The Gigabyte Gazette

The Monthly Newsletter

of the

Sun City Summerlin

Computer Club

https://www.scscc.club

June, 2021

Table of Contents

Issue Contributors

Tom Burt **Peggy Cushman**

Kathy Kirby **David Kretchmar**

Jeff Wilkinson **John Krout**

President's Message

Don't Let Your Identity be Compromised!

by Jeff Wilkinson

We should all be cautious answering those seemingly innocuous questions posted on social media sites such as "*What Year Did You Graduate High School*", or "*What City were you Born in*", "*Can you remember your childhood phone number*?" or "*Who was your first-grade teacher*?", and on and on. These interesting questions appear harmless and appealing as you develop friendships and reminisce with old and new friends on social media, but beware! Many of these answers can be used to answer or reveal answers to security questions that you chose when you setup accounts at your bank, utility company, etc. When you forget your password, as happens all too often, you will be asked to answer security questions from when you originally setup your account, in most cases some time ago! Answers to these types of questions posted on social media or quizzes can be used to build a profile on you with the information needed to open a new account!

Where did you grow up: STOP
Favorite color: GIVING
First pet's name: PEOPLE
Street you grew up on: YOUR
Favorite Childs Name: PERSONAL
Favorite sports team: INFO
High school mascot: TO
Favorite food: GUESS
What was your first car: YOUR
Moms name before she married: PASSWORD
First job: AND
Favorite band: SECURITY
Favorite food: QUESTIONS

Keeping your identity secure on social media is essential to your financial and personal safety. Identity theft is evolving with thief's making use of the latest technology to move from credit card counterfeiting to checking and savings account takeover. A May 2020 study by Javelin Strategy and Research found account takeovers — identity theft where a criminal gains unauthorized access to an online account belonging to somebody else — are trending at the high loss rate, up a staggering 72 percent over the prior year.

Remember that when you first create a social media account you provide personal information such as name, age, email address etc. And I venture to guess that most of us have never read the small print terms of service provided by the host. As you traverse the various pages, forums, postings etc., data mining creates a profile of your behavior, your likes and dislikes and this information is often monetized by the host sites you visit, meaning sold to third parties. Facebook collects data from all devices you have installed their app on and it can include such things as your device location, your data provider or internet service provider the language used and time zone. Data on sites you like or visit via a link on Facebook is also collected.

What can the consumer do to protect themselves?

- Keep your software up to date
- Log out of social media sites when finished, particularly when in a public location or using a public computer
- Use two-factor authentication wherever possible.
- Used strong passwords - keep track of them with a password manager

- Use a screen lock on portable devices
- Don't conduct business or share critical information on public Wi-Fi
- Put a credit freeze on your accounts with credit bureaus.
  Equifax, Experian, Innovis, TransUnion
- Protect your social security number – only give it out when absolutely necessary
- Be aware of billing cycles – if financial information is late or doesn't come, follow up
- Be cautious of participating in viral memes such as "name you most memorable concert"
- Set strict privacy settings on Facebook, Twitter, Pinterest, Instagram, and LinkedIn

If you are a victim of identity theft, report it to the FTC online and create an account to create a report and generate a recovery plan. You will gain access to recovery plan updates and prefilled form letters to send to creditors. You should also report medical identity theft to Medicare's fraud office and tax identity theft to the IRS.

It should be clear that this is something you want to avoid so a little awareness and preventative steps taken can help avoid some potential serious problems.

Let's be careful out there …

Jeff Wilkinson, President
(702) 527-4056 ***pres.scscc@gmail.com***

General Membership Meeting

There will be no General Meetings in June, July or August. Our next General Meeting will be held at **2 PM on Thursday, September 2nd**.

For Club information: go to www.scscc.club, contact Jeff Wilkinson, President at (702) 527-4056 or email him at pres.scscc@gmail.com.

June 2021 Printable Calendars

To view this month's classroom and lab calendars, click the following hyperlink:

http://www.scscc.club/Calendars/scscc_calendar_2021-06Jun.pdf

SCSCC Board of Directors Actions

The Computer Club Board of Directors took the following actions on May 12, 2021

Chuck Wolff made a motion that the **minutes of the April 14, 2021 Board Meeting be approved as submitted.** The motion was seconded by George Lobue and unanimously approved by the Board

Chuck Hagen made a **motion** that the meeting adjourn. Howard Verne **seconded** the motion, and it was unanimously **approved** by the Board. The meeting was adjourned at 9:45 AM.

Submissions Welcome

We are always looking for new information to share with our club members. If you have computer or technical information you would like to share with members of the club, send your articles to editor **Tom Burt** at tomburt89134@cox.net. Thank you to everyone for your contributions.

Welcome New Members

The following new members have joined the Computer Club from April 28th to May 27th.

Lorin Cary	**John Meola**
Cheryl Connole	**Jose Perez**
Sandra Krause	**Duke Sims**

As of May 27th, the club has 492 paid memberships for 2021.

As of December 31st, the club had 614 paid memberships for 2020.

Special Interest Groups and Kaffee Klatches

Currently, all seminars, SIGs and Q&As are being conducted as Zoom webcasts. Unless explicitly stated, advance registration is not required for SIG sessions.

Special Interest Groups (SIGs) provide a forum for general discussion on a specific computer related subject. Admission to all SIGs is on a first-come, first-seated basis and is subject to the maximum allowed by fire code regulations. <W>, <L>, <M> or <H> indicate whether a SIG would be of interest to a Windows, Linux, MacOS or Hand-held Device user.

Apple SIG / Q&A <M/H> via Zoom Gail Weiss (702-355-6220)

3rd Monday, 10 a.m.
DARK in June.

Bring your Apple iPhone, iPad, Watch or MacBook to get one on one help with your questions about how to use any Apple device and popular iOS or MacOS apps.

Repair SIG <W/L/M > Chuck Wolff (702-233-6634) and Chuck Hagen (702-418-2614)

Live in the Classroom. ***Reservation Required***

Every Tuesday, 12:30 p.m. to 3:30 p.m.

The Repair Lab provides **CLUB MEMBERS ONLY** with no-cost assistance for those having upgrades and / or hardware and software problems with their computers. Bring in only your PC tower, your Mac or your laptop and your problems. Our TECH team will give you our best effort. ***Be sure to mark your cables so you can re-connect when you get home***.

Internet Investing <W/M/H> via Zoom Tom Burt (702-341-7095)

3rd Thursday, 9:00 a.m. in even months

Next meeting: June 17th

The Internet Investing SIG provides a forum for members interested in using Internet resources for researching and managing investments to meet, discuss, and learn more about the topic. The SIG's target audience is members with intermediate computer skills and investment experience, but all members are welcome.

Networking SIG <W/M/H> via Zoom

2nd Thursday of odd months at 9 a.m.
Robert Ambrose (rna@muttsoft.com)
DARK indefinitely.

This SIG is a discussion forum on computer network technology including modems, routers, firewalls, protocols and ISPs.

Kaffee Klatch <W/M/H> via Zoom

Every Tuesday, 8:30 a.m.
Jeff Wilkinson (702-527-4056)

This Kaffee Klatch is an open, free-form discussion group for all users, from beginning to advanced. KK discussions are not restricted to any one subject, computer platform or computer-knowledge level but should be computer or technology related. We will try to answer your questions, help you keep your systems updated and provide some useful "tips and tricks."

Windows 10 SIG In-person

First and Third Saturdays at 9:30 a.m. *Next meetings: June 5 and June 19*
Bill Wilkinson (702-233-4977)

If you are a novice or near-beginner computer user, or if you just want some refresher information together with a refreshing cup of coffee, then jump-start or recharge your computing knowledge by attending these Win 10 SIG / Q&A sessions. At each session, attendees will explore several topics of interest to beginners and near-beginners. The topics are always announced a couple of days in advance via e-mail to SCSCC members who have subscribed to the club's SCSCCNews mailing list. Each topic is presented in a step-by-step manner and is supported by "how to" notes that can be easily and conveniently downloaded from the SCSCCBKK.org web page. Following each "up front" presentation of one or more topics (approximately 60 minutes in duration), an informal open-ended Question and Answer period takes place for those who wish to participate, listen, reflect, or inquire.

Seminar Offerings

Currently, all Seminars, SIGs, Q&As and Kaffee Klatches are being conducted as Zoom webcasts. Unless explicitly stated, advance registration is not required for Seminar sessions.

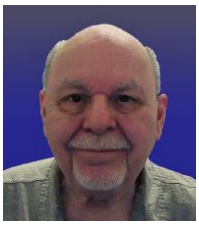
Introduction to LibreOffice 7

Thursday, June 30th 9:30 AM – 11:00 AM *via Zoom*
Presenter: Tom Burt
Location: Zoom Webcast

LibreOffice 7 is the latest version of a comprehensive suite of office programs, including a word processor, spreadsheet, presentation graphics, drawing tool, math tool, charting tool and database manager. LibreOffice (a descendent of Star Office and Open Office) is a FREE, open-source software package from The Document Foundation. It can load and save documents in Microsoft Office format with very high fidelity. There are full versions for Windows, Linux, MacOS, iOS and Android.

This 1½ - hour seminar will provide an overview of the entire LibreOffice 7 suite and then will look in more depth at the Writer word processor and the Calc spreadsheet. Included will be a walk-through of the steps to download and install the suite. We'll also edit some Word documents and Excel spreadsheets to illustrate compatibility.

The latest presentation notes will be available about June 24th at: http://www.scscc.club/smnr.



Tom's Tech-Notes

Credit Card Fraud

A Personal Experience

Mrs. Burt and I recently experienced an unusual form of credit card fraud. There were various ramifications, and it took us about 4 weeks to completely resolve the issue with the credit card company. I'll share the story and then discuss some of the implications and steps you can take to help prevent having a similar experience.

Strange ATM Withdrawals

Mrs. Burt regularly checks our various credit card accounts online to watch for fraudulent transactions. On one of our cards, she noticed some ATM cash advance transactions that occurred in a small town in Iowa. In all there were three such that had occurred within a day of each other.

We called the credit card company immediately to report the transactions as fraudulent. The service rep cancelled the current card number and arranged to send us new cards. So far, so good. In discussions with the service rep, she suggested we set up a PIN number on the new cards so that only someone who knew the PIN could do ATM cash advances.

An Illegitimate Extra User

Two days later, after we had received and activated the new cards, Mrs. Burt logged in to the online website account for that credit card to set up the PIN. When she selected that option, the website asked "For which authorized user? And displayed a list which had her name, my name and a *third name of someone who lived in Iowa*. This provided the missing link as to how someone in Iowa had been able to do an ATM cash withdrawal against our credit card. When they issued us new cards, they carried this illegitimate user over to the new card (and probably sent him a new card as well!).

We called the credit card company again, explained the issue and got connected to service rep in the security and fraud division. She deleted the unauthorized user, but, after conferring with a supervisor, told us they would have to kill the newly issued card and issue us yet another new card. The security and fraud rep did some digging and advised us the illegitimate user had been added as a result of a telephone transaction. This was a surprise. We had gotten NO notice by email or phone that a new authorized user had been added to our card.

Evidently, this person in Iowa came by Mrs. Burt's card number and enough personal information to be able to have a female accomplice call the credit card company and impersonate my wife well enough to get them to add his name and address to our card as an authorized user. They sent a card to his address in Iowa. Once he had it, he immediately started getting cash advances. Luckily, Mrs. Burt noticed these within a few days.

Our account with the credit card company is now back in operation with a PIN required for ATM cash advances. At the suggestion of the security rep, we have also added a "verbal password" that any caller must provide before they can do any transactions with a service rep.

Secondary Consequences

Because we didn't know the extent of the fraudster's penetration of our security information, I had to immediately move to change the passwords on all our online financial accounts. This was a serious bit of work, but absolutely essential. Once we had a clean card with the credit card company, because we use it as the card for recurring charges, I had to go to several websites (for example, Amazon.com) and update the credit card information. In all, I spent about 8 hours getting everything reworked. A lot of this time was spent meticulously recording all the changes in our LastPass password manager. As I write, I still have work to do to reconnect Quicken to our financial accounts so it can download transactions.

Preventive Measures (*See also Jeff Wilkinson's article on page 2*)

Our Sun City Summerlin Computer Club offers members a lot of information on how to be more secure. You can find this material on the club website at https://www.scscc.club/smnr.

One key thing we did several years ago is to set up **security freezes** at all three of the major credit bureaus. This prevents a fraudster from opening new credit accounts in our name.

With very few exceptions, we avoid having merchants or service providers keep our credit card numbers on file. You can't depend on these merchants to keep your information secure.

We also make it a point to use **very strong passwords** on all our financial accounts and to not reuse the same passwords on different sites. It's also important to change these passwords from time to time, even if there's no sign of fraud. If available, we use two-factor authentication.

It's critical to monitor *all* financial accounts regularly to detect any fraudulent transactions. The sooner you detect a problem, the less grief you will experience.

We also keep personal information on social media sites to a bare minimum. That makes it harder for fraudsters to impersonate you.

Conclusions

We don't know how the fraudster came by our card number and the personal information used to convince a service rep at the credit card company to add him as an authorized user to our account. Most likely it was picked up from the dark web after some merchant's sales databases got hacked.

I'm bothered that the credit card company would add an authorized user in response to a phone call without at least sending an email alert. Also, we had never heard about adding a PIN for cash advances or a "verbal password" for phone transactions. We plan to put these in place, if available, on our other cards and accounts.

We fortunately incurred no significant economic losses from this incident, but it did eat up a lot of my time and we were both feeling quite a lot of stress.

Kretchmar's Korner

Does Amazon Have Too Much Power?

Opinion

By David Kretchmar, Computer Technician

I have been an Amazon Prime member for a couple of years and, like many people, have regularly made small and large purchases through Amazon. I enjoyed the fast, often two-day "free" shipping for a time with Prime, although more recently this turned into two-week shipping on my sandals from Zappos (an Amazon subsidiary). The protection Amazon gives consumers is second to none in the online or offline world.

Amazon has become THE dominant online retailer in America, currently accounting for over 50% of online retail purchases in the United States. This is despite most formerly 100% brick and mortar operations such as Walmart, Home Depot, Target, and Best Buy, moving strongly into online selling.

Amazon's third-party marketplace, made up of millions of merchants, has become a critical part of Amazon's e-commerce business. The marketplace now accounts for more than half of Amazon's overall sales.

With Amazon's massive size comes power. It would be a miracle (and downright un-capitalistic) if Amazon did not take advantage of its massive size. Sadly, in recent years, Amazon has been using its power to force consumers to pay more for an item than they would otherwise pay if Amazon did not exist.

I can anecdotally attest to this as a result of my personal experience. I enjoy shopping online, at least much more than I like physically visiting a retail store. For each purchase I search a number of online resellers, getting a good idea of who has the best price.

For many years I continued to shop online at Amazon and other sellers, sometimes finding that Amazon had the best price, yet also often finding a better buy elsewhere. I made kind of a game of it and enjoyed finding a better price (including tax & shipping) on sites other than Amazon. I did this a little out of jealousy (I have never owned Amazon stock) and because of a nagging feeling that Amazon and Jeff Bezos were taking over the world.

In recent years I have found it increasingly difficult to find a better price than Amazon's on many popular items. I did not know how or why, but the rules seemed to have changed.

The Anti-Trust Lawsuit

On May 25, 2021 the Washington, D.C. Attorney General, Karl Racine, announced he was suing Amazon on antitrust grounds, claiming the company's practices have unfairly raised prices for consumers and blocked innovation. The lawsuit alleges Amazon illegally maintained monopoly power through pricing contracts with third-party sellers. An Amazon spokesperson said Tuesday: "The DC Attorney General has it exactly backwards — sellers set their own prices for the products they offer in our store." I believe this is untrue.

Karl Racine is seeking to end what he alleges is Amazon's illegal use of price agreements to reduce competition; the lawsuit also asks for damages and penalties to deter future similar conduct. The suit asks the court to block Amazon's ability to harm competition by imposing a variety of reliefs, up to and including breaking up Amazon.

How Amazon Raises Prices

The lawsuit, filed in D.C. Superior Court, alleges Amazon illegally maintained monopoly power by using contract provisions to prevent third-party sellers on its platform from offering their products for lower prices on other platforms. The attorney general's office claimed the contracts create "an artificially high price floor across the online retail marketplace," according to a press release. Racine stated that these agreements ultimately harm both consumers and third-party sellers by reducing competition, innovation and choice.

Amazon requires third-party vendors who want to do sell on Amazon to abide by its business agreement. Until 2019, Amazon included a clause in that agreement that prohibited sellers from offering their products on a competitor's online marketplace at a lower price than what their products sold for on Amazon. Amazon removed that rule in March 2019 as it faced growing antitrust scrutiny.

The complaint alleges that even after Amazon removed the "no cheaper" pricing provision from its agreements with third-party sellers, it added an identical policy it called its "fair pricing policy." The fair pricing policy enables Amazon to "impose sanctions" on a seller that offers their product for a lower price on a competing online marketplace.

Do Sellers Really Set Their Own Prices?

Yes, they do – but only as long as they follow Amazon's pricing rules. Amazon's pricing agreements were also a topic of scrutiny in the House Judiciary subcommittee. In their final report lawmakers agreed that Amazon uses its dominant position in e-commerce as leverage with third-party sellers to require they adhere to pricing restrictions.

These clauses are at least anti-competitive, especially when a company like Amazon has virtual monopoly powers.

APCUG Guest Article

The Day the Music App Died

By John Krout, Writer/Presenter
Potomac Area Technology and Computer Society
www.patacs.org krout75 (at) yahoo.com

Introduction

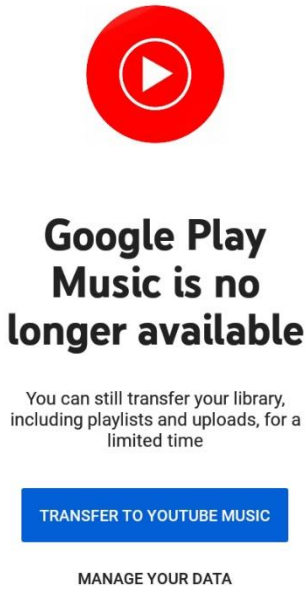
Google's **Play Music** app is gone on some Android devices, and soon will be completely gone.

I am a music collector. I have a large collection of audio CDs; roughly 1,600 songs are on the micro-SD card in my Samsung Galaxy S10 phone. I bought that phone in late 2019, and my carrier recently upgraded the phone's Android OS to version 11.

I started my Android experience on a Galaxy S5 phone, which I still own. That phone runs Android 6. I also own two Galaxy tablets, a recently purchased S5e running Android 10, and a much older A model running Android 8.1.0.

On February 1, 2021, I started the Play Music app on my Galaxy Tab S5e. The app displayed a screen stating that Play Music is "no longer available". The same announcement recommended installing the YouTube Music app.

You can see that screen in **Illustration 1**.



Why I Won't Use the YouTube Music App

YouTube is owned by Google. The intent of the YouTube music app is to play music stored "in the cloud".

There are three reasons why that cloud storage approach is not ideal for me.

First, that network-intensive method is a classic way for a dedicated fan of music to run into the ceiling on cell network data usage very quickly each month, with financial penalties for exceeding the ceiling, if your carrier contract has such a limit.

Second, despite claims that music stored in the cloud is available wherever you go, there are vast stretches of the US where data service is minimal or is completely absent. Drive through any mountainous area and that becomes obvious very quickly. With 5G, which has a much shorter range than 4G, that problem will be even more acute. The mountains will be the last place carriers build the extra towers necessary to make 5G work on every mile of interstates. Don't count on that to happen on other mountain highways in the next ten years.

Third, there is a privacy issue. Music stored and accessed in the cloud is an invitation for the cloud storage provider to learn about one's music preferences and monetize that knowledge, such as through endless ads.

What Google Decided to Do

I went to my desktop computer and googled the status of the Play Music app. I learned that, in 2020, Google announced that the company would no longer support the app as of December 3, 2020.

That end of support, by itself, does not cause the app to stop working. I use the Play Music app daily on my S10 phone. So far, the app still works just fine.

The fact that Google **disabled** the Play Music app on my Tab S5e tablet was quite an unhappy surprise. Even with the music indexing quirks in Play Music, which I wrote about a couple of years back, the Play Music app was reliable and reasonably easy to use.

I surveyed the fate of the Play Music app on my other Android devices. On the S10 phone, running Android 11, the app can still play my music collection stored on the phone. On the S5 phone, running Android 6, the app can still play my music collection stored on the phone. On my Galaxy Tab A, the app acted like the app on the Tab S5e, displaying the no longer available screen.

I expect that the end is near for the Play Music app on my current S10 phone and my old S5 phone.

There Are Many Other Music Player Apps

Of course, I went to the Google Play Store and looked for music player apps. That category is a huge, bewildering forest. The Play Store app recommended some alternative searches, including "music player no ads", so I tried that. Ads are another unwelcome use of cellular network data.

For each app, I looked at the review rating average, the number of reviews, and the total number of downloads. I also made sure that each was capable of playing music stored on the phone, not in the cloud.

Musicolet has been downloaded 5 million times and has a 4.7 rating average in almost 120,000 reviews. That is a very strong rating average. So, I downloaded that app on my Tab 5e.

When I started the Musicolet app and worked through its setup steps, I learned that it has one feature I liked immediately. The app provides the option to specify one or more particular folders on the phone or tablet in which to find sound files. I chose the folder on my micro-SD card where I parked my 1,600+ songs (1,637, according to Musicolet). The advantage is that, unlike Play Music, the app will ignore my voice memos that are stored in a different folder. Play Music app automatically threw in all my voice memos, which are far less entertaining than my music.

Musicolet also offers a feature to play songs in random order, sometimes called Shuffle Play, just like the Play Music app. I use that constantly so that my music sounds like an FM progressive music station in the 1970s. I have other music on my phone as well, from the 1950s through the 2000s.

Another ad-free music player app with just about the same attractive stats is **Pulsar Music Player**. This one claims to support use on car sound systems via Android Auto.

Most sound systems in recent cars already provide Bluetooth capability. If you only want to access phone or tablet music, and you do not have the Android Auto feature in your car, you can play music from your phone on the car stereo via Bluetooth. Android Auto offers other advantages.

The Bottom Line

I hope other app publishers do not follow this disappointing Google precedent. When support is ceased, let the user base continue to enjoy the capabilities of the app, at least until an Android OS update breaks the app.

Lab Monitor Schedule

Facial coverings and social distancing of 3 feet required.
This may change after June 1 pending changes in state, cunt and association rules.

The Open Lab session is held once per week: 9 am to noon on Saturdays.

June 2021	Monitor Schedule
Jeff Southwell Carol Przybycien	Saturday 06/05/2021
Fred Cohen Ann Warhaftig	Saturday 06/12/2021
Kathy Kirby John Zuzich	Saturday 6/19/2021
Karen Ristic Ray Ristic	Saturday 06/26/2021