Newsletter
Connecticut PC User's Group

September 2014
Vol. 33 No. 1

Next CTPC Meeting — Tuesday, September 23, 2014 - 6:30 p.m.

Roundtable Discussion

Passwords are a necessary evil for secure computing. We hate them but we acknowledge their importance. This month's CTPC meeting is a round-table discussion about how to handle passwords – how to make them strong and how to keep track of them.

Weak passwords such as "password" or "12345" are easy to remember but also easy to crack. The name of your street or your pet's name is easy to remember but can be easily deduced. Using the same password (even a strong one) for every website you visit works fine until one site you visit is hacked – then your entire online security is compromised.

What can you do? Here's a range of ideas:

- Write down your passwords on sticky notes.
- Create strong passwords that are difficult to figure out but difficult to remember.
- Keep all your passwords in a text file or spreadsheet.
- Encrypt the text file or spreadsheet.

Continued on Page 6

Sept 23rd, Tuesday, 6:30 p.m.
CTPC Meeting
Location: United Congregational Church, 275 Richards Avenue, Norwalk

Oct 28th Tuesday, 6:30 p.m.
CTPC Meeting
Location: United Congregational Church, 275 Richards Avenue, Norwalk

GENERAL MEETINGS

Meetings are held on the 4th (not last) Tuesday of the month. There is no charge to attend general meetings. See back page for directions.

www.ctpc.org

Diane Fahlbusch, President, ICON PC User Group (ICONPCUG), Long Island, NY, May 2014 issue, ICONPCUG, Graphic, editor (at) iconpcug.org

Multitasking: the Big Myth

Multitasking became the highly touted skill to possess back at the start of the millennium. The business world thought that more work could be accomplished with the same amount of people with this method. However, do we really all mean the same thing when we say it? Can one learn how to multitask? And, the most important question, does multitasking make one more productive? Well these questions have been the focus of numerous studies worldwide spanning over a decade. They have yielded some interesting results.

Multitasking is actually defined as performing more than one task simultaneously. An example of this is holding on a conversation while typing an email to a business associate. According to Earl Miller, a professor of neuroscience at MIT, we just cannot focus on more than one thing at a time. However, many people use the same expression to describe performing one task at a time, and then switching to another one quickly. Working in one program on your computer, and then switching to a different program in another open window is a common example. This is actually called "task switching", but it is often lumped under the category of multitasking.

Another statement is that one must "learn to multitask". This is true to a certain extent – all activities are learned. But "learning to multitask" is the wrong expression. What it really means is learning tasks so well that you do not need to concentrate to perform them properly. Think back to when you were four or five years old and just learning how to tie your shoelaces. You needed to concentrate and could not focus on anything else. But now you probably could NOT tie your shoelaces if you ACTULLY concentrated on doing it. However, when at least one task requires you to concentrate to accomplish it, multitasking is not necessarily happening. One is typically not doing either task well. As an example, most people listen to the radio while driving. But can you actually name the songs that were played, or remember the words? (Even when not attempting to multitask, most people do not pay attention to the lyrics. Think back to when the President Ronald Reagan quoted "Born in the USA" in a patriotic speech, and missed that it was NOT a patriotic song.) The more prevalent example is driving and talking on the cell phone. In spite of the laws that have been passed, people still do it.

But can one improve one's multitasking ability? "According to David Strayer, director of the applied cognition lab at the University of Utah, who studies multitasking in the fertile realm of distracted driving, 'ninety-eight percent of people can't multitask—they don't do either task as well.' … And he found that, sure enough, the very structure of the supertasker brain looks different than those of 98 percent of us. 'These brain regions that differentiate supertaskers from the rest of the population are the same regions that are most different between humans and nonhuman primates,' says Strayer. In other words, the brains of supertaskers are just that much further away from those of apes, 'the leading edge of evolution,' says Strayer. Specifically: 'Certain parts of the frontal cortex are recruited in an interesting way,' says Strayer. In fact, these areas show less activity when multitasking than do the same areas in normal, human, mammalian, non-alien-overlord brains like mine. And it's distinct—you either efficiently recruit this region or you don't. You're either a supertasker or you're not." [1]

So much for learning to multitask! So what about giving task switching a try? Here are some fascinating facts.

Continued on Page 8

Table of Contents

Multitasking: the Big Myth	1
Password Managers: How to Use One	2
Backup...Backup...Backup	3
Be Careful of Buying Old Versions	4
The Tip Corner	5
CTPC News	6
Interesting Internet Finds	7

Mike Morris, *President / Editor, Front Range PC Users Group, Fort Collins, CO, Originally published in k-Byte, the newsletter of the Front Range PC Users Group, www.frpcug.org*

Password Managers: What They Are and How to Use One

Introduction

A password manager application is ". . . software that helps a user organize passwords. . . . The software typically has a local database or a file that holds the encrypted password data for secure logon onto computers, networks, web sites and application data files . . . ." (Wikipedia) (http://bit.ly/PhVjkz).

Before you ask "why bother," think for a moment about how many web sites you connect to that require a password. Do you use the same (or very similar) password for most or all of those web sites? If you are like the overwhelming majority of computer users, the answer to that question is likely to be "yes."

You should, very definitely, NOT do that!

All of the computer security experts (and there are a lot of them these days) warn us not to use the same password for all accounts. For example:

"The message of password reuse security is one that Hord Tipton, executive director of the International Information System Security Certification Consortium (ISC2), echoes. (www.ics2.org)

"Diversifying your passwords for each account is essential to protecting all of your online information," Tipton said. "Once a password has been stolen, hackers often attempt to access multiple accounts, compounding the potential damage.""

Source: Yahoo Email Is Breached: Lessons Learned (http://bit.ly/1h5jSZi)

See also Password Security, Protection, and Management (http://1.usa.gov/1fYSklG)

With respect to Mr. Tipton, "diversifying your passwords" is much easier said than done . . . unless you use a password manager.

There are a number of these applications (for example, see this http://bit.ly/PhT1Sg), but one, KeePass, is a ". . . free, open source, cross-platform and light-weight password management utility for Microsoft Windows, with unofficial ports for Linux, Mac OS X, iOS and Android . . . ." Wikipedia (http://bit.ly/1k8zUV3).

In fact, if you need a lot of passwords (I counted over 70 web sites that I use that need a password), it is almost impossible to keep track of them. But even if you have just a few (10 or a dozen), a password manager can be extremely helpful, and provide **an extra measure of security for you**.

How do password managers provide this extra security?

With KeePass the extra security is provided through these features:

1. All your passwords are stored in one database.

2. The database is locked with one master key or a key file, so you only have to remember one single master password (OK, you also need to remember the password to your computer, so that's 2 passwords you have to remember).

3. The database(s) is (are) encrypted using (one of) the best and most secure encryption algorithms currently known (AES).

4. KeePass can generate strong random passwords for you.

Source: KeePass Password Safe (http://bit.ly/IzB7qC)

Since KeePass is open source, you get this extra security for free.

If all of those features sound a little "techie," don't worry, KeePass is actually easy to use. Therefore, KeePass (v. 2.20) will be used to demonstrate how you use a password manager application. As with all good things, it takes a little effort to enter the data—at least, it does if you need as many passwords as I do.

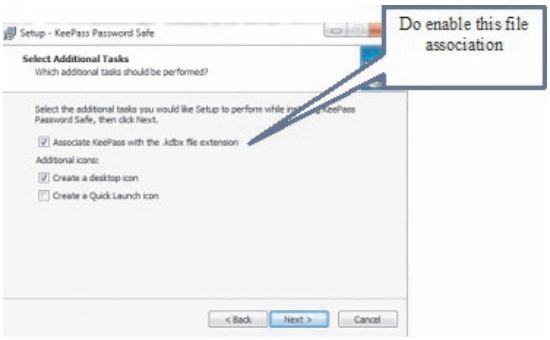
Installation

You can download the current version (which, as of 02/04/2014, for Windows, is 2.25) from the KeePass web site, http://keepass.info/. The installation follows the usual Windows sequence. However there is one window in the sequence worth a comment (see top of next column):

This step may not be necessary at this point, but establishing that file association at the beginning probably reduces the risk of future problems.

Set Up

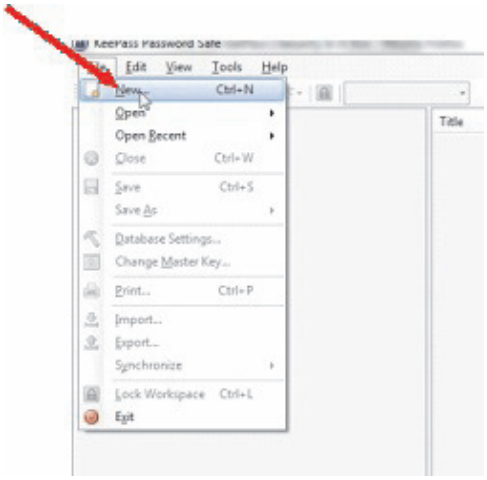
Once the installation is complete, at the first launch you will see the KeePass main screen.



At this point, you have two primary set up tasks:

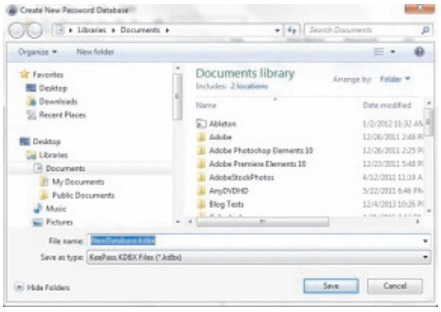
1. Create a database
2. Enter data into the database

You create a database with these steps:



Click on File, then on New:

You will be asked (in the usual Windows format) to decide where you want to save the program. Here is an example of that window from my computer:



The default Save location for Windows 7 is, of course, Documents. Remember, you can choose to save the database anywhere on your computer. I set up a separate folder called KeePass in the root

Continued on Page 5

Phil Sorrentino, Past President, Sarasota PCUG, FL, February 2014 issue, PC Monitor, www.spcug.org, philsorr (at) yahoo.com

Backup...Backup...Backup

I know you've all heard this before, but it is very true. Backup your data and backup your system. When we talk about the Backup activity, we mean copying the files that you definitely want to have, should you lose your computer. But first, I'd like to discuss some Backup Philosophy. There are many levels of backup. The correct amount of backup is that level that lets you sleep at night. (Kind of like a well balanced portfolio.) You have to have enough backed up and you need enough backup copies. No doubt this can be taken to the extreme, as I'm sure it is by many obsessive-compulsive types. But, everyone needs to make these decisions;

1. What shall I backup
2. How often shall I backup, and
3. How many backup copies do I need.

Before we answer these questions, a few words on why we back up. In a perfect world we would not need to backup anything. Every time we turned on our computer, it would turn on without a hesitation or problem. And, there would never be cause to worry about viruses, spyware or any such malware, because they would not exist. Unfortunately this is not a perfect world and we have to be concerned with potential hardware and software problems. Hardware sometimes fails, and software problems and malware do exist. So, backup is protection against some hardware failures, namely hard drive failures. And backup is protection against software problems or an infection of malware. In either case not having your data and system backed up may force you to re-load your system and begin from a fresh start, and/or spend a lot of time reproducing the data that was lost.

Now back to those questions. The first one, what to backup? Generally, the answer is: all of the data that you have produced and is difficult to re-create, and your system (Operating System and applications that you are using). So this really has two components, data and system. Data backup is the easier. Just copy all the files you want to backup to another drive (internal, not on the same physical drive, or external), or to other memory devices such as CDs, DVDs, and flash memory devices. The amount of data to be backed up helps determine the backup media. For small amounts of data, CD or flash memory devices work just fine. For large amounts of data, a second internal hard drive, or an external hard drive is probably a good choice. (External hard drives seem to becoming the best choice for most backup needs.)

Data Backup

So, what exactly are we backing up?

1. All of your digital pictures. These are usually .jpg or .bmp file types. Actually, there are many other file types that could be pictures or graphics. But with modern digital cameras, most of the pictures are going to be .jpg (or .jpeg, or .jpe) file types. These are probably in a general "photos" folder.

2. All of the data that you have created using "Office like" applications. Such as .doc, .xls, .ppt, .pps, .docx, .xlsx, .rtf file types. These files usually include personal and financial data that you have created for convenience. These could be in a general "Personal Information" folder or they could be spread out among a few folders.

3. All of the video files you have created or collected. Again, there are many video file types. Some of the more common ones are .mov, .avi, .mpg, .vob, .wmv, .swf. Many of these are created by digital cameras shooting video, or video cameras. These are probably in a general "video" folder.

4. All of the music files that you have bought, created, collected, or ripped from CDs. Some common file types are .mp3, .wma, .m3u, aac. There are many other audio file types that could be produced by common applications in use. These are probably in a general "music" folder.

5. Any other data that you feel you cannot live without, such as Quicken or Money backup files, or the data files from TurboTax or TaxCut. These may be spread out among many folders.

How often to backup is the next decision. Basically, as soon as a file is created or changed, it is a candidate for backup, but, let's be practical. If during the day, there were a large number of files created or changed, then they are probably reason enough to backup at the end of the day. If there are very few changes from day to day, then daily backups are probably not necessary. So, some days you might backup certain folders and some days you may not. But, at the end of the week, it is time for a weekly backup. (This doesn't have to be any specific day of the week, but must happen at least once a week.) With this philosophy, in the worst case, all of your data is only one week old, and your important data is only one day old. This should let you sleep pretty well.

Now, on to the decision of how many backup copies? This is a very personal decision. For many, one copy on an external hard drive will more than suffice. That can be augmented by copying all of the files, once or twice a year to DVDs. That way, if the external hard drive goes down, and you haven't replaced it, in the worst case, you have the latest DVD copies to go back to, although that data could be 6 month old. For guaranteed safety, two external hard drives, one updated weekly, and the other updated once or twice a month, and a set of DVDs every six months should make almost anyone feel good and sleep well. An even greater precaution taken by most businesses and some people is to take one set of Backup files (External or DVDs) and store it off-site, in a bank vault or a friend or relative's house. (For businesses, this is almost a necessity.)

Now, for the question, how to implement a backup strategy? If you only have a few files, you can just copy them to the backup device on the schedule that you have established. If you have a large to medium collection of files, you will probably need the assistance of a software application to make it palatable. The first backup is simply a copy of all of the files to be backed up. Each backup after the first need only to be a copy of the new files created and the files that have changed since the last backup. This is called an incremental backup. As your number of files to be backed up grows, you will grow to appreciate the incremental backup. The software will determine which files, in the folder to be backed up, are either new or changed and then only copy those files to the backup device. Some applications call this "synchronizing" the files. Synchronizing can be done in a few different ways and the application will allow you to choose the one that is right for you. For backup, make a selection that will not change the source files. Source files are those to be backed up, and target or destination files are the backup copies.

System Backup

So far, we've only backed up our data files. Now, on to backing up the system.

Continued on Page 7

Sandy Berger, CompuKISS, www.compukiss.com, sandy (at) compukiss.com

Be Careful of Buying Old Versions

Don't be fooled by a cheap price on a product. It may be last year's model. While sometimes this is okay, for others it is a real rip-off. Here are some examples that you may want to read. Remember being a savvy consumer is essential in today's high tech world.

In the recent past, when a new version of a product was introduced, the old versions were removed from the retailer's shelves. So when you went into the store, you were sure of getting the latest and greatest version of each product.

But times have changed. Now the manufacturers are keeping their old versions available right alongside the newest models. In some cases, the product names have changed enough that the average person can easily tell the new from the old. For example, the iPad Air is Apple's newest full-sized iPad. You will see that Apple is also still selling the older iPad 2 model. In this case, the name actually changed and the marketing will usually indicate which is new and which is old.

In many cases, however, the name of the product doesn't change. There are often several versions of the same product with the same name or similar names selling at different prices.

Take the iPad mini, for example. Apple recently introduced a new, improved version of that product. The cheapest current version is selling for $399. So when Walmart advertised the iPad mini for $299 and it offered a $100 gift card with that purchase, it seemed like a fantastic deal. However, Walmart was selling last year's model in that ad. They didn't have to stipulate anything other than "iPad mini" because both last year's model and the latest version are both simply called "iPad mini". The same is true for devices from other manufacturers, as well. The Microsoft Surface tablet has an original version and a newer updated version. If you purchase a Nexus tablet, you will find a version from last year right alongside the newest 2013 version that was just released.

The newer versions almost always have improved functionality and new features, but buying last year's model is not necessarily bad. To be a smart consumer, however, you need to know exactly what you are buying. It is always wise to ask if you are purchasing the latest version. Even better, take the time to research the older version and compare it spec-by-spec with the newest version. That is the only way to know if the price difference is worthwhile for you.

Luckily, the Internet makes such research easy. Right on the Apple website you can find a comparison for the two versions of the iPad mini. The newer iPad mini has a much improved screen resolution and a faster processor but the main specifications of the device remain the same. If you don't care that much about the screen clarity or the speed, the savings may be worthwhile.

You may not always need to purchase the latest and greatest version of each product. Only you can determine exactly what you need and which features you will use, and which you can do without. Doing research on the products can be time-consuming, but it is a worthwhile endeavor that will help you find the perfect device at the right price.

When it comes to high tech gadgets, being a savvy consumer is essential. You need to be "in the know" so you can make an informed decision on whether you would rather have the best device currently on the market or a little extra money in your pocket.♠

Bill Sheff, Lehigh Valley Computer Group, PA, April 2014 issue, The LVCG Journal, www.lvcg.org, nsheff (at) aol.com

The Tip Corner

Tech Support

Before calling or e-mailing for support do have the following information handy:

Have the model and serial numbers.

Also be close to the product.

Have paper and pencil for instructions or contact information.

Try googling for the information before contacting anyone.

Ensure that you have lots of time available.

Have all purchase information available.

If there is a charge, have more than one credit card available.

When connected, write down the support representative's name and any case number assigned.

Windows hidden "god mode" folder

Windows offers a centralized Control Panel for all of the OS settings, which makes it easy for users to tweak everything from desktop background to setting up a VPN. To enter this mode, create a new folder with this exact name (copy and paste it): God Mode.{ED7BA470-8E54-465E-825C-99712043E01C}. The folder icon will change to a Control Panel-style icon, and you will be able to jump in and change all kinds of settings. Note: Don't try this on Windows Vista 64-bit as it's known to cause a reboot loop.

Problem Steps Recorder

This handy tool automatically records any mouse clicks and takes screenshots for you. If you need tech assistance with your computer, go to Run by typing Windows + R, and then type "psr." Use the tool and by the time you are finished, you can send this information, neatly compiled automatically, to the person helping you with the issue. It will make the process of finding the problem much easier for them, which means you will be able to get your system up and running faster.

WinDirStat

Find and Delete large files cluttering up your hard drive. A tool called WinDirStat (Windows Directory Statistics) will help you find files and folders that are taking up the most space on your drive. Once found they can be deleted.

Use the Cloud

If you are working on some serious stuff don't just save it to your hard drive. Use the Cloud to backup important files. You can use services like Dropbox, Google Drive, or many of the other popular cloud storage solutions. They usually offer two to ten GBytes of free storage. More than that can cost, but it will be a while before you have to go that route. The files are then available to you no matter where you are or on which computer. A little setting up can put the folders in easy reach. Try it out.

Typing Tricks

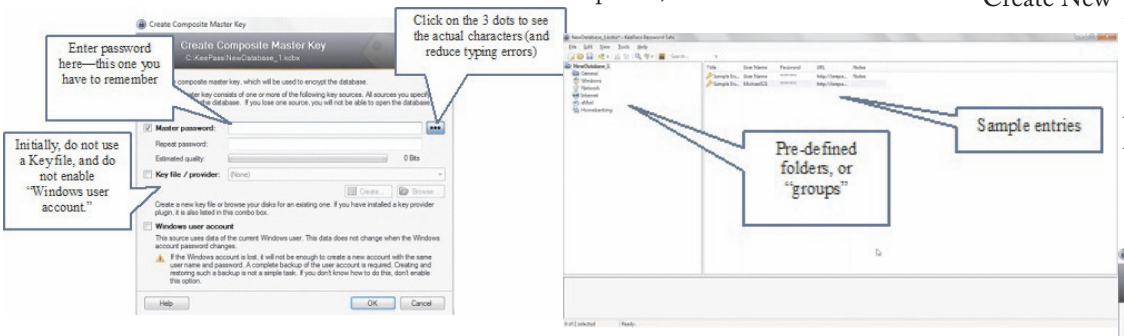
Ctrl + Bksp will delete an entire word.

Continued on Page 6

directory of my hard drive and saved the database there (just my preference).

Note also that a default "File name" is entered. I modified that name, in the expectation (as yet unproven), that I will eventually need multiple databases. I chose NewDatabase_1.

With the location and file name selected, click on Save. You will see:



You enter a Master Password into this window. It needs to be a "strong" password, but it also needs to be something you can remember. A "strong" password is:

"A password that is hard to detect both by humans and by the computer. Two things make a password stronger: (1) a larger number of characters, and (2) mixing numeric digits, upper and lower case letters and special characters ($, #, etc.)."

Source: PC Magazine (http://bit.ly/1h5lq5l)

This password you may want to write down (yes, using the old fashioned pencil and paper); and although this should be obvious, don't identify it on that piece of paper. You may also want to keep it with you.

From the KeePass Help file (Composite Master Key):

"If you forget this master password, all your other passwords in the database are lost, too. There isn't any backdoor or a key which can open all databases. There is no way of recovering your passwords."

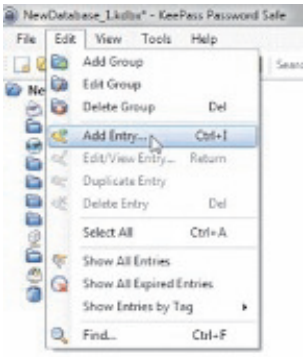
A more detailed discussion of passwords vs. key files is available from the Composite Master Key section of the KeePass Help file.

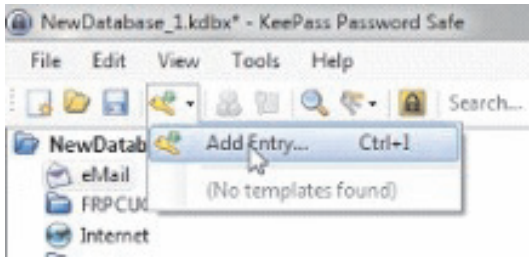
If creating a strong password that you can remember seems contradictory, enter:

how to create strong passwords that you can remember into your favorite search engine. You will find many articles with suggestions.

After you enter your password, click on the OK button at the bottom right of the Create Composite Master Key window. You will see something similar to this (I will talk about the Database Settings window that is part of the database creation process later—the default values are acceptable):

You can add groups, and/or modify their order. However, you are, at this point, ready to enter data. You use the "Add Entry" window for this task. It is available from the Edit menu and from the Toolbar:





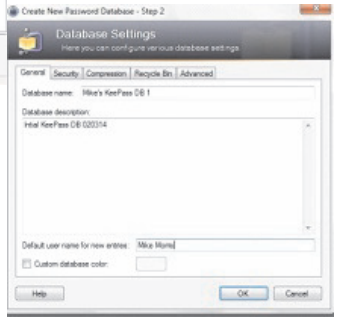
When the Add Entry window is displayed, it will already contain an automatically generated strong password (see screenshot at right):

Your user name will also be included. The only field required, other than the password, is the URL of the web site for which you want to use this password.

By the way, that Notes field is a handy place to record the answers to all those security questions you are asked when you register at any web site.

You add as many entries as you need passwords. If you choose to organize them into groups, click on the group name in the left panel before you click on Add Entry.

I want to depart momentarily from this sequence and return to the Create New Password Database steps. You will see a Database Settings window during this set up (you can also access Settings from the File menu after the database is created). All of those settings can be left at their default values. However, you may want to enter a description. For example (see Page 7):

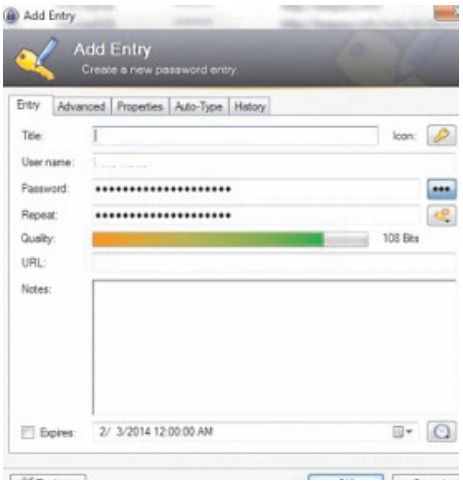


How to Use the Password

Here are the steps for using the password:

1. Connect to the log in window of the web site of interest. You can also connect

Continued on Page 7



The Tip Corner – *continued from Page 4*

Move the Cursor to the beginning of the next or previous word by using Ctrl + left or Right Arrow.

Instead of using Paste Special to get unformatted text type Ctrl + Shift + V.

Cycle through open windows

Pressing ALT+TAB allows you to cycle through currently open windows. This makes switching back and forth between running processes quick and painless.

UNDO

You can undo almost any action by using CTRL + Z. This is not only to fix typing errors. If you accidentally delete or move a file, CTRL + Z brings it right back to where it was. In Chrome and Firefox you can also undo closing a tab using CTRL + SHIFT + T.

CTRL + ALT + Delete

This handy shortcut Interrupts all processes and should be a standby for us all. Something happens, the computer freezes and in most cases Ctrl + Alt + Delete will interrupt all processes, including the one that is bogging down your system, which might save you from a restart and lost data.

If you want to open the task manager directly and bypass the interrupt that happens when pressing CTRL + ALT + DEL just type CTRL + Shift + ESC.

File Management Trick

Rename a file quickly Right-clicking and selecting rename is not very efficient. Instead, simply press F2 while a file is selected to change its name. To alter the name of another file, type TAB without deselecting the current file.

Rename files sequentially

In Windows You actually don't need to download any programs to perform a batch file rename in Windows. Instead, you can select all the files you want to change, right-click the first one in the list, select rename (or use F2), and type in the name. This will automatically change all the other files with the same root name with a suffix: (1), (2), and so on.

Minimize all windows

If you have a few programs open and want to get to the desktop, Windows + D will minimize everything you have open. Beats pressing the minimize button for each window.

Close current window

Close the current window/tab. Sick of moving all the way to that X button? Press CTRL + W and the current window will close.

System information window

Not too many uses around for the Pause button. Bring this one up by pressing Windows + Pause/Break and the System Information panel is there.

Making sub and superscript text

If you need to make sub or superscript text (think exponents for superscript) , press CTRL + = for subscript and CTRL + SHIFT + = for superscript

Security Tip

Run programs on an infected PC

Often times, malware will prevent a computer from running certain programs. Changing the name of the .exe file can often override this. If that doesn't work, changing the extension to .com is another useful alternative, and the program will still be able to run in spite of the extension change.

Web Browsing Trick

Automatically add www. and .com to a URL You can shave off a couple of seconds typing in a URL by simply click CTRL + Enter after you type the name of the site. Need .net instead of .com, press CTRL + Shift + Enter instead.

Korora

Korora takes Fedora and adds things like Adobe Flash and various multimedia codecs as well as a big selection of software to make it a great system for those fairly new to Linux.

Korora Linux is available with a number of desktops including KDE, Cinnamon and the one we checked out Gnome3. Korora has modified the Gnome desktop a bit by adding a places icon to the top panel which allow you to quickly access files on your file system, network, or external media. Korora is nice looking and responsive.♠

Mike Alcorn, CTPC Newsletter Editor

CTPC News

Many members might not notice that the publication of the August newsletter represented the end of 32 years for the CTPC. I want CTPC members to know that I've decided to step down at the end of the year as newsletter editor. The post is open but I somehow doubt that anyone will step up.

I reviewed the CTPC history and found that Gleason and Jody Greene gave up their jobs as webmaster and newsletter editor respectively in September, 1998. Starting in October, 1998 Harold Frost took over as webmaster and I signed on as newsletter editor.

Members will hear more about the future of the CTPC in the October – December newsletters and at upcoming meetings. I encourage all members to attend the September meeting where I'm sure there will a discussion about the club's future. ♠

Next CTPC Meeting

Continued from Page 1

- Store the encrypted file in the cloud so you can access it from anywhere.
- Use a password manager such as LastPass, KeePass, 1Password, RoboForm or Keeper.

A password manager (or password vault) helps you create strong passwords and stores them for you in the cloud. Your passwords are encrypted and can be accessed with a single master password each time you visit a password protected website.

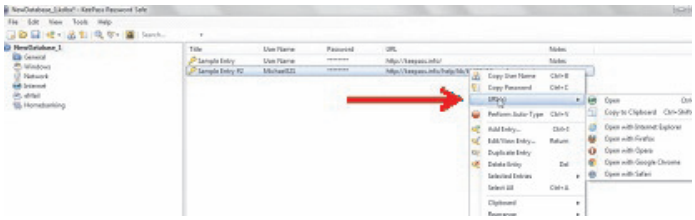
Please come join in the conversation. Let us know if you've found the right solution for managing your passwords or share your experience with one of the available password managers.

Don't forget our new location: the United Congregational Church of Norwalk on Richards Avenue. If it's a very warm night we can take the folding chairs outside and have an outdoor meeting – as we did for the July meeting!

Pizza and refreshments at Uncle Joe's will follow. ♠

Password Managers – *continued from Page 5*

to the web site from KeePass. Right click on the entry for that web site and then click on URL. If you have more than one browser installed (as I do), you can choose which one to use from the list that is displayed:



2. Once you are connected to the web site's log in window, in KeePass, right click on the entry for that web site and then click on "Copy User Name":

> Return to web site log in screen and paste the user name into the appropriate field (you could, of course, just type that in).

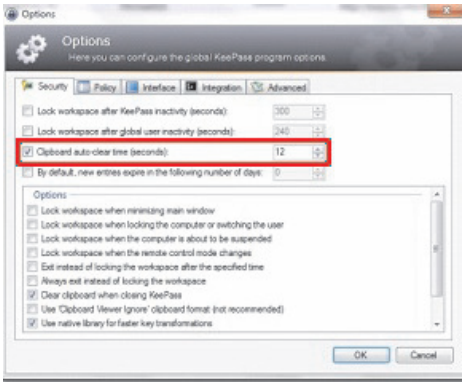
3. In KeePass, right click (again) on the entry for that web site and this time click on "Copy Password."

Return to web site log in screen and paste the password into the appropriate field.

4. Click on the log in or sign in button for the web site.

There is one important note regarding these steps. You have only a limited (but adjustable) time to paste the user name or password after you copy it. KeePass will clear the Clipboard after some number of seconds for security reasons. That time is set in the Security tab of the Tools/Options menu item:

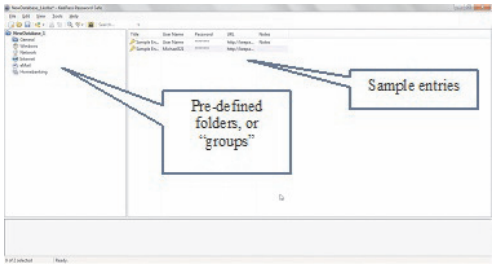
Note that in the image on the right, that time is set to 12 seconds.



Extras

So far, these instructions cover just the basics. There are many extras, three of which are worth mentioning, although not discussed here in detail (see the KeePass Help file).

1. Generate your own passwords: If you are not satisfied with the automatically generated passwords, you can create your own. Click on the icon under the 3 dots and you will see:



2. Mobility: There is a "portable" version (http://keepass.info/download.html) that you can install on a flash drive that will allow you to use KeePass on any other computer (with some restrictions—see the KeePass Help file) "without creating any new registry keys and it doesn't create any configuration files in your Windows or application data directory of your user profile."

3. Plugins: There are a large number of plugins available (http://keepass.info/plugins.html), including one called KeeForm that will "(open) websites and fill in the login data automatically, for Internet Explorer and Firefox." Before you install any plugin, be sure to read the Plugins for KeePass 2.x (http://bit.ly/PhVjkz) information.

Acknowledgements

Thanks to Front Range PC Users Group member Bert Broekstra for his help with learning this program.

Thanks to Front Range PC Users Group member Herb Cantor for finding the "Yahoo Email is Breached . . ." article and for sending the link to me.♠

Backup...Backup...Backup . . . – *continued from Page 3*

The whole system has to be backed up, in total. The system is not backed up by a simple copy of the system files. The system must be backed up by saving the system as an "image", using imaging software, specifically designed for this purpose. Normally, the system doesn't change as frequently as the data files. However, each time you get an update from Microsoft, the system changes, albeit slightly. The system also changes each time you install (or uninstall) an application, peripheral device (like a printer), or hardware driver.

So, how often should we backup the system, another very personal decision. A good strategy for the system backup is to "take an image" every time a big change is made (a software installation, a software un-installation, or a Service Pack installation), or a fixed amount of time has passed, say 3 months. Taking an image takes a good bit of time, so you don't want to do this too often. If you have many large software applications on your system, it may take hours to take an image. Images are usually saved compressed, and the amount of compression is usually adjustable, for example low, medium, or high. The low compression choice will take an image quicker, with a larger image file being created. The high compression choice will be the slowest, but the file created will be the smallest. Medium will be somewhere in between. Highly compressed image files can be from 2 to 10 GB, so you need to have a good bit of storage just for the images. These images should be stored on a different physical drive from the drive that your C: drive is on. Saving them on another partition on the same physical drive will not help you if the drive goes down.

Just how many copies of the system image backup should be kept? Considering the size of the image files, you may want to keep only a few, maybe 3 or 4, and some that were taken at key points. These key images might be the initial load of the operating system, or the initial load of the operating with the initial applications installed, or before any critical application was installed and checked out. Actually, any image that you are confident is reliable, and would be a worthwhile starting

Continued on Page 8

Multitasking – continued from Page 1

"In the brain, multitasking is managed by what are known as mental executive functions. These executive functions control and manage other cognitive processes and determine how, when and in what order certain tasks are performed. According to researchers Meyer, Evans and Rubinstein, there are two stages to the executive control process. The first stage is known as 'goal shifting'" (deciding to do one thing instead of another) and the second is known as 'role activation' (changing from the rules for the previous task to rules for the new task).

Switching between these may only add a time cost of just a few tenths of a second, but this can start to add up when people begin switching back and forth repeatedly. This might not be that big of a deal in some cases, such as when you are folding laundry and watching television at the same time. However, if you are in a situation where safety or productivity are important, such as when you are driving a car in heavy traffic, even small amounts of time can prove critical."[3]

This gives a greater perspective about what one is actually doing. But what about enhancing the ability to task switch? Switching between rote tasks is relatively simple, but when the tasks become more complicated, the results are quite interesting. This finding is pretty much a no-brainer: "Recent research also proves that as we get older the brain is less able to focus on more than one task at a time, and takes longer to switch between tasks."[2] According to the Harvard Business Review from a study conducted by the Institute of Psychiatry, trying to focus on more than one task DECREASES your productivity by 40%, and lowers your IQ 10 points. The study also found that excessive use of technology also reduced workers' intelligence. Other studies have shown that multitasking/taskswitching reduces one's mental abilities TWO TIMES the effect of smoking marijuana, or the equivalent of losing a full night's sleep. It also increases one's stress. And of course the all famous talking on the cellphone while driving, even with a hands free device, decreases reaction time the equivalent of a blood alcohol level of .08%. As a side note, having a conversation with a passenger is only slightly less distracting, as per insurance industry statistics.

But this finding is actually shocking. "In a 2009 study, Stanford researcher Clifford Nass challenged 262 college students to complete experiments that involved switching among tasks, filtering irrelevant information, and using working memory. Nass and his colleagues expected that frequent multitaskers would outperform non-multitaskers on at least some of these activities. They found the opposite: Chronic multitaskers were abysmal at all three tasks. The scariest part: Only one of the experiments actually involved multitasking, signaling to Nass that even when they focus on a single activity, frequent multitaskers use their brains less effectively."[4]

My mother always said, "Do one thing at a time. …Turn the television/radio off and do your homework." She was so right, and ahead of her time. So this adds up to some very harsh realities. Multitasking is a "hardwired" ability for 2% of the population, but a giant myth for 98% of the population. Additionally, tasks requiring the same cognitive ability can NOT be performed simultaneously, such as watching a movie and responding to emails. (Both require visual and linguistic cognition.) Most people are actually task switching. This is fine when the activities are simple tasks that are well learned and do NOT require the same cognitive ability. The more one attempts to task shift, the worse one gets, not to mention damaging to overall mental functioning, perhaps permanently. One final conclusion from multiple studies is that the people who insist that they can multitask are the WORST at it. Does this sound like anyone you know? ♠

[1] "This is Your Brain on Multitasking" by Garth Sundem, February 24, 2012, www.psychologytoday.com

[2] "Think You're Multitasking? Think Again", by Jon Hamilton, October 2, 2008, www.npr.org

[3] "The Cognitive Costs of Multitasking", by Kendra Cherry, March4, 2014, http://psychology.about.com/od/cognitivepsychology/a/costs-of-multitasking.htm

[4] "Don't Multitask: You Brain Will Thank you", by Issie Lapowsky, April 17, 2013, http://business.time.com/2013/04/17/dont-multitask-your-brain-will-thank-you/♠

MEETING LOCATION

United Congregational Church
275 Richards Avenue, Norwalk

Heading north on Richards Avenue from the Post Road, go past NCC and past the traffic light at Scribner Avenue – the church is on the left hand side, just past Temple Shalom. We will meet in the fellowship area adjacent to the sanctuary so park in front and come in the front door.

REPRINTING OF ARTICLES

Unless otherwise noted, nonprofit user groups may reprint or quote from any uncopyrighted articles appearing in the CTPC newsletter without prior permission as long as credit is given to the author and the original publication.

Backup – from Page 7

point, can be kept.

Once your backup philosophy is established and a backup strategy is put in place, and you execute the strategy, that is, you routinely backup your data and your system, you will be able to sleep more soundly at night, never having to worry about "what happens if".

If a hard disk failure occurs, your backup data can quickly and easily be copied to the new hard drive. If your C: drive with the system goes down, the last image can be restored to the new C: drive. If a software problem or malware infection occurs, the last image can be restored and you are back up and running. All of these problems are now less a problem because you can recover from them without any question and in a reasonable amount of time.♠

DISCLAIMER

The opinions expressed herein are those of the authors and do not necessarily reflect those of the CTPC or its members.

Neither the CTPC, contributors nor the Editor of this newsletter assume any liability for damages arising out of the publication or non-publication of any advertisement, article or any other item in this newsletter. Articles are published at the discretion of the Editor.