Interface

Lorain County Computer Users Group
LCCUG.com (or) info@LCCUG.com
Volume 34 Number 03 March 2023

2023

Inside This Issue

Thursday
March 9, 2023

Google Voice and VPN (Virtual Private Networks)

Presented by

LCCUG

Using Zoom & In Person Meeting

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

LCCUG Meetings will be happening on ZOOM & in Person

At our new time: from 10 am. - noon

Workshop will be held after the meeting starting at Noon

Please Email: info@lccug.com if you have any questions or concerns!

A Word From Our President

Spring is just around the corner, and we invite you to join us at the LCCC Lorain Learning Center on Thursday, March 9th at 10 am. Our discussion will center around the advantages of using a VPN and Google Voice, both of which are free tools that can be beneficial to us.

Last month, we explored ChatGPT, a highly discussed program that brings the world of Artificial Intelligence to us as a large language model. We examined a dozen examples and discussed their pros and cons, leaving everyone impressed and amazed. For more information, please visit our webpage under Presentation Weblinks.

After the meeting on March 9th, we will continue to offer our workshop to answer any hardware or how-to questions you may have. We encourage you to take advantage of this membership benefit and let us know beforehand if you plan to attend by emailing info@lccug.com.

Don't forget to stay updated on the latest technology news by following our Facebook page http://www.facebook.com/groups/lccug.

We also want to remind our members to consider attending the Monday Noon ZOOM meetings presented by Tech for Senior. Several computer club "seniors" from Canada, Oklahoma, Arizona, and Florida make presentations and answer questions. These sessions are recorded and posted on their Youtube page, and we have shared some of their segments during our meetings. For more information, please visit https://www.techforsenior.com/home, and feel free to ask us if you have any questions.

We value your input and would like to know what interests you. Are you interested in doing more on your phone? Learning about EVs (Electronic Vehicles), Cutting the Cord (watching TV without Cable), or security issues? Let us know!

Sandra Ruth
LCCUG President

LCCUG

LCCUG Officers For 2023

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	**Vacant** membership@lccug.com
Director of Advertising	Richard Barnett advertising@lccug.com
Director of Education	Neil Higgins education@lccug.com

Newsletter Editor: Pam Rihel using Microsoft Publisher, 2016

This Month's contributors: Micky Knickman, Sandra Ruth, Pam Rihel, Don Hall, Neil Higgins, Michael John Neill, Scambusters, Ask Leo, Jim Cerny, David Kretchmar, APCUG, Google images, Microsoft Office art online,

Newsletter is now
Online at:

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

Thursday
March 9, 2023

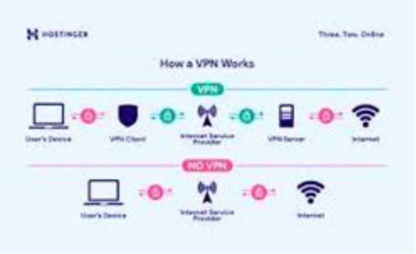
Google Voice and VPN (Virtual Private Networks)

Presented by

LCCUG

Google Voice is a free, powerful communication tool that allows you to make and receive phone calls, send and receive text messages, and even make international calls from your computer or mobile device.

A VPN is a network that allows you to access the internet securely and privately by routing your connection through a server and encrypting your online activity.



During the meeting, we will provide an overview of the basic features of VPNs and Google Voice, as well as some tips and tricks to help you get the most out of these platforms. Micky will share his experiences using these services.

Join us for this program! Hope to see you there!

apcug

Member of Association of Personal Computer Users Groups

LCCUG is on Facebook

Come and visit our Facebook page for interesting facts and ideas. You can get a lot of computer information from our Facebook page. Have a question ask it on Facebook.

https://www.facebook.com/groups/lccug

Woohoo!

Membership Dues

Your renewal dues have been changed from $15.00, To 3 years for $15.00. When everyone else is raising their prices our Computer Club is lowering their dues, so tell your friends to come and Join in the fun and learn computer information.

Tell your family and friends about this great deal. Once in a lifetime opportunity.

Executive Board Meeting Minutes

JANUARY 31, 2023

The board Zoom video meeting for February was held January 31 and attended by Sandee Ruth, Don Hall, Micky Knickman and Pam Rihel.

The board agreed their March board meeting would be Thursday, February 28.

Amazon has cancelled our Amazon Smile account. Pam will remove it from the ***INTERFACE.***

Various topics were discussed for future programs.

Sandee and Micky will check on the best place for the club's money (CDs).

Micky moved, Pam seconded the meeting be adjourned.

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

John Kolb

General Meeting Minutes

FEBRUARY 9, 2023

President Sandee Ruth called the hybrid meeting to order. A motion to accept the minutes as shown in the February issue of the *INTERFACE* was made by Ellen Endrizal, seconded by Doug Smith. Motion passed by voice vote.

Sandee announced next month's program will be about Google Voice and VPNs.

She mentioned members might consider a social get together sometime this summer.

Sandee then presented her well-prepared program on AI (Artificial Intelligence). She showed the many, many AI sites and explained the pluses and minuses of each. She said Google, Microsoft and Facebook are coming out with new versions of their AI.

MEMBERSHIP WITH LCCUG:

Yearly dues are now $15.00 For 3 years. For more information contact:

LCCUG
Director of Membership,
membership@lccug.com.

Meeting Location:
At a new time: from 10 am. - noon
in a new location: LCCC facility at
201 W. Erie, Lorain

Our meeting space is on the first floor – easily accessible – larger – refreshments available!
Please email
info@lccug.com if you have any questions.

Lorain County Computer Users Group

2023 Calendar of Events

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

Using Zoom & In Person

Meeting & program starts at 10 am

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

January 11, 2023 - QR Code 101 ZOOM ONLY

February 9, 2023 - Artificial Intelligence

March 9, 2023 - Google Voice, VPNs

April 13, 2023 - Amazon Warehouse and Digital Payments

… to be determined ...

December 12, 2023—Please check our website LCCUG.com for more updates. If you have anything you would like to know about, PLEASE let up know. We would really like your input.

Genealogy Tip of the Day

***michaeljohnneill,* Genealogy tip of the day**
March 6, 2023

Rootdig.com mjnrootdig@gmail.com

Per stirpes means "per branch." The phrase is often used in wills and other estate records to indicate how property is to be divided if some beneficiaries pre-decease the original writer of the will or owner of the property.

A relative has three children and in their will gives their estate to their children or to their children's descendants per stirpes.

Let's say the relative, named A has three children, B, C, and D. B has two children, C has three children, and D has four children. A dies and B, C, and D have already passed. All the grandchildren of A are living when they die. B, C, and D, had they been living, would have each received 1/3 of A's estate. That's how much each group of their children will split. Each of B's two children will get 1/2 of B's 1/3 share of A's estate, meaning they get 1/6 each of A's estate. Each of C's three children will get 1/3 of C's 1/3 share of A's estate, meaning they get 1/9 each of A's estate. Each of D's four children will get 1/4 of D's 1/3 of A's estate meaning they will get 1/12 each of A's estate.

Per stirpes as a way of splitting an estate is also often used to craft estate ownership when an individual dies with no valid will and the property is inherited by their heirs according to the appropriate state statute.

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 5:00 am to 3:00 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 or 440-308-8196
6:00 p.m. to 9:00 pm Monday thru Thursday
Genealogy help
prihel1947@gmail.com

Denny Smith Unavailable at this time
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 Workshops

All Are Free And some are Open To The Public

Problem Solving Workshop

Date: Thursday- March 9, 2023
Time: 12PM –Please show up by 12:30 Instructor: Micky Knickman
Place: LCCC @ 201 W. Erie Ave., Lorain, OH

Learn how to repair or update your computer by changing hard drives, memory, CD ROMs, etc.

This workshop is limited to LCCUG members in good standing.

The Problem Solving Workshop is being held at our new building, LCCC, 201 W. Erie Ave. Lorain, Ohio

You are asked to bring in your computer, laptop and other electronics that you need help with unless the problem/question can be replicated on any device.

Learning About Electronics

Date: Thursday - March 9, 2023
Time: 12PM –Please show up by 12:30
Instructor: Sandee Ruth
Place: LCCC @ 201 W. Erie Ave., Lorain, OH
Learn how use you electronic devices.

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

IMPORTANT NOTICE

Changes to the day of our meetings

Our meetings will now be held on the 2nd Thursday of the month
From January 2023 thru April 2023.
The times will be the same.
Workshop is also on Thursday after the meeting.

ScamBusters.org

LISTEN UP: DON'T GET CAUGHT BY THESE HEARING AID SCAMS

A revolution in the hearing aid world has opened the door to faster and cheaper access to devices - and to a new wave of bad practices and scams.

Since last October, consumers have been able to buy certain types of hearing devices "over the counter" (OTC), that's to say, without an exam or prescription.

The idea behind the move is to eliminate some of the costs of buying an aid if you suffer from mild to moderate hearing loss.

It means you could skip a hearing exam, fitting, and adjustment and just buy in a store or even online. Of course, that's not always a good thing, since everyone's hearing is different, and the best way to get a device that works well for you and fits properly is still to consult an audiologist and have your hearing issues properly diagnosed.

Nevertheless, the US Food and Drug Administration (FDA) has updated regulations to allow people aged 18 and over, with a low level of hearing impairment, to buy what are called "air induction" hearing aids without going through this process.

ENTER THE SCAMMERS

In a way, the new rule is akin to shoppers' ability to buy reading glasses over the counter. It's up to you, the consumer, to decide what you need.

Certainly, it brings the cost of buying a device into the hundreds of dollars rather than the thousands you could pay via a prescription.

But some firms are exploiting the change by using misleading ads and using all sorts of dubious marketing tricks.

These include:

- Making false or misleading claims about the technology behind devices
- Offering huge discounts based on fictional retail prices
- Pretending your part of a trial that gives you a special low price
- Selling devices that are not proper hearing aids but just sound amplifiers
- Failing to offer suitable trial periods, returns policies and warranties
- Hiding additional fees and upcharges
- Limited time deals forcing people to act too quickly
- Supposed "free" offers that are actually covered by the price you pay
- "Free" tests designed to talk you into

  buying more expensive devices

Letting you think you're buying a pair before discovering you're only buying one device

1. In other words, some of these shysters aren't really interested in your hearing, just in how many devices they can sell.

2. In one recent case, a leading hearing aids dealer was ordered to stop running ads claiming there's a government program that pays a Covid-related grant of up to $3,000 toward the cost of a device.

3. Another firm allegedly made a similar claim, saying buyers were entitled to a stimulus payment of $1,000. Their mailing even included a document that looked like a $1,000 check made out to the recipient.

4. BEFORE YOU BUY OTC

5. There are an estimated 37 million Americans with a hearing disability, but only a fraction of them - around 6 million - use hearing aids. High cost is a major factor; the FDA hopes the new rules will encourage the rest to consider following suit.

6. The first challenge is that unless you consult a professional, you probably don't know whether your hearing loss is worse that "moderate." But you could arrange an exam-

(Continued on page 8)

(Continued from page 7) Listen Up: Don't Get Caught By These Hearing Aid Scams

ination, which may be covered by insurance, to get a diagnosis before you buy. Check with your insurer.

7. The National Council on Aging (NCOA) also notes that buying OTC could mean missing out on professional sizing, custom earpieces, advice on proper use and maintenance, or follow-up fine tuning.

8. Still, according to the FDA, average costs of OTC hearing aids are about a third of the price of prescription devices, making it a worthwhile route to consider to deal with a mild or moderate impairment.

9. HOW TO PROTECT YOURSELF

10. But your hearing is too important to take risks. If you're thinking about going this route, here's what you can do to avoid getting caught out by the tricksters.

Research and understand the difference between a hearing aid and a simple amplifier. See Medical News Today: Hearing Amplifiers vs. Hearing Aids: What's the Difference?

1. Related to this, check if the device's sound settings can be customized - that is, that they don't just have a volume control.

2. Ignore the "free" come-ons. Offers might include a small payment for just taking a test, a buy-one-get-one-free, a year's supply of batteries. You're paying!

3. Don't yield to deadline sales pressure. Take your time.

4. Secure a reasonable trial period - 30 days as a minimum, 90 days ideally.

5. Similarly, check return policy and warranties - and get them in writing. No warranty? Don't buy.

6. Shop around to compare prices and features.

7. Always look for evidence to back up claims, particularly about technology.

8. Check the reputation of a seller by doing an online search and checking ratings with the Better Business Bureau.

9. Check if the supplier is registered with the FDA and the seller can prove devices comply with the regulations. Even though they're sold direct, OTC hearing aids are still regulated by the FDA.

10. Beware of being tricked into buying add -ons you don't need - for example, a Blue

tooth radio connection.

Check if the provider offers aftercare - such as adjustments, repair, replacement, and so on. To learn more, see this report from the NCOA: Over-the-Counter (OTC) Hearing Aids—What to Know.

Above all, take the time to do your hearing aid research so you know exactly what you're looking for. And steer clear of outrageous claims and offers. They simply don't add up.

THIS WEEK'S SCAM ALERTS

Crypto Crooks:

The cryptocurrency industry and its users lost more than $4 billion to hacks and scams last year. In a horrifying incident, a Canadian man was recently scammed out of his home and entire life savings. Crooks tricked him into making an initial investment then pointed him to a phony dashboard showing massive gains and luring him into putting in more and more until he had nothing left.

Sour Note:

Watch out for email attachments that end in ".one". This is the format for files used in Microsoft's digital notebook app OneNote. Clicking on the attachment loads malware onto your PC. Researchers report a surge in these messages during the past couple of months. They say because it's new and relatively unusual, it may have been able to bypass security software.

Why Is It Important to Have Different Passwords on Different Accounts?

It's one of the most important things you need to do.

by Leo A. Notenboom

Using a different password for every login is crucial -- and it doesn't have to be difficult.

Extracting a Password

Is it safe to have the same password for all of my email accounts? If one has an account in Yahoo! mail, Gmail, Rediff mail, etc., and sets the same password for all of them, will it be easier for a hacker or phisher to find out about it?

Using different passwords is *much* safer than using one password everywhere. In fact, it's critical.

Why?

Because hackers know that most people have more than one account *and* that most people don't take the trouble to set different passwords.

Admit it, you're lazy

I'll admit it: I'm lazy. When it comes to managing passwords, I'll bet money that most people are.

One password everywhere is *so much* easier. It's easier than even the easiest password management system.

It simplifies our lives not to have to remember passwords or use any special tools to remember for us.

The problem is, it makes hackers' lives easier, too.

Hackers know we're lazy

Hackers know that people find it easier to have one password everywhere.

Hackers know that people generally have more than one account.

Hacking a single account acts as a foot in the door to the others and leads to all sorts of mayhem.

One account leads to more

It's easy to guess that if a person logs in with username X and password Y on a system like Yahoo! mail, it's likely they'll replicate both username X and password Y on other services.

Once they've breached one account, hackers get clues that let them access other accounts.

Account confirmations and notifications are frequently sent via email. What that means is that your hacked email account contains many clues as to what other accounts you have.

If you use the same password everywhere, it's easy sailing for the hacker to quickly try those out and log in as you at multiple services.

For example, your Facebook login is your email address and a password. Well, if they've hacked your email account and you use the same password everywhere, they now know how to log in as you on Facebook.

The hack might not be your fault

Hacks happen through no fault of your own. You could be maintaining perfect security and still end up compromised.

Consider all the places you have online accounts. Let's assume that the one with the poorest security gets hacked, and the contents of their entire username/password database is stolen.

You just got hacked, and it wasn't your fault.

However: if you're using one password everywhere, the hackers now know it.

There can't be only one

The bottom line is that using one password everywhere is a risk you shouldn't take.

At a minimum, use unique passwords for your important accounts, like banking and other financially-related activities *and email*.

All of your email accounts are important, particularly if they can be used for password re-

(Continued on page 10)

(Continued from page 9) Why Is It Important to Have Different Passwords on Different Accounts?

covery on other accounts. All a hacker needs to do is hack your email account and then run over to some other account and request a password reset to be emailed to the email account they now control.

Managing lots of passwords

Whenever I talk about giving each login a different, strong password, people strongly object. “No way am I going to remember all those passwords, especially if you’re going to insist that they’re complex on top of everything else.”

You don’t have to.

For example, I don’t know my online banking password. Who’s going to remember something like yFK86jk8q45B? (And no, that’s not it. I said something *like* that.)

Yet I use my account frequently.

Let your computer do the remembering for you.

I’m a big fan of password management programs, in particular 1Password.

It creates a secure database of your login IDs and passwords and stores them so that only you can get at them with your single, master password. (And yes, **that** password needs to be strong and memorable.)

Password vaults ease the entire process of logging in by filling in the user ID and password for you; you don’t even need to know what they are.

They use strong encryption to keep your password database secure on your machine(s) and support synchronizing or accessing that database across multiple machines and mobile devices.

And they enable you to use different and strong passwords on every single site.

“Default” apps or programs in Windows

By Jim Cerny, Vice President, Education Chair, and Forums Coordinator
Sarasota Technology Users Group
https://thestug.org/
jimcerny123@gmail.com

Most of us know what “default” means when talking about computers or technology. But in case you forgot, “default” means: “This is what you get until you change it to something else.”

Computer technology is full of defaults (you may have also heard the term “default settings”). The best way to understand this concept is to use an example. Suppose you are writing a document using Microsoft Word (or some other word processor app); you can start typing words in your document immediately without selecting the FONT or FONT SIZE first. That’s because the app has a default font setting (such as “Times New Roman” in the font box and “12” in the font size box). Yes, you can go to those boxes and pick any other font size you want, but the app already starts with something in the box. That’s the default. Other examples in everyday life are thermometers using Fahrenheit, but you can change it to Centigrade, or your speedometer from miles-per-hour to kilometers-per-hour. If you don’t like the default setting, change it to something else.

Let’s go one step further and discuss using that essential Windows app called “File Explorer.” With file explorer, you can find any file on your computer. And when you find the file you want, you can OPEN that file by double-clicking on the file name. Of course, there are many different types of files – photo files, document files, spreadsheet files, and many more. So, when you double-click on a file name in Microsoft File Explorer, Windows uses the DEFAULT app to open that file. Let’s take a photo file as an example. In File Explorer, if I double-click on a photo file (a file type of “.jpg”), it will open the photo in the Windows Photo Viewer app, and I can see the photo. But if I want to open that

(Continued on page 11)

(Continued from page 10) “Default” apps or programs in Windows

photo in a different app, say the Windows Paint app, I have to open that app first and use the app to open the photo file.

It turns out that your Windows computer already has selected specific apps for many file types to use as the default apps. And it’s no surprise that your default apps are Windows or Microsoft apps.

Here is one more example. If you click on a web page link, your computer will open and use the default web browser to go to that web page, probably Microsoft Edge. But you can change your default web browser to Google Chrome, Safari, Firefox, or any other browser you want. To do this, click on the Windows start button in the far bottom left corner of your desktop, type in “Default apps” in the search results, select “Default apps,” and then click on the Web browser to see a list of the web browser apps you have and click on the one you want as your new default browser.

This is how to change ANY default app on your computer to a different one. You can also get to the “default apps” area through your computer “settings” or “control panel.” In addition, you can change the default app used for different file types. It is not difficult to do this. For example, to learn how to use Google search on the internet, enter “How do I change my default app for .jpg file types” or anything else.

The benefit of knowing about default apps is that you will understand why a specific app is used when you click on something to open it. This also explains the question you sometimes get “Select the app you want to use to open this file,” which could mean you may not have an app that can open it. The best way to make sure you use the specific app to open a file is to open the app first and use the app to select the file. Unfortunately, the default is not the default of your computer!

Fixing a Nasty Computer Hack

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

I recently completed a repair on a club member’s computer after he allowed a “helpful” technical representative, probably from the other side of the world, to remotely access his computer. Unfortunately, the victim in this case apparently failed to read or heed my article in the November 2021 *Gigabyte Gazette* (https://www.scscc.club/Gigabyte/gg_2021-11Nov.pdf) warning that these types of scams were becoming increasingly prevalent.

The “bait” in this instance was an official-looking email, supposedly from Cox, stating that the victim had been substantially overcharged on his Cox bill and he was due a refund of $400. The victim telephoned the scammer using the phone number in the email. Next, he went online and downloaded and installed remote access software at her instruction. He then allowed the purported technical representative to initiate a remote access session and log into his system. The victim began to feel uneasy when he saw that things were being done on his computer that had nothing to do with Cox. He finally became alarmed and hung up on the scammer when she asked for his bank account information “to process his refund.”

Unfortunately, this victim did not immediately shut off his computer, so the scammer could continue to mess with his system remotely, I suppose as a departing coup de grace for a failed scam. The victim could no longer access his computer, which displayed the Windows 11 “Gray screen of death” right after he entered his PIN

(Continued on page 12)

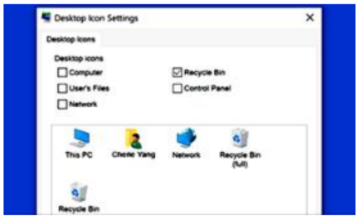
(Continued from page 11) Fixing a Nasty Computer Hack

during login. Microsoft has finally replaced its famous “Blue screen of death,” which provided a bit of mostly useless information, with a “Gray screen of death,” which provides no information.

The victim, who runs an online business, called me in a panic. This was especially interesting to me since I have had minimal experience working with pooched Windows 11 machines. I was curious to see if there was a substantial difference in addressing issues in Windows 11 versus Windows 10 (there was not, at least for this user’s issue).

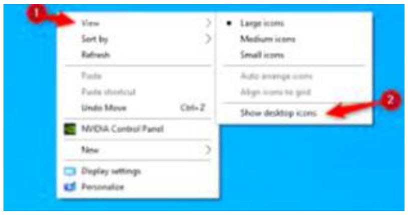
I researched the gray screen issue online and did not find much helpful information. Many writers suggested the problem was bad video drivers or a bad hardware connection. I knew there was no physical issue since the miscreant obviously never had physically assessed the victim’s computer. And I doubted the graphics card drivers were the problem since messing with them would cause an immediate catastrophic system failure, even if it could be done remotely on the fly. After providing answers that did not solve the issue, many sites did offer to sell me their software, which they said would fix the problem. No thanks.

I finally decided to approach the Windows 11 system the way I would Windows 10. Getting past the gray screen of death was straightforward; I booted into Safe mode and repaired the Windows startup. When I finally got into the victim’s computer, I removed the remote access software. Then I did a system refresh, keeping all of his original data files and programs but replacing all of the system files. I wanted to assure the club member that there were no nasty surprises on his system due to his encounter with the scammer.



Desktop icons
□ Computer ☑ Recycle Bin
□ User's Files □ Control Panel
□ Network

Yet when I could finally boot to the victim’s desktop, I saw something very strange. The victim’s desktop icons, files, and folders had disappeared. I considered that the scammer could have put the victim’s computer in tablet mode, which messes up the desktop. I learned that Windows 11 does not have a dedicated tablet mode. Again, an online search for the problem was mostly useless. Most writers suggested going to Personalize themes, Icons and checking the icons I wanted to appear on the desktop. This did not address the issue of nothing showing on the desktop, files, folders, and icons. Naturally, many of those offering useless advice online had a software package to sell, which they assured would fix any problems. Again, no thanks.



I found an article that suggested I right-click on the desktop, left-click on View (#1), then make sure “Show desktop icons” was checked (#2). Yes, that sneaky scammer had hidden everything on the victim’s desktop with three clicks of her mouse. However, when I left mouse clicked on “Show desktop icons,” the victim’s desktop appeared normally. This was the first time I had seen a scammer throw two problems onto a victim’s computer.

When contacted, a scammer will often state that to help you, they must remotely access your system. They will try to get you to download remote access software that will give the scammer access to your computer. Just say NO! There are few legitimate reasons someone needs to access your computer to provide assistance.

I mentally divide computer hacks/scams into two categories: tarantulas and scorpions. Tarantulas are big and scary looking, yet their bite is virtually harmless to humans. The most dangerous scorpions are the tiny ones you are likely not to see until they have stung you, and they can send you to the emergency room or at least to bed for a day or two. The unfortunate victim in this story ran into a scorpion that stung him twice. The sting would have been even worse had he allowed them access to his bank account.

TECH-NO-PHOBIA – are YOU a VICTIM YET?

By Jim Cerny, Education Chair & Forums Coordinator
Sarasota Technology Users Group
https://thestug.org/
jimcerny123@gmail.com

How did all this happen so quickly? Some days I feel like I am left in the dust behind the high-speed train technology. Yes, I am glad technology is progressing. We all benefit from the advances in health care, safety, entertainment, and portability. But there is a downside too. What do you find overwhelming about technology? Let's compare some everyday things from the past to today's latest internet-connected mega-optioned computer-controlled devices.

There were no real "couch potatoes" watching TV in the old days; we got our exercise by having to get up OFF the couch to change the channel or adjust the volume. Today in my living room, I have four device controllers for the TV (the TV itself, the internet TV box, an old DVD player, Apple TV, and a few more I can't identify) – and all of them have dozens of buttons to push. My daily challenge is to figure out which one I should use before I even try to guess which button. Unfortunately, I usually guess wrong the first two times.

The big thing for young kids in the past was being able to read the comics in the Sunday newspaper. Remember Sunday comics in color? My parents would encourage me to read them, and I would pretend I could -- but my mom and dad were so proud I was learning to read at the age of 7 or 8. Today parents shove an iPad or iPhone into their kid's hands to amuse them at one-and-a-half. By age two, the child knows more about the phone than their parents. And by age four, they are answering tech hotline questions.

Learning to drive when I was a teenager was a real adventure. I learned the gas, brake, clutch pedals, gear shift, and the two-gauge dashboard (speedometer and fuel). Radio was a luxury. Today cars have several computers to monitor all the "systems" on the vehicle and, hopefully, keep you safe. And don't forget the ever-bigger TV screen on the dashboard -- it gives you access to thousands of options and a nice view when you back up your car. In a few years, there will be no need for car windows (see predictions later in this article).

Going grocery shopping was fun years ago; there were different stores for different things. You would walk to the downtown or shopping street (before malls) and get meat at the butcher's, bread at the bakery, can goods and cereals at the market, and you had to hope fruits and veggies were available in season somewhere. Today it is all online, even fresh fruit and veggies. The downside is that you get what they deliver. Somehow, I find no enjoyment in ordering food online, where I see only a picture of what I may get.

So, what do you think the future will hold for our children or grandchildren with technology? Will you allow me to make some predictions?

All windows will be replaced with high-resolution TV screens (sort of like Disney's Star Wars hotel). So, you will see what you want or want someone else to see.

Food will be ordered based on your eating history and automatically delivered to you when you need it – even placed into your kitchen pantry or fridge by personalized food delivery services.

There will be no need for germ-spreading handshakes, touching, or personal contact.

All entertainment will be provided for you, including images for your sight, ears, nose, and nerve sensations by technology directly to your brain.

And shortly after all this, computers and robots will take over the world, and we will no longer be needed. So, I recommend we enjoy the technology we have while we can.