Interface

**Tuesday
December 10, 2019**

Decembers Christmas/Holiday Dinner

Sponsored By

LCCUG

Come learn with us!

The Lorain County Computer Users Group
P.O. Box 792
Amherst, Ohio 44001
Phone: 440-363-1232

© Lorain County Computer Users Group © 2017

☺New Meetings Now Held at LCCC ☺

LCCC Community Learning Center
at Lorain High School
2600 Ashland Ave. Lorain, Ohio

Doors will open at 6:00 PM, program starts at 6:30 PM

A Word From Our President

I've been hearing a lot in the news about the involvement of the Cleveland and Sandusky NASA facilities in the resurgence of America's space program. I was especially interested hearing about the Orion spacecraft for Artemis. It was headed to NASA's Plum Brook Station in Sandusky for testing.

I remember our club's visit to that facility in April of 2011. At that time the facility was largely unused, as I recall. It is exciting to follow the developments in the space program and especially the local connection.

During our visit we learned *that the Sandusky facility does a variety of testing, including the Space Power Facility which is the home of the world's largest space environment simulation chamber. The facility has tested parts of rockets, Mars landers and space stations. As a Spacecraft Propulsion Research Facility, this is the world's only test facility capable of full-scale rocket engine firings and launch vehicle system level testing at high altitude conditions, just to name a few functions at this location.*

LCCUG TOUR OF NASA
PLUM BROOK 4/26/11

I hope all of you can attend our Christmas dinner party, December 10th, at Sugarcreek in Sheffield Lake. We have a lot of items for the raffle this year so we hope we'll have a big turnout. We can take your reservation right up to the last minute… just let Micky or Sandee know at info@lccug.com.
See you there!

Sandra Ruth
LCCUG President

LCCUG Officers For 2019

Office	Name / Email
President	Sandee Ruth president@lccug.com
Vice President	Carole Doerr vp-programs@lccug.com
Secretary	Don Hall secretary@lccug.com
Treasurer	Micky Knickman treasurer@lccug.com
Newsletter Editor	Pam Rihel newsletter@lccug.com
Web Page Editor	Richard Barnett webpage@lccug.com
Statutory Agent	Sandra Ruth statutory_agent@lccug.com
Director of Membership	Dennis Smith membership@lccug.com
Director of Advertising	Richard Barnett advertising@lccug.com
Director of Education	Neil Higgins education@lccug.com

Decembers Christmas/Holiday Dinner

Come and join us at the SugarCreek Restaurant for a celebration of the Holidays. It is a time to socialize with friends and family and enjoy a good meal. There will be a 50/50 raffle, and many great prizes, more than ever before. The list will be at the bottom of this column.

LCCUG Board is holding our Holiday/Christmas Dinner

Where: SugarCreek Restaurant, 5196 Detroit Rd., Sheffield Village, Ohio

Date: December 10, 2019

Time: 5:30pm

Price: $5.00 for members and $17.00 for non-members.

There will be another 50/50 raffle, plus a large number of raffle items.

We have had a nice crowd these past 2 years and we would like to see everyone back again this year. Please let us know how many are coming so we can tell the restaurant owners how many people to expect. Hope to see you there.

Raffle Tickets are $1.00 each or 6 for $5.00

Prizes:

2 TB external hard drive donated by Glenn Pubal
Amazon Fire TV Stick-Streaming Media Player, Black
Amazon Fire 7" Tablet WiFi 16 GB (Fire OS) Black
Amazon Eco Dot (3rd Generation), Charcoal
Lexar JumpDrive S50 16GB USB Flash Drive
Lexar JumpDrive S50 32GB USB 2.0
Logitech M325 Wireless Optical Mouse, Ambidextrous, Celebration Black
Mini Dash Cam Full HD Car Camera
1600mAh Dual USB Portable power bank
40 watt 6 port USB power charging system
2 Wyze indoor wireless 1080P cameras
Adata SU634 240 GB SSD hard drive
Pack of printing paper
Echo wall mount
M&Ms candy

All monies collected will be donated to the Salvation Army.

Hoping to see you all there.

Executive Board Meeting Minutes

NOVEMBER 5, 2019

The board Google Hangout video meeting was attended by Sandee Ruth, Don Hall, Micky Knickman, Pam Rihel, Richard Barnett and Dennis Smith.

The board approved prizes for the November 12 meeting which will include a 10 inch Tablet.

Sandee will inform the Lorain School we will not be using the lab December 10th. The raffles for the Christmas Dinner were finalized.

The board raised the question about the future of the club due to the lack of new members.

Pam moved, Richard seconded the meeting be adjourned.

Our links can be found at:
LCCUG.com/links, There you will find many interesting places to visit. Check them out and see what you can find interesting

---

MEMBERSHIP WITH LCCUG:

Yearly dues are $25.00. For more information contact:
Dennis Smith
Director of Membership,
membership@lccug.com.

Meeting Location:
LCCC Community Center at Lorain High School
2600 Ashland Ave, Lorain Ohio
6:00 - 8:00 PM
Meeting room is on the second floor.
Elevator access is available for those in need.

**Association of Personal
Computer User Groups**

General Meeting Minutes

NOVEMBER 12, 2019

President Sandee Ruth called the meeting to order. A motion to accept the minutes as shown in the November issue of the *INTERFACE* was made by Pam Rihel, seconded by Richard Long. Motion passed by voice vote.

There was one new guest attending the meeting.

After donating a 2TB external hard drive to the club Glenn Pubal of Royal Business Equipment Co. presented his program, "What's New in Computers". Glenn said about 80% of their business was with schools and that Chromebooks were taking over vs. computers in the schools. He talked of the new Disney + video service available for $6.99 a month and answered the many questions from attending members about computers and software.

Richard Long won the Attendance Raffle, Margie Soto-Rivera won the Roll-Over Raffle and picked the Joker to win the big prize. Ron Dix won the Hardware/Software Raffle.

Neil moved, Dennis seconded meeting be adjourned.

Elections of Officers
Elections to be held in December

President
Sandee Ruth
president@lccug.com

Vice President
Carole Doerr
vp-programs@lccug.com

Secretary
Don Hall
secretary@lccug.com

Treasurer
Micky Knickman
treasurer@lccug.com

Newsletter Editor
Pam Rihel
newsletter@lccug.com

Web Page Editor
Richard Barnett
webpage@lccug.com

Statutory Agent
Sandra Ruth
statutory_agent@lccug.com

Director of Membership
Dennis Smith
membership@lccug.com

Director of Advertising
Richard Barnett
advertising@lccug.com

Director of Education
Neil Higgins
education@lccug.com

If you would like to run for one of these offices, please contact any officer and let them know which office you would like to be nominated for. Thank you and hope to see you all Dec. 10th.

Step up and become an officer, your dues are paid for by the club.

Lorain County Computer Users Group
2020 Calendar of Events

https://lccug.com
email: **info@lccug.com**

**LCCC Community Center
at Lorain High School
2600 Ashland Ave, Lorain Ohio**

Doors open 6pm – program starts at 6:30

2nd Tuesday of each month. Changes are announced on the webpage and the newsletter.
All meetings are open to the public

January 14, Utilities - Presented by LCCUG officers

February 11, Cutting the Cord, an Update

All other months to be announced.

NEED HELP?
Here's Who to Contact:

Neil Higgins
440-967-9061 - higgins.neil@gmail.com
Evenings 6 p.m. -10 p.m. + Weekends
Hardware, Linux & Windows Operating Systems,
Chromebooks, Tweaking your system

Micky Knickman
440-967-3118 - micky@knickman.com
Daily 6:00 am to 4:00 pm. Leave message if no answer.
General Software Configuration, Hardware Installation,
Basic to Advanced Windows

Richard Barnett
440-365-9442 - Richard216@aol.com
Evenings & Weekends
General Software Configuration, Hardware Installation,
Basic to Advanced Windows & Web Page Design

Sandee Ruth
440-984-2692 - sandee29@gmail.com
Basic Word Processing, Windows, & Web Design
Advanced Internet

Pam Casper Rihel
440-277-6076
6:00 p.m. to 10:00 pm Monday thru Thursday
Genealogy help
prihel1947@gmail.com

Denny Smith
440-355-6218 - dennis.smith@windstream.net
Microsoft EXCEL
Leave message on machine.

If any of our members are interested in helping other users with what programs you are adept at, please contact any of our officers with you name, what program or programs you would be willing to give help with, you email address and or phone number and when you would like to have them call you. Thanks

---

Newsletter Editor: Pam Rihel using Microsoft Publisher, 2016

This Month's contributors: Micky Knickman, Sandra Ruth, Pam Rihel, Don Hall, Dennis Smith, Neil Higgins, Carole Doerr, Michael John Neill, Dick Eastman, Terry Flanagan, Steve Costello, Bill Crowe, Cal Esneault, Keith, Scambusters, APCUG, Leo Notenboom, NEOPC, Microsoft Office art online, Newsletter is now

Online at:

lccug.com/newsletters or **lccug.com**

LCCUG ONGOING WORKSHOP
ALL ARE FREE AND OPEN TO THE PUBLIC

Problem Solving Workshop

Date: Tuesday - December 17, 2019
Time: 5:30 - 8 pm In-structor: Micky Knickman, Neil Higgins, Richard Barnett
Place: Learn how to repair or update your computer by changing hard drives, memory, CD ROMs, etc.

Members are encouraged to bring their computers anytime before 7:30 pm for as-

CANCELLED

Learning About Electronics

Date: Tuesday - December 17, 2019
Time: 5:30 - 8 pm Instructor: Sandee Ruth
Place: Learn how use you electronic devices.

Members are encouraged to bring their tablets, iPod, kindles, etc. at 5:30 pm for

CANCELLED

Learn About – Hands on Demonstration

Date: Tuesday– December 17, 2019
Time: 5:30- 8 pm Instructor: Neil Higgins
Place: Lorain County Community College 2600 Ashland Avenue, Lorain
Instructor: Neil Higgins

CANCELLED

Glary Utilities offers free powerful and easy-to-use system tools and utilities to help fix, speed up, maintain and protect your PC. Video tutorial available, which we will re-view. Available as a portable app as well.

It allows you to clean common system junk files, as well as invalid registry entries and Internet traces. You can manage and delete browser add-ons, analyze disk space usage and find duplicate files along with the ability to view and manage installed shell extensions, encrypt your files from unauthorized access and use, split large files into smaller manageable files and then rejoin them.

Furthermore, Glary Utilities includes the options to optimize memory, find, fix, or remove broken Windows shortcuts, manage the programs that start at Windows startup and uninstall software. Other features include secure file deletion, an Empty Folder finder and more.

All the tools within Glary Utilities can be easily accessed through an eye-pleasing and totally simplistic interface.
Glary Utilities website: https://www.glarysoft.com/

Please bring a flash drive to obtain software and handouts. If you would like to participate and get copies of the material for this presentation, please let Neil know by sending an email to Education@lccug.com.

Genealogy Tip of the Day

Living Along the Creek?

Geography matters in genealogical research. No one lives on a flat piece of white paper.

It never really clicked that my Rampley family all lived along Bear Creek in Hancock County, Illinois, until I was tracing where the creek emptied into the Mississippi River. When I traced the creek through Walker Township using an 1874 plat map, there they were: every member of my Rampley family. James and his sons all owned at least one piece of property through which Bear Creek flowed at least in part. Based upon the map, they also tended to favor land that contained a fair amount of timber.

I need to look at the locations in Ohio (where the family lived before they moved to Illinois) and Maryland (were the father, James Senior, was born) and compare the terrain. People tend to settle in an area where there is some familiarity.

Have you given thought to your ancestor's sense of geography?

New to the Library

Google Apps Made Easy – Learn to Work in the Cloud
Author: Terry Flanagan, Club Librarian, GVR Computer Club, AZ October 2019 issue, Greenbytes
www.ccgvaz.org   Newsletter@ccgvaz.org

Just added to the club library is *GOOGLE APPS MADE EASY – Learn To Work In The Cloud*. Google Apps is Google's response to Microsoft Office and LibreOffice. The table below lists the various functions and the names used.

FUNCTION	GOOGLE APPS	M/S OFFICE	LibreOffice
Word Processing	Docs	Word	Writer
Spreadsheet	Sheets	Excel	Calc
Presentation	Slides	PowerPoint	Impress
Database	N.A.	Access	Base
Forms	Forms	N.A.	N.A.
Note Taking	Keep	OneNote	N.A.
Photo Organizing	Photos	N.A.	N.A.
Vector Graphics	N.A.	N.A.	Draw
Email	Gmail	Outlook	Thunderbird
COST	Free	$100/yr.	Free

What makes Google Apps different? First and foremost Google Apps are web based. You do not download and install a program on your computer. You use your web browser, preferably Google Chrome, to go to www.google.com and log into your account and there they are. You do not have to be concerned with updates, maintenance, and backup issues. They are also platform or operating system independent. It does not matter if you are using a M/S Windows, Apple MAC or Linux computer, an Android smart phone, iPhone or iPad. The applications and your files are there in the cloud for you to access from wherever you are.

There are several advantage and disadvantages to working in the cloud. Being on the cloud makes it easier to share your files with others, which makes collaboration easier. There is no need to send email attachments back and forth or copy files onto flash drives. Also, all of your data will be consistent between your devices. If you make changes in Google Docs on your PC and later open the file on your iPad the changes are there. Even if you save the file locally to your computer it will be synchronized to the cloud version. The disadvantages are that you must have an internet connection since most of the things you will do with these apps are cloud-based and done online. The applications do not have as many features as the other office suites and some may have security concerns about their data being on the cloud.

From the chart above, you will note that each office suite

has applications that the other does not. Google Apps does not have a database module, but this is not a frequently used application by home users. Many common database functions can be handled by a spreadsheet. M/S Office and LibreOffice do not have a photo editing module, but there are a number of good stand-alone programs to perform those tasks.

Google Forms stands out as a unique application. Forms does what the name implies. You can easily create forms to gather information or take surveys. The data is automatically transferred to a spreadsheet and reports created to summarize the results and display them in easy to understand charts.

One final point – notice the bottom line in the chart above. Google Apps are free along with 15 gigabytes of cloud file storage. More space is available for a fee.

NEOPC Meetings

12/10 The NEOPC Luncheon will be held at Stella Mia Ristoronte 28751 Center Ridge Rd., Westlake December 10th at ll:45am. All members and guests are welcome to join us for good food and conversation. Please RSVP Lenore at:

lenorebman@gmail.com if you plan to come.
**Check out their website at:
http://www.neopc.org**

The Lorain County Chapter of OGS

is having it's next meetings on :

REGULAR MEETING LOCATION

**Check our webpage for the next program.
http://loraincoogs.org/events.html**

North Ridgeville Library, 35700 Bainbridge Rd. North Ridgeville, Ohio. Meetings are free and open to the public. Social time is at 6:30 PM and the program begins at 7:00 PM.

Jean Copeland: **jecopeland1975@gmail.com**.

Computer Club News

**Don't Forget to Bring
in Your Used Ink Cartridges
LCCUG is collecting empty ink
Cartridges**

*For every cartridge you will receive a
ticket for our special drawing.*
Recycle & Help Our Club Too!

ScamBusters.org

Two-Factor Security Check Is Not Enough — This is What You Need
By Keith

Simple phishing trick could help crooks crack two-factor authentication: Internet Scambusters #877

Two-factor authentication — the technique of requiring a second security check on your password — may no longer be enough to protect you.

A simple phishing trick may be all it takes to con you into giving away this precious sign-on information, as we explain in this week's issue.

Plus, we have the lowdown on a bug that hit the top-selling LastPass password manager — and news on how to claim compensation from Yahoo! after their security breach.
Let's get started…

Two-Factor Security Check Is Not Enough — This is What You Need

One password is not enough for your safety. We already told you that. To increase security, especially on sites that have our confidential information, it's common to have to answer a secret question.

But, increasingly these days, secure sites offer us the opportunity to use two-factor authentication. In very simple terms, that means that after entering a password, the site sends a code via email or to your cell phone that you have to key in to prove you're you.

We wrote about this a couple of years ago (see How to Easily Enhance Your Password Security) and much of what we wrote then still stands.

With one big exception.

According to latest investigations, there's a way to beat two-factor authentication. But you can still beat the crooks.

That's because they still have to trick you into giving up certain information. If you're wise to their scam, you won't fall for it.

At a conference on Amsterdam a few months ago, security experts showed how it works.

Crooks can use two pieces of software that work together to steal your two-factor (or 2FA as it's sometimes called) information.

First, they use tricks similar to those used in phishing to take victims to a fake sign-on site, where they have to key in their log-on details.

The scammers then use this information to log onto the genuine

(Continued from page 8) Two Factor Security Check is Not Enough...

site the victim was hoping to visit, which then generates the 2FA code and sends it to the victim's phone.

Alternatively, the user is asked to use a piece of authentication software on their phone, which generates a random code that has to be input within 60 seconds.

Either way, the victim keys this number into the fake page, giving the scammers everything that they need to pass themselves off as the user.

All of this is done automatically by one of the pieces of software, enabling the crooks either to use the hijacked account or monitor transactions.

In many cases, once the two-factor code has been entered on a site, users can opt to not have to use it again on the same computer, or to delay inputting it again for a few weeks.

This gives the crooks complete freedom to roam around victims' online accounts and do whatever they want on the site.

Researchers believe 2FA is still a worthwhile security device but urge users to be more vigilant than ever about landing on a fake, phishing page. That means checking the site is secure.

And that means looking for the 's' in the 'https' on the address line — though this too can be faked — checking that you keyed in the correct address without errors and avoiding clicking on links that pretend to take you to a legitimate page.

A better, more effective security contender has appeared recently that might be worth considering in the future. It's referred to as "universal second-factor' (U2F) authentication.

This involves a physical device, often a USB or fingerprint reader connected to the computer that the criminals can't get their hands on. The authentication takes place on the user's PC. These are not expensive, starting at around $15, and are easy to use. But, generally speaking, the more you pay, the more secure and effective the device is — according to online reviews.

LastPass Bug
Staying on the topic of passwords, you might have read recently about a bug found in the most popular password manager, LastPass.

Like all password managers, this software works by requiring a user to key in a master password. It can then automatically generate and "remember" sign-on details for any site.

Without getting technical, the newly discovered bug could have enabled hackers to gain access to data from sites previously accessed by the user.

The bug affected only users of Chrome and Opera browsers and LastPass was quick to put it right.

However, if you use this software and don't have it set to automatically update, do it now. The "safe" version is number 4.33.0.

To check the number of your version, click on the LastPass dropdown icon and then on "Account Options." From there, click on "About LastPass," which opens a small screen with details including the version number.

To update, you have to download the latest version of the program and install it. You don't have to uninstall the previous version. This is used to transfer data from the old to the new.

Going forward, we're likely to see more improvements in password and Internet security, but you should always let "caution" be your watchword. And if you have any reason to suspect you've been hijacked on a particular site, whether through two-factor authentication or any other means, change your password immediately.

Alert of the Week
One-time darling of the Internet, Yahoo!, has agreed to a settlement to compensate victims of a data breach.

The organization, now owned by phone company Verizon, is to pay up to $358 to users who had a Yahoo! email account between 2013 and 2016. But you have to jump through a few hoops to get your money.

Interesting Internet Finds – September

Author: Steve Costello
scostello@sefcug.com

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).

Here's What You Should Use Instead of CCleaner
https://www.howtogeek.com/361112/heres-what-you-should-use-instead-of-ccleaner/

I still use CCleaner, but others have concerns lately. For those who no longer use it, this post tells you what you should use instead.

Gmail For Mobile: Disable Conversation View?
https://www.askdavetaylor.com/gmail-for-mobile-android-disable-conversation-view/

Did you know that you can disable conversation view on your mobile (Android only for now)? Dave explains what conversation view actually is, and how to disable it in Android Gmail.

Why Is It So Important to Use a Different Password on Every Site?

by Leo A. Notenboom

Using different passwords on different sites is not only good practice; it's necessary to keep your accounts safe. I'll review why, and how best to handle a plethora of passwords.

I keep hearing that I'm supposed to use a different password on every internet site where I have an account. What a pain! I can't remember all of those passwords. Yeah, I know. You want me to use a password manager thing, but that seems like putting a bunch of really important things into a single basket. What if that basket gets hacked? I use a strong password. Why isn't that enough?

The hacks of several online services have brought this issue to light once again.

I'm sorry, but a single strong password just isn't enough anymore. You must use *different* strong passwords on every site where you have an account — at least every important site.

And yes, you must devise a way to manage them all.

Let me run down an example scenario that's a cause of all this emphasis on different passwords.

The all-too-common scenario
The scenario I'm about to describe is *very* common. While the specifics won't apply to you exactly, conceptually it will illustrate what can happen.

Let's say you have an account at some online service. I'll call it Service A. In addition, you have a Yahoo! account, because you used it years ago; a Google account, because you now use Gmail and a number of other Google services; a Microsoft account, because you have Windows; and we'll throw in a Dropbox account, because you've been listening to me recommend it. You probably have other accounts I haven't listed here, but you get the idea. You have lots of accounts at a number of online services.

You have a wonderfully strong password that you've memorized: 16 completely random characters.

And you use that same wonderfully strong password for all those accounts.

Here's how it can go horribly, horribly wrong.

Anatomy of a hack
Service A has the best of intentions, but honestly, they don't "get" security. Perhaps they store passwords in their database in plain text, allowing anyone with access to see them. They do that because it's easy, fast, and solves the problem quickly. They make the assumption that the database containing your password will be impenetrable.

Hackers *love* it when site designers make assumptions like that, because, of course, the assumption is wrong.

One day, a hacker breaches service A's security and steals a copy of the user database. The hacker walks away with a database that contains the following information for every user:

- Their login ID
- The email address associated with the account

The password (or enough information from which the password can be determined)[1]

Password hints/security questions

They can log in to your account on Service A. That may or may not be a big deal, depending on exactly what Service A is and how you use it.

But it opens a very dangerous door.

It doesn't have to be a hack
It's important to understand that while this example centers around what we hear about in the news most often — the hack of an online service and theft of their user database — it's certainly not limited to that.

Essentially, anything that could compromise your password brings you to this point. That includes:

- Sharing it with the wrong person.

Keyloggers and other malware sniffing your password as you type it in.

Improper use of an open Wi-Fi hotspot.

And so on.

Anything that puts your single password into the hands of a malicious individual puts you at greater risk than you might assume.

Password skeet shooting
Once they have your password, the hackers go hunting.

As most people have accounts on one or more of the major services I mentioned, the hackers start trying the information from Service A as if it were the correct information for Gmail, Microsoft, Yahoo, Facebook, Twitter, Dropbox, and more.

They try your email address with the password they stole from Service A to log in to the email service that you're using.

They try your login ID and password (or that email address and password) on as many other services as they can —

- and very often, *it works.* The hackers gain access to some other account of yours that was completely unrelated to the

(Continued from page 10) Why Is It Important To Use A Different Password On Every Site?

initial security breach.

Unrelated, of course, except that you used the same password at both.

If you use the same password everywhere, a *single* leak of that password puts *all* your accounts at risk. Hackers will be able to log in to your other online accounts as well. Maybe not all; maybe only a few…
…but a few is all it takes.

The weakest link
Note that this has absolutely nothing to do with the security expertise of the sites where your account is eventually compromised. Gmail, Outlook.com, Yahoo, and others have excellent security, but that doesn't factor into this scenario at all. Service A was the weak link. Their security wasn't up to the task. Their database was breached. Their information was leaked. Your account information and password — the password you use everywhere — was exposed.
Service A was at fault.

But the real problem is your use of that single password everywhere.

It shouldn't be this way
I'll happily admit that things like this shouldn't happen.
But they do. Not terribly often, but often enough.

And most services are better at security than our fictional Service A.

But it's also not a black-or-white equation. Even large corporations, which either don't know any better or simply make a mistake, can put your information at risk. For example, a hack at Adobe a couple of years ago potentially exposed the passwords of 130 *million* Adobe account holders. I hate to say you can't trust anyone, but ultimately, you *shouldn't* trust anyone not to accidentally expose your password.

And, as I mentioned above, it doesn't have to be a big service breach for there to be a problem.

Using a different password on each site limits your exposure if any site is compromised.

Managing lots of passwords
So it comes down to how to manage a lot of different, long, and complex passwords.

I still recommend LastPass, and use it myself.

Doesn't that put all my eggs in one basket?

Yes, it does. But it's a very good basket. And I've taken additional steps to ensure that it stays that way.

I talk about LastPass in more depth in LastPass – Securely Keep Track of Multiple Passwords on Multiple Devices, but I'll highlight two important reasons I consider LastPass secure:
The people at LastPass don't know your master password.

●They couldn't tell you what it is if they wanted to. They cannot access your data *at all*; all they can see is the encrypted data. Even if a hacker were to somehow gain access to their databases, *which has never happened*, the hacker would also be unable to decrypt and view your information, because LastPass does encryption right. Decryption happens locally on your machine, so the only thing ever transmitted between your computer and LastPass is the encrypted data.

●Of course I use a strong password. But LastPass also supports two-factor authentication, and I've enabled it on my account. If you somehow got my master password, you'd still need my second factor *in your possession* to be able to unlock my LastPass vault.

●Ultimately, it's up to you. There are several password managers out there, but LastPass is the one I trust.

The very short bottom line
My recommendation remains:
- ●Use long, strong passwords. Twelve characters minimally, ideally more, and randomly generated (there are several random-generator tools available, including one in LastPass). Alternately, and if allowed, use a pass*phrase* at least four words long, ideally with spaces.
- ●Use a different password for every login account you have. *Every single one*.
- ●Use a password manager like LastPass to keep track of them all for you.
- ●Use a strong password or pass*phrase* on LastPass itself. Enable two-factor authentication on LastPass for additional security of that very important basket of information.

This work by Ask Leo! is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. Additional information is available at https://askleo.com/creative-commons-license/.

Pam Rihel prihel1947@gmail.com
Dick Eastman
http://www.eogn.com.

Have you tried AncestorSearch on Google Search for Searching for Ancestors (or Living People) Lately?

Randy Majors is well-known to readers of this genealogy newsletter. He has created several mapping utilities that add functionality to Google Maps, primarily for use by genealogists. See https://duckduckgo.com/?q=site%3Aeogn.com+%22Randy+Majors%22&t=brave&ia=web for a list of past newsletter articles about Randy and his many Google Maps enhancements.

Now for something completely different. Randy has written a new and somewhat different bit of software to use Google Search (not Google maps) to find ancestors and even for finding living people.

He writes, "Enter AncestorSearch on Google Search, a free search tool that uses Google search enhancements so that you are much more likely to find mentions of the ancestors (or living people) you're looking for that are otherwise buried in thousands of Google search results. Basically, it uses Google advanced search operators behind the scenes so you don't have to spend time typing a bunch of awkward symbols."

You can read the full story on Randy Majors' web site at: https://www.randymajors.com/2019/11/have-you-tried-ancestorsearch-on-google.html.

Do you have comments, questions, or corrections to this article? If so, please post your words at the end of this article in the Standard Edition newsletter's web site where everyone can benefit from your words. You might also want to read comments posted by others there.

Governor Cuomo of New York has Signed Legislation Allowing New York Adoptees to Obtain Records of **Their Birth Information** New York Governor Andrew M. Cuomo signed S3419 into law on November 14, 2019, making New York the tenth state in the country to secure or restore equal rights for adult adopted people. More information, including the full text of the New York's newly "adopted" (pun intended) Public Health Law § 4138 may be found in the Adoptee Rights Law web site at: https://adopteerightslaw.com/new-york-obc/.

"OBC" IS AN ABBREVIATION FOR "ORIGINAL BIRTH CERTIFICATE"

My thanks to newsletter reader Bill Hinkle for telling me about the new legislation.

Do you have comments, questions, or corrections to this article? If so, please post your words at the end of this article in the Standard Edition newsletter's web site where everyone can benefit from your words. You might also want to read comments posted by others there.

Lock Up Those Photos

Author: Bill Crowe, Director, Sarasota Technology User Group, FL
October 2019 issue, STUG Monitor
www.thestug.org
director1@thestug.org

Last month I lost my wallet. Not a good day. I knew the last time I had used the card, and from there I went straight home. They did not have the card at my last stop, so I had either lost it on the way to the car or at home. After an extensive search, I had to go about cancelling and replacing all my credit cards. I had to do the same for all my other cards like medical cards, Driver's license, Costco's, and others. Not a fun job. The job would have been so much easier if I had kept a record of all my cards. I got to thinking that if I had taken a picture of each card (front and back), I would have had them on my iPhone. That would have solved the problem.

Thinking about it further, what if someone got my phone or was able to access my iCloud and gain access to my info? All my cards were there for the taking. I was hoping that there was a way to lock photos on my iPhone, but Apple has not yet provided one. I knew there must be an app for that, and 'By Golly' there is.

Credit: www.privatephotovault.com

There are, of course, many applications that can do it, but one of the best is called Private Photo Vault. The following is a brief introduction to Private Photo Vault. Private Photo Vault is one of the best free applications to protect your personal photos and videos by password/pattern-locking. This feature-rich app allows easy album organization by allowing you to transfer images and videos from iPhone's photo app to your new protected album. All you need to do is select photos you want to hide and password-protect them on your private album.

Private Photo Vault has a tri-protect system. You can either hide your photos via a secure password system or a nifty pattern lock system. There's also a pin lock option that lets you hide an image by entering a 4-digit pin.

Of many additional features, my favorite is the decoy password option. It allows users to enter two passwords – one for general access and another for those albums you want to really secure. With a smooth interface, and simple yet extremely secure protection option, the app is a good way to hide your photos on your phone.

By the way, the end of my story is that after I cancelled most of my cards, I found the wallet. It was in about the only place in the house I had not turned upside down.

See the tutorials at https://privatephotovault.com/tutorials/

Open Source Lab

Linux Mint 19.2

Author: Cal Esneault, Former President and leader of many Open Source Workshops & SIGs, Cajun Clickers Computer Club September issue, Cajun Clickers Computer News www.clickers.org   tsa70785@ gmail.com

Linux Mint is a Linux distribution based on Ubuntu. A long-term support version, Linux Mint 19, was released in June of 2018. An updated version, Mint 19.2, was released in August 2019. This version is known as a "point" release, and only software developed by Linux Mint has new

Menu Name	Program name	Funciton
Update Manager	mintupdate	Safely install software
Files	Nemo	File manager
Text editor	Xed	Edit text files
Image Viewer	Xviewer	View photos
Document Reader	Xreader	View PDF files

features different than Mint 19 (the majority of programs remain tied to the latest Ubuntu LTS repository). A few of the applications maintained by the Linux Mint team are listed below.

Users of Mint 19.1 can do a guided "in-place" upgrade to Mint 19.2 using the Mint Update Manager tools. Just be sure to first back-up the operational parts of your system using "Timeshift" and run the entire upgrade without interruption. None of your personal files will be affected. After reboot, you will be running the newest version.

Linux Mint developers have always tried to minimize user problems after updates. First, they classified updates into categories with respect to breadth of system impact. With increased frequency of Linux kernels, they made recovery from system-wide problems easier. As more installed but inactive kernels began to accumulate and increase system backup overhead, they allowed removal of older kernels one at a time using the Update Manager. With mint 19.2, they added a feature to remove multiple kernels simultaneously.

The Update Manager dialog screens changed significantly in the 19.2 version. The main menu reduced the number tabbed controls from five to three (see screen below).
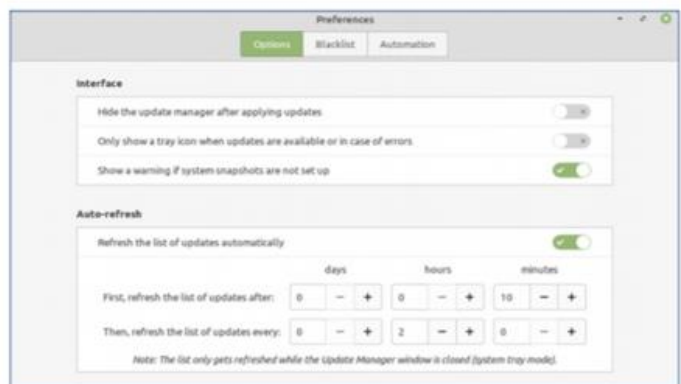
Besides simplification, the "levels" tab was eliminated. This seems to de-emphasize the previous strategy of impact categorization in favor of installing all updates with ability to roll-back the OS in case of failures.

If you are currently running Mint 19.1, this is an easy upgrade with very minimal risk. In that case, it is recommended to upgrade. If you are running Mint 18.x or another distro, however, this install would require a full rebuild and necessitate a lot of effort to maintain your existing information. In that case, don't install it unless you have studied the situation and have decided this is best for your long-term needs.

Current location of LCCUG meetings

Lorain High School / LCCC
2600 Ashland Ave.
Lorain 44052

The East side of the new Lorain High School is the College annex as seen in the photo.

You see parking area in the front there, facing Ashland Avenue.

Note: This building is behind the Frank Jacinto Elementary School.

Note: 26th St runs from the LCCC Bldg on Ashland Avenue to the George Daniel Fields football stadium on Oberlin Avenue.

This is an example of the classroom in which we will be meeting. Inside the door to the building entrance is an elevator that takes us to the second floor where this room is located.