THE COMPUTER CONNECTION
SAUK COMPUTER USER GROUP

MAY 2020

VOLUME THIRTY
NUMBER FIVE

INSIDE THIS ISSUE:

The Whiteside County Senior Center is still shutdown due to the Cornonavirus. Hope you aren't going crazy with cabin fever, but staying safe. We may try using the Zoom app from APCUG to have some type of remote meeting later this month. We can join a virtual conference, this Saturday, May 2nd sponsored by APCUG. See forwarded email for details.

Joe Fornero

Windows FREE Snip and Sketch Tool

By Jim Cerney

The new Windows "Snip and Sketch" tool was part of the Windows 10 October 2018 update. This tool is intended to REPLACE the old "Snipping Tool" of previous Windows editions. But they (Microsoft) did something to actually help us users this time – they kept the old tool! So you can play and learn the new Snip and Sketch and keep the old Snipping Tool too! Maybe they learned not to force users into using updated or changed apps right away – we need time to adjust and learn, right? Everything you could do in the old Snipping Tool you can do in Snip and Sketch, plus you get a few more tools and options. Thankfully these new additions are easy to see and use, and they can be ignored if you do not want to use them. Microsoft promises more options to come. Be sure to search Google for videos on how to use Windows Snip and Sketch! I am including here only the basic options. Click on the Windows logo in the lower-left corner of your desktop and you will find Snip and Sketch in the alphabetical list of apps that appear. It is not inside the Windows Accessories folder of apps (where the Snipping Tool still remains). I recommend dragging this app to your desktop screen to always keep it handy. But you can also open it anytime by holding down the Windows key + Shift key + S on your keyboard. Upon opening the app, your whole screen goes gray and you will see the small controls rectangle at the top. Here you select HOW you want to select what you want to snip or capture. From left to right you can select a rectangular area, freeform selection, the entire window, or your full screen. If you select the rectangle, you drag your mouse on the screen to select whatever you want. As soon as you release your mouse – presto, your selected image has been captured and saved on the clipboard to do with whatever you want! You can open a Word document for example, place your cursor where you want, and "paste" your clip right in your document. Or you can open the Windows Paint app and you can "paste" it there if you want to do more editing. At the same time that your snip is placed on the clipboard, you will also see a message stating that you can edit, draw, or markup your selection. Click to do that and Snip and Sketch opens in its own window with its own menu of options. Various easy marking tools are available for you to play with and try. There are highlighters and markers, and clicking on the down arrows will open things like color choices, etc. Once you have "sketched" on your "snip" you can save it as a ".jpg", ".png", or ".gif" format by clicking on the old floppy disk save icon and selecting the file type you want. The new Snip and Sketch is easy to use and very helpful for saving and sketching on any image on your screen for any purpose. Why not give it a try?

Author: Jim Cerny, Forums Coordinator
December 2019 issue, STUG Monitor
www.thestug.org
jimcerny123 (at) gmail.com

Club Information

Sauk Computer User Group
PO Box 215
Sterling, IL 61081-0215

Art Bendick - President
abendick278@gmail.com

Website
www.saukcomputerusergroup.org

SCUG Email

saukcomputerusergroup@gmail.com

Editor and Printing done by:

Joe Fornero

Member of apcug

An International Association of Technology & Computer User Groups

Perform your own vision check at home for free

By Dave Johnson-CNet contributor

Any opportunity to spend less time in a doctor's office is welcome, but right now -- in the middle of a pandemic -- it's not really even an option for routine visits like an eye exam. That's OK; if you're in need of new glasses, you can skip the optometrist entirely and do your own eye test at home. Right now, EyeQue is offering the Personal Vision Tester for free when you apply discount code **STAYHOME** at checkout. That'll save you $35 off the current price of the device. When you use the code, though, you don't get free shipping. EyeQue charges you $6 for that, so I suppose that you're getting the package for six bucks. Which is still an awesome deal.

Before I get to the details, let me explain how to claim your mostly free PVT. Don't enter the discount code on the first checkout page, or you'll have the same experience I did: It'll reject the code. Instead, go through the whole checkout flow and enter the discount code at the end, on the page you enter your address and billing information. That's where you should see the price drop from $35 to $6.

The Personal Vision Tester is a device that works in conjunction with your smartphone to test your vision, one eye at a time. In just a few minutes, it can measure the lens power needed to correct your nearsightedness, farsightedness and astigmatism as well as any near-vision additional power you might need. The app generates eyeglass numbers -- what your optometrist would typically scribble down for you to take to the eyeglass center -- that can be used to order glasses online. The numbers can be used for single-vision glasses, bifocals and even progressive lenses.

The first use of the EyeQue PVT is free, but after that, you'd generally need to pay a $5 annual fee for each family member who wants to use the device and the service. But if you sign up before the end of April, EyeQue will waive that those annual user fees for the first year as well.

The bottom line is that armed with the PVT, you can get a complete set of new glasses with lenses adjusted for your current vision, without leaving the house, and you only had to pay a total of $6 for everyone under your roof.

The Next Drawing

The regular drawing for next meeting whenever that happens, will be $50 gift certificate from Forest Inn, a $25 gift card from Pizza Ranch and a local family restaurant and a 1Tb flash drive, plus some misc. items.

Joke from Joe II

A Recent Scam Experience

By Jeff Wilkinson

Recently I received the "Social Security" scam call, the recorded message informing me that I should call an 800 number because my account was about to be suspended. I decided to play along and see what the suspected scam pitch was; since I was 99.99% sure that Social Security doesn't call you.

I called the 800 number, exclaimed my surprise that there was a problem and breathlessly asked what the problem was. The responder, "Officer Ronald Smith" explained, in an almost unintelligible accent, that he was a senior investigator and I should get a pencil and paper and write down his name and badge number, which he proceeded to give me. He then went on to outline the "problem" which included seven bank accounts opened under my social security number. He said the accounts had been used for money laundering and an investigation was underway with an arrest warrant about to be issued. In addition, there were multiple credit cards also under my social security number which had been linked to illegal activity.

"Officer Smith" then asked if these were my accounts. Upon my answering No, he explained he needed to know how many bank accounts and their approximate balance and how many credit cards I had and their credit limits. I responded with fictitious information of course. He advised me that this conversation was being recorded and I was repeatedly told to listen to his instructions very carefully. When I told him in a frightened, exasperated voice that the accounts he described were not mine, he wanted the local police department phone number so he could call to see if we could clarify some additional information. I gave him a fake phone number and he put me on hold; he came back a short time later and said that the number I gave him was incorrect!

"Officer Smith" then told me I could get the number from the yellow pages or Google and said he would wait while I looked it up. When I asked why *he* didn't have it, he exclaimed he did but was not allowed to give it to me. I looked up the number in the city I had claimed to live in and gave it to him; he again put me on hold and returned a couple of minutes later. He said he had a senior investigator on his other line, and she would be calling me. I was to put him on hold when she called. Then my phone rang! The call was from the number I had provided which was the number of the Palo Alto, CA police department! "Officer Smith" told me to put him on hold and to add the new caller to the conversation.

Throughout this entire 22-minute ordeal he had not yet asked for any money or access to my computer. I was tempted to continue the charade, but the language barrier became intolerable along with the level of minutia, so I ended the calls. Almost immediately my phone began ringing from an unknown 800 number, over and over until I blocked the number. I believe the ploy was to obtain my information such as date of birth, address and social security number so they could steal my identity.

Although I didn't get far enough to determine the full scam, I was very surprised that they added so much credibility by calling me back and "spoofing" (faking the Caller ID) of the actual police department number I had provided and they had checked!! As we know, spoofing a phone number occurs often on junk and scam calls. This specific trick could cause a reluctant mark to falsely think they were maybe being too cautious. The scammer may attempt to retrieve your date of birth, name, address and partial social security number by asking throughout the conversation for you to verify the information. With those items, it is possible to initiate a change of address and phone number with Social Security and then redirect your direct deposit to a different bank.

Having repaired two cases of scammers gaining access to computers that week, one which was able to gain bank information and withdraw a four-figure sum of money from a retiree, I was interested in experiencing the actual pitch. It can't be stressed enough that allowing remote access to your computer from random phone calls, emails or web page screens is to be avoided. Also do not release any personal information to unknown callers no matter how official they attempt to sound, with so much information available in the public domain many times only a small about of additional information is needed to initiate an identity theft.

By Jeff Wilkinson, President, Sun City Summerlin Computer Club, NV
December 2019 issue, The Gigabyte Gazette
www.scscc.club
Clearmeadows11 (at) gmail.com

Back to Basics: File Extensions – Helpful and Not

By Jim Cerny

So someone sends you a file attached to their email – you try to open the file and you can't, why is that? I mean they obviously could open the file on their computer, why couldn't you open it on yours? Unfortunately, this is the frustrating part about FILE EXTENSIONS (also known as "file types").

If you use a program to CREATE a file, it is nice to have the SAME PROGRAM to open or work with the file you created. Naturally, if you use your computer to create a file then your computer has the program needed to open the file later. The problem is when someone creates a file on their computer and sends it to you – you need to have a program that can open the file on your computer. Let's look at one example:

I have the Microsoft Word app (or program) on my computer and I create a new document with it. I save the document as a file, and the computer assigns it a "file extension" or "file type" of ".docx". The file extension is always the last three or four characters of the file name right after the dot. This indicates that this file was created using the latest version of Word. If I send this file (as an attachment to an email) to someone else and they do NOT have Word, they cannot open the file!

It is an option in Windows whether to display the file extension, so your computer may not show you the file extension as part of the file name. To see the file extension when you use File Explorer, open the File Explorer app, click on the "View" menu tab and check the box labeled "File Name Extensions". This will display the file extensions (file type) as part of the file name for all files.

Things have changed over the past few years as there are more options to open the file to READ it or to EDIT it. Your computer may suggest some internet sites or free apps that may be able to open the file for you.

A good app like Microsoft Word may allow you to save your file as a different type of file – so you can pick one that is easier for more people to open. You could save it as a ".pdf" or ".rtf" file type if you want. A ".pdf" file can be opened by many apps but usually, the contents, or text, of the file can NOT be edited, only read. The ".rtf" file type (Rich Text File) can also be opened by several other apps and can be edited, BUT the text will have lost any formatting or options used in Microsoft Word.

Are you working with photo files? Most photos or pictures today are saved as a ".jpg" file type and any app that can open or work with photos will be able to open this file. That's nice.

Here are just a few of the most popular file extensions (types):

.doc or .docx – Microsoft Word

.html – webpage

.jpg – picture or photo image

.pdf – a document file that can be open or read by many apps but cannot be edited

.rtf – rich text file that contains formatting (the Wordpad app creates these files)

.txt – plain text file will no formatting

.xls and .xlsx – Microsoft Excel spreadsheet

There are probably many thousands of different file types, but thankfully you do not have to know them all. If you have any questions about a particular file type, just Ask Google and you will find out what apps could have created the file and which apps can open or work with that file.

I know this all sounds a bit confusing, but you should only run into a problem when you try to open a file that you did not create on your computer. Should this happen you may have to contact the person who sent you the file and ask them to send it to you again as a different file type – one that you know you can open.

Hopefully, you will become comfortable with the most common file types that you use. Remember you can always Ask Google for help!

Author: Jim Cerny, Forum Leader, Sarasota Technology Users Group, Florida
October 2019 issue, Sarasota Monitor
www.thestug.org
jimcerny123 (at) gmail.com

Staying Safe Online - A Rational Approach

By Pam Holland

We get *many* questions about online security. And we often get brought in to help clean up after an incident of fraud. As a result, we have developed what we consider 'a rational approach' to online security. Rather than focusing on all of the possible risks, we urge our clients to first address factors that present the highest risk. With respect to protecting from online risk, we apply the 80/20 rule. In short, 80% of the risk comes from 20% of the possible causes. In other words, if we just address the top possible risks, we eliminate the most common ways people are victimized online.

We suggest thinking about protecting your data as you might approach protecting your home. We all take reasonable steps to secure our homes; we lock our doors, close windows, and leave lights on. The goal is to *reduce* risk as eliminating risk is nearly impossible. The same is true in our digital lives. Taking small measures goes a long way towards keeping us safe, but it is nearly impossible to eliminate all risk.

Consider your personal risk factors. This is not unlike assessing your home for the risk of a break-in. If you live on the top floor of a high-rise, leaving your windows open does not present the same risk as if you were on the ground floor. With respect to your tech, do you have people regularly in your home that you need to protect your data from? Do you bank online? Do you have sensitive financial or other documents on your computer? Do you only use your computer for email? Do you or a family member have cognitive issues that might make you more vulnerable to fraud?

Based on our experience seeing the aftermath of fraud, taking steps to cover these six items will go far towards your online safety:

Use Unique Passwords. I know this isn't what many want to hear, but unfortunately, the risk in re-using the same password is increasing. A few years ago, the common advice was to create a unique password that was hard to guess. Today, the risk is not that someone will guess your password - the fraudsters already know it. Large corporate data breaches (e.g., Equifax and Marriott) may have put our passwords into the hands of fraudsters. If you typically use the same password for multiple accounts (and worse if you have used it for years), fraudsters are more likely to be able to access your other accounts. To return to the home analogy, it is as if you have given out your

Staying Safe Online - A Rational Approach (cont.)

key to numerous people over the years - it's now time to change the locks. Some options:

Use a password manager - This might mean allowing Chrome or your Mac to save your passwords or using a third-party service like LastPass. I am often asked if they are safe. The only answer that I can really give is that they are safe until they aren't. I have chosen to allow my passwords to be saved on my Mac. For me, it has reduced my risk (because I don't need to reuse passwords) while (somewhat) saving my sanity. *But a caution: If others have access to your computer, they may be able to view your passwords.*

Write them down - This works well for many. Of course, it is important to keep the passwords in a safe place.

Develop a unique naming convention - For example, you might take a short phrase that you will remember then add something unique to that account site.

Make your passwords safer by using two-step authentication - This is an option in most online accounts (email, Facebook, banking). How does it work? When you log in from a new device or location, you'll be sent a code via smartphone or landline. This makes it harder for fraudsters to log into accounts even if they have your password. To set up, go to the account or privacy/security settings in your online accounts.

***Never* Allow Remote Access to Your Computer** (unless you have sought reputable assistance like from Tech-Moxie 😉). Fraudsters would like nothing more than to gain access to your computer. They pretend to be from Amazon, Microsoft, Apple or another company you know well, offering to "help" you with a service issue. Assume fraud if you get an email, call or computer alert from a familiar company or government name. Once in your computer, they can access accounts and passwords. We have seen quite a lot of damage from these schemes.

Think Before You Click. Assume links in the email

are fraudulent unless you can prove otherwise by checking with the sender. Fraudsters easily create emails that look like they came from a friend, bank or even the government. The email might be friendly (*"Hey, check this out"*) or intended to provoke anxiety (*"your Amazon order for a diamond ring has just shipped"*) or seemingly innocuous ("*your computer needs service"*). Fraudsters are hoping to get passwords or other personal information. Remember, customer service doesn't come to you! Instead of clicking, go to the website directly via the internet.

Beware of Pop-Ups A "pop-up" is a window or box that opens on your computer - often with a warning. Do not believe pop-up warnings claiming there is a problem with your computer. Never give them remote access. Warnings may claim to be from Microsoft, Apple or another company you are familiar with. What to do? Shutdown and restart your computer and the pop-up should be gone!

Update Devices Regularly. Companies like Microsoft, Apple and Google lookout for software vulnerabilities that fraudsters can take advantage of. They issue updates to fix these issues. Some devices may be set to automatically update, but others may require you to take a specific action. This applies to computers, tablets and smartphones.

Beware the Telephone. Scams change but follow common themes. Neither Apple nor Microsoft will call to alert you of problems. Government agencies such as IRS, Social Security Admin nor the local Sheriff will call claiming you owe money. If you are still in doubt, hang up and call the agency from a number that you have looked up independently.

We hope you find these tips helpful - and as always, we are here to help!

Pam Holland, Founder and President, Tech-Moxie
December 2019
https://www.tech-moxie.com/
Pam (at) tech-moxie.com

There will be a Question & Answer Session starting at 1 PM the next time we meet. Bring any questions you have about your computer or problems you may be having. It will be conducted by: **Art Bendick & Neal Shipley**

The next meeting of the Sauk Computer User Group will be

?

Question & Answer : 1 PM

Business Meeting : 1:30 PM

Presentation: 2:00 PM

Place: **Whiteside Senior Center**
1207 West 9th Street
Sterling, Illinois 61081

Neal Shipley will be doing the presentation with videos from the 2020 Las Vegas Consumer Electronics Show