MC^3 Newsletter

January 2019

VOLUME 36 NUMBER 1

The January meeting of the McHenry County Computer Club is **January 12, 2019 at Salvation Army Building 290 W. Crystal Lake Ave., in Crystal Lake, IL.**

NOTE: *Enter the building on the parking lot level under the awning.*

Meeting Agenda

- Introductions & Reports
- Q & A
- Working With GPS - Bob Wagner

Upcoming Demos - Subject to Change

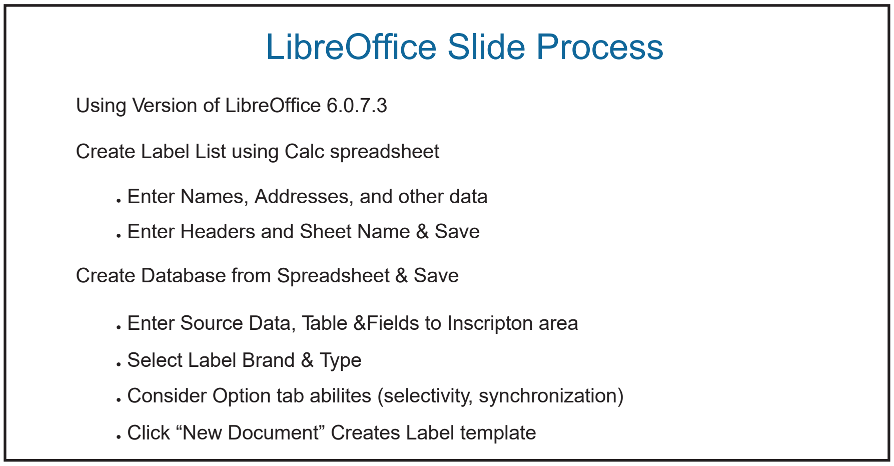
February 2019 - Using PassMark by Al Edlund
March 2019 - Topic Needed

APCUG Virtual Technology Conference

The first Conference of 2019 will be held on February 9th. I will remind Lyle to send out the details as soon as they're received.

The last Conference in November was very entertaining and contained some excellent information, so I would encourage all members to take advantage of this benefit of our APCUG membership.

LibreOffice Slide Process - Bill Lapp



LibreOffice Slide Process

Using Version of LibreOffice 6.0.7.3

Create Label List using Calc spreadsheet

- Enter Names, Addresses, and other data
- Enter Headers and Sheet Name & Save

Create Database from Spreadsheet & Save

- Enter Source Data, Table &Fields to Inscripton area
- Select Label Brand & Type
- Consider Option tab abilites (selectivity, synchronization)
- Click “New Document” Creates Label template

continued on next page

McHenry County Computer Club
Established 1982
MC^3

Our membership is $26.00 a year.

NOTE: This fee offsets the running of the club; membership benefits include help with computer problems. Please pay Lyle Giese, our treasurer, or the designated Board Member in his absence.

MC³ OFFICIALS

President:
Larry Freeman
lpfreeman@hotmail.com

Vice President:
Bob Wagner
rmwagner@ameritech.net

Secretary:
Bruce Ecersberg

Treasurer:
Lyle Giese
lyle@lcrcomputer.com

Database Manager:
Lem Erita

Newsletter:
info@Mc3ComputerClub.org
(for articles & suggestions)

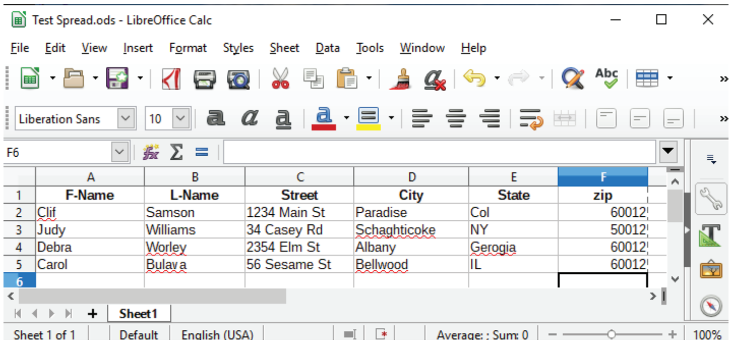
Past President:
John Katkus

Webmaster:
Cindi Carrigan

Board Members:
Jack Luff, Al Edlund,
Ken Schuring

LibreOffice Label Making Process

•Spreadsheet with Headers, Data, & Sheet Name


Test Spread.ods - LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans
10
F6

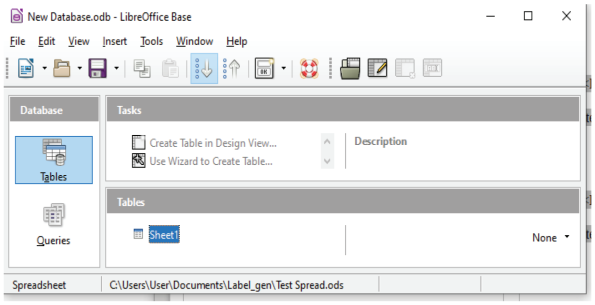
	A	B	C	D	E	F
1	F-Name	L-Name	Street	City	State	zip
2	Clif	Samson	1234 Main St	Paradise	Col	60012
3	Judy	Williams	34 Casey Rd	Schaghticoke	NY	50012
4	Debra	Worley	2354 Elm St	Albany	Gerogia	60012
5	Carol	Bulava	56 Sesame St	Bellwood	IL	60012
6						

Sheet1
Sheet 1 of 1
Default
English (USA)
Average: ; Sum: 0
100%

- Save Spreadsheet
- Select File, “New / Database”

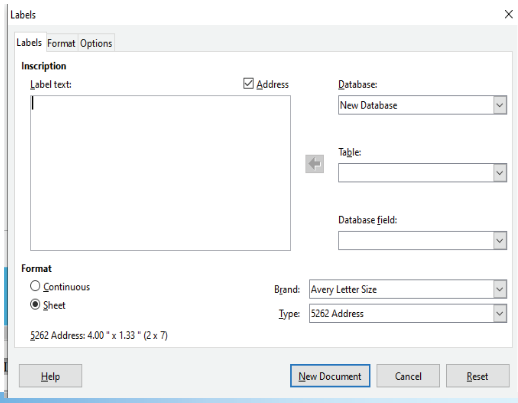
LibreOffice Label Making Process

- New DataBase
- Save Database
- Click on Sheet & view Database info
- Goto File New / Labels


New Database.odb - LibreOffice Base
File Edit View Insert Tools Window Help
Database
Tables
Queries
Tasks
Create Table in Design View...
Use Wizard to Create Table...
Description
Tables
Sheet1
None
Spreadsheet
C:\Users\User\Documents\Label_gen\Test Spread.ods

LibreOffice Label Making Process

- Note Tabs of Label Format & Options (Make sure you check the Synchronize check box)
- Select Database Table Data fields Avery Label form desired Etc
- Click New Document
- Creates Label Template



Labels

Inscription

Label text:

☑ Address

Database: New Database

Table:

Database field:

Format

○ Continuous

● Sheet

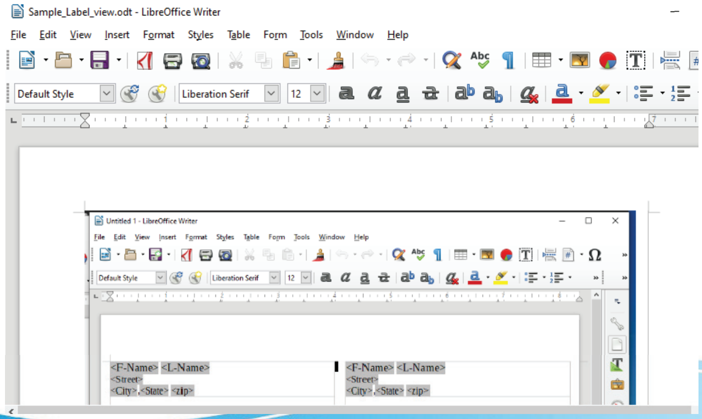
Brand: Avery Letter Size

Type: 5262 Address

5262 Address: 4.00 " x 1.33 " (2 x 7)

LibreOffice Label Making Process

- Make any format changes to fields in 1st block as desired.
- Click the Synchronize button to propagate changes across labels.



Sample_Label_view.odt - LibreOffice Writer

Default Style | Liberation Serif | 12

Untitled 1 - LibreOffice Writer

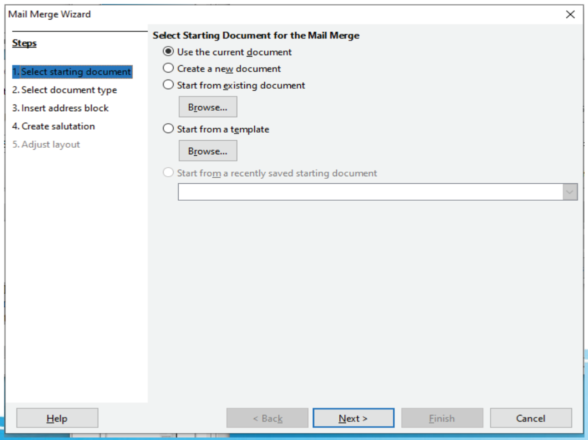
Default Style | Liberation Serif | 12

<F-Name> <L-Name>
<Street>
<City>, <State> <zip>

<F-Name> <L-Name>
<Street>
<City>, <State> <zip>

LibreOffice Label Making Process

- Click on Tools & “Mail Merge Document” Creates dialog below
- Click through the various dialogs (No changes needed)



Mail Merge Wizard

Steps

1. Select starting document
2. Select document type
3. Insert address block
4. Create salutation
5. Adjust layout

Select Starting Document for the Mail Merge

● Use the current document

○ Create a new document

○ Start from existing document

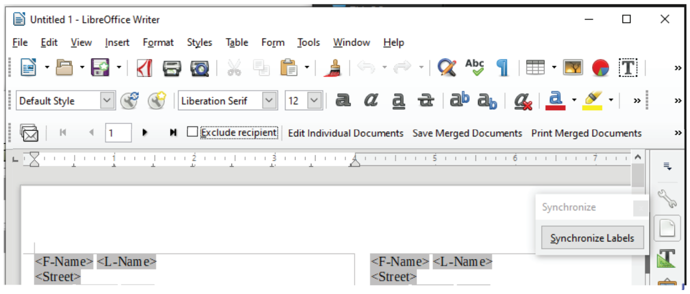
Browse...

○ Start from a template

Browse...

○ Start from a recently saved starting document

LibreOffice Label Making Process



Untitled 1 - LibreOffice Writer

□ Exclude recipient Edit Individual Documents Save Merged Documents Print Merged Documents

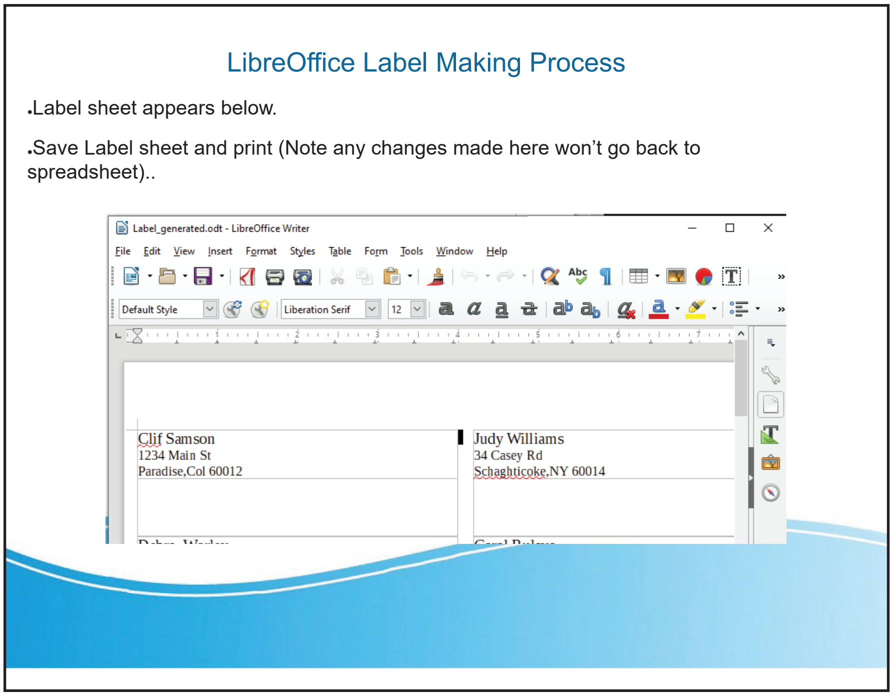
Synchronize Labels

<F-Name> <L-Name>
<Street>

<F-Name> <L-Name>
<Street>

–Click Finish

Note LibreOffice Write added



LibreOffice Label Making Process

- Label sheet appears below.
- Save Label sheet and print (Note any changes made here won't go back to spreadsheet)..

Label_generated.odt - LibreOffice Writer

Clif Samson
1234 Main St
Paradise,Col 60012

Judy Williams
34 Casey Rd
Schaghticoke,NY 60014

File Edit View Insert Format Styles Table Form Tools Window Help
Default Style
Liberation Serif
12

Help, I'm Stuck! What do I do now? - Dorothy Fitch. GVR Computer Club

Have you ever forgotten how to do something you have done before in a software program or operating system? Or perhaps you know you should be able to do something you need to accomplish, but don't have a clue how to do it? Wandering through menus and settings can be laborious and often, not very productive. So, how can you get "unstuck" in your task?

There are lots of resources you can try. If you aren't in a hurry, you can check out your local library.

If you need immediate help, your first instinct might be to use the program's Help system. However, I sometimes think that people who write Help information aren't really using the program in a "real-world" setting and don't cover everything you might encounter. They tell you what they expect you want to know, not what you really do need to know.

The best way I have found to get "unstuck" is to search the Internet instead. In your favorite search engine, type name of the program and exactly what you are trying to do. I am relearning InDesign, an Adobe product for graphic design, and it is very complex. The version I have is older and pressing F1 for Help doesn't work, as the product is no longer supported. All I wanted to do was to put a box around some text, and so I googled this: indesign put box around text.

I immediately got lots of answers, some with video tutorials (which you aren't going to find in the application's Help system). Not only did I find many ways to put a box around text, but I also learned how to remove a box, which might come in handy someday. And how was I to know to look for the Glyphs menu to insert a special character? The Web to the rescue yet again.

Sometimes, a Help system doesn't mention what you are looking for because the product can't do it. I had to search the Web to learn that Paint.net, my favorite (free) graphics editing software, supports RGB color format, but not CMYK, which was what I needed. Their Help information didn't even mention CMYK.

And what do you do if you get an error message you don't understand? Just google the text of the message! I encountered this cryptic error message in InDesign when creating a PDF and couldn't figure out how to resolve it.

"The document's transparency blend space doesn't match the destination color space specified in the Export Adobe PDF settings. To avoid color appearance changes in the PDF, click cancel and change either the document's transparency blend space, or the destination color space."

When I searched for indesign the document's transparency blend space doesn't match, I got several suggestions of what to do, and eventually figured out how to fix the problem.

The bottom line is that people who answer questions in a User Forum or blog, those who take the time to create tutorials and videos, and authors of Tips and Tricks columns are more likely to get you "unstuck" than any product's Help system. All you have to do is ask the Web for help.

Cure Desktop Clutter - Joe Isaac - Central Kentuck Computer Society

If you have more than four rows of icons on your desktop, you probably have too many for efficient use. Desktop icons should only be something used often. The icon idea is to put a program or project up front, so you don't have to spend a lot of time looking for it. Quick access is the key! If you have several dozen icons there, the ability to find something quickly is much less likely. We usually start with just a few, but they tend to grow in number as we install a new program. Every program writer thinks his/her program is the absolute most important one, so they hang another icon on your desktop.

So here is what I recommend you do. Look over the icons on your desktop and identify the ones you haven't clicked on in weeks or maybe months. Right click somewhere on your Desktop. Select NEW, then click on FOLDER, name the new folder Misc. or Stuff. Then hit Enter.

Now, left click and drag your least used icons into this one folder. Leave only the frequently used icons in view. Those rarely used icons are still available to you should you need one of them.

Get to work! You will be glad you did!

Have you taken control of your passwords yet? - John Fair - Computer Users of Erie, PA

No one can guarantee you will never be hacked, however there are published guidelines that I'll summarize that can minimize the risk. Only you can decide what to do with these recommendations. First, create strong passwords. This is not easy. We have repeatedly been told to create unique passwords combining numbers, special characters, upper- and lower-case letters. Complexity or randomness is good but you can add strength by making your passwords longer - as long as the site allows. Consider pass phrases or a collection of random words but remember that hackers have access to databases of song and book titles, lyrics, poems, etc. so randomize what you use.

Second, treat your email password with special care. Make it as strong as you can and never use that password or a variation of it for anything else. If hackers gain access to your email they can use it as a key to resetting passwords of your other accounts thus locking you out.

Stop thinking of hackers only as the lonely figure in a hoodie crouched over a laptop in a dimly lit room. Hacking is also done by businesses employing many folks using lots of computing power and large databases to try to separate you from your personal information and hard earned cash. They buy and sell information from data breaches and scour social media and public databases to use in their pursuits. This realization might spur you to take more seriously protecting yourself online.

Never reuse a password! If you do, your security is only as good as the weakest site on which that password is used. It's easy for a hacking program to test one stolen password on all of your sites. And slight variations of that password (add a number) or simple substitutions ($ for s) still make it easy to guess. Don't use as passwords what has become public information because of social media (pet names, birthdays, family names, addresses, phone numbers, etc.) or what can be found in public databases. They are easy guesses for hackers. And, of course, passwords that are user names, simple dictionary words, adjacent keyboard combinations, etc. make it too easy for hacking schemes. Perhaps it should go without saying, don't keep a file containing your passwords on your computer. That list of passwords you keep in writing is a bit safer if inconvenient to update.

Why do we violate good password guidelines? The National Institute for Standards and Technology (NIST) had issued password guidelines we have all been following for the last 15 years. Use at least 8 alphanumeric characters sprinkled with capitals and special characters and change passwords every three months. The unintended result of this complexity was that most people gravitated toward common patterns and hackers exploited these predictable patterns. One author of the original guidelines described the results of imposing these arbitrary rules: "It drives people bananas and they don't pick good passwords no matter what you do."

NIST's newly released password guidelines are more user friendly, requiring only what significantly improves security, putting more burden on the verifier and using 2 factor authentication where possible. Longer passwords are better. Further, they recommend you change passwords only in the event of a data breach. Arbitrary complexity that drives poor practices shouldn't be required. The verifier should screen for and not allow commonly used passwords, eliminate the need for hints and security questions and limit the number of incorrect guesses allowed. You might find that verifiers are a bit slow to adopt their end of these guidelines because of the cost involved.

Because of the number of passwords people (should) use and the complexity of each one, security experts now suggest considering the use of a password manager.

Password managers store your passwords and other information in an encrypted vault, either on your computer or in the cloud, that is accessed by a single VERY STRONG master password that is encrypted and never stored in plain text.

They can generate complex, random passwords of any length for you to use on any site. They work in conjunction with your browser and can autofill username and password for sites you have chosen.

Most have a subscription fee of from $12 to $40 a year, but a few have a limited function version for free. While Wikipedia lists over 30 password managers on the market, most experts suggest staying with one of the top four: LastPass, Dashlane, 1Password or KeePass.

I purchased 1Password before they moved to a subscription-based service and am grandfathered in using it. I found it relatively easy to use, love the excellent security ratings and have it on my Mac, iPad and iPhone. However, if you choose to follow security experts recommendations and give a password manager a try, you might want to avoid paying even a nominal subscription fee in the beginning until you understand what additional features you might need that you must pay for. I suggested giving LastPass a try since the free version does what most folks want from a password manager and, since it is cloud based, can synchronize across computer, smartphone and tablet. It is also very highly rated for security.

If you think LastPass might be of interest, first review their website for information and user forums. That will help you to understand how LastPass might be of value to you. If you want to try out LastPass, STOP!! Don't take any action until you have devised a very strong master password. The LastPass website will offer guidance in how to do that but note that you can use a very long master password and you could take advantage of the security that will offer. One way to generate a long but memorable master password is to use four or more random, unrelated words separated by spaces. To understand the logic behind this just Google "correct horse battery staple."

Really. You want a master password that is easy to remember so that you can access your password manager vault without consulting a written password.

Think this through before you download and try any password manager. You want a master pasword you will never forget since the password manager company does not store an unencrypted version of your password and thus will not be able to help you recover your vault contents if you should forget your master password.

If you are at all nervous about using a password manager, do not put your banking information or email password in it. I have not. You will see a real benefit from using it for all the rest of your passwords. I have also used 2 factor authentication in LastPass. That gives me the additional convenience of using my fingerprint on my iPhone and iPad to open LastPass since they are identified as trusted devices (the second factor).

Currently there are three authentication factors used to prove your identity in the digital world. One factor is username, password, PIN - something you know.

The second factor is something you have - ID badge, smart card, device (phone, tablet, computer). And the third factor is something you are - biometric factor such as fingerprint, facial recognition, iris scan.

Using at least two of these factors provides more proof of your identity and is one of the new NIST recommendations for digital security.

Using a password manager requires some setup time. When you log in to a new site LastPass will ask if you want to save the login information (username and password) and that is very convenient. What is not convenient is changing the passwords you currently have to much more secure ones. You will have to go to each site or app and change its password.

LastPass will suggest complex, random passwords you would never remember, but the password manager will. Think about all the passwords you have and the time it will take to log in to each site or app and go through the process to change the password. This effort is what limits most people in the use of a password manager. But if all you do is institutionalize your poor password practices by saving your existing poor or repeated passwords, the password manager will do you no good.

You need to make all those passwords stronger - that is the point of having that password manager: to allow you to use individual passwords that are so complex you could never remember them. You don't have to change all your passwords at one time, just start with the most important ones and work on them gradually.

Password managers can also encrypt and store other information that is convenient to have such as passport, drivers license and credit cards. I have entered all this information including the phone numbers of the credit card companies if my cards are lost or stolen. This has replaced the (insecure) scanned paper copies that I used to carry with me when I traveled.

I can't end this article without mentioning that Apple has made using password mangers easer on smartphones and tablets using iOS 12. That mobile device operating system now supports autofill in Safari and third-party apps if you are using LastPass, Dashlane or 1Password. And it makes using password managers very convenient when you are out and about.

No more list of passwords tucked into my iPad case. How insecure was that! Android Oreo and Pie operating systems support autofill with LastPass but older versions do not. Adoption of new Android operating systems is far slower than new versions of Apple iOS so Android users will be limited in their convenient use of autofill. Browser extensions of LastPass on your computer provide autofill as well as the option to fill in forms online including your credit card number. I like and trust password managers but not enough to automatically fill in my credit card number on a form whose origin may not be as trustworthy. 1Password at least requires you to acknowledge you want to fill in a credit card number, an extra step to verify that you are comfortable doing so.

I cannot guarantee your online safety nor can I guarantee your password manager can never be hacked. I don't think you would use "Password123" as your master password but in the event, you do, all bets are off. You can, however, reduce the risk of bad things happening by carefully using a password manager with a strong master password.

Interesting Internet Finds - Steve Costello - SEFCUG

The Dumbest USB Gadgets You Can Buy

https://www.reviewgeek.com/5774/the-dumbest-usb-gadgets-you-can-buy/

This is not the kind of thing I usually share, but I just couldn't believe some of the things shown. Also, if they are for sale, I assume someone is dumb enough to by one (not you or me, of course).

When 2FA Goes Bad

https://askbobrankin.com/when_2fa_goes_bad.html

Yes, I know that everyone says you should be using two factor authorization on all you accounts that support it even if SMS messaging is the only option. But, I think you also need to be aware of what can go wrong. Bob Rankin talks about what happened recently to Reddit.

OneDrive Tips & Tricks: How to master Microsoft's free cloud storage

https://www.zdnet.com/article/onedrive-tips-and-tricks-how-to-master-microsofts-free-cloud-storage/

This is a great read for anyone who uses Microsoft OneDrive, especially for those who are using an Office 365 Home or Personal subscription.