Interface

Lorain County Computer Users Group
www.LCCUG.cominfo@LCCUG.com
Volume 32 Number 7 July 2021

2021

Inside This Issue

Tuesday
July 13, 2021

Digital Asset Estate Planning

Your ID Isn't Safe, Even After You've Died

Presented by

Judy Taylour,
SCV Computer Club

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

UNTIL FURTHER NOTICE MEETINGS ARE HELD ON ZOOM DUE TO COVID19

Meeting opens at 6:00 PM, program starts at 6:30 PM

GENERAL MEMBERSHIP MEETINGS CONDUCTED VIA THE ZOOM APP UFA

A Word From Our President

Most of our readers here should have received an email from me about the APCUG Tech4Seniors program every Monday at NOON (EST). In case you didn't see it, I will reiterate…...

This program is created by several members of APCUG. The Monday ZOOM event is facilitated by Ron Brown, a retired Doctor from Canada who winters in Arizona. The other presenters are from other many cities and they cover a different variety of relevant subjects each week. These presenters are the same ones who have been doing some of our presentations over the last year and they are comfortably familiar.

These sessions fulfill the geek in me and I look forward to them. They are also archived on YouTube. There is also a Chat session that several of these presenters offer on **Facebook live** on Thursdays (not ZOOM) or **Tech for Senior - Live – YouTube**. People are invited to sit in or watch the recording on Facebook or YouTube afterwards.

One of the subjects talked about is what they had learned about Windows 11 which is coming soon. I learned that not all of our computers will have the ability to run Windows 11. It sounds like it is going into another direction.

https://www.microsoft.com/en-us/windows/windows-11-specifications This webpage gives a lot of what is known so far about what's coming.

Neil has been posting various articles on what's being reported about Windows 11 on our Facebook group, **https://www.facebook.com/groups/lccug.**

Micky will be posting relevant information on our group's link page.

https://lccug.com/links/ as it becomes available.

If any of our members would like to review Cutting the Cord issues, let us know! (**mailto:president@lccug.com**) This area is always changing and we can share what our cord cutters have learned.

Our July meeting presenter will be sharing with us issues that we should be thinking of involving our digital legacy! The meeting title is, "Digital Asset Estate Planning: Your ID isn't safe even after you've died."

We're still looking forward to starting hybrid meetings in the fall. Stand by for more information as it develops.

Sandra Ruth

LCCUG Officers For 2021

President	Sandee Ruth president@lccug.com
Vice President	**Vacant** 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

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!

Tuesday
July 13, 2021

Digital Asset Estate Planning

Your ID Isn't Safe, Even After You've Died

Presented by

Judy Taylour,
SCV Computer Club

Each year the identities of nearly 2.5 million deceased Americans are used to fraudulently open credit card accounts, apply for loans and get cellphone or other services, according to fraud prevention firm ID Analytics. (Source: AARP)

The complexity of our digital lives has resulted in many different types of accounts, logins and passwords. The year after somebody dies is one of the most at-risk times for identity theft. Because death certificates are public records and obituaries are posted in newspapers, it is easy for criminals to search through the recently deceased's records and create fake identities. This presentation covers many ways your identity can be stolen and ways to prevent it being stolen after you are no longer here. You will also learn how to make it easier for your Digital Asset Executor to close your accounts.

THIS WILL BE A ZOOM MEETING
Please join us via ZOOM. A link to the ZOOM meeting will
be provided in a reminder email to be sent a few days before the meeting.

The Lorain County Chapter of OGS

is having its next meeting online:

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

We are having our meetings virtually using bluejeans.com.
To join the meeting on a computer or mobile phone:
https://bluejeans.com/5006724159?src=calendarLink
Also a link will be sent to you before the meeting.

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. Canceled Until further notice due to Covid-19

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

Executive Board Meeting Minutes

JUNE 1, 2021

The board Zoom video meeting for June was attended by Sandee Ruth, Don Hall, Micky Knickman, Pam Rihel and Neil Higgins.

Ray Baxter of APCUG will present his program on music thru the ages next week.

The July program choice by the board was 'Your Digital Legacy" by Joe Kissell. Sandee will check to see if he is available on our meeting date.

The August program has not been decided.

Sandee is awaiting a reply on meeting time for a joint meeting with another computer group.

Sandee is trying to set up a date and time for board members to visit the LCCC Lorain Learning Center at City Center to view their facilities as a possible club meeting place.

Neil moved, Pam seconded the meeting be adjourned.

General Meeting Minutes

JUNE 8, 2021

President Sandee Ruth called the Zoom video meeting to order. A motion to accept the minutes as shown in the June issue of the *INTERFACE* was made by Pam Rihel, seconded by Cliff Salisbury. Motion passed by voice vote.

Sandee advised members that next month's program will be Judy Taylour speaking on "Digital Asset Estate Planning".

Ray Baxter presented his program, "HOW TECHNOLOGY HAS CHANGED THE WAY WE LISTEN TO MUSIC". Ray is a Rock & Roll historian starting in 1956 with vinyl records (33's & 45's). His program was well received and interesting to our membership.

My first 78 record was ELMER'S TUNE and an Admiral record changer in 1941 for Christmas.

Genealogy Tip of the Day

Michael John Neill Genealogy Day 2021 Rootdig.com
mjnrootdig@gmail.com

There are Few Absolutes

Normally an ancestor has to be dead to have an estate settlement, has to be born to have a birth certificate, etc.

Think about what really HAS to be true about your ancestor or relative when you're researching them. He didn't have to get married to reproduce. He didn't have to name his oldest son after his father. She didn't have to get married near where her first child was born. He didn't have to have a relative witness every document he signed. There are few "have tos" in genealogy. Make certain you aren't using "have tos" to make brick walls for yourself.

When this tip appeared originally, I used the phrase "when your ancestor wrote his will." Of course not every ancestor was male and females had wills as well. But it's unlikely your ancestor actually wrote his or her will–it was crafted by an attorney or another legal professional. Most likely the only writing your relative did on their will was to sign their name on it.

MEMBERSHIP WITH LCCUG:

Yearly dues are now $15.00. For more information contact:

Dennis Smith
Director of Membership,
membership@lccug.com.

Meeting Location:
LCCC Community Center at Lorain [illegible]
2600 Ashland Ave, [illegible]
[illegible] - 2:00 P[illegible]
[illegible] is on the second floor.
E[illegible] is available for those in need.

No Meetings at the College

LCCUG WORKSHOP Class Ideas?

Neil needs your input into what classes you would like him to present to our members.

Please tell Neil [illegible] other officers what you would like to learn and we will be happy to [illegible] on your subject./subjects.

Neil Higgins Education@lccug.com.

No Meetings at the College

Lorain County Computer Users Group

2020 Calendar of Events

http://lccug.com
email: info@lccug.com

Using Zoom

Meeting opens at 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 12, 2021, Avast & PC Security

February 9, 2021 Password Managers by John Kennedy from APCUG

March 13, 2021 The Cloud is Here - Don't Get Left Behind - by Judy Taylour from APCUG

April 13, 2021 TeamViewer and AnyDesk - by John Kennedy from APCUG

May 11, 2021 Back Up Your Stuff - by Micky Knickman and Neil Higgins

June 15, 2021 How Technology Has Changed How We Listen to Music - by Ray Baxter APCUG

July 13, 2021 Digital Asset Estate Planning...

August 10, 2012 TBA

All other months to be announced.

Interesting Internet Finds

Steve Costello
scostello@sefcug.com

How To Log Out Of Facebook On Any Devices You're Logged Into
https://www.digitalcitizen.life/where-you-are-logged-on-facebook-log-out/
Have you signed in to Facebook on different devices? If so, you need to periodically follow the directions in this post to be sure you are logged out of any devices you don't need to be logged in on.

It's Unsubscribe Season! Clean That Inbox
https://www.askwoody.com/2020/its-unsubscribe-season-clean-that-inbox/
I followed the advice in this post and now have a much cleaner inbox.

How to Buy a Laptop for Linux
https://www.howtogeek.com/185286/how-to-buy-a-laptop-for-linux/
This post from How-To-Geek explains why you shouldn't just buy a Windows laptop and then install Linux on it. Instead, it explains the advantages of buying a laptop designed for Linux from the start, with links to some Linux you can buy now.

Member of Association of Personal Computer Users Groups

Thinking of shopping with Amazon? Well you can now go to our **lccug.com** website and just click on the amazonsmile link and start shopping.

Our club gets rewarded for any items purchased from our website. So the more you buy the better it is for our club. SO START SHOPPING.

NEED HELP?

Here's Who to Contact:

Neil Higgins
440-985-8507 - **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 9:00 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 no answer

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

LCCUG Ongoing Workshop

All Are Free And Open To The Public

Problem Solving Workshop

Date: Tuesday - July 20, 2021
Time: 5:30 - 8 pm Instructor: Micky Knickman, Neil Higgins, Richard Barnett
Place: Lorain County Community College @ 2600 Ashland Avenue, Lorain

Cancelled

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 assistance from Micky, Neil & others.

Learning About Electronics

Date: Tuesday - July 20, 2021
Time: 5:30 - 8 pm Instructor: Sandee Ruth
Place: LCCC @ 2600 Ashland Avenue, Lorain

Cancelled

Learn how use you electronic devices.

Members are encouraged to bring their tablets, iPod, kindles, etc. at 5:30 pm for assistance from Sandee and any other knowledgeable members. The public is welcome to sit in on these classes.

Learn About– Hands on Demonstration

Date: Tuesday– July 20, 2021
Time: 5:30- 8 pm Instructor: Neil Higgins
Place: LCCC @ 2600 Ashland Avenue, Lorain

Cancelled

Do you know the specifications of your computer? What is really inside? We'll demonstrate three portable Windows programs (run from a USB Stick) that will tell a computer's storage, CPU, video, and other useful information (including your Operating System Product Key) . This will help determine if your computer will run certain programs, and will help find out what memory or video card upgrade you need.

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.

ScamBusters.org

SOCIAL SECURITY SCAMS HAVE BECOME AN EPIDEMIC, GOVERNMENT SAYS: INTERNET SCAMBUSTERS #865

Pretending to be from the IRS is getting tougher for scammers -- so they've switched their attention to Social Security.

In fact, Social Security impersonations have moved into the top slots among impostor scams.

We'll explain what the crooks are up to in this week's issue - and tell you about 10 things you can do to avoid the scammers.

Let's get started...

SOCIAL SECURITY TRICKS HIT TOP OF SCAMS LIST

Social Security imposter scams have now reached epidemic proportions in the US, outstripping IRS impersonation scams for the first time, according to the federal government.

Some 76,000 complaints valuing losses at more than $19 million were filed in the 12 months prior to April 2019. The comparable IRS sum was $17 million.

But it gets worse. Almost half of those complaints came in the final two months of that period, signaling criminal activity on a huge and growing scale. That can only happen because the scams actually work.

And that $19 million accounts for a tiny 3.4 percent of the complaints. The rest relate to reports of Social Security number (SSN) thefts, which can subsequently be used for identity theft.

The median or midpoint among individual losses comes out at around $1,500 per victim, which is about four times the amount lost in other types of fraud.

An indication of the scale comes from the 55+ age group organization AARP. Its director of fraud victim services says a massive 94 percent of calls to its Helpline are about Social Security scams.

The current main scam comes in a call from an impostor claiming the victim's SSN has been used in a crime and so it has been suspended. Sometimes, they already have the individual's SSN. If not, they ask for it as "confirmation."

PAY A FEE

Then, in order to reactivate or unfreeze the account, the victim will have to pay a fee, usually in gift cards or a virtual currency like Bitcoin.

Often, crooks also doctor your caller ID so it looks like the call is genuinely coming from the Social Security Administration (SSA).

The calls may also be automated (robocalls) but invite recipients to "press 1" to speak to an SSA official.

This can all seem pretty convincing except for one major factor - the SSA does not suspend Social Security numbers. Period. Nor do they call and demand money. So, if you get one of these calls, you can safely hang up.

Other variations of Social Security scam tricks aimed at stealing your info include calls or emails saying that you're entitled to a refund; you need to "update your account information"; the SSA computers are down; you need to enroll in a new program; they need you to answer some security questions such as giving your mother's maiden name.

It's all about identity theft.

SNAIL MAIL VERSION

Another scam even arrives by regular snail mail. It's a letter that offers additional security for your Social Security account - but, of course, there's a form to fill in with all your personal info.

Right now, there's an additional scam threat to Social Security recipients. Due to an oversight, the SSA actually "forgot" to deduct Medicare-related premiums from 250,000 Social Security payments for the first five months of this year. Yes, they really did this.

(Continued on page 8)

Newsletter Editor: Pam Rihel using Microsoft Publisher, 2016

This Month's contributors: Micky Knickman, Sandra Ruth, Pam Rihel, Don Hall, Dennis Smith, Neil Higgins, Michael John Neill, Scambusters, APCUG, Leo Notenboom, Steve Costello, Phil Sorrentino, Dan Douglas, Dorothy Fitch, Cal Esneault, Google images, Microsoft Office art online,

Newsletter is now
Online at:

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

Woohoo!

Your renewal dues have been reduced from $25.00 to $15.00. When everything else is raising their prices our Computer Club is lowering their dues.

(Continued from page 7) Social Security Scams...

That means, you may get a bill from a Medicare Advantage or drug plan insurer for the outstanding sums. But because the issue is potentially confusing, scammers will almost certainly use it to try to lever more money out of older folk.

If you get one of these bills, verify that the money genuinely hasn't been deducted from your Social Security check. Then download this explanation of what to do from Medicare.

ACTION LIST

Here are some other things to know to avoid falling victim to this scam:

1. Note that the SSA never emails requests for personal information.
2. Nor does it visit homes without making a prior appointment.
3. Never provide personal, financial and other confidential information in response to an unsolicited call. Any such request is a scam.
4. Don't wire money to someone you don't know, even if they say they're from the SSA.
5. Don't be fooled by callers who already have your SSN or the last four numbers.
6. Don't trust your caller ID.
7. Ignore phone threats. That's not the way government departments operate.
8. Securely protect and store your SSN and card.
9. If you're in any way concerned the call might be genuine, call the SSA on 1-800-772-1213 or 1-800-269-0271 -- or contact your local Social Security office.
10. Stay in touch and learn about the latest tricks from Scambusters - and please share this report with friends and family.

If we're too late with this warning and you already believe you're a Social Security scam victim, file a report **at https://oig.ssa.gov/report or www.identitytheft.gov/SSA.**

ALERT OF THE WEEK

The 419 Nigerian scam is alive and well. You remember; it's that email from a prince or government official who wants your help to smuggle money out of the country.

The past few months have seen a surge in this scam (which asks you for cash first so the big money can be sent to you).

When Backups Might Not Save You from Ransomware

Some ransomware goes beyond encryption.

by Leo A. Notenboom

Ransomware is known for encrypting your data and holding it hostage. It turns out that it can do more that backups won't protect against.

Not long ago, I ran across an article entitled “Why System Backups No Longer Shield Against Ransomware“.

As an absolute statement, that title is incorrect and sensationalistic. System backups remain a critical defense — perhaps your single most important defense — against ransomware.

And yet, as expected, ransomware is evolving. It’s important to understand what it’s evolving into, and what you need to do, if anything, to defend yourself.

Become a Patron of Ask Leo! and go ad-free!

Backups vs. Ransomware

Most ransomware simply encrypts files on your computer, and possibly your backups. Backups remain the most important safety net to recover from all malware, including nearly all ransomware. Some recent ransomware also threatens to publicly expose your data unless the ransom is paid. The best defense against this and all forms of malware are the steps you should already be taking to stay safe: using up-to-date software, having security measures in place, avoiding risky behaviors online, and being skeptical of phishing and malicious attachments.

Ransomware and encryption

Ransomware’s reputation is based on its personal and destructive nature.

When infected, ransomware methodically encrypts your files, after which it presents a message indicating that you can purchase the

(Continued on page 9)

(Continued from page 8) When Backups Might Not Save You from Ransomware

decryption key for some amount of money — the ransom. If you don't pay, your files remain encrypted and inaccessible.

If you do pay,1 you're supposed to receive the decryption key or a tool that will decrypt your files for you, returning your accessibility to your own data.

Backups play a key role in protecting you from this form of ransomware. By having backed up your files prior to their being encrypted, you can "simply" restore the files in their unencrypted state and get on with your life as if nothing had happened.

Backups can be complicated, but critical

I put "simply" in quotes above because it's not necessarily that simple.

Most ransomware does, indeed, just encrypt your data files without further impact. All you need to do is remove the ransomware malware, and then restore your files from backup. That actually is pretty simple.

Related

It's not as common as "plain" ransomware, but it happens: Will Ransomware Encrypt Backups?

Some ransomware takes the additional step of encrypting any backups it finds. It's not as common, but it can happen. Defending yourself requires a little extra preparation, typically in the form of taking some of your backups offline.

In either case, however, having those backups in the first place is what allows you to recover and move on without needing to pay the ransom.

Keep backing up.

Backups don't protect against a new threat

In recent months, the folks behind ransomware have modified their approach slightly. It's become a two-step process:

Steal a copy of all your data.

Encrypt your data.

This means they've taken your data hostage: they threaten to release their copy of your data publicly unless you pay the ransom.

That has little to nothing to do with the data encrypted on your system, and is a completely separate threat from anything backups can prevent. Restore all you want; the threat of public exposure remains.

The new threat is an old threat

It's important to realize that this isn't a new threat. Hackers have been stealing data and posting it publicly for decades. It's called a data breach: a system is infiltrated and data is copied and then posted publicly, often in hacker forums.

What's new is bundling it with ransomware and offering you an opportunity to prevent them from exposing your data.

Well, "prevent" might be a strong word. If you pay, they promise not to expose your data, and often promise to delete their copy.

Until sometime later, of course, when it turns out — surprise! — they didn't delete your data, and decide to extort more ransom from you.

The new defense is the old defense

I keep saying it over and over: ransomware is just malware. It's malware that has particularly destructive behavior, but it's nothing more than malicious software — malware.

Related

It's my single most important article: Internet Safety: 7 Steps to Keeping Your Computer Safe on the Internet

You defend against ransomware the same way you defend against any malware, and hopefully the same way you've been protecting yourself against malware all along.

Keep software up-to-date.

(Continued on page 10)

(Continued from page 9) ***When Backups Might Not Save You from Ransomware***

Have properly configured security software and hardware configurations.

Avoid risky online behaviors.

Don't fall for phishing attempts, and don't open unexpected, untrusted email attachments.

That last one is worth special mention. Opening email attachments is now the #1 way that ransomware infections and data breaches happen. No amount of security software, hardware, or policy can protect you from yourself.

The glimmer of good news

If all this seems a little far-fetched — who would hold your data for ransom, after all? — you might be right.

If you're an individual.

On the other hand, if you have a business — small, medium, or large — or have some other situation where you're holding sensitive data, you're clearly at higher risk of having serious problems if exposed publicly. Hackers know this, and if you happen to get infected with ransomware, you're among those more likely to get this more threatening combo package of encryption and theft.

Keep. Backing. Up.

No, backups won't protect you from absolutely everything — nothing can. But backups protect you from so many different types of threats and failures, you simply must keep doing them.

Tweak them if you like for additional safety from the malware known as ransomware, but keep backing up.

And don't let your guard down in other areas. Keep doing all the things you know and need to do to keep yourself safe from any and all malware in the first place.

The best and safest scenario is to never let the malware hit your machine in the first place.

But keep backing up.

Related Questions

Do backups protect against ransomware?

Yes, backups protect against most ransomware. Backups are probably the single most important defense against a ransomware attack. To protect against the threat of backups themselves being held hostage, periodically copy a backup offline so as to be inaccessible to any machines possibly infected with malware such as ransomware.

Can ransomware infect cloud backups?

Ransomware can infect cloud backups by infecting the machine they're backing up. While the cloud backup itself is not "infected", the files encrypted by ransomware may automatically be backed up, possibly overwriting their unencrypted predecessors. Many cloud storage services include detection of large scale changes typical of ransomware, and include recycle bins or other recovery methods.

How do I keep my backup secure?

Backups can be kept secure by restricting access to them and moving at least some of them offline to different locations. Some backup programs automatically restrict access to the backups they create, preventing unauthorized users from making changes, such as would happen with a ransomware infection. You can add additional security for this, and from other forms of disaster, by taking copies of the backups offline and placing them in other physical locations.

NEW!!!

$5.00 given away to members joining our meeting. If your name is called you will receive the full amount, no matter how many names we pull before someone is at the meeting.

Apps and Applications – Mobile and Desktop

By Phil Sorrentino, Newsletter Contributor, Sarasota Technology Users Group
January 2021 issue, STUG Monitor
www.thestug.org philsorr@yahoo.com

When we talk about computer software nowadays, we typically use the term Apps, referring to any software that is running on a computer, smartphone, or tablet. The term Applications was originally used for software other than the Operating System, but that seems to have changed over the last few years with the advent of Mobile devices - Smartphones and tablets. Also driving the change has been the migration towards the "Client – Server" architecture, where smaller Apps running in a client device (smartphone or tablet) can control a much more elaborate collection of Applications software running in a much larger server (in the cloud). Computing has been moving in this direction ever since the internet and the World Wide Web have become available to us. The term "App" has become very popular. In 2009, technology columnist David Pogue even proposed that the new mobile smartphones be nicknamed "App Phones".

And in 2010 App was listed as the "Word of the Year" by the American dialect Society.

So, here are some definitions, at least for this discussion. A computer program is a generally structured collection of instruction sequences that perform a specific task when executed by a computer. (How's that for a "Nerdy" definition?) Software is a general term and will refer to all types of computer programs for all types of computers. An Operating System is a collection of computer programs that manage computer hardware and software resources and provides common services for Application programs. An Application program is a computer program designed to perform a group of coordinated functions, tasks, or activities for the benefit of the user, for example, a Word Processor, a Spreadsheet, an Accounting program, a Web Browser, or even a computer game. These applications are designed to run on the computer hardware with the assistance of the Operating System (like Windows10, macOS, or Android), which is mainly involved with managing the computer hardware.

Before the Smartphone, circa 2007, we only had Desktop Applications, because we only had Desktop computers. Yes, I know laptops were available and they could be easily moved around, but basically, they were just portable desktop computers. So, Desktop Applications are software programs intended to be run on a desktop (or laptop) computer. Then came the Smartphone (and shortly later, circa 2010, the tablet), and these devices were very much different in that their screens were noticeably smaller and there was no mouse for selection/navigation, only a touch-sensitive screen. So, applications that could be used in this new smaller environment had to be created specifically to run on a small screen using your finger as a pointer/navigation device. These applications are software programs intended to be run on a mobile computer, a smartphone, or tablet, with limited input and output capabilities. So, a mobile app is a computer program designed to run on a mobile device, like a smartphone or tablet, with the assistance of the Mobile Operating System (like Android or iOS, or even Windows 10 for tablets).

Desktop applications are usually "fuller featured", whereas the Mobile app equivalent is usually smaller, "lesser featured", simpler, and may or may not be easier to use. This should not be unexpected when you consider that most desktop Apps are built to be used with the more capable input and output devices, (a mouse, a keyboard, and a much larger display), whereas mobile Apps are intended to be used with only a finger and a much smaller screen.

With the arrival of mobile devices, many popular Desktop Applications were the basis for new mobile Apps for the new mobile devices. Many Google desktop applications have been recreated for mobile devices. Your Google email can be accessed from the desktop application or the mobile App. Both devices will provide the same information from the Google email server. But, as we have noted, Mobile Apps are different from Desktop Applications in that they have

(Continued on page 12)

(Continued from page 11) Apps & Applications…

to run on a much smaller device with limited input and output capabilities. And not ony is there a display size and input/output capability difference, but the mobile devices are different way down at the hardware level, the central processing units, most of which are slower than their desktop counterparts. So, many applications exist as both desktop and mobile versions. Microsoft Word is available in a desktop version, the one that most of us learned word processing on, and Microsoft has released a mobile version that is available for both Android and iOS devices. This also holds for Excel and PowerPoint. Adobe Photoshop image editor is a desktop application and Adobe Photoshop Sketch is a mobile app that lets you draw and paint on a mobile device but is a condensed version of Photoshop.

Besides the Apps that have migrated from the Desktop world, there are hundreds of thousands of Apps that have been developed for mobile devices that take advantage of the fact that these devices are mobile. These Apps use the power of the server to provide capabilities to the user that could never have been accomplished with only the processing power of the device itself. Maps and navigation immediately come to mind. The memory and the processing power required for these capabilities, at least with the current technology, would never fit into a device the size of a smartphone. And some Apps take advantage of the fact that they know your location; remember smartphones have GPS and other techniques for location determination. For example, Glympse lets you send your current location to another device, so the user of that device will know where you are (for as long as you choose to give him that information). There are even some Apps that use your location to notify you if one of your friends (or contacts) is nearby. The capabilities that can be developed for the mobile devices have only scratched the surface. It almost looks like the software applications development emphasis has moved from desktop Applications to mobile Apps.

Dan's Desk

Backing Up

By Dan Douglas, President, Space Coast PC Users Group
The Space Coast Journal
www.spcug.com **datadan@msn.com**

We've discussed the subjects of performing backups recently at our meetings, so I thought I would update the article I wrote on the topic back in 2018.

Two types of files are required to be backed up. There are your personal files, normally stored in the following folders under your login account in Windows: Desktop, Documents, Downloads, Favorites, Music, Pictures, and Videos. Each user that has an account on a PC has their own set of these folders. If the user only uses the programs that come with Windows or has a standard set of programs that they add to Windows that are can be easily re-installed either from a DVD/CD backup or a download file, then that makes backup and recovery much easier. The other type of files to be backed up would be the Windows System Files. These include the Windows Operating System itself plus all of the programs/apps, files, and data used by those programs/apps.

If you have all of your personal files backed up and you have the files required to reinstall your programs, then you can easily get a replacement PC or hard drive restored completely.

Just about every PC user has heard that they should back up their PC, but based upon what I've seen, only about 20% have an active plan in place.

The reasons that I've been told that users do not perform backups regularly are along these lines:

- I don't know how to set it up
- It will slow down my computer too much
- It's too costly

(Continued on page 13)

(Continued from page 12) Backing Up

- I forget to do it

None of these are acceptable excuses anymore!

Let's go through these one by one and see how to address the issues.

Setting up your backup
In Control Panel, under every version of Windows since Vista, there is an app named Backup and Restore or Backup and Restore (Windows 7). This app is suitable for 99% of the user community.

This app lets you pick a target location for where your backup will be stored either on a local drive or a network storage location, which can include cloud storage. A schedule can be set for what frequency you want to use for creating your backups – daily and what time of day or weekly by day of the week and time of day or monthly by day of the month and at what time of day. You can also determine if you want just your file libraries backed up or the whole disk(s). In both cases, a System Image will always be created as well. The System Image can be used by a restore program to exactly duplicate your hard drive onto a new PC or a new hard drive. The retention period can also be set for how long to keep a backup for or you can allow Windows to manage the space and to automatically replace the oldest backup with the newest.

Selecting the best time to perform your backup
When you select the time of day to run the backup as described in the previous section, you must pick a time that will be when your computer will be powered on. The backup program cannot power on a PC that is turned off to perform a backup. So if you use it each Sunday at 7 pm, make sure you leave your PC on every Sunday evening. A backup that runs when you are using the PC can impact your responsiveness and will take longer to complete than running at a time that no one is using the PC.

Cost of running the backup
Since the backup program is included with every copy of Windows, there is no software cost. In addition, almost all external backup drives include a backup program of some sort. Cloning/backup software from Macrium is also recommended. The only cost is that of providing a backup drive, either as a local hard drive or a network-accessible location such as a Network Accessible Storage (NAS) or cloud storage. This drive can be used for other purposes so even that cost can be split across other activities. An external 5TB USB 3.0 drive can be bought for less than $130 lately, so that's cheap insurance for not losing all of your data.

Set it once and it's automatic
As we saw in the sections above, once you set up the backup program, it will run automatically as long as the backup location is accessible and the computer is turned on at the scheduled time. Perhaps a repeating calendar reminder note will help make sure that you are always protected!

Restoring from a backup is best suited to situations where your hard drive is damaged and some files can no longer be accessed or the system won't even boot up. I've seen a lot of computers recently, where the owner complains of poor performance and upon investigation, I've been able to determine that it was a hard drive failing that was causing the lack of responsiveness. The hard drive would sometimes retry reading a file hundreds of times before either being successful or unsuccessful. This causes the hard drive to fall behind in any other requests for data and therefore the whole system slows down.

The File History app, which was introduced in Windows 8, is the best program to use for restoring individual files. Every time a file is created, changed, or deleted a copy can be written to the file history backup drive. This drive can then be used to restore a previous version if required. This is a great recovery tool if you are ever a victim of a ransomware attack where your personal files are encrypted. You can add additional directories to be backed up in addition to the normal set of personal file folders.

(Continued on page 14)

(Continued from page 13) Backing Up

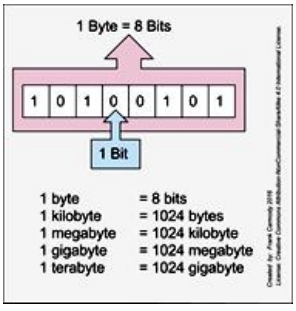
The option of Save copies of files specifies how often File History runs automatic backups. The default is hourly, but you can set the frequency to 10, 15, 20, or 30 minutes; 3, 6, or 12 hours; or choose to back up files once a day. Please note that a new version is created only when at least one item has changed in the file. The Keep saved versions option specifies how long to keep the backups. By default, these are kept forever, but you can also select 1, 3, 6, or 9 months, or 1 or 2 years. If your backup drives are tight on space, you can select the "Until space is needed" option and risk losing older backups quickly.

The best approach is to use the Backup and Restore program regularly, perhaps just using the System Image backup function, together with File History to fully protect all of your important files and folders. That way you will be protected against both hardware failures of the hard drive as well as accidental deletion or corruption of important documents.

Don't pass up the free cloud storage from Microsoft, Google, and others that can supplement what you backup to a local/network drive. Cloud storage is impractical for full drive/image backups due to the extremely long time that it would take to do a full recovery over the internet, but for individual files, it's great.

Bits & Bytes of Memory

By Dorothy Fitch, Editor, GVR Computer ClubNovember 2020 issue, Green Bytes
https://www.ccgvaz.org/ dmfitch@cox.net



Down in these parts of AZ south of Tucson, if your memory momentarily fails you, you might say you are having a "Green Valley moment." Your computer, of course, also has memory. Let's take a look at how it is organized. You have probably heard of bits and bytes, megabytes, and gigabytes. Do you know what each one is? What comes after a gigabyte?

A bit (BInary digiT) is like a light switch. It is either on or off. On represents a 1 and Off represents a 0. Your computer works by combining bits with each other to make larger units.

4 bits = 1 nibble, as in 0000, 0010, 0111, 1011, 1111, etc.

8 bits = 1 byte. You can do a lot more with a byte! There are 256 possible combinations of bits in a byte. A byte can store one letter of the alphabet. For example, an uppercase letter A is stored as 01000001 (which is 65 in the deci mal system).

2 bytes (16 bits) = 1 word

1 megabyte (MB) = 1024 bytes (1024 is 2 to the 10th power)
1 gigabyte (GB) = 1024 megabytes
1 terabyte (TB) = 1024 gigabytes
1 petabyte (PB) = 1024 terabytes
1 exabyte (EB) = 1024 petabytes
1 yottabyte (YB) = 1024 exabytes (a yottabyte = 1 trillion terabytes)

Those are the officially recognized units of memory, However, additional ones have been proposed (each one is 1024 times the previous one): Brontobyte, Geopbyte, Saganbyte, Pijabyte, Alphabyte, Kryatbyte, Amosbyte, Pectrolbyte, Bolgerbyte, Sambobyte, etc., all the way to Blamnebyte!

You can see them all here. This website says that if you are downloading 1YB (yottabyte) of data using a super high-speed Broadband, it will take 11 trillion years to download. It's all quite mindboggling, isn't it?

Now when you have a "Green Valley moment," you can call it something classier, such as a Yottabyte moment!

ScamBusters.org

5 SCAMS SET TO TRAP ANCESTRY HUNTERS

HOW SCAMMERS CAN TAKE YOU DOWN THE WRONG ANCESTRY PATH: INTERNET SCAMBUSTERS #742

Ancestors in front of old house

Forget about Sherlock. Real-life detective adventures are available for anyone trying to uncover their ancestry.

And as in any good mystery plot, villains are lurking around every corner waiting to trick family historians into handing over their money for little or nothing in return.

Forget about Sherlock. Real-life detective adventures are available for anyone trying to uncover their ancestry.

And as in any good mystery plot, villains are lurking around every corner waiting to trick family historians into handing over their money for little or nothing in return.

In this week's issue, we explain how these ancestry scams work and offer a view from one expert on how to give these crooks the slip.

Let's get started…

5 SCAMS SET TO TRAP ANCESTRY HUNTERS

Tracing your ancestry is all the rage these days. In uncertain times or as we get older, people develop a passion for finding out about their roots and building a family tree.

Although there are many professional genealogists, most ancestry "detectives" are amateurs and their sleuthing sometimes leads them into scams.

For instance, family historians are being targeted by crooks using the well-known inheritance con trick.

Most of us would be fascinated and delighted to learn that one of our ancestors was extremely wealthy.

It's just a short step from there to be taken in by a report that this ancestor left an unclaimed inheritance and that you could be in line to collect.

Scammers comb ancestry research websites for names and contact details of researchers and then deliver the "good news" about the inheritance.

As usual, they tell victims they have to pay a fee and other supposed processing charges in order to collect. Victims who pay up are then strung along with excuses and requests for more money until they finally realize they're being conned.

THE BOOK OF YOU

A second, well-practiced scam involves mailshots telling recipients their family history, and particularly the story behind their last name, has already been researched.

They may even say the history has been published as a book titled something like "The World Book of ....." (insert your surname here!) or "History of the ..... Family."

"These 'family surname history' books are little more than glorified phone books," says genealogy expert Kimberly Powell on the online research and information service About.com.

"Usually they will include some general information on tracing your family tree, a brief history of your surname (very generic and providing no insight on the history of your specific family) and a list of names taken from a variety of old phone directories."

MORE ANCESTRY SCAMS

If you're into family history, here are three more ancestry scams to beware of:

Phony Experts. As we said earlier, there are many professional genealogists who can often help solve

(Continued on page 16)

(Continued from page 15) 5 Scams to Trap Ancestry Hunters

some of the challenges of tracking down your ancestors.

But there are also plenty of others who set themselves up as experts but know little more than you do about how to conduct research.

Anyone can claim to be a genealogist; there's nothing illegal about that. But it's fraudulent to lie about experience, credentials, and qualifications.

There are several professional organizations, such as the Association of Professional Genealogists and the International Commission for the Accreditation of Professional Genealogists, that vouch for the skills of their members. In some cases, members may have had to undergo training and exams to vouch for their skills.

It's down to you to check them out before hiring. To learn more about these organizations and how to verify claims of membership, see this article: What to Look For in a Genealogist You Contract With to Research Your Family Tree.

Anyone can claim to be a genealogist; there's nothing illegal about that. But it's fraudulent to lie about experience, credentials, and qualifications.

There are several professional organizations, such as the Association of Professional Genealogists and the International Commission for the Accreditation of Professional Genealogists, that vouch for the skills of their members. In some cases, members may have had to undergo training and exams to vouch for their skills.

It's down to you to check them out before hiring. To learn more about these organizations and how to verify claims of membership, see this article: What to Look For in a Genealogist You Contract With to Research Your Family Tree.

* **Deceptive Software.** There are stacks of websites, computer programs, and applications that help enthusiasts create their family tree. They can be a boon for genealogists, especially as trees grow and become more complex.

But some of them are not worth the money you pay, either because similar products are available for free or because they're simply very poor products or services that may actually complicate the research process.

"Unfortunately, some of the biggest offenders are websites that pay for high placement in search results on Google and other sites," says Kimberly Powell. "Many also appear as 'sponsored links' on reputable websites that support Google advertising..."

The best way to avoid being hoodwinked into paying for this type of software or site membership is to find out what others are saying about them by doing an online search.

Beware, though, of websites claiming to list the "best" genealogy software. Some of these sites are as deceptive as the software they promote; they simply charge the program makers a fee to be included in the list.

* **Fake Coats of Arms**. What could be nicer or more impressive than displaying your family crest in your home?

Well, that depends on whether it's genuine or simply a figment of the imagination of the person who sold it to you.

Unless your ancestors were genuinely wealthy or members of the so-called nobility, it's highly unlikely that there's a family crest.

One trick some firms selling these products use is to employ graphics from the world of heraldry.

Heraldry is a complex collection of symbols, such as lions, armor or feathers, that represent qualities like bravery, justice or membership of the nobility.

There are hundreds of these symbols, so it's perfectly possible for anyone to combine a few of them into a badge that supposedly represents a name.

It's fun but it's phooey!

"Except for a few individual exceptions from some parts of Eastern Europe, there is no such thing as a 'family' coat of arms for a particular surname -- despite the claims and implications of some companies to the contrary," says Powell. "Coats of arms are granted to individuals, not families or surnames."

Producing these coats of arms is not strictly illegal, although the seller should be honest enough to explain what they're doing. So, it's okay to buy one of these products if you want, but be aware of what you're paying for -- basically a piece of creative fiction.

Discovering family history is a great legacy anyone can pass on to their descendants, and have fun in the process of doing the research. But avoid getting car-

ried away by your enthusiasm, or you could become an ancestry scam victim.

ALERT OF THE WEEK

Yoo-hoo! Need to speak to Yahoo!? Well, that phone number you found is a fake.

The famous news, email, and search provider has warned that, since it doesn't offer phone-based customer service, any number you discover on a search won't be genuine. Nor does it charge a fee for customer support.

So, if you see a search result with a phone number or use a service that charges a fee for support issues like changing your Yahoo! password, it's a scam.

LCCUG'S NEXT VIRTUAL GENERAL MEETING WILL BE HELD July 13, 2021

This is our eighth virtual meeting. We are hoping for more members to join in on these programs.

These meeting are fun and interesting and you also get to visit with other members that you have not seen in months, due to the Coronavirus - Covid 19 Pandemic.

It is not hard to join in on these meetings, as Sandee sends out the web address and all you have to do is click on it and when is opens up, find the icon that says JOIN, its as easy as that. Then Sandee will sign you in;

So please join in the fun and learn

Digital Asset Estate Planning

Your ID Isn't Safe, Even After You've Died

If you are in need of some help, well just call one of the board members and you will be helped.

If there is a program you would like to learn about just let the officers know and we can fix you right up.

You don't know what your missing by not tuning in to these great programs. Besides learning something new you get to visit with all your friends.

Hope to see some new faces at our next meeting and some old faces too. You know we miss you all. Be there or be square...

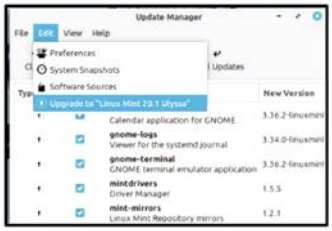
Linux Mint 20.1

By Cal Esneault, former President of CCCC and leader of many Open-Source Workshops & SIGs
Cajun Clickers Computer Club
February 2021 issue, CCCC Computer News
www.clickers.org office@clickers.org

Linux Mint is a Linux distribution based on Ubuntu. A long-term support version, Linux Mint 20, was released in June of 2020. An updated version, Mint 20.1, was released on January 8, 2021. This version is known as a "point" release, and only software developed by Linux Mint has features different from Mint 20 (the majority of programs remain tied to the Ubuntu 20.04 LTS repository).

Point releases tend to "refresh" some of the GUI features, and I checked out the Mint 20.1 version with the Cinnamon desktop. Examples of changes that were upgraded to the newest Cinnamon 4.8 desktop and a new set of screen backgrounds.

Mint continues its practice of making an upgrade from the previous LTS as easy and automated as possible. First, it will alert the user that a new "Update Manager" app is available. When this is updated, a new entry appears in the "Edit" section that gives a "one-click" upgrade. Be sure to perform all the other regular upgrades before proceeding.



The first steps in the upgrade lead you through a series of pages (see below) where you click "continue" to progress down a list. First and foremost, you are encouraged to back up your system in case issues arise.

There are sections on "Release Notes" (issues commonly encountered or helpful configuration hints) and on "New Features" (detailed descriptions of improvements and changes). You can skip the links if you wish, but I always find it advisable to take a quick glance. If you later need to review them after install, you can find these items on the Mint website.

Before anything is changed, you must check a box stating you understand any potential risks (for this type of release, risks are minimal). The upgrade only takes a few minutes, and a message at the end indicates if it was a success. You have to reboot for the upgrade to take effect.

As usual, this interim upgrade went smoothly on my machine. Although only a few minor items were changed, it is always good to keep current.