

DATA LINE



Published by Santa Clarita Valley Computer Club ... We're User Friendly
Serving the Santa Clarita Valley, CA since 1988

Volume XXIII, Issue 6
Editor: Judy Taylour

Meetings
SCV Senior Center
22900 Market Street
Newhall CA 91321
www.scvpcg.org

Wednesday, June 8, 2011

6:00 pm - Utilities to make your computing experience easier.

In This Issue

- 2 Ten Tech Tips Your Mother Never Told You
- 3 The On-Ramp to the Internet
- 5 Tips & Tricks | Tutorial Better File Information with Windows Explorer
- 7 Microsoft's New Standalone System Sweeper
- 10 Cyber Security Tip - Using Caution with USB Drives
- 11 Word 2007 - A few useful tips
- 13 The Lighter Side
- 14 The Google 2-step!
- 15 Smart Computing Tips
- 17 2011/2012 Officers Membership App



7:00 pm - **Personal Safety with SafeTREC** - a different way Shuly Partush, Director of Distribution will give a presentation showing ways you and your family's personal safety can be improved working with your cellphone or smartphone.

- Summon immediate help with the push of a Panic Button
- Instantly connect with emergency contacts and 24/7 Response Call Center
- Direct call routing to nearest 911 responder
- It's like OnStar for mobile phones

Come and learn all about it. This is the next generation mobile safety. Attendees will receive a free introductory package.

www.safetrec.me

Ten Tech Tips Your Mother Never Told You

Written by Sandy Berger, Compu-KISS

<http://www.compukiss.com> / [sandy\(at\)compukiss.com](mailto:sandy(at)compukiss.com)



Your Mama probably gave you some good advice about table manners and street smarts, but here are a few things your Mama may not have told you:



1. Don't put your email address on the Internet. Many people have a tendency to put their email address at the end of a post on a forum or message board. Don't. The spammers have web spiders that peruse the Internet harvesting any email address that they find for their spam lists.
2. Use a good surge protector or UPS (Uninterruptible Power Supply). Both surge protectors and UPS devices will protect your equipment from power spikes and surges. A UPS will give you the added feature of providing a battery backup when the electrical power fails.
3. Unplug your electrical equipment in a lightning storm. Even with a good surge protector or UPS, a direct lightning hit can devastate your computer and other electrical equipment. While you may not want to run around the house unplugging everything, it is the only way to protect your equipment from a close lightning strike.
4. When the power goes out, get the flashlight and candles, and then unplug your computer and other costly electrical equipment. Often when the power goes back on, there are power spikes and surges that can hurt your equipment. If you are available when the power goes off, the smartest thing to do is to unplug the equipment and plug it in again after the power has returned and the initial spikes and surges have stopped...five to ten minutes is usually adequate.
5. Don't click on email attachments that you don't expect. Even if they seem to come from a friendly source, email attachments can contain viruses. Don't open them unless they are from a trusted source and you are expecting them.
6. Don't fall for phishing schemes. The government has just warned about counterfeit email that looks like it comes from the IRS, Justice Department, or FTC. These are fake messages that lure users to realistic, but bogus websites and trick them into giving out personal information. Such email is often proposed to be from banks, credit card companies, and Internet sites like PayPal, eBay, and Amazon.
7. Reboot to clear a problem. When you have trouble with your computer, the first thing you want to do is to reboot. Turning the computer off then on again allows the computer to reset itself and often corrects the problem. Remember that many devices today have computer chips and rebooting them may also be beneficial. I have had to reboot or reset cable and satellite boxes as well as iPods to solve problems.

8. Look for the obvious. When you have a problem, look for the obvious before you call tech support or pull your hair out. Always make sure the device is plugged into a working outlet and that all connection cables are secure. If you are working with software, read everything on the screen, even the things you normally ignore, for clues to solve your problem.

9. Try three times. You'll not find this advice in any tech manual, but it often works. If something doesn't work the first time, try again. You may have made a mistake the first time or some unusual circumstance may have screwed things up. If it still doesn't work, try one more time to be sure. This three-time rule often works wonders. Last month, my laptop came up with a blank screen when I pressed the start button. I turned it off and tired again. It gave me a cryptic error. The third time was the charm. It worked perfectly and has been working ever since. I'll probably never figure out exactly what happened, but who cares if everything keeps on working.

10. Be adventurous. Your mother may have advised you to play it safe, but in the computer world you may be better off to be at least a little bold. Try new things. Computer knowledge is cumulative. What you learn using a new program will help you with your next endeavor. Find new ways to do things. There are almost always two or three different ways to do things when working with computers. If you know several ways to do the same thing, it can come in handy when something goes wrong.

Of course, when you are working with a computer it may seem like things go wrong quite often. But perhaps these ten little things will help you keep trouble away and deal with it when it does come. After all, isn't that what your mother's advice often did for you?

The On-Ramp to the Internet

By Phil Sorrentino, President, Sarasota PCUG, Florida

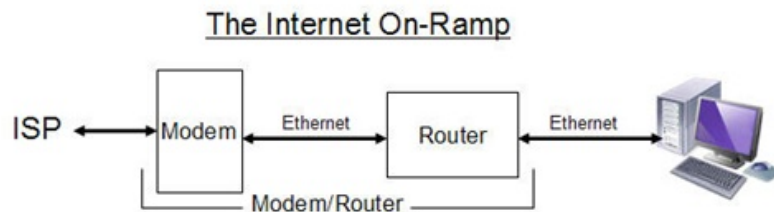
May 2011 issue, Sarasota PC Monitor

www.spcug.org / [president \(at\) spcug.org](mailto:president@spcug.org)

The Internet is the highway to many wonderful places. Places where you can engage in conversation with friends and family members, and even see them, with the right setup (ala Skype). Places where you can see things you may never get close enough to see in person. Places where you can correspond with companies and/or individuals. Places where you can buy items not available in your local shops and stores. Places where you can store your favorite pictures, videos and documents. All these places are on the internet and you can get to them using a computer and your own On-Ramp. The On-Ramp to the Internet is simply an Internet Service Provider (ISP), and a Modem (typically, a router is included to provide Local Area Networking {LAN} capability). With these items, you can get on to the Internet with any of your desktop or laptop computers.

So, now that we know why you might want to get on to the internet, let's see how we build an On-Ramp. First, and maybe the easiest, is to find an ISP. In this geographic area there are many providers, but the major players are Verizon, Comcast, and Brighthouse. Verizon provides FIOS, a digital connection; or DSL, a copper wire connection. Comcast and Brighthouse are cable providers so they provide a cable connection. (Long-time users will remember that there is also a dial-up connection that could be had using the telephone wiring in your house, but this provides an On-Ramp with such a speed limit that it is almost un-useable.)

Each provider will provide a modem that is capable of connecting to its specific network, which in turn connects to the Internet. For the technically, or etymologically, interested, the word modem is a combination of the two functions that it provides, MODulation and DEModulation. The signals going to the Internet must be Modulated, and the signals coming from the Internet must be DEModulated. If you use only a modem (no Local Area Network) then the modem connects directly to your computer. But, more typically a router is used so that many computers can use the On-Ramp simultaneously. (The router can be a separate enclosure or included in the Modem enclosure.) So, the signals from the ISP first go to the Modem, then to the Router and finally to the computer(s).



In terms of wiring, the ISP connector (Cable, FIOS, or DSL) goes to the Modem, if a router is in the same enclosure, an Ethernet cable goes from the Modem/Router to the Computer Ethernet port. If an external Router is used, an Ethernet cable goes from the Modem to the WAN (Wide Area Network) input of the Router, and another Ethernet cable goes from a LAN port of the Router (usually one of four) to the computer Ethernet port. The Ethernet connector is called an RJ-45 connector and looks like an oversized telephone connector (for those of you who have looked at a telephone connector).



Now that the Modem and Router are wired, we're ready to go. Well, yes, but there is a Power-On sequence to keep in mind whenever the Modem, Router, and Computer(s) are to be powered up. Start with all the equipment turned off, and power up the modem first. After about a minute or so, the blinking lights on it will stop blinking, mostly. Next, if the router is a separate enclosure, power up the router, and wait for a minute or two, till its lights stabilize. (If the Router is part of the Modem, the electronics in the Modem/Router will take care of the sequencing.)

Next, the computer(s) can be powered up. (Note that if you ever have a power failure, or turn all this equipment off intentionally, or you experience very strange networking problems, you should go through this power-on sequence once again.)

Your On-Ramp requires very little maintenance. Once everything is up and running well, the Modem and Router can be left on 24/7 (unless you are leaving your home for an extended period of time). The only things you might want to shut down at the end of the day are the computers, if you so desire. Following the above few guidelines will help keep your On-Ramp in good repair and allow you to get on, and stay on, the Internet, and enjoy all those places you intend to visit.

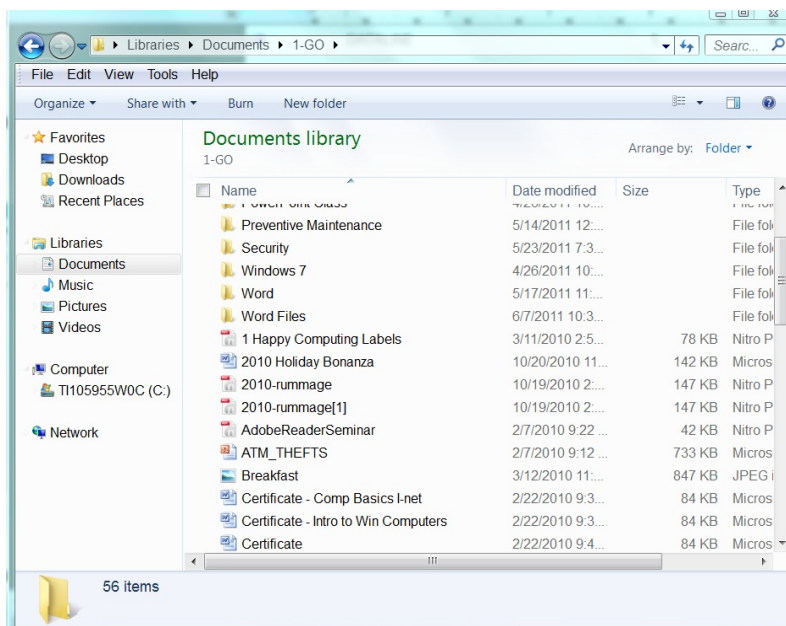
Once the On-Ramp is in place and useable, your browser, on your wired computers, should be able to get you onto the Internet. If things don't connect right away, there may be a few networking windows that may need to be visited to get the network connection up and running, such as the "Network and Sharing" window, which is part of the Control Panel. (The networking windows are slightly different for each of the Operating Systems, XP, Vista and 7.) Also, if the Router is not part of the Modem enclosure, the router may have to be setup, although most routers right out of the box will probably get your wired computers on to the Internet with their default settings. The wireless computers may take some additional setup, which will have to be part of a future "wireless networking" article. Or, you could get all of the information needed to setup a wireless network by attending one of our wireless networking educational classes. Hope to see you there, some day.

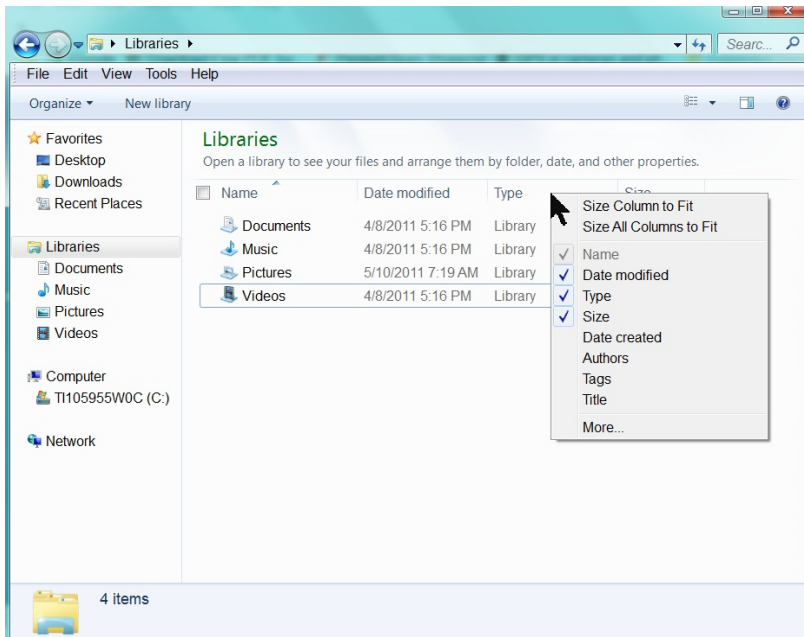
Tips & Tricks | Tutorial
Better File Information with Windows Explorer
By Les Townsing, a member of the Melbourne PCUG, Australia
April 2011 issue, PC UPDATE

Sort your files more intelligently with a few simple clicks.

There is often a lot of information automatically recorded when you save a file. This information can be easily displayed and can prove to be useful when sorting/categorizing files.

Normally, when you open Windows Explorer (right-click on the Start button and select 'Explore') you get displays indicating the file name, size, date modified, and other general information.





If, however, we right-click anywhere on the Column Heading bar we get a lot of additional columns we can add. Depending on the type of files you can select some meaningful columns. If we are looking at picture files (jpg) some appropriate columns may be Date Taken, Dimensions or file size.

If you right-click on a file and select properties, you get to view all the possible information as well as the ability to edit some of the fields.

You can now sort your files by any of the columns (just left click on the column heading).

If we right-click on a file, we can select Rename and change the name to a more meaningful title rather than a bunch of numbers. These features may be more meaningful if we use music files as an example.

Unfortunately, some of the "Ripper" programs (programs that copy CDs and often convert the files to MP3s) get it wrong or leave a lot of stuff out, which can be quite annoying, particularly if it is the artist's name or the title of the song.

When selecting a CD Ripper program this is one item worth checking.

Extra Tip

If you select a file (click on it) then hold down the shift key whilst clicking on another file then the system will select all the files in between and including the first and last file you clicked on. Now, if you right-click on any one of the selected files and choose properties, you can edit a field for all the selected files. This is no good for titles as every file must have a different name. However, it is good when you want to edit the album title or artist for a number of tracks.

Extra Extra Tip

Often the files you want to select are not consecutive in a list. No problem, hold down the control key then click on the files you want. As you click on the files they become marked as selected. You can then right-click on any selected file to edit the properties of all the selected files.



Microsoft's New Standalone System Sweeper

By Ira Wilsker, Member, Golden Triangle PC Club, TX;

Columnist, The Examiner, Beaumont, TX;

Radio Show Host, Mondays, 6-7pm CT, KLVI.com

iwilsker (at) sbcglobal.com

WEBSITES:

<http://connect.microsoft.com/systemsweeper>

<https://connect.microsoft.com/systemsweeper/content/content.aspx?ContentID=24894>

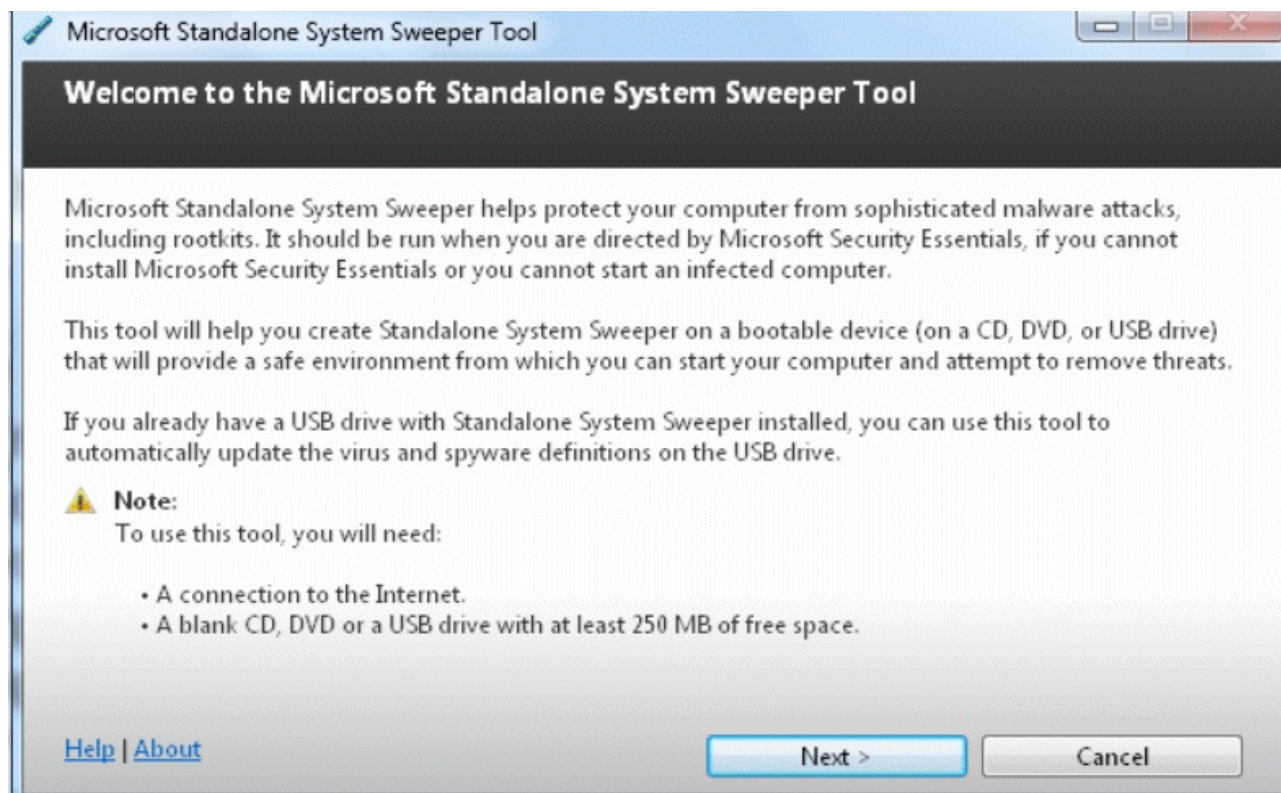
<http://technet.microsoft.com/en-us/library/ee460911.aspx>

<http://www.techsupportalert.com/create-bootable-rescue-cd.htm>

<http://www.techsupportalert.com/content/probably-best-free-security-list-world.htm>

Sometimes, despite our best efforts, it seems impossible to remove the spyware and other malware from our computers. Despite their efficacy, there are just some times that the traditional and well proven malware killers will not be able to neutralize the malware on our computers. While some of the so-called "experts" simply give up and reformat the hard drive resulting in the loss of any programs and files on the computer (unless properly backed up), this is not an appropriate step in trying to restore the computer.

There are a variety of utilities, both free and commercial, that can create a bootable CD or USB drive that contain the necessary files to boot the computer, and then detect and remove any malware from the infected computer. The reason for booting from a special CD or bootable USB flash drive rather than Windows is that the substitute bootable media does not load the full version of Windows, but instead loads a substitute for Windows. Because this clean substitute for Windows is not loading any drivers or other files from the infected computer (including a possibly infected Windows itself), there are no malware files loaded into memory (RAM) that interfere with the cleaning process, or otherwise protect themselves from detection and destruction. A variety of security software companies, including Kaspersky, Avira, F-Secure, Panda, BitDefender, DrWeb, AVG, and Spybot Search & Destroy have published free utilities that can create bootable media that will run and remove malware, without the need to load Windows. When I am called to clean badly infected systems, I routinely create at least a pair of updated bootable CDs from a variety of the above companies, such that if I encounter a difficult to clean computer, one or both of the bootable CDs will likely be able to detect and remove the offending malware. Just recently Microsoft has joined this august group of software publishers that have released a free utility to create a bootable CD or flash drive that can detect and remove malware from a badly infected computer. This new utility is the Microsoft Standalone System Sweeper Beta (Beta means that it is functional, but not a final release).



Microsoft Standalone System Sweeper Beta (connect.microsoft.com/systemsweeper), like the other utilities mentioned above, can be used to boot an infected computer and perform a malware scan that can identify and remove malware and rootkits. This is especially useful when the malware on a computer prevents the installed security software from running, as many of the contemporary malware titles explicitly destroy the legitimate security software installed on the computer. Many of the current crop of malware infections also make it impossible to run already installed detection and removal utilities, as well as prohibit web access to online services that may be capable of detecting and removing the controlling malware. Some malware also prevents the infected computer from booting, making it nearly impossible to run any of the traditional scanning utilities. For this reason, it is sometimes necessary to be able to boot the computer into some operating system other than the full Windows, and run a scan utility. This is explicitly what Microsoft Standalone System Sweeper Beta (and the other bootable scan utilities) is intended to do.

Microsoft Standalone System Sweeper Beta is available in both 32 and 64 bit versions, and the proper version for the compromised system should be downloaded to another uninfected computer from connect.microsoft.com/systemsweeper. Using that clean computer (not the infected machine!), the user needs a blank CD, DVD, or USB flash drive (with at least 250 megs of free space) to create the bootable media. According to Microsoft, "The architecture of Microsoft Standalone System Sweeper Beta does not have to be the same as the Windows operating system of the computer used to create the bootable media. It does need to be the same architecture (32-bit or the 64-bit) as the Windows operating system of the computer infected with a virus or malware."

The initial download is a small installer (576 kb for the 64 bit version), which is used to start the media creation process. This small installer file is run, and a series of windows appear that walk the user through the media creation process. The first window informs the user that he needs some appropriate media and internet access to create the bootable media, followed by the EULA (End User License Agreement). The third screen gives the user the option to use a blank CD, DVD, USB flash drive, or to create an ISO image that can later be burned to a CD using an ISO file burner to create the bootable CD. I chose to use a blank CD, but any of the appropriate options would be adequate choices. Since virtually all Windows XP SP3, Vista, and Windows 7 computers can be booted with a CD and run the System Sweeper, regardless of the operating system that was on the computer that was used to create the bootable media, I prefer the bootable CD media. Many computers, especially older ones, cannot easily boot from a USB flash drive, which is why I create a CD. Just be sure to create the media with the correct 32 or 64-bit version; you need the setup file that matches the infected computer's architecture, not the architecture of the clean computer. If the infected computer is 64 bit, you will need the 64 bit installer, regardless of the version on the clean computer. Likewise, if the infected computer is 32 bit, use the 32 bit installer on the clean computer to create 32 bit bootable media.

The actual file that was downloaded from Microsoft by the small installer was 206mb, which took a few minutes to download. Once downloaded, it only took a few more minutes to create a bootable CD containing the Microsoft Standalone System Sweeper Beta, as well as its latest malware signature database. While there are some methods that can be used to update the malware signatures, I prefer to create a fresh CD with the latest signatures prior to each use.

After the bootable CD, DVD, or USB drive is created on the clean machine, the media is used to boot the infected computer. Once booted, the interface looks very similar to the established Microsoft Security Essentials, and uses a similar scan engine to detect and remove malware. I would suggest that the user selects a full scan, and allows the software to neutralize whatever it finds. Once the scan and clean function has been completed, remove the bootable media, and reboot the computer into Windows. If the computer still will not function properly, as it appears that it is still infected after running the System Sweeper, one of the other bootable scan utilities listed above may be necessary to remove the infection. If it does boot successfully, I choose to perform a redundant scan with a third party utility such as Malwarebytes (malwarebytes.org) or SuperAntispyware (superantispyware.com). Since much of the malware in circulation destroys the installed security software, it may be appropriate to reinstall the real-time security software of your choice.

The Microsoft Standalone System Sweeper Beta is only intended to boot and clean a badly infected system, and provides no permanent protection, which is why it should not be used as a substitute for a good security suite. Since blank CDs are cheap, it would be a worthwhile precaution to frequently create a bootable CD using Microsoft Standalone System Sweeper or one of the other bootable utilities, label it with the date, and keep it on hand just in case it is needed.

Ira Wilsker is the Director of the Management Development Program at Lamar Institute of Technology, in Beaumont, TX. He also hosts a weekly radio talk show on computer topics on KLVI News Talk AM560, and writes a weekly technology column for the Examiner newspaper <www.theexaminer.com>. Ira is also a police officer who specializes in cybercrime, and has lectured internationally in computer crime and security.

Cyber Security Tip ST08-001 Using Caution with USB Drives

By Mindi McDowell

Produced 2008, 2011 by US-CERT, a government organization

<http://www.us-cert.gov/cas/tips/STYY-XXX.html>

Note: This tip was previously published and is being re-distributed to increase awareness.

USB drives are popular for storing and transporting data, but some of the characteristics that make them convenient also introduce security risks. What security risks are associated with USB drives?

Because USB drives, sometimes known as thumb drives, are small, readily available, inexpensive, and extremely portable, they are popular for storing and transporting files from one computer to another. However, these same characteristics make them appealing to attackers.

One option is for attackers to use your USB drive to infect other computers. An attacker might infect a computer with malicious code, or malware, that can detect when a USB drive is plugged into a computer. The malware then downloads malicious code onto the drive. When the USB drive is plugged into another computer, the malware infects that computer.

Some attackers have also targeted electronic devices directly, infecting items such as electronic picture frames and USB drives during production. When users buy the infected products and plug them into their computers, malware is installed on their computers.

Attackers may also use their USB drives to steal information directly from a computer. If an attacker can physically access a computer, he or she can download sensitive information directly onto a USB drive. Even computers that have been turned off may be vulnerable, because a computer's memory is still active for several minutes without power. If an attacker can plug a USB drive into the computer during that time, he or she can quickly reboot the system from the USB drive and copy the computer's memory, including passwords, encryption keys, and other sensitive data, onto the drive.

Victims may not even realize that their computers were attacked.

The most obvious security risk for USB drives, though, is that they are easily lost or stolen (see *Protecting Portable Devices: Physical Security* for more information). If the data was not backed up, the loss of a USB drive can mean hours of lost work and the potential that the information cannot be replicated. And if the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it.

How can you protect your data? There are steps you can take to protect the data on your USB drive and on any computer that you might plug the drive into:

- Take advantage of security features - Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost (see *Protecting Portable Devices: Data Security* for more information).
- Keep personal and business USB drives separate - Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer.
- Use and maintain security software, and keep all software up to date - Use a firewall, anti-virus software, and anti-spyware software to make your computer less vulnerable to attacks, and make sure to keep the virus definitions current (see *Understanding Firewalls*, *Understanding Anti-Virus Software*, and *Recognizing and Avoiding Spyware* for more information). Also, keep the software on your computer up to date by applying any necessary patches (see *Understanding Patches* for more information).
- Do not plug an unknown USB drive into your computer - If you find a USB drive, give it to the appropriate authorities (a location's security personnel, your organization's IT department, etc.). Do not plug it into your computer to view the contents or to try to identify the owner.
- Disable Autorun - The Autorun feature causes removable media such as CDs, DVDs, and USB drives to open automatically when they are inserted into a drive. By disabling Autorun, you can prevent malicious code on an infected USB drive from opening automatically. In *How to disable the Autorun functionality in Windows*, Microsoft has provided a wizard to disable Autorun. In the "More Information" section, look for the Microsoft Fix it icon under the heading "How to disable or enable all Autorun features in Windows 7 and other operating systems."

Word 2007 - A few useful tips

By Lynn Page, Editor, Crystal River Users Group, Florida
February 2011 issue, CRUG newsletter
www.crug.com / [newsletter \(at\) crug.com](mailto:newsletter@crug.com)

The Ribbon

With Office 2007 Microsoft introduced a totally new interface that has carried forward into Office 2010. The new Ribbon interface provides access to program features organized into logical groups on tabs relating to a type of activity. Some tabs appear only when needed like the Picture Tools tab, shown when a picture is selected. When a tab is selected the Ribbon becomes a graphical presentation of the program commands in that group.

So commands are readily available and noticeable making it easy to see things you may not have known existed or were too much trouble to find.

Office Button



One problem with the Ribbon interface was finding the old File drop down menu commands. The Office Button replaced the File drop down menu and Options dialog box. Clicking the Office button at the top left of the application window opens a drop down menu. From the menu you can create a new document, open an existing document and save or print the current document. It also provides a list of recently accessed documents.

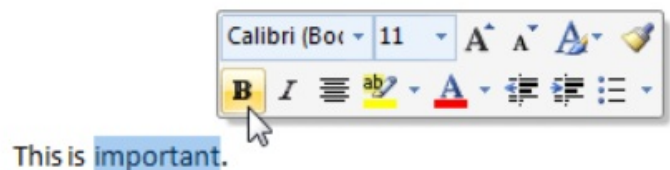
The Word Options dialog box is also accessed from the menu.

Quick Preview

A really great feature is quick preview. It lets you see formatting changes before applying them. With the movement of the mouse over the proposed formatting, you see how the document looks with that formatting.

Mini Toolbar

When working within a Tab, the Commands available on others are not visible. However some formatting commands are so important they are available all the time through the Mini toolbar. With text selected point at the selection and the Mini toolbar appears near the selected text in a faded fashion. Pointing to the Mini toolbar makes it become solid. Click a



formatting option on the toolbar to apply the format.

Quick Access Toolbar

The Mini toolbar is great for formatting options, but doesn't offer other commands. For these the Quick Access Toolbar is a solution makes frequently used commands available for easy access, regardless of which tab of the Ribbon is active. It is the row of buttons next to the Microsoft Office Button above the Ribbon. By default, the Quick Access Toolbar contains buttons for Save, Undo, and Repeat (Redo). In addition, the toolbar can be customized to contain personal favorites.

Click the down arrow beside the toolbar to open the Customize Quick Access Toolbar drop down menu. In the drop down menu, click a command to select it for inclusion in the toolbar. For more versatility, add commands directly from the Ribbon. Find the command on the Ribbon, right click it and click Add to Quick Access Toolbar.

A Few Useful Commands

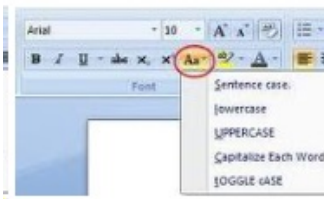
Paste Special

The Paste Special command controls the format of pasted text. This is good when copying text or a graphic from another document or a web page to paste into a Word document. The Paste Special dialog box gives options for the format of text or graphic being pasted. The "Unformatted text" option cleans up pasted text. It pastes bare, unformatted text only. All other formatting information is stripped out, including bold, underlining, italics, indents, bullets etc.

Character Spacing

Character spacing found on the font dialog box is useful in final editing to eliminate orphans and widows.

Change Case



Change Case is accessed from the Home Tab in the Font Group. It is not in the Font dialog box. Select the text and Click the Change Case icon in the Font group on the Home tab. Select Sentence case, lowercase, UPPERCASE, Capitalize Each Word and TOGGLE cASE in the drop down menu.

Text Wrapping Break

Text Wrapping breaks along with text wrapping control how text is placed with respect to graphics. Add a Text Wrapping Break to start the next line of text below the graphic.

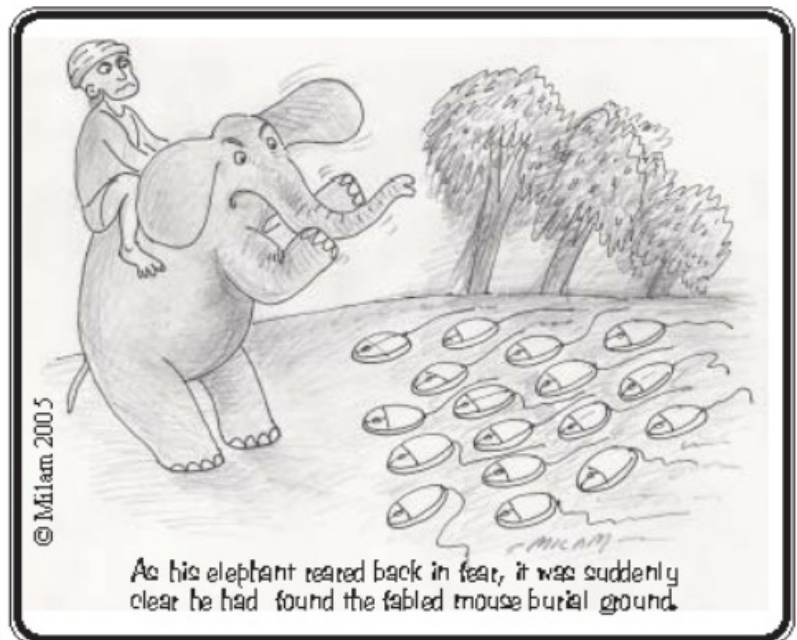
Any type of break is added from the Page Layout tab. In the Page Setup group click Breaks.

From the drop down menu select the appropriate break. Page, Column and Text Wrapping breaks are in the Page Breaks section. The different types of Section breaks are available in the Section Breaks section. They include next Page, Continuous, Even Page and Odd Page.

The Lighter Side

Bucky Milam is a master of the fine arts, with an emphasis on the cool and casual. He is the recipient of numerous awards for his painting and graphic design, which has been displayed at the Dallas Museum of Fine Arts, the Museum of Modern Art, the Chicago Art Institute, and the London and Tokyo Museums of Fine Art. A trumpet virtuoso, he performs widely in clubs throughout the region and is a recognized composer of jazz and classical music for brass.

Bucky comes to computing as an accidental tourist. His peculiar perspective is of the visual media and the image they project of our civilization and culture. You can find his musings in each monthly issue of dacs.doc.



(Danbury Area Computer Society)

The Google 2-step!

By Drew Kwshnak, a member of the Danbury Computer Society, CT

June 2011 issue,

www.crug.com / [newsletter \(at\) crug.com](mailto:newsletter@crug.com)

If you are one of those users with "password" as your password, might I suggest you use Google for your email, calendar and other online needs! Even if you use a password not on the list of "The Top 500 Worst Passwords of All Time" it might be a good idea to use Google's 2-step verification.

The 2-Step Verification is, in Google's own words:

2-step verification adds an extra layer of security to your users' Google Apps accounts by requiring them to enter a verification code in addition to their username and password, when signing in to their account.

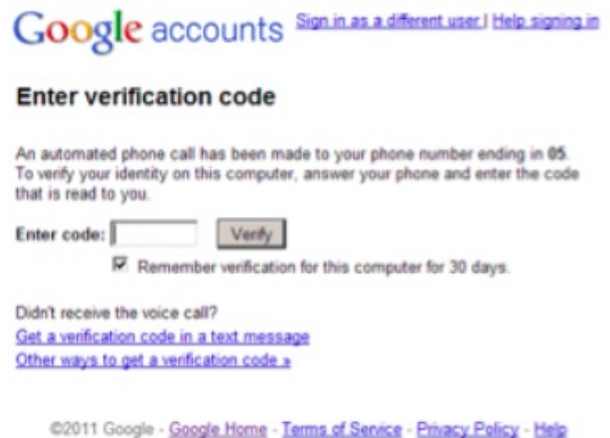
This Verification code is not another password to memorize. Instead, the verification code is generated at the time you try logging in, and is only valid for a short period of time. Even if somebody were to pluck your username, password AND verification code out of the air they are to act quickly before the verification code is expired.

Corporations have made use of this verification method for years but have had to rely on distributing a keychain FOB with an automatically changing verification code. Google uses something more readily available; your phone.

When turning on 2-step verification for your Google Account you are walked through the set up process. At minimum you have to supply a phone number and you have the option receiving the verification code either as an SMS (text) message, or an automated voice message.

While you can change which method to receive the verification code when logging in, you cannot change where it is sent. This also means anybody trying to log into your account cannot redirect the verification code to their phone. You can, however, set up a second backup phone and method. This is helpful just in case you don't have your phone handy.

That's it! The next time you log into your Google Account, or any of the numerous Google Apps, you will get the familiar login request except when you click Sign In, you will see a page asking for your Verification code and within moments your phone will be receiving this code.



Once you have successfully logged in, you don't have to worry about going through this process every time. It remembers the computer you are using and afterwards it will function with just your username and password, unless you log completely out.

Since most local applications, such as email or chat clients, do not know how to handle a verification code, you can create what is called Application Passwords. These are randomly generated, strong passwords that allow only applications to access your Google Applications, not a browser and not your account settings.

These passwords can be easily created and deleted as necessary only after logging into the account using the 2-step Verification. This could be used for temporary use, easily changing the password every so often, or having each system or application use their password.

So not only does Google add a layer of security with the additional verification code, it also separates application-level access with the account settings controls to limit the damage somebody can do if they were to gain access to your username and password.

Once set up it is not a difficult process to follow, and the return of greater security is well worth it in my opinion.

[1] <http://www.whatsmypass.com/the-top-500-worst-passwords-of-alltime>
[2] <http://www.google.com/support/a/bin/answer.py?answer=175197>

Drew Kwashnak spends way too much time on the web and ran across this feature from Google when his account was closed for "suspicious activity". Since then, he hasn't had any issues with "suspicious activity" or the like.



Smart Computing Tips
www.smartcomputing.com

Pictures In Word Documents

Pictures can add a great deal to the otherwise boring-looking Word documents. But when it's necessary to rotate the pictures, things can get a little tricky. To rotate a picture in Microsoft Word 2007, first click the picture or graphic you want to move. Once you see the outline around your object, left click the top green knob, hold the object, and then rotate it. You can rotate pictures, graphics, and even text.

Two Computers, One Set Of Peripherals

If you've got two computers at your desk, you don't need a separate keyboard, mouse, or monitor for each PC. You can connect the peripherals to a KVM (keyboard, video mouse) switch

and share the display and input hardware. Many KVM switches also include inputs for printers and other USB peripherals.

Internet Explorer Address

The pointing device on your notebook PC doesn't always make it easy to click the address bar in Internet Explorer. So next time, just press the F6 key instead. This will place the cursor in the address bar and highlight the text inside, too.

External Hard Drives & Power

Among an external hard drive's advantages over adding a second internal drive to a PC is the fact that an external unit typically receives power from an AC adapter. Hard drives take a lot of power to start their disks spinning when you turn a PC on. If the computer's power supply is only marginally able to run the rest of the devices as it is, it might not be able to start the PC at all should you install another internal drive. You can buy drive enclosures to turn internal hard drives into external ones for about \$25 and up. Be careful to buy one with the correct interface for the drive you have (such as EIDE [Enhanced Integrated Drive Electronics] or SATA [Serial ATA]) and a cable interface supported by your computer (such as USB 2.0 or eSATA). Some enclosures work best with EIDE drives with jumpers set to CS (Cable Select) instead of Master or Slave.

Keep Up With Updates

Many types of viruses and malware use known vulnerabilities in Microsoft's Windows operating system to find a loophole into your computer. Typically, the Windows Update patches fix the known issues and help keep your PC secure. If you don't want Windows to automatically update, at least configure Windows Update to notify you of the latest patches, so you can check out if there are any security updates that may be needed to fix holes in Windows.

Turn Off Auto Formatting

If you've ever created a numbered or bulleted list in Microsoft Word, you know that Word automatically makes formatting changes once it senses a pattern in your list. However, the auto-formatted text can become tedious to change when you want to begin a sentence with a number or bullet point without beginning a new list. If you want to turn off auto formatting in Word 2003, click the Tools menu, select AutoCorrect Options, choose the AutoFormat As You Type tab; remove the checkmarks from the Automatic Bulleted Lists and Automatic Numbered Lists, and click Apply. In Word 2007, click the Office button, Word Options, and Proofing; click the AutoCorrect Options button; select the AutoFormat As You Type button; remove the checkmarks from the Automatic Bulleted Lists and Automatic Numbered Lists, click OK, and click OK again.



2011/2012 SCV CC OFFICERS

President	Judy Taylour scvcomputerclub (at)gmail.com
Vice President	Dave Melton davey@melton.com
Secretary	OPEN
Treasurer	OPEN
Membership	OPEN
Program Director	OPEN
Information Line	661.513.4612
Snail Mail	18727 Nadal Street Santa Clarita, CA 91351
General Meeting	2 nd Wednesday / month SCV Senior Center 22900 Market Street Newhall CA 91321

Membership Benefits Around Town

Show your Santa Clarita Valley Computer Club Membership Card to receive the below discounts.

Jay's Computer Shop

In-shop and on-site PC repair services
Free phone support for all SCV Computer Club members

\$10hr off on all on-site service
(regularly \$85hr)

\$5hr off on all shop service (regularly \$50hr)

Open Monday – Saturday
818.362.8015 / Located in Sylmar
jay@jayscomputershop.com
www.jayscomputershop.com

Membership Application
(Please Print)

Name

Address

City/State/Zip

Home Phone

E-mail

Areas of Interest

Level of computer skills (please circle)

Novice Average Expert

Mail to: SCV CC, 18727 Nadal Street

Precision Computers

10% on Service
19188 Soledad Canyon Road
Canyon Country
661.299.2228 (ph)
www.precisionpc.com

Rogers System Specialist

(Various Discounts)
25570 Rye Canyon, Ste. A, Valencia
661.295.5577
Give Judy's telephone number for the discount
661.252.8852

ATS LASER - 25%

661.296.5500 / atshpguy@earthlink.net
www.HpPrinterRepair.net
ATS makes house calls. Printers - Copiers -
Fax Repair + Toner Cartridges .
ATS will beat any super store price.

The information appearing in this newsletter is distributed solely for use by SCV Computer Club members. Permission is enthusiastically granted to reprint all or any part by similar non-commercial publications *provided credit is given to the author of the article and the DATALINE.*

The publication of information in this newsletter constitutes no guarantee of accuracy and its use by readers is discretionary. All opinions expressed are those of the authors and not necessarily those of the SCV Computer Club.

The SCV Computer Club is dedicated to supporting the needs of its members and to the exchange of information about computers, peripherals, services, hardware and software through meetings, its web page, and the distribution of this newsletter.

The SCV Computer Club is a proud member of SCRUGS
Southern California Regional User Group Summit

Annual Membership Dues	\$30.00
Annual Family	\$54.00
Senior	\$27.00



O'Reilly User Group Program
35% Discount for SCV
Computer Club members -
Print & ebooks
Discount Code DSUG
www.oreilly.com

Free Shipping on orders of \$29.95 and up!



35% discount / UE-23AA-PEUF
www.peachpit.com



Focal Press User Groups

learn · master · create www.focalpress.com

30% Discount / Code MEETUP
www.focalpress.com

webucator
customized INSTRUCTOR-LED training services

One free class / quarter (raffle)
www.webucator.com



www.quepublishing.com/promotions/