The Rochester Computer Society, Inc.
Since 1982

MONITOR

Vol. 32, No. 9 Sept. 2014

Next Meeting

Tuesday, Sept. 9

Mark Zinsow Will Discuss Scribus
Art Trimble Will Discuss Close-Up Photography
Jerry Seward Will Discuss Indesign

Contents

Three Better Ways to Store Your Files Joel Lee 1
Legitimate Ways to Save Money on a Cell Phone Ira Wilsker 4
Ask Mr. Modem 8
Seven Cool Things You Can Do with Drop Box Bob Rankin 9
ALERT: Serious Security Flaw in USB Drive Bob Rankin 11
Linux and the Malware Threat Bill Wayson 12
Ten Stupid Things You Can Do to Mess up Your Computer Bob Rankin 14
Society News 16
The Lighter Side 17

apcug Member of the Association of Personal Computer User Groups

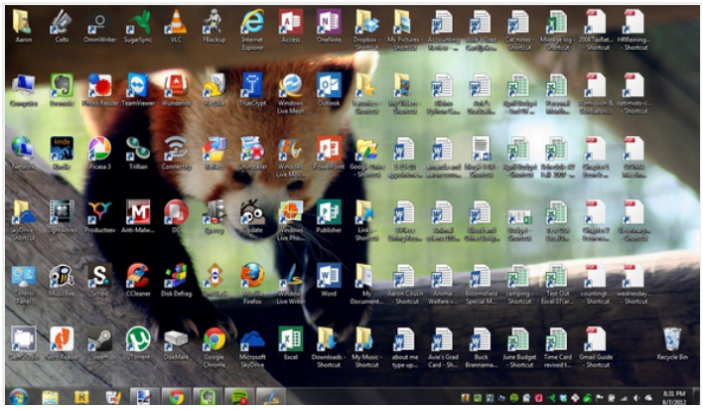
Three Better Ways to Store Your Files than on the Desktop

by Joel Lee
MakeUseOfCom.com

Did you know that storing files directly on your desktop can harm your productivity? I used to be one of "those" people who downloaded files straight to the desktop. If you can identify with that, then I have good news for you: you can do better. Desktop storage is simple, sure, but it comes with hidden drawbacks you may not know about.

Kick the bad habit with these alternative file storage methods. They may not be as convenient but I promise that you'll learn to love them in the long run.

The urge to save files to the desktop is understandable. It provides immediate access with a single click, which means that it's tempting to turn the desktop into a de facto headquarters for storage. But unless you are strict with maintenance, you"ll eventually succumb to these issues:



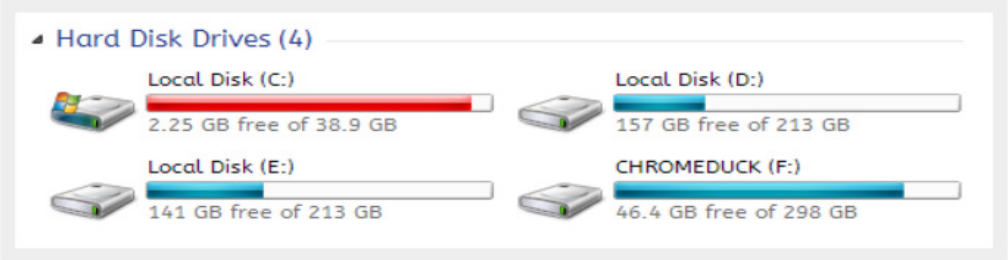
No file protection. As noted by *PC World*, certain directories are not affected by System Restore, the most recognizable location being My Documents. Files on the desktop are affected by System Restore, which can result in unexpected file disappearances.

No file backups. Many file backup programs ignore desktop files by default. Most programs worth their salt will allow you to change the settings and include the desktop if necessary, but all it takes is one forgetful moment to accidentally lose an important desktop file.

Clutter, clutter, clutter. The story is always the same. You begin your desktop collection with a few documents. Over time, the collection grows to include images, music, programs, zip files, and more documents. Suddenly, finding the right document takes more time than actually opening it.

Separate Drive Partitions

One bit of computer wisdom that you should learn is this: "Never save data on the same partition as your operating system." In Windows, the location of the desktop on the file system does reside on the same partition as the operating system itself.



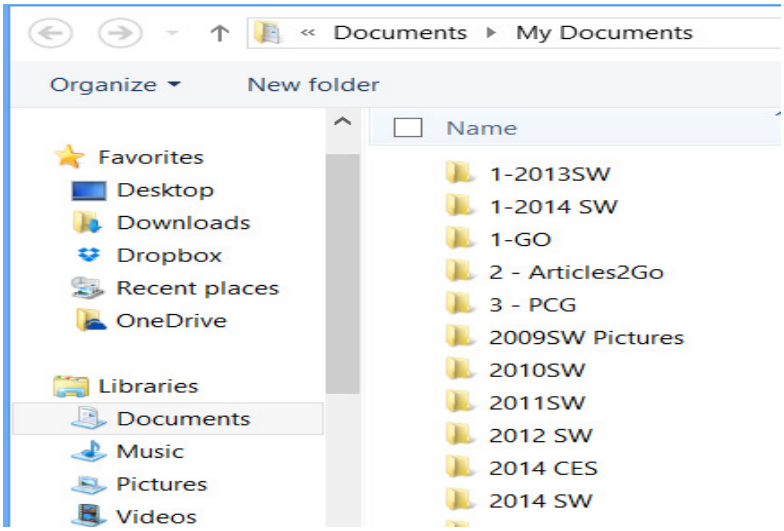
Why is this important advice? Because you want to avoid putting all of your eggs in the same basket.

Let's say that you happen to contract a mild virus or malware that attacks your operating system. It might wipe all files related to the operating system itself OR it may affect the entire partition that holds the operating system. By losing the operating system, you lose all of your saved data as well.

But if you installed Windows to the C: partition and stored all of your files on the D: partition, your files on D: would be safe even if C: were wiped clean. The only way D: would be affected is if the physical hard drive itself was wiped or damaged.

One additional benefit of having separate partitions is that you can reinstall Windows without losing your saved data. Tina has written on the subject of resizing Windows partitions, so check it out if you want to take advantage of this feature. http://bit.ly/1lfBCDe

Use Windows Libraries



Every installation of Windows comes with a directory called My Documents. In Windows 7, it was renamed to Documents and came with a couple of buddies: Music, Pictures, and Videos. They're called libraries and you've probably seen them before, but never really used them, right? Well, you should reconsider.

In truth, these four libraries are special. They aren't just directories; they're collections of multiple directories. In each library, you can specify different directories to be included and that library will show the content from all included directories. It sounds more complicated than it is.

Think of it like this: You can save your videos to many different locations and link those directories to the Videos library. Then, whenever you access the Videos library, you'll see all of those files in one place.

It's just as convenient as storing everything on the desktop, yet infinitely more flexible and organized. For more details on how to take advantage of this feature, check out Chris' writeup on how to use Windows Libraries. http://bit.ly/1iMkORF

Store Files in the Cloud

Cloud storage has been a big buzz term over the past few years and for good reason. While cloud-related solutions like Dropbox, G+ Drive, or Microsoft OneDrive come with privacy concerns <http://bit.ly/1lzsQ4F>, they also offer many benefits and I think people are too quick to throw the baby out with the bathwater.

Here's how it works: You set aside one or more directories that automatically sync with whatever service you're using (comparison of cloud storage services). These files can be accessed from anywhere and they can be set to private or public.

Why is this better than storing straight on the desktop?

Immediate backups. Due to automatic synchronization, you rarely need to worry about lost files. If your computer gets wiped somehow, those files still reside on the cloud and you can always retrieve them again.

Revision history. Not every cloud service offers a revision history, but most do and it's an important feature. Basically, the service will track every change that's made to the file (it may be limited to the last X changes) and allow you to instantly revert to a past version if necessary.

One Drive (aka SkyDrive) comes integrated with Windows 8 and can help you keep your files synced.

Need Quick Access to Files?

Sometimes convenience wins out over practicality and reason. The desktop is great because it allows for immediate access, right? With one small compromise, you can maintain that convenience. The answer is to use shortcuts.

Creating a shortcut is as simple as dragging a file using the right mouse button to where you want the shortcut to appear, then selecting Create shortcut here from the menu. Even if a shortcut gets wiped, the actual file will still be safe.

But instead of putting the shortcuts on the desktop, why not take it one step further?

Right click on any file shortcut and select either *Pin to taskbar* or *Pin to start menu*. It's a self-explanatory feature that works just as well as, if not better than, traditional desktop shortcuts. I use it day in and day out and I wouldn't have it any other way.

Conclusion

Ultimately, personal preference will always win. For those of you who have been "desktopping" for years, you'll probably find it near impossible to break the habit. I still do it from time to time, though I try my best to clean up after myself when I realize what I'm doing. It just doesn't make sense to store everything on the desktop anymore.

Do you clutter up your desktop with files and folders galore? If so, are you convinced enough to try a safer method of file storage? Share your thoughts with us in the comments! http://www.makeuseof.com/tag/3-better-ways-store-files-desktop/

Courtesy of APCUG.

Alternative Ways to Legitimately Save Money When Buying a Cell Phone

by Ira Wilsker

Over the past few weeks, I have been searching for a new smart phone to replace my existing, malfunctioning smart phone. A visit to my carrier's website and company owned phone store offered a wide selection of new phones, but for the high-end models that I was considering, the prices were exorbitant. I had even considered a highly rated smart phone that had been on the market for well over a year which was a "generation" old, and been supplanted by a greatly enhanced newer model. This "older model" would still cost about $650 at the carrier store if purchased outright, or an extra $27 per month for 24 months added to my cell phone bill if paid off over a two year period. I was well aware that these were full retail prices, and that the carrier often had selected phones on sale for up to half off, but during their recent sale period the phone models that I liked were either not on sale, or were not reduced enough to put them in the "good deal" category.

Being known by the local computer club and by my coworkers as the "resident cheapskate," I decided to search for alternative ways to legitimately purchase a new (to me) smart phone with the features that I was looking for at an acceptable price. Initially, I had narrowed my first choice for a phone to a Samsung Galaxy S4, an Android phone, which has been on the market since the Spring of 2013, but now replaced by the Galaxy S5, and other worthy competitors. Showing a retail price of $699 if purchased outright from a major cell phone provider without a contract, but as low as $49.99 from one carrier if purchased with a two-year contract in which the full price of the phone was amortized over the life of the contract, with the price of the phone being built into the monthly rate. Some of the carriers offered "refurbished" Galaxy S4 phones discounted to around $400, with one carrier being listed on a daily deal website offering a "one day only" online special on a refurbished Galaxy S4 for $348, which was very tempting. If purchased from a carrier, that device is typically "locked" and can only be efficiently used on that particular carrier. My old phone was still somewhat functional, so I decided to continue to shop around.

My first place to look was eBay, as at any given time, they have countless thousands of new, refurbished, and used cell phones listed. eBay had hundreds of listings for the Galaxy S4

varying in condition from "new in box" to being sold for parts only, with the majority being listed as used, while a handful were listed as "refurbished." Several variants of the Galaxy S4 were also listed, including a waterproof model. Not willing at present to switch cell phone carriers, I narrowed the search to phones locked to my existing carrier, or GSM phones that were listed as unlocked, meaning they would likely work on any GSM carrier. Some points to note are that locked phones generally can only be used on the carrier that "locked" or originally sold them, and that unlocked phones using the same method of communicating as my carrier (like GSM or CDMA), may offer at least basic functionality, but may not be totally compatible with the latest offerings of the carriers in terms of high speed data, such as 4G-LTE compatibility. Be aware that some people are selling versions of the same phone that were originally designed for foreign carriers, and while shown as unlocked, may have some serious compatibility issues on domestic networks. Most of the sellers of that phone on eBay listed the manufacturer's model number, which could be easily searched on the internet or the maker's website, which will expressly show the capabilities of the phone. A quick comparison with the specifications on the carrier's website will indicate the likelihood of compatibility; I found several apparent "good deals" on "refurbished - like new" unlocked Samsung Galaxy S4 GSM phones that would apparently work on my carrier's network, but were incompatible with the latest type of 4G data speeds offered by my carrier, but would work fine at the older (slower) 3G or 4G speeds. Similar unlocked offerings were listed on Amazon, but Amazon also often offered the locked phones sold by the carriers, with or without a contract, often at discounted prices. Other bargain prices on new cell phones can be found on a daily basis at "daily deal" websites such as deals.ebay com and at dealnews.com /c171/Electronics Phones-Cell-Phones.

One warning about buying any used cell phone from any source, including individuals, local advertisements, pawn shops, mall kiosks, eBay, and other sources; it is no secret that huge numbers of cell phones are lost or stolen every day. Every cell phone has a unique serial number, often known as an IMEI or ESN number, which if reported lost or stolen, can often prevent that particular phone from being used on its original and often other compatible networks. All of the carriers offer a free online check to confirm the validity of a serial number, or the carriers can be contacted by phone to check to see if a particular phone has been previously reported as lost or stolen. So called "hot" phones may apparently be in excellent condition, and offered at a great price, but there is a good chance that they can never be connected to a compatible domestic network. T-Mobile phones can be checked at t-mobile.com/verifyIMEI.aspx, while Verizon phones can be checked at verizonwireless.com/b2cnso/enterDeviceId.do (item #2 on the list). AT&T, Sprint, Virgin, and other carriers offer similar services online or by calling their respective 800 numbers.

Buying from a local or online big-box store may possibly offer better prices than the cellular carrier's company owned stores or independently owned agency stores. Online stores such as Newegg, TigerDirect, Rakuten (formerly known as buy.com), and others often list new, used, and refurbished, locked or unlocked, cell phones at deeply discounted prices. Buying from a major, reputable seller may have some advantages, as they are more likely than lesser companies to stand behind their products in the event of any problems. As an example, a quick search on one of the above sellers displayed the Samsung Galaxy S4, branded and originally sold by one of the major domestic carriers, but now unlocked, new for $349, and used for $285. It should be noted that there are numerous builds and sub-groups of Galaxy S4 phones, such that the buyer should be acutely aware of what he is buying, and to compare the different models offered, even if they have the same general model number such as "Galaxy S4."

As I was doing my research on a new smart phone, I read many reviews both on my carrier's website and third party websites, seeking that perfect phone that would meet my needs, but at a reasonable price. As I expanded my search to other models of compatible phones, I found that I could purchase fully functional new phones, at deeply discounted prices. I was surprised to find Google was directly selling new, unlocked Android phones, manufactured by the major companies, with the same model numbers as the carrier phones. The phones sold by Google lacked all of the proprietary utilities and app "overhead" of the identical phones sold by the carriers, which freed a substantial amount of the storage (memory) on these phones, and according to some reviews, actually slightly improved their performance. These phones are listed as the "Google Play Edition," and currently include the HTC One (M8), Moto G, and the Samsung Galaxy S4. Coming from Google, these phones are listed as having the latest version of Android installed that is compatible with that model phone, and will automatically receive the next version of Android when it is released. While Google will sell these phones directly at retail price ($649 for the Galaxy S4), they also wholesale these phones to third party sellers. Google claims that these phones are ready to go and fully functional on any compatible carrier, which for the GSM phones are T-Mobile and AT&T.

One of the online stores that offered deals on the Google Play Phones was the Bloomington, Illinois, based eXpansys (www.expansys-usa.com). Being somewhat suspicious of online services offering excellent prices, and since I was unfamiliar with the company, I checked the Better Business Bureau website, and found that the company is eight years old, and has an "A" rating from the BBB. Now, with some degree of credibility, I found that they are selling new and unlocked, the Google Play Edition of the Samsung Galaxy S4 for $399 with $10 shipping; a full $250 to $300 less than the same model phone would cost if purchased outright from a local phone store.

Other fully featured, unlocked, discounted Google Play Edition phones listed by eXpansys are the Sony Z Ultra for $349.99 (retail, $649), HTC One for $399.99 (retail, $649), and the LG G Pad 8.3 for $225 (retail, $330). Many other models of new phones, both locked and unlocked were available, and "Deal of the Day" and "Wednesday Markdown" specials are offered; in fact, I originally found this company on one of the larger "daily deal" websites.

I was seriously considering the Google Play Edition Samsung Galaxy S4 listed above, and had just about made up my mine to purchase one, when I saw a freshly published review of another just released smart phone. The specifications of this new smart phone totally outclassed the Galaxy S4, was highly competitive or superior in terms of features and function with the newer Galaxy S5, and even outperformed most of the features in the latest iteration of the iPhone, but at less than half of their retail prices. Again being suspicious, I thoroughly checked out other independent reviews of the mystery phone and its maker, and made a decision to buy one.

Many people may not recognize the manufacturer, Huawei, but they are a major manufacturer of cell phones, producing several models of cell phones sold by the major carriers. This particular phone, the Ascend Mate2, has a large, sharp, and bright 6.1 inch HD screen, putting it in a class that some pundits refer to as a "Phablet," as it is almost as large as the popular 7 inch Android tablet, but has the usability of a smart phone. The screen on this phone is made of the almost unbreakable Corning Gorilla Glass 3, and has a very long lasting battery. Extremely fast and feature rich, using a 1.6GHZ Quad-Core processor, 32 GB of internal memory (expandable up to another 64GB using a common micro SDHC memory card), this phone is thin, and surprisingly lightweight for such a large phone. I mostly carry my phone in a shirt pocket, and this phone does fit in most of my shirt pockets.

The Ascend Mate2 operates on one of the latest builds of Android, and will be upgraded to newer versions of Android after they are tested and proofed, including the upcoming version nicknamed "Android L." Huawei decided to sell the Ascend Mate2 directly to the consumer, without the additional markups imposed by the big carriers. Currently available in GSM only, this phone is fully compatible with T-Mobile and AT&T, including their latest and fastest versions of 4G, such as 4G-LTE. Available with free shipping from Huawei at gethuawei.com, or from its other sole source seller, Amazon, this phone sells for only $299 (plus sales tax) with free shipping. Since it is a direct purchase and unlocked, it only requires that a compatible SIM card be installed in the back of the phone. Most current AT&T and T-Mobile customers can simply remove the SIM card from their current phones and insert it into the Ascend Mate2; no further activation is normally required, and both carriers now readily accept this phone on their respective networks. Other users, those without an AT&T or T-Mobile ac-count, may have to obtain a compatible SIM from the respective carrier, and sign up for an appropriate service plan, but monthly rates may be more reasonable as they are not including the cost of the phone in the monthly plan.

For those who are currently happy with their phones, but who may wish to take advantage of the newly lowered monthly rates and improved plans offered by competitors without purchasing a new phone, help is on the way. Both houses of congress recently passed HR1123, the "Unlocking Consumer Choice and Wireless Competition Act, which will again legalize consumers "unlocking" their cell phones, and using them on another compatible carrier. Expected to be signed by the president into law by the time you read this, this law will not excuse users from any existing contractual obligations with their current carrier, but will allow users to take their current phone with them when they switch to another compatible carrier, such as between AT&T and T-Mobile. Some of the major cell phone carriers have already implemented a "We'll pay your early termination fee" program for those switching to the new carrier, but now consumers may be able to continue to use their current compatible phones, rather than be required to purchase new phones from the new carrier. To encourage new business and to retain existing customers, almost all of the major carriers already have a "bring your own phone" policy. As the title of the law says, this should increase consumer choice among carriers, as another potential obstacle of switching carriers has come down.

For those willing to take the time and effort to do a little research, a greater selection of compatible cellular phones are readily available, often at deeply discounted prices, when compared to the offerings of the cell phone companies. Unless you want the convenience of purchasing a new (or refurbished) phone or tablet directly from your carrier, substantial savings on new phones may be available from others, such as those Google Play Edition and Huawei phones mentioned above.

Websites:

https://beta.congress.gov/bill/113th-congress/house-bill/1123
http://bits.blogs.nytimes.com/2014/07/25/bill-legalizing-unlocking-cellphones-passes-congress/
http://www.ktvu.com/news/news/national/congress-oks-unlocking-phones-carriers/ngpKY/
http://www.t-mobile.com/verifyIMEI.aspx
http://www.verizonwireless.com/b2c/nso/enterDeviceId.do
http://www.gethuawei.com
http://e.dx.com/collection/201407/Doogee/auus/default.html
http://www.expansys-usa.com
http://deals.ebay.com
http://dealnews.com/c171/Electronics/Phones-Cell-Phones/

Courtesy of Mr. Wilsker.

Is Windows XP Coming Back?

Q. I am debating about buying a new laptop with Windows 8. I know that some people don't like Windows 8. Do you think Microsoft will keep this format in the future or will it go back to something like XP or the Windows 7 format? How do you feel about Windows 8?

A. I think Windows 8 is fine. I like the touch screen interface, which is what it was designed for, though it certainly can be used with a traditional mouse and keyboard. Historically, whenever a new operating system makes its debut, there are people who like it and people who don't like it. I call it the Broccoli Syndrome.

Microsoft is not going to return to an older format because a few people complain, however. Windows 9 is already in the works and will be the next step in the evolution of Windows, but it isn't going to revert back to something akin to Windows 3.1, 98, XP or even Windows 7. Time and technology move ahead with us or without us.

When Windows 98 was released eons ago, there were some people who hated it because it represented such a big change from the previous version. The same thing occurred when XP replaced Windows 98. Over time people settled down and became comfortable with the new operating system and that will happen with Windows 8, as well. Then, when Windows 9 is released, the Broccoli Syndrome will return. If you decide that you do not want Windows 8, you can still purchase Windows 7 on amazon.com or from other retailers.

Q. Is there a limit to how many times I can use my Windows 7 Recovery Disk to format my hard drive?

A. There is no limit, so you can use your Recovery Disk until the cows come home – if you are, indeed, expecting bovine visitors. Doing so will not damage the Recovery Disk so there is nothing to be concerned about as far as over-using it.

Q. How do I delete all data from a flash drive so that I can put new information on it?

A. Formatting a flash drive will wipe all data off the drive. If that's what you would like to do, start by inserting the flash drive into a USB port on your computer. Click Computer (depending on your version of Windows), then right-click your flash drive icon and select Format.

You will see the capacity of the drive and various bits of technical information nobody ever pays attention to. You might want to consider changing the Volume Label, which is the name that will appear next to the drive letter for your flash drive. I like to name my flash drives

something short like “Morry” or “Edith,” but other people prefer something more descriptive, such as MP3Files or WorkDocs. You don’t have to change the Volume Label at all, if you prefer to leave things as they are.

Remove the check mark beside the Quick Format box, then click Start to format your flash drive. The formatting process will probably take a few minutes and you may see a green progress bar. Once formatting is complete, your flash drive will be squeaky clean and devoid of all data that it previously contained.

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

NaughtyCodes.com

Though it sounds like an adult-oriented Web site, it is not. This site provides access to a database of discount codes that are available to shoppers when placing an online order. Select an online store from the drop-down menu and you will see the code and the discount. Sure it’s naughty, but it’s also kind of nice. A similar site that I have used successfully a number of times is Retailmenot.com

www.naughtycodes.com

The Labyrinth

If you are a student of Medieval Studies – and who among us isn’t? – you won’t want to miss this. Sponsored by Georgetown University, The Labyrinth provides free access to a plethora of resources, including connections to databases, services, texts, and images around the world. Each user will be able to find an Ariadne’s Thread through the maze of information on the Web. (As we all know, Ariadne was the daughter of King Minos of Crete. Minos had Daedalus build a Labyrinth, which was a house of winding passages. So who is Daedalus? Yes, it’s THAT Daedalus, the father of Icarus, uncle of Perdix and Iapyx, of course.)

http://bit.ly/1j8k7Zz

Twisted Questions

Would you rather die by a boulder falling on you, falling off a mountain, or getting hit by a meteor? Or let’s say you’re standing on a stage in front of a huge audience, about to play a lengthy violin solo. The problem is, you don’t know how to play the violin. What do you do? Described as a “playground for the mind,” this site asks bizarre, occasionally troubling questions and invites your input and participation. Some questions may occasionally be a bit on the coarse side, so be forewarned.

www.twistedquestions.com

Use Promo Code MODEM 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. Courtesy of Mr. Modem.

Seven Cool Things You Can Do With Dropbox

by Bob Rankin

You can do more than just drag-and-drop files to Dropbox, and you don’t have to jump through a lot of hoops to do so. Here are seven of the coolest things you can do with Dropbox…

Dropbox is a free web-based service that enables file storage, sharing and syncing. You can think of it as an extra hard drive in the cloud, or a convenient way to keep files synchronized across your desktop, laptop, tablet, or smartphone. You can share files with family, friends or work mates. Dropbox is also handy for sharing large files that are too big to be sent by email.

But those are just the obvious things mere mortals can do with Dropbox. There are several clever uses for Dropbox that may save you time or money, and possibly turn you into a wizard.

Here are some things you can do with Dropbox that made me slap my forehead and say

"Wow!" the first time I came across them. You may want to don protective headgear before proceeding...

1. Choosing Favorites – Designating a file stored in your Dropbox as a "favorite" downloads a copy to your device(s), so you can read, watch, or listen to favorites even when Internet access is unavailable. Might come in handy for ebooks, music, videos, or work-related documents.

2. Documents Folder on Steroids – Using your Dropbox folder as your default My Documents folder means never leaving important work behind when you rush to the airport. Changing the physical location of My Documents requires some simple commands in Terminal for Mac OS or a minor tweak to the Properties of My Documents in Windows.

For Mac OS, open Terminal (under Utilities) and type "cd Dropbox" then press Enter. Next, type "ln —s ~/Documents /Documents" and hit Enter once again. For Windows, Click the Start button and then click your user name. Locate and right-click the My Documents folder. Click Properties, then Location, then Move. Select your Dropbox folder.

3. Just Email Me – Emailing files as attachments is an alternative way to get them to your Dropbox. Just sign up for a free account at SendToDropbox.com and get a custom email address for that service. Every file attachment your email to that address will instantly appear in your "Attachments" folder on Dropbox. You can also automatically forward file attachments sent to Gmail addresses to your SendTo Dropbox.com email address.

4. A Drop in the Bucket – On a related note, URLDroplet takes a file directly from a URL (web address) and adds it to your Dropbox. You don"t have to download the file and then upload it to Dropbox; just copy the file's URL into the URLDroplet.com input box, or use the bookmarklet.

5. Back it Up! – Entire Web sites that you control can be backed up to Dropbox automatically. The Wordpress Backup to Dropbox plugin is one easy way to ensure that your Web content is safely backed up constantly.

6. Instant Webmaster – Dropbox can even "host" a simple Web site for you. You don't need to buy a domain name or learn HTML. Using services like DropPages or Pancake.io you can create and share portfolios of files stored on your Dropbox account, or automatically display the ever-changing contents of a Dropbox folder.

> Did you know…? Your free Dropbox Basic account gives you 2 GB of free cloud storage space and you can earn up to 16 GB of additional space by referring friends, taking a Dropbox tour, connecting your Facebook or Twitter accounts, or using it to manage your mobile email.

7. Cover Your Tracks – Mozilla Firefox Portable Edition is the Firefox browser bundled with the Launcher app created by PortableApps.com. Download the Firefox Portable kit and install it, designating your Dropbox or another cloud service folder as the installation location. Then you can use Firefox from any computer and all your custom settings, bookmarks, etc., will be available. But when you finish a session and move on, no traces of your online activity are left behind.

Dropbox encourages app developers and third-party service providers to develop neat new services that incorporate Dropbox's capabilities. There are many more examples than these.

ALERT: Serious Security Flaw in USB Drive

Is Malware Lurking in Your USB Gadget?

To demonstrate the vulnerability of USB drives, the researchers wrote some proof-of-concept malware (which we can only hope no one copies) called BadUSB. It is a collection of malicious apps that can modify any software installed from a USB drive on a target computer; completely take over control of an infected PC; and even redirect users' Internet traffic.

Erasing or reformatting the USB drive does not destroy the malware, which hides in the USB device's firmware that controls the drive's basic functions. This previously unknown vulnerability is part of the USB standard's design; as such, it can't be eliminated without re-engineering every USB device.

"These problems can't be patched," says Karsten Nohl of Black Hat. "We're exploiting the very way that USB was designed." Nohl and Jakob Lell, of SRLabs in Berlin, planned to demonstrate their code at the BlackHat 2014 conference held on August 7th. That will either shine a bright light on the problem, or spawn a cottage industry of hacking USB devices, or both.

We've long known that using USB flash drives can be dangerous, because a virus can be stored as a file on the drive. But any decent anti-virus tool will catch that type of thing. However, standard anti-virus scans can't see or touch the firmware that controls a USB drive's basic input/output functions. Security pros would have to reverse-engineer the firmware of a USB device and know what to look for in order to detect this threat. That would require some specialized expertise and equipment to analyze firmware.

It's Not Just Your Flash Drive...

But wait, the news gets worse: it's not just USB flash drives that are vulnerable. Any USB device, from a mouse or keyboard to a digital camera or smartphone charger, contains firmware with the same exploitable vulnerability. While such devices aren't shared among users as promiscuously as USB flash drives are, it's very possible to pick up an infection from anything that plugs into a USB port.

As Nohl says, you must "treat USB devices like hypodermic needles that can't be shared among users." This drags safe computing, safe sex, and drug use into the same murky metaphor pool. But it's a real problem that shouldn't be ignored.

The BadUSB demo malware suite can do a lot of evil tricks. It can sneak Trojan software past anti-malware defenses. It can imitate a USB keyboard and execute any commands on the target PC. It can hijack Internet traffic and change DNS settings to redirect a user's outbound traffic to any server it pleases. If planted on a phone or other USB device with an Internet connection, it can eavesdrop on a user's communications.

There is currently no way to ensure that your USB device's firmware is clean of such malware. There are no digitally signed versions of USB firmware that can serve as certified "clean" standards.

The only defense against the USB attack vector is to jealously guard your USB devices. Don't plug them into any port that is not a trusted device, say the experts. But following that protocol will drastically reduce the usefulness and convenience of USB devices.

For example, you can't safely plug your flash drive or phone charging cable into a friend's computer, unless you are 100% certain that person's computer is virus-free. (Plugging into a USB port on a PUBLIC computer has never been safe.) Neither can you trust a flash drive, mouse, keyboard or digital camera that you've borrowed, bought used, or that has been used by someone who is not diligent about security. Presumably, USB devices purchased new will be safe.

What's The Solution?

USB device manufacturers will have to step up and address this problem. One solution is

to implement "code signing," an encrypted digital certificate that certifies a firmware package was clean when it left the factory and has not been altered. But first, we"ll have to convince OEMs that this is their problem, not just ours. And that solution will only fix the problem for new USB gadgets, not the untold millions already in circulation.

Nohl told *Wired* magazine that he contacted an unnamed USB drive maker and described his team's findings. The vendor repeatedly denied that it was possible. *Wired* contacted the USB Implementers Forum, a trade organization that manages the USB standard. Its spokesperson responded with this statement:

"Consumers should always ensure their devices are from a trusted source and that only trusted sources interact with their devices," she wrote. "Consumers safeguard their personal belongings and the same effort should be applied to protect themselves when it comes to technology." In other words, it's your problem and no concern of the people who sold it to you. That will not sit well with consumers.

Let me reiterate ... any USB device (flash drive, external hard drive, smartphone, digital camera, mouse, keyboard, etc.) that has been plugged into an untrusted computer should be treated with suspicion – much like a used hypodermic needle. Further, erasing, formatting, or using anti-virus tools will not remove malicious code from the firmware of USB devices. And there is no known method at this time to scan USB devices to see if they are clean.

So on a practical level, what should you do? I think it's important to recognize that this vulnerability is new, and (as far as we know) it hasn't been exploited yet. So it seems likely to me that we don't have USB gadgets with infected firmware in circulation, for now. My advice is that if you use USB devices, do so with this threat in mind from now on. A 32 GB flash drive sells for about $15. If you have a flash drive that's been connected to unknown or public computers, you might want to discard it.

You can sign up for Bob Rankin's regular postings at www.askbobrankin.com

Linux and the Malware Threat

by Bill Wayson

By now, all users of Windows should be aware of the CryptoLocker ransomware Trojan software and be alert for it. If you are not, CryptoLocker is a nefarious type of mal ware that uses social engineering to do its work. It's often disguised as an email attachment, and users who unwisely click on the payload launch a program that encrypts their files, deposits the decryption key on a server, and then displays a demand for payment from the user to have the files decrypted. If the user doesn't pay within a certain length of time, the decryption key is erased, rendering the files essentially inaccessible and, if not backed up, lost. There is some variation, but this is the essential theme. This is nasty software, but is it something that Linux users need to be concerned about? The answer depends on what Linux is being used for.

Linux users, in general, do not need to be as concerned as Windows users about CryptoLocker or other mal ware threats. There are a few reasons for this: Not much malware is written for Linux; the Linux security and user models make it much harder for broadly damaging attacks to succeed; and vulnerabilities in Linux and open source applications are usually fixed quickly and continuously. Let's dive a little deeper into how each of these contribute to decreasing Linux's vulnerability to malware.

Some simply declare that Linux does not suffer from malware threats because nobody writes malware for Linux, and that little is written simply because the number of users of Linux is so small. While the first statement is true – there is little malware out there that targets Linux, and the number of home users of Linux is small, the two are not necessarily related.

The reason few crackers write mal ware for Linux is more complex than just the lack of a large target audience. Writing such malware is difficult. A significant hurdle is the number and variety of Linux distributions. A malicious executable program written for one distribution of Linux, and sometimes for one specific kernel version, may very well not even run under a different distribution or kernel. If you want to propagate a large scale attack using executable programs, you may need to write or compile a specific version for each distribution on your target list. While the Linux home user base is small, Linux is used in situations that are very tempting targets for the bad guys. A successful attack against Apache, a very popular Web server, or Bind, a popular DNS server, would place that malware at a major internet junction with access to millions of computers of every variety. Yet such attacks remain very rare. It is probable that little malware is written for Linux and open source software because of the difficulty of doing so coupled with the following two reasons:

- The Linux user model lends itself to users being able to work on their computers with just enough privileges to do so, and no more.
- This works in tandem with the file and folder security model, which assigns different rights to the owner, a specific group of users, and everyone else for each file and folder. On any computer, successful malware can only damage what the user account it runs under can damage. Since virtually all software running under Linux does so as "normal" (i.e. unprivileged) users, significant parts of the computer, such as the operating system itself, are protected. If I inadvertently launch malware while using my Linux PC, unless it can escalate its privilege level, only my personal files and folders are vulnerable. The rest of the PC will survive unscathed.

If some mal ware does successfully run on a Linux PC, achieve root (the Linux administrator account) privileges, and wreak widespread damage, such success will be short-lived. Linux and popular open source software are constantly being developed, fixed, and improved. Each Linux distribution vendor provides a software management system that easily keeps not only its Linux OS, but all of the software included in the distribution up to date with fixes for vulnerabilities that are found. Even the revelation of the embarrassingly long-lived Heartbleed flaw in OpenSSL led to a change in the culture of that project that should reduce the possibility of a similar recurrence. Thus the hard work of a good malware writer is soon rendered moot.

There are some users of Linux who should be very wary of malware, not be cause of their vulnerability, but because they may pass it on to others who are less fortunate. A notable example is anyone running a Linux-based mail server. They should be running up-to-date mal ware scanning software to avoid delivering malicious messages to email clients. Several Linux-based applications exist, for doing just this.

Linux and open source software are not immune to malware. But the variety of versions and distributions make a successful, widespread attack much more difficult to achieve. And like any system, its vulnerability is directly related to its weakest link, which is usually the human user. If users can be convinced to do something they really should not do, all bets are off. Linux users can be more comfortable with the security of their PCs, but they should remain vigilant and aware. If something seems fishy, it may very well be fishy.

From July 2014 issue of The Outer Edge*, newsletter of the Channel Islands Channel Islands PC Users Group .*

10 Stupid Things You Can Do to Mess up Your Computer

by Bob Rankin

askbobrankin.com

Aside from actually drop-kicking it or smashing it with a sledge hammer, it's fairly difficult to actually break a computer. That said, there are a number of ways to render your computer just slightly more useful than a doorstop. Certain careless acts can cause crashes, freezes, painfully slow performance, loss of data or invasion of your privacy. Here's my list of stupid things you can do to really mess up your computer...

Okay, I'm using a little reverse psychology on you... If want to keep your computer running smoothly and avoid becoming a target for cyber criminals, here are ten things you should NOT do.

1: Not Using Anti-Malware Protection – This is perhaps the most common way to make a system inoperable, and the easiest problem to avoid. Not using an anti-malware program (or using one that's out of date) is akin to leaving the front door of your house wide open with all of your valuables on prominent display. Having an unprotected system is an invitation to allow all kinds of nasty things like spyware, trojan horses, viruses and root kits to access your system. Virus and spyware creators do this in the hope of gaining control of computers for nefarious purposes, or getting access to sensitive information that may be stored on a hard drive. And of course, viruses and spyware can significantly slow down a machine.

Be safe, use a good anti-virus program to keep out the bad stuff. See my recommendations in *Free Anti-Virus Programs and Five Free Malware Removal Tools*.

2: Failing to Apply Security Patches – New computer security threats crop up almost daily, as hackers, crackers and other cyber villians attempt to find and exploit holes in the operating system and application software we use every day. Unpatched vulnerabilities can lead to virus infestations, enslavement in a botnet, or even identity theft. And no software is immune, whether you run Windows, Mac, or Linux. You need to configure your system to automatically download and install security patches for your operating system, office software, web browser, Java, email program, PDF reader, media player and other software you use. How do you do that?

Take advantage of the tools built into your operating system – Windows Update, Mac OS X Software Update, or Ubuntu Update Manager – and make sure they're set to run on auto-pilot every day. Other software that you've installed may offer the same type of automatic updating capability. Don't ignore the warning messages from the updaters, and apply fixes as soon as they are available. See *Computer Security: The Missing Link* to learn more about securing the software on your computer.

3: Clicking on Bogus Popups – Popup ads are intrusive, annoying and seemingly everywhere on the Web. Yet, it is amazing how often some computer users will mindlessly click on them. Popups will promise you anything from a free dinner for two to ridding your machine of viruses with one click. These ads can mask spyware and malware that gets loaded onto your machine behind-the-scenes. Also, a lot of them are just annoying links to endlessly long surveys that offer a free laptop or iPod, with the catch being that you have to sign up for a lot of paid services that you probably really don't need. The use

of a good anti-malware program plus using the popup blocker that comes with a lot of browsers, can help keep the popup ads at bay.

Here's a tip to tell the bad popups from the ones that are important. A type of popup called "balloon notifications" are attached to the Windows taskbar at the bottom or side of your screen. These are usually important and should be heeded. Malicious popups typically appear in a window floating in the middle of your screen. (Some good ones, too, though.) If you're unsure, ask a friend, Google the text in the popup, or just close the window by clicking the red button at the top. Don't click inside the popup window, or you could get sucked into a vortex of cyberslime.

4: Not Using a Firewall – Yes, your computer needs a firewall. But probably not the kind everyone is telling you to install. Chances are, you already have an excellent firewall built in to your high-speed modem/router. Find out more about the two kinds of firewalls, and which one you need in my *Do I Need a Firewall?* article.

5: Unsafe Downloading – It can be tempting to download "free" pirated versions of games, movies or popular software packages. But beware the warez... tools like Bittorrent, and rogue download sites can lead to nasty surprises. Some downloads have been modified to contain embedded viruses or trojan horses that can compromise your system. Stick with safe download sites such as FileHippo, where you can find tons free software and shareware that's certified malware-free. (See *Is Bittorrent Downloading Illegal?*)

To make matters worse, some previously trustworthy downsites have become landmines of unwanted "foistware." My article *Downloading? Watch Out For These Danger Signs* will show you how to download safely, while avoiding unwanted toolbars, sneaky spyware, and changes to your settings.

6: Falling for Phishing Scams – The Nigerian email scam has become as well-known a confidence game as the old shell-game. But it still is astonishing how many will fall for it. The news reported recently about a woman who lost almost half a million dollars to email scammers. Also, be on the lookout for those very official looking phishing attempts. An email may come to your inbox that looks like it's from your bank, Ebay, or Paypal. You open it up and it is asking you to verify your information by entering your password, social security or account number. And it's scary how precisely the emails (and the sites they link to) match the real ones.

Bottom line: no one has any business asking for your private information via email. If you have any questions about a suspicious email that looks like it came from a place you do business with, call that company to verify, and always use a bookmark or manually key the address of sites that require a login. Read more about phishing, and how to protect yourself from these online scams in *Can You Smell a Phish?*

7: Not Securing Your WiFi – Ever notice your Internet connection slowing down? This could be the result of strangers mooching off your wifi bandwidth. If you leave your wireless router wide open and unsecured, it's an open invitation for neighbors and passers-by to connect. But in addition to sharing your internet connection, you're also exposing yourself to hackers and possibly even legal liability. Best practice is to enable encryption on your router by setting up a strong wifi access password as the key. Many users neglect to change the

default username and password of their home routers, information which can easily be found online. Why take a chance? Read my article *Wireless Security Checklist* for help getting your router secured.

8: Haphazard Deleting – It's not so hard to fill up a hard drive these days, even with the large storage capacity that comes with machines. But when you feel like doing some housekeeping on your system, make sure you know what you are deleting. The deletion of files residing in system folders or program folders can cause your operating system or applications to crash. Usually, Windows will not let you delete critical system files, but play it safe: if you are not sure what you are deleting, leave it alone and do some research on it first. When it come to housekeeping, better options for freeing up drive space are removing unnecessary software with Add/Remove Programs, or running the Disk Cleanup utility. For heavy duty disk scrubbing, read my tips for a *HOWTO: Clean Up Your Hard Drive*.

9: Forgetting to Back Up – This is a heart-breaker because it so easy to avoid. Sooner or later, you WILL accidentally delete an important file, or experience a hard drive failure. Always make sure that you back up any critical files, and on a regular basis. Backing up is so easy now with external drives and online backup services. No messy tapes or piles or floppy disks... Shame on you once if you lose a file, shame on you twice if you didn't remember to back it up. See my related pieces on *Demstifying the Backup and Free Online Backup and Software Options*.

10: Still Running Windows XP? – Microsoft dropped support for Windows XP on April 8th, 2014. That means no more updates or security patches will be issued for this rusty old operating system. See my article *Windows XP: Game Over* for details on why you really should upgrade, and learn about *A Free Windows XP Alternative.*

President's Message

On Tuesday August 12th our computer club had a very successful "GEEK PICNIC." The way the weather was in the morning I knew the rest of the day had to be much better. What made this picnic one of the best is everyone there helped by doing whatever had to be done, without asking. There were 21 members and a guest in attendance. Once again Tony Delello did an excellent job cooking the meats. I had my best friend's daughter, a RIT photo student, take photos so we would have a record. Emma, thank you.

After eating we all went outside and participated in two geek type games. Hard disk toss (shot put) seven took part and Tony almost put it in the pond. We can now call Tony "the arm." The second game a geek version of cd golf. No one got a hole in one. After the first round we had a tie. Wally won the run off, (I think he had a little help. His granddaughter is a weather person on Channel 8). She might have helped him by taking in the direction of the wind. (ha,ha) We got back inside and did it rain.

The action at the auction table was hot and furious. We covered everything from books, wine, cookies, a complete lap top, a desk top computer, monitor, and keyboard.

In closing we got to meet a couple of our newest members. Now I have a face to put with e-mail. Everyone thank you.

–Steve Staub

WINDOWS: Please enter your new password.
USER: cabbage
WINDOWS: Sorry, the password must be more than 8 characters.
USER: boiled cabbage
WINDOWS: Sorry, the password must contain 1 numerical character.
USER: 1 boiled cabbage
WINDOWS: Sorry, the password cannot have blank spaces.
USER: 50bloodyboiledcabbages
WINDOWS: Sorry, the password must contain at least one upper case character.
USER: 50BLOODYboiledcabbages
WINDOWS: Sorry, the password cannot use more than one upper case character consecutively.
USER:50 BloodyBoiledCabbagesShovedUpYourAssIfYouDon'tGiveMeAccessNow!
WINDOWS: Sorry, the password cannot contain punctuation.
USER: ReallyPissedOff50BloodyBoiledCabbagesShovedUpYourAssIfYouDon'tGive MeAccessNow!
WINDOWS: Sorry, that password is already in use.