Computers and stuff.

Sam Houliston.

jaycar
2020 Engineering & Scientific Catalogue
hardcore electronics by
jaycar
think. possible.
Check out our monthly specials + promotions
Click here
2.5" USB 3.0 HDD ADAPTOR WITH CASE
JUST $29.95
XC4152
DVI-D TO DVI-D VIDEO CABLE
JUST $29.95
WC7590
Prices are correct at time of publication and may be subject to change.
USB PORT TO RS485 CONVERTER
JUST $49.95
XC4136

Welcome again to **Jaycar** as the sponsor of Sam's "Computers and Stuff" page. As they are prepared to support us, please show your appreciation and support them. There's always a store near you, click HERE to find the closest.

Beware the privacy and security risks of smart speakers.

TechTalks

"You can turn it off?" he said.
"Yes" said O'Brien, "we can turn it off. We have that privilege."

From 1984 by George Orwell, describing Winston Smith's amazement that Party Official O'Brien was allowed to turn off the device that listens to conversations the whole time. Orwell would have been astounded if he could have known that 70 years after his book was written, people not only had such devices in their homes, but that they had actually gone out and bought them.

Would you be willing to equip your bedroom or living room with an internet-connected microphone that could record and send all your conversations to the data-hungry server of a giant tech company or to a random person in your contact list?

That is basically the privacy and security risk you're taking when you bring home an Amazon Echo, Google Home or other smart speaker.

Since the introduction of the Echo in 2014, smart speakers have moved from a niche domain for geeks and gadget freaks to an inherent part of the lives of tens of millions of people in the U.S. and across the world. Thanks to advances in artificial intelligence and natural language processing (NLP), smart speakers provide us with a hands-free and easy-to-use interface to interact with computers and accomplish tasks that previously required a display and input devices such as a mouse and keyboard.

The convenience and benefits of smart speakers are obvious, but like every other technology they come with their own tradeoffs, highlighted by the many stories that have raised, and exaggerated, concerns about the security and privacy implications of having a smart speaker in your home. Here's what you need to know.

Smart speakers are always listening

Smart speakers become activated with a "wake word." For the Echo, it's "Alexa," and for the Google Home, it's "OK Google." After hearing the wake word, the smart speaker starts analysing whatever comes after it. But to catch the wake word, smart speakers have to keep their microphone active at all time, which is why they call them "always listening" devices.

This has raised concerns about Amazon and Google listening to and storing all your conversations, especially after stories surfaced in which Alexa recorded and shared users' voices without being ordered to do so. However, while smart speakers' "always listening" mode is a privacy issue, it's often exaggerated.

Echo and Google Home must send conversations to their cloud servers because the AI algorithms that analyse and process voice commands require processing capabilities that the devices don't possess. The device doesn't send anything to the cloud before the wake word triggers it. In fact, Google and Amazon would be overwhelmed with useless data if they were recording their smart speakers all day long.

However, this doesn’t mean that a smart speaker, which is basically a computer packed with a microphone and an internet connection, doesn’t have the capability to record and store your conversations in the cloud. In fact, if it’s hacked, or if it malfunctions, that’s exactly what will happen.

But then again, the same threats apply to your phone, which is also a computer with a microphone (and a camera and GPS) and connected to the internet and you always carry it with you instead of letting it sit on a table in your living room.

Data stored in the cloud.

Both Google and Amazon keep a copy of every voice command you send their smart speakers in the cloud. They do so to “improve their services.” This means that if someone gets a hold of your phone, they’ll be able to go through your recorded conversations by accessing the Amazon or Google account associated with your smart speaker. Or if the police serve a warrant, the law of the land and the manufacturer’s devotion to user privacy will determine whether they’ll get access to voice recordings stored in the cloud.

But again, this is basically no different from someone gaining access to your email account and reading through your emails. Like all online accounts, using two-factor authentication and strong passwords is an effective measure to prevent unwanted access to your recordings, however, in contrast to email and messaging services, which offer a range of privacy settings such as PGP and strong, end-to-end encryption, using smart speakers is predicated on letting the manufacturer collect and process your voice.

Users can also go through the accounts linked to their smart speakers and delete their recording history, but it will probably affect the performance of the device.

Unwanted triggering of commands

Smart speakers are pretty decent at answering to queries for information such as the time, the weather and appointments, but the real convenience they bring to consumers’ lives is the accomplishment of tasks. Alexa and Home support thousands of applications such as setting up alarms, playing music, placing orders, setting appointments and more. They’re also capable of manipulating IoT devices such as smart door locks, air conditioners, coffee makers, fridges, toasters and a bunch of other useless stuff.

What this means is that anyone who’s within the hearing range of your smart speaker will be able to send it commands to perform functions. All they need to do is say the magic word. Of course, this can happen if someone breaks into your home (in which case you’ll have bigger problems than your Amazon Echo being used without your permission), but what if your smart speaker was close enough to the window for someone from outside to order it to unlock the door?

Both Echo and Home have also shown that a person doesn't necessarily need to be within their vicinity to activate them. Smart speakers will take command from any device that can play an audio file that says the wake word. Last year, Burger King ran a TV commercial that asked Google to explain what a Whopper is. Tests showed that when a Google Home device was next to the device that played the commercial, it would start describing the whopper.

Another episode involved a 6-year-old kid who accidentally (or intentionally maybe?) ordered an expensive dollhouse while playing with the Amazon Echo in her family's home. Afterwards, a local morning show covered the story and the anchor made a remark about Alexa ordering dollhouses, which triggered even more unwanted orders and refunds. This shows how smart speakers can cause innocent (and sometimes expensive) accidents.

Beyond accidents however, there are real security implications for the remote activation of smart speakers. For instance, a hacker could lure a victim to a malicious website that runs an audio file of a command for Alexa or Google Home. Given the number of functions that the devices can perform, there are many ways this functionality can be put to evil use, such as unlocking doors, making money transfers and more.

Smart speakers usually have settings that add security checks to functions such as shopping. They also have settings that link profiles and functions to specific voices. Users who care for their security should activate those or avoid using smart speakers for critical tasks altogether.

Adversarial attacks

One of creepier security threats of smart speakers is what is known as "adversarial attacks" in which malicious actors send commands to the devices by exploiting weaknesses in the AI algorithms that power them. The way deep learning algorithms and deep neural networks analyse and process audio is different from that of humans. With meticulous work, a malicious actor can create an audio file that sends a hidden command to a smart speaker while sounding like music to human ears.

Adversarial attacks against smart speakers are still in proof-of-concept stage and there still hasn't been a real-world example of the Echo or Home being compromised in this manner, but it's only a matter of time before hackers find ways to put them to destructive use. Unfortunately, there's not much users can do about this and it will be up to manufacturers to harden their devices to minimize the risk of their AI algorithms being exploited to harm their customers.

Closing thoughts

We often misunderstand and exaggerate the security and privacy implications of smart speakers. Where privacy and personal information are concerned, the security threats of smart speakers

run parallel to that of other services we've been using for the past decades. The appearance and methods might be different, but the nature is the same.

However, what makes the smart speaker security important is the access they have to our physical world and daily life. As we increasingly trust smart speakers to accomplish tasks on our behalf in our homes, cars and offices, we must also be wary of who else will be able to do the same.

How do those dead bugs get into enclosed light fixtures?

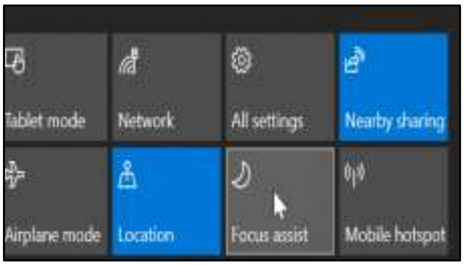
Focus.

TechGenix

If you look, you'll find your computer has tools and applications to help you stay focused on your work. Microsoft has been hard at work making features available that protect us from the other features they created to keep us connected. Finding that balance is a real problem for everyone these days. We need to be connected and responsive but we also need to be able to get some work done. Blocking out all of the distractions is what these focus tools are all about. Here are a few that will help you.

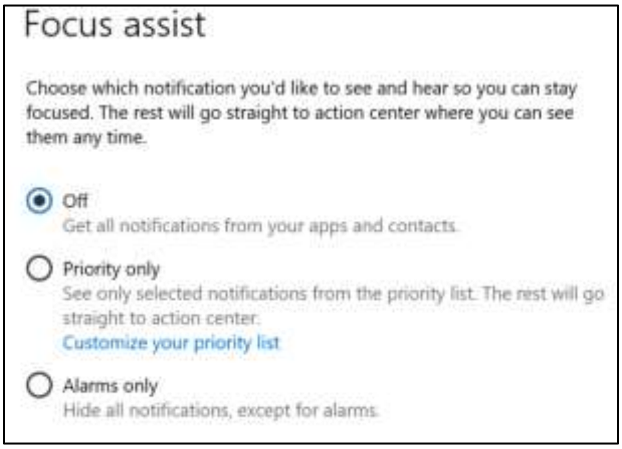
Focus Assist.

Focus Assist is the flagship tool that Microsoft has been refining since Windows 8. By pressing Focus Assist in the notification area, you can immediately stop your computer from popping up notifications. (the "Notification Area" is accessed by clicking the small square with the V at the bottom to the right of the time indicator on the task bar at the bottom right of your screen see HERE.) If you don't see the icons at right, you might need to click *Expand* to see them. You can also configure activities and a time range that when you enter that activity or time range your computer automatically goes into Focus Assist.



To start Focus Assist, click on your notifications centre, then press the Focus Assist button. You can press it multiple times to toggle through Priority only, Alarms only, and off.

To customize your automatic Focus Assist settings, press your Windows key, type Focus Assist, in the little window bottom left and open *Focus Assist Settings*. It's not obvious but once you turn on the "During these times" option, you can click the hours and it will let you set a time range. So maybe rather than overnight, you want it to be from 10 a.m.-12 p.m., for example. You can do that.



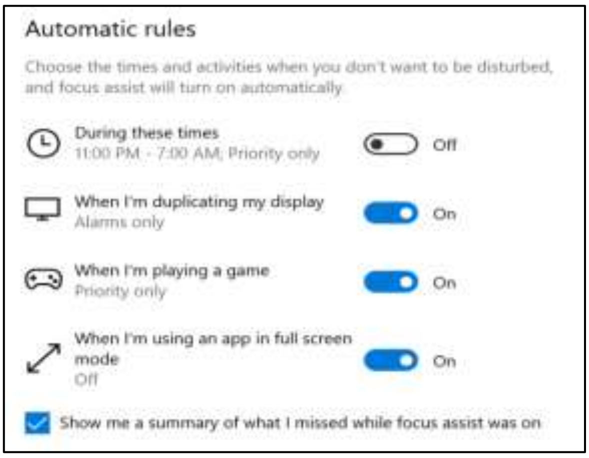
Focus assist

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

● Off
Get all notifications from your apps and contacts.

○ Priority only
See only selected notifications from the priority list. The rest will go straight to action center.
Customize your priority list

○ Alarms only
Hide all notifications, except for alarms.



Automatic rules

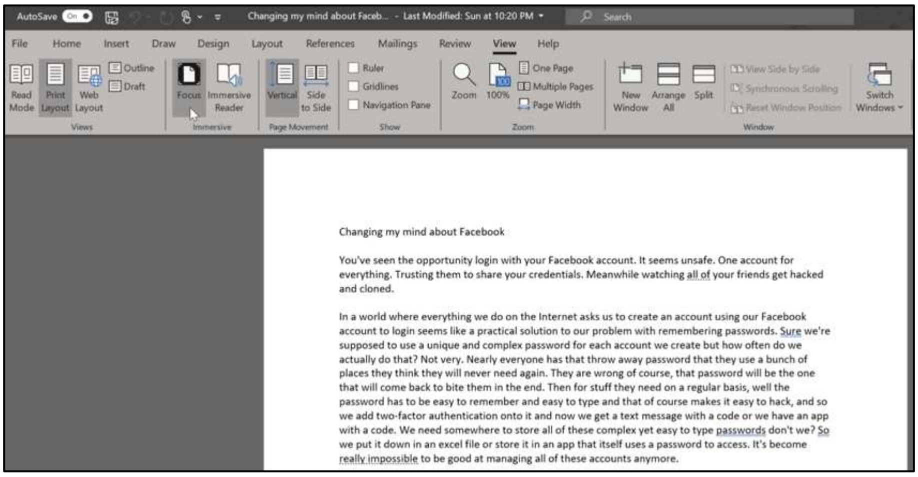
Choose the times and activities when you don't want to be disturbed, and focus assist will turn on automatically.

During these times 11:00 PM - 7:00 AM; Priority only		Off
When I'm duplicating my display Alarms only		On
When I'm playing a game Priority only		On
When I'm using an app in full screen mode Off		On

☑ Show me a summary of what I missed while focus assist was on

Word Focus View.

Microsoft Word has a focus view for Office 365 subscribers only. To enter focus mode in Word you go to the View menu and choose Focus in the Immersive tag (below). Basically, Focus mode in Word is a page on a blank screen. All of the menus go away. Focus mode is for when you just want to get the words down on the page.

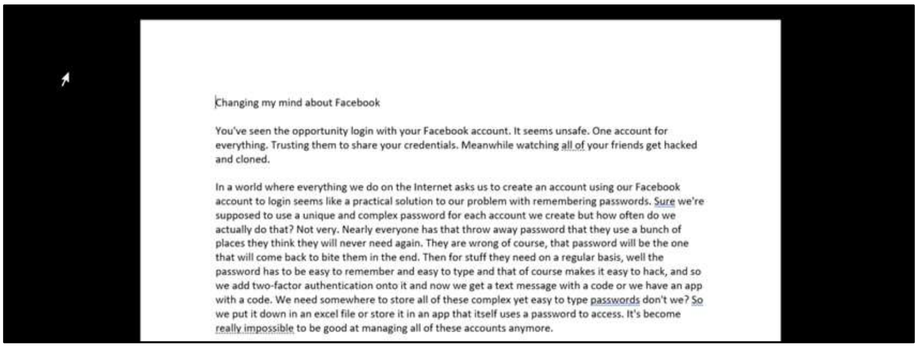


Changing my mind about Facebook

You've seen the opportunity login with your Facebook account. It seems unsafe. One account for everything. Trusting them to share your credentials. Meanwhile watching all of your friends get hacked and cloned.

In a world where everything we do on the Internet asks us to create an account using our Facebook account to login seems like a practical solution to our problem with remembering passwords. Sure we're supposed to use a unique and complex password for each account we create but how often do we actually do that? Not very. Nearly everyone has that throw away password that they use a bunch of places they think they will never need again. They are wrong of course, that password will be the one that will come back to bite them in the end. Then for stuff they need on a regular basis, well the password has to be easy to remember and easy to type and that of course makes it easy to hack, and so we add two-factor authentication onto it and now we get a text message with a code or we have an app with a code. We need somewhere to store all of these complex yet easy to type passwords don't we? So we put it down in an excel file or store it in an app that itself uses a password to access. It's become really impossible to be good at managing all of these accounts anymore.

The page above becomes the page below when focusing:



Changing my mind about Facebook

You've seen the opportunity login with your Facebook account. It seems unsafe. One account for everything. Trusting them to share your credentials. Meanwhile watching all of your friends get hacked and cloned.

In a world where everything we do on the Internet asks us to create an account using our Facebook account to login seems like a practical solution to our problem with remembering passwords. Sure we're supposed to use a unique and complex password for each account we create but how often do we actually do that? Not very. Nearly everyone has that throw away password that they use a bunch of places they think they will never need again. They are wrong of course, that password will be the one that will come back to bite them in the end. Then for stuff they need on a regular basis, well the password has to be easy to remember and easy to type and that of course makes it easy to hack, and so we add two-factor authentication onto it and now we get a text message with a code or we have an app with a code. We need somewhere to store all of these complex yet easy to type passwords don't we? So we put it down in an excel file or store it in an app that itself uses a password to access. It's become really impossible to be good at managing all of these accounts anymore.

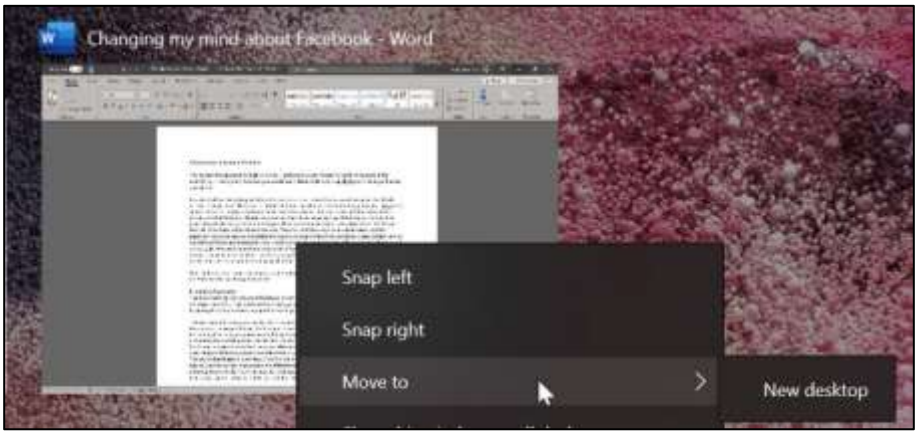
F

You exit focus mode by pressing Esc to get the menus back. Most people will find they are so used to the menus that they will find writing without them to be somewhat unsettling. But there certainly are no distractions.

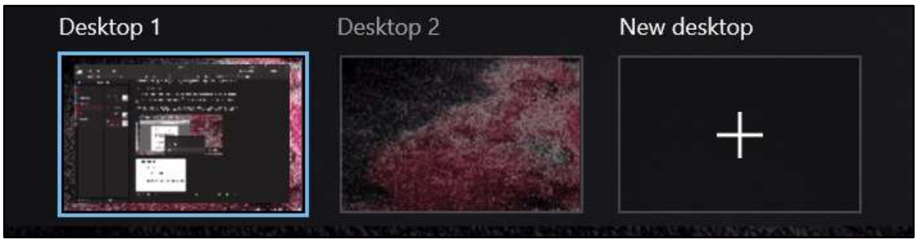
Windows 10 virtual desktops.

In Windows 10 you can create virtual desktops. A virtual desktop is just another name for multiple desktops. This means that when you're ready to work on something you can leave behind your default desktop and move onto the desktop space that has only the applications that you need to complete the job. All of the distractions will be left behind, too.

If you want to remove distractions while working on a Word document, you could move it onto a new desktop by clicking on Task View on your Windows taskbar, then right-clicking on the Word applications and choose Move to, *New desktop*. (You access the *Task View* by clicking this small icon ⧉ which you'll find at the bottom left of the task bar.)

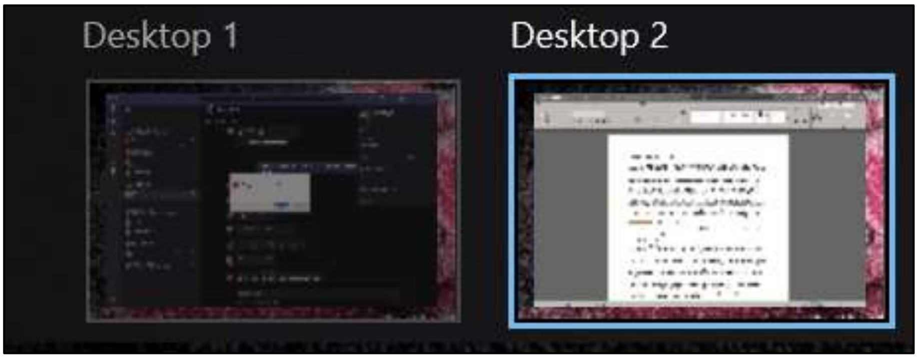


When you do, you'll be presented with a choice of desktops. Desktop 1 is the main desktop and the others are virtual.

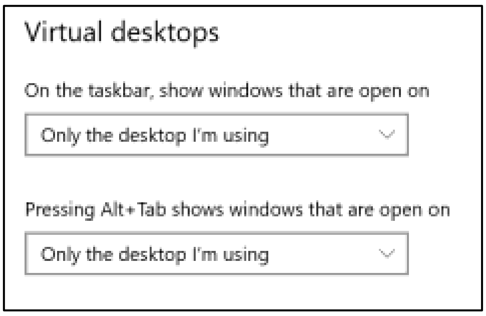


After you choose Desktop 2, the Word document you're using disappears from Desktop 1 and moves onto Desktop 2.

G



Since Word is your only open application on Desktop 2 you're not distracted by any other applications or notifications.



Virtual desktops

On the taskbar, show windows that are open on

Only the desktop I'm using

Pressing Alt+Tab shows windows that are open on

Only the desktop I'm using

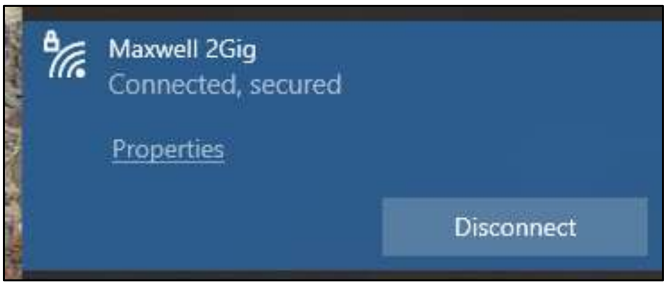
You have two settings in Windows Settings for virtual desktops. These are whether to show the applications that you have pinned to your taskbar or not and whether or not you want Alt-tab to allow you to switch between applications on your virtual desktops.

You could find virtual desktops handy when you have a deadline and really need to disconnect from everything else that might be happening. To switch between desktops, use Windows+CTRL, then the left or right arrow to move between them.

Metered Connections and Quiet Time.

Microsoft probably didn't intend for these two features to be used to create focused time but they work. Metered connections are a type of WiFi service where you have a limited amount of data usage available to you. When you mark a WiFi connection as metered, Microsoft will pause updates but it also ends up reducing the number of distractions caused by applications asking for your attention. The result of minimizing data usage is that your apps get less annoying too. It's wise though not to have your device running on Metred Connections full time as this will not allow your device to update itself. It is very important that you allow your device to install all and every update made available by your OS and also your anti-virus software.

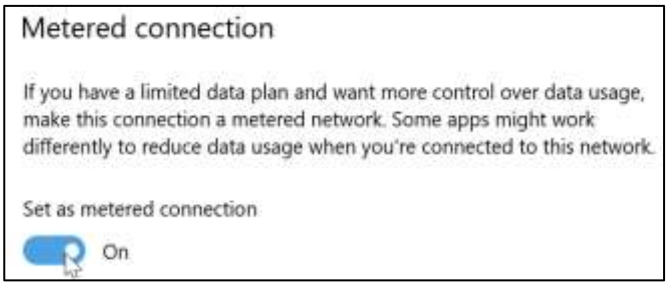
To make a WiFi connection a metered connection, click the connection icon, that's this little icon down the bottom right of your task bar then click properties. Flip the Metered Connection setting to on. Don't forget to turn it off again after you're finished.



Maxwell 2Gig
Connected, secured

Properties

Disconnect



Metered connection

If you have a limited data plan and want more control over data usage, make this connection a metered network. Some apps might work differently to reduce data usage when you're connected to this network.

Set as metered connection

On

My wife said that if I don’t get off my computer and help with the dishes she’ll slam my head on the keyboard, but I think she’s jokiasdfasdfq23r41234asdfasdfasdfqr45123451345sdgfasdgf

Introducing Microsoft 365.

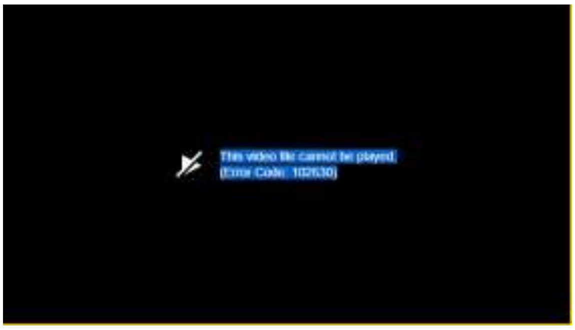
On the 21st April 2020, Office 365 became Microsoft 365. Your subscription still includes everything you enjoyed previously, such as premium Microsoft Word, Excel, OneNote, PowerPoint and Outlook apps as well as 1 TB of OneDrive cloud storage, plus, you can still share your subscription with up to five other people. There’s more info HERE.

This Video File cannot be played?

Are you getting “This Video File cannot be Played” error on your device? Read on and learn every possible fix for the different “videos not playing” errors.

The videos not playing issue can be encountered by most browsers as well as Android phones. Since there could be all kinds of reasons for this, we need to first diagnose the problem and later resolve it.

Part 1: Why are you unable to Play Videos?



This video file cannot be played.
(Error Code: 102630)

Before we get into the details, it is important to know why you are getting the file could not be played issue. Ideally, it can be caused due to the following reasons:

- The video you are trying to play can be corrupted.
- There might be some issue with the media player installed on your device.
- You might be using an old or corrupted browser.
- The video you are trying to play might not be supported by your browser.
- The browser might not have the needed extension or an add-on player installed.
- If the file has been hosted online, then it can become unavailable or corrupt.
- You can no longer have the access to the file anymore.
- A faulty extension or browser add-on can also cause this problem.
- You might be trying to play the video that is not allowed in your location.
- A VPN or third-party firewall could have blocked the video playback.

Apart from this, there could be any other software related issues for videos not playing on a phone or computer.

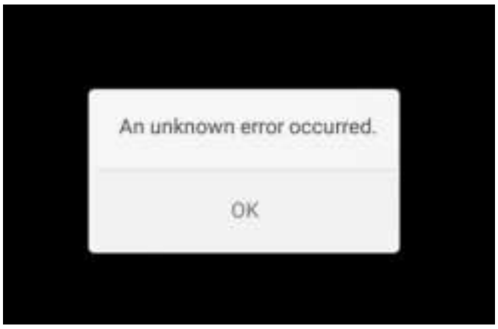
I

Part 2: How to Fix General “This Video File Cannot Be Played” Error Codes?

Following are some common errors that users encounter while playing a video on their computers or handheld devices.

An Error has Occurred.

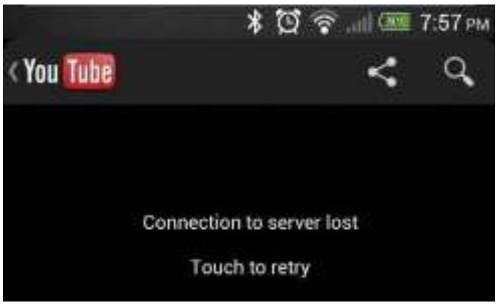
This is one of the most general errors for videos not playing. It mostly occurs when the internet connection on the device is lost in between or the video has been removed from the server. Try to replay the video and make sure you have a stable internet connection to fix it.



An unknown error occurred.

Connection to Server lost .

As the error message states, the issue happens when the device loses its connection to the internet. Just make sure that the phone or the computer is connected to a stable internet connection. Also, check if the video is available on its main server or not.

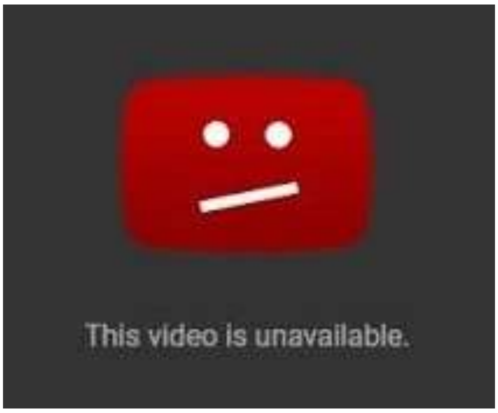


Connection to server lost

Touch to retry

The Video is Unavailable.

If you are unable to play a video and have got the error, then it means the video has been removed or deleted from its original location. The situation is more common in Google Drive videos not playing when the content gets removed from its source. Platforms like YouTube could have deleted the video if it was violating its terms and conditions.



This video is unavailable.

Video Error 500

This video file cannot be played error is more common in streaming services like Amazon Prime, Hulu, Netflix, YouTube, and so on. It usually happens due to an internal problem with the browser. If you cannot play a video due to this, then just consider clearing the browser’s cache. Just launch the browser, hold down the CTRL and SHIFT keys then press the DELETE key.

This Video File Cannot be Played (Error 102630)

This is a scenario for videos not playing on Android for third-party media players. For instance, the JW Media Player often displays the “This Video File Cannot be Played: Error 102630” when the app is corrupted. You can easily fix the issue by reinstalling or updating the app. Alternatively, you can try any other media player and check if the file could not be played or not.

J

Apart from this, there could be several other errors that are caused by browser, app, or the device itself.

Part 3: Fix “This Video File Cannot Be Played” in Different Scenarios

Not just Android phones, a lot of people are unable to play videos on their computers or browsers as well. Following are some of these major cases for videos not playing that you can encounter (and fix).

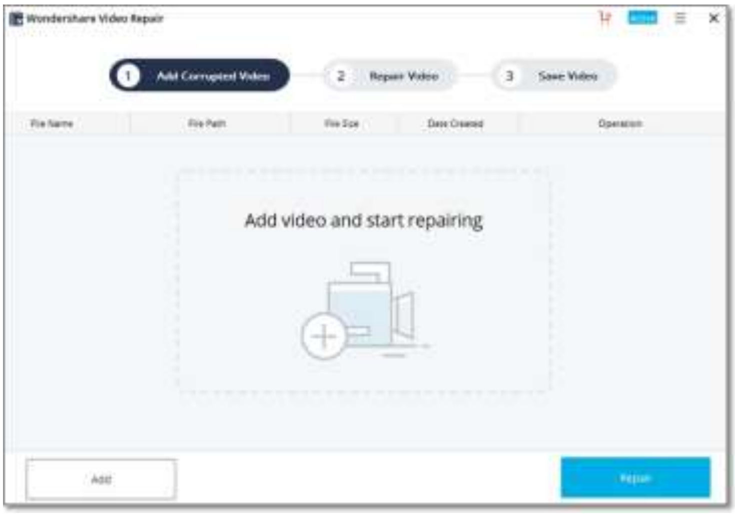
Situation 1: Computer Not Playing the Stored Videos

If the video is already saved on your computer and you are not able to fix it, then there might be an issue with the player or the video itself. To fix “This video file cannot be played”, you can try to play the video with another player or repair the corrupted video as well.

Fix 1: Use another Media Player
Chances are that there could be a problem with the media player that you are using. In this case, you can just try another media player and check if the video is getting played or not. For instance, if the MOV video player is displaying an error, then you can use Windows Media Player or VLC Player instead.

Fix 2: Repair the Video using a Professional Tool
If the video has been corrupted, then you can use a professional tool like Recoverit Video Repair. It is a user-friendly DIY tool that can repair videos of every major format like MOV, MKV, MP4, FLV, AVI, and more. (It is not free, you must pay for it). From a logical error in the file to syncing problems and video corruption to frozen videos – the application can fix the videos not playing issue under all scenarios. It features two different repairing modes – quick and advanced video repair that you can choose as per your requirements. If you want it, you can download it here
Download | Win   Download | Mac

With the software, you can follow these simple steps to repair the saved videos on your computer.



Step 1: Load the corrupted or damaged videos
To start with, just install and launch the Recoverit Video Repair application on your computer. Now, just drag the videos you wish to repair and drop them on the interface. You can also click on the “+” button to launch a browser window to select multiple videos to load.

Step 2: Repair the added videos
Once the videos are added, you can just click on the “Repair” button to start the process. You can load a single or multiple

videos as per your requirements. Let the application complete the process and don’t halt it in between to get the best results.

Step 3: Save the repaired videos

In the end, you will be notified when the video repairing process is completed. You can now just save the repaired videos wherever you want on your system.

Step 4: Perform an advanced repair (optional)

If it fails to repair the broken video in Quick mode, then click on the “Advanced Repair” option on the interface. This will ask you to upload a sample video that is of the same format and was shot on the same device. The application will keep it as a reference to perform a more sophisticated repairing operation on the video. Finally, click Repair button to repair your video.

Situation 1: Videos Not Playing on Android

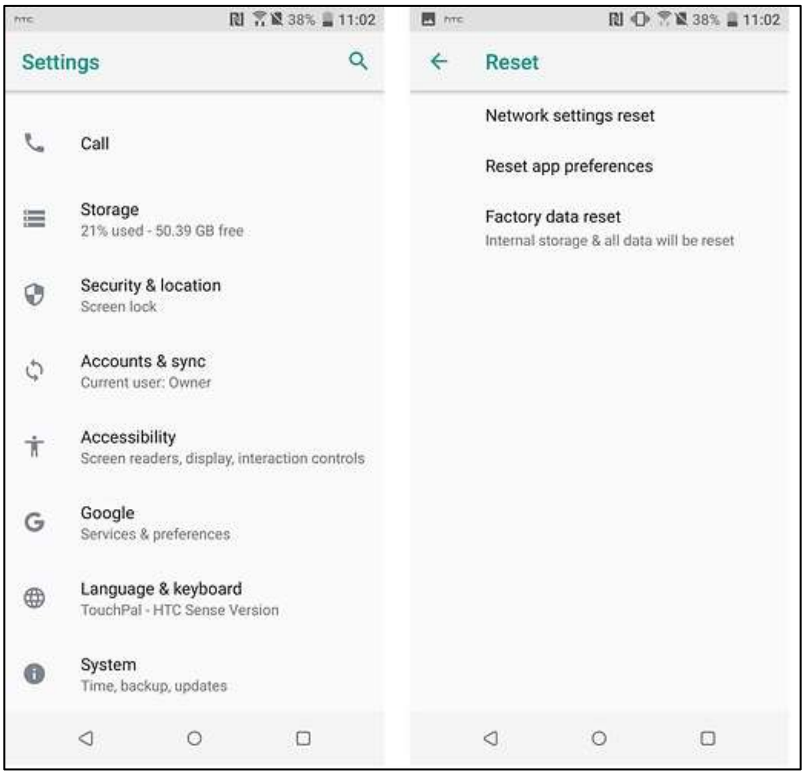
As well as videos not playing on your computer, you can also get the “This video file cannot be played” on an Android. The error can be caused due to a malfunctioning application or system settings.

Fix 1: Reset network settings.

The videos not playing error can arise due to some change in the network settings on the device. To fix this, you can just reset its network settings by visiting its Settings > Reset or WiFi & Network Settings.

Fix 2: Update the App.

If the videos are not playing on an Android phone for particular apps, then you can consider updating them. For instance, if you are not able to play videos on YouTube, then just go to the Play Store, look for YouTube, and update it. If you are using an old app, then you would get an option to update it on its interface as well.



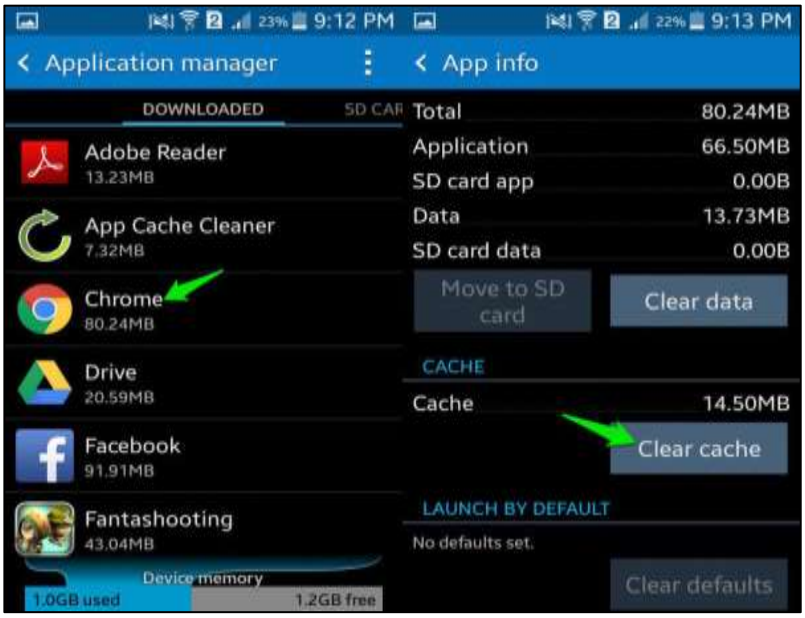
Situation 2, Error Loading Media: File could not be played on Chrome

Sometimes, users are unable to play a video specifically on Google Chrome. In this case, you can try any other browser (like Firefox or Opera) and check if the problem sustains or not. Otherwise, there might be an issue with your device instead.

L

Fix 1: Check network connections
Needless to say, your device should be connected to an active network. You can also turn on the mobile data on it to further check the problem. Also, turn on the Airplane mode and turn it off after a while. Now, try to access the video again and check if the file could not be played or not.

Fix 2: Clear Chrome Cache
If the Google Chrome application has accumulated a lot of data, then it can cause the videos not playing problem. To fix this, just go to your device's Settings > Apps or Application Manager. From here, select the Chrome application and tap on the "Clear Cache" button.



9:12 PM

< Application manager

DOWNLOADED SD CAR

Adobe Reader 13.23MB

App Cache Cleaner 7.32MB

Chrome 80.24MB

Drive 20.59MB

Facebook 91.91MB

Fantashooting 43.04MB

Device memory 1.0GB used 1.2GB free

9:13 PM

< App info

Total	80.24MB
Application	66.50MB
SD card app	0.00B
Data	13.73MB
SD card data	0.00B

Move to SD card Clear data

CACHE

Cache 14.50MB

Clear cache

LAUNCH BY DEFAULT

No defaults set.

Clear defaults

Situation 3: This Video File Cannot Be Played on Google Drive

There are times when users are unable to play the video on Google Drive. This can happen while accessing Google Drive on their browser or via its dedicated application.

Fix 1: Clear browser history
If you are accessing Google Drive on any browser, then you can just go to its settings and choose to clear the browser history. After that, close the application, and restart it to access the video.

Fix 2: Check the video format and resolution
Google Drive does not support every video format and resolution. Therefore, before you upload a video, make sure that the format and resolution are supported by Google Drive.

Fix 3: Check if the video is still available
If you are trying to access a video on Google Drive that is hosted by someone else, then check its availability. The video could be deleted or the owner might have revoked the permission to the video access.

Situation 4: Cannot Play Video on Media Player

Lastly, you might encounter the videos not playing on your phone while browsing certain apps like Facebook or Twitter. In this case, you can just close the app from running in the background and reopen it. If it won't resolve the videos not playing issue, then go to the Play Store and consider updating the app. You can also delete the app and later reinstall it on your device as well.

Windows 7 – EOL.

Malwarebytes

End-of-life (EOL) is an expression commonly used by software vendors to indicate that a product or version of a product has reached the end of usefulness in the eyes of the vendor. Many companies, including Microsoft, announce the EOL dates for their products far in advance.

Every Windows product has a lifecycle. The lifecycle begins when a product is released and ends when it's no longer supported. Knowing key dates in this lifecycle helps you make informed decisions about when to update, upgrade, or make other changes to your software.

For those that are unaware, Windows 7 reached EOL on the 14th January, 2020. When a Windows Operating System (OS) hits the end of its lifecycle, it no longer receives updates from Microsoft. That means Microsoft no longer supports users of Windows 7, and Windows 7 will no longer receive updates, although Microsoft has been known to make exceptions for urgent vulnerabilities, and while organizations may be able to extend support by paying for it, home users are advised to move on to more modern operating systems.

Now is the time to shift to Windows 10. Get robust security features, enhanced performance, and flexible management to keep your employees productive and secure. If cybercriminals discover a vulnerability in Windows 7, there is no guarantee that this vulnerability will be patched by Microsoft and while there is still a large Windows 7 user base, it pays off for the cybercriminals to weaponize such a vulnerability and use it to their advantage. Keep in mind that most of the exploit kits active in the wild focus on older vulnerabilities, which will not be patched if you are using EOL software.

Is Windows 10 more secure?

While the call to move on to Windows 10 by Microsoft makes it sound mighty safe, what exactly are these security features that Windows 10 has over Windows 7? We know it'll be supported by Microsoft and therefore any known vulnerabilities will be patched. Its other security features are as follows:

- Windows 10 includes Windows Defender by default, which provides a baseline level of antivirus protection.
- SmartScreen is a reputation system that tries to block harmful and unknown file downloads.
- Windows 10 includes Microsoft Edge instead of Internet Explorer, which is targeted most often by exploits.

On the downside, you might argue that Windows 10 has a lot of new features that tend to come with new problems and risks, however, Windows 10 has been around for a while now, so the worst problems should have been tackled, however, we want to stress:

- Moving on to a new operating system, while safer than sticking with a legacy system, is no substitute for a strong security solution. Even Windows 10 machines need anti-malware protection.

According to a spokesperson from Microsoft's malware removal staff, the correlation between browser use and malware is actually higher than the one between OS version and malware. Meaning: The browser you use has a much bigger impact on the likelihood of being infected than the OS that you use, so even if you switch over to Windows 10 but keep using Google Chrome, you can still be easily infected. Now that Windows 10 has switched over to Edge, many cybercriminals are focusing on exploits for Google Chrome, one of the most popular browsers today.

Other operating systems.

To avoid potential infection, or because they're looking for a change, some Windows users might consider moving to entirely different operating systems, such as Mac or Linux, but layering up built-in protection with security software is important, even if you decide to switch.

For example, the long-standing myth that Macs are safer than Windows systems has been proven wrong. As you can read in Malwarebyte's 2020 State of Malware Report, Mac threats increased exponentially in comparison to those against Windows PCs in 2019, with nearly double the threats per Mac endpoint than Windows. And while Macs don't get viruses, Mac adware is more sophisticated and dangerous than traditional Mac malware. In some cases, people may consider switching to a Chromebook, which is certainly a cheaper option if it offers enough capabilities to replace your current Windows desktop or laptop. But even Chromebooks can—and do—get infected.

A lot of users won't switch to a more hardcore Linux OS, because they expect a huge learning curve (another misconception) or think their favourite software would not be available (sometimes true, but not always). However, even if they did, Linux OSs are not free from malware, they're primarily attacked less often because cybercriminals understand their user base isn't large and is probably more knowledgeable about malware, so their payday isn't as big. The American NSA, keen to hack others but not keen on being hacked themselves, are thought to use Linux PCs 'hardened' with 'Mandatory Access Controls' and with competent antivirus software. It's surprisingly easy to set up something like that for home use.

Windows 7 user base

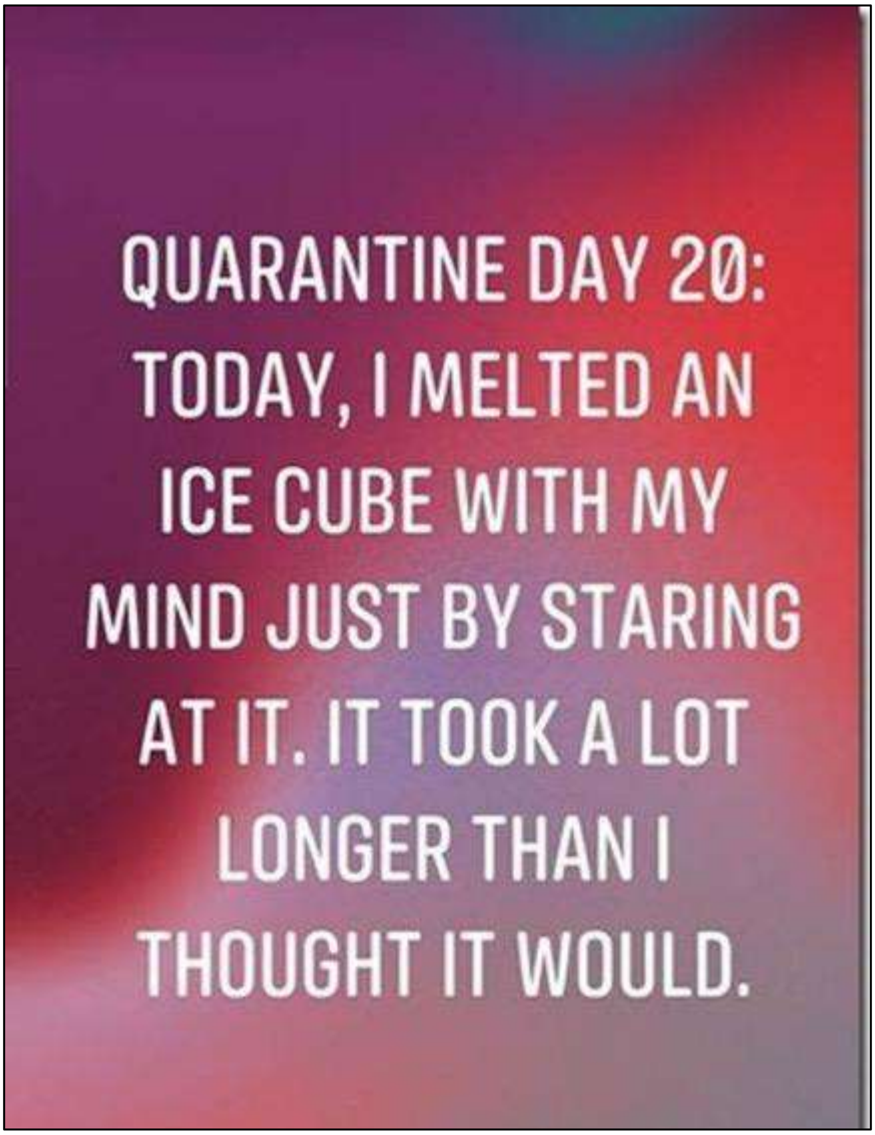
Currently over 23 percent of Windows users worldwide are still on Windows 7, and only 69 percent have already switched to Windows 10, the rest are using the less popular Windows 8 or versions of Windows that have gone EOL long before Windows 7. Oddly enough, the percentage of Windows 7 users has hardly decreased after reaching the EOL date in January (from roughly

O

24 percent to 23 percent) and with this huge amount of potentially unpatched systems still active in the market, any exploitable vulnerability will result in a widespread disaster.

Would WannaCry have had such an enormous impact if Windows XP and Windows Server 2003 had been abandoned before it spread? We will never know. What we do know that Windows 8 and 10 did not need to be patched for the vulnerability that was used to spread WannaCry. They were not contributing to the choir of systems trying to infect their neighbours. Emergency patches were released for several older Windows versions, including Windows 7. At the time, Windows 7 was still supported.

If you're still using Windows 7, it is strongly suggested you upgrade to Win 10 now. You can still do it for free, I wrote how to so do a while back, see HERE



QUARANTINE DAY 20: TODAY, I MELTED AN ICE CUBE WITH MY MIND JUST BY STARING AT IT. IT TOOK A LOT LONGER THAN I THOUGHT IT WOULD.