Southern Districts Computer Users Club Inc

Supporting inexperienced users with local expertise

Be Connected

August 2018

https://beconnected.esafety.gov.au/

Club Web Site   http://sdcuci.com

Email Address: sdcucinc@gmail.com

Vol. 18

No. 8

News Letter Editor James Brown Paddock **E** :-parakylia@hotmail.com

SDCUCI

Yardbroom Report August

I simply could not miss another month without a report so here you are.

We have been out of town for a while and have missed the committee meeting so I can't say much about that. I do know that the Facebook evening produced a lot of very interesting and useful information. Well done Cameron. I am equally sure that David's presentation on Google Earth will be both interesting and informative.

We recently had occasion to personally reflect on Jim Greenfield's popular hobby horse – frequent backups. We do backup regularly (but not as often as we should) and this has been our saving grace (thanks Jim). For some inexplicable reason the SSD on our desktop computer failed. This is not unknown but apparently fairly rare for a SSD. The end result is that the SSD had to be replaced and therefore all the data thereon went in the bin as well. We recently backed up all our photos and documents and other bits and pieces so a major disaster has been averted. However, the many small programs and shortcuts have probably disappeared (not sure about this as we have not been able to access the computer yet). I foresee a few nights recovering the lost information.

The lesson learned is that our backup strategy is far from perfect. How far do you need to go to recover EVERYTHING? Maybe a refresher presentation on backups would be useful. I can do with a few finer pointers – what about you?

How to Fix a PC Stuck on "Don't Turn Off" During Windows Updates

by **Chris Hoffman** on June 25th, 2018

The "Getting Windows ready, Don't turn off your computer" message appears while Windows is installing updates. Windows will normally finish the installation process if you give it time—but, if it's been hours, you may just need to restart your PC. Unfortunately, it's normal to wait a while for Windows to update, and this wastes an immense amount of time. Microsoft says there are about 700 million Windows 10 devices and that the April 2018 Update will take 10 to 30 minutes to install. So, assuming an average of 20 minutes for 700 million computers, that's over 26,000 years of humanity's collective time wasted waiting for Windows 10 to install a single update.

What Happens If You Restart Your PC?

The update installation process will fail if you restart your PC during this process. But how badly will it fail? Will it cause problems with your computer? To find out exactly what happens, we ran some tests.

First, we told Windows to install a standard update from Windows Update. We forcibly restarted our PC while the "Getting Windows ready. Don't turn off your computer" message appeared on the screen. The PC restarted and we quickly saw the normal sign-in screen.

After we signed in, Windows displayed a "We couldn't finish installing updates" notification. The update installation had failed, but Windows was still working properly. Windows will just try installing the update later.

Second, we restarted our PC while the screen said "Working on updates, 27% complete, Don't turn off your computer."

Windows restarted normally and we saw a message saying "We couldn't complete the updates, Undoing changes, Don't turn off your computer." After the process was complete, Windows booted normally and everything worked as expected.

We also tested this process while installing a major Windows 10 update, going from the Fall Creators Update to the April 2018 Update. We rebooted our computer when the message "Configuring update for Windows 10, 10% complete, Do not turn off your computer" appeared on our screen.

After the computer restarted, we saw a simple "Please wait" message, and then the sign-in screen appeared normally. Once again, we saw the "We couldn't finish installing updates" notification.

Finally, we tried restarting the PC when it said "Working on updates 48%, Don't turn off your PC. This will take a while." A "Restoring your previous version of Windows…" message appeared as Windows rolled back the update, and our PC booted and worked normally afterwards.

In every test, turning off the computer didn't cause any problems. Windows just decided to stop updating and roll back any files that were updated. Windows does insist on re-downloading the update before trying to install it again, just in case there was a problem with the download. The updates then installed normally afterwards.
.

How to Fix a PC Stuck on "Don't Turn Off" During Windows Updates

How Long Should You Wait?

Be patient and give Windows some time to finish installing updates if this message appears on your screen. Depending on how big an update Windows has to install and how slow your computer and its internal storage are, this process could take a while to complete.

It's common for this message to appear on your screen for up to five minutes. However, if this message has appeared on your screen for a long time, you may need to restart your PC. We recommend waiting two hours, just in case Windows is doing a lot of work. Windows may just need some time to finish the process, especially if it's a big update and your hard drive is slow and full.
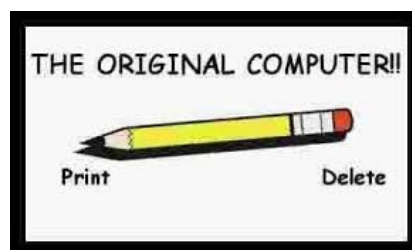
If you see a percentage number on your screen and it's increasing, leave Windows alone as long as it appears to be making progress. If the percentage appears stuck on a particular number for a long time, the update process may be stuck. However, it's normal for Windows to appear "stuck" at a particular point for a long time before speeding through the rest of the installation process, so don't be too impatient.

Yes, You Should Turn Off Your Computer If It Gets Stuck Here

As we've shown above, restarting your PC should be safe. After you reboot, Windows will stop trying to install the update, undo any changes, and go to your sign-in screen. Windows will try reinstalling the update again later, and it should hopefully work the second time. This shouldn't be necessary, but Windows has bugs, and sometimes you have to restart your PC to fix them. This is true even when Windows is telling you not to turn off your computer.

To turn off your PC at this screen—whether it's a desktop, laptop, tablet—just long-press the power button. Hold it down for about ten seconds. This performs a hard shut down. Wait a few seconds, and then turn your PC back on. Performing a hard shut down is never ideal, but it may be your only option in cases like this.

Warning: While we've successfully tested this process, there are no guarantees that your Windows operating system will work properly after you perform a hard shut down. However, if the update process is actually frozen, performing a hard shut down is the only thing you can do. We recommend always having backups of your important personal files, just in case

\

THE ORIGINAL COMPUTER!!
Print   Delete

Disclaimer: The information contained herein is of a general nature. Always do your own research and seek advice before proceeding on information you don't understand.

Runtime Error Definition

Runtime Error

A runtime error is a program error that occurs while the program is running. The term is often used in contrast to other types of program errors, such as syntax errors and compile time errors.

There are many different types of runtime errors. One example is a logic error, which produces the wrong output. For example, a miscalculation in the source code or a spreadsheet program may produce the wrong result when a user enters a formula into a cell. Another type of runtime error is a memory leak. This type of error causes a program to continually use up more RAM while the program is running. A memory leak may be due to an infinite loop, not deallocating unused memory, or other reasons.
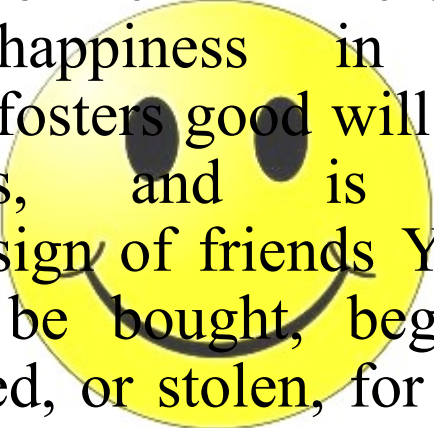
A program crash is the most noticeable type of runtime error, since the program unexpectedly quits while running. Crashes can be caused by memory leaks or other programming errors. Common examples include dividing by zero, referencing missing files, calling invalid functions, or not handling certain input correctly.

NOTE: Runtime errors are commonly called referred to as "bugs," and are often found during the debugging process, before the software is released. When runtime errors are found after a program has been distributed to the public, developers often release patches, or small updates, designed fix the errors.

Recommended reading for fixing Runtime Errors

http://www.the-tech-addict.com/how-to-fix-runtime-error-in-your-pc/

A smile creates happiness in the home, (fosters good will in a business, and is the countersign of friends Yet it cannot be bought, begged, borrowed, or stolen, for it is something that is of no earthly good to anybody till it is given away

Ever wonder where the phrase "It's raining cats and dogs" comes from?
In the 17th century many homeless cats and dogs would drown and float down the streets of England, making it look like it literally rained cats and dogs

Face's Left Side More Attractive Than Its Right Side

Which is your better side?

New research shows that the left side of the human face is generally more appealing to others than the right side--which may help explain why portraitists tend to paint their subjects' left profiles.

For the study, published in the journal Experimental Brain Research, Wake Forest University psychology professor Dr. James Schirillo and his co-author, Kelsey Blackburn, asked 37 male and female college students to rate photos of 10 male and 10 female faces. The photos were presented as originally taken and in mirror image form, so that right cheeks appeared to be left cheeks, and vice versa, Dr. Schirillo told The Huffington Post in an email.

What happened? Photos showing the left sides of faces were rated more "pleasant" than those showing right sides--no matter whether the portraits were shown as taken originally or in mirror-reversed form. The researchers corroborated that finding by gauging the pupil size of the study participants' eyes. Research has shown that gazing at pleasant or interesting images causes an increase in pupil size, whereas gazing at unpleasant images causes pupils to constrict.

"Our results suggest that posers' left cheeks tend to exhibit a greater intensity of emotion, which observers find more aesthetically pleasing," the researchers said in a written statement. "Our findings provide support for a number of concepts--the notions of lateralized emotion and right hemispheric dominance with the right side of the brain controlling the left side of the face during emotional expression."

Did You Know

Facebook is predominantly blue in color because Mark Zuckerberg is red-green colorblind and blue is the "richest color" that he can see

What Are Woofers, Mid-Range Speakers, and Tweeters?

by **Brady Gavin** on July 18th, 2018

Woofers, mid-range speakers, and tweeters are all types of loudspeakers. Most often, all three types of speakers are mounted in a single enclosure, but you can also find each in discrete enclosures. Let's take a closer look at how they work.

Loudspeakers are a type of electrical transducer that converts an electrical audio signal into sound. The most widely used type of speaker today—the dynamic loudspeaker— was first built in the 1920's. It uses a magnetic field to move a flexible diaphragm back and forth very quickly to produce sound waves that carry those sweet tunes right to our ears. That diaphragm is usually fabric, plastic, or paper, and is most often conical in shape, though some speaker makers use different designs.

We categorize speakers by the range of sound they put out, as measured in Hertz (Hz). Some speakers are considered full-range, since they attempt to put out all the frequencies they are sent. The trouble with that is that the size of these full range speakers typically limit how good they sound. Small full range speakers just can't get enough of that bass, and larger ones tend to not do well with the higher frequencies.

Other speakers are more specialized to different ranges. Woofers handle the lower range, mid-range speakers handle the middle range, and tweeters handle the highest range. Put these discrete speakers together, and you get a much fuller, more accurate sound reproduction than you get with a single full-range speaker.

Woofers

Woofers are made to handle the lower range of frequencies (sound waves) for a speaker system, and there are a few different types, depending on your needs. Although they are all built very similarly, there are some distinct differences between each type:

• **Standard Woofer:** A standard woofer produces frequencies from 20 Hz up to 2,000 Hz (2 kilohertz, or 2 kHz). The woofer is often characterized by its bassy sound which comes from the lower frequency sine wave. You'll typically see standard woofers as part of higher-end speakers that contain either a woofer and tweeter (a setup known as a 2-way speaker) or a woofer, tweeter, and mid-range speaker (a setup known as a 3-way speaker).

• **Subwoofer:**

• Subwoofers are only capable of producing tones lower than 200 Hz in consumer systems. They are made up of one or more woofers, often mounted inside a wooden enclosure. Although the human ear is only able to pick up a frequency as low as 12 Hz, subwoofers working at lower frequencies can only be felt, if not heard. Subwoofers are the most common add-on to a consumer speaker setup. They are typically placed in their own, isolated enclosure and provide the low-level thump that you just can't get with standard woofers.

• **Midwoofer:**

• Midwoofers land right in the middle of the 'woofer' range, coming in from 200 Hz -5 kHz. Having such a wide range of frequencies, this speaker will produce the best quality sound from 500 Hz-2kHz and start to deteriorate at either end of the spectrum.

Rotary Woofer: A rotary woofer is a woofer-style loudspeaker that uses a coil's motion to change the pitch of a set of fan blades, instead of using the cone shape. Since the pitch of the blades is changed by the audio amplifier, the power required is much less than that of a conventional subwoofer. They are also far superior at creating sounds well below 20 Hz, below the normal level of human hearing, able to produce frequencies down to 0 Hz by compressing the air in a sealed room.

In most consumer speaker setups, you're likely to find a standard woofer as part of your main speakers and possibly an additional, but separate, subwoofer.

What Are Woofers, Mid-Range Speakers, and Tweeters?

Mid-Range Speakers

Mid-range speakers are targeted to handle the 'middle' range of the spectrum, coming in between 500 Hz-4 kHz. This is probably the most important range of frequencies due to most audible sounds, such as musical instruments and the human voice, being produced here.

Since the human ear is most sensitive to the mid-range frequency, the driver can remain at a lower power, while still providing good sound in terms of quality and volume. Because mid range speakers are unable to produce the extreme low or high spectrum, they often sound dull, or flat, and need the support of a woofer or tweeter to get the full level of sound.

You'll find mid-range speakers used as part of a speaker that also includes a woofer and tweeter, and they're also used in the centre speakers often used with surround sound systems.

Tweeters

On the high end of the sound spectrum, we have tweeters, which get their name from the high tweet of birds. Tweeters typically cover the range of 2 kHz-20kHz, though some specialty tweeters can go as high as 100 kHz.

Traditionally, tweeters were designed pretty much the same way as other speakers—just smaller. The trouble is that sound at that frequency is pretty directional, meaning that the highs in your music sound best when the tweeters are pointed right at you. Modern tweeters are starting to adapt a dome version that uses a soft dome diaphragm made from polyester film, silk, or polyester fabric that has been impregnated with a polymer resin. Dome tweeters are capable of a wider area of sound distribution.

GET OFF YOUR SOAPBOX

The proverbial soap box, as in "Get off your soapbox." or "Don't mind him, he's on his soapbox.", was once quite literal. In the late 1800s and early 1900s, public speakers would stand on large and sturdy crates used to ship soap or other dry goods to grocers in order to elevate themselves above the crowd.

BROWSER EXTENSIONS ARE A PRIVACY NIGHTMARE

STOP USING THEM

Browser extensions are much more dangerous than most people realize. These small tools often have access to everything you do online, so they can capture your passwords, track your web browsing, insert advertisements into web pages you visit, and more. Popular browser extensions are often sold to shady companies or hijacked, and automatic updates can turn them into malware.

Why Browser Extensions Are So Dangerous

Browser extensions run in your web browser, and they often require the ability to read or change everything on web pages you visit.

If an extension has access to all the web pages you visit, it can do practically anything. It could function as a keylogger to capture your passwords and credit card details, insert advertisements into the pages you view, redirect your search traffic elsewhere, track everything you do online—or all these things. If an extension needs to scan your for receipts or other small things, it probably has permission to scan your email for *everything*—which is extremely dangerous.

That doesn't mean that every extension *is* doing these things, but they *can*—and that should make you very, very wary.

Modern web browsers like Google Chrome and Microsoft Edge have a permission system for extensions, but many extensions require access to everything so they can work properly. Even an extension that just requires access to one website could be dangerous, however. For example, an extension that modifies Google.com in some way will require access to everything on Google.com, and therefore have access to your Google account—including your email.

These aren't just cute, harmless little tools. They're tiny programs with a huge level of access to your web browser, and that makes them dangerous. Even an extension that only does a minor thing to web pages you visit may require access to everything you do in your web browser.

How Safe Extensions Can Transform Into Malware

Modern web browsers like Google Chrome automatically update your installed browser extensions. If an extension requires new permissions, it will temporarily be deactivated until you allow it. But, otherwise, the new version of the extension will run with all the same permissions the previous version did. This leads to problems.

In August 2017, the very popular and widely recommended Web Developer extension for Chrome was <u>hijacked</u>. The developer fell for a phishing attack, and the attacker uploaded a new version of the extension that inserted more advertisements into web pages. Over a million people who trusted the developer of this popular extension ended up getting the infected extension. As this is an extension for web developers, the attack could have been a lot worse—it doesn't appear that the infected extension functioned as a keylogger, for example.

In many other situations, someone develops an extension that gains a large amount of users, but doesn't necessarily make any money. That developer is approached by a company that will pay a large amount of money to purchase the extension. If the developer accepts the purchase, the new company modifies the extension to insert advertisements and tracking, uploads it to the Chrome Web Store as an update, and all the existing users are now using the new company's extension—with no warning.

BROWSER EXTENSIONS ARE A PRIVACY NIGHTMARE

STOP USING THEM

This happened to Particle for YouTube, a popular extension for customizing YouTube, in July 2017. The same thing has happened to many other extensions in the past. Chrome extension developers have claimed they constantly receive offers to buy their extensions. The developers of the <u>Honey</u> extension with over 700,000 users once ran an "Ask Me Anything" on Reddit, detailing the kind of offers they often receive.

In addition to the hijacking and sale of extensions, it's also possible that an extension is just bad news, and secretly tracks you when you install it in the first place.

Chrome has been under attack due to its popularity, but this problem affects all browsers. Firefox is arguably even more at risk, since it doesn't use a permission system at all—every extension you install gets full access to everything.

How to Minimize the Risk

Here's how to stay safe: Use as few extensions as possible. If you don't get much use out of an extension, uninstall it. Try to pare down your list of installed extensions to just the essentials to minimize the chance one of your installed extensions goes bad.

It's also important to only use extensions from companies you trust. For example, an extension for customizing YouTube created by a random person you've never heard of is a prime candidate for becoming malware. However, the official Gmail Notifier created by Google, OneNote note taking extension created by Microsoft, or LastPass password manager extension created by LastPass will almost certainly not be sold to a shady company for a few thousand bucks.

You should also pay attention to the permissions extensions require, when possible. For example, an extension that only claims to modify one website should only have access to that website. However, many extensions need access to everything, or access to a very sensitive website you want to keep secure (like your email). Permissions are a nice idea, but they're not too useful when most things need access to everything.

It's a fine line to walk, of course. In the past, we might have said that the Web Developer extension was safe because it was legitimate. However, the developer fell for a phishing attack and the extension became malicious. It's a good reminder that, even if you could trust someone not to sell their extension to a shady company, you're relying on that person for your security. If that person slips up and allows their account to be hijacked, you'll end up dealing with the consequences—and they could be a lot worse than what happened with the Web Developer extension.

Windows 10 Keyboard short cuts

Windows key + Comma	Temporarily peek at the desktop.
Windows key + C	Open Cortana in listening mode.
Windows key + R	Open Run dialog box

How do I download a copy of my information on Facebook?

If you want to download a copy of your information from Facebook, you can use the **Download Your Information** tool.
To download a copy of your Facebook data:
1. Go to the top right of Facebook and

click [ ].
2. Click **Settings**.
3. Click **Your Facebook Information**.
4. Go to **Download Your Information** and click **View**.
5. To add or remove categories of data from your request, click the boxes on the right side of Facebook.
6. Select other options, including:
o The format of your download request.
o The quality of photos, videos and other media.
o A specific date range of information. If you don't select a date range, you'll request all the information for the categories you've selected.
Click **Create File** to confirm the download request.
After you've made a download request, it will appear as **Pending** in the **Available Files** section of the Download Your Information Tool. It may take several days for us to finish preparing your download request

Once we've finished preparing your download request, we'll send a notification letting you know it's ready.
To download a copy of data you requested:
1. Go to the **Available Files** section of the Download Your Information tool.
Click **Download** and enter your password. You can also click **Show more** to view information about your download request, such as the format and when it will expire.
I don't have an active Facebook account. How can I request my personal data stored by Facebook?

Tonight's Topic
GOOGLE EARTH
to be presented by Mr. David Porteous