Interface

Lorain County Computer Users Group
www.LCCUG.cominfo@LCCUG.com
Volume 32 Number 6 June 2021

2021

Inside This Issue

President's Letter Pg.2
LCCUG Officers Pg.2
Program Pg.3
LCC-OGS Pg.3
Calendar of Events Pg.4
Genealogy Tip of the Day Pg.4
How Do I Remove a Virus… Pg.5
Minutes Pg.6
Interesting Internet Finds Pg.6 & 13
Classes & Workshop Pg.7
Never Attribute To Malice… Pg.8
Crazy Claims & Con Tricks Chase Keto Diet Pg.10
Next Virtual Meeting Pg.11
Alerts, Notifications & Alarms… Pg.12
Ransomware Threatens Pg.13

Tuesday
June 8, 2021

HOW TECHNOLOGY HAS CHANGED THE WAY WE LISTEN TO MUSIC

Presented by

Ray Baxter,

APCUG President & Treasurer;
President, Payson Computer Meet-Up Club

zoom

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

There is a program available that might be useful to some of our members or their family: The Emergency Broadband Benefit (EBB). We have posted about this on our Facebook page but here is some information for the rest of you.

This benefit will pay $50 every month toward the cost of your internet service. You must be eligible by making under a certain amount of income. There are a number of ways to qualify. The FCC has a “Do I Qualify” page online that should be checked if you think you might be eligible.

This was started during the Pandemic to assist families who need broadband for online school and jobs that require you to work at home. But you are not restricted to those reasons to be eligible for help paying for your Internet. Check out: https://getemergencybroadband.org/how-to-apply/.

Our **June 8** meeting should be a lot of fun as we review how we listen to music. Starting back with early records and moving through time to the current methods of streaming and downloading. Ray Baxter from APCUG will help us enjoy the music styles throughout that time as well.

We are planning an August program to help us deal with our digital life after death. How do we plan for what to do with our passwords? Our social accounts? Online memberships? Electronic banking? Re-occurring payments? We need to assure our security during this time. Watch our website to learn of the details as we get closer.

The stories in the newspapers about the demolition of St Josephs Hospital / Community Center have reminded me of the years we met there. We had over 300 members back in a day! Memories!!

JOIN US

Sandra Ruth
LCCUG President

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
June 8, 2021

HOW TECHNOLOGY HAS CHANGED THE WAY WE LISTEN TO MUSIC

Presented by

Ray Baxter,

APCUG President & Treasurer;
President, Payson Computer Meet-Up Club

This presentation will be a quick review of our music listening habits during the last 65 years and a look at today's download and streaming offerings. From 78s to 45s, LPs, the 8-track tape, cassettes, the Walkman, Compact Discs, iPods and more – Ray will cover it all.

Ray considers himself an early Rock and Roll historian and has a digital collection of over 45,000 songs that began when he first started collecting records (most of which he still has) in his pre-teenage years. When living in California, he was the President of the Doo-Wop Society of Southern California, a non-profit organization that for almost 14 years produced live quarterly musical stage shows featuring vocal groups of the 1950s.

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**.

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 TBA

August 10, 2012 TBA

All other months to be announced.

Happy Father's Day

Genealogy Tip of the Day

Michael John Neill Genealogy Day May 31, 2021 Rootdig.com mjnrootdig@gmail.com

Occupational Clues

Are you looking in other records besides census records for occupational clues on your ancestor?

Estate inventories are good places to get an idea of what occupation your ancestor might have had. Those with city-dwellers in their family tree should use city directories for clues of this type. Land records in some locations may provide occupations as a way to clearly distinguish the individuals involved in the transaction. And don't forget some European church records use occupations to distinguish men of the same names from each other.

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 now $15.00. 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
[illegible] - [illegible] PM
Meeting rooms on the second floor.
Elevator access 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 or one of the other officers what you would like to learn and we will be happy to hold classes on your subject./subjects.

Neil Higgins Education@lccug.com.

No Meetings at the College

How Do I Remove a Virus from My Browser?

By David Kretchmar, Computer Technician Sun City Summerlin Computer Club
http://www.scscc.club dkretch@gmail.com

Our computer operating systems have become more secure, so developers of malware have turned their attention to a more vulnerable target, our web browsers.

Chrome, Edge, Firefox, Safari, and Opera are the browsers most of us use to connect to the Internet. All of these browsers can be infected by a redirect virus, despite their built-in security.

Redirect viruses, also known as hijackers, can make your online life very difficult.

In this article, I'm going to describe the process of acquiring, identifying, and removing an infection from your browser. I'm going to focus on Google Chrome; the techniques are similar, yet slightly unique for each browser. Most users should be able to use the described procedures on their own systems, with small variations depending on the browser and underlying operating system (Windows, Apple, or some flavor of UNIX/Linux).

Redirect viruses can come from several sources.

Extensions

Hijackers can sometimes be "Trojan Horsed" in with browser extensions; extensions are small programs for a browser that serve the desired purpose, such as weather, price comparison, coupons, or productivity tools. If you install these extensions, you could unknowingly grant them the ability to influence your browser settings or change your preferences such as your home page or your default search provider.

Extensions are usually the first place to examine if you suspect you might have an infection.

Spam emails

On at least a weekly basis I receive an email telling me that my account at Amazon, Facebook. eBay, PayPal, etc. have been frozen due to suspicious activity. The email contains a link to click on to resolve the problem. In reality, if I clicked on the link provided, my problems would be just starting. If you receive an email informing you of a problem with, for instance, your Amazon account, access your Amazon account the way you would normally if you think there might be a problem.

Social Media

Links from your Facebook or Twitter feed could also be rerouted in phishing, redirects, or browser hijacking. Facebook is notorious for allowing questionable items to appear in your feed. Some bad links might be posted by unsuspecting Facebook friends who find it easier to copy and paste or just click Share than to vet an item. And no, Costco is not going to send you a $50 voucher if you just take this survey revealing all sorts of personal information.

Free software downloads from unreliable sites.
Hijackers can get added along with free software downloads. Often web sites will offer a desirable program but try to trick the user into downloading malware. Always look at the address bar to make sure you are downloading software from the legitimate provider's site.

Without realizing it, you could lose control of your browser by clicking on the wrong link on the wrong website.

Do I have a browser virus?

A browser virus on a PC or Mac is a browser hijacker that targets your browser. This type of malware is used to generate web traffic and collect information.

How do you find out if your browser has a virus? Here are the main symptoms:

- Your homepage redirects to a website different from what you expect.
- Unwanted extensions appearing in your browser (you might see icons at the top right side of your browser).
- Ads show up more often than they should, usually in unexpected places.
- Pop-ups and banners that advertise fake updates or software regularly appear.
- The link you click in search results redirects to dubious or possibly malicious websites.

Your browser performance decreases dramatically no matter where you go on the Internet..

A virus can also ask you to update a program such as Adobe Flash Player or download any other tool (program) that would help you fix the problem it is creating. These warnings don't always mean that you have issues with the browser but should be suspect.

If you notice any of these signs, your computer browser is possibly infected with a virus.

Potential risks of a browser virus

As a browser hijacker, a pop-up virus is categorized as a potentially unwanted program (PUP). Once the malicious program attacks your computer, it starts

(Continued on page 12)

Executive Board Meeting Minutes

MAY 4, 2021

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

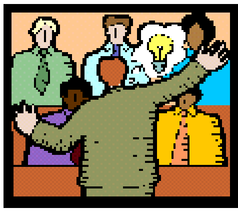
Sandee mentioned the May program will be Neil and Micky speaking on backing up your computer information. The June program will be with Ray Baxter from APCUG, subject: MUSIC.

Sandee has had discussions with other computer groups about joint ZOOM meetings. Discussions will continue to work out meeting time differences.

Dennis reported the person needing computer help from the Lorain County Community Action Agency is not responding.

Sandee mentioned Dina Ferrer of LCCC computer lab said they are hopeful the lab will open this fall

Dennis moved, Neil seconded the meeting be adjourned.



General Meeting Minutes

MAY 11, 2021

President Sandee Ruth called the Zoom video meeting to order. A motion to accept the minutes as shown in the May issue of the *INTERFACE* was made by Neil Higgins seconded by Micky Knickman. Motion passed by voice vote.

Sandee announced Ray Baxter of APCUG will present next months ZOOM program about music thru the ages. She also questioned member about what type of programs they would like to see in the future.
Also mentioned was the possibility of hybrid meetings this fall if a new meeting place becomes available.

Micky and Neil presented different versions of computer backup programs free and paid. The key message was Backup, Backup, Backup!

Neil moved, Pam seconded the meeting be adjourned.

Interesting Internet Finds

Steve Costello
scostello@sefcug.com

How To Clear Cache On Android (And When You Should)

https://www.makeuseof.com/tag/clear-cache-android/

Do you use an Android? If the answer is yes, you need to read and follow what this post says.

Opting Out Of Amazon Sidewalk

https://firewallsdontstopdragons.com/opting-out-of-amazon-sidewalk/

Have an Amazon Echo or Ring device? If so, read this post and learn how to opt-out of Amazon Sidewalk. I have opted-out for increased security reasons.

Member of Association of Personal Computer Users Groups

amazonsmile

You shop. Amazon gives.

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?

CALL FOR HELP! Computer Services

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

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, Davit Kretchmar, Dorothy Fitch, 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.

LCCUG Ongoing Workshop

All Are Free And Open To The Public

Problem Solving Workshop

Canceled

Date: Tuesday - June 15, 2021
Time: 5:30 - 8 pm Instructor: Micky Knickman, Neil Higgins, Richard Barnett
Place: Lorain County Community College
@ 2600 Ashland Avenue, Lorain

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

Canceled

Date: Tuesday - June 15, 2021
Time: 5:30 - 8 pm Instructor: Sandee Ruth
Place: LCCC @ 2600 Ashland Avenue, Lorain

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

Canceled

Date: Tuesday– June 15, 2021
Time: 5:30- 8 pm Instructor: Neil Higgins
Place: LCCC @ 2600 Ashland Avenue, Lorain

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.

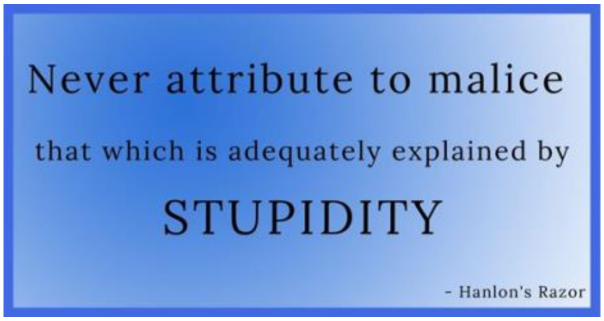
Please bring a flash drive to obtain software and handouts. If you would like to participate and get copies of the material for this presentation, please let Neil know by sending an email to Education@lccug.com.

Ask Leo! by Leo Notenboom

Never Attribute to Malice . . .

Jumping to the wrong conclusion rarely helps.

by Leo A. Notenboom



Never attribute to malice

that which is adequately explained by

STUPIDITY

- Hanlon's Razor

Malicious intent is commonly understood to be the cause of technological trials and tribulations. It's usually the wrong assumption to make. The pithy statement above is referred to as Hanlon's Razor.

It keeps coming to mind as I hear from people who are absolutely convinced that malice is at play in whatever they're experiencing.
It's *rarely* the case.

In Short

Many people jump to malicious intent to explain a problem with their computer or technology. That's rarely the case. More common are simple missteps, mistakes, failures, and errors. Looking for a malicious actor when there isn't one is time better spent focusing on the likely causes of odd behavior.

Hanlon's Razor, extended
When it comes to computers and technology, I extend Hanlon's opinion a little further.

Never attribute to malice that which is adequately explained by stupidity, error, or failure.

Just as it's rarely malice at play, it's not always stupidity either. All people, smart and stupid, make mistakes. Failures — particularly hardware failures — happen.

Any or all of those can be used to more than adequately explain the various and sundry problems we experience with technology.

My ISP is blocking a website…
This topic came to mind recently when I received a question about an individual's inability to access a specific website. He knew other customers of his ISP also could not access the site, whereas customers of other ISPs could.

Clearly, to him, his ISP was blocking the site.
That could be.

It's just not likely

There are other more plausible explanations.

Most likely, his ISP's **DNS** had a problem and couldn't resolve the IP address for the website in question. It's also possible the website in question experienced something it mistakenly interpreted as an attack[1] and blocked the ISP. It's possible the website's DNS was misconfigured, and due to DNS caching, his ISP was the first to see a problem that would eventually affect everyone.

Or it could be something else.

Malice is possible, as might be stupidity somewhere along the line; but errors and failures are much more likely.

My computer is behaving oddly…
Whenever someone's computer behaves in an unexpected way, many people's first response is, "Oh my God, I've been hacked!"

No. Just … no.
Seriously.

Hacking as the cause for odd computer behavior is *so rare*, I'm very comfortable just saying it's not the cause of the problem you're experiencing.

Software bugs, hardware failures, failed updates, flaky internet connections, worn-out batteries, exceeded disk capacities, and many more things are much more likely. All of these manifest in obvious ways that make it clear what's going on, or in ways that appear completely random as if the machine is "possessed" — just not by hackers.

And that doesn't even begin to touch on what we lovingly refer to as "operator malfunction": mistakes made by the person using the computer.

Ads are stalking me…
I have to include this class of behavior here, though it may be the most difficult to accept.
Without a doubt, there are privacy issues on the internet. But ads following you around *is not one of them*. Showing ads for something you've seemed to express an interest in isn't malicious; it's marketing. It's nothing more than salesmanship using today's technology.

Creepy? Maybe, if you don't understand what's happening. But malicious? No. Not in my book.

(Continued on page 9)

(Continued from page 8) Never Attribute to Malice….

Speaking of marketing…

Things change just to piss us off…

I hear this one after any major change to an operating system, application, or web service. Things looked one-way yesterday, and look different today. Companies must be doing this just to annoy us, right?

If you think about it, that doesn't even make sense. Change *intended* to annoy your customers is business suicide, as is change for the sake of change. No company wants or does that.

Related

Here's one thing that can *dramatically* improve your relationship with technology: embrace the most important attitude.

If your favorite OS, app, or website never changed, *it would be just as bad* for business. Never changing means not keeping up with current trends, not taking advantage of new technologies, and failure to adapt to new ways of doing things. You may be happy with an operating system that works the same way as it did 20 years ago, but the company that made it would be out of business if that's what they offered. Businesses that don't change, adapt, and grow die. It's a simple as that.

Growth is not malicious. Bad decisions about how to grow are not malicious — they're just bad decisions. To refer back to my extension of Hanlon's Razor, they're errors or failures.

That you're pissed off is certainly not intentional.

So, is there malice?

Of course, there is malice out there. Hackers hack, scammers scam, and spammers spam. Businesses knowingly leverage your information in malicious and often illegal[2] ways.

My point here is that when you experience something unexpected with your computer, technology, online experience, or data, unless you have evidence that says otherwise, *malicious intent isn't the place to start looking*.

The actual causes are usually significantly more mundane.

And, honestly, that's a good thing. More mundane causes are easier to deal with.

ScamBusters.org

CRAZY CLAIMS AND CON TRICKS CHASE KETO DIET

10 TIPS TO BEAT KETO PILL SCAMMERS: INTERNET SCAMBUSTERS #963

The keto diet claims it can help you lose weight. Perhaps. But some of the claims surrounding it are certainly fake, as we report in this week's issue.

We'll highlight the most common types of keto scams and give you 10 sound tips on how to avoid getting snared by the crooks.

We also have a warning about the rise in fake travel websites, as airline services resume some of their services.

Let's get started…

Diets come and go, but maybe none has attracted more scams and con merchants than the so-called keto diet.

Keto is based on the principle of ketosis -- in very simple terms, a process that sends your body into burning fat for energy instead of glucose from carbohydrates, leading to dramatic weight loss. In other words, it's a low-carb diet. It's already controversial because, although it usually does achieve a weight-loss result, some nutrition experts claim it's not healthy.

We're not about to enter into that debate, but we do want to warn about some of the outrageous claims and con tricks that follow in its wake.

Mostly, these center on pills, rather than foods, that claim to be able to send a body into ketosis.

That's not to say that all keto supplements are a fake but there's limited evidence that they work unless the person taking them has also cut their carb intake. And there are certainly instances of phony claims that keto pills and diets are endorsed by celebrities.

Many well-known names have been used, including actress and cookbook author Chrissy

(Continued on page 10)

(Continued from page 9) **Crazy Claims and Con Tricks...**

Teigen and TV entrepreneur and host Oprah Winfrey.

A good example is a suggestion that a keto "miracle" pill was taken up by the popular TV ideas-backing show *Shark Tank* and backed by one or more of the panel of investors.
The pills were claimed to melt away fat in a matter of days or weeks.

According to one of the leading keto sites (ketoreport.org), based on a number of investigations, including by the Better Business Bureau, there was never a *Shark Tank* episode featuring a keto pill.

"Many of these stories are riddled with keto buzzwords and optimistic claims," explains public health specialist Heather Acott.

"Some even have 'before' and 'after' pictures of celebrities who supposedly lost a drastic amount of weight by using these products. It's easy to see why many were digging out their credit cards ready to get their hands on the wonder pill."

Furthermore, while supplements containing certain chemicals are said to aid followers of the diet program, the supposed *Shark Tank* product packaging didn't list its ingredients.

"Putting unknown ingredients into your body can have a negative effect on your health and cause some serious damage to your body," Acott warns.

And this isn't the only keto scam. AARP, the organization representing older folk, reported recently that in a matter of just a few months it received 25 reports of keto pill scams.

A common trick was to offer a supply of pills free of charge. Consumers just had to pay a shipping and handling charge of a few dollars. What they didn't realize was that they were signing up for a recurring monthly shipment costing a couple hundred dollars. Instead of losing weight, they lost their money.

In some cases, victims found they had also "enrolled" in other offers, with charges regularly deducted from their payment cards.
As in other con tricks, attempts at activating a "money back guarantee" usually fail. In one case, a victim was told they could only have their money back if they returned pill bottles unopened!

One of the challenges is that so-called dietary supplements are unregulated by the US Food and Drug Administration (FDA), although it and the Federal Trade Commission (FTC) are able to prosecute alleged scammers.

If you're considering trying a keto diet, it's important to investigate the claimed pros and cons of any health and effectiveness claims, as well as understanding that any pills, if they work at all, still need you to limit your carb intake.

MORE ADVICE
Here are 10 more keto scam and advice pointers from both Acott and the FDA:

1. Beware of outrageous claims of huge weight loss in a short amount of time -- like losing 10 pounds in a week.

2. Avoid products that "guarantee" weight loss or make claims of a "scientific breakthrough" or that taking the pills is "risk free."

3. Be skeptical of spammed marketing emails. You should never even click on links in spam messages. Poor English or even use of foreign language are also red flags.

4. Avoid products that don't list ingredients in the packaging. Most likely, a pill that may support keto weight loss will contain beta-hydroxybutyrate (BHB).

5. If you plan to go on any kind of diet, talk to your doctor or other appropriate nutrition or health professional first.

6. Be skeptical of claims of celebrity endorsements.

7. Look for and check out companies that are registered with the FDA and certified to follow the agency's Current Good Manufacturing Practices (cGMP). Remember, anyone can make these claims -- so check them out with the FDA.

8. Favor products that offer at least a 60-day, no-strings, money-back guarantee. And

(Continued from page 10) **Crazy Claims and Con Tricks...**

pay with a credit card, which offers a degree of fraud protection.

9. Read the small print in any mail order service that you sign up for, checking if there's a recurring charge. Beware of "free trial" offers that involve automatic billing.

10. Research the name of any keto pill adding the word "scam" into the search box.

In these days of movement restrictions and work-from-home practices, anecdotal reports suggest that many people have gained unwanted weight. Some of these will clutch at straws and are ready to try anything. Keto pill scammers know that.

ALERT OF THE WEEK

The gradual easing of travel restrictions after recent limitations has sparked a wave of airfare scams.

Fraudsters are known to have created fake airline and travel websites, offering cut-price tickets that actually don't exist.

Make sure you know for sure who you're dealing with and only provide credit card and other financial information to organizations you've thoroughly checked out.

That's it for today -- we hope you enjoy your week!

Copyright Audri and Jim Lanford. All rights reserved. Reprinted with permission. Subscribe free to Internet ScamBusters at http//www.scambusters.org

Here are two PDF files you can get by going to these web pages. Very good information on Estate Planning and these are two different books. Please check them out.

AARP Personal Estate Planning Course Record Book pdf-pepc-record-book.pdf

AARP Personal Estate Planning Course Lesson Book pdf-pepc-lesson-book.pdf

Click on the website by placing the cursor on the website and click control that will open it up in a pdf.

LCCUG'S NEXT VIRTUAL GENERAL MEETING WILL BE HELD June 8, 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

HOW TECHNOLOGY HAS CHANGED THE WAY WE LISTEN TO MUSIC

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...

(Continued from page 5) How Do I Remove a Virus from my Browser.

modifying browser settings. For instance, it changes the default search engine and homepage, without asking for your permission.

The most serious problem created by having this virus is the ultimate invasion of your privacy; secretly harvesting as much of your personal information as possible to engage in identity theft. Some browser viruses are all about collecting personal details (IP address, location, searches, etc.) and sharing them with third parties. This may cause serious problems related to privacy and data security.

How to get rid of the browser virus

Delete unrecognized extensions

1. Go into your browser settings (in Chrome it is the three perpendicular dots at the upper right side of the browser).
2. Click on the Extensions tab.
3. Look for any extensions that shouldn't be there. If you find anything, select it and hit the Uninstall button to remove it.

Look for any extensions that shouldn't be there. If you find anything, select it and hit the Uninstall button to remove it.

Check your homepage and search engine settings

These settings appear in the settings area of your browser. In Chrome go into the browser settings and click on Settings. Make sure your homepage and default search engine are correct.

Additional things to check

1. Go to the Applications or Applications and Features folder and find any suspicious software. It may disguise as the desired application, so search for anything you don't remember downloading. Also, note the install date to identify possible problems and look at the last program you downloaded before noticed problems.
2. Check your Downloads folder for items recently downloaded from the Internet for clues about the possible problematic vector that has introduced the malware into your browser.
3. Once you detect the malware, drag it to Trash and empty it, or delete it and then remove it from your Recycle Bin.

Get rid of every trace of malware

After the above steps, download and perform a Malwarebytes scan as well as a full scan with your installed virus protection to make sure no harmful PUPs are left on your system.

Conclusions and Recommendations

To avoid getting browser viruses, pay attention to the websites you visit, files you download, and apps you install. Avoid using third-party software downloaders and installers - they usually include PUPs. Never ignore the warnings if your browser alerts you that a website is not secure.

Still, it's always better to prevent the problem than to try to deal with it. Browse wisely!

Alerts, Notifications, and Alarms - Oh, My!

By Dorothy Fitch, Editor, GVR Computer Club, AZ
January 2021 issue, Green Bytes
https://www.ccgvaz.org/
dmfitch@cox.net

I have started using alerts, notifications. and alarms to get my attention. Some of these come to my phone and some by email. Most of the time, I can choose what works best for me for each purpose. Of course, there are notifications that you get even if you didn't specifically ask for them, such as doctor appointment reminders, books that are ready to pick up at the library, and many others.

Here are some of my finds and handy tools.

Alerts:

My bank's website allows me to set up alerts for activity related to the bank and credit card accounts. For example, whenever my credit card is charged, either in a store or online, I immediately get an email. If that card is ever stolen or hacked, I will know right away. I can also set up alerts for payments due, deposits, balances, etc.

We have a smart indoor thermometer that alerts us to temperature changes outside a specific range that we set up. That way we can tell from wherever we are reading email if the house gets too hot or cold.

(Continued on page 13)

(Continued from page 12) Alerts. Notifications, and Alarms...

Notifications:

You can sign up at the AZDOT website to be notified of construction activity, accidents, or delays on I-19. After you submit your email address, you can choose which areas of the state, including I-19, you wish to include. These notifications were particularly handy when the Irvington construction area was still active. They also have a phone app that can notify you of highway events.

The US Postal Service offers a free Informed Delivery service to let you know what mail is coming to your mailbox. As mail is scanned in the postal processing center, an image is sent to your email address. (Lately, my email keeps showing me a picture of a postcard from the USPS that says that mail may be delayed. Ironically, that postcard still has not yet arrived!)

UPS's My Choice system tracks your packages and notifies you of their delivery. It's fun to check the map that shows the exact location of the delivery truck when it is in your neighborhood! FedEx has a similar Delivery Manager system and offers to deliver the package to a secure location where you can pick it up if you don't want it left outside your door.

On Election Day, I learned of the phone app from The Guardian that sends alerts to the "lock screen" of my phone when breaking news occurs. The Guardian is a British newspaper with a great reputation and worldwide coverage. So during the evening on 11/3, as election results started coming in, I would hear the distinctive tone I set up for my phone. That sound would prompt me to go look at the television to see the latest results. It was very handy. I am still enjoying the breaking news. I'm using the free version of the app, though a premium version is also available.

I have also subscribed to the free New York Times Morning Briefing and "breaking news" emails. (I usually get the Guardian notifications about 5 minutes before the NYT ones!) Their Morning Briefing has a summary of news headlines and a mini crossword puzzle. To read the entire article or enjoy the full crossword puzzles, you need to pay for a subscription. Lately, the headlines have been enough for me!

The weather station on our roof sends us an email every day with the day's high and low temperatures, wind speeds, and other data (the rain measure has never worked well, so its rainfall reports are rather suspect). It even has its own website, which I can access from my phone. If we ever get to travel again, we'll be able to see what the weather is like at home!

Alarms:

Alarms aren't just for waking you up. They can be great reminders to take your medicine, walk the dog, or whatever suits you. I use the Alarm feature of the Clock app on my Android phone and expect that an iPhone offers the same functionality.

Another phone alarm goes off at 6:59 pm Mon–Fri. We're usually preparing dinner at that time, and we like to listen to "Exploring Music" with Bill McLaughlin on the radio (KUAT, 90.5 FM). This reminds me to set the tuner to the radio so we can listen.

Once a month, my husband needs to submit data for his Rainlog project, where citizen scientists report the amount of rain received in their rain gauge. So, that alarm goes off on the first day of each month at noon as a reminder for him to do that. We have it on our shared Google calendar as a recurring task, but do we ever look there anymore? That calendar is rather empty these days.

It's nice that you can set up and customize multiple alarms to recur on specific days and times.

There are so many possibilities out there that you can subscribe to or set up. Give it a try! If you have a favorite attention-getter you would like to share, reply to this newsletter and let me know.

ScamBusters.org

RANSOMWARE 'THREATENS SAFETY AND HEALTH OF AMERICANS'

FIVE KEY DEFENSES AGAINST RANSOMWARE: INTERNET SCAMBUSTERS #961

Ransomware is costing US organizations and individuals an estimated $20 billion this year.

But the financial cost is only part of the worries about the spread of this malware.

It also puts people's health and safety at risk by disabling crucial networks and systems, as we report in this week's issue.

Let's get started…

RANSOMWARE 'THREATENS SAFETY AND HEALTH OF AMERICANS'

The growth of ransomware has reached crisis proportions to the point where it "jeopardizes the safety and health of Americans."

That was then-US Acting Deputy Attorney General John Carlin speaking a couple of weeks ago as he announced the launch of a new Department of Justice (DOJ) task force to tackle what is becoming one of the biggest malware crimes in the nation.

In fact, since we last wrote about the scam five years ago, the annual cost of ransoms to US citizens and organizations has ballooned from a few million dollars to several billions. One forecast suggests the total cost this year could be around $20 billion.

Businesses and public organizations like health and local government authorities are the main targets, shelling out as much as $20 million or more to get back access to their operating systems and frozen data.

Carlin says the affected organizations often pay up because they know the costs of damage from being locked out from their data could be many times higher than the amount of the ransom.

Organized crime gangs in China, Russia, and Eastern Europe are the main perpetrators. But individuals are also seeing a big uptick in ransom attacks, mostly from the Indian subcontinent and small gangs in the US.

Individuals usually face a ransom demand of between $500 and $1,000 payable in Bitcoin cybercurrency. Even if they pay, there's no guarantee the scammers will remove their lock. After all, they're crooks!

Consumers are also in danger when, as has happened, health service networks are attacked. This runs the risk that patients' health records and crucial monitoring and procedural programs are not available because files are locked up.

As you likely know by now, ransomware involves a hack attack or malware upload that, when activated, encrypts (jumbles and makes unreadable) the contents of a disk or even an entire network until a ransom is paid, usually in an untraceable format such as cybercurrency.

Most recently, home users have been targeted with a fake Microsoft Windows update that arrives by email and as a pop-up on infected websites.

"By any measure, 2020 was the worst year ever when it comes to ransomware and related extortion events," Carlin said in the *Wall Street Journal*. "And if we don't break the back of this cycle, a problem that's already bad is going to get worse."

One reason things might get worse is that people and organizations continue to pay their ransoms. As long as that happens, the crime is bound to grow. Some observers believe the only solution is for it to become illegal for organizations to pay up.

Ransomware payloads can be planted on corporate networks by hackers. But with home users, they usually arrive on personal computers via email links and attachments. Despite countless warnings, users still click on them, often because they are cleverly disguised to look like genuine communications.

100 MILLION ATTACKS

Big organizations use security specialists, purpose

(Continued from page 14) Ransomware Threatens Safety...

-designed toolkits, and other safety routines to protect themselves. But they still get caught out. So, what chance is there for the rest of us to stay safe? Many consumer Internet security providers are now including ransomware protection inside their software suites, underlining the importance of not only having one of these programs installed but also of ensuring it's regularly updated.

Computer security firm Trend Micro says it has blocked more than 100 million ransomware attacks in the past five years. During that time, the attack level has increased fifteen-fold.

These suites also include the ability to schedule regular backups so that if a ransomware attack succeeds, a user can reinstate an earlier backup.

However, "sleeper" ransomware could pose a new threat. After being installed on a system, it could remain dormant until activated sometime later. If malicious code is present but "sleeping" on a computer, it might also be copied onto a backup and activate when this is reinstalled.

Not surprisingly, therefore, a number of new services are appearing that claim to be able either to unfreeze a ransomed machine or at least recover locked-out data. But no one has yet come up with an infallible protection and recovery routine.

Some of the big names in software, like McAfee and Microsoft, also set up their own task force at the end of last year to tackle the issue. Security industry watchers are hoping this group will join up with the new DOJ team and work together rather than duplicating each other's efforts.

5 IMPORTANT ACTIONS

In the meanwhile, here are the 5 most important actions you can take to protect yourself from a ransomware attack and its effects.

Install and update security software as mentioned above. Here's a useful guide to some of the latest and best anti-ransomware products: The Best Ransomware Protection for 2021.

1.Take and keep regular system backups so that, even if your last backup was infected, an earlier one may be "clean." These should be stored on a separate device, disconnected from your PC or network, such as a removable drive, and preferably stored elsewhere.

2. Store your data -- documents, photos etc. -- on a separate disk or partition from your main operating system. That way, even if you lose access to your operating system, your data files might remain intact.

3. Avoid automatically clicking on links and attachments with emails, even if they appear genuine. If you can, take the time to check with the supposed sender.

4. In a worst-case scenario, where you lose valuable programs and data, or when the crooks fail to unlock, it may be possible to dis-encrypt the ransomed material. There are some specialist products for this but, generally, you will need to call in a professional. Even then, there's no guarantee it will work.

5. Should you pay a ransom? It's a tough call. However, the FBI is clear in recommending victims not pay. Plus, security experts at CyberEdge Group say that less than one in five victims who do pay get their files back.

Furthermore, as extortion victims in other types of crime know, once you pay, it makes you a potential easy target for future ransomware and other cyber-attacks.

ALERT OF THE WEEK

Tech security expert and podcaster Tom Merritt has published new guidance on defending against cybercurrency scams.

Find his five best tips here: Top 5 Ways to Protect Against Cryptocurrency Scams.

That's all for today -- we'll see you next week.

Interesting Internet Finds December 2020

By Steve Costello
scostello@sefcug.com

In the course of going through the more than 300 RSS feeds, I often run across things that I think might be of interest to other user group members. The following are some items I found interesting during November 2020.

Proxy Vs. VPN: When To Use A Proxy Server And When To Use A VPN?

https://www.digitalcitizen.life/when-use-proxy-and-when-use-vpn/

Have you heard about Proxies and VPNs. Do you know the differences, or when you should use which and why? Check out this post to learn more.

How To Configure Your Mouse For Comfort

https://www.makeuseof.com/how-configure-mouse-comfort/

With all the online classes and conferences, more and more people are using their mice for longer periods. If you don't already know how to make your mouse use comfortable, check out this post, and follow the advice.

7 Zoom Tests To Perform Before Your Next Meeting

https://www.online-tech-tips.com/computer-tips/7-zoom-tests-to-perform-before-your-next-meeting/

I have been doing a lot of Zoom meetings, and there have been times things just didn't go right. Now, after reading this I check these things out at least a half-hour before the meeting starts.

I'm Tired of Windows, So What Next?

https://askbobrankin.com/im_tired_of_windows_so_what_next.html

Bob Rankin explains some options for you if you are tired of putting up with Microsoft Windows.

Less Common Reasons Your Computer May Slow Down

https://askleo.com/less-common-reasons-your-computer-may-slow-down/

Most of us know the common reasons our computers slow down. Leo Notenboom covers some of the more uncommon reasons in this post.

How To Check If Your Android Smartphone Has RCS

https://www.howtogeek.com/702461/how-to-check-if-you-have-rcs/

If you have been hearing about RCS, and wonder if it is available for you on your Android, check out this post from HowToGeek.

What Is A USB Security Key, And Should You Use One?

https://www.reviewgeek.com/63448/what-is-a-usb-security-key-and-should-you-use-one/

I read this post and think it is overkill for my needs. But, if you use your laptop for business, have a lot of confidential information on your laptop when you travel, this post explains how you can benefit from a USB security key and what the disadvantages are.

Fire TVs Becoming Cable Box Substitutes

https://www.thestreamingadvisor.com/fire-tvs-becoming-cable-box-substitutes/

This article has some good information, especially for those who use both cable boxes and streaming services.