Bits of Bytes

Newsletter of the Pikes Peak Computer Application Society, Colorado Springs, CO

Volume XXXVIII | May 2018 | Issue 5

The Prez Sez

by Toni Logan, President, P*PCompAS

I wasn't able to attend last month's meeting because I got a bug, but hope it was a good meeting. Next month Cary Quinn will have an interesting program for us. The breakfast meeting group this month was a cozy one, since we had a pretty good snowfall during the night. It was nice to get out and have some lively conversation with others.

A reminder for all that **the next meeting will be held on the second Saturday of May instead of the first.** The church has asked us to move the meeting to accommodate their schedule. The breakfast in May will still be on the third Saturday as usual. Keep warm and see you in May. ☺

Next P*PCompAS meeting: Saturday, *12 May* 2018
Note that we are meeting the second Saturday of the month in May.
No topic has been announced.

Meeting Minutes

by Pat Krieger, Secretary, P*PCompAS

The 7 April 2018 membership meeting was attended by only 14 members because of inclement weather. Cary Quinn took over the role of chairing the meeting because president Toni Logan was unable to attend.

OFFICERS REPORT

Treasurer Bill Gardner reported we have a total of $4181.91 in our treasury after a purchase of $1157.91 for a new computer, and necessary additions, such as a cable. The computer was purchased locally and comes with a one-year warranty. Thanks to Joe Nuvolini for his part in acquiring this for our club. We are donating our former computer to the church. The computer, an Acer, is in excellent condition because it has had very little use.

OLD BUSINESS

Joe Nuvolini told us the specs of the new computer.

We need a new coffee pot. Dave has offered to buy it.

ANNOUNCEMENTS

Reminder to all members: Our May meeting will be 12 May because of a conflict with the schedule of the church.

We received the sad news of the death of member Jim Way.

AROUND THE ROOM

John Pearce said a Windows 10 update will be released this month.

Bill Gardner and others talked about difficulties with Malwarebytes. The consensus was to delete it (some said difficult to do) and reinstall.

Jim Miller asked for advice on how to transfer application and data files from one computer to another. Suggestions included copying data to CDs, or backing up to an external hard drive, or the cloud and installing from those sources. Or using Windows 10 Migration (ask Cary for more information on that.)

If a computer is off, it can still be in sleep mode, which has some advantages. If interested in this, bring it up at the next meeting for a better explanation than I was able to write down.

PROGRAM

Our program this meeting was excellent, and it's a shame so many members missed it. Cary provided videos that had much information, first some for more advanced computer users, and a second one loaded for information for those of us with less training. This second one would be a help to any computer user. I wish there was an accompanying book available, for this video contained so very much information that it would be helpful to have it in a reference that can be referred to when needed.

Continued on page 2

In This Issue

Articles

P*PCompAS

Officers

President: Toni Logan
bradtonilogan@gmail.com

Vice President: Cary Quinn
cary.quinn@gmail.com

Secretary: Pat Krieger
pkrieger@centurylink.net

Treasurer: Bill Gardner
wgplace@comcast.net

Staff

APCUG Rep/Webmaster: Joe Nuvolini
Barista: David George
Drawings: Bob Logan
Editor: Greg Lenihan
Librarian: Paul Godfrey
Membership: Ann Titus

Committees

Audio: A.J. Whelen
Hospitality: Pat Krieger
Programs: Cary Quinn
Publicity: Cary Quinn
Nominating: Gene Bagenstos

Board of Directors

John Pearce
Joe Nuvolini
Peter Rallis
Paul Godfrey
Ann Titus

Meeting Minutes (Continued from page 1)

Many sources of help were included. Three books were recommended: Is This Thing Turned On? by Abby Stokes, Computer Buyers Absolute Buy Guide, and Seniors Computers for Dummies.

Also Kim Komando, "How to Geek", Lynda.com (free library source), PC Magazine, PC World, manufacturers tutorials, gcflearnfree.org, which are YouTube computer-related videos, the "Help" functions built into your computer (good luck with those), Tech Boomers—free videos and some written presentations, Chrome browser—go to index box to get a menu, Customer Service of manufacturers, and more. ☺

Cary preparing for the April presentation.

In Memoriam: Jim Way
Lt. Col., USAF (Ret)
August 7, 1930 - April 4, 2018

Jim was a long time member of our group who also held office. He had two degrees in chemical engineering so you know where he got the inherent desire to join a computer club. Jim flew several types of jet aircraft during his 22 years in the Air Force and was married to Becky, his wife for 62 years.

Our society expresses sympathy and condolences to his family. ☺

Tip: Virtual Desktop

Did you know you there's an icon on your desktop to see called Task View? It's the little rectangular box to the right of your "Type here" taskbar.

Click on it to see all the windows you have open. Or click on New Desktop to create a new workspace without closing the windows you have open. ☺

Tip: Task Scheduler

Task Scheduler helps you schedule tasks on your computer, like turning it off at a specific time each day. Type "task scheduler" into your taskbar to get started. ☺

5 Quick Fixes for a Finicky Computer

by Kim Komando at Komando.com (tip from 4/21/18)

Computers live by Murphy's Law: "Whatever can go wrong, will go wrong." Which is why, at some point, your computer will freeze, or flicker, or even shut down. Most of us are comfortable using computers as long as everything is going smoothly.

Maybe your old computer is just running slowly. Click here for 9 ways make an old PC run faster.

Below are five common computer problems that you can usually solve yourself. Computers have many moving parts, and you may eventually decide to call in reinforcements. But with a little direction, you may be able to fix minor issues all on your own.

1. Unexpected reboots

—Windows—

Troubleshoot an unexpected reboot with a program called WhoCrashed. It scans your computer to identify the problem, and it may suggest a solution. According to WhoCrashed, the problem may not have anything to do with hardware; instead may be related to its device drivers. Or it may be a problem with pieces of coding called kernel modules.

One caveat: WhoCrashed states that "the software is not guaranteed to identify the culprit in every scenario," so if the problem persists, you should consult a professional.

—Mac—

Mac users have another option: you can find a folder under ~/Library/Logs/DiagnosticReports/ which will have detailed reports of application crashes and hardware issues.

2. Basic software troubleshooting

A recurring freeze could be the result of a buggy program. Windows users can try the keyboard shortcut CTRL + SHIFT + ESC to open Windows' Task Manager and then select the Performance tab. In Windows 8.1 and 10, you might need to click the More details link at the bottom of the Task Manager to see it. Click here for more Task Manager tricks that you should know.

—Windows—

1. Start using your computer as normal, but keep an eye on the CPU, memory and disk categories.
2. If the computer freezes, and one of these shows an unusually high number, then that could be your answer. Make a note of which area was really high then restart the computer and open Task Manager again.
3. This time, however, choose the "Processes" tab. Sort the list by CPU, memory or disk, whichever was really high last time the computer froze, and see what process pops up to the top of the list as the computer freezes. This should tell you what software is acting up so you can uninstall or update it.

Click here to learn how to unravel what processes tell you about your programs.

Continued on page 4

There was snow on the ground, but that did not dampen the spirits or appetites of the digerati that attended the April breakfast on the third Saturday. In fact, the good fellowship and food made it all that much better. Rain or shine, join the club at the Country Buffet next month.

Finicky Computer (Continued from page 3)

You might also have hidden software, such as a virus, causing problems. Be sure to run a scan with your security software to uncover something that shouldn't be there.

—Mac—

To view open processes and computer resources usage, use the Activity Monitor. The quickest way to access the Activity Monitor is by using Spotlight Search. Click the magnifying glass on the right side of the menu bar at the top of your screen, or press Command + Spacebar to open a Spotlight window and start typing the first few letters to auto-complete Activity Monitor. Just press enter to access the tool.

Another way of accessing the Activity Monitor is through the Launchpad. The Activity Monitor is in the Other folder. Optionally, you could then drag its icon to the dock for easy access in the future.

3. Basic hardware troubleshooting

Maybe your computer freezes in both normal mode and Safe Mode. This may be a problem with your computer's hardware – your hard drive, an overheating CPU, bad memory, or a failing power supply. In some cases, it might also be your motherboard, although that's a rare occurrence.

Usually, with a hardware problem, the freezing will start out sporadically, but increase in frequency as time goes on. Or it will trigger when the computer is working hard, but not when you're doing more basic things. Fortunately, you can run some checks and see if that's the case.

—Windows—

Use a program like CrystalDiskInfo to check your hard drive's S.M.A.R.T. data for signs of impending failure. A program like SpeedFan can tell you if your computer processor is overheating, or if the voltages are fluctuating, which might be a problematic power supply.

If you want to go more in-depth, you can grab a diagnostic CD like FalconFour's Ultimate Boot CD. It has plenty of other tools for checking out your computer, including MemTest for putting a strain on your computer's RAM to see if it's working OK.

If your computer is newer, it might still be under warranty, in which case you'll want to contact the manufacturer or seller.

For an older computer, you need to decide if it's less expensive to repair or replace it. Click here to find out at what point you should just cut your losses.

—Mac—

Apple has two built-in programs, Apple Hardware Test (for Macs built in 2012 or earlier), and Apple Diagnostic (for Macs released in 2013 or later).

To access either program, disconnect all external devices and close all your windows. Then go to Apple Menu >> Restart, then hold down the D key. This will automatically fire up Apple Diagnostics, which will analyze your computer and present a report.

4. Pop-up ads and odd messages

Running into a pop-up ad while you're surfing used to be a serious annoyance, but modern browsers include pop-up protection to prevent the clutter. If you still see regular pop-ups on more than one site, it could be a badly configured browser.

Then again, if pop-ups are coming at you when your browser isn't even open, you may have a virus. This is especially true if the pop-ups advertise some magic cure-all to your "virus woes."

—Windows—

If you are bombarded with pop-up ads, first run a scan with anti-spyware software to double-check. Try SpyBot Search & Destroy because it digs deep into your settings to find any problems spyware has left behind.

Keep an eye on your email's "sent" folder and on your social network posts. If you notice emails and posts that you don't remember sending or posting, it's likely that you have a virus.

—Mac—

Apple's macOS has long been touted as the virus-resistant operating system, but it's not invulnerable, and Apple-targeting viruses are becoming far more common. Try Malwarebytes for Mac, a popular malware removal tool which is comparable to SpyBot Search & Destroy.

5. Getting things going again

The oldest advice is sometimes the best: if you want to get your computer back on track, try restarting it.

Remember, though, if your computer freezes, you won't be able to restart the computer using the on-screen menu. Instead, you'll have to press down the power button and hold it until your computer shuts off. This is sometimes referred to as a "Hard Reboot," and although it's not ideal, it is essentially the same thing as restarting.

Another thing you can do that's easy is clearing out your browser's cache. This won't fix every problem, but it does help by giving you a blank canvas to work with.

The process is very easy. Every browser has a different method, but here's how you can do it in Chrome. Go into your browsing history, then click the button at the top that says, "Clear browsing data."

Of course, if these simple fixes don't help, then you might have a bigger problem to worry about. Maybe you just need to buy a new computer. Click here to erase data for good stored on the hard drive. ☺

What Happens When I Die?

By Leo Notenboom, https://newsletter.askleo.com; published under the Creative Commons License

If you're not around to unlock all the digital data you take such care to secure, who will be able to access it, and how?

Making technology both convenient and secure is a problem we deal with daily. We make trade-offs and use techniques that we hope strike an appropriate balance.

A more difficult dilemma that we rarely think about, however, is death. If something were to happen to you, would the people you leave behind be able to access the information they need? What happens to your encrypted data, online accounts, social media, online finances, pictures, and digital-whatever-else if for some reason you're not around or able to access it?

I hear regularly from people frantically trying to access important, sentimental, or critical data that a recently deceased or incapacitated friend or family member has locked up tightly.

It's not particularly pleasant to think about, but with all the security measures we put into place to keep bad people out, it's worth having a plan for letting the good people in.

Left behind

The wife of a military member killed overseas wanted access to her husband's email account to retrieve critical information, as well as get a glimpse into the last days of his life. The service was a free email account with no customer support. There was nothing I could do to help.

The children of an elderly gentleman needed to access his password-protected computer to retrieve the only copies of some very important family pictures. Fortunately, there are ways to break into many (though not all) Windows machines, if you have physical access.

These are just two examples of scenarios I hear regularly. Sometimes I can help. More often I cannot.

These are also scenarios I worry about myself. I have a large amount of encrypted data, and do many things online that require secure access. If something were to happen to me, what would my wife do?

At odds with security

This kind of disaster planning is at direct odds with the conventional wisdom that says "never share your password with anyone." Yet that's exactly what you must do in case something were to happen.

It's not an easy scenario to solve, and not all solutions work for every person…

… but solve it you must.

It's critical for those of us who would leave behind a confusing, encrypted, password-protected digital mess to ensure that the right people are able to access and make sense of it all.

Who do you trust?

As with so many things, it boils down to trust. Who do you trust?

And are you certain that, trusting them today, you will still trust them a year from now? Five years from now? Twenty years from now? How many friendships, relationships, and even marriages last that long?

Fortunately, you don't have to commit to twenty years of trust. Set up properly, a timely password change or two can protect you when trust is lost. But the fact that trust can be lost must be built into the system.

Whenever the answer to "do I trust them this much?" changes, it's time to take action to protect yourself, and then find a new trustee.

It's not always easy, but it is important.

What do you trust them with?

Once you have someone you trust, what is it, exactly, you give them?

On one hand, you don't want it to be every single password to every possible account or encrypted thing you have. It's a maintenance nightmare, as you'd have to update your friend every time you add or change a password, without fail. Chances are you won't, and the passwords held by your friend would quickly end up out of date.

You *definitely* don't want to use a single

Continued on page 6

When I Die (Continued from page 5)

password everywhere. While easier to maintain with your trusted friend, it would also make it easier for a hacker to *instantly* have access to *everything,* should that password ever leak out.

The ideal solution is to give them access to exactly one thing – one account or one encrypted file – in which you either automatically or periodically keep your information up-to-date.

One approach: Lastpass

Using a password manager such as Lastpass can help in a disaster situation.

You keep information in your Lastpass vault up-to-date simply by using it. You can even add secure notes to Lastpass for items that aren't covered by its online log-in-focused database.

All you need share with your friend is your Lastpass master login ID and password. The only time you would need to update this is if either of those two things changes. Should you ever lose trust … simply change the password.

That's it. When disaster strikes, your trusted contact has access to *any* of your online accounts maintained in Lastpass.

Another approach: explicit encryption

In the past, my approach to disaster access used explicit encryption in the form of a TrueCrypt volume I used every day.

Anything important was stored inside the encrypted container. Once again, simply mounting and using it – which was a side effect of simply using the computer – naturally kept the contents up to date.

All I needed to share with my trusted friend was the location of the container, and the passphrase to open it up. Once inside, everything was there, including files containing additional instructions. And once again, should trust be lost … simply change the passphrase.

There are a variety of encryption tools that work well in this scenario, including TrueCrypt, VeraCrypt, AxCrypt, BoxCryptor, and others.

How do you trust them with it?

Simply giving someone complete access to your password manager, or your entire collection of personal files, can feel scary – and rightfully so. It's not something to do lightly.

To be honest, if you're not sure a specific individual can be trusted with the information, it's likely they shouldn't be. You want someone that you can really trust.

One way I've found that helps just a little is to provide that critical information on paper in a sealed envelope. The implication is that you could ask for the envelope back, and, seeing it still sealed, know your trust was not misplaced.

Two-man variation

A variation of this approach is to use what's called a "two man rule." With this approach, you never give a single person your complete password, but instead select two (or more) individuals, and give each of them a portion of it. Only when they are in agreement can they assemble the pieces and gain access.

A lengthy password (or a pass*phrase)* is ideal for this, as long as the phrase is nonsensical. You should not be able to guess a missing piece of the phrase with only the portion you've been given. "Correct horse battery staple" is a good example of this, since – aside from its notoriety as an example passphrase – the words are completely unrelated to one another.

A little documentation and a lot of trust

It all boils down to a little documentation and perhaps a couple of simple additions to your existing routine. You should already be making sure that your data, passwords, and identity are secure. Chances are, building in a secure mechanism for disaster recovery isn't going to be all that difficult.

Trusting the right person should be the part requiring the most thought. The rest is, essentially, just paperwork.

Responsibilities of "the keeper of technology"

My view is that as the "keeper of the technology" for your family or business, you have a responsibility to make sure that if something happens, they're protected.

Your needs might be different. Your solutions might be different. A CD in a safety deposit box might be enough. Perhaps keeping certain information with a family lawyer is right for you.

Or perhaps the password-sharing approach I've outlined above works for you.

But most important of all is to simply realize what not to do.

Don't leave your family, friends, or business without access to the information they might need should you not be available.

That could elevate a tragedy into an even worse disaster. ☺

Why Does Every Camera Put Photos in a DCIM Folder?

By Chris Hoffman, reprinted with permission from HowToGeek.com

Original article at: https://www.howtogeek.com/204228/why-does-every-camera-put-photos-in-a-dcim-folder/

Every camera — whether it's a dedicated digital camera or the Camera app on Android or iPhone — places the photos you take in a DCIM folder. DCIM stands for "Digital Camera Images."

The DCIM folder and its layout come from DCF, a standard created back in 2003. DCF is so valuable because it provides a standard layout.

Meet DCF, or "Design rule for Camera File system"

RELATED: Why Do Removable Drives Still Use FAT32 Instead of NTFS?

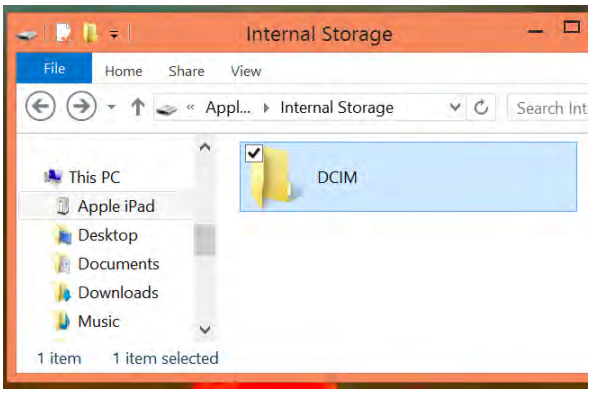
DCF is a specification created by JEITA, the Japan Electronics and Information Technology Industries Association. It's technically standard CP-3461, and you can dig up the arcane standards document and read it online. The first version of this standard was issued in 2003, and it was last updated in 2010.

The DCF specification lists many different requirements with a goal to guarantee interoperability. The file system of an appropriately formatted devics — for example, an SD card plugged into a digital camera — must be FAT12, FAT16, FAT32, or exFAT. Media with 2 GB or larger of space must be formatted with FAT32 or exFAT. The goal is for digital cameras and their memory cards to be compatible with each other.

The DCIM Directory and Its Subfolders

Among other things, the DCF specification mandates that a digital camera must store its photos in a "DCIM"directory. DCIM stands for "Digital Camera Images."

The DCIM directory can — and usually does — contain multiple subdirectories. The subdirectories each consist of a unique three-digit number — from 100 to 999 — and five alphanumeric characters. The alphanumeric characters aren't important, and each camera maker is free to choose their own. For example, Apple is lucky enough to have a five-digit name, so their code is APPLE. On an iPhone, the DCIM directory contains folders like "100APPLE," "101APPLE," and so on.

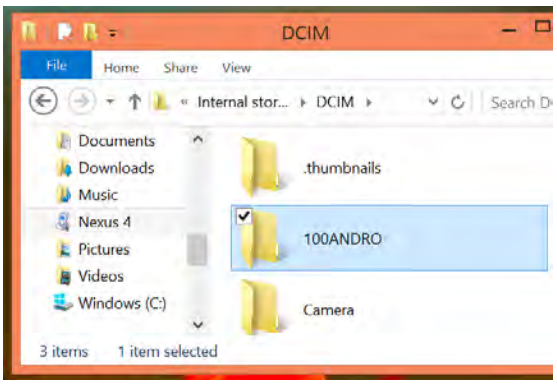


Inside each subdirectory are the image files themselves, which represent the photos you take. Each image file's name starts with a four-digit alphanumberic code — which can be anything the camera maker wants — followed by a four-digit number. For example, you'll often see files named DSC_0001.jpg, DSC_0002.jpg, and so on. The code doesn't really matter, but it's consistent to ensure the photos you take are displayed in the order you took them.

For example, the layout will look something like:

DCIM

- 100ANDRO
  - DCF_0001.JPG
  - DCF_0002.JPG
  - DCF_0003.WAV
- 101ANDRO
- 102ANDRO



Continued on page 8

DCIM Folder (Continued from page 7)

You may also see .THM files that represent the metadata for files other than JPG images. For example, let's say you took a video with your digital camera and it was stored as a .MP4 file. You'll see a DSC_0001.MP4 file and a DSC_0001.THM file. The MP4 file is the video itself, while the .THM file contains a thumbnail and other metadata. This is used by the camera to display information about the video without loading it.

There are more arcane details here that the DCF specification requires, but they're not really important.

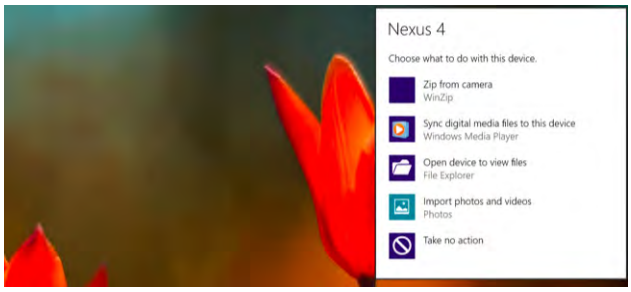
So Why Does Everyone Follow This Specification?

RELATED: How to Buy an SD Card: Speed Classes, Sizes, and Capacities Explained

DCF is a "de facto" standard, which means that enough digital camera and smartphone makers have adopted it that it's become a consistent standard in the real world. The standardized DCIM format means digital camera picture-transfer software can automatically identify photos on a digital camera or SD card when you connect it to your computer, transferring them over.

The DCIM folders on smartphones serve the same purpose. When you connect an iPhone or Android phone to your computer, the computer or photo-library software can notice the DCIM folder, notice there are photos that can be transferred, and offer to do this automatically.

DCIM may not be the most obvious name the first time you see it — how about "Photos"? — but it's more important that it's a standard. If every digital



camera manufacturer or smartphone operating system had its own unique pictures folder, software programs wouldn't always be able to automatically find photos on a connected device. You wouldn't be able to take an SD card from one camera and plug it directly into another digital camera, accessing the photos without reformatting the device or rearranging the file system.

Ultimately, just having a standard is important—whatever the standard is. That's why the DCIM folder has followed us from point-and-shoot cameras to smartphone and even tablet camera apps. The Picture Transfer Protocol, or PTP, isn't the same as the DCF standard, but it serves a similar purpose. It's been superseded by MTP and other standards, but PTP is supported by Android devices and iPhones for communicating with photo-management applications that support this standard.

As usual, we're all carrying an old-and-arcane standard forward because it's better to be compatible with everything than design something new from scratch. That's the same reason why email is still so popular! ☺

I Wuz Hacked

By Stu Gershon, Sun City Summerlin Computer Club, NV., Gigabyte Gazette, www.scscc.club/, www.scscc.club/, tomburt89134 (at) cox.net

One Sunday morning, I checked my email, like I do every morning. Nothing came through. I tried again, and it was the same. I called COX to see if any of their servers were having trouble or down. The line was busy. The line is never busy unless they are having trouble because they've always had fantastic customer service. I tried twice more during the day with the same results.

I finally got through to COX at about 6:30 that evening. They were not having any problems, and they couldn't help me because I have Gmail accounts and they would only intervene if they were COX accounts. I said to the technician, "What should I do?" He replied, "Call Google!" I said, "Who are you going to call at Google, they have no customer service!" He offered, "I have a number for Google support!"

He gave me the number and the first thing Monday morning I called 1-844-400-1570. I asked if they were "Google Support" and the gentleman said "Yes." His name was Daniel. We discussed the problem and he said I'd have to let him into my computer, so he could check. REMEMBER - COX gave me this number. I had to give permission and put in a code number to let him into my computer. He looked around for a while, "scanned" my computer for viruses and malware and told me I had probably been "hacked." I asked, "What do we do now?" Daniel said he'd fix it and said the charge would be $299.99 including a one-year warranty on my computer. I figured it was worth

Continued on page 9

I Wuz Hacked (Cont. from page 8)

it to get this problem fixed.

He continued to work on my computer, while I watched what he did, and we talked over the phone, throughout. He worked on my computer until 5:30 pm (from 9:30 am) and said he did what he could, the email was working with some "work-a-rounds," but it was the end of his shift and he'd call me back at 10 am the next morning.

He asked to be paid, and since my computer was adequately working and he'd been working on it for 8 hours, already, I gave him my credit card and paid the $299.99.

The next morning, at 10 am, he called back and worked on it until almost noon. He's put ten hours into my computer, he had given me his name, and said he'd call back the following week to check if everything was alright. With Daniel's "work-a-round," my computer worked fine.

On Tuesday, September 12th, he called back promptly at 10 am, said "hello" and asked how everything was working. I told him it was working fine, but by adding the "work-a-round" (a new email address getting the email from the old one), I was getting a lot of duplicate emails. He took another look, but this time he used a different software.

Since Gigabyte Gazette on 18 December 2017 we were still in communication over the phone, I asked "why?" and he replied, "My company has installed a new software in the past week."

The guy had already worked on my computer for TWELVE HOURS and, remember, I CALLED HIM! He said, "Look, you've been hacked, so I'm going to refund your money because we didn't do our job!"

He said, "Let me be sure." Then my PC's screen went BLACK! I asked, "Daniel, what's going on?" He replied, "It's the new software, don't worry." Coincidently, my cell phone was right next to my

computer. As the screen was black and I couldn't see what he was doing, I received text messages on my cell phone, "PayPal Gift Card - $100!" "PayPal Gift Card - $50!" On and on. I asked Daniel, "What's going on?"

He answered, "Nothing, I'm fixing your computer!" I answered, "Money is being taken from PayPal!" He replied "Don't worry! It's so we can give you your refund!"

I said, "Not from what I see! Goodbye!" and I pulled the plug! I immediately called PayPal, and stopped the $450 in Gift Card charges! Then I called my Bank and put a freeze on all my credit cards. Remember, Equifax had been hacked the week before, so they were NO HELP!

Then I called Amazon, where I spend much of my money. They informed me they had "denied" a charge for a $500 gift card (because I had never ordered something like that before, and they were trying to contact me to verify, but my computer and two phones were all in use – it's called "profiling".)

I called my friend, Chuck, at the Computer Club and he told me to bring my computer over (the Tuesday Repair SIG – Special Interest Group, had just started). I brought it over and when the guys started up my computer it required a password (which I had not made) to enter.

This is called RANSOMEWARE – They lock up or scramble your computer and make you pay a fee to release your computer from their control! Chuck, and the other guys, took out the hard drive, did something to it to remove the password, and then I got my external hard drive and we restored the computer to BEFORE this incident began.

In the meantime, Daniel called five times and told me to buy three $100 iTunes gift cards, and when I put in the pin numbers from the back of each card, the "hack-ware" would be uninstalled! He had already taken $299.99 in payment for his services, tried to buy $450 in PayPal gift cards, tried to purchase a $500 gift card from Amazon, and now he wanted $300 more? Nope! So now, two weeks later, I've restored my main computer, the email is working fine, I'm currently restoring my second laptop because I also allowed Daniel to check those email settings. I've changed all my credit cards and my passwords and I'm exhausted. I haven't lost any of the "charges" yet, because they are all in "dispute," and because PayPal, Amazon and my bank worked quickly, and I'm disputing the initial charge of $299.99.

If that's the price I must pay, "A lesson learned, is a lesson earned!" and maybe someone can benefit from this experience. REMEMBER – I called Daniel because my trusted Internet Provider GAVE ME THE PHONE NUMBER!

The only people SCSCC members should let into their computers are our Computer Club's Repair SIG which meets every Tuesday from 1 to 4 pm in the Computer Club Classroom at the Pinnacle, and the only requirement is joining the Computer Club! They know what they are doing, and they live HERE!" ☺

P*PCompAS Newsletter
Greg Lenihan, Editor
4905 Ramblewood Drive
Colorado Springs, CO 80920
e-mail: glenihan@comcast.net

Coming Events:
Next Membership Meeting: 12 May beginning at 9 am (see directions below)
Next Breakfast Meeting: 19 May @ 8 am, Country Buffet, 801 N. Academy Blvd.
Newsletter Deadline: 19 May
Check out our Web page at: http://ppcompas.apcug.org