(membership includes monthly subscription)

The Digital VIKING

Twin Cities PC USER GROUP NEWSLETTER

Minneapolis & St. Paul, Minnesota USA • Vol. 45 No.6• January 2025

TC/PC Exists to Facilitate and Encourage the Cooperative Exchange of PC Knowledge and Information Across All Levels of Experience

January 2025

4

General Meeting

Tuesday, January 14, 2025

7:00 PM

Show Us Your Gadget!

Via Zoom Only

This month, members can bring their newly acquired or well-worn "gadgets" to the zoom screen to share with the group. A "gadget" could be an electronic device or computer component or phone app or computer program or a service you've found or even a YouTube video or channel you think we can all benefit from watching. Please bring some kind of image that can be used in next month's newsletter and the description and price that can be used as well.

Note: All TC/PC Meetings and SIG Groups will be virtual until further notice. Visit tcpc.com for info.

Tech Topics with Jack Ungerleider via Zoom at 6pm before the General Meeting.

The Digital Viking

The Digital Viking is the *official monthly publication of the Twin Cities PC User Group, a 501(c)(3)organization and an all-volunteer organization dedicated to users of IBM-compatible computers. Subscriptions are included in membership. We welcome articles and reviews from members.* The Digital Viking is a *copyrighted publication and reproduction of any material is expressly prohibited without permission. Exception: other User Groups may use material if unaltered and credited.*

Advertising

Full page (7½ x 9½)	**$100.00**
Two-thirds page (7½ x 6)	**80.00**
Half page (7½ x 4¾)	**65.00**
One-third page (7½ x 3)	**50.00**
Quarter page (3½ x 4¾)	**40.00**
Member Bus. Card (2 x 3½)	**10.00**

Multiple insertion discounts available.

Contact Sharon Walbran at:: SQWalbran@yahoo.com

Deadline for ad placement is the 1st of the month prior to publication. All rates are per issue and for digital or camera-ready ads. Typesetting and other services are extra and must be requested in advance of submission deadlines.

Payment must accompany order unless other arrangements are made in advance. Place make checks payable to: **Twin Cities PC User Group**

TC/PC 2024-2025 Board of Directors

Meets once or twice per year. All members welcome to attend.
Visit www.tcpc.com for meeting details.

President —Lee Kaphingst	leekap@comcast.net
Vice President —Curtiss Trout	ctrout@troutreach.com
Secretary - Sharon Walbran	sharon.walbran@gmail.com
Treasurer - Sharon Trout	strout@troutreach.com
Newsletter Publisher Sharon Walbran	952-925-2726 sharon.walbran@gmail.com
Web Master Curt Trout	ctrout@troutreach.com
Board Members:	
Steve Kuhlmey	skuhlmey@hotmail.com
Lon Ortner	612-824-4946 lon@csacomp.com
Lee Kaphingst	leekap@comcast.net
Jeannine Sloan	Ambassador for Friendship Village
Curtiss Trout	ctrout@troutreach.com
Sharon Trout	strout@troutreach.com
Jack Ungerleider	jack@jacku.com
Sharon Walbran	sharon.walbran@gmail.com

TC/PC Member Benefits

Product previews and demonstrations

Special Interest Groups
Monthly Newsletter

Discounts on products and services

Contests and prizes

Business Member Benefits

All of the above PLUS:

FREE ½ page ad on payment of each renewal

20% discount on all ads Placed in the *Digital Viking* Newsletter

Up to 5 newsletters mailed to your site (only a nominal cost for each additional 5 mailed)

Newsletter Staff

Editor Sharon Walbran

Why I am a morning person!

By Lynda Buske
Published in Ottawa PC News (October 2023)
Ottawa PC Users' Group, Ontario, Canada
https://opcug.ca
Editor: brigittelord(at)opcug.ca

In a previous column, I wrote about taking photographs in the evening or nighttime. (https://opcug.ca/Photography/EveningPhotography_v3.pdf). However, I prefer to shoot in the morning, especially during the blue hour before the sun comes up. While not everyone wants to get up that early (often 4 am in the summer), there are some definite advantages and photo opportunities that you don't get in the evening.

Technically, many of the tips are similar, like compensating for low light by using a tripod, opening aperture wide (small f-stop number), bumping your ISO (sensitivity to light), or perhaps using a cell phone, which tends to cope with low light situations well. When my phone is set to "night sight," it takes multiple short exposures and combines the images into a single, appropriately exposed photo.

However, this column will discuss the non-technical advantages of shooting pre-dawn rather than post-sunset (the two blue hours). These tips, however, apply mostly to landscape photography; if you like to shoot the city nightlife, you will not find much going on in the morning. If someone is still partying, then they are probably not worth photographing!

Depending on the time of year, there is a good chance you can catch some interesting frost or mist during the morning blue hour. Both often disappear shortly after dawn when the sun burns off fog or melts frost.

Birds get very active just after dawn. It is not just sheer luck catching migratory geese at dawn. You can hear them getting excited in the dark, and the minute the sun rises, they take off.

I find the early morning very relaxing. There is less city noise from traffic, especially in the summer when it is way before rush hour. Roads in the evening, regardless of the time of year, are busy before and after sunset. Parking is a breeze in the morning, and there is no competition for my favourite vantage points. If you are lakeside, the reflections are great in the morning before wind and boat traffic ruin them.

I like fewer people around, but the evening might be better if you want a lot of human interest in your photos. I usually have just enough fishermen, joggers, bikers, or kayakers to add interest if I want it. However, they seldom get in my way.

As a petite lady, I am nervous when strange men approach me in the evening. I am never sure of their intentions (innocent though they may be), and I concentrate more on picking up verbal or physical clues than on my photography. People can be distracting when asking questions about your gear (always the guys) at a critical moment when I'm trying to shift from blue hour settings to dawn settings. If someone says a few words at 5 am, I do not feel threatened, and conversations are usually short since perhaps neither of us has had a coffee! I think most of the baddies are simply not out at that hour.

Two-Factor Authorization Fiasco

Greg Skalka, President
Under the Computer Hood Users Group Home (uchug.org)
1editor101 (a) uchug.org

If you are accessing a personal account or app on the web, you should be concerned about that account's security. Bad actors (and I don't mean those who can't get a job in Hollywood) constantly search for our login credentials, hoping to access our accounts and steal money or personal information. The best ways to protect online accounts include using strong passwords and protecting them, resisting attempts by others to gain access to those accounts through scams and phishing communications, and using two-factor authentication on those accounts.

Two-factor authentication, or 2FA, requires at least two identification items of different types to log into an account. It is a subset of multi-factor authentication (MFA). This can be enabled for most online accounts; some account providers now require it. It typically requires providing two or more identifying items from three categories for account access. These categories are something you know (like a password, birthdate, or the answer to a security question), something you have (could be a specific phone, computer, or email account, or a security key, fob, or dongle), and something you are (a biometric like a fingerprint).

To get money from an ATM (assuming you are not trying the big truck with a chain approach), you must provide something you have (an ATM card) and something you know (a PIN). With a 2FA-enabled online account, to gain access, you would typically need something you know (a password) and something you have (either a smartphone or computer that can receive a security code through text message or email). Entering the correct code sent to the device that presumably only you have validates your identity in a second way (in addition to the password).

Your account provider may be using 2FA, and you don't even realize it. Even if you only enter a password for access, the provider may look at the IP address or other identifying information from your device's connection to validate that it is really you (something you have). If you usually log in from one device and then suddenly use another, the account provider may ask for additional verifying information, like the answer to a security question.

It should be evident that trying to make it more difficult for others to access your accounts could also make it more difficult for you. Going through additional steps, like entering a six-digit code you were sent through a text message, takes time and opens up the possibility of being denied access. If you lose your phone, have phone communication problems, have a malfunction in your fingerprint scanner, or lose control of your email account, you may not be able to get timely access to your accounts.

I was a little apprehensive about 2FA at first due to concerns about my being denied access due to some problem outside of my control. I don't remember if I started using 2FA because I enabled it or if some account I already had started requiring it. I have used 2FA for several years on most of my critical accounts. Whenever I am asked to enable it, I look to enable it on some accounts (I have found some that did not support it then; I'm starting to think less of those companies). I typically use my phone as the second form (something I have); I need to ensure I have my phone handy when I want account access on my computer. Receiving a code as a text on a phone is supposed to be more secure than receiving it in an email. It may be a little more work, but I have had a few problems with it denying me access when I needed it.

Recently, however, I have had a few instances of being denied access to accounts through 2FA. My first instance was about a week ago when I was trying to access my Scripps online medical account on my computer to perform an electronic check-in for a medical appointment. Of course, I was in a hurry, trying to do this late at night, just before bed for an appointment the next day, and I would not have time to do it later.

After successfully entering my username and password on the MyScripps web login page, a page was provided to select the method for sending a code: email or text. I have found that my phone usually receives the text in just a few seconds. This time, however, the text did not come right away as expected. I waited maybe 60 seconds (remember, I wanted to finish this and go to bed) and then clicked "Send code again." Again, I waited, this time a little longer. I checked my phone to see that it was on and not in airplane mode or something else that would turn off reception.

After waiting longer than I wanted, I finally selected email to deliver the code. Then, I had to start Thunderbird (my email program) to access my Juno email on my computer. Fortunately, the email with the code was there, and I successfully logged into Scripps and completed my task. At the time, I thought it was strange, but I didn't consider the problems I had any further. The following day, I found that the texts had come in at night.

A few days later, I tried to log into my US Bank online banking account from my computer; I again needed to check my account balance with some urgency. The US Bank 2FA code enter screen comes up right after entering a valid username and password; I may enable only texts to my phone for this. Again, I was used to having the text with the code pop up on my phone immediately, but I waited several minutes without receiving the text message. I now remembered my Scripps incident. There was no email delivery selection on the 2FA code entry screen on the US Bank website, but there was a link to "verify another way." I had hoped it would lead to verification through an email, but instead, it asked me to enter my debit card PIN.

I don't use a debit card for any of my accounts; I may have been sent one by the bank years ago, but I never activated it and had no way to get its PIN. This lack of access to my account was beginning to make me angry.

I canceled out of that screen (the only option) and tried going into the login page to get another code sent, but no code text message came to my phone. Finally, the bank locked me out of online access for too many unsuccessful attempts. I would need to change my password to get access again, and the first step for that was to send me a code that I'd need to enter. Good grief! I searched their website and finally found a number to call for online access support (they don't make things like this very obvious on their site).

While still on their site, I called the number and started my way down their automated phone menu system. Suddenly, while listening to the next set of options, I heard the sound of text messages being received on my phone. I found a bunch of texts from US Bank with 2FA codes that had just come through on my phone. I hung up the call and returned to the web page, but after entering the code from the last text, it said the code had expired, and a new one would be sent. Again, no code text was received. I called the US Bank support number again and found that action again appeared to trigger the receiving of text messages on my phone. Again, I was too late to enter these codes, but I now saw a pattern.

I returned to the bank website and asked for a code to change my password. I then immediately called the US Bank support number, and after a few entries in their audio menu, a text arrived on

my phone. I could enter this code in time, change my password, and regain access to my online accounts.

I finally got the information I needed off the website, but I was concerned about what I had to go through to get it. Why were my texts not coming through right away? It seemed like making the phone call (or pressing phone keys) triggered the reception of texts that appeared stuck somewhere.

This seemed like a problem, so I cycled power on my phone and then tried logging into my US Bank online account. This time, the text message with the 2FA code was received right after my password was accepted, just as it had been.

Something in my phone went awry, and cycling the power fixed it. I try to remember to do that periodically; I need to be better at making that a part of my tech management routine.

I still understand that online security is essential, but I also know how it feels to be locked out due to some malfunction in the system. The lesson in resiliency to take away is not to decrease security to prevent being affected by such a failure. Still, instead, I plan so I'm not doing things at the last minute and making myself vulnerable to problems when something inevitably breaks down.

Go to Page 1

Using the Windows Start Button

By Jim Cerny, 1st Vice President
Sarasota Technology Users Group
https://thestug.org/
JimCerny (at) gmail.com

All editions of Windows have a Windows icon in the lower-left corner of your desktop screen, sometimes known as the Start button. The “start” button on Windows is a very useful way to access any app or controls on your computer! (This article is for Windows 10, but the information is relevant to all Windows versions.) Left-clicking your mouse on the Start button brings up, among other things, a list of all your apps in the left column that are installed on your computer. Windows has many free apps, and you may have installed others. They ALL will be on this list.

One difficulty with scrolling down this list is that the scrollbar is almost invisible on the right side of this column. Gently move your mouse icon to the right side or edge of the column, and at just the right place, the vertical scrollbar will appear in normal size so you can use it. Note that many apps are stored in “folders” containing several apps since there are so many apps. All folders will have a yellow icon and a small arrow “>” on the right. Clicking your mouse on this arrow will open the folder and display the apps contained in it.

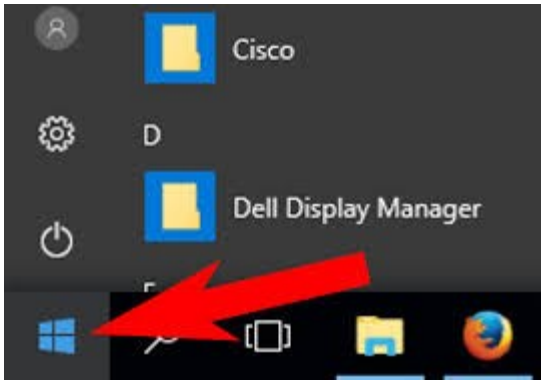
Practice scrolling down this list and finding the apps you have been using. You will also see many apps you have no idea were on your computer! There are lots to explore here when you have time, or “Ask Google” about any of them.

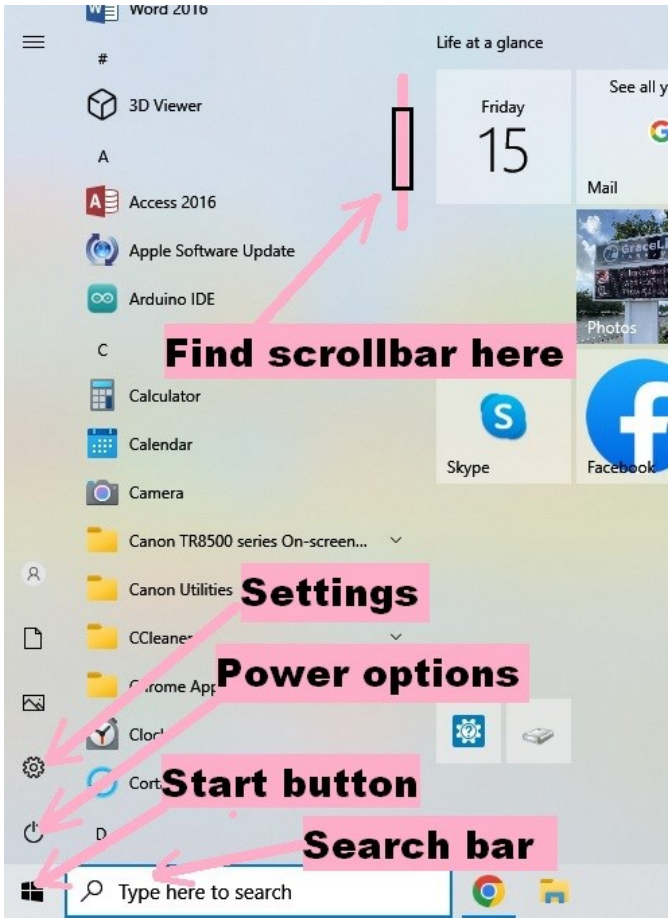
You can also find any app by typing the app name into the search bar just to the right of the Windows icon. When you use this search bar, it will search not only your computer but also the internet and your files and folders, so you will see many things related to whatever you searched for.

Back to the app list; what can you do after you find an app on the list? Well, you can right-click your mouse on the app to get a short list of what you can do. You can UN-install it -- that is, remove the app from your computer. You can also “pin” the app to the Taskbar at the bottom of your screen or the start menu. When you “pin” something like this, it will remain in that location until you delete or move it somewhere else. You can choose “pin to taskbar,” then move or “drag” the app icon from the Taskbar to your desktop.

You can also “drag” any app directly from this list to your desktop. To do this, place your mouse arrow on the app, HOLD down the left mouse button, and move your mouse to any blank area on your desktop. Let up the mouse button, and the app is on your desktop! An app icon on your desktop is a “link” that lets you open and use the app just by double-clicking your left mouse button. If the app icon is on your Taskbar, you only left-click it once.

In addition to displaying a list of all your apps when you click on the start button, you also get a short list of icons on the very left of this window. One is “settings” (which looks like a gear wheel), which gives you all the set-up options and controls for your computer. Another option you always use is the “power” option to turn off your computer or put it into “sleep” mode. You can look up or “Ask Google” what each menu item can do for you or information about any app. The Start button and the Search bar are always handy and helpful in finding apps and files on your computer, so don’t be shy about using them.


Cisco
D
Dell Display Manager


Word 2016
Life at a glance
3D Viewer
Friday
15
Mail
Access 2016
Apple Software Update
Arduino IDE
Photos
Find scrollbar here
Calculator
Calendar
Skype
Facebook
Camera
Canon TR8500 series On-screen...
Canon Utilities
Settings
Power options
Start button
Search bar
Type here to search

Go to Page 1

Boarding Pass to Your Data?

By Ron Brown
Tech for Seniors

Boarding Pass to Your Data? - Fasten your seat-belts, folks! We're about to take off on a journey through the not-so-friendly skies of airline app data collection. It seems that our trusty travel companions might be doubling as undercover agents, collecting more than just our boarding passes.

The Check-In - You know the drill: download the airline app, check in, and get your digital boarding pass. But while you're picking your favorite seat, the app might be picking out details from your phone. From passport details to your snack preferences, these apps are getting a first-class ticket to your personal info.

The Layover - Cybernews' investigation into 14 major airline apps revealed a startling truth: some apps have the potential to access a treasure trove of sensitive data on your device. We're not just talking about the usual suspects like your name and email. These apps could be eyeing your location, peeking at your contacts, and even noting down your device ID. It's like having a travel buddy that's a little too interested in your personal life.

The Frequent Flyers - Among the apps investigated, American Airlines and United Airlines were like the data-hungry monsters of the group, collecting more info than their peers. On the other end of the spectrum, Philippine Airlines played it cool, collecting the least amount of data. It's like the difference between a nosy neighbor and the one who just waves from across the street.

The Fine Print - Here's where it gets interesting: the "Data Safety" section on the Google Playstore is supposed to tell you what data these apps collect. But guess who fills out that section? The developers themselves. It's like asking a fox to report on the henhouse security. So, can we really trust them to spill the beans?

The Destination - So, what's the final destination for all this data? Some of it might be used for those 'personalized' ads that follow you around like a lost suitcase. But with the US Department of Transportation stepping in for a privacy review, we might see some new regulations on how our data is handled at 30,000 feet.

The Baggage Claim - Before you swear off airline apps and go back to smoke signals, remember that not all apps are created equal. Some are just doing their job, while others might be taking advantage of the open skies policy a bit too literally. It's all about reading the fine print and keeping your data on a short leash.

The Credits - For a more detailed account of which apps might be flying too close to the sun with your data, check out the original article by Paulina Okunytė on Cybernews. It's an in-depth look at the data collection practices of the airline industry that might just make you want to keep your feet on the ground.

You'll find that article at: https://cybernews.com/security/airlines-apps-data-collection/

If you're interested, you'll find my video (**Norbert "Bob" Gostischa)** on this topic at: https://youtu.be/NqG2kufIA34

If you find it helpful, don't forget to like, share, and subscribe. Thanks.
subscribe. Thanks.💻

Go to Page 1

Firefox Browser
What is new and improved

By Jasmine Blue D'Katz
Lake County Area Computer Enthusiasts
http://www.lcace.org/
cynthia.g.simmons (at) gmail.com

During a Zoom meeting with one of my Milwaukee computer clubs and Senior Planet "Lunch and Learn," there was a discussion about the Firefox web browser. I do not personally use Firefox as my primary browser, but I decided to give it a quick look to see what is new.

Firefox constantly receives updates with new features and improvements, so some new features might depend on which version you are using. Here are some noteworthy features recently added to Firefox:

ENHANCED PRIVACY

- **Copy Link Without Site Tracking:** This feature ensures that copied links no longer contain tracking information attached by websites. This is a handy tool for preventing your browsing activity from being monitored across different platforms.

- **Global Privacy Control:** This opt-in feature allows you to inform websites that you do not want your data shared or sold. It is enabled by default in private browsing mode and helps you take control of your online privacy.

- **Enhanced Canvas Fingerprinting Protection:** Firefox's private windows and ETP-Strict privacy configuration now includes improved protection against canvas fingerprinting, a technique used to track users based on their unique browser configurations.

- **Cookie Banner Blocker:** This feature automatically blocks cookie banners and refuses cookies for supported websites in private browsing mode. It is currently being rolled out for users in Germany and might become available in other regions soon.

- **URL Tracking Protection:** This feature removes unnecessary tracking parameters from URLs, making it harder for websites to track your browsing activity across different platforms. It is enabled by default in private windows for all users in Germany and might be expanded to other regions later.

IMPROVED PERFORMANCE AND FUNCTIONALITY

- **Hardware decoding support for AV1 video codec:** This feature enables smoother

layback of AV1 videos by utilizing your **c**omputer's graphics hardware. It requires the Microsoft AV1 Video Extension on Windows systems.

- **Voice Control commands on macOS**: Mac users can now control Firefox using voice commands, making browsing more convenient and hands-free.
- **Wayland compositor on Linux:** Firefox on Linux now defaults to the Wayland compositor when available, leading to improved touchpad and touchscreen gestures, swipe-to-navigate functionality, better graphics performance, and more.
- **Larger and clearer focus indicator**: The focus indicator highlighting the currently active element in Firefox has been improved with increased size, contrast, and a white box shadow for better visibility.

These are just some of the recent new features in Firefox. The browser is constantly evolving, so be sure to keep an eye out for future updates that might bring even more exciting improvements and privacy protections.

I hope this gives you a good overview of some of the cool new things you can find in Firefox! Let me know if you have any questions.💻

Go to Page 1

Meetings start at 7:00 PM (9:00 AM on Saturday) unless otherwise noted. *Virtual Meetings during Covid pandemic..

January

February

SUN	MON	TUES	WED	THU	FRI	SAT
			1	2	3	4
5	6	7	8	9	10	11 Linux on Saturday SIG 9am—Noon
12	13	14 7pm General Mtg Show Us Your Gadget 6pm Tech Topics	15	16	17	18 MS Office SIG (includes Access) 9am—Noon
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8 Linux on Saturday SIG 9am—Noon
9	9	10 7pm General Mtg TBA 6pm Tech Topics	11	12	13	14 MS Office SIG (includes Access) 9am—Noon
15	16	17	18	19	20	21
22	23	24	25	26	27	28

Twin Cities PC USER GROUP

You have just read an issue of The Digital Viking.

Would you like to receive this delivered directly to your email or business each month?

As a member of TC/PC, the Twin Cities Personal Computer Group, one of the benefits is reading this monthly publication at www.tcpc.com..

As a member of TC/PC, you may attend any or all of the monthly Special Interest Group (SIG) meetings and be eligible for software drawings. The small membership fee also includes access to real-live people with answers via our helplines, discounts, and various other perks.

Does membership in this group sound like a good way to increase your computer knowledge?

It's easy to do! Simply fill in the form below and mail it to the address shown.
(If you use the form in this issue, you will receive an extra month for joining now.)

1/25

Here's the info for my TC/PC Membership:

Full name_____

Company name_____

Address_____

City_____ State_____ Zip_____

❍Home ❍Business ❍Change address: ❍Perm. ❍Temp. 'til _____

Home phone_____ Work phone_____

Online address(es) _____

Where did you hear about TC/PC? _____

❍ I DO NOT want any of my information disclosed.
❍ I DO NOT want to receive any mailings

Administrative Use Only Rec'd_____ Chk#_____

I'm signing up for:

❍ Individual/Family Membership ($18)
❍ Business Membership ($100)
If an existing member your # _____

Make checks payable to:

Twin Cities PC User Group
341 County Rd C2 W
Roseville, MN 55113

Or sign up on our website:

http://www.tcpc.com

❍ Check #_____ ❍ Bill me
❍ New member ❍ Renewal ❍ Prior member

I'm interested in:

❍ Training classes ❍ Volunteering
❍ Special Interest Groups: New User, Access, etc.
List here:

January 14, 2025
7:00 pm

General Meeting

Show Us Your Gadget!

Via Zoom Only

Twin Cities PC USER GROUP

341 County Rd C2 W
Roseville, MN 55113

FIRST CLASS MAIL