, and OS/2 was competing with Windows as a PC operating system (that's a whole 'nother story). A developer built an email client in Java so that it could run on any operating system. It was called JStreet Mailer, and it was perfect for people like me who dual booted between OS's. I made it my email program.

As good an idea as it was, it did not take off. The developer ceased working on the mailer, but he was generous enough to release the source to some volunteer coders. They maintained it for a while as Polarbar Mailer. The last update was somewhere around 2003.

It is a very well thought out program, but needless to say, the feature set is behind the times. And frankly, under Windows 7, it freezes up regularly. I still use it every day, though. At this point, I have so many addresses and folders of saved emails that the task of migrating to a new program is too daunting to consider.

New Data, Old Base

My database program is even older. Back in the DOS days, when Lotus was its own company, they developed the 1-2-3 spreadsheet. When the transition to Windows came along, they purchased a great word processor called Ami Pro and renamed it Word Pro. And they purchased a database program called Approach. It was a relational DB, not flat file, and it was a good one. They put these together with some other programs and marketed the package as SmartSuite. They had both OS/2 and Windows versions, so this one was also perfect for dual booting.

Then came Microsoft Office -- enough said. The last version of SmartSuite was released around 2002. I bought that update for about $35 from a vendor at a computer show. Approach itself was worth many times that amount. I used it to learn how to design and build databases. I did one for my

passwords and another for our user group's attendance sheets, and I still use them both. The program may be behind the times, but it works, so I hang in there – again, it's too much of an effort to move.

A Pre-App App

Then there is my address book. I had forgotten this one until I went to do my Christmas cards.

I had a Palm III that I bought used from a guy back when Palm was the thing. It came with a nice desktop application that synched with the Palm and made it easy to enter information in either place. (You could also beam information between devices – remember that? The original Near Field Communications.) The Palm itself has long been retired, but there were so many contacts in that desktop program, it was easier just to leave them there. So every December, I crank up the Palm Desktop program to retrieve my old addresses for the holidays.

From the Days of DOS

I go even farther back with my diary program. It's not even a Windows application. Lotus again comes into play. The story is that Mitch Kapor, the mind behind 1-2-3, had a habit of keeping notes on slips of paper. Looking for a way to organize information the way spreadsheets organized numbers, he had Lotus develop a personal information manager called Agenda – running in DOS.

Agenda was my kind of program. It was a free-form database with calendaring functions and organization on the fly. I could create projects, enter notes, set up due dates, and track completions. I bought the first version from an online auction for a Boston PBS station, back when I used CompuServe for access – pre-internet of course. (I bought a 2400 bps modem at that same auction to upgrade from a 1200 model.) The second version of Agenda came out in 1992, and that was the end of development. When Lotus developed SmartSuite for Windows, it bought an organizer called – yup – Organizer. It just wasn't the same.

For whatever reason, I can't find a program that works my way as Agenda does. These days I have to run it in DOSBox. People coming by my desk want to know what website I am using or whether the program would work for them. I just tell them to find something else. It's too much to explain.

A Pioneer's Second Act

The last example is not as ancient, but I have never heard of anyone else using it. In the early days of PC's, before Lotus 1-2-3, there was VisiCalc, a prototypical spreadsheet designed by Dan Bricklin. It was one of the foundations of the desktop computer revolution. Years after VisiCalc, Dan developed ListGarden, an application that lets web designers convert website entries into RSS feeds. I found it because I was looking for exactly that type of utility, and it was literally the only one that I could find. I have been using it for years, and I know that it is time to move to a CMS that will handle news feeds, but here again, there is a lot of work to make that transition. It's on my to-do list. But for now, ListGarden does the job, and I appreciate it being available. I have searched in vain to find anyone else using it, so I guess I am a leftover.

All of this is not to say that I don't keep up with new things. I'm writing this article on a dual-monitor system using Office 10 and saving the document to Dropbox. I keep notes these days in OneNote. And I am learning Access for my database management.

But the old software still works well enough for now. So I'll hang onto Agenda for now – and wait for the next version.

How Do Viruses Spread?

by Bob Rankin
askbobrankin.com

All the advice you've ever heard about how to avoid getting infected by a computer virus may be wrong. Well, at least some of it... A new study shed lights on how viruses and other malware are most commonly spread in today's Internet environment. Read on for details...

Where Are Viruses Lurking on the Web?

The 2013 Cisco Annual Security Report includes some disturbing data about how malware (viruses, spyware and other nasties) infects millions of computers each year.

The surprising conclusion of the Cisco study is this: All of the advice you've received about sticking with known, trusted Web sites seems to be wrong. In fact, the more legitimate a site is, the more likely you are to catch a malware infection from it.

The report found that the vast majority of malware comes from mainstream sites visited by mass audiences, not from shady sites that relatively few people visit. E-commerce sites are 21 times more likely to deliver malware than counterfeit software sites, for example. Viewing an online advertisement, you are 182 times more likely to be served malware than you are when viewing porn.

Cisco looked at some major online applications and the percentage of total malware exposure found on each type:

Malware Rising: How Do Viruses Spread?

Search Engines: 36%
Online Video: 22%
Social Networks: 20%
Advertisements: 13%
Other: 9%

Obviously, legitimate sites such as Google, Bing, Youtube and Facebook are not trying to give you malware. But malware distributors strive to inject malware into the most popular sites, and the ones that people trust the most. You may be wary of clicking a link on a gambling site if you are not sure what it does, but you might not hesitate to click it while visiting your favorite search engine, online shopping or social media website.

Hackers are constantly looking for vulnerabilities in the software that powers websites. Sloppy coding practices may open the door for "SQL injection attacks," and "buffer overruns." Poor security and weak passwords may allow breaches where malicious code can be planted.

When Malware Attacks...

Once malware infects your computer, it can use your system's resources to spread itself even further. Malware may access your contacts lists and send phishing links via email to friends and family. It may re-direct browser requests for legitimate websites to rogue sites. Unknown to you, one malware

program may download and install others. Malware may copy itself to a networked computer, USB drive or other removable media that you insert into your computer. Email attachments, removable media, free software containing Trojan Horses, and file-sharing on home or office networks still play roles. It's as important as ever to keep your anti-malware program up to date and practice safe computing habits.

Web exploits are by far the biggest malware vector online. On the plus side, email spam is down 18% worldwide. Mobile malware accounted for only 0.5% of malware exposures in Cisco's Security Report, although Android malware instances increased over 2500% in 2012. (Take that number with a grain of salt, though. A large chunk of the Android malware problem comes from sketchy third-party app markets. See Do You Need Mobile Security Protection? for some additional advice.)

The moral of this story is: keep your guard up no matter where you are online. Don't ignore the warnings of your anti-malware program just because you're visiting a site that's familiar and trusted. It's entirely possible that site has been infected with malware since your last visit. And remember that you don't have to shell out big bucks for good computer security. See my article Free AntiVirus Programs for a list of free alternatives to Norton, McAfee and other commercial antivirus software.

A reader asks "How can I send a text message for free?" My mobile phone carrier gives me a small number of free texts, then charges me ten cents to send or receive a text. Is there a way to send a free text message?' Actually, yes! Here's how it works...

How to Send Text Messages For Free

Text messaging is a wildly popular feature of cell phones, and one of the industry's fattest cash cows. But ironically, the growing popularity of smartphones is threatening the enormously profitable SMS text message, as free text messaging services that use data connections challenge traditional cellular SMS service.

Text messages brought a whopping $20 billion to cell phone companies last year; Verizon alone earned $7 billion in text message revenue. Profit margins are high, too. The cost of delivering a text message is estimated at one-third of a cent. Most wireless operators charge 10 to 20 cents per text message, or a flat monthly rate of around $20 for unlimited text messaging. International text messages can cost even more.

Free Text Messaging

Free text messaging services have been around for several years. There are many web-to-phone text services like Txt2Day that let you send a text message from your computer to any cell phone. Txt2Day promises you won't get spammed as a result, and they won't share your number with anyone. And in order to prevent anonymous harassment, all messages are tagged with the sender's IP address. Txt2Day will provide this info to law enforcement when requested, and will also filter out most common "abusive" words. (NOTE: There are some "spicy" ads on the Txt2Day site.)

Unfortunately, you typically cannot receive a reply via these web-to-text services. One notable exception is the Pinger free web texting service. Pinger assigns you a free phone number, and lets you send and receive texts from a slick web-based interface that lets you view a log of messages sent and received.

Another is Google Voice's free text messaging service. You can text to any SMS-enabled phone in the U. S. or Canada for free, and receive replies. Of course, your correspondents will have to pay their carriers' usual text message charges.

Most mobile carriers also have an email-to-text feature that allows you to send a message to a special email address that forwards to the recipient's cell phone. For example, you can send an email to 123-456-7890@vtext.com, and Verizon will deliver it to the user with that cell phone number. If you want to send a photo, change the domain to vzwpix.com. Users on other major carriers can be reached as follows @txt.att.net (AT&T); @tmomail.net (T-Mobile); @messaging.sprintpcs .com (Sprint). For a comprehensive carrier list, see SMS gateways. Recipients can reply to your message, if their carrier allows them to send texts to an email address. The downside of course, is that you have to know in advance which carrier the recipient uses.

Help's Half Hour

Led by Bill Statt

Notes by Jan Rothfuss

Q: The fan is beginning to make a lot of noise when using games in Facebook.

A: Check the grate on the tower, looking for dust. Since it is about four years old, you may need to replace the fan. If it begins to shut down, there is a heat issue.

Q: A member is looking for the copyright symbol. Does anyone use Photoshop?

A: You need to use a combination of keys. It might be best to Google the request to get the keystrokes needed. It was also suggested that the member try GIMP, a free photo editing program. Raw Therapy is also good for providing options as you work with raw files.

Q: When using Excel 2007, he uses the F2 key to edit. The cell content is truncated. He has to enter in the long entry area.

A: You may have to look in the Tools options. Sometimes updates can have unwanted effects. Also check the Help options.

Q: Occasionally, a member wants to open his browser in Google. Sometimes he gets a message that the page is not available.

A: He uses Chrome. Check the options menu and make sure that the URL has not been extended beyond www.Google.com. Be aware that AVG's update may cause the default page to change.

NOTE: Windows now has a new version that can be downloaded for Windows 7 users. It was also recommended that you turn off Windows Security Essentials and replace it with AVG or Avast!

Q: One member got a message about Chrome Background.

A: No one else has seen this. It might be a Trojan.

Q: Does anyone use Ebay Sniper? Auction Century is no longer available.

A: There is a free Bid Watcher software.

Q: Is there another software to be able to use Contact Pages?

A: You may be able to use Picassa. Fast Tone may also have it.

Q: Has been using AOL for years. He gets many messages a day, telling him that he needs to update.

A: This is suspicious. Why not switch to Gmail?

Q: Steve is having a problem generating the labels for our newsletter. He is using Word/Excel. He is unable to get the file of labels to go continuously so that multiple pages appear in one file.
A: It was suggested that he use Libre Office.
Q: A Thunderbird user is getting lots of junk email.
A: It was suggested that he start a new email address.

The Lighter Side