The Space Coast PC Journal

July 2020 Vol. XXXVI Issue VII

Fleeceware: The Big App Rip-Off — Plus 5 New Coronavirus Scams

By Scambuster Keith. Scambusters Newsletter, June 3, 2020

People who use smartphones and tablets are being warned about an avalanche of fleeceware that could potentially take them for a small fortune.

“Fleeceware” is a relatively new term to describe apps that simply rip off users, either by overcharging them at the outset, or sneaking up on them after they’ve installed the app with new and often recurring charges.

A report a few months ago from online security firm SophosLabs -- who coined the fleeceware term -- claimed that more than 600 million copies of 25 offending apps had been downloaded by Android users. More recently, the firm says it has found 30 fleeceware apps on Apple devices.

The problem for both Google (which runs the Google Play store for Androids) and Apple (for iOS apps) is that the software is not illegal or malware-laden, so it may not initially be spotted through security checks.

Both firms have acted to remove apps when they become aware of the excessive charges but then others appear, more notably on Android devices.

Tech magazine Wired explains: “Though fleeceware apps don’t grab your data or run ad fraud from your device, they often flout the standards that Apple and Google set for when and how developers can present in-app purchases and subscription fees.

“Some claim to offer a trial period but will prompt you to pay the first time you open the app. Others say that a subscription will be one amount

Continued.........................page 4

The Monthly Publication of the Space Coast PC Users Group, Inc.

Visit Our web Site at www.scpcug.com

July 2020 Vol.XXXVI Issue VII

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

JOURNAL STAFF

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

From The Editor

As it has in most areas, the pandemic has had its effect on us. Because the library was closed, we were unable to conduct the Learning Center meetings as well as the General meeting.

Some thought was given to using some form of video conferencing to take up the slack. Because of limited numbers of participants in some of these programs it was finally decided to just accept the fact that meetings could not be held while closure was in effect.

The library opened its lobby for book borrowing and return, but the meeting rooms remained closed.

This month they informed us that the auditorium would be available for meetings with the safety measures in effect. So this month's meeting was scheduled.

Even if the Conference Room was opened, we decided that spacing requirements would severely limit the number of attandees and would pose unacceptable risks to those who could attend.
Maybe next month.

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			
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	338-5414

yjm1938@yahoo.com.

.

Professional also includes DriveScrubber, a utility

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 Articles

Fleeceware........................ 1
Tech Trek..................................8
What to do 11
Scambuster Under Spell..........14
Fixing a Sluggish PC............. 16
Chinese APP Adapter..............17
Ask Leo..................................18
Video Conferencing..................21
ZOOM: Is it Safe......................23
Smart Devices At Home 26
Cleaning a Hacked PC............29
Google Sued.............................31

.

Regular Articles

From the Editor...................2
From the Cashier's Cage......5
Dan'sDesk...........................6
Webmaster Wanderings........7
Brevard User Group...........30

Notices

Presentations Schedule......32
Calendar of Events................32
Learning Center......................33
Computer Doctors..................34

Presentation
June 18, 2020

Meet in the Auditorium
2 PM
Get together welcome meeting
Discussion, Q&A

Bring Some Friends

Fleeceware.....................................from page 1

in most of their app materials, but then actually charge a higher fee at checkout."

The apps also exploit users who don't know how to cancel subscriptions and, in some cases, ignore even those who do know and try to cancel. They just keep on taking the money.

Obscene Fees

Some of these rogue app developers are charging what Sophos refers to as "obscene fees" for fairly basic products. A horoscope app, for example, was offered at $70 -- not for a year or even a month but for a week. That adds up to more than $3,600 a year!

According to Wired, fleeceware is often found in the same genre of apps that are used for mobile scams and attacks.

"These are generally benign-looking tools like simple photo and video filters and editors, horoscope apps or fortune-telling tools, QR code and barcode scanners, or utilities like flashlights and custom keyboards," magazine senior writer Lily Hay Newman explains.

Sophos also suspects that some of these scammers may have found ways of posting fake five-star reviews about their apps to encourage users to opt for them. They may also disguise the fact that what appears to be a monthly fee is actually charged weekly.

Another trick is to set an impossibly short free-trial period and then hit the victim with an annual lump sum fee. If they don't cancel within as little as 48 hours, they face a full year's subscription.

Both Google and Apple claim to be tightening up on attempts to sell fleeceware on their app sites. Google has changed its policies on making charges explicit from next month and Apple's rules already prohibit unreasonable pricing or the use of tactics to lure in victims and then charge them more.

"While pricing is up to you," Apple tells developers, "we won't distribute apps and in-app purchase items that are clear rip-offs. We'll reject expensive apps that try to cheat users with irrationally high prices."

But these policies may still leave a little wiggle room for scammers, since the question of what is reasonable is a matter of opinion rather than fact.

How Not to Get Fleeced

So, what can you do to avoid fleeceware scams? Here are seven key actions:

1. When considering buying an app, check reviews elsewhere, not on Google Play or the App Store. Also beware of five-star reviews that just use two or three words.

2. Compare prices and features of similar apps.

3. Preferably buy apps from established developers who already have good reviews of multiple products.

4. Use the "subscriptions" feature on your device (look it up if you don't know how) to see exactly how much and how often you're paying, or to cancel these subscriptions. This isn't infallible, though. In a trick encountered by a Scambusters team member, multiple "free" apps were used that eventually required him to pay a subscription outside of the official stores. The developer then ignored all his cancellation requests and he was forced to change his credit card account to stop the scam. Fortunately, the credit card company refunded $90 of payments the scammers had already taken.

5. Don't sign up for free trials offering less than a week of use.

6. Read the small print in the app's description. Again, this isn't infallible but

From the Cashier's Cage

Financial Report for Month
Ending May 31, 2020

<u>CHECKING</u>	
Beginning Balance	**19.87**
Deposit - USB sales	**160.00**
Ending balancee - includes $18.41 snack fund	
179.87	
<u>SAVINGS</u>	
Beginning Balance	**305.05**
Transfer to Checking (100.00)	
Interest	**.03**
Ending Balance	**305.11**
<u>TOTAL ACCOUNTS BALANCE</u>	**484.98**

if it's poorly worded or confusing, that's certainly a red flag.

7. Know that, despite what you may think or are tricked into believing, removing a fleeceware app from your device doesn't cancel a subscription.

5 Latest Coronavirus Scams

Here's a brief rundown of latest Covid-19 scams and misleading claims that have crossed our desks in recent weeks:

- The US Federal Trade Commission (FTC) has warned another 50 firms about making unproven or misleading claims about products they suggest can help treat or prevent the virus. Company names here: https://tinyurl.com/FTC-covid-list

- Malware-infected Excel spreadsheets are being sent out as email attachments purporting to come from respected organizations. The spreadsheets supposedly carry data and updates on the pandemic. Don't click on them!

- Crooks are posing as members of contact tracing teams. They make calls or send out messages saying the recipient may be infected and then ask for personal details such as Social Security numbers and financial account details. Genuine tracers won't ask for this information.

- Scammers are cashing in on stay-at-home victims' desires for pets as company. Posing as breeders, they offer pets at outrageous prices and then simply disappear with the money.

- Don't believe the latest "free groceries" scam that claims retailer Target is giving away products. A text or email message says the recipient is entitled to $175 worth of groceries. But if they click the link in the message, all they end up with is malware.

That's it for this week but stay vigilant for those Coronavirus scams. They're spreading almost as fast as the disease! ❑

"In return for an increase in my allowance, I can offer you free unlimited in-home computer tech support."

Dan's Desk

Back to business (somewhat)!! Starting June 18, we'll be resuming our monthly meeting schedule. We'll be in the large auditorium, well-spaced out and masks are encouraged. Saturday learning sessions are still on hold as the Merritt Island Library has not re-opened on Saturdays yet, hence no available meeting rooms.

The recent release of Windows 10 version 2004 has been released and you should be seeing it on your PC soon if not already installed through the regular automatic Windows update procedure. I've installed it on about 20+ PCs so far with no issues that I've seen. I've noticed a few tweaks here and there, but nothing major to confuse your normal interactions. You can go to the Update section of Settings and there is a link to take you to the Microsoft web site that has all of the details of the changes contained in this release.

I look forward to seeing you all again at some future meeting and until then stay safe!

.

If you have suggestions for topics that you would like to see explained, please let me know! ❑

"We forgot to back up our files, so we're asking everyone to remember everything they've typed during the past 10 days."

"We can't replace your old computer. That would be age discrimination."

Webmaster Wanderings

Jere's Tech Tips

Windows, Android, Linux tips from Jere Minich, Advisor, Region 5 (AL, FL, GA, SC).

New items include:

How to Use Your Android Smartphone as a Webcam on Windows 10

Google Messages Tops 1 Billion Installs on Android

The Best Chrome Extentions for Online Safety and Security

How to Check the Now Playing History of Songs on Google Pixel

USB 4 Specs and Features: Everything You Need to Know About the New Double-Speed USB

What is Cell Phone Contact Tracing?

The 10 Best Free eBook Download Sites

10 Windows Task Manager Tricks You Probably Didn't Know.

https://apcug2.org/jerestips/

: APCUG 2020 Summer & Fall Online Workshops

- Get to Know Windows from An Insiders Point of View at 12pm ET the second Wednesday of the month (May 13, June 10, July 8, August 12). These four 2-hour workshops will be on how to get the best out of Windows 10. There will be how-tos, hands-on demos, and discussion with ample time for Q&A. Moderator is Bill James, APCUG Advisor, Region 8.
Week 1 - What's New with Windows 10, the 2004 Spring Feature Update
Week 2 - Settings
Week 3 - File Explorer
Week 4 - Edge

APCUG 2020 Summer Online Workshop Week 1 -

Week 1 of the Online Workshop - "Getting to Know Windows from An Insiders Point of View" was held May 13. Week 1 covered "What's New with Windows 10, the 2004 Spring Feature Update." Our SCPCUG Membership Chairperson Linda Glassburn attended and provided a link to the Presentation Video and 2 PDFs. The PDFs are available for download on the Special Events page as well as the link for the Presentation Video. The Presentation Video runs 1hr 38min followed by a Q&A. Total video time is 2hrs 34min.

APCUG's Spring Virtual Technology Conference (VTC-36)

APCUG's FREE 2020 Spring Virtual Technology Conference (VTC-36) was held May 2. Topics included: Let's Go Shopping; Audible Audio Books; A hearing revolution with healthable devices; Digitize old album photos into Google Photos and Chromecast to TV; What's happening with your group while everyone is staying safer in place? View Presenter Bios and get links to Presentation PDFs and YouTube Videos when available at: https://apcug2.org/apcugs-free-2020-spring-virtual-technology-conference-vtc36/

2020 APCUG Virtual Technology Conference Dates - Future 2020 VTC dates: Aug 15, and Nov 7.

1 New Link

Voicebot.ai - Covers Market Data, Stats, and News for Various Artificial Intelligence Voice Assistants. Also has Webinars and Podcasts along with Latest News on Devices Using Amazon Alexa, Google Assistant and Apple Siri. https://voicebot.ai/ (http://www.scpcug.com/infolink.html) -

At Voicebot our goal is to gather in one place the most important news, commentary, research and analysis of voice technology. While other publications will cover AI generally, chatbots or related technologies, our focus will be on the emerging voice segment. Voice is the user interface change that will drive a new industry and a new way for people to interact with and control computing

Continued.......................................page 8

resources. We publish both original content and provide links to relevant third party content at Voicebot.ai, distribute a weekly email newsletter and host the weekly Voicebot Podcast. We also produce original research. and industry analysis for general publication and for private consumption. The editorial decisions are solely the responsibility of the Voicebot team and do not necessarily reflect those of our partners, customers or other organizations.

Misc Items

Windows 10 Patch Tuesday for May 2020

This update rolled out May 12 with plenty of security fixes. Microsoft patched 111 vulnerabilities across 12 different products, from Edge to Windows, and from Visual Studio to the .NET Framework. Of the 111 vulnerabilities, 13 are classified as Critical, 91 as Important, 3 as Moderate, and 4 as Low. This patch was the third-largest in Microsoft's history. March 2020 had 115 bugs patched and April 2020 had 113 patched. There were no actively-exploited zero-day vulnerability bugs requiring patching this month but threat actors are regularly in search of bugs that can be easily exploited. It's really critical to update asap.

Windows 10 May 2020 Update

People have asked when is the new version of Windows 10 coming out. The Windows 10 May 2020 Update (also known as version 2004 & 20H1, and previously as the April 2020 Update) is expected to roll out to mainstream users on May 28. This version will bring new features to help with productivity, security, and speed. ZDNet says the update should take between 7 and 17 minutes to install. Microsoft will now end support for Win10 ver1809 (the October 2018 update) Home, Pro, Pro Education and Pro for Workstations editions in November 2020. It was originally scheduled for May 12, 2020 but is now delayed due to the impact of Coronavirus.

Windows 10 Ver1909 on 33.4% of PCs

Per AdDuplex Win 10 ver1909 is now being used on 33.4% of all Windows 10-based PCs. That's up 5% from last month. This is based on a survey of roughly 100,000 Windows 10 PCs. Versions 1903 and 1909 combined now account for 82.6% of all Windows 10 PCs in use, up from 78.9% last month. Due to PCs being upgraded, ver1903 percentage actually went down while ver1909 usage went up.

Smart Speakers Adoption Rate Increases

The total U.S. adult population is 255 million. A Voicebot consumer survey in January 2020 found 87.7 million U.S. adults are using smart speakers. The addition of over 20 million new smart speaker owners in 2019 raised the installed base of users to 34.4% of U.S. adults. Smart speakers have been the most vital new consumer electronic device segment over the past five years. Smart speakers are important because they provide a new interactive digital endpoint in the home, thus providing access to over one-third of U.S. adults. This endpoint

President's Corner

Tech Trek - Traveling with Technology Part 2 - The Tech You Leave Behind

Author: Greg Skalka, President, Under the Computer Hood User Group

December 2019 issue, Drive Light

www.uchug.org
president (at) uchug.org

We all use a lot of technology in our everyday lives - various devices and services that make our lives better. They help us communicate, keep us safe and well, inform us, get us where we want to go, get us the things we need and entertain us. When we travel, we usually want to take all those benefits along with us.

Many of the tech devices and services we use every day are the "don't leave home without them" kind you will insist on taking on your trips. Smartphones, laptops, tablets or e-readers, digital cameras, music players, noise-canceling headphones and GPS devices are all devices that can

enhance your travels when you bring them along. Technology has revolutionized travel planning and arranging, with the Internet the main way most people now research and book transport, lodgings and entertainment for their trips. With the arrangements covered and the devices packed, many forget that technology can also help protect the home, possessions, resources and loved ones you may be leaving behind. The tech you take on your travels is important, but also important is the tech you leave behind.

The more you have, the more you have to protect while away. There are plenty of tech products and services to help keep your stuff safe and allow you to have peace of mind while traveling. Your home is often your biggest asset; no one wants to return from vacation to losses from theft or damage. Your resources and data need to be protected and possibly accessed safely while away. You may need to leave pets, elderly relatives or others behind, perhaps under someone's care, while traveling. Knowing that everything back home is fine can help you have a more enjoyable trip.

Just as with trip planning, making arrangements to protect your assets while away must be done well in advance. There are lots of ways technology can help, but few benefits can come when planning starts the night before. Fortunately, the same things that can help protect your stuff while on a monthlong cruise can also be of benefit when you are just away for the weekend, or simply at work or out to the store.

Your local police can provide plenty of tips to help reduce the chances of your house being broken into while away on a trip. Things like making sure your doors and windows are closed and locked and ensuring your house looks occupied are just common sense. Having lights come on and off, making sure the landscaping looks maintained and not all dried up and preventing packages, newspapers, and mail from piling up out front are important in discouraging burglars from picking your home as a target. Technology can help with all of these.

A home alarm is one important tech item to leave behind when you travel. No matter how simple or complex, whether externally monitored by a company or only by the homeowner, any security system is better than no security system. While you can contract with a security company like ADT to install a system in your home and monitor it, there are also many good systems available for self-installation. Technology has made home security more capable and available at a low enough price point for everyone to have some protection.

I know a lot of folks that have the SimpliSafe system; it has come to define the moderate-cost self-installed security system. Amazon's Ring Alarm Security System and Google's Nest Secure are among others competing in this same space. These systems start in the $200 to $400 range for basic setups, but more sensors, cameras, and accessories can always be added. They can be self-monitored or professionally monitored for $10 to $20 per month. Most can be part of larger smart home setups with other products, including voice-activated assistants.

Network home monitoring cameras are also useful ways to provide home security, with or without an alarm system. They can be set to inform you of unexpected activity or noise, like an alarm system. They are also useful for periodic checks on pets or family members left behind. They are typically Wi-Fi cameras and can be battery or line-powered, with prices ranging from $40 to $300. With apps for setup and monitoring, motion detection, video, and audio monitoring, media and cloud storage, email and push notifications and night viewing capabilities, they can be mini-security systems by themselves.

I've had and used network cameras at home for many years. Like a lot of tech products, however, no device or service is perfect or works perfectly all the time. I'm a big believer in diversity and backups for tech gear. On my most recent vacation trip with my wife, I had three different network camera types set up to monitor our home.

My oldest cameras are Samsung SmartCams; I've had three for about two years now. You can live-view from their web site (through IE only) or app, and store video on the internal micro-SD card or to their cloud account (subscription fee required). They have infrared LEDs for night vision and can

Continued...page 10

Travelling with Technology...........from page 9

be set to provide email or push notifications to your phone if audio or motion is detected (it can attach a captured image to the email, so at least you have that if the camera is taken). These work pretty well, but I have not found a way to set them up to completely avoid false triggers (I'd get a few each day). There were also a few days on our trip when something must have been wrong with their web service, as I could not access any of these cameras. Fortunately, I had others.

My wife gave me four Blink cameras for Christmas last year. At the time they were a private company, but now they are owned by Amazon. They are waterproof and battery-powered, so they are more versatile in terms of placement. Because they are limited by battery power, they should not be viewed in continuous video mode for long. I mostly take snapshots on them or use their motion detection to send notifications to my phone. They have free cloud storage, so you will have video clips to show the police if your cameras are taken in a break-in. The batteries are supposed to last 1-2 years under normal use. They work very well as a security system, less so if you just want to observe a live stream of someone you left at home.

My third camera is a Panasonic HomeHawk indoor camera. It is a lot like the Samsung, but is newer, costs less and seems to work a bit better. While its notification and recording functions seem to work well, its app menus make it less convenient to use. The Blink camera app is the most convenient, as each camera has a single button in the app to enable/disable detection, notification, and recording. For Samsung and Panasonic, you must enable motion detection and sound detection separately, in addition to notification and recording; these are on several app pages. The Panasonic camera seems to work well as a security camera, but like the Samsung, it is more difficult to switch between "home" and "away". It also can't preserve an image or video of a break-in anywhere but on its own internal memory.

Another important aspect of protecting your home is making it look like you are not away when you are. Lots of new smart home devices can help with that. There are sophisticated systems that can control lights and draperies, but simple and inexpensive smart bulbs and light controllers can provide much of the same capability. There are many companies that make these items. They are all typically connected through Wi-Fi, controlled through apps and almost always can integrate with Alexa and Google Home Assistant.

Again, for robustness, I currently use three different smart light products. Belkin makes Wemo smart home products, including smart plugs and light switches. I have several of these smart plugs with lamps connected to them. There are many companies making smart bulbs, which simply replace Edison-base light bulbs in lamps and light fixtures. I currently have smart bulbs from TP-Link and Feit Electric. These are easy to install and many have dimming and color-changing capabilities. While the apps often provide the ability to schedule light events, on my last trip I simply switched lights on manually through the evenings with my apps. The apps give feedback that the light was switched, and I could also confirm this by looking at my network cameras. I've found these smart light products work very well.

For those with extensive landscaping, Wi-Fi smart sprinkler controllers can keep your irrigation going while away or at home. They often have rainfall sensors or weather monitoring capabilities to help save water as well.

Indoor water should also be considered for control when traveling. Many years ago, a good friend returned home from a trip to find a stream of water running down his driveway. A plumbing failure has caused a leak; his prolonged absence had allowed water to flood the inside of his home, resulting in major water damage and extensive renovation costs. Ever since I've always shut off the main water valve into the house (and shut off the water heater) right before leaving on a trip. It also serves as a plumbing test on our return; if I hear a flow when the valve is turned on again, it means I have a slow leak somewhere that I need to locate.

Leaks can cause damage anytime, whether you are away on vacation or just to the store, or even while you sleep at night. There are many new smart home electronic water shutoff systems available

to continuously monitor and protect your home from water damage. Some, like Belkin's Phyn device ($600), are connected in line with your water supply pipe and can monitor the flow and cut off the water to the house if a leak is detected. Others, like the Guardian Leak Prevention System ($200), use water sensors placed at likely leak sources to automatically rotate your existing main water shutoff valve (no plumbing change required) and shut off the water. The Xenon Smart Wi-Fi Water Valve mounts on your existing water valve in a similar way, allowing your water to be shut off by Alexa, Google Assistant or through an app. The Streamlabs Wi-Fi Home Water Monitoring System ($140) takes a different approach, ultrasonically monitoring the flow in your home supply line (it clamps on the pipe with no plumbing changes) and alerting you via a notification on your smartphone to shut off your water valve manually. Even Zircon's $44 Water Leak Detector could provide a useful warning to your smartphone if it detects water where it is placed.

Electronic locks and safes can help provide additional protection for your home's contents and valuables while traveling. The Schlage Encode Smart Wi-Fi Deadbolt replaces your front entry lock and allows remote management of the lock through an app. This allows you to lock your door while on the way to the airport if you forgot to or let in a trusted friend to check on that possible leak while away. Electronic safes are great for locking away valuables and that computer backup you should have made before traveling; many are not expensive. A USB external hard drive with hardware encryption, like the Western Digital My Passport drives, provide an easy way to protect your most valuable data while away. Simply copy all your important data or backups to the encrypted drive and leave it with a trusted friend before departing (with encryption, you don't have to trust them absolutely).

While you can get a neighbor to pick up your newspaper and mail when on travel, some of us, unfortunately, may have closer relationships with fellow online gamers in other countries than with the people that live across the street. It is good to have a neighbor watch over your place, but if you are not sure you want your neighbors to know your home or apartment is temporarily vacant, technology can still help. I now get the newspaper electronically as a pdf so I can read it remotely, help the environment and avoid a pile of papers on the driveway while on vacation. You should contact the USPS to stop your mail delivery while you are away (you can set it up online). If you are concerned about mail theft, you can also sign up for Informed Delivery on the USPS web site. This allows you to view images of letter-sized mail that will be delivered to you and manage package deliveries. This could allow you to determine if mail is being stolen from your box.

No matter where you travel, you'll want to know everything you left of value will be there when you return. If you leave the right technology behind, you can monitor and control your home and property remotely and be assured there is no place like home to come back to. ❑

What to do when Windows can't run *EXE*s

By Fred Langa

Executable program files are the beating heart of Windows and most applications.

So when Windows 7, 8.1, or 10 can no longer properly run files with the **.exe** extension, it's serious trouble! Here are four fixes that can help.

Plus: Several weaknesses hobble Win10's print-to-PDF applet.

PC sidelined by weird executable problem

AskWoody Subscriber Colm Brangan's PC somehow ran into the deep weeds — and now he can't find his way out. (Colm's PC is running Win7, but Windows 10 and Win8.1 can suffer the same fate.)

- "My Windows 7 Home Premium system has

Continued...page 12

What to Do..............................from page 11

> stopped working properly. None of the EXE files will run. (I can still get to the Internet via links.) Launched apps stop with a **ShellExecuteEx has failed Error Code 1155.** I can't reboot with a USB-based rescue drive because **setup.exe** will not run, and right-clicking an application doesn't show a **Run** command.
>
> "As my laptop is old, I don't have the option to choose UEFI boot; it needs the **Legacy** bios. I have the original re-installation disk and your excellent article on 'Win 7's no-reformat, non-destructive reinstall.' [Langa.com copy here]. Your help, please! All other avenues, including Microsoft and Dell, have failed."

That's a frustrating problem, to be sure. But it might be easier to correct than you think.

A typical Windows7/8/10 setup contains between 3,000 and 5,000 executable files — just for Windows. So if the OS truly can't run ***any*** EXE files (say, through a system-level file-association/-permissions error), it wouldn't run much at all.

But your PC ***does*** run — just very weirdly! That suggests your PC's system-level EXEs are more or less OK and still working, but EXEs you click on (or otherwise trigger through the user interface) are not.

This suspicion is buttressed by the "ShellExecuteEx has failed Error Code 1155" message. Although this isn't a very specific error code, it at least suggests that something's preventing the Windows user interface (the "shell") from working properly with the OS.

The question is, what's that "something"? Although this behavior is sometimes caused by malware, it's also a valid software setting that can be invoked via a software or user error — or even deliberately as a prank! (Do you have a practical joker in the vicinity?)

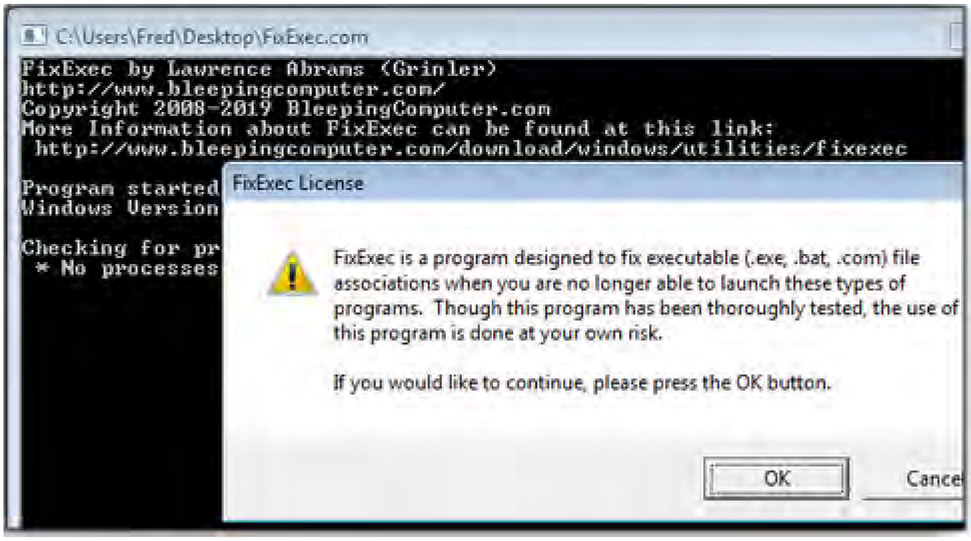
For example, it's possible your PC is now in **kiosk mode** (aka "display," "lockdown," or "assigned access" mode), all of which turn a standard PC into a more-or-less display-only device. IT departments may employ kiosk mode in a controlled way to prevent unauthorized changes. But, again, malware, pranksters, or software error might trigger this limiting mode in an unexpected or uncontrolled way, effectively locking you out of your own PC. (See links at the end of this text for more info.)

Most browsers also have some form of kiosk mode, suppressing menus and controls. This might explain Colm's comment that he can still use Internet links. (Again, see the end of this item for more information.)

There can also be problems with Windows' security settings or a malfunction in Windows **Attachment Manager,** which is supposed to block only unsigned Web-based executables (MS info).

You get the idea: there are ***many*** ways to mess up a PC's handling of executables.

But whatever the cause of this problem, you probably can recover via one of the following four steps. The only initial prep is the usual: ensure, if possible, that all your essential files are safely backed up and out of harm's way. (If you don't have a current backup and can't run an EXE-based backup tool, at least copy/paste your important files to a safe location — or use a self-contained, self-booting backup tool [example: Google search] to safeguard your most important files.)
Start with an ultra-easy, automated fix, such as BleepingComputer's free **FixExec** utility (site). It can correct simple problems with EXE, BAT, and COM file extensions. The tool itself is offered in COM, PIF, and SCR versions, which may work even if you can't run EXEs. (See Figure 1.)



```
FixExec by Lawrence Abrams (Grinler)
http://www.bleepingcomputer.com/
Copyright 2008-2019 BleepingComputer.com
More Information about FixExec can be found at this link:
 http://www.bleepingcomputer.com/download/windows/utilities/fixexec

Program started
Windows Version

Checking for pr
 * No processes
```

FixExec is a program designed to fix executable (.exe, .bat, .com) file associations when you are no longer able to launch these types of programs. Though this program has been thoroughly tested, the use of this program is done at your own risk.

If you would like to continue, please press the OK button.

Figure 1.

Bleeping Computer's free FixExec tool is well designed, but it still works under the Windows hood. As the warning says, use it at your own risk.

If FixExec doesn't work, try sneaking your way into **regedit.exe,** Windows' Registry editor.
Type **regedit** (without the ".exe") in the Windows search box. When the Regedit icon appears, ***don't touch the mouse or move the cursor from the Search box*** — just press Enter.

Regedit didn't open? Try it again — but this time, move the cursor to, and click, the Regedit icon.

One way or the other, if you can get Regedit open, use it to make the changes shown in the MS Support article "Can't open .EXE files in Windows 7 or Windows Vista."
If neither FixExec nor Regedit works — or if they initially work but the problem comes back — verify that your PC isn't infected by malware. Because you can't run EXE files, your best bet is to use a ***self-booting/ self-contained*** malware-scanning tool — either a bootable DVD or flash drive that contains its own operating system (often Linux) plus a fully current anti-malware app. There are many such tools available, free and paid, as this sample Google search shows.

If even *that* doesn't work, this almost certainly will: Download a self-contained, bootable copy of the Windows installation files and burn them to an optical disc or a flash drive. Start your PC directly from the disc or installation drive. When your PC is running entirely from the Windows setup disc or drive, you can repair, reinstall, or clean-install Windows as you wish. (Because the disc or drive is running its own self-contained copy of Windows, whatever's affecting your for-real setup won't interfere with the EXEs on the disc or drive.)

If you want to **repair or reinstall Windows 7,** you can get a fresh, official copy of the latest Win7 setup/ installation files from the Microsoft Software Download page. Start your PC with those files on a bootable disc or drive and have at it. If you want to try a repair, press **F8** as the PC wakes up (before the Windows 7 logo appears). Then, on the *Advanced Boot Options* menu, select **Repair your computer.** Choose your options from the next screens. Of course, you also can choose a reinstall or clean install — it's up to you.
Note: Keep in mind that Win7 is in its last months of support. So rather than investing time and effort into repairing it, this might be a great time to consider making the move to Windows 10. It's even possible that you'll still be able to upgrade for free — Microsoft is still letting some Win7 and 8.1 systems perform an upgrade at no charge. (See related item at Langa.Com.)

Millions Fall Under The Spell of Virtual Influencers + Coronavirus Scams Latest

by Scambuster Keith, Sscambuster Newsletter, May 27, 2020

You’ve heard about fake news. You know about deep fake videos. We’ve even told you about social media influencers who get paid to promote products. But how about influencers who aren’t even people at all -- virtual influencers?

Yes, that’s right; we’ve entered the age of virtual influencers -- characters who look like real people but who exist only as computer code and in the minds of whoever created them.

You might think it’s an inevitable next step in the realms of image manipulation. The worry is that it’s another step in the realms of people manipulation, leading us down the path to scams.

The idea is known as computer-generated imagery or CGI. And if you think you wouldn’t be fooled by one of these virtual beings, as they’re called, guess again. A study last year of the most tech savvy generations -- millennials and Gen Zers -- found that 42% of them had followed a CGI influencer without realizing they were fakes.

And if you think it’s only a few people who follow these characters, statistics show that one of them, known as “Lil Miquela,” has 2.2 million Instagram followers. “She” quietly operated for two years before she was revealed to be a virtual being created by a little-known Silicon Valley start-up.

In 2018, when CGIs were just starting to become visible, Miquela was named one of the 25 most influential people on the Internet. Now we see her modeling clothes (Calvin Klein, Chanel, and Prada for example), grocery shopping and generally having the good life we’d all like!

If you have an Instagram account, you’ll find her at @lilmiquela, where she’s described as a “change-seeking robot.”

Let’s stress that, as of right now, there’s no evidence that CGI characters are scamming. But we already know that human influencers have been caught out promoting products without acknowledging they’re getting them for free and that they’re actually being paid to praise.

And, according to a study published late last year, more than half of all people who followed CGI influencers admitted to buying products recommended by them.

Action Urged

So far, one anti-scam organization we’ve written about before -- Truth in Advertising (TIA) -- has suggested the US Federal Trade Commission (FTC) might consider updating its influencer endorsement guides to encompass the activities of what TIA calls “brand-loving bots.”

In these guides, the FTC argues that the most important principle of being an influencer is authenticity -- the authentic experience and opinion of the endorsement.

"But what if the endorser isn't human?" TIA asks.

We've reported already that the FTC has chastised some celebrities for failing to mention that they were being paid for the products they were showing and wearing. One imagines that it will be far easier for eager manufacturers and retailers to use CGIs for the same purpose.

Or, as the global news site Business Insider recently noted: "(F)ake people don't necessarily have to follow the same rules in terms of sponsored content that real influencers do -- a loophole brands could use to their advantage."

People are open to being manipulated by this new wave of marketing, Insider warns.

After all, CGI producers can, quite literally, put the words into the mouths of their virtual endorsers. And they can make their "bots" look exactly how they want them to, to show off products to best advantage.

More to Come

Our guess is that we're going to be seeing a lot more of these characters in the coming year.

As Robins Kaplan, a legal firm specializing in this area, commented: "Human influencers have been around for a while and certainly provide a good channel for brand promotion and marketing, but virtual influencers are now taking the limelight and are set to completely transform the current influencer industry."

And despite the fact that many millennials and Gen Zers can't tell them from real humans, it is usually possible to distinguish them, at least for now.

Often, the lips of virtual characters don't always sync or move correctly with the words that are being spoken. They also usually have unbelievably smooth complexions, blink slowly, and move their heads in an artificial-looking manner.

That's for now. CGI techniques are bound to improve, so the best advice to follow is the same as if and when you tune in to real human influencers: Don't buy on impulse. Do your research.

Human influencers have been around for a while and certainly provide a good channel for brand promotion and marketing, but virtual influencers are now taking the limelight and are set to completely transform the current influencer industry.

Coronavirus Scam Alerts

New scams that exploit the Coronavirus (Covid-19) crisis are emerging every week.

Because some people haven't yet received their stimulus checks, scammers are phoning them offering to "help" in return for a fee.

No help needed. If you want to check what's happening with your check, just ask the IRS. Go to: https://www.irs.gov/coronavirus/get-my-payment

Continued..page 16

Scambusters................................from page 15

And we warned last week about fake insurance agents selling non-existent health insurance. Now they've switched to selling fake travel insurance claiming to cover the illness.

Most travel insurance does not cover pandemics and you'd be unlikely to buy anything that does right now. But if you want to know more, hang up on the scammers and talk to your reputable, local insurance agent.

Time to conclude for today -- have a great week! ❑

Fixing a Sluggish PC

By Fred Langa/Windows Secrets Newsletter

It was a typical winter day in Seattle — gray, rainy, and raw — when I visited Windows Secrets reader Gary Nobel.

Gary's system would occasionally slow "to a crawl." I was there to find out why.

This was the first in a new series of House Calls, an occasional project where I visit a reader's home or business and attempt to diagnose and cure real-life PC problems. The idea behind House Calls is simple: selected Windows Secrets readers and I collaborate to learn new techniques for analyzing, maintaining, and improving personal computers — which we then share with all Windows Secrets readers.

It works like this. Some months ago, I issued a call for volunteers for a personal, onsite, PC troubleshooting session. From time to time, I select one of the more interesting problems plaguing a reader — a problem that might apply to a wider audience. And rather than diagnose the problem remotely, I pay the reader a personal visit to his or her home or place of business — at my own expense. I do whatever I can in one day to solve the problem (or problems) and make the hardware and software run as well as it can.

Each House Call article, like this one, will explain what we found and how we fixed it. I hope that will give you the information you need to perform similar diagnoses and repairs on your system — or on systems you maintain for others.

The problem: Slowdowns with no clear pattern

When I asked for House Call participants, Gary Nobel sent this:

"I have a desktop computer with a 2.5GHz Pentium Dual Core CPU and 2GB of system memory. I'm running Windows 7 Home Premium.

"The computer occasionally slows down to a crawl. I think Outlook 2007 or IE — or both — might be involved. Rebooting solves the problem, but I have to reboot every few days. Sometimes I get the rotating ring with IE. Clicking the red X doesn't close the window, and I resort to a forced close using Task Manager.

"I run Microsoft Security Essentials and occasionally things like Malwarebytes and Ad-Aware. But they rarely find anything except cookies."

Gary's note caught my eye because it's a nearly universal problem — almost everyone experiences unexplained PC slowdowns from time to time.

When a slowdown follows a clear pattern, it's usually not too difficult to figure out cause and effect. But slowdowns that occur only occasionally — or have no clear pattern — are much tougher to track down.

Kelly says:
April 24, 2012 at 12:13 am
When the command doesn't work typed in Search for XP:
Go into control panel>Performance and maintenance>System. Click on the Advanced Tab and then in the Performance section, click on the Settings button.
Click on the Advanced tab at the top and go to the section for Virtual memory. Click the Change button there. Click to fill the dot for the System to manage the size. Be SURE to click the SET button or this will not work. Click OK and you will get a message that you must restart your system for the setting to take effect. ❑

Chinese App Detector Banned From Google

by John Lister , June 8, 2020 Infopacketys Newssletter

Google has removed an app designed to highlight any Chinese-made apps on an Android device. The straightforwardly-named "Remove China Apps" was particularly popular in India, where it was developed.

Exactly why the app was removed isn't clear other than Google saying it violated unspecified app-store policies. Based on what the developers claim, it doesn't appear to pose any serious security or privacy risks. It didn't actually remove any apps but instead produced a list that the user could manually install.

Continued...page 18

Chinese App Detector ....from page 17

Border Dispute Sparks Boycott

While security concerns about Chinese tech have become a talking point in the West, the popularity of Remove China Apps is more likely to do with local political issues. It comes amid a dispute over the border between India and China that's led to boycotts of Chinese goods and services.

The app reportedly had almost five million downloads in India within five days and was briefly the most popular in the country in the official Google Play Store.

Detection Methods Unclear

The performance of the app and its methods for determining a Chinese app was somewhat questionable as one of the apps it removed was video conferencing tool Zoom. The service was founded by a Chinese-born person but the company and app are in California.

The developers have a poorly worded disclaimer that reads "Detecting the country of origin is based on the market research, but we do not guarantee for any correct/wrong information, so users should act only at their own will." (Source: onetouchapplabs.com)
Meanwhile, Remove China Apps was unable to spot and remove pre-installed Chinese apps on some Android handsets made in China that are particularly cheap and thus popular in developing markets such as India.

An online community had built up recommending Indian-built alternatives to "Chinese" apps highlighted through this process. However, some of these appeared to have been quickly developed and in some cases "borrowed" code from elsewhere. (Source: ft.com)
What's Your Opinion?

Should Google have removed this app? Is it a tool you'd be interested in using? Should apps be subject to political boycotts in the same way as physical products? ❑

Can I Move My Old Computer's Hard Drive to My New Computer to Transfer Data? My Recommended Approach

You can take the internal hard disk of an old computer and install it as an additional drive in a new one; or, consider a more flexible alternative.

//

My sister has a computer with Windows. However, it is crashing on her. She got a new computer with the latest Windows. My question is, can she install her old hard drive onto her new PC so she can transfer her files over to her new hard drive? She is very illiterate when it comes to computers.

A working hard disk formatted for use by any prior version of Windows can certainly be read by Windows versions that come later.
Of course, you'll have to open the box, extract the drive, and do something with it.

Can I Move My Old Computer’s Hard Drive to My New Computer

- You can almost certainly remove the hard drive from an older machine and attach it to a newer machine.
- You may be able to install it internally, if the interfaces are compatible, and most are.
- You might instead consider placing it into an external drive enclosure to make it an external USB drive.
- You will not be able to transfer installed applications or Windows itself.

Installing the drive in another machine

This is a fairly common approach used by computer geeks. We’ll take a hard drive from an old computer and install it as the second drive in a new one. What used to appear as the C: drive on the old computer might now appear as the D: drive on the new one. Once it’s set up, copying files from old to new is easy and fast.

This approach comes with a bonus. Once you’re done copying the files you want to keep, you can leave the old hard drive in the new machine, reformat it, and use the extra disk space for whatever you like.

The downside is, you need to be somewhat computer-hardware literate to install the drive. It does mean opening up your PC and connecting the old drive in the right way in the right place. There’s no “one way” to do it; it varies based on the type of computer and hard disk you have.

Continued...page 20

Can I Move My Old..................from page 19

A more flexible approach: the external drive

A more flexible approach I prefer instead is to take the drive out of the old computer and install it into an external USB drive enclosure.
That's essentially what external USB drives are: hard drives in an enclosure, providing power and a circuit board to provide the USB-to-hard drive interface.

There are two things you need to know before purchasing an external USB enclosure.

- The drive size.Two common sizes of hard disk drives.
  By size in this case, I mean the physical size of the drive. The external enclosure you select needs to match the physical size of the old drive you're about to put in it.
- The interface.The two hard drive interface types: SATA and IDE (aka PATA).
  There are two primary disk interfaces these days: SATA (on the left, above) and IDE (on the right). Almost all drives on newer machines are SATA, and even when they're not, newer machines include SATA interfaces. Particularly on very old machines, you may run into IDE. The external drive enclosure you get must match the drive you have.

Once you've installed the drive in the appropriate type of enclosure (a screwdriver is really the only tool you'll need), all you do then is connect it via USB to any computer (and perhaps to power) and you'll be able to access the data on it.

What you can't do

I want to caution you about transferring software. You can't.

Any program that required running a setup program to be installed on the old machine will need that setup program run again to install it on the new machine. This is not something typically available on the hard disk you just moved — you'll need to get, or download, the latest setup for the software you want[1].
Similarly, this doesn't work for Windows at all. Windows is, itself, configured for the specific hardware it's used on. Your old machine's configuration is different than your new machine's. Even if you could just copy it over somehow, its configuration would be unlikely to work properly. Much like an application, Windows must be set up properly for the machine it will run on.

Some skills required

Regardless of whether you install the hard disk in a different computer or into an external enclosure, you will need to be comfortable opening up the old computer to disconnect and remove the drive. Then, depending on your choice, you'll need to install the drive in its new home.

If that sounds like too much, perhaps it's time to find a technician (or at least a techie friend).

It's usually a fairly quick and easy operation for someone who knows what they're doing.

If you found this article helpful and you'd like more tips like this, you'll love Confident Computing! My weekly email newsletter is full of articles that help you solve problems, stay safe, and increase your confidence with technology. ❑

Video Conferencing for Clubs

Author: Dick Maybach, Member, Brookdale Computer User Group, NJ

www.bcug.com
n2nd (at) att.net

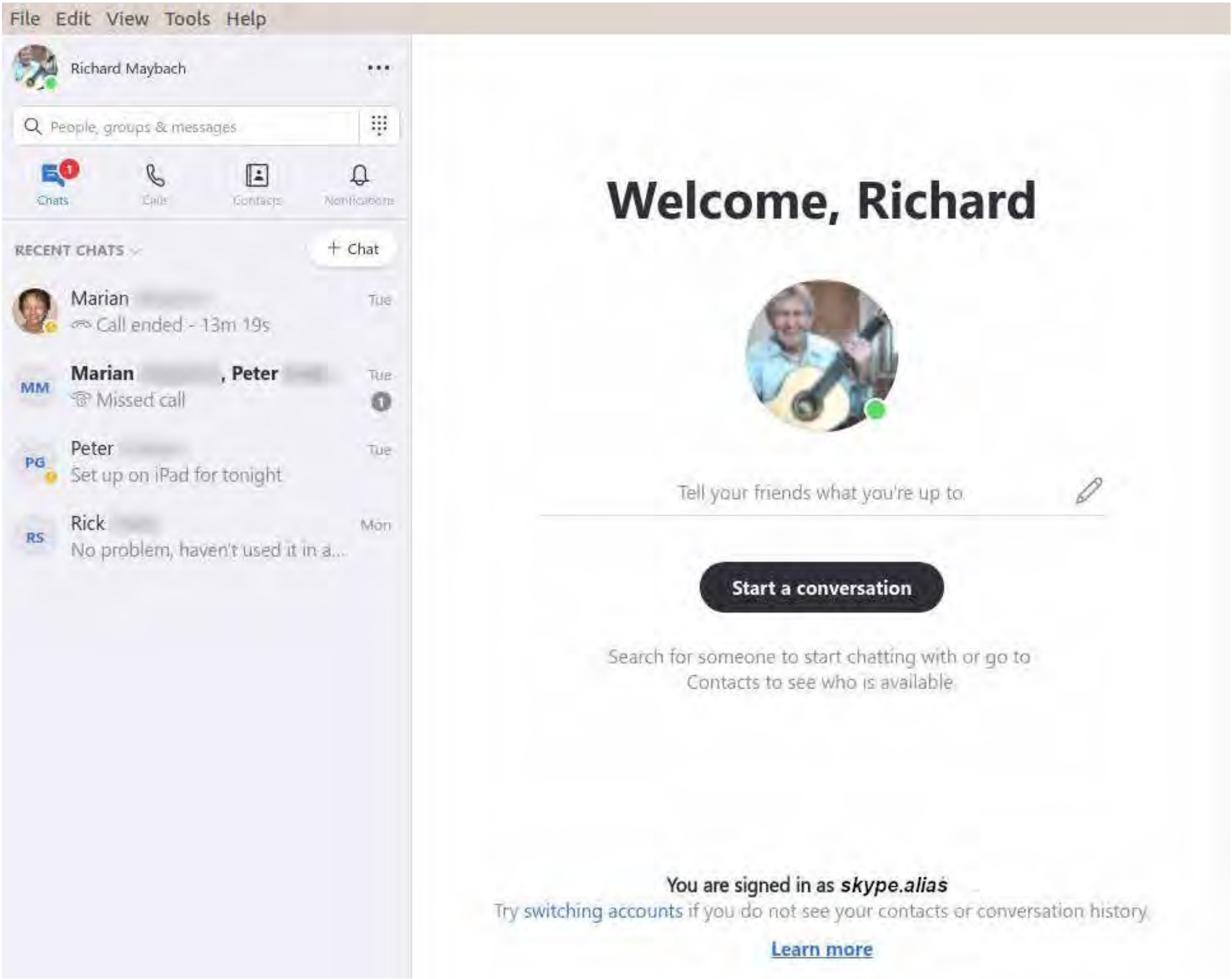
Many clubs have periodic general meetings, often with refreshments, speakers, and perhaps demonstrations or hands-on activities. The social interactions here, including the welcoming of prospective members, are vital for the organization's health. Equally important are the committee meetings that support the organization. Here, much smaller groups, whose members know each other well, plan the club's activities, and it may be more efficient to conduct some of these as video conferences, which would eliminate the associated travel. There is a major caveat: teleconferencing is ineffective if there are tensions within the group. Meet in-person to discuss a controversial issue.

There are two popular free services suitable for meetings of small groups: Facebook Messenger (http://www.facebook.com/messenger/) and Skype (http://www.skype.com/en/). Both require that participants register for the respective service, and all can be accessed from Linux, Windows, and Mac computers as well as Android and iOS devices. (These free services are provided by for-profit companies, and the usual caveat applies; they can be changed or discontinued any time their owners determine they aren't sufficiently contributing to the bottom line.) If your club outgrows the scope of the free services, most vendors offer for-fee variants with more capabilities. You might also consider inexpensive paid services, such as EZTalks (http://www.eztalks.com/video-conference/) and Zoom (http://zoom.us/). Neither requires that users other than the moderator register for a service, but participants need to install the software. Both have trial versions that limit conferences to 40 minutes, which is certainly adequate for testing.

I'll use Skype as an example, only because I already use it for one-on-one calls. Microsoft is refreshingly open about what it considers fair use (http://www.skype.com/en/legal/fair-usage/). In particular, "Group video calls are subject to a fair usage limit of 100 hours per month with no more than 10 hours per day and a limit of 4 hours per individual video call. Once these limits have been reached, the video will switch off and the call will convert to an audio call." See the above URL for the other, quite reasonable, limits.

Skype's interface varies with its version and your hardware and software; as a result, what you see may differ somewhat from the screenshots here. Figure 1 shows Skype's opening screen, after the user has selected the Chats icon toward the upper left, and it shows one of Skype's puzzles for new users. My name appears at the upper left, but you must contact me by my Skype name, which is "skype,alias" and appears towards the bottom right of the welcome screen in the sentence, "You are signed in as skype. alias." (If you are not on the opening screen, find your Skype name by selecting the three dots to the right of your name at the top of the left panel, and then "Settings" followed by "Accounts & Profile.) Skype names are unique, but a search on a person's given name will likely produce dozens of hits.

Continued...page 22



Marian [redacted] Tue
Call ended - 13m 19s

Marian [redacted], Peter [redacted] Tue
Missed call

Peter [redacted] Tue
Set up on iPad for tonight

Rick [redacted] Mon
No problem, haven't used it in a...

Welcome, Richard

Tell your friends what you're up to

Start a conversation

Search for someone to start chatting with or go to Contacts to see who is available

You are signed in as ***skype.alias***

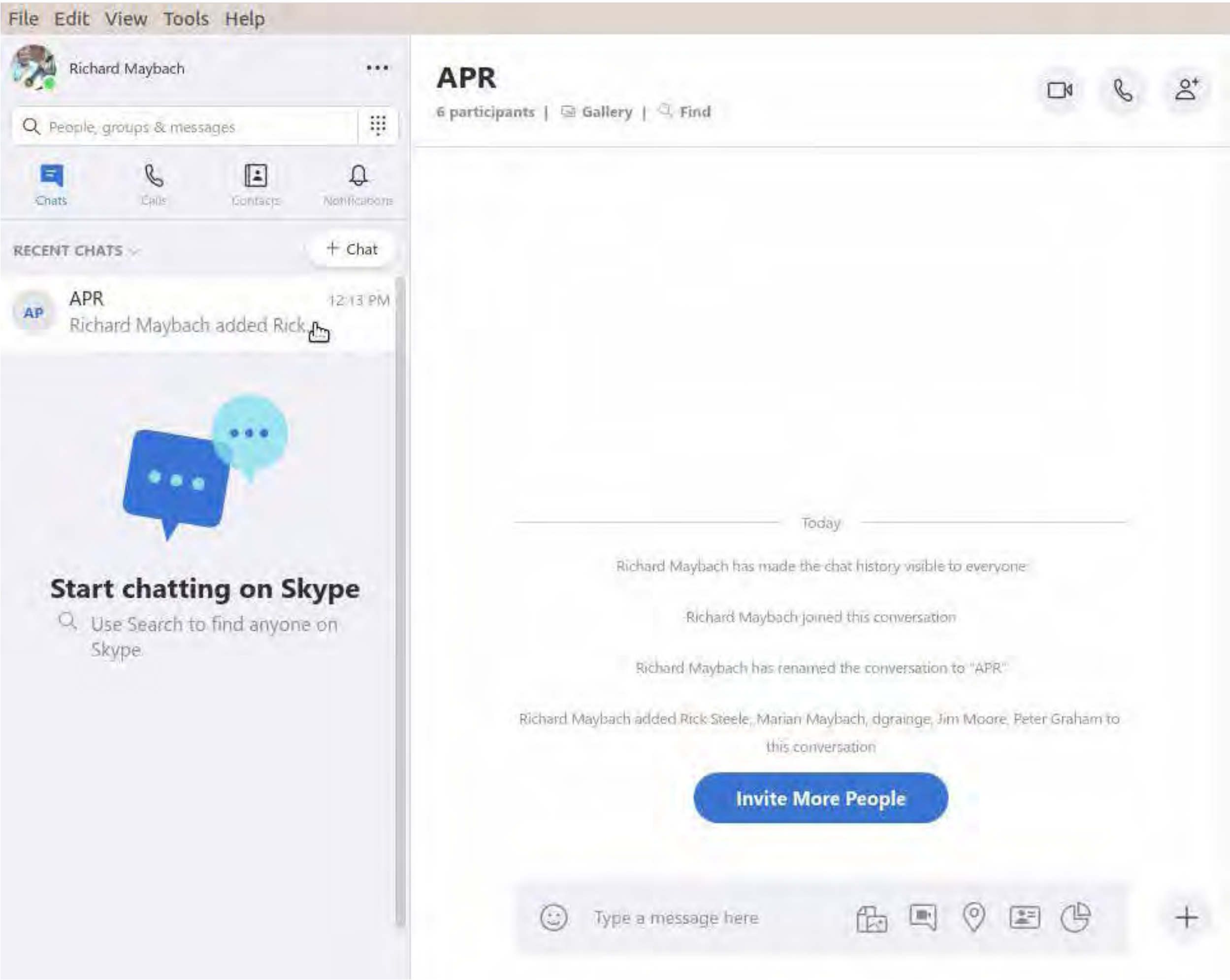
Try switching accounts if you do not see your contacts or conversation history

Learn more

Figure 1. Skype Opening Screen

To communicate with someone you must first add their name to your contact list. Select “Contacts” in the menu bar toward the upper left, then select the + button; enter their Skype name, and select the associated Add button. This will work only if they have enabled “Appear in search results.” (Go to Settings as above, then “Contacts” and “Privacy” to make this choice.) Many Skype names have the form “live:.cd.6f73e115260c0804”, and sometimes searches using the full name fail, but succeed if you delete the “live:.cd.” prefix.

Skype is different in that the moderator places a call to the participants, while other services require that the participants call into a conference. The set-up procedure varies with the version, and in Linux, it’s done by setting up a group chat. Select “Chats” in the menu bar toward the upper left and the “+ Chat” button, and finally “New Group Chat.” The result is in Figure 2. Select either the round button at top right, or “Select More People” toward the bottom, and add participants from your contact list. Selecting the camera icon at the upper right will start a video conference, and selecting the handset icon a voice conference. As the call begins, you will have an opportunity to ring the participants to alert them, which



Richard Maybach added Rick

Richard Maybach has made the chat history visible to everyone

Richard Maybach joined this conversation

Richard Maybach has renamed the conversation to "APR"

Richard Maybach added Rick Steele, Marian Maybach, dgrainge, Jim Moore, Peter Graham to this conversation

Figure 2 Define a Group Chat

ZOOM: Is It Safe?

By Lincoln Spector, Ask Woody Newsletter, May 15, 2020

Have you noticed that the start of every article about Zoom suggests that it has quickly turned into the most needed app on the planet?

Continued...page 24

ZOOM: Is It Safe.........................from page 23

Thanks to the pandemic, what was created as a business-conferencing tool has become the de facto means for ordinary people to connect to each other. My wife, a faculty member at the San Francisco Conservatory of Music, uses Zoom to teach her students miles away. Family get-togethers, schools, charity events, remote concerts, and even television hosts now depend on the service.

But while Zoom's stock was exploding, the programmers who built the platform seemed to be tripping over their shoelaces. Problems kept popping up, often followed by official apologies. And then came the reports of questionable privacy policies and online trolls crashing meetings. With good reason, people started asking, "Is Zoom safe?"

In a previous article about Zoom and similar services (2020-04-06 AskWoody issue), I concentrated on video-conferencing etiquette and ease of use (or lack thereof). I wrote that article in March, just as we were getting used to the new world of stay-at-home socializing. We were all learning as we went along. Thus I ignored one of the more difficult questions about these services: To what degree are Zoom and its competitors spying on us?

Because I ultimately recommended Zoom as the easiest video-conferencing service for users of any technical skill — yes, even Uncle Fred could get it working — I'm going to focus on its failings. Both accidentally and intentionally, the company has put your privacy at risk. Much has been written about these problems in recent weeks, so I'll give you a summary of what you really should know about the service — and others.

A potential threat to school kids

In early April, New York City banned Zoom for school use — even though "thousands of teachers and students began using it for remote learning," according to an article penned by Chalkbeat's Alex Zimmerman. It went on to say: "The education department received reports of issues that impact the security and privacy of the platform during the credentialing process … ."

A month later, the city lifted the ban after Zoom made security changes. Quoted in a Spectrum News NY1 article, New York DOE Schools Chancellor Richard Carranza stated: "The security of our students and staff is paramount, and we've worked with Zoom to create a tailored platform that provides the safety and functionality schools need to engage in remote learning."

In a Zoom blog post, the company claims to be hard at work providing a safer environment. Are these real and significant fixes? Or are they little more than the digital equivalent of slapping on some new paint? We just don't know yet. But based on the aforementioned blog, Zoom does seem to be taking its issues seriously.

Party crashing and other bad behavior

As with all major events, the current pandemic has created its own vernacular. One of the more unique additions is **Zoombombing** — which I sincerely hope you'll never experience. This is the Internet version of crashing a party, starting fights, and painting offensive epitaphs on walls … except you'll never know who ruined your fun.

As noted in a CNET article, it's horribly easy to Zoombomb a meeting. If you search for URLs containing **zoom.us,** you might get hundreds of vulnerable Zoom-enabling sites. Fortunately, the article provides some tips for blocking Zoom hooligans.

But not all the service's problems are as visible or caused by outside actors. As reported in a Vice article, the iOS edition of Zoom was for some time sending personal data to Facebook — even if the user was not a Facebook subscriber. At the time, there was no mention of Facebook in Zoom's privacy policy. Privacy Matters activist Pat Walshe called that policy "shocking."

Once the information came out, Zoom, not surprisingly, stopped sending information to Facebook.

When I researched my earlier article, I skimmed through Zoom's 3,855-word privacy policy. Among numerous worrisome points was the statement that it "covers all Personal Data that you affirmatively provide during your interactions with us, information that we automatically collect when you interact with our Products, and information that we collect about you from third parties." That sounds intrusive, but it's hard to know whether that's any worse than, say, Facebook, Windows, or macOS.

The latest version of the statement, dated March 29, claims that "We do not sell your personal data." I haven't studied the entire statement — it has ballooned to 5,225 words — and probably wouldn't understand it all if I did. But you might want to read the top bullet points and judge for yourself.

Just how bad is this?

Given its history and recent news coverage, it's not surprising that people describe Zoom as "fundamentally corrupt" and "malware." Nevertheless, it's still extremely popular; it has become the Google of personal video conferencing. So whether to use it mostly comes down to what you're willing to tolerate. Even Windows has been dubbed "malware" (Computer World article).

Zoom used to claim that its service had *end-to-end encryption* — an assertion made by redefining the concept. When it turned out not to be so, the company had to eat crow. Zoom acknowledged "a discrepancy between the commonly accepted definition of end-to-end encryption and how we were using it."

In a May 7 Zoom blog post, the company announced that it had acquired an encryption startup called Keybase — I assume to improve the service's privacy problems. That might help small gatherings, but it's unlikely today's technology can handle simultaneous end-to-end encryption for 100 or more nodes.

Most troubling, Zoom's technology exposed personal devices to malware. Last year, a security researcher discovered that the program installed hidden and potentially vulnerable Web servers onto Macs. Soon after that became public knowledge (July 2019), Zoom reported that it had removed the code via an update.

Why not simply use another service?

There are, of course, alternatives to Zoom — Cisco's Webex, Google Meet, and Microsoft Teams, to name just a few. (I discussed Webex and Google Duo in my April 6 article.)

Sure, there might be better choices, but we're up against the Facebook dilemma — i.e., you might prefer a less intrusive social network (MeWe, for example), but all your friends, family, and business associates are glued to Godzilla. Zoom is now the behemoth of both business and non-business video conferencing.

For a Consumer Reports Digital Lab article, privacy researcher Bill Fitzgerald took on the arduous task of examining the policies of several video-conferencing platforms. The conclusion: "While there are differences … on balance, the differences aren't enormous … from a privacy point of view, none of these options is great."

So even if you could convince your acquaintances to move to another meeting service, it probably wouldn't remove the underlying privacy problems.

Am I sticking with Zoom?

Continued...page 26

ZOOM: Is It Safe?c ....from page 25

Probably. Until the virus is under control, we need a way to socialize without endangering our lives or those of others. I’m not willing to take the risk of shopping in public without a mask, but I am willing to possibly lose some privacy in order to continue connecting with friends and family. And there really isn’t a significantly better option.

Whether you’re using Zoom or one of its competitors, assume that someone untrustworthy might be recording what you’re saying. So don’t read out your personal bank account number, or proprietary business info, or the secret family recipe for gefilte fish in a Zoom meeting.

If you really need to keep something private, use an encrypted email service such as Sendinc — or just use the phone! ❑

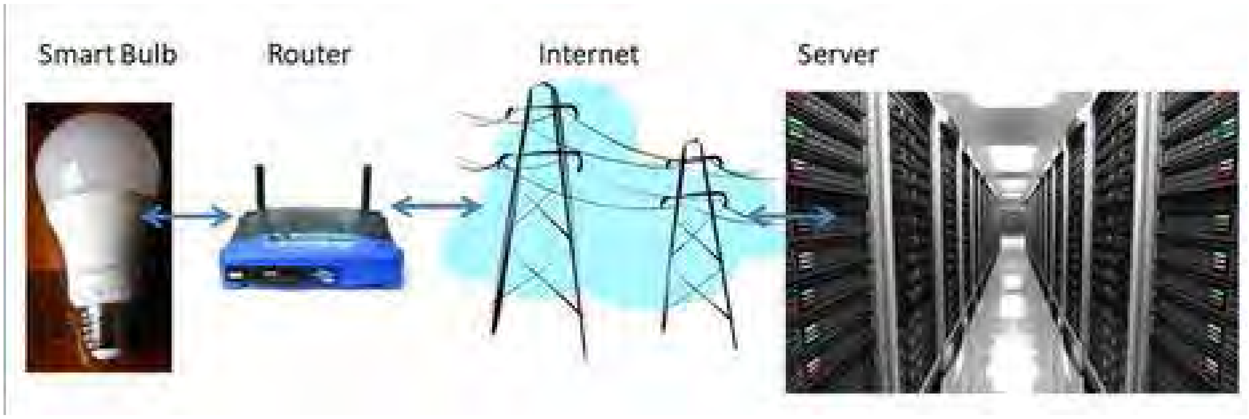
Smart Devices in the home – With voice control

Author: Phil Sorrentino, Contributing Writer
The Computer Club, Florida September 2019

www.scccomputerclub.org
Philsorr@ yahoo.com

There are a whole host of smart devices available for use in the home now. Some of the most basic and least expensive ones are smart bulbs, smart plugs and smart cameras. (Yes, I know cameras can be expensive, but there are some fairly inexpensive in-door-only cameras.) First of all, what makes these devices smart? Well as I have alluded to in previous articles, it’s all about Client – Server technology. The devices have some limited intelligence in them. Read “intelligence” as basic processing power, downloadable firmware, and wi-fi electronics. This allows them to be able to communicate with a local wi-fi router, which in turn allows them to access the internet. Once they can access the internet, they can take advantage of the servers on the internet (sometimes referred to as “in the cloud”).

The intelligence in the accessed server is where all the magic happens. Here read “intelligence” as very fast, very powerful, server computers capable of handling millions of re-quests for service per second.



So it's the combination of the smart device, the internet, and the server that really makes the smart device: smart.

Once you have your smart device ready for installation, it is the App on your smartphone that takes over and steps you through the installation process. (Yes, a smartphone is required for the installation, either Android or Apple.) The App that you will use for installation will be the App from the specific smart device manufacturer. So for example, if you have a TP-Link smart bulb, you would have to get the TP-Link App for your smartphone. In this example that would be the "Kasa" App. Similarly, if you have a Wyze smart bulb you would use the Wyze App for the installation. These Apps are free and are intended to work with the servers from the specific manufacturer. (So just as an aside, think about this. If the company that operates the server, the smart device manufacturer, goes under and the server goes away, your smart device will no longer be smart. The bulb may not even be able to be turned on if there is no server to command it to turn on.)

The installation process is usually pretty easy; after all, it's the App that is doing all the work. The first thing you have to do is get the device ready for installation. The App will usually start this by having you select something like "add a device," or "add a product", or maybe you just have to select the "+" on the screen (as found on the Kasa App) to add a de-vice. You will have to let the App know what type of device you are adding. This is usually done by just selecting the device type from a list of device types manufactured by that specific manufacturer. Once the device type is selected, you are ready to go into the setup mode. The App will give you instructions for getting the device into the "Setup" mode. On smart plug with a push-button switch it is really easy because pushing the button as directed by the App will get the smart plug ready for installation. With a smart bulb, usually you quickly turn the power on and off maybe three times and the smart bulb goes into the Setup mode. You will know the device is in setup mode when whatever you were watching changes. With a smart bulb, the light may start to pulsate slow-ly, with a smart plug, the small light on it may blink or change color. Once the device is in the setup mode, it will need to know the name of your wi-fi network and the password for that network. (Note: some de-vices only support 2.4 GHz networks only; not 5 GHz networks.) You may have to use your "Settings App" on the smartphone during the setup; just follow the directions from the App. Once you enter the wi-fi net-work name and the network password you may see a timer count down for a few seconds till the installation is complete. Finally you will be asked to name the smart device; something like "desk light" or "bedroom plug". (Keep in mind that each manufacturer's App will be a little different, this is just a general example.)

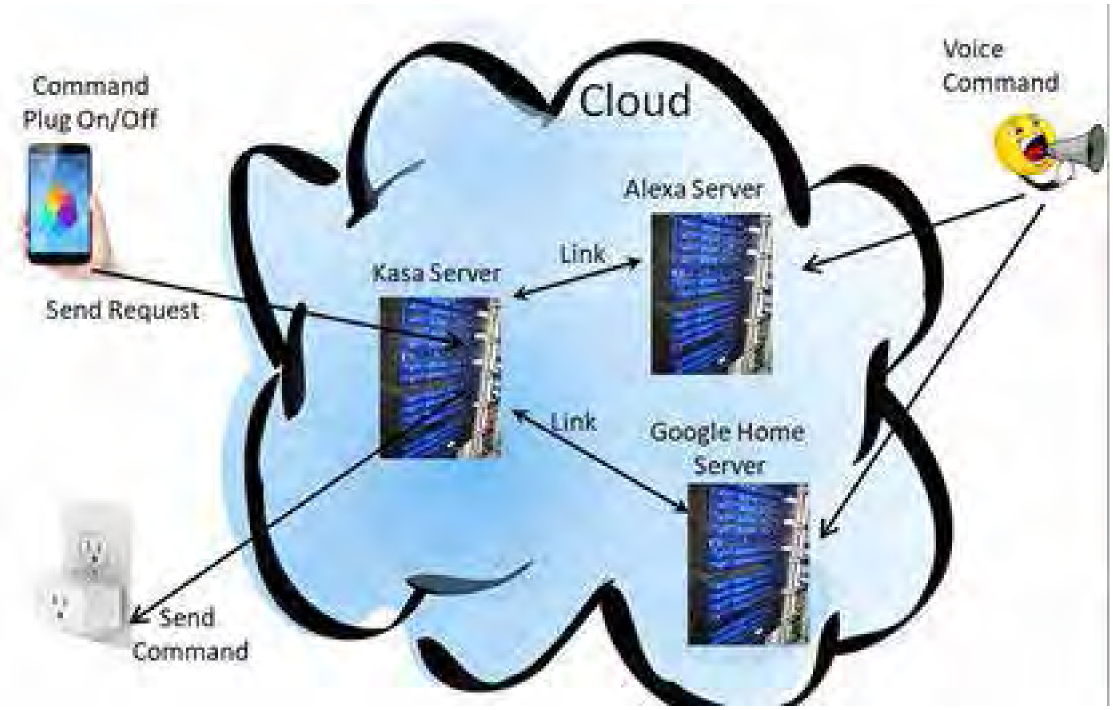
The installation may seem complex but after you have done it once or twice it will probably be-come automatic. However, you might want to keep those instructions that you get with the device in a safe, convenient, place because you might have to go through the whole process again. (Before I lose the instructions, I scan them into a file and place the file in a "Home Automation" folder so I can review the directions when I have to do another installation. This was recently necessary when I changed my router and the new wi-fi network had a new name and new password. This forced me to reinstall every device that used the house wi-fi. At the time, I had 7 smart devices that had to be reinstalled.) So now with the smart device installed you can control it from your smartphone App. Typically, you can turn it on and off and maybe even set up a schedule.

Once the device is installed and working, it's time to move on to voice control. Voice control is supported by Amazon's Alexa and Google's

Continued...page 28

Smart Devices in the Home..........from page 27

Google Home. You can use either of these or both. Amazon calls the link between Alexa and smart devices “skills.” Google Home refers to them as links. In either case you need to have the appropriate App on your smartphone; the “Amazon Alexa” App for Alexa, and the “Home” App for Google Home. Again, the Apps are free and available for Android and Apple. Once you have the appropriate App, you just have to follow the instructions to link your smart device. Typically you will have to select the type of device and the device manufacturer. On Alexa this is started by selecting the “+” on the “Devices” screen and then selecting “Add device,” and then the type of device, and then selecting the manufacturer of your device from a list of manufacturers. To make sure you are linking “your Alexa” to “your smart device,” the App will require the Username and Password for the manufacturer of your smart device. (So, as a general rule, make sure you know the Usernames and Passwords for all of the manufacturers of the smart devices that you use.) Once you have authenticated yourself with your Username and Password, a link will be made between the Alexa server and the smart device manufacturer’s server. And now you can control the smart device, at least to the extent that the skills allow, by voice control. Now enjoy the feeling of power. ❑



Cleaning a Hacked PC

By Ron Weinberg, TPCUG
April 2019

My friend returned from the bank with a locked account, new password, and advice to have his PC cleaned. His Savings and Checking accounts had been fraudulently manipulated by a hacker. He asked for my help to clean his PC.

Before I undertook the job, I did some research. The prevailing opinion of experts was that once attacked there was no way to determine how far into the system malware had penetrated. The recommendations were tough, either discard the PC or vigorously scrub it clean it down to the bone. I agreed to undertake the job.

Warning: this was expected to be a time-consuming process and it was. Literally everything on the system would be lost. Like many layman users whose PC use and experience was limited, he had no backups of any kind and could not locate any OS disks. His was a Dell desktop, out of warranty, which had been updated to Windows 10. Dell Support furnished a free download that would restore the system to its original configuration which included Windows 8. They would not provide free Windows 10.

1. My first step was to remove the victim hard drive and connect it to my PC as an external drive using a USB to SATA/IDE Adapter. As an external drive, used with care, my system would not be contaminated.

I copied and saved his Documents and Pictures.

2. Completely wiped the drive to DOD standards using “Disk Wipe”.

3. Formatted the drive.

4. Replaced the drive back in the Dell chassis.

5. Installed the Dell system and Windows 8.

6. Copied his Documents and Pictures back.

7. Reinstalled Windows 10 from created media.

8. Downloaded and installed Chrome, Avast Anti-Virus, and Adobe Acrobat Reader. Email was web-based Yahoo and was not affected.

Job completed, with a little polite admonition about keeping better backups. ❑

BREVARD USERS GROUP

B U G Officers

President
Bill Middleton
President@bugclub.org
Treasurer
Loretta Mills
Treasurer@bugclub.org
Secretary
Bill Middleton
Secretary@bugclub.org
Member At Large
Jim Townsend

Webmaster
Chris Crisafulli
Webmaster@bugclub.org

Special Interest Groups

Beginners' SIG:
beginners@bugclub.org

Hardware (Tinkers) 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,

WHEN IS OUR NEXT MEETING?

The answer is probably on July 6 at One Senior Place. As of Monday of this week, the Libraries have received no instructions on restoration of public meetings at their facilities. One Senior Place will be allowing limited meetings with participants RSVP- ing, wearing face masks, having their temperature taken when they enter the building (not rectal) and with seating prearranged to keep the socialized distancing. Hopefully, these restrictions will be loosend a the little by July. We are canceling the June meeting because Chuck will be out of town (and we know your lists of questions are growing) and Bill might still have something sticking out of his nose from a bit of sinus surgery. We will let you know as soon as we hear something from the Libraries, but we do not expect them to be open for public meetings until July. At the earliest. Possibly. Maybe.

Please check the July meeting announcement for RSVP-ing instructions if it is still necessary. So far Brevard County has been relatively fortunate with the spread of this pandemic. It is far from over. The damn virus is still out there and getting people every day. Please take care – our age group is among the prime targets. Florida Today has made its website free to everyone during this crisis. It is probably the best source for local information.

Hope to see everybody healthy in July.

Google Sued Over Incognito Mode

http://www.tpcug.org

Google faces a class action lawsuit over claims it “misled users of Chrome’s private browsing mode.” But suggestions users are in for a $5,000 windfall are premature, to say the least.
That’s the minimum amount the lawsuit seeks per affected user, though for starters that assumes not only that the plaintiffs win the case, but that the court agrees to that amount. It also assumes the amount isn’t reduced by lawyer fees and that anyone eligible is able to sign up to the case and provide any necessary proof.

The crux of the case, brought in the United States District Court for the Northern District of California, is a claim that Google unlawfully collects data about users without their consent or knowledge when they use the «Incognito» mode.

Private Browsing Warning

On the face if it, Google is clear about what it doesn’t save during Incognito mode, namely «Your browsing history», «Cookies and site data» and «Information entered in forms.» It does warn that website operators, employers, schools and Internet service providers might still be able to track user activity.

However, the lawsuit alleges that Google continues to track user activity while using Incognito mode. This comes from services offered to websites, such as Google Analytics (which provides stats about visitors to a site), Google Ad Manager, and tools such as one that lets users sign into a site using their Google account. The lawsuit says “70 percent of all online publishers use such a service.”

(Source: bloomberglaw.com)
To provide these services, Google does collect information about a user’s browsing activities, even when using Incognito Mode. For example, when somebody visits a website, Google can provide details of the last site they were on, which can help site operators see which inbound links are most effective
.

A Matter Of Perspective

Google says it will defend the claims vigorously and notes that such data collection is covered by the warning about website operators seeing activity. (Source: bbc.co.uk)
The heart of the case is thus the plaintiff’s argument that Google doesn’t stress this enough, particularly that it doesn’t make clear that it›s collecting the data that is then seen by website operators.

What’s Your Opinion?

Do you use Incognito Mode? Do you think you have a good understanding of what it does and doesn’t do? Do you think the case has any merit? ❑

Bug Club Treasurers Report

By Loretta Mills , Treasurer

Checking Account **July 1, 2019**

Beginning Balance
$ 1052.36

Ending Balance
$ 1052.36

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

For 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

June 18, 2020 - Club Meeting, 2 PM
Auditorium, Merritt Island Library

June 30, 2020 - Deadline for Journal Input

Presentations Schedule

June 18, 2020

Meet in the Auditorium
2 PM
Get together welcome meeting
Discussion, Q&A

Bring Some Friends or Neighbors

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
DataDan 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 pickup

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 ____________________________________

Make check payable to: Space Coast PC Users Group
Mail to: SCPCUG , 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
June 18, 2020 2 PM

Merritt Island Library Auditorium 1185 North Courtenay Parkway, Merritt Island, FL

To get to Auditorium after entering the front door, go to the seccond door on the left.

Guests are always welcome at the Space Coast PC Users Group meeting.