January 2020 Vol. XXXVI Issue I

The Space Coast PC Journal

SEASONS GREETINGS FROM YOUR BOARD OF DIRECTORS

Can you believe that we're already approaching another Christmas?!!
The party is scheduled for December 14th, from 1-4 PM.
Once again we'll be holding it in the clubhouse at the Merritt Towers.
If you haven't been there before, it's on South Sykes Creek Parkway
on the east side of the Merritt Square Mall.
We'll provide subs, meat, cheese and veggie trays, bread for
sandwiches, cake, soft drinks, and coffee.
If you wish, bring a favorite appetizer, side dish, or dessert.
Our President , Dan Douglas, and his better half, Gail are in charge
of those
things the club is providing. Call Dan if you have any questions
regarding the food at 321 301-1075.
Curt Potsic, our Webmaster is receiving RSVP's
If you haven't told him you intend to come, please do so ASAP.
321-632-7185 or cmpotsic@att.net
Come on out and share the fun! Get better acquainted with your
fellow members. Talk about something other than computers for a
change.
Anyone wishing to participate in the fun White Elephant gift exchange
should bring a wrapped gift ($10.00 value), new or recycled from home.

map on page 5

The Monthly Publication of the

Visit Our web Site at www.scpcug.com**SEASONSSA**

Space Coast PC Users Group, Inc.
Users Helping Users

January 2020 Vol.XXXVI Issue I

Editors Emeritus: Lois Hoover, Peter Gaul, Dan & Peg Currie

Journa L st aff

Editor	Ron Ingraham	321-777-2578
Database	Ron Ingraham	
Circulation	Ron Ingraham	
Electronic Journal	Ron Ingraham	
Proof Reader	Lori Ingraham	

....

All work on the Journal is performed by unpaid volunteers.

submitting articles to the Journal

We encourage all of our members to submit original computer-related articles for publication in

The Space Coast PC Journal.

Writing a Product review

It is really not that difficult to write a good review for *The Space Coast PC Journal*. These guidelines will help you get started:

Product information

- List the product name, release level, and manufacturer.

use

- What does this product do?
- How easy is it to learn and use? Is it for beginners or does it have advanced features?
- List and describe some of the features. If this is an upgrade, what is new to this version?
- What did you like or dislike about it?
- Did you have to call Customer Support? What for? Were they helpful?

installation

- How much disk space did the product take?
- How long did it take to install?
- Was it difficult to install?
- Specify requirements such as: DOS level, Windows level, Windows type, etc.

recommendations

- Would you recommend this product?

Remember these are guidelines. They are not meant to be all-inclusive, nor should they limit your creativity. But all of them should be included as part of your article. Then the review will practically write itself!

Preparing your articles

To assist us in incorporating articles into the *Journal*, it would be helpful if certain minimum standards were followed. Use this quick-step guide:

format: The preferred format is ASCII text files.We can also work with other formats, but check with the editor before using them.

text: Single-space the text—even between paragraphs. Don't indent paragraphs. Use hard returns only at the ends of paragraphs.

Use only one space after periods, colons, and question marks. Follow standard capitalization rules.

Use left justification only. Do not right justify or block your text. (Word processors add extra spaces between words to justify the text and each of those extra spaces must then be removed.)

Graphics: The preferred format for graphics accompanying your text is TIFF—in separate files from the text. Embedded graphics are not useable. Most image editing programs have a "resize" option to alter the size of graphics. Please try to keep your graphic file sizes to around 1 meg in size. Call the editor if you have questions.

Be sure to include your name and phone number so we may contact you if we have any questions. Anonymous articles will not be published.

Submit your article by uploading the file to ringram728@earthlink.net or bring your disk and hardcopy to the Monday meeting or mail to:

Editor, SCPCUG Journal
Space Coast PC Users Group, Inc.
1360 Mayflower Avenue
Melbourne, Fl 32940-672

3Articles must be received by the 28th of the month to appear in the next issue, and all are, of course, subject to editing. □

From The Editor

I frequently have occasion to browse the older issues of the Journal looking for past similarities in articles or activities. In doing so I often run across input from presidents at the time.

I won't attempt to name them, though many of you would surely remember them. Many of them have passed away. I have no intention of denigrating their contributions to the group, just suffice it to say that they varied based on their background .

What I wnat to stress is that we have been very fortunate to have had such people willing to devote their time and energy for the benefit of the group.

Which brings me to our current Pressident, Dan Douglas.

The main thing is that we have never to my recollection had one with a background such as his. Connection to the software side dating back to the 70s and more recently the hardware side, which enables him to provide assistance to those in need in both areas.

We are truly fortunate to have him serving the group.

Ron Ingraham, Editor

The Space Coast PC Journal
Published monthly by the
Space Coast PC Users Group, Inc.
1360 Mayflower Avenue
Melbourne, Fl 32940-6723

Those who have listed an e-mail address would prefer to be contacted by e-mail rather than by phone whenever possible.

CLUB OFFICERS

President	Dan Douglas	datadan@msn.com	301-1075
Vice President	Larry Bennett	lbennett@qualitek.biz	259-2400
Secretary	Harry Pearson	harrymp@cfl.rr.com	868-1814
Treasurer	Irene Nelson	irenelnelson@gmail.com	806-4032
Journal Editor	Ron Ingraham	ringram28@cfl.rr.com	777-2578
Web Master	Curt Potsic	cmpotsic@att.net	632-7185
Membership Chairperson	Linda Glassburn	glassburn@earthlink.net	.216-334-7555

STAFF MEMBERS

Hospitality	Barbara Mead
New Member Orientation	OPEN
Orientation Hostess	OPEN
Publicity	Larry Bennett
Help Desk	OPEN
Facilities	OPEN

HELPLINES

Internet/HTML	Curt Potsic cmpotsic@ att.net	632-7185
Windows10	Curt Potsic.cmpotsic@att.net	632-7185
General Computer Us	Tom Marr Calling Hours 10-6 yjm1938@yahoo.com.	338-5414

.

Professional also includes DriveScrubber, a utility that can securely

if there is a progam not listed that you feel comfortable with, let us list you as one of our helplines contact ringram28@cfl.rr.com

The SCPCUG Home Page is at:
http://www.scpcug.com
Check it out!!!!!

In This Issue

Feature Aticles

Rgular Aticles

Notices

Presentation
December 14, 2019

Christmas Party
Recreation Building
Merritt Towers Condos
Sykes Creek Parkway
East of JC Penney
Merritt Square Mall
12-4 PM

Bring Some Friends

Security – June 2019

By David Shulman, Director, Weekly Update co-editor, intergroup liaison, and aco-organizer of WPCUG's Meetup, Westchester PCUG, NY

June 2019 issue, Westchester PC News

www.wpcug.org
intergroupliaison (at) wpcug.org

Malwarebytes, the protection software you can run alongside your antivirus, has reported that personal attacks are down this year. Cause for celebration? NO! "The Malwarebytes Labs Cybercrime Tactics and Techniques Q1 2019" report found businesses at the butt end of a bad joke. In just one year, threats aimed at corporate targets have increased with Trojans, such as Emotet, and ransomware in particular revving up in the first quarter.

Included in the report is analysis of sharp declines in consumer cryptomining and other threats, further cementing the shift away from individual targets and toward businesses, with SMBs suffering because of lack of resources.

"Consumers might breathe a sigh of relief seeing that malware targeting them has dropped by nearly 40 percent, but that would be short-sighted," said Adam Kujawa, director of Malwarebytes Labs. "Consumer data is more easily available in bulk from business targets, who saw a staggering 235 percent increase in detections year-over-year.

Cybercriminals are using increasingly clever means of attack to get even more value from targets through the use of sophisticated Trojans, adware, and ransomware." Read more here: https://press.malwarebytes.com/2019/04/25/malwarebytes-q1-cybercrime-report-emotet-and-ransomware-attacks-renew-focus-on-enterprise-trojan-detections-grow-200-percent/
http://bit.ly/2wprohB

Delivery scam—revived from a decade ago and more clever now.
Watch out for this one! A delivery service calls you to verify that your address is correct because they have a delivery for you. Then a delivery truck pulls up and the uniformed driver carries a basket of goodies to your door. He says that he knows you got a verifying call and has your package. As you are reaching for this, he says that he must verify that it's you because it contains alcohol (or some such) and asks that you produce a credit card that can be scanned so he is protected from an accusation that he delivered to a friend of his—"but don't worry, it's only for verification." If you scan your card, hundreds of dollars will be charged to your card before you can blink.

Order confirmations in your inbox—Have you received an email confirming a purchase you didn't make? Is there a link at the bottom labeled "Report a Problem!" or "Payment Resolution"? Don't click anywhere in this email. Just delete it.

Affinity offers--These are offerings that pander to an interest of yours: knitting, car racing, airplanes, travel, food, diet, boating, whatever. How do they know so much about you? Over the last few years, so many companies, so many credit companies, so many special interest venues, etc., have been penetrated that a surprising amount of detail is known about you. As time goes on, and your life becomes more connected, and more data is aggregated, and less restriction is placed on this collection, your life is literally becoming an open book.

HOW DO YOU PROTECT YOURSELF (ASIDE FROM MOVING TO MARS)?—My suggestion is this: everything you get by email has a sender's email address. Examine it by either hovering over it with your cursor or clicking on it to reveal it. If it has no relation to the content, it is spam. Now what happens if the address might be legit? Contact the company directly. Don't use a link in the email, but get a good link online, or a telephone number.

WHAT ELSE CAN YOU DO? Protect your privacy! Use a private window for browsing, use a VPN, use a disposable credit card number (yes, they exist from some credit card issuers), use an email address that is disposable (Yahoo and Gmail have them) for a particular purchase that forwards to your main email. Don't freely supply your email to every site you visit. Use a junk email account for that. Yes, YOU can have a junk email address for your own use.

PLEASE—CHANGE YOUR PASSWORDS AND MAKE THEM LONG AND UNIQUE. Remember that all your precious online and electronically stored "stuff"—your pictures, important papers, memories—all of it—can disappear FOREVER if you do not have a good, verifiable, disconnected BACKUP. ❑

From the Cashier's Cage

Financial Report for Month
Ending November 30, 2019

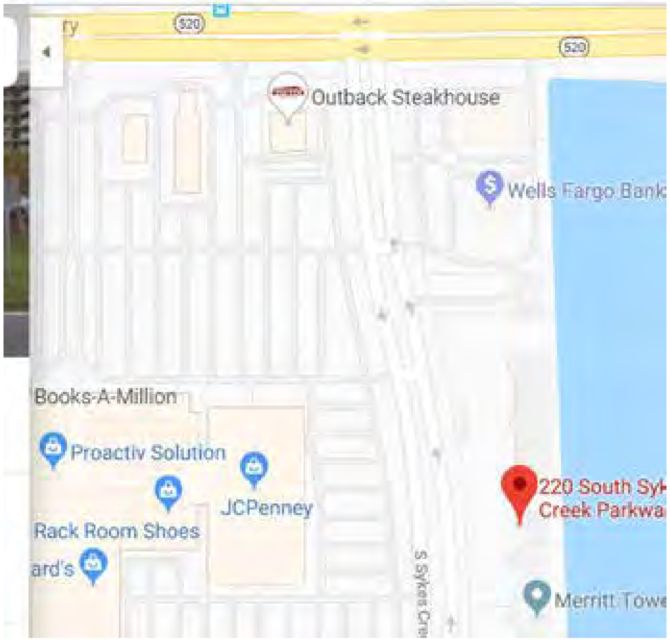
Checking

Beginning Balance	November 1, 2019	741.47C
Barbara Mead – September snacks		(10.00)
Snack fund – November donations		19.00
APCUG renewal		(50.00)
Dan Douglas Xmas Party Supplies		(29.01)
Ending Balance - Includes $173.80 Snack Fund Balance		671.46

Savings

Beginning Balance	November 1,2019	404.64
Interest		.08
Ending Balance		404.72

tTotal Acount Balance November 30, 2019 1076.18



Club Meeting Minutes November 7, 2019

Dan Douglas, President opened the meeting at 2:05 PM. Board Members present
were President Dan Douglas, Webmaster Curt Potsic, Journal/Learning Center Ron Ingraham, Treasurer Irene Nelson and Membership chairperson Linda Glassburn. Vice President Larry Bennett and Secretary Harry Pearson were absent.

Attendance was 20 and 0 guests.

Dan declared for the secretary that the minutes for the October Meeting are in the Journal on page 5. There are no additions or corrections.

Irene read the Treasurer Report, confirming a balance of $1146.11.

Ron stated the December Journal is in process.

Curt read his Webmaster Report and a copy will be emailed to members.

Linda reported that membership increased to 11 new members in 2019 versus 9 new members in 2018.

There was no speaker scheduled therefore questions and answers were discussed on topics of printers, browsers, Outlook, and fire alarms.

Members voted 20/20 and approved renewing membership for $50 to APCUG (Association for Personal Computers User Group) for year 2020.

Members voted 20/20 to REVOKE the option to get two tickets when wearing a SCPCUG t-shirt due to the unfair advantage that gives people who have t-shirts that are no longer available.

Members voted 20/20 that monthly meeting gift cards will not be given in 2020 and monies will remain in the Treasury.

There will be no formal monthly club meeting in December 2019.

The 2019 holiday party: Dan to bring cake, soda, meat tray, and three types of Jersey Mikes sandwiches. Members can bring a pot luck side dish and an optional $10 gift for the "White Elephant" drawing. Members are encouraged to email an RSVP to attend. Member and one guest are welcome. An email invitation will be sent in November.

Barbara brought refreshments and cupcakes.

The Drawing Followed – Francine Pease won the monthly gift card and members won many interesting prizes.

3:40 PM – Adjournment
Respectfully submitted by Linda Glassburn,

Dan's Desk

There is an email virus going around that I thought you should know about so you will recognize it when/if it strikes you. There is no known solution although the threat has been recognized for a while.

Even Norton and McAfee have admitted that they have not been able to come up with a solution.

The symptoms are:

1. You send the same email twice.

2. You send a blank email.

3. You send an email to the wrong person.

4. You forward an email back to the person who sent it to you.

5. You forget to attach the attachment you refer to in your message.

6. You hit SEND before you're finished writing your message.

7. You hit DELETE instead of SEND.

8. You hit SEND when you should have hit DELETE.

9. You send a blind copy to your blind friend.

10. You don't realize you've done anything wrong until someone points it out to you.

The virus is being referred to as the "C-NILE" virus, but no one would tell me why. (Personally, I think they were trying to hide something from me.)

One analyst working on the problem has found that "C-NILE" seems to most frequently affect PC's while being used by someone born prior to 1960. The virus apparently disappears once that user stops using the PC.

One of the officials I spoke with told me he is not sure why this appears to be the case. He was an elderly fellow that I ran into at the Post Office while trying to retrieve my email.

Please refer to the attachment if you have questions.

Let's just thank goodness that none of us has been struck yet!

Oh, and have a Very Merry Holiday Season! ❑

Continued..page 8

Webmaster Wanderings

Jere's Tech Tips

Jere Minich, Advisor, Region 5 (AL, FL, GA, SC)

New Items Include

How to make hrome your default browser;\
How to set up dark mode on your favorite apps;
Why you should sign in with Google, Facebook, or Apple;
How to enable dark mode on Outlook for Android, iPhone, or iPAd;
How to assign tasks to Google Drive;
How to connect your android device to a projector;
9 ways to use Windows (safely) when support ends;
How to share your Wi-Fi credentials with a QR Code on Android 10;
Delete this new batch of crappy android adware apps from your device;
How safe are password managers?
How to customize your GMail address on the fly;
How to change your email address without screwing everything up;;

1 N ew Link

OnMSFT.com – Microsoft-Oriented Website provides In-Depth Microsoft News & Information on Windows 10, Surface, How-To, Office 365, Edge, and Windows Insider. https://www.onmsft.com/
General Information Links page (http://www.scpcug.com/infolink.html) - Miscellaneous Links

Founded in 1998 as WinBeta.org, OnMSFT.com (pronounced On Microsoft) is one of the original Microsoft-centered communities. Although a Microsoft-oriented website they are not affiliated with Microsoft. Their intention is to provide in-depth Microsoft news & information. We're Microsoft enthusiasts first and foremost, although we're not shy about pointing out problems as they arise.M

Article Samples: Microsoft is "elevating" the Phone Screen experience by removing its dependency on Bluetooth; Windows 10 May 2019 Update now on more than half of surveyed PCs; Here's what you need to know about the Windows 10 November 2019 Update; How to find missing files in Windows 10; How to print to PDF in Windows 10; Is Microsoft Edge Chromium close to a stable release? How to manage updates for Office 365.

Misc Items

n ew Wake-up Lighting and s leep t imer f eatures for a lexa-Powered s mart Lights

These new features will let you set wake-up lighting and sleep timers for your smart lights using Alexa. This only works in USA only for now. You can set recurring daily alarms that turn your smart lights on and off with commands like, "Alexa, set an alarm for every morning at 9AM with my bedroom light ," and, "Alexa set a 30-minute sleep timer with lights." Note this works with both Smart Bulbs and a Smart Plug connected to a regular light bulb. The alarm set time must be more than 2 minutes away from when the command is issued. When the alarm goes off Alexa plays your selected alarm sounds and turns on the smart light. Saying "Alexa, Stop" just turns off the alarm sounds. The smart light can be turned off separately. Smart bulbs are also dimmable so you can select a specific brightness or trigger a gradual brightness change over 5 min to one hour. Amazon has now sold more than 100 million Echo devices and integrated Alexa with 85,000 smart home products. Alexa app has over 100,000 skills.

Windows 10 November 2019 Update

The Windows 10 November Update (also known as version 1909) will be ready on November 12, 2019. In addition to new features, there will be plenty of bug fixes and performance improvements. One of the new features is the ability to create calendar events without directly opening the Win 10 Calendar app. Events and appointments can be created directly from the taskbar. Another includes the ability to change how notifications are handled. The difference between "banner" and

Continued..page 8

Webmaster Wanderings................from page 7

"Action Center" is indicated by now using images to make the experience more user-friendly. One can now easily identify and choose how to receive notifications on your banner and Action Center.

Windows 10 Ver 1903 on 57% of Pcs

AdDuplex reports that Win 10 ver 1903 is now on 57% of PCs vs other versions. This is an 11% increase and is based on a 90,000 PC survey. Per AdDuplex: Almost all of 11% gained for ver 1903 comes from ver 1803 and not ver 1809. That is because ver 1803 is approaching the end of support. The bottom line is, ahead of the release of ver 1909, most PCs are running on the last two Win 10 releases (1809 & 1903).

Google's New Ai -Powered s earch

Google's new Artificial Inteligence-Powered search moves the Google search engine from spitting out results based on keywords to something closer to language. By injecting this new technology into its search engine Google hopes to better interpret the billions of web queries it gets each day. Google says, while it is still far from solving the problem fully, it is a huge step forward. The new system relies on a Google artificial intelligence tool. The tool is designed to parse long, complicated sentences, rather than just strings of words. In tests, Google said it produced far more precise results. The new system will be applied to search results in English first. Also it will not immediately affect search advertisements. ❑

WYSIYG WEB WATCH (www) - June

by Paul Baecker, Editor, Sterling Heights Computer Club MI

June 2019 issue, WYSIWYG

www.shcc.org
webwatch (at) sterlingheightscomputerclub.org

This column attempts to locate sites containing valuable, amusing, and free content, with no overbearing pressure to purchase anything.

Why do some web site addresses start with WWW2?
https://www.maketecheasier.com/sites-with-www2

Find wood imperfections with mineral spirits (2-min. video).
https://www.todayshomeowner.com/video/find-wood-imperfections-with-mineral-spirits/

Raspberry Pi kits:10 options for beginners as well as experienced makers.
https://www.pcworld.com/article/3244253/best-raspberry-pi-kits.html

How to install and use Microsoft Office on Linux (with a license key, of course).
https://www.makeuseof.com/tag/install-use-microsoft-office-linux/

Still using your kid's birthday as your universal password? You're heading toward trouble. Here's a review of password manager software choices.
https://www.pcmag.com/roundup/300318/the-best-password-managers

Kodi was described in an April 2019 newsletter article. Here is a list of 10 legal Kodi add-ons for free movies.
https://www.makeuseof.com/tag/best-legal-kodi-add-ons-free-movies/

A list of 'best' WordPress hosting providers recommended by the author.
https://www.makeuseof.com/tag/best-wordpress-hosting-providers/

Backstabbing, disinformation, and bad journalism: The state of the VPN industry. In the Internet era, everyone needs a VPN — just be cautious with your choosing.
https://www.pcmag.com/commentary/368081/backstabbing-disinformation-and-bad-journalism-the-state

They don't always get away with it. Some spammers have been caught and punished. Here is a rundown of cybercriminals who have done (or are doing) hard time for their misdeeds.
https://askbobrankin.com/spammers_and_scammers_in_the_slammer.html

Don't erase, overwrite: How to avoid being that person who resells or recycles a drive with data still on it.
https://www.pcworld.com/article/3390742/dont-erase-overwrite-how-to-avoid-being-that-person-who-resells-a-drive-with-data-on-it.html

Rock Pi 4B : M.2 & USB 3.0 SBC — Unpacking and using a more powerful Raspberry Pi alternative. (22-min. video)
https://www.youtube.com/watch?v=C4p9EpjA0ZM&list=PL2m2YvnrOYxJQXzFWX5fC1tTfi7COIpAY

"The ultimate guide to your PC: Everything you wanted to know — and more." Near the top of this article is a link to download the entire guide to your PC as a .pdf file — go get it!!
https://www.makeuseof.com/tag/download_your_pc_inside_and_out_part_1/

20 awesome uses for a Raspberry Pi.
https://www.makeuseof.com/tag/different-uses-raspberry-pi/

Getting started with a Raspberry Pi 3 (hardware assembly and software installation and use). (15-min. video)
https://www.youtube.com/watch?v=juHoJYX86Dg ❑

Windows Secrets N ewsletter: How to Get a Deleted File Back?

July 14, 2011 Windows Secrets Newsletter

Facebook Twitter Linkedi n

PC Pitstop is proud to welcome our friends at Windows Secrets as guest contributors. The weekly Windows Secrets Newsletter brings you essential tips for Windows, applications, and computing on the Internet.

By Fred Langa/Windows Secrets Newsletter

y ou deleted a file yesterday; now you *really* need it back. Your Windows recycle bin is empty — what now?

Your next-best option is the **r estore Previous Versions** tool — a truly great, automatic data-protection feature buried in Win7.

I say "buried" advisedly; most people have never even heard of it. You've heard of it, of course — you read Windows Secrets! But I'll still bet you rarely, if ever, use it. And if you ***have*** used it, I'll bet your initial explorations were probably like mine — a click here, a poke there, some head-scratching, and then mostly ignoring it.

But it's a mistake to ignore or underuse this feature, because it really is a hidden gem.

What is restore Previous Versions, exactly?

Introduced in Vista and now present in all editions of Windows 7, ***previous versions*** are local backups of ***every data file and folder*** that changes on your system. The backups are created automatically and are instantly accessible. Previous versions do for your standard documents (text files, spreadsheets, photos, whatever) what Windows System Restore does for system files.

The function that creates previous versions is enabled by default and is probably working ***right now*** on your PC, whether you've ever used the previous-versions feature or not.

As Microsoft's FAQ puts it:

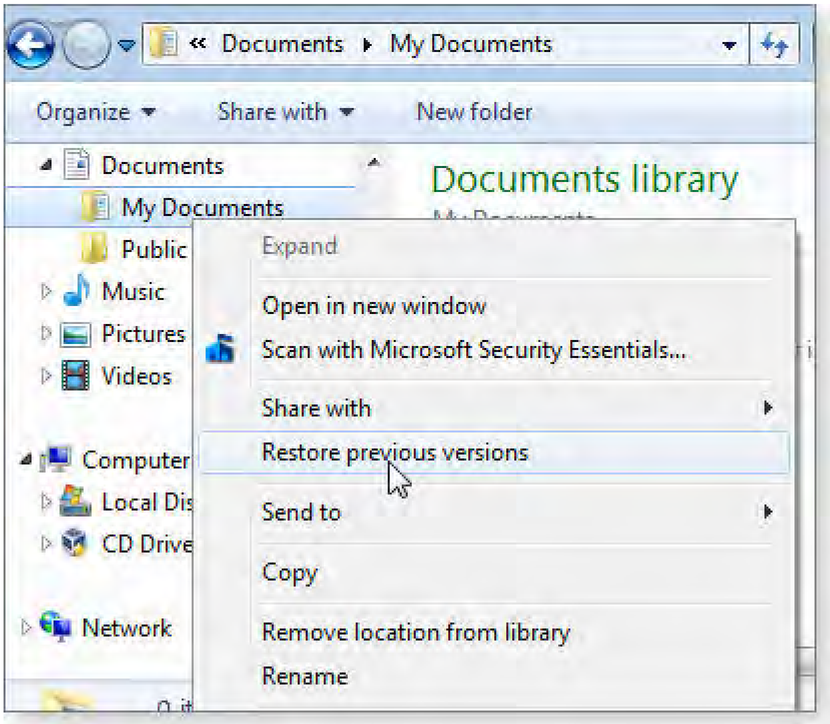
- "You can use previous versions to restore files and folders that you accidentally modified or deleted, or that were damaged. Depending on the type of file or folder, you can open, save to a different location, or restore a previous version."

In the next section, I'll walk you through the **r estore previous versions** command, using my PC as an example. Follow along on yours — it's quite safe; no files will be changed unless you specifically command it — and it'll only take a few minutes.

If you don't know about **r estore previous versions** — and maybe even if you think you ***do*** know — you just might find it eye-opening.

Continued...page 10

Windows Secrets............................from page 9



exploring your previous-version files

By default, Vista and Win7 make copies of changed folders and files at least once a day. But you can adjust the schedule at will. (I'll discuss previous-version scheduling options later.)

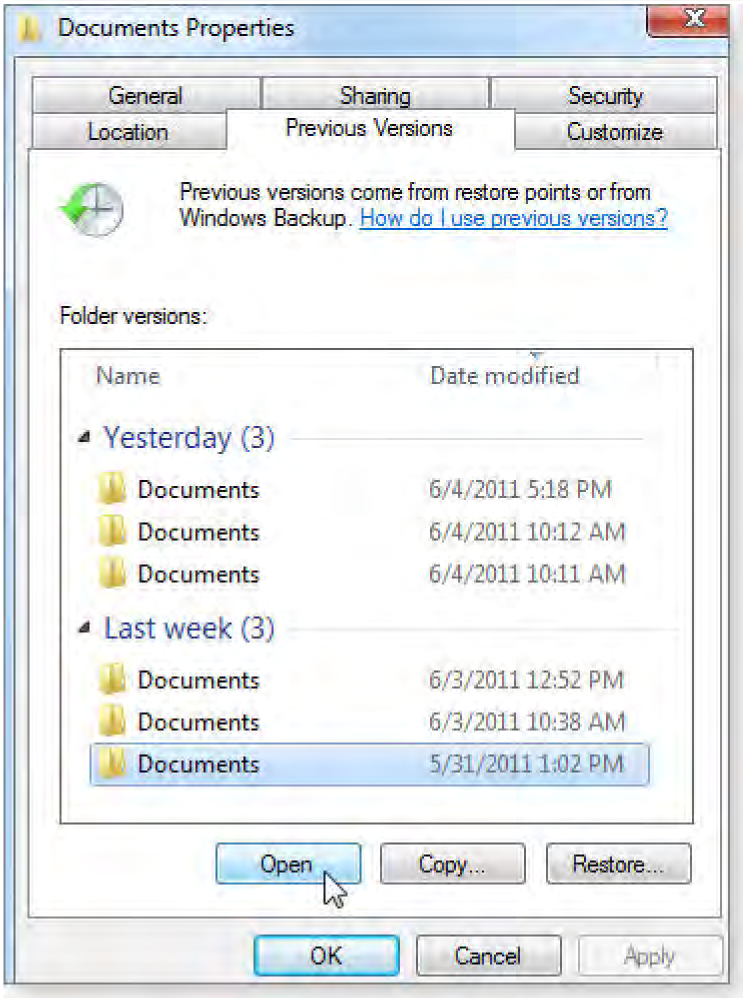
Because this backup system stores only files that have changed, the best place to see it in action is in a folder that you use a lot — one where you frequently alter the folder's contents. The **my documents** folder is usually a good example, so that's what I'll use in this demo.

figure 1

To start, open Windows Explorer, right-click My Documents, and select **restore previous versions,** as shown in Figure 1.

Restore previous versions **is enabled by default in all editions of Win7. It lets you recover recently lost or altered documents, spreadsheets, pictures, etc.**

A dialog box similar to the one shown in Figure 2 will open, revealing the available previous versions. (Of course, your list will differ from mine.)



Previous versions come from restore points or from Windows Backup. How do I use previous versions?

Folder versions:

Name	Date modified
Yesterday (3)	
Documents	6/4/2011 5:18 PM
Documents	6/4/2011 10:12 AM
Documents	6/4/2011 10:11 AM
Last week (3)	
Documents	6/3/2011 12:52 PM
Documents	6/3/2011 10:38 AM
Documents	5/31/2011 1:02 PM

Figure 2.

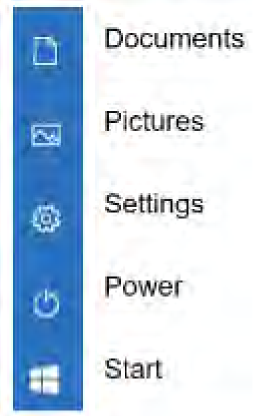
on my test system, the Previous Versions tab had six backups of my documents folder available for restoration. ❑

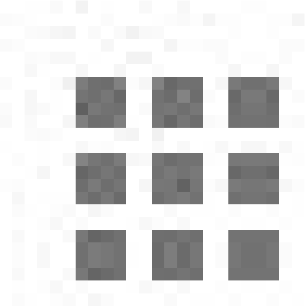
Tiny Icons for Big Functions

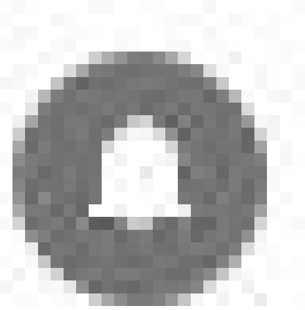
Author: Nancy DeMarte, 1st Vice President, Sarasota Technology Users Group, FL

July 2019 issue, Sarasota Monitor

www.thestug.org
nanellend (at) gmail.com







In recent years, the number of functions that computers and other devices can perform has increased greatly. It appears that to make more room on the screen, tech companies have reduced the amount of text and replaced it with symbols or icons, often without giving users notice. A good example is Google's block of dots representing their many apps. One day about a year ago I found my Gmail contacts list was missing. Eventually, I found it in the center of the Google app icon (shown at right) on the Google home page. This change to icons was so subtle that many users didn't notice it until they couldn't find a tool or function.

The trend is not only on the Internet, but also in Microsoft's Windows and Office apps. When I click the Windows 10 Start button, I see a list of important functions represented by icons. Fortunately, Microsoft has tried to make each icon resemble its name, as shown below. But not all the icons are as obvious as the gear for Settings or a house to indicate the Home page.

In Office, some icons are so small that they are easy to miss. On the Home tab in Word, for example, several of the groups of tools have a tiny diagonal arrow in the lower right corner. Clicking this icon in the Font group opens a dialogue box which lets me set specific properties for text, as shown. I can make my choices and, if I wish, set them as the default font, meaning that these settings will remain until I change them. ❑

Settings – What happened to Control Panel?

Author: Phil Sorrentino, Contributing Writer, The Computer Club, Florida

www.scccomputerclub.org
Philsorr (at) yahoo.com
Author: Phil Sorrentino, Contributing Writer, The Computer Club, Florida

Way back in the days of Windows 7, the Control Panel was the way we adjusted the operation of certain parts of the Operating System. Control Panel was easily found because it was in a short list of options when you clicked the Start button. When you clicked “Control Panel,” you were presented with a set of Apps (originally called Applets), that would allow you to change the way certain features operated. (To get this list you had to choose “View by Icons” rather than “View by Categories.”) The list of Apps included, Display, Keyboard, Mouse, System, Default Programs, Power Options, Programs and features, Folder Options, Network and Sharing, Device manager, just about all the features that you can adjust. Maybe the statement at the top of the set of Apps was prophetic in its language. The Apps were introduced by a text line that said, “Adjust your computer’s settings.” And maybe the thought of Settings was carried over from the Smartphone world, (i.e. Apple’s iOS and Google’s Android) just about when Windows 10 was being developed. No matter how it evolved, Settings seems to be the preferred term for the place to go to change the way the device operates.

“Settings” has become a common feature on many computing devices. It even shows up on other things like electric ovens, exercise machines, thermostats, and kitchen appliances. So now Settings is the place to set many of the features of Windows 10. Yes, Control Panel still exists, but it is not as apparent, or easy to find. It seems like it has been moved to different places in different Windows 10 editions. But, fortunately, you can always find it just by clicking the “Type here to Search” circle next to the Start button, and then typing “Control” into the Search bar.

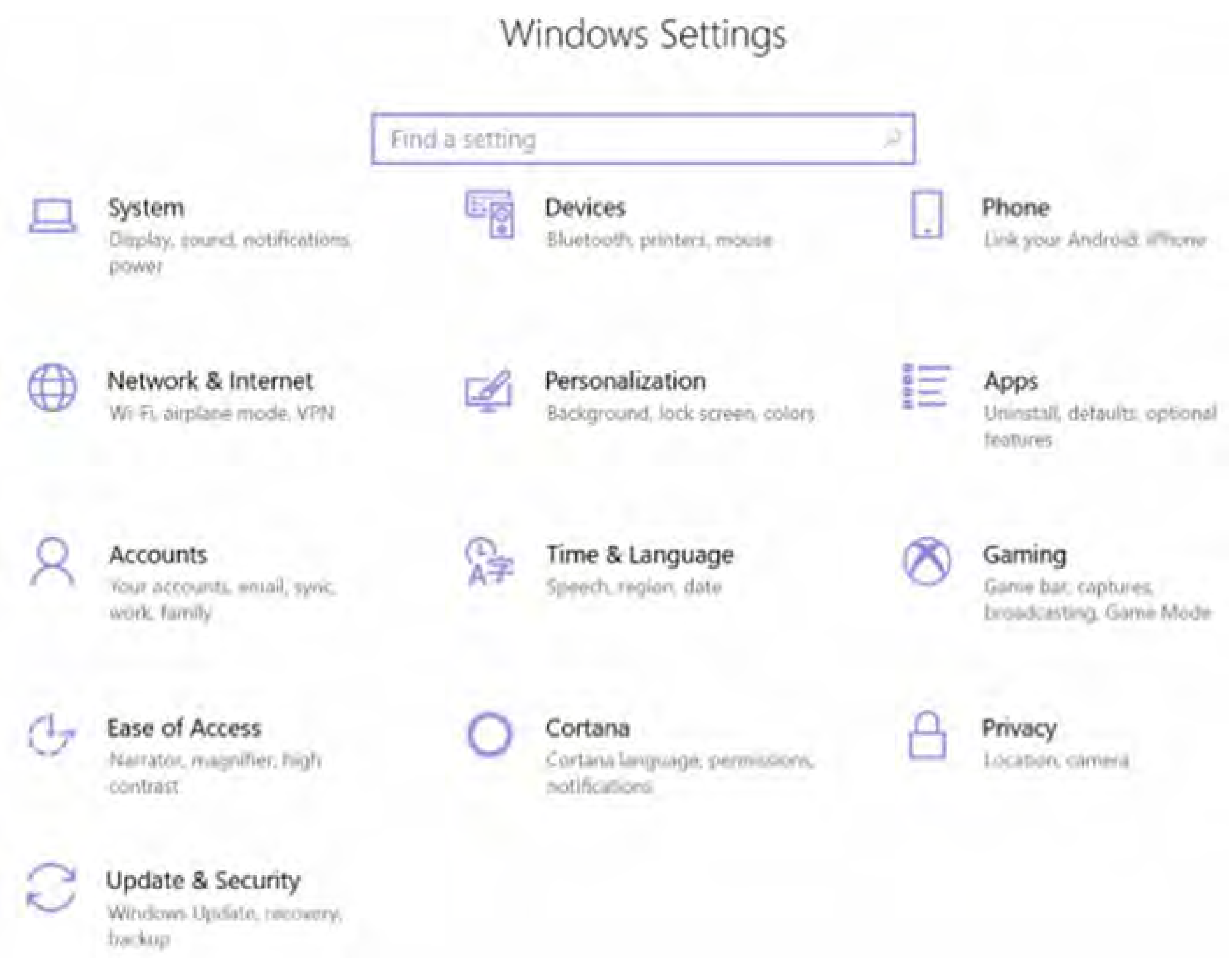
You may not even have to go to Control Panel for most of the things you may want to change, because clicking Settings will more than likely get you there. And, Settings is very easy to find; just click the Start button and the Settings icon, which looks like a gear, appears right above the Power icon. Click the icon and you will be shown all the Settings categories. Just to add a little confusion, these new categories are not the same categories that are used in Control Panel, although some of the titles will be familiar. The Settings screen on one of my machines is as shown on page 13

Notice that they are not is alphabetical order. Note too, that System is the first category, so Microsoft must consider these to be important settings. Here are the items in the System category:

Display. Here you will find Display-related information and settings. The first setting is “Night light,” which allows you to set a schedule for the Night Light and set the “Color temperature at night.” The introduction explains that “Screens emit blue light, which can keep you up at night.” So, by using warmer colors, there may be less interference with your sleep. (I’m only the messenger.) Here is where you can “Change the size of text, apps, and other items,” if so desired. The Resolution of the display is another setting that can be changed. (Keep in mind that if you choose a higher resolution, the text and pictures on the screen will be smaller, so if you want larger items on the screen, you will have to lower the Resolution. I know that sounds counter-intuitive.)

Sound is where you choose your output or input devices, volume, manage your sound devices and troubleshoot those devices.

Notifications & actions is where you set up the Quick Actions, the icons you see when you click the Action Center icon at the right-hand end of the taskbar. (Clicking the Action Center icon also shows you any notifications that are available.) This is also where you get to determine the notifications you can receive, and who can send you notifications.



Windows Settings

Find a setting

System
Display, sound, notifications, power

Devices
Bluetooth, printers, mouse

Phone
Link your Android, iPhone

Network & Internet
Wi-Fi, airplane mode, VPN

Personalization
Background, lock screen, colors

Apps
Uninstall, defaults, optional features

Accounts
Your accounts, email, sync, work, family

Time & Language
Speech, region, date

Gaming
Game bar, captures, broadcasting, Game Mode

Ease of Access
Narrator, magnifier, high contrast

Cortana
Cortana language, permissions, notifications

Privacy
Location, camera

Update & Security
Windows Update, recovery, backup

Focus Assist is where you can choose which notification you'd like to see and hear so you can stay focused. The rest will go straight to the action center where you can see them any time.

Power & sleep. You can customize how long the screen will stay on after the last keystroke, and when the computer will go into the sleep mode. If you have a laptop, these settings are made for both "On battery power" and "When plugged in."

Battery. Here you will see a battery charged percentage indication and if you click "Battery usage by app," you will see how the battery is being used by various Apps. Battery saving options are also shown here.

Storage is where you can see the size of each local storage device (drive) and how much is being used. There are also a few storage related items here such as "Change how we free up space," and "Manage Storage Spaces." You will probably want to customize these options. You will also find "Change where new content is stored," which determines where various file types, like documents, music, and pictures will be stored.

Tablet mode optimizes your device for a touch screen so you don't have to use a keyboard and mouse.

Multitasking gives you control of the "Snap" feature, that is the ability to snap windows into half the overall screen. This can be useful if you want to Copy & Paste between two documents.

Continued..page 14

Settimgs - What Happened......from page 13

Projecting to this PC gives you the ability to wirelessly project some Windows and Android devices to your device. If you give presentations, turn on "This PC can be discovered for projection only when it's plugged in."

Shared experiences lets Apps on other devices open and message apps on your device, and vice versa. This feature improves the ability to share documents and apps among all of your devices and may or may not be useful to you.

Clipboard. You can save multiple items to the clipboard to use later as well as sync them across devices, pin frequently used items, and clear the clipboard data.

Remote Desktop lets you connect and control your PC from a remote device by using a remote desktop client. Note: You never want to enable this unless you completely trust the person who wants to take over control of your PC. You might do this if someone you know and trust is trying to help you with something and they are at a remote location.

About contains a lot of device specification information. This is where you will find hardware information such as Device name (with the ability to change the name), Processor type, Amount of memory, and the system type, 64bit or 32 bit. Here you will also find Software information such as the Windows 10 edition, like Windows Home or Pro, and the version number.

"Settings" is a very important and comprehensive part of Windows 10. In this article, we have only reviewed the first category, System; there are 12 more categories full of various types of settings. Stay tuned. ❑

© Benjawan Sittidech | Dreamstime.com

SAFETY & SECURITY

6 ransomware attacks you need to watch out for

BY MARK JONES, KOMANDO.COM

•

NOVEMBER 22, 2019

It doesn't matter if you're working on a home computer with lots of sensitive documents and family photos, or if you're a small business owner with years of client files and tax records. You're likely storing more data than you realize.

Cybercriminals know you value your files, so they threaten you with ransomware. The most common way to fall victim is through phishing attacks from malicious links or corrupt documents. If you don't pay, there goes all your data. Worse, you can pay and the criminal could delete it anyway.

You don't have to be a victim. Back up your files and keep them safe in a cloud service. We recommend using our sponsor, IDrive. Get 90% off 5TB of cloud backup at IDrive.com when you use promo code Kim at checkout.

Nasty ransomware attacks making the rounds

Ransomware strains can cripple tons of systems all over the globe — it just depends on how successful the distribution campaign is behind the strain.

Emsisoft recently published a report detailing global ransomware stats for Q2 and Q3 of 2019. The report is based on data submitted to the company between April 1 and September 30. It includes more than 230,000 submissions.

Even though you hear more about ransomware attacks on governments and businesses, the most prevalent ransomware targets home users, especially those who use pirated software from torrent sites. Here is a list of the six most commonly reported ransomware strains of 2019, according to Emsisoft:

1. STOP (DJVU)
STOP, aka DJVU, was the most commonly reported ransomware strain during Q2 and Q3. It actually accounted for 56% of all submissions.

This ransomware variant targets home users and is mostly distributed through torrent sites. It hides in applications like key generators that are used to activate paid software for free.

2. Dharma
Dharma was the second most common strain of ransomware during the time period in question. It's been around since 2016, but saw a spike in activity in recent months.

This variant typically targets businesses and has impacted a number of organizations, including a hospital in Texas. The ransomware encrypted hospital records and files that contained critical patient records like names, Social Security numbers and credit card information
.

Continued..page 16

Ransomware ....from page 15

3. Phobos

Holwichaikawee | Dreamstime

Phobos is similar to the Dharma strain and was first reported earlier this year. It primarily targets businesses and public organizations. In July of 2019, a Wyoming school district lost access to data after being hit with Phobos.

The ransomware variant entered the school district's system through a brute force attack on an outside port. Officials with the school district ended up paying nearly $40,000 worth of Bitcoin to recover the encrypted files

.

4. GlobeImposter 2.0

In June of 2019, an Auburn Food Bank was hit with GlobeImposter 2.0. Nearly all of the food banks' computers were encrypted by the ransomware.

The food bank's director chose not to pay the ransom. Instead, they opted to wipe the affected systems and rebuild their network. It wound up costing about $8,000 in recovery costs. The unfortunate truth is they could have saved all that time and money if they'd had a backup in an off-site cloud service, like IDrive.

5. Sodinokibi

Sodinokibi, aka REvil, was first spotted in April of 2019. This is what's known as ransomware-as-a-service and relies on affiliates to distribute and market the ransomware.

Its specialty is using advanced techniques that help it avoid being detected by security software. Sodinokibi attacks were primarily in Asia, but have recently spread to European organizations and could end up attacking victims around the globe.

6. GandCrab

GandCrab is another ransomware-as-a-service variant. Like Sodinokibi, GandCrab was constantly updated by the criminals behind it to keep it from being detected by antivirus software.

Once installed, GandCrab locks Windows files using RSA encryption and it displays a ransom note demanding payment for the "GandCrab Decryptor" needed for unlocking the files.

Ways to protect against phishing scams and ransomware

© Videopricesolutions | Dreamstime

Since phishing scams are the most common way for your device to be infected with ransomware, it's important you know how to stay protected from them.

Continued..page 18

Ransomware..............................from page 17

Here are a few suggestions to avoid falling victim to phishing attacks:

- **be cautious with links** – If you get an email or notification you find suspicious, don’t click on its links. It’s better to type the website’s address directly into a browser. Before you ever click on a link, hover over it with your mouse to see where it’s going to take you. If the destination isn’t what the link claims, do not click on it.

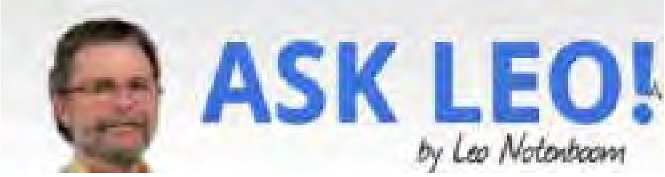
- **Watch for typos** – Phishing scams are notorious for having typos. If you receive an email or notification from a reputable company, it should not contain typos; however, scammers are getting better at tricking people and are making phishing emails look more realistic than ever, so be cautious — even if you don’t spot mistakes.

- **use multi-level authentication** – When available, you should be using multi-level authentication. This is when you have at least two forms of verification, such as a password and a security question, before you log into any sensitive accounts.

No one is perfect. No matter how vigilant you are in trying to avoid phishing scams, there is still a chance you could fall for one, resulting in an infected device. That’s why you need to stay a step ahead. The best way to outsmart a ransomware scammer is to have your critical files backed up before they’re compromised.

IDrive helps protect you from scammers and hackers in major ways, while also being a great data storage system for your computer and other devices. Keep scammers away from your data and get IDrive today. Get 90% off 5TB of cloud backup at IDrive.com when you use promo code Kim at checkout. ❑

Reprinted with permission. Copyright 2019. Kim Komando.
www.komando.com
Kim can be heard locally in Melbourne: WMMB1240AM, Saturdays starting at 10am-1pm; in Cocoa: WMMV 1350AM Sim WMMB, Saturdays starting at 10:00 AM - 1:00PM.



Why is it so important to Use a Different Password on Every Site?

by Leo A. Notenboom

Using different passwords on different sites is not only good practice; it’s necessary to keep your accounts safe. I’ll review why, and how best to handle a plethora of passwords.
//
I keep hearing that I’m supposed to use a different password on every internet site where I have an account. What a pain! I can’t remember all of those passwords. Yeah, I know. You want me to use a password manager thing, but that seems like putting a bunch of really important things into a single basket. What if that basket gets hacked? I use a strong password. Why isn’t that enough?

The hacks of several online services have brought this issue to light once again.
I'm sorry, but a single strong password just isn't enough anymore. You must use different strong passwords on every site where you have an account — at least every important site. And yes, you must devise a way to manage them all.

Let me run down an example scenario that's a cause of all this emphasis on different passwords.

The all-too-common scenario

The scenario I'm about to describe is very common. While the specifics won't apply to you exactly, conceptually it will illustrate what can happen. Let's say you have an account at some online service. I'll call it Service A. In addition, you have a Yahoo! account, because you used it years ago; a Google account, because you now use Gmail and a number of other Google services; a Microsoft account, because you have Windows; and we'll throw in a Dropbox account, because you've been listening to me recommend it. You probably have other accounts I haven't listed here, but you get the idea. You have lots of accounts at a number of online services.
You have a wonderfully strong password that you've memorized: 16 completely random characters.
And you use that same wonderfully strong password for all those accounts.

Here's how it can go horribly, horribly wrong.

Anatomy of a hack

Service A has the best of intentions, but honestly, they don't "get" security. Perhaps they store passwords in their database in plain text, allowing anyone with access to see them. They do that because it's easy, fast, and solves the problem quickly. They make the assumption that the database containing your password will be impenetrable.

Hackers love it when site designers make assumptions like that, because, of course, the assumption is wrong. One day, a hacker breaches service A's security and steals a copy of the user database. The hacker walks away with a database that contains the following information for every user:

Their login ID
The email address associated with the account
The password (or enough information from which the password can be determined)1
Password hints/security questions
They can log in to your account on Service A. That may or may not be a big deal, depending on exactly what Service A is and how you use it.
But it opens a very dangerous door.
It doesn't have to be a hack
It's important to understand that while this example centers around what we hear about in the news most often — the hack of an online service and theft of their user database — it's certainly not limited to that.
Essentially, anything that could compromise your password brings you to this point. That includes:

Sharing it with the wrong person.
Keyloggers and other malware sniffing your password as you type it in.
Improper use of an open Wi-Fi hotspot.
And so on.

Anything that puts your single password into the hands of a malicious individual puts you at greater risk than you might assume.

Continued...Page 20

Why is it important....................from page 19

Password skeet shooting

Once they have your password, the hackers go hunting.
As most people have accounts on one or more of the major services I mentioned, the hackers start trying the information from Service A as if it were the correct information for Gmail, Microsoft, Yahoo, Facebook, Twitter, Dropbox, and more.
They try your email address with the password they stole from Service A to log in to the email service that you're using.
They try your login ID and password (or that email address and password) on as many other services as they can —
— and very often, it works. The hackers gain access to some other account of yours that was completely unrelated to the initial security breach.
Unrelated, of course, except that you used the same password at both.

If you use the same password everywhere, a single leak of that password puts all your accounts at risk. Hackers will be able to log in to your other online accounts as well. Maybe not all; maybe only a few…
…but a few is all it takes.

The weakest link

Note that this has absolutely nothing to do with the security expertise of the sites where your account is eventually compromised. Gmail, Outlook.com, Yahoo, and others have excellent security, but that doesn't factor into this scenario at all.

Service A was the weak link. Their security wasn't up to the task. Their database was breached. Their information was leaked. Your account information and password — the password you use everywhere — was exposed.
Service A was at fault.
But the real problem is your use of that single password everywhere.

It shouldn't be this way

I'll happily admit that things like this shouldn't happen. But they do. Not terribly often, but often enough.
And most services are better at security than our fictional Service A.

But it's also not a black-or-white equation. Even large corporations, which either don't know any better or simply make a mistake, can put your information at risk. For example, a hack at Adobe a couple of years ago potentially exposed the passwords of 130 million Adobe account holders. I hate to say you can't trust anyone, but ultimately, you shouldn't trust anyone not to accidentally expose your password.
And, as I mentioned above, it doesn't have to be a big service breach for there to be a problem.
Using a different password on each site limits your exposure if any site is compromised.

Managing lots of passwords

So it comes down to how to manage a lot of different, long, and complex passwords.
I still recommend LastPass, and use it myself. Doesn't that put all my eggs in one basket?
Yes, it does. But it's a very good basket. And I've taken additional steps to ensure that it stays that way.
I talk about LastPass in more depth in LastPass – Securely Keep Track of Multiple Passwords on Multiple Devices, but I'll highlight two important reasons I consider LastPass secure:
The people at LastPass don't know your master password. They couldn't tell you what it is if they wanted to.

They cannot access your data at all; all they can see is the encrypted data. Even if a hacker were to somehow gain access to their databases, which has never happened, the hacker would also be unable to decrypt and view your information, because LastPass does encryption right. Decryption happens locally on your machine, so the only thing ever transmitted between your computer and LastPass is the encrypted data.

Of course I use a strong password. But LastPass also supports two-factor authentication, and I've enabled it on my account. If you somehow got my master password, you'd still need my second factor in your possession to be able to unlock my LastPass vault.

Ultimately, it's up to you. There are several password managers out there, but LastPass is the one I trust.

The very short bottom line

My recommendation remains:

Use long, strong passwords. Twelve characters minimally, ideally more, and randomly generated (there are several random-generator tools available, including one in LastPass). Alternately, and if allowed, use a passphrase at least four words long, ideally with spaces.
Use a different password for every login account you have. Every single one.
Use a password manager like LastPass to keep track of them all for you.
Use a strong password or passphrase on LastPass itself.
Enable two-factor authentication on LastPass for additional security of that very important basket of information.
ly is conventional wisdom. I disagree, and then discuss whether periodic password change can even happen reliably.

Footnotes & references

1: Thankfully, services rarely store the actual password – though of course they could. (If your service can tell you your actual password, then they're doing it wrong, and they've stored the password itself somewhere). Rather, they store what's called a "hash" of the password. Depending on several factors – typically, poor decisions made by whoever implemented the authentication mechanism – it is occasionally possible for hackers to indirectly reverse-engineer passwords from hashes.

Posted: November 30, 2019 in: Passwords
This is an update to an article originally posted November 9, 2013
Shortlink: https://askleo.com/11788
Tagged: Featured, LastPass, password management, password reuse, passwords
« Previous post: How to Diagnose Wi-Fi Signal Strength Issues
Next post: Embracing the Most Important Attitude »
New Here?

Let me suggest my collection of best and most important articles to get you started.
Of course I strongly recommend you search the site -- there's a ton of information just waiting for you.
Finally, if you just can't find what you're looking for, ask me!
Leo Who?

I'm Leo Notenboom and I've been playing with computers since I took a required programming class in 1976. I spent over 18 years as a software engineer at Microsoft, and after "retiring" in 2001 I started Ask Leo! in 2003 as a place to help you find answers and become more confident using this amazing technology at our fingertips. ❑

How Chat Rooms, Fake Customer Reps, and Phony Surveys Steal Your Info

By Scambuster Keith

Snippets issue exposes continuing chat room scams: internet scambusters #882

Although online chat rooms are not as popular as they used to be, they're still a big hit with scammers.

And in other new tricks, they're hiding behind top online trading names like Amazon and American Airlines to trick victims into giving their sign-on details.

We'll explain their latest tactics in this week's Snippets issue

Let's get started…

How Chat Rooms, Fake Customer Reps and Phony Surveys Steal Your Info

Remember chat rooms? At one time, they were all the rage — online meeting places where users with similar interests could virtually gather to ask questions and discuss topics.

Back in the 90s, more than half of all teenagers and a quarter of adults were regular users.

You don't hear so much about them these days and the number of users has plummeted, with other social media becoming the preferred forums.

But, for certain interests like dating, very specialist interests and, ahem, adult-type issues, they're still flourishing.

And so is targeting these particular groups for scams and other crimes.

A favorite trick is to include links in a posting, claiming they'll connect with relevant photos or videos relating to the chat room topic.

We're always warning of the dangers of clicking links but often in chat rooms, they're an essential part of the way they operate.

In this case, however, clicking the links downloads malware. One increasingly common trick, most recently found on dating sites, uploads pornography onto the victim's computer or phone.

Then the scammer poses as someone from law enforcement and demands payment of a fine, stating that pornography has been detected on their device.

Even if they realize it's a scam, some victims may be reluctant to report it to the police for fear of being accused of downloading porn. However, police can easily detect the source of such downloads, proving that the victim was not involved.

It's possible too that the scammers may simply contact victims directly, threatening to expose them if they don't pay.

Either way, if this happens to you, you definitely shouldn't pay. And safely report the crime to police.

You should also be wary about clicking links in chat rooms, and be sure to run security software after each visit.

Phony Amazon Reps

And would you be wary if you received a telephone call or a link from a customer service rep who says he/she is from online retailing giant Amazon?

Well, it'd be very unusual for Amazon to make an unsolicited call, though they will often call you if you ask them to first.

But posing as an Amazon rep is just one of many effective tricks that scammers use to try to get hold of your sign-on information and other account details.

If they tell you there's a problem with your account, you might be inclined to believe them, since most of us do buy from Amazon and occasionally encounter blips.

But if this "rep" then asks for your username and password, you can be one hundred percent sure it's a phishing scam because Amazon never asks for your password.

What the crook is after is not only the ability to buy stuff on your dollar, but also to get ahold of other useful information such as the three-digit security code on the back of the card.

Sometimes, the scammers realize you wouldn't be so naive as to give out your password so easily. So, instead, they say they'll email you a link to a secure sign-on area where you can verify your information.

That's even worse, because now victims who visit these fake Amazon-looking sites will not only have to disclose their sign-on information but also their full credit card number and other personal details.

If anyone calls you claiming to be from Amazon, chances are high it's a scam. Even if you think it might be genuine, don't follow any email link they offer. Instead, go to amazon.com and sign in there to check your account.

Amazon also provides very detailed guidance on how to check if an email, web page or call is genuine, here: About Identifying Whether an E-mail, Phone Call, or Webpage is from Amazon.

Fake Airline Survey

Another clever phishing trick comes in the guise of a request for you to take a survey about recent air travel. Or it may pretend to be a change notification for a flight you recently booked.

It looks like it comes from a well-known airline — we've seen several including Delta and American — and if that happens to coincide with an airline you recently used, it'd be easy to think it's genuine.

Once again, there's a clickable link that takes you to a fake sign-on page. But in some cases, there's also an extra sneaky trick: When you try to click on a link, nothing happens. Then you spot a message, saying if you're having difficulty you can view the message online by clicking another link.

This is particularly clever because we're used to seeing links just like these on genuine messages.

Furthermore, we're also accustomed to getting survey requests from people we've done business with that don't actually use the firm's regular web address. It may, for instance, use the name of the survey company.

So, there are a number of reasons why this scam might seem convincing. But remember this: A survey company would never ask for your sign-on details.

And if the message seems to come from an airline, check it independently by keying in the airline's Internet

Continued..page 24

Steal Your Info...............................from page 23

address and check your account there. Or use the airline's smartphone app.

Alert of the Week

We have another Amazon scam to alert you to this week: A voicemail asking you to verify that you signed-up for the retailer's Amazon Prime membership.

It warns that the fee is about to be charged to your account and that if you disagree, you must phone a toll-free number. But if you do, you'll be asked for your account details.

Phooey! Just hang up. And if you're unsure, again go to amazon.com and check things from there.

Time to close today, but we'll be back next week with another issue. See you then! ❑

Reprinted with permission from Internet Scambusters,
The #1 Publication on Internet Fraud.
Copyright (c) Audri and Jim Lanford
To subscribe to their newsletter visit:
http://www.scambusters.org.

Making Your Tech "Fit"

Does Size Matter?

Author: Debra Carlson, Technical Advisor, CVC Computer Club, CO

Q2 2019 issue, t ech-n otes

cvc.computer.club (at) gmail.com

Last quarter we talked about tech and eyes. This quarter we will talk about something that can be related … Does size matter?

A few principles:

Keyboards -- "full size" addresses the width of keys but not the angle of the keyboard, height of the keys, pressure that is required to depress keys, or the optional keys and support for their programming.

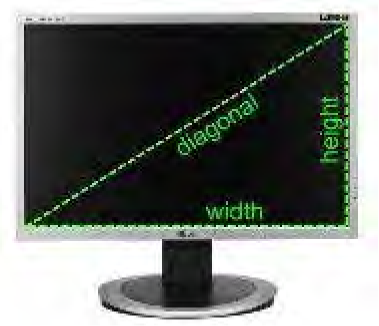
Ergometric keyboards" that force you to hold your elbows away from your body are "healthier", in large part, because they force you to take breaks from typing. Keyboards with many curves do the same – and breaks are important.

Mouse -- If a mouse is too small it will stress your hand and wrist. It will also make it harder to relax while using the wheel for scrolling.

If you need to save money on one of these devices, save on the keyboard and spend on a mouse that fits.

Now for the more complicated size question – the monitor.

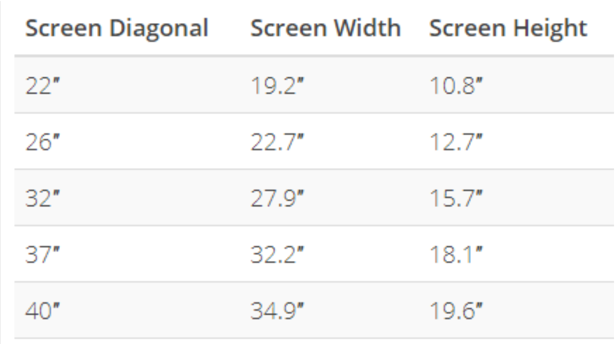
First, monitor size is both the physical size of the screen and the size of the items on the desktop (the screen with its icons, etc. is called the desktop).



Many writers say, “get as big a monitor as you can afford.” While this may work for the newer high-end televisions, it is possible to overload the optical sensors at the distance we use for computer monitors.

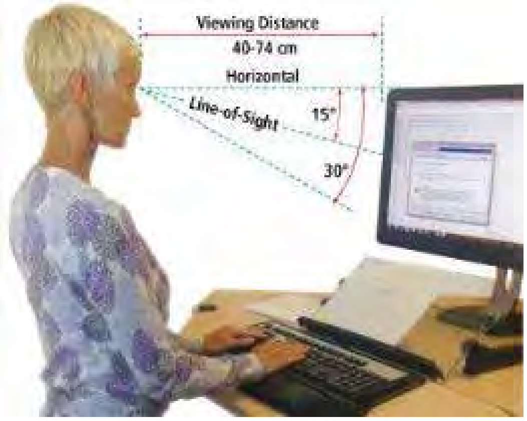
Monitor size is measured diagonally.

Approximate sizes on your desk are shown below.



Screen Diagonal	Screen Width	Screen Height
22"	19.2"	10.8"
26"	22.7"	12.7"
32"	27.9"	15.7"
37"	32.2"	18.1"
40"	34.9"	19.6"

OSHA (US Occupational Safety and Health Administration) suggests the following setup.



Optometrists suggest the monitor distance is 16 to 30 inches.

It is important to note that people who use bifocals / trifocals / progressive lenses will often need to look through the bottom of lenses if they do not use computer glasses so raising the monitor and setting it a bit farther back will help with neck strain.

It is important to place the monitor in a location that eliminates glare on the screen. This optimally means perpendicular to a window, but this may not always be possible.

Options include modifying the natural (shades / curtains), or artificial light (sometimes this means turning on a light) when using the computer.

Continued...page 26

Does Size Matter?.......................from page25

Standard resolutions (icon and font sizes) for current monitors are (many more are possible):

1280x720

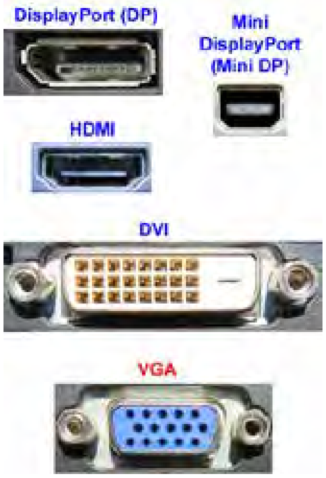
1366x768

1600x900

1920x1080

Generally, adjusting icon size more than 125% is not recommended unless you are using a discrete graphics card as it will cause slow response time and hanging / ghosting of images. Plan to mix changing resolution and setting icon size for best results.

It is usually possible to get a good 24" monitor for $150 and a good 27" for between $200 and $250. Be sure you have a desk with space that allows you to move a monitor away from the chair before investing in a 32" monitor because of optical overload potential … and invest in a 4K monitor if you are going that large to help avoid the pixilation that can happen on a large monitor.



If you are using a laptop, of course, sizes are different but resolution information is the same. Most laptops will allow attaching an external monitor for ease of use when sitting at a desk … check to see what kind of connection you can make. Most laptops will use VGA or HDMI.

For all users – when replacing your monitor, futureproof your purchase by including DisplayPort or HDMI on the monitor or TV you purchase for your viewing pleasure.

Next month we will look at Things in your hands (mouse, stylus, pen mouse, finger, clicking, swiping, touching, and other stuff), followed by Cords, Voice, Sound, and other hazards.❑

a ndroid m alware e xtracts Passwords from a ny Legit a pp

by John Lister

Infopackets Newsletter, December, 5 2019

Security researchers say a serious Android bug could let malware pose as a legitimate app and gain unwanted access to a phone's data and functions. The concept of the 'StrandHogg' bug has been known for several years, but now it's being actively exploited to target online banking.

In simple terms, the bug has two unwanted effects: it can trick users into giving malware sensitive 'permissions' to access the phone, and it can hijack legitimate apps to trick users into handing over login details and sensitive information.

Researchers at Promon explain the bug is with a security setting called "taskAffinity," which is to do with the way a phone keeps track of its "to do" list of tasks when running multiple applications. The idea is that taskAffinity shows which app a particular task relates to, making it easier to rearrange or update the list of tasks into a more efficient order. (Source: promon.co)

The StrandHogg bug effectively means apps can use a bogus taskAffinity setting. This means that Android treats tasks from the malware as if they were being carried out by a legitimate app.

Permissions System Abused

The first unwanted consequence of this bug is that the malware can "cut in line" when a user taps on the icon to open the legitimate app. The malware can then ask the user to grant a particular permission, such as accessing GPS data or reading text messages. To the user it will appear the legitimate app is asking for the permission, so they will be more likely to grant it.

The second unwanted consequence also involves the malware activating when the user opens a legitimate app. In this case the malware displays a bogus login screen for the legitimate app. Once login details are submitted, data is sent to the malware creator; the malware then closes itself and tells the phone to open the legitimate app. (Source: bbc.co.uk)

The biggest concern with s trandHogg is that it's a bug with Android itself rather than any specific app. Promon says it tested the bug with 500 leading apps and found all were vulnerable.

Malware Spreads Through 'Safe' Apps

The main mitigating factor is that the malware has to get on the phone in the first place.
Promon says in the real world examples it found, the malware wasn't directly in any Google Play Store apps. However, Play Store apps did act as a Trojan "dropper", meaning that once installed on a phone, they then downloaded and installed the malware.

While Google often finds and blocks such dropper apps, the sheer number of apps it deals with means some slip through. One dropper app, which was billed as a PDF creator, had more than a hundred million downloads.

Google is investigating what if any changes to make to Android to fix the StrandHogg bug. In the meantime the best advice for users is:

- Take extra care when installing apps, even ones in the Google Play store.

Continued..page 28

Android Malware........................from page 27

- Think twice when granting permissions or typing in sensitive data.
- For the most sensitive apps such as online banking, prefer apps that don’t require you to type in the entire login details in one go. Instead prefer ones with biometric logins or those which ask you to type specific characters from a password.
-

What’s y our o pinion?

Are you surprised such a bug exists? Does it put you off using Android? Do you take a different approach to security on mobile devices compared with PCs?

Windows 10 Taskbar Options

By Jim Sanders, Director / WebmasterNorth Orange County Computer Club,

cao range b ytes, s eptember 2019

www.noccc.org
jsanders (at) ligasmicro.com

The taskbar is a very important part of the Windows 10 operating system. Arguably, it’s primary purpose is to make computing life for you, the user, easier.

Like a lot of things in Windows 10, most of the features in the taskbar can be implemented or modified in more than one way. Some, directly on the taskbar itself. For instance, the order in which shortcut icons appear on the left end of the taskbar can be rearranged by simply moving the cursor to that icon, left click and hold with the mouse, then drag the icon left or right to the position where you want it to be

The taskbar is a great location for any shortcuts that you use often. One way to get that shortcut onto the taskbar is to right-click on any shortcut icon on the desktop and choose “pin to taskbar” from the list of options in the window that pops up. Or, click on start, pick the program that you want from the list that you can scroll through, right-click on that program, in the window that pops up, left-click on “more” and on the sub-window that pops up, click on Pin to taskbar.

If a program shortcut icon has already been pinned to the taskbar, you can “unpin it” by the same procedures.

One feature that some people love, and others hate, is auto-hide the taskbar. When the taskbar is at the default bottom of the screen location, and auto-hide is turned off, the taskbar is always visible and covers up at least one line of information at the bottom of the screen. When auto hide is turned on, the taskbar is hidden until you move the mouse cursor to the bottom edge of the screen. At that point the taskbar rises to visibility. I happen to prefer that setting.

One taskbar function that few people seem to be aware of, assuming “Lock the Taskbar” is not checked, is that by simply moving the mouse cursor to the top edge of the taskbar, a double-headed arrow appears. With the double-headed arrow visible, a left click and hold will allow you to move your arrow up and in-crease the number of lines that the taskbar covers, to half the screen if you want, or vice versa. Increasing the height of the taskbar allows you to have more of the larger icons that are easier to read.

The taskbar incorporates a large number of functions that could make your computing life easier if you studied up a bit on all the things that it can do. When you right-click on the taskbar, the first item on the window that pops up, at the bottom, is taskbar settings. It is recommended that you click on that and read all of the possible variations that the settings screen allows you to make. In particular, the section on system icons. ❑

Thoughts from a Clicker

Author: Tiny Ruisch, Member, Cajun Clickers Computer Club, LA

a ugust 2019 issue, cccc c omputer n ews

www.clickers.org
tsa70785 (at) gmail.com

This month I'm going to rant, rave, criticize and complain just a little. About a year ago, before I moved to the Baton Rouge area, my wife and I were in one of the home improvement stores. I thought that it would be a good time to pick up a new water filter for our refrigerator. I went over to appliances and told them I needed a new filter for a Whirlpool. He immediately asked me which of the nine filters I needed. Of course, I didn't have the filter number memorized. So, I found our refrigerator on the sales floor and told the salesman, "One to fit that model." I got home and found that it was the wrong size filter. When I went back to exchange it, I found out that a different model year almost always uses a different filter.

What does all that have to do with computers and electronics? It got me to thinking about some things I hate about technology. I've probably got 10 or 20 different USB cables in the junk box in my computer room. Every time you buy something that is USB supported, you get another cable. Why is this? It's because each manufacturer has their own proprietary plug. They have to include a cable because none of my other 20 cables will work with the darn thing. I recently got a new cell phone. Same manufacturer, different model. You guessed it. I've got another USB cable in my collection. Wouldn't it be nice if everything had a standard plug and didn't have the cable included? Think of the money that could be saved. Wait a minute! Then they couldn't sucker people into paying $20 for 3 dollars' worth of wire.

Another thing that makes me mad are End User License Agreements (EULA). I'm one of the few people who research them before installing anything on my computer. My complaint isn't the fact that lawyers write them by lawyers. I can use the internet to explain the legal terms. My objection is that I have seldom found a EULA that can be read full screen. Instead they write them in a little window that usually covers about a tenth of my screen. I think this is done to discourage people from reading the agreements. Just get them to click "I agree" and get it over with.

I can live with SPAM (I usually don't even see it). I don't mind getting bombarded with internet advertisements (I can always go to other sites). What I hate it when websites pop up a window asking for information that they will likely never use. For instance, there is a website that I won't name that wants to know my age, sex and country. They then store the data in a cookie on my computer. When I tell them that I'm a 28-year-old female, I get the same advertisements as the dirty old men get. Why do they waste my time? I also dislike software that isn't user-friendly. Some programs have windows that can't be resized. I'm getting older and my eyesight isn't what it used to be. If I can't make the window bigger and read the font, I likely won't use the software. Then there is software that won't let you choose where to install it. I don't install all programs into "program files". Many times, I don't even install them on the C drive.

Continued..page 31

BREVARD

B U G Officers

President

Bill Middleton

President@bugclub.org

t reasurer

Loretta Mills

Treasurer@bugclub.org

s ecretary

Bill Middleton

Secretary@bugclub.org

m ember a t Large

Jim Townsend

Webmaster

Chris Crisafulli

Webmaster@bugclub.org

s pecial i nterest g roups

b eginners' sig :

beginners@bugclub.org

Hardware (t inkers) sig :

Bob Schmidt 952-0199

hardware@bugclub.org

bug Web Page

http://bugclub.org

Brevard Users Group Secretary's Report

By Bill Middleton

Monthly General Meeting Report, November 11, 2019

1. The meeting was called to order by President, Bill Middleton at 3:30 PM.
2. Members were urged to pay their dues and make sure their registration details were up to date. . Dues may be paid at any meeting or mailed to the BUG Club, PO Box 2456, Melbourne, FL 32901. Please make sure your current email is included with any mailed-in dues. We've almost got the mailing list for this newsletter straightened out, but two members reported they didn't get last month's newsletter. We'll try again...
3. The ever-ongoing Windows 10 updates were reviewed. No one reported any major problems with Updates, but few had the 1909 Feature update installed, yet. Installation has been reported faster & easier than previous Feature updates.
4. The new version of the BRAVE browser was displayed & demonstrated including the TOR mode for greater security & going to the dark side (of the Web).
5. The current hard drive connections of SATA I, II &III, M2 and NVME were explained.

6. Two new gadgets were discussed: the Facebook Portal cheap Mesh Router and the Bitdefender Box security device.
7. Members were urged to come to the December General Meeting which will be our annual Security briefing, this time by the Florida State Dept. of Consumer Affairs.
8. A few other, previously-discussed problems were revisited.
9. The meeting was adjourned shortly after 3:30.
10. Respectfully submitted by Bill Middleton, Secretary.

Hi,

The December schedule is upon you. The Viera meeting will be, as expected. on Monday, Dec. 2 at 2:00pm. This meeting will feature a Chromebook demonstration, Update Agonizing and a Q&A session with Chuck.

Our Eau Gallie Meeting will be on Monday,Dec. 9 at 2:00 will be a SECURITY briefing by The State Dept. of Consumer Affairs on current Cyber threats and scams in Florida. Note that the Dept. of Consumer Affairs is NOT in the Attorney General's office (which gave us a briefing two years ago). Everyone is urged to attend this meeting - it could be Verrrry enlightening. (John - please mention this meeting in the notice for the Viera meeting. Thanks).

The Fee Ave. meeting will be at 1:00PM on Monday, Dec.16. Content will be similar to the Viera meeting. Note: a 2:00 time slot has been obtained for this meeting starting in January, 2020

Because of the Security Briefing, Election of Officers, is being postponed until the January General meeting.

Bill M

Bug Club Treasurers Report

by Loretta Mills, Treasurer

c hecking a ccount	**July 1, 2019**
Beginning Balance	$ 1052.36
Ending Balance	$ 1052.36
Saving Account Balance	$ 1087 65
Combined Balances	$ 2140.00

Thoughts from a Clicker.............from page 29

I wonder if Microsoft will ever fix one little thing that has bugged me for as long as I remember. When you use file explorer to copy, move or delete a list of files; Windows estimates how long it will take. If you're doing an operation on a lot of files, the estimated time will change every time you check it. On older systems it can be even more aggravating. Wouldn't it be nice if the estimate was close once in a while?

Hate might be too strong of a word, but I've always disliked how companies will use a proprietary document format. The perfect example is word processing. Why must each program have a different extension? Is it good for a business to make consumers remember .doc, .odf, .wps, .docx, .odt, .txt, .rtf,.abw,.abi and hundreds of others? Almost all word processing software has a save as feature to save files to other formats. They can't be that much different. Why isn't there a standard where all programs save in a standard format? After all, this idea seems to work well for HTML internet files.

That's enough ranting and complaining. Next month I promise to write something useful for the newsletter. By the way, did I mention that the two water filters had two different prices? Does that remind you of anything else technology related?

Keep on clicking and thanks for reading. ❑

Going North for the summer
or coming back?
Don’t miss a single issue of your

Space Coast PC Journal

If your email address will be different

Please give us the correct email

f or your temporary location

*****Reminder*****

We need your e-mail addresses!

We’d like to keep in touch with you, especially if there is a last minute change in venue for the club meeting.

Please send e-mail addresses and changes to
Linda Glassburn glassburn@earthlink.net

Are you having problems with your hardware or software?
Did you find the solution yourself?

How about sharing that information with your fellow club members? Sit down for a few minutes open up that word processor and put your ideas to paper. Aside from the value to the members, you’ll get your name in print!

Don’t worry about the details, we’ll edit it for the best appearance and presentation.

Calendar of Events

December 7, 2019 - Learning Center
Merritt Island Library
12 - 3:30 Pm

December 14, 2019 Annual Christmas Party Merritt Towers Clubhouse
12-4 Pm

December 31, 2019 - Deadline for Journal input

January 4, 2020 - Learning Center
Merritt Island Library

January 16, 2020, 2019 - SCPCUG Meeting
Merritt Island Library Auditorium
2:00 Pm

January 31, 2020 Deadline for Journal Input

Presentations Schedule

December 14, 2019

Christmas Party 12-4 PM
Recreation Building
Merritt Towers Condos
Sykes Creek Parkway
East of JC Penney
Merritt Square Mall

Beginners or Advanced
Bring Your Questions
Get Technical Help
Share Your Knowledge

at Your SCPCUG

Learning Center

Open 1st, 3rd, 5th Saturdays,
12 to 3:30 p.m.
Merritt Island Library
Conference Room

Please restrict your visits to these times.

Bring your hardware or software problems,
We'll do all we can to help.

If you bring a desktop computer please bring the keyboard, mouse, and power cord

Call Ron Ingraham, 321-777-2578, for more information.

The
Space Coast PC Users Group Journal

is produced using

Adobe InDesign CS3

All SCPCUG club members are entitled to receive the electronic version of the Journal in pdf format. You'll need Adobe's widely available Acrobat Reader X.X (free) to view the eJournal.

Contact Ron Ingraham
ringram28@cfl,rr,com to get on the eJournal mailing list

Space Coast PC Users Group is proud to be a Charter

Member of
Association of Personal Computer User Groups
APCUG

The Space Coast PC Users Group's

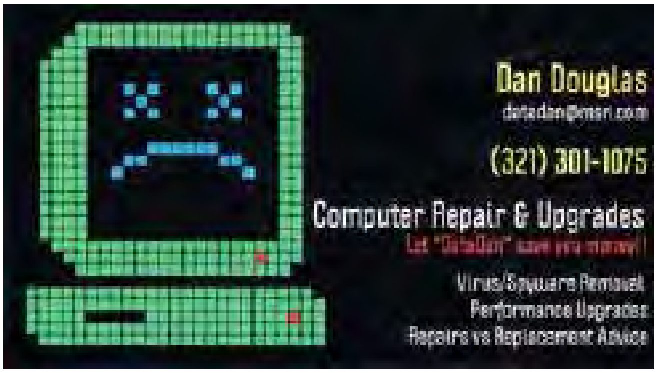
Computer Doctors
Make House Calls

Free **to**
SCPCUG Members!

Dan Douglas, owner of
Data Dan Computer Services,
will accept phone requests
for computer assistance
(321) 301-1075
After a phone call, a house call may be made within 5 miles of Merritt Island

Free Remote Support
For those using Windows 10
Quick Assist

The above member will help you with ***a particular*** computer glitch on your personal (not business) computer. In some cases, he may even make a house call. But, please do not expect him to install your computer nor teach you how to use it. If you have continuing problems or need additional help, please take a class, or check the ads in the *Journal* and hire a consultant, etc.



Dan Douglas
datadan@msn.com
(321) 301-1075
Computer Repair & Upgrades
Let "DataDan" save you money!
Virus/Spyware Removal
Performance Upgrades
Repairs vs Replacement Advice

Computers 4 Kids

C4K Volunteers Need
Donated

Computers, Keyboards, Mice
etc

for

Building PC Systems

complete with software
for

Needy School Children

Call

Ken Clark @ 223-7402

To arrange pickupF

Space Coast PC Users Group, Inc.
MEMBERSHIP APPLICATION

membership dues
$25.00 [ ] Check [ ] Cash

Check No. ____________

NAME ____ [ ] New [ ] Renewal

ADDRESS ____ Date ____________

CITY ____________________________________ STATE _________ ZIP _____________

Home Phone _______________________ Work Phone (Optional) _______________________

E-mail ____

Would you like to attend: a class for BEGINNERS? [ ]
an ADVANCED DOS class? [ ]
a WINDOWS class? [ ]
an ADVANCED WINDOWS class? [ ]
What other topics would you like covered in a class? _________________

Do you have expertise that you would like to share? Please describe.
____ □

Would you be willing to be listed in the Helpline of the *Journal*?
If so, what subject? _____________ Calling hours: ___________
Phone _____________ E-mail _________________

Would you like to help the Club in the following areas?
Resource Center Staff ______ Journal Staff ______
Computer Doctor ______ Room Setup ______ Teach Class ______
Other ______

What topics would you like to see for monthly programs?

What can the SCPCUG do to help you and others?

If you were told about the SCPCUG by a club member, write that member’s name here ____________________________________

DRAM

Are You

CPU

Bewildered?

HTML

Windows

Modem

Join the
Space Coast PC Users Group
and learn the lingo!

Membership benefits:
- The *SCPCUG Journal*
- Computer Literacy Classes (e.g. Windows 7-10)
- Seminars and Workshops
- Computer Doctors - computer help - **FREE**!
- Group Purchases, Raffles, and Door Prizes!
- Helplines - get help from the experts

Join Now!

make check payable to: Space Coast PC Users Group

mail to: sc Pcug , 801 del rio Way, #304, merritt island, fl 32953

ADVERTISING RATES

SIZE	1 Month	3 Months	6 Months	1 Year
		~10%*	~15%*	~ 25%*
Full Page	$90.00	$243.00*	$459.00*	$810.00*
Half Page	45.00	123.00*	230.00 *	405.00*
1/4 Page	23.00	62.00*	117.00*	207.00*
Business Card		35.00	59.00 *	105.00*

* = Discount from regular monthly rate. Discount applies to ads running in consecutive issues.
Payment **must** accompany order. Make checks payable to:

Dimensions (W x H) for ads are as follows:

Full page:	7” x 9 1/4”
Half page:	7” x 4 3/8” or 3 3/8” x 9 1/4”
Quarter page:	3 3/8” x 4 3/8”
Business card:	3 3/8” x 2”

Camera ready ad copy is due by the 28th of the month to ensure that the ad will appear in the next issue. Mail ad copy to the Editor at1360 Mayflower Avenue, Melbourne, Fl 32940-6723 Prices will be quoted for design work. Questions? Call (321)777-2578.
All advertisements are subject to the approval of the Editor.

SPACE COAST PC USERS GROUP, INC.
801 Del Rio Way, #304,
Merritt Island, Fl , 32953

Statement of Purpose

The Space Coast PC Users Group is an independent, not for profit, computer group open to anyone interested in computers. It is not affiliated with any business. Our purpose is to serve as an educational, scientific, and literary organization designed to enhance computer literacy.

Disclaimer : Neither the Space Coast PC Users Group, Inc. (SCPCUG), its officers, board of directors, nor members make any expressed or implied warranties of any kind with regard to any information or offers disseminated in th~~e *Journal* via advertisements or articles, including but not limited~~ to warranties of merchantability and/or fitness for a particular purpose. Opinions provided by *Journal* articles, or by speakers, members, or guests who address the SCPCUG meetings are individual opinions only, and do not represent the opinions of the SCPCUG, its officers, the board of directors, or members. All opinions, information, and advertisements should be carefully considered by every individual and neither the group, its officers, board of directors, nor members shall in any respect be held responsible for nor be liable for any and all incidental or consequential damages in connection with or arising out of the furnishing or use of any information, advertisements, or opinions provided by or through the Space Coast PC Users Group.

Initial Membership $25 . Annual Dues have Been Suspended

benefits : Members get the monthly *Journal*. In addition, <u>only</u> members can:

· copy from the Shareware library
· participate in meeting drawings
attend special seminars/workshops
talk to one of our computer ‘doctors’
· use the Helplines

NEXT MEETING
December 14, 2019

Christmas Party Recreation Building Merritt Towers Condos
Sykes Creek Parkway East of JC Penney Merritt Square Mall
12-4 PM