OTTAWA PC NEWS

Volume 38, Number 3 March 2021

ARTICLE

Creating a rescue account

by Chris Taylor

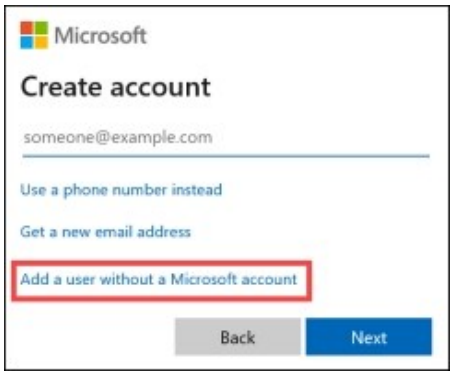
A default installation of Windows will result in a single, administrator-level account. What if you forget the password to that account, don't have it recorded anywhere, and haven't set up a means of recovering the password? What if the profile for that account gets corrupted? You will be locked out of Windows. All data on the hard drive could be lost forever.

It is simple to create another administrator-level account to allow you to recover should you ever have a problem signing into your main account. Only an administrator account has the ability to create new accounts, access all files on the computer, modify all configuration settings, install new software and more.

Press ⊞ + i (hold down the Windows key and press i) to load the *Settings* app. Click on *Accounts*. In the left panel, click on *Family & other users*. In the *Other users* section, click *Add someone else to this PC*.

At this point, you have to veer away from what Microsoft prompts you to do. Microsoft would have you create a *Microsoft account*. What you want is a *local account*, which is not dependant on any Microsoft infrastructure on the Internet. It is totally local to your computer.

Don't enter an "email or phone". Click the link *I don't have this person's sign-in information*.



Microsoft will again try to have you create a *Microsoft account*. But resistance is ***not*** futile.

Click on *Add a user without a Microsoft account*. You are–finally–presented with the screen to create a local account. Give it a name and password. Make sure you record this in a secure location. For approaches to managing passwords, see *Protecting your passwords* - https://opcug.ca/Reviews/ProtectPasswords.html and *Passwords* - https://opcug.ca/Articles/1912NEWS.pdf

You need to choose three security questions that can be used in case you forget your password. Make sure the answers can't be researched or guessed. There are two approaches that can guarantee this. You can enter nonsense answers and record those answers in a secure place. Or you can answer correctly (making it easy for you to remember the correct answer) and then add something only you know to add. In the example below, I added "Q-" to each answer.

(Continued on page 7)

Inside this issue:

Next Meeting: WEDNESDAY, March 10th, 2021

Next Meeting

Wednesday, March 10th, 2021

This meeting will be via Zoom video conference.
(connection details below)

Topic: Keeping passwords safe
Speaker: Chris Taylor, President, OPCUG

We are told: don't write down passwords; don't reuse passwords; make passwords long and complex. Once you get beyond half a dozen or so logon IDs, it becomes impossible to keep them all in your head. Chris Taylor will show how to use free software that stores all your usernames and passwords along with related information and protects them with a single, very strong password.

Chris will demonstrate how to synchronize the password database between a desktop computer and a smart phone. As well, he will show how the program can be configured to log on to web sites automatically.

Don't let your online accounts get compromised. It's easy and free.

The Zoom link will be live at 7:20 pm.
Join us at **https://tinyurl.com/opcug-meeting**.

The above link includes the meeting ID and password. However, if you are ever prompted for the information, use:
Meeting ID: **924 9556 0898**
Password: **opcug**

Instructions for using Zoom are provided here:
https://opcug.ca/wp-content/uploads/Zoom-instructionsv3.pdf

There will be a Q&A session after the regular meeting at approximately 9 pm and on the same video conference. Everyone is welcome to attend Q&A sessions and to ask questions about their specific computer-related problems.

Coming Up…

Next weekly Q&A sessions:

February 24
March 3

Regular Meetings:

April 14th

Sharing Photos (Lynda Buske, OPCUG)

This lecture will show you how to put your pictures up on line so they can be viewed by friends and family. See how to set up a shared site at Shutterfly.com with unlimited, FREE storage and how to customize your site. Learn how to add and organize both photos and albums and how to enable people to make comments. Learn why and how to reduce the resolution of images if you are emailing them, using a cloud service like Dropbox to share photos, etc.

May 12th

Typography (Chris Taylor, OPCUG)

Typography—the art and technique of arranging type—has been around for thousands of years and is constantly evolving. Good typography makes it easy to read and can be eye-catching. Bad typography can be distracting and hard to read.
Chris will outline the somewhat arcane terminology used. He will discuss some of the historical significances of type.

(click on the meeting titles for more details)

All scheduled events, including regular monthly meetings, weekly Q&A sessions, and OPCUG@OPL presentations, are posted on our website at https://opcug.ca/. All events are via video conference until further notice.

2021 CALENDAR

Meetings	Date	Time and Venue
Regular Monthly Meeting	Wednesday, March 10th	7:30 pm via Zoom video conference: **https://tinyurl.com/opcug-meeting** To see all scheduled events, visit http://opcug.ca/
Q&A Session	Wednesday, March 10th	Immediately following the Regular Monthly Meeting. (approx. 9 pm) on the same video conference.
Beer BOF (Wing SIG East)	Wednesday, March 10th	Enjoy a cold brew or other beverage in the comfort of your home during the video conference.

ARTICLE

Controlled folder access update

by Chris Taylor

In the April, 2018 issue of *Ottawa PC News* (http://www.opcug.ca/Articles/1804.pdf), I reviewed *Controlled Folder Access* (CFA), a feature Microsoft introduced in the 2017 Fall Creators Update for Windows 10. This is an update to that review and reflects changes to how CFA behaves in the ninth major update to Windows 10: v2004, released in May 27, 2020.

I think a lot about current cyber threats and how I can protect my computers and information from them. A significant threat is ransomware, which will encrypt your data files and demand a hefty fee for the decryption key. CFA was created to address this threat; it blocks unauthorized programs from modifying files in specific locations.

The best insurance from ransomware is a good backup. I run automated backups every night. But my backup drive is connected to my computer 24x7. Ransomware could encrypt my backups, rendering them useless. I could then recover from an off-site backup, but with my processes, that backup could be as much as a month old.

If you are interested in CFA, please read my first article on how to use CFA. One important difference from that review is that in order to get to CFA, you now run *Windows Security | Virus & threat protection | Ransomware protection*.

I found CFA had many problematic aspects, which I detailed in my previous review. Three years and five Windows 10 feature updates later, I count Microsoft as batting .500 in fixing CFA problems. Not bad in baseball; not so great in software problems.

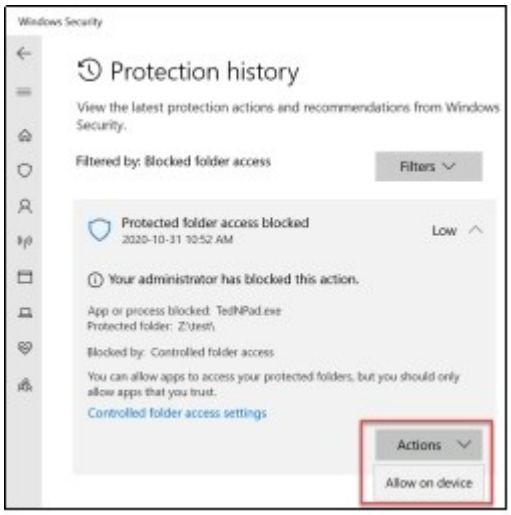
My first complaint was that you can't remove any of the default protected folders. That restriction remains.

My second complaint was about the opaqueness of what programs are blocked by default. Microsoft now says "Controlled folder access works with a list of trusted software. If an app is included in the list of trusted software, the app works as expected. If not, the app is blocked from making any changes to files that are inside protected folders. Apps are added to the trusted list based upon their prevalence and reputation."

Personally, outside of programs digitally signed by Microsoft, I don't want Microsoft to decide if they are "trusted". I ran into a peculiar example of a program Microsoft "trusted". I ran FotoSketcher: a photo filter program. I tried writing a modified image to a protected folder and got a toast notification that FotoSketcher had been blocked. But strangely, without doing anything to unblock it, when I re-ran FotoSketcher, it was able to write to the protected folder! Even worse, FotoSketcher was not showing up on the list of programs I had allowed to access controlled folders. It appears that Microsoft decided on its own that FotoSketcher is "trusted software". While I trust FotoSketcher, I want it to be me that makes that assessment, not Microsoft.

My third complaint was that Microsoft made it too complicated to let a blocked program write to protected folders. In this regard, Microsoft has done a stellar job in fixing things. The toast notification you get when a program has been blocked now has an option to unblock right from the notification.

Click on *Click to see settings* to be taken to the right place where you can unblock the program.



My fourth and perhaps most alarming complaint about CFA was that it appeared to base its blocking on the filename of the executable. When testing two blocked programs, if I unblocked one and then renamed the second to the name of the first, it was unblocked. This has been addressed and, while I have no idea what mechanism is used to determine if a program is blocked or not, simply having the same name and location is insufficient. I would hope it was based on a hash (which uniquely identifies a file) of the executable would be used.

But it is not just a hash. I discovered that when I unblocked a program and then moved it, it was blocked when run from that new location. If I allow a program on my computer to write to protected folders, I think it shouldn't matter where the executable is located. I reported all of my latest complaints through Windows Feedback.

For some Microsoft documentation on how CFA works, see https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-controlled-folders

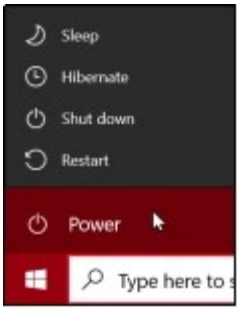
♦♦♦

ARTICLE

Fast startup in Windows

by Chris Taylor

Fast startup in Windows … starts Windows faster. Who woulda thunk? But exactly what it is doing has some implications that are not obvious. First, let's look at the options available when you click the Start button and choose *Power*.



- *Sleep* – keeps you signed in, all your programs/documents are kept open, turns off the display, and goes into a low power mode. When you want to use your computer again, press a key, move the mouse, or press the power button (depending on your computer). You will be back to the state your computer was in when you put it to sleep. You don't have to worry about losing work if your battery completely drains; Windows will go into hibernation mode automatically if the battery level drops too much.

- *Hibernate* – writes the current state of the computer's memory to the hibernation file and then shuts down the computer. When you restart the computer, it reads the hibernation file to return the computer to the same state it was in when you chose Hibernate, with programs and documents open.

- *Shut down* (if *fast startup* is enabled) – all programs are closed and users signed off. Then the state of the computer's memory is written to the hibernation file and Windows is shut down. When you next start the computer, it reads the hibernation file to return Windows to that state and presents you with the sign in screen.

- *Shut down* (if *fast startup* is disabled) – all programs are closed and users signed off. Then Windows is completely shut down. When you next start your computer, Windows is started by loading the kernel and drivers and you are presented with the sign in screen.

- *Restart* – same as "*Shut down* (if *fast startup* is disabled)", but the computer is then automatically restarted.

Note that there are two listings for *Shut down*; with *fast startup* enabled or disabled. Most computers have *fast startup* enabled and Microsoft says that is "recommended". I think the only computers that will have *fast startup* disabled by default are those that don't support hibernation. While *fast startup* will normally speed up getting Windows running, there are a few potential downsides.

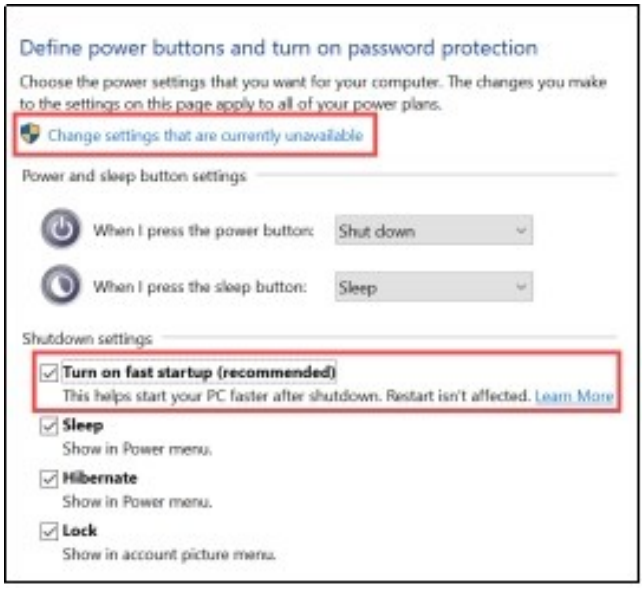
- Some updates require a true shutdown and they won't be applied properly if you do a shutdown with *fast startup* enabled. This problem can be bypassed by doing a *Restart* rather than *Shut down*.

- *Fast startup* locks the system disk when you choose *Shut down*. If you multi-boot with different operating systems, the Windows partition is not available from the alternate operating system.

- You might not be able to access BIOS/UEFI settings when you start your computer. If this happens, you can access them by choosing *Restart* rather than *Shut down*.

- If you use a solid state drive (SSD), *fast startup* writes to the hibernation file every time you shut down. These additional write cycles will reduce the life of your SSD, albeit possibly minimally. And it may only shave a few seconds off the time it takes to start your computer.

To toggle *fast startup* on or off, run *Control Panel* | *Power Options* | *Choose what the power buttons do.*



In the *Shutdown settings* section, if the options are not enabled, click *Change settings that are currently unavailable.* You can then enable or disable *Turn on fast startup*.

♦♦♦

Lawrence's Thoughts

Password Experts vs an old sage

By Lawrence Patterson
lawrence@opcug.ca

Thought I would warm up the crowd to Chris's upcoming presentation "KEEPING PASSWORDS SAFE" this March 10th, with a review of current experts' password advice and my impressions of the practicalities of what's being proposed.

Let's start off with the following humorous definition of the word Expert: "*A person with more data than judgment*". A perfect example of this is the infamous Windows 8 upgrade from Windows 7. As we're all aware now, it was a flop, not because of the intentions of well meaning experts analyzing years of how we used Windows, but because it was those same experts not realizing that just because the majority didn't use the Windows 7 menu as intended, didn't mean we wanted the menus to be replaced. And it didn't help that it took those same experts many months to finally realize how much we wanted the start menu to stay the way it was presented in Windows 7.

A further word to the wise, as we peruse the advice below, do consider that the baddies can be just as lazy and such are looking for the low hanging fruit (i.e. people who don't patch their systems or who use the same passwords over and over again). As such, following most of the recommendations below will provide sufficient protection from being hacked.

Do not use personal information. https://us.norton.com/internetsecurity-how-to-how-to-secure-your-passwords.html

- Ok, in one sense this is good advice, but having a secure password doesn't mean it can't be personal and therefore something unique and easy for you to remember. Just don't make it obvious and don't overuse it (if everything you wear has the colour pink in it, I would advise against making the word pink part of your password regimen).

Don't Recycle. https://www.consumerreports.org/digital-security/tips-for-better-passwords/

- Yes, practical advice. Although it is advised not to re-use any password you have ever created, we humans can be pretty stubborn when it comes to keeping things easy. There's nothing wrong in keeping things fresh by mixing up or misspelling the same phrases in a way that can be remembered.

Avoid common words and character combinations in your password.
https://www.cnet.com/how-to/9-rules-for-strong-passwords-how-to-create-and-remember-your-login-credentials/

- Those of you that are wordsmiths won't have a problem with said advice. Many of us are not. This is where password phrasing is useful in that stringing together many common words (mixing up the occasional characters with a numeric or symbol helps) will make it easy to think up new passwords as we go through life's experiences.

Don't tell anyone your password.
https://www.mcafee.com/blogs/consumer/family-safety/15-tips-to-better-password-security/

- Whatever your data is (and password - login credentials are just more data) you need a good backup plan. You do not want to be the fellow that forgot the password to his now very valuable bitcoin vault. Yes, make sure you absolutely trust whomever, but remember, it's just as important to make sure your passwords (and the device that contains them) are accessible by **someone** if not by you (and "passing on" is just one factor to consider).

Use a password manager and a random password generator. https://blog.avast.com/strong-password-ideas

- No problems with the first part of this advice - the 2nd part is what I have concerns with. As much as password managers provide good support for most login needs, they won't work with all. And I don't know about you, but trying to type in a totally random set of characters can be frustrating. Like most things in life, don't be lazy about your password generation, and use life experiences to create unique sayings that can be remembered.

Avoid using two factor text - SMS (short message service) authentication. <various>

- This is technically true, especially with SIM swapping a major concern. Unfortunately, not all websites use an Authentication service (Google & Microsoft being prime examples) and if all that is offered is text - SMS, take it, as it is better than password alone.

Remember that using a unique, memorable, funny phrase for your password phrasing will help keep you ahead of the baddies.

Take care.

THROUGH THE LENS

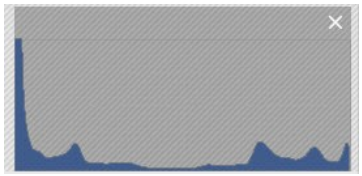
A guide to digital photography for computer enthusiasts. After the click of your camera, you're only half done!

How to use photographic histograms

by Lynda Buske

A photographic histogram is a graphical representation of the distribution of the various levels of brightness in your photo. If you think of a black and white photo, the histogram displays the frequency of pixels that are pure black (no brightness) those within the grey spectrum (mid-tones) and those that are pure whites (brightest sections).

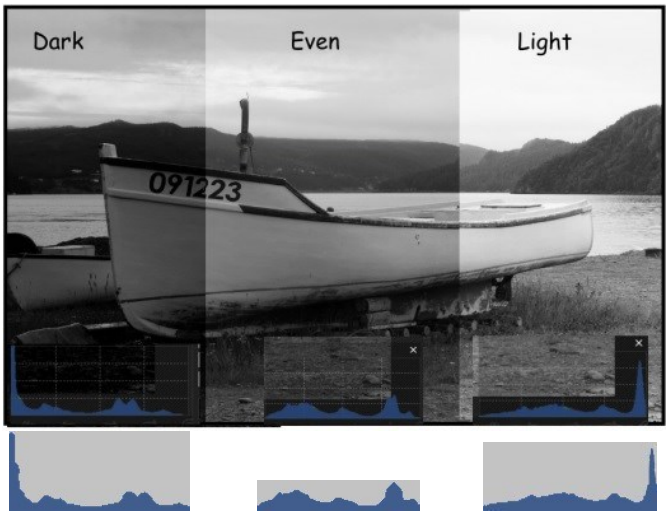
In the histogram below, the far-left side represents the amount of pure black and the far-right side is the amount of pure white. In the example, you can see there is a lot of pure black (high on the Y axis) indicating that perhaps the photo needs to be lightened.

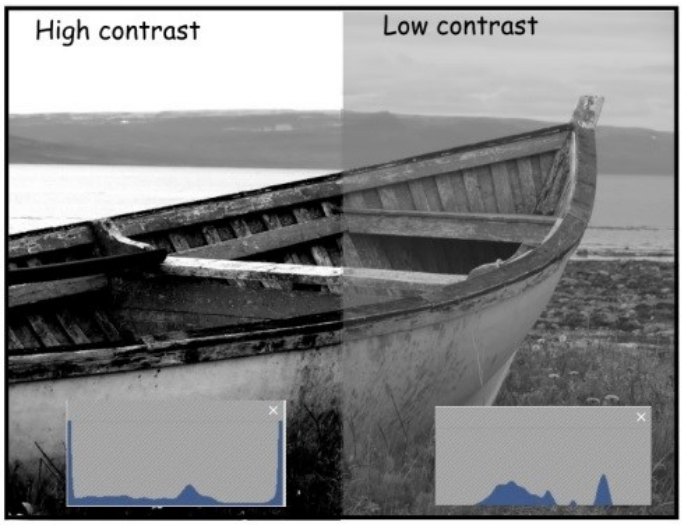


Histogram of dark photo

Some cameras provide a histogram view while taking a photo (or while reviewing the photo in-camera) so necessary adjustments can be made on site. If your camera doesn't have this feature, the exposure can be adjusted (to a certain extent) with photo editing software during post processing on your computer.

A lot of pure black and pure white in a histogram usually indicates a photo of high contrast. If you wish a more even distribution, you can lighten shadows and darken highlights causing some pure black and white areas to shift to grey. If you prefer instead to add contrast, you can do the opposite or set black and white points if your software allows. See examples with accompanying histograms below:





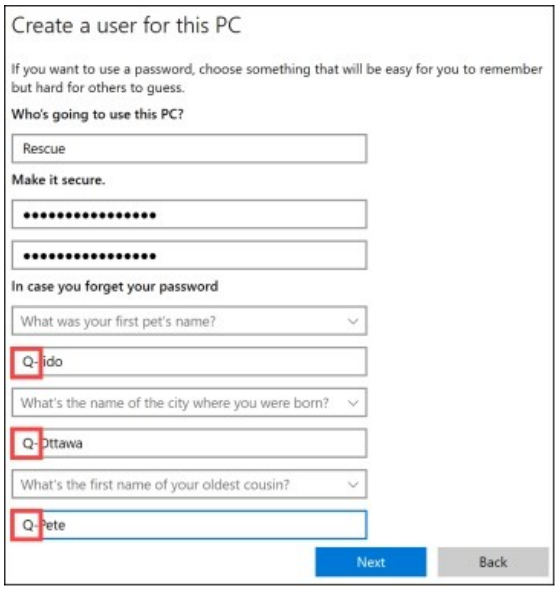
There is no right or wrong when adjusting light; it simply needs to reflect what you want the image to look like.

In some circumstances the areas of pure black and white may not be adjustable in post processing. This is called clipping. In this instance, your camera sensor is saturated (if clipping occurred in the highlights) or the sensor was unable to capture any information (if clipped in the shadows). Even if you don't have a histogram on your camera, it may indicate overexposure by blinking areas in the playback mode, however there will be no indication of underexposure. In some cases, it is unavoidable (e.g., having the sun in your photo) but it is usually best to limit areas of extreme darkness or brightness to small areas of your image.

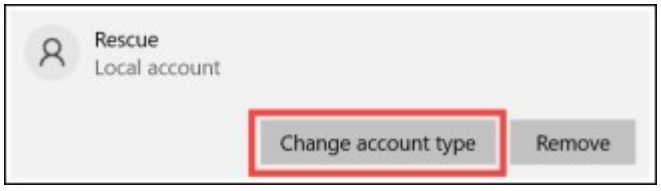
Histograms usually display information for three primary colors – red, green and blue – and are known as RGB histograms. Coloured histograms can show if clipping is happening in only one of the colour channels.

*Lynda regularly gives presentations for the OPCUG at the **Ottawa Public Library** (https://opcug.ca/opl-presentations/).*
This article is also in PDF format on the OPCUG website (https://opcug.ca/digital-photography/).

Rescue account *(continued from page 1)*



Back at the *Accounts* screen your new account will be listed in the *Other users* section. Click on the account name and click the *Change account type* button. Choose *Administrator*.



Sign in to Windows using the new account at least once to complete the creation of the profile for that account. If you ever have a problem with your normal account, you can sign in using this account and try to fix the problem with your normal account. Even if you can't fix the problem, you can always get your data files and create a new account.

♦♦♦

Review of the OPCUG Financial Records for the year 2020

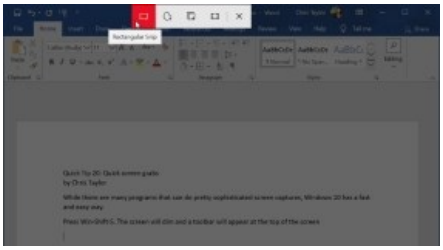
Thanks to Alan German for another year of exemplary bookkeeping. I did not find any discrepancies in the General Ledger, Documentation and Bank Statements.

Richard Aylesworth
January 31, 2021

The Board of Directors would like to thank Richard for his thorough review of the club's accounts.

Quick Tip 20: Quick screen grabs *by Chris Taylor*

While there are many programs that can do sophisticated screen captures, Windows 10 has a fast and easy way.



Press Win-Shift-S. The screen will dim and a toolbar will appear at the top of the screen. Select from four options to capture; *Rectangular Snip*, *Freeform Snip*, *Window Snip*, and *Fullscreen Snip*.

For the first two, click and drag to select an area. For *Windows Snip*, point to a window and click. For *Fullscreen Snip*, click that option on the toolbar.

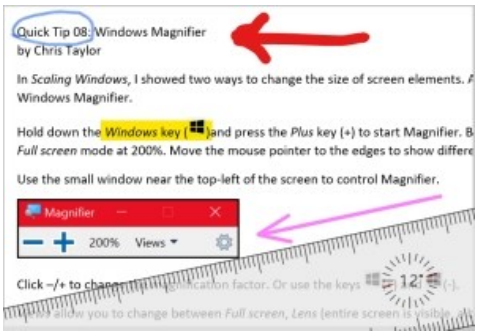
The image of the selected area will be copied to the clipboard. You can then paste it elsewhere, such as a document or image editor.

It is worth noting that most other screen capture programs can't do a *Freeform Snip* which allows for an irregularly shaped capture.

Quick Tip 21: Snip & Sketch *by Chris Taylor*

In Quick Tip 20, I described how to do a fast screen capture using Win-Shift-S. *Snip & Sketch*, found on the Start menu, provides additional capabilities.

- optionally delay the start of the screen capture by 3 or 10 seconds.
- when the capture is done, it opens in *Snip & Sketch.* Modify it using drawing tools; *Touch writing*, *Ballpoint pen*, *Pencil*, *Highlighter*, and *Image crop*.
- to draw straight lines, use the *Ruler* tool. Rotate the ruler with the scroll wheel on your mouse or two fingers on a touch device.
- save your work of art as a PNG, JPG, or GIF file. Share it by email or directly to *nearby devices*. Or copy it to the clipboard and paste it into a document or image editing program.



OTTAWA PC NEWS

Ottawa PC News is the newsletter of the Ottawa PC Users' Group (OPCUG), and is published monthly except in July and August. The opinions expressed in this newsletter may not necessarily represent the views of the club or its members.

Member participation is encouraged. If you would like to contribute an article to Ottawa PC News, please submit it to the newsletter editor (contact info below). Deadline for submissions is three Sundays before the next General Meeting.

To receive the monthly newsletter by email, send an email to:
opcug-newsletter+subscribe@googlegroups.com (leave subject and body fields blank)
You do **not** need to create a Gmail or Google Groups account.

To subscribe to other OPCUG Google Groups member services, go to:
https://opcug.ca/google-groups-how-to/

Group Meetings

OPCUG meets on the second Wednesday in the month, except July and August, at the Riverside United Church, 3191 Riverside Drive, Ottawa. Parking is free at the church. OCTranspo bus #90 stops nearby. Details at https://opcug.ca/venue/.
(NOTE: Due to COVID-19 safety guidelines, all our events are via video conference until further notice. Details at https://opcug.ca/venue/)

Meetings are 7:30–9:00 p.m. followed by a Q&A Session until 10 p.m.

OPCUG Membership Fees:	$20 per year
Mailing Address:	3 Thatcher St., Nepean, Ontario, K2G 1S6
Web address:	**https://opcug.ca**
Follow us on Facebook:	**https://www.facebook.com/opcug**
Follow us on Twitter:	**https://www.twitter.com/opcug**

President and System Administrator
Chris Taylor — **chris.taylor@opcug.ca** — 613-727-5453
Meeting Coordinator
Lawrence Patterson — **meetings@opcug.ca**
Treasurer
Alan German — **alan.german@opcug.ca**
Secretary
Gail Eagen — **gail.eagen@opcug.ca**
Membership Chairman
Mark Cayer — **mark.cayer@opcug.ca** — 613-823-0354
Newsletter
Brigitte Lord (editor/layout/e-distribution) — **brigittelord@opcug.ca**
Public Relations
Lawrence Patterson — **PR@opcug.ca**
Facilities
Bob Walker — 613-489-2084
Webmaster
Brigitte Lord — **webmaster3@opcug.ca**
Privacy Director
Wayne Houston — **privacy2@opcug.ca**
Special Events Coordinator
(Mr.) Jocelyn Doire — **jocelyn.doire@opcug.ca**

Q&A HAS GONE ON-LINE!

Because of the pandemic, the OPCUG is holding weekly Q&A sessions in Zoom video-conferences.

Join us every Wednesday at 7:30 pm to discuss computer issues. Questions (and answers) on any computer-related issue are welcome. Or, do you have a favourite computer program or topic that you would like to share with the group? Send your questions, answers, or the details of what you would like to share to: SuggestionBox@opcug.ca.

Everyone is welcome to attend Q&A sessions and to ask questions about their specific computer-related problems. Join us at: https://tinyurl.com/opcug-meeting (if you use the Zoom client, the meeting ID is **924 9556 0898** and the password is **opcug**).