

***THE
GIGABYTE
GAZETTE***

The Monthly Newsletter
of the
***SUN CITY SUMMERLIN
COMPUTER CLUB***

<https://www.scscclub.com>

November, 2023

Table of Contents

President’s Message.....	3
General Membership Meeting	4
SCSCC Board of Directors Actions	4
November 2023 Printable Calendars	4
Submissions Welcome	5
Welcome New Members	5
Special Interest Groups and Kaffee Klatches	6
Class and Q&A Offerings	8
Tom’s Tech-Notes	9
Kretchmar’s Korner.....	13
APCUG Guest Article	17
Lab Monitor Schedule.....	19

Issue Contributors

Tom Burt

Gail Weiss

Kathy Kirby

David Kretchmar

Jeff Wilkinson

Kurt Jefferson



President's Message

November News

by Jeff Wilkinson

Now that Autumn has started and the candy corn has been harvested, we begin to feel the change of seasons, which also brings an abundance of scams. These trick or treaters offer, almost exclusively, tricks of increasing complexity and deceitfulness. Now is a good time to review your backup plans, password management and virus protection. And of course, don't let unknown strangers remote into your computer. Our website: <https://www.scscclab.com> contains lots of useful information and notes from past presentations.

We are preparing for our election of club officers and board members at our December 7 meeting and holiday party. Nominations are now open. To nominate someone, including yourself, contact [George Lobue](#), our election committee chair.

We are always looking for suggestions on what seminars and classes to offer and welcome anyone as an instructor to share their knowledge and expertise.

Have a safe holiday season!

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

General Membership Meeting

The club's General Meeting will be at **2 PM on Thursday November 2nd** in Desert Vista Room 5. The nominating committee will present its proposed slate of officers and directors for 2024 after which additional nominations will be accepted from the floor. Our program will be a tutorial video and discussion: "What is Artificial Intelligence?" We'll also have the usual coffee and cookies.

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

SCSCC Board of Directors Actions

The Computer Club Board of Directors took the following actions on October 11, 2023

George Lobue made a motion that the **minutes of the September 13, 2023 Board Meeting be approved as submitted**. The motion was seconded by Jeff Wilkinson and unanimously approved by the Board.

George Lobue made a **motion** that the **meeting adjourn**. Chuck Hagen **seconded** the motion, and it was unanimously **approved** by the Board. The meeting was adjourned at 10:10 AM.

November 2023 Printable Calendars

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

https://www.scscclub.com/Calendars/scscclub_calendar_2023-11Nov.pdf

Submissions Welcome

We are always looking for new information to share with our club members. If you have computer or technical information or tips 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 2023 members have joined the Computer Club from September 28 to October 29, 2023.

Robert Fitzgerald
Carol Liberty

Joann Malkin
Eleanore Wenzel

As of October 30th, the club has 549 paid memberships for 2023 and 17 for 2024.

As of December 31st, 2022 the club had 570 paid memberships for 2022.

The Computer Club is now accepting new and renewed memberships for 2024. Annual dues are \$10 per person, good for the remainder of 2023 and all of 2024.

Special Interest Groups and Kaffee Klatches

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.

Android Help <H> *Live in the Classroom*

Gene Koch

Third Thursday at 1 PM monthly

Next meeting: Thursday, November 16, 2023

This hands-on Q&A session offers one on one help to Android phone and tablet users.

Apple iPhone / iPad Help <H> *Live in the Classroom*

Zane Clark 702-332-5747

First Wednesday, 9 a.m. monthly

Next meeting: Wednesday, November 1, 2023

The help session offers one-on-one help with your questions and problems. Come anytime, leave anytime.

Internet Investing <W/M/H> *via Zoom*

Tom Burt (702-341-7095)

3rd Thursday, 10 a.m. monthly

Next meeting: Thursday, November 16, 2023

The Internet Investing SIG provides a forum for members interested in using Internet resources for researching and managing investments. The groups meets to discuss, and learn more about investing, finance, tax, estate planning and legal matters. The SIG's target audience is members with intermediate computer skills and investment experience, but all members are welcome.

Kaffee Klatch <W/M/H> via Zoom

Jeff Wilkinson (702-527-4056)

Every Tuesday at 8:30 a.m.

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.”

Repair SIG <W/L/M> Live in the Classroom

Chuck Hagen (702-418-2614)

Every Tuesday, 12:30 p.m. to 3:00 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.***

Windows 10/11 SIG Live in the Classroom

Bill Wilkinson (702-233-4977)

First and Third Saturdays at 9:30 a.m.

Next meetings: Saturday, November 4 and November 18, 2023

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 Windows 10/11 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.

Class and Q&A Offerings

The club's educational sessions are being conducted either as Zoom webcasts, live in-person or a hybrid of the two. Check the weekly calendar on the [club website](#) to see which mode the session is using. Unless explicitly stated, advance registration is not required for these sessions.



Managing Your Contacts in Gmail and On Your Mobile Devices

Saturday, November 25th 9 - 11 AM Live and Zoom

Presenter: Gail Weiss

Location: Classroom

In my November class we will discuss how to manage your contacts in Gmail and your mobile devices (iPhone and iPad). We will discuss how to sync up your iPhone/iPad contacts to Gmail and how to import your Google contacts to your iPhone/iPad.

I also know a bit about Android phones, and I will discuss the settings you need to sync your device contacts.

This class will be held in the Computer Club Classroom, so please bring your own laptops or mobile devices if you want to follow along. For more information about this class or if you have any questions or ideas for future classes, please email me at gmweiss5@gmail.com.



Cyber Security Refresher

Wednesday, November 29th 10 – 11:30 AM *via Zoom*

Presenter: Tom Burt

Location: Zoom Webcast

Our computer club regularly educates our members on how to protect themselves against the myriad of cyber security threats that can impact their personal and financial safety or cause the loss of critical or precious information.

This seminar will review important things you can and should do to strengthen your own cyber security. We'll also delve into some of the newest forms of authentication you can use to go beyond simple passwords when accessing sensitive online accounts.

The presentation notes will be available about November 24th at:
<http://www.scscclb.com/smnr/ImageEditingWithGIMP.pdf>.

We will be recording this seminar and posting it to the club website.



Tom's Tech-Notes

Adobe Express Artificial Intelligence in Image Editing

Tom Burt, SCSCC Vice President

One of my regular seminar topics is image editing. I've presented seminars on GIMP, Photopea, Paint.Net and Windows Photos and even have one prepared on Adobe Photoshop Elements in case my colleague Mary Lou Miles someday decides to give up her activities in the education program.

One of my presentation projects is to make a portrait using a head shot composited against a simple background. To do this, the background of the headshot must be removed and replaced with transparency. Then the desired background is added in a separate layer behind the head shot. This is conceptually a fairly simple process, but it can prove very difficult to remove the background from the original headshot image while retaining all the subtle elements of the subject. Often, the background is very cluttered and also may have elements that have similar colors to those of the subject. Hair is the biggest problem, especially when the subject is female.

Traditionally, my method has been to use the image editing program's eraser to paint out the background. Near the edges of the subject, I work at high zoom levels with a small eraser size and with the hardness of the eraser brush set to about 30% so the edges are softened a bit. This helps make the composite look more natural. My method is slow and demands a steady hand on the mouse. I have to work in small steps so that if I make a slip, I can undo it by pressing Ctrl+Z without undoing very much of my prior work.

In the past year or two, image editing software has begun to incorporate "AI" technology to help address these difficulties. You can now just ask the program to completely remove the background or perhaps remove an undesired element, like a photobomber, from the image. Adobe and Google have added these types of features to their products. As we'll see below, Adobe now has a web-based free product, **Adobe Express**, that has some remarkable features. The free Google Photos likewise has some surprisingly powerful AI features.

Let's look into my simple portrait example. I wanted to make a new portrait of myself for Facebook and to use a thumbnail here in the Gigabyte Gazette and for my class notices. I used my webcam to take a high-resolution selfie.



Original Head Shot with Messy Home Office Background

There's a lot of visual clutter in the image and there's some spherical distortion caused by the wide-screen webcam lens. My first step was to go to: <https://www.adobe.com/express/> and select "Quick Actions" from the menu bar and then select "Remove Background". I then downloaded the result to my PC hard drive as a .png file.



Head Shot with Background Removed by Adobe Express

Adobe Express did the background removal in less than a second. This used to take me at least half an hour to do by hand and the Adobe results were better. It did remove a bit of my hair because my hair blended into the gray background.

Next, I added a background layer filled with a radial zoom light gray fading to dark blue. This creates a halo effect around the subject. Here's the result of that.



Head Shot with New Background



To wrap up, I cropped the image and used Windows Photos' spot healing brush to clean up a few small spots.

I then saved a resized copy of the final image to use as my new thumbnail in various places.

Once you have your original subject in an image with a transparent background, you can composite it with all kinds of interesting real or synthesized backgrounds.

My radial gradient's colors could be adjusted for different seasons or moods or to compliment artwork in the newsletter.

Adobe Express has a rich set of features for image and video generation and editing. Included is one that's quite impressive: "Text to Image". You can enter a text description of a desired image and Adobe Express will use AI to synthesize a series of images that match the description.

Let's look at a simple example ...

I chose "photo" as the content type and for the text description I entered the following: "Dachshund side view".

I then clicked 'generate'. Adobe Express worked for a few seconds and then offered up a set of four different images of dachshund dogs in different orientations. There was also a "Load more" link in case none of the first ones presented were what I was looking for. I clicked "Load more" a few times to see what the alternatives looked like. I finally chose the following image ...



Adobe Express AI-generated Dachshund

Note – this is not an image that Adobe Express found; it *generated* it based on having been trained on a large number of images of dachshunds. Try it yourself!

I've only touched on two aspects of AI in image editing as offered by Adobe Express. There's a wealth of other features. All this is available for free after you sign up for an Adobe Account – no credit card required. No doubt you will receive promotional emails encouraging you to purchase other Adobe Products.

Artificial Intelligence in image generation and editing is a rich and growing field to which we will return in future months.



Kretchmar's Korner

Cyber Security

David Kretchmar, Hardware Technician

Recently SCSCC Vice President Tom Burt provided members with a link to an interesting article from *Malwarebytes* about cyber security:

<https://www.malwarebytes.com/blog/news/2023/10/the-3-crucial-security-steps-people-should-do-but-dont>

Malwarebytes (2 week free or trial version) is an excellent product that I and other SCSCC technicians frequently use to search for malware and other potential PUPs (potentially

“Everyone’s afraid of the internet and no one’s sure what to do about it.”

unwanted programs) on computers. *Malwarebytes professional* is their paid-for real time protection that is sold for \$30 - \$45 per computer per year.

The essential point of the article was that many internet users employ “dismal cybersecurity practices” and are too lax in their implementation and use of security measures designed to keep them safe and secure. Some experts estimate that one-third of individuals experienced some sort of security breach within the past year. This sounds reasonable based on my personal experience, but I also find it comforting that older adults (Baby Boomers) are estimated to be 4 times less likely to experience a security issue than younger users. I’m unsure if we are more careful than younger users or if we just do less online?

While anything that makes people aware of the dangers that stalk all of us online is valuable, I disagree with 2 of the 3 major points raised in the article. The article was provided by *Malwarebytes*, and since they sell subscriptions to their products to stay in business, it is arguably in their interest to frighten people, who then will be more likely to become customers.

In the following paragraphs I will discuss the essential 3 points made in the article that I find misleading, outright untrue, and mostly true (multi-factor authorization).

1. “Just 35 percent of people use antivirus software.”

I call BS on this. In fact, it is rare for me to come across a computer that has no antivirus software running. Microsoft Windows Defender runs by default on Windows computers and does not have to be turned on by the user. This is by far the antivirus software utilized by most individuals, and it has the advantage of having no cost beyond what a user initially pays for a Windows PC.

In addition to being “free”, the Microsoft Windows Defender program code is updated at least monthly. The monthly security update release is scheduled for the second Tuesday of each month. The Microsoft Windows Defender virus intelligence database is updated almost daily in

case of newly discovered threats, also known as a 0-day or zero-day vulnerabilities. The term zero-day refers to the fact that the vendor has just learned of the flaw – which means they have zero days to address it.

It might be that only 35% of users subscribe to an anti-virus software tool other than Microsoft Windows Defender. Certainly, *Malwarebytes* would like you to buy their product, but the article is stating an untruth when it says that only 35% of computers are protected.

I believe Microsoft Windows Defender provides excellent protection for most users. The modern version of this security package was implemented with Windows 10 in 2015 and is further improved with Windows 11. I have examined hundreds of computers since 2015 and have never had to remove a virus protected by Microsoft Windows Defender. Before 2015 our club's hardware technicians spent as much as half our time at our Tuesday Repair SIG removing viruses from systems, but this work is no longer necessary.

2. “Just 15 percent of people use a password manager.”

Again, I call BS on this. It is not uncommon for club members who come to the Tuesday Repair SIG, when asked for their password to, for instance, their Google account to state, “I don't have a password; I just click on Gmail, and it appears.” They are unknowingly, and effortlessly using a password manager.

You cannot use an application such as Gmail or any other mail program without a password. Many users set up a password for Gmail, or any number of other applications, when they initiate use of that service, or they have this done for them by whomever is helping to set up their device.

Many users forget they really do have the required password because it is entered automatically and seamlessly by their browser's built-in password manager. Google, Edge, Firefox, and Safari all have integrated password managers, with features like autofill and a password generator. They can also store credit card and other personal information, which makes your online life easier. Smartphone operating systems on the Apple iPhone, Samsung Galaxy, etc. also store user credentials.

A password generator will create a unique password such as, “8X!4tZ7pas@vFyY” which is impossible to guess and almost impossible to memorize. This bizarre string of characters is best utilized by a password manager. I have seen people write down and manually enter a generated password, but obviously it is tedious and often takes multiple tries.

Are passwords saved by browsers secure?

Google states “Google Password Manager and the passwords it generates are considered safe compared to similar password managers. Google uses military-grade encryption to protect your usernames, passwords, and payment information.”

Microsoft states, “Microsoft Edge stores passwords encrypted on disk. They're encrypted using AES and the encryption key is saved in an operating system (OS) storage area”.

Firefox states, “Firefox Desktop uses simple cryptography to obscure your passwords. Mozilla doesn't have the ability to see passwords, but Firefox Desktop does decrypt the password locally so that it can enter them into form fields.”

In other words, the “free” password managers built into browsers and operating systems use security schemes that are like paid password managers. Naturally marketers of these paid-for third party services such as Nordpass, Norton, OneLogin, and LastPass claim built-in password managers are vulnerable.

Unfortunately, third party password managers have been hacked, with user information severely compromised. OneLogin was hacked in 2017, and LastPass was hacked in 2022. In March 2023, LastPass stated that the breach resulted in unauthorized and unknown users gaining full access to customers' vault data, including personal information like usernames and passwords.

Yet third party password managers urge users to buy their product rather than depend on the security built into browsers and operating systems. But any account or device can be hacked.

Unless you write down your passwords using a pencil and paper, you are going to have to trust someone and use a password manager. I would rather trust a massive entity such as Google, Microsoft, or Apple over a relatively tiny software provider. Even larger entities, such as Norton, have been subject to internal dishonesty and theft of client data.

3. Use multi-factor authentication (MFA)

Clearly this is NOT BS. Multi-factor authentication (MFA) requires users to provide at least two of 3 categories of authentication to access an account.

- **Knowledge:** a password or PIN code,
- **Possessions factor:** a secondary device (i.e. Smartphone) or account you have, in addition to a knowledge factor.
- **Biometrics:** any part of the human body that can be offered for verification, such as fingerprints or facial recognition.

I only have one account, Interactive Brokers, that *requires* MFA. When I want to access my account, a notification is sent to my iPhone, which opens the Interactive Brokers application on my phone and identifies me using facial recognition. Thus all 3 factors of MFA are utilized, which is about as good a set of authentications as you are going to find today.

Disadvantages of MFA

The second factor, the secondary device or account, is much stronger when a separate device is utilized. Many MFA schemes send a code to an email account, which is obviously useless when that happens to be the account you are attempting to access. Using only an email account for secondary authentication rather than a discrete device, such as your smartphone, provides weaker security.

MFA can wind up locking you out of your account when your discreet device (phone) is unavailable, runs out of juice, or lacks an internet or cellular connection.

Conclusions and Recommendations

Microsoft Windows Defender runs by default on Windows computers and does not have to be turned on by the user. Microsoft Windows Defender provides excellent antivirus protection.

The password managers provided by browsers and operating systems are reasonably secure. I believe they are similar in security compared to password managers provided by third-party vendors, maybe better. These credentials operate seamlessly with the operating system or browser used and can make for a much smoother internet experience.

Multi-factor authentication is the way to go if you want real internet security. Using the 3 categories of authentication, knowledge, possession, and biometrics provides some of the best security available today.

APCUG Guest Article

Popular Email App Undergoes Major Overhaul with Complete Redesign Due in 2023

By Kurt Jefferson, Editor, Central Kentucky Computer Society
<https://ckcs.org/> lextown2 (at) gmail.com

Hate your email app?

Consider switching. One option is Mozilla's **Thunderbird**, a major player that's been around for years. However, it's now undergoing a major redesign since it was first created nearly 20 years ago. It's an open-source app for managing email, calendar, news feeds, newsgroups, and a chat feed.



Version 102 is introducing folder colors, new icons, a revamped address book, and more. Developers say this is just the beginning. They plan to introduce a greatly "modernized" Thunderbird in 2023 with version 114.

Thunderbird is already one of the most popular email apps in the world – with more than 20 million users running it on Macs, Windows, and Linux computers. An Android version is in the works, and developers are eyeing the possibility of a version for iOS.

Thunderbird is free, but if you use the app on a regular basis, developers ask you to donate here: <https://give.thunderbird.net/en-US/>

TechRadar says Thunderbird offers "one of the best sets of features you'll find in an email client." All Things Newz writes, "Mozilla Thunderbird is having a resurgence right now, armed with an expanded team of developers and a plan to take over the email world (including Android)."

Thunderbird began 19 years ago when the Mozilla Foundation – known for its Firefox browser – introduced Thunderbird's predecessor.

In 2012, Mozilla announced it was no longer making Thunderbird a priority and stopped ongoing development. An all-volunteer council met in Toronto and decided there was enough demand to keep Thunderbird alive and add features users requested.

In 2020, a new wholly owned subsidiary called MZLA Technologies Corporation assumed project leadership.

Fast forward to 2022, and headlines proclaim:

The Thunderbird Mail Client Will Be Full of New Features This Year

Here's How Mozilla Thunderbird is Making a Comeback in 2022

Mozilla Thunderbird Will Receive a Major Update with Version 102

Because Thunderbird is open-source software, it's developed, tested, and supported largely by dedicated volunteers.

One of the features that sets it apart from most other email apps is the ability to customize Thunderbird through extensions and themes – similar to the Firefox web browser.

TechRadar concludes, "Thunderbird is a desktop email client we can recommend all day. It offers an extensive feature set for users despite being free. Because it's open source, there's an endless number of customizations for the platform, which sets it apart from the competition. The main drawback is that it's pretty difficult to use, making it best suited for technical users." <https://www.techradar.com/reviews/mozilla-thunderbird>

If you've never tried Thunderbird, you might want to give it a chance. You can download Thunderbird for Mac, Windows and Linux at www.thunderbird.net.

Version 102 (released in late June, 2022) supports Windows 7 or later, macOS 10.2 or later, and most Linux distributions that have GTK+ 3.14 or higher.

If you're already running Thunderbird version 91.12.0, you can upgrade to version 102:

Mac: Click on Thunderbird in your menu bar. Click on "About Thunderbird" in the drop-down menu. A box will open on your screen allowing you to update and restart Thunderbird. If you're running a version older than 91.12.0, you need to replace your current version by downloading version 102 and install it from the www.thunderbird.net website.

Windows: Click on Thunderbird in your menu bar and select "About Thunderbird." The About Thunderbird window will open and start downloading the latest version. If you're running a version older than 91.12.0, you need to replace your current version by downloading version 102 and install it from the www.thunderbird.net website.

Linux: Open the "About Thunderbird" box from the Help menu or click on the small (i) icon next to the version number in the main window and upgrade to 102. If you're running a version older than 91.12.0, you need to replace your current version by downloading version 102 and install it from the www.thunderbird.net website.

As I type this, Thunderbird has now been updated to version 102.4.1. Look for more incremental updates before versions 103, 104, and especially version 114, arrive next year.

Thunderbird 102 details:

<https://blog.thunderbird.net/2022/06/thunderbird-102-released-a-serious-upgrade-to-your-communication/>

(Ed. Note: As of October, 2023, Thunderbird is up to version 115.4.1. Kurt's upgrade directions should still work.)

Lab Monitor Schedule

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

November	Monitor Schedule
Jeff Southwell Linda McMullin	Saturday 11/4/2023
Linda Muench	Saturday 11/11/2023
Marilyn Gramms Linda Muench	Saturday 11/18/2023
Linda Muench	Saturday 11/25/2023