Computers and stuff.

Sam Houliston.

Word Count.

Have you ever written a letter or a story or an article in Word and wondered how many words you've written? You could count them all or get an average by counting how many in a line then multiplying by the number of lines, that's a bit tedious, surely there's an easier way.

Well there is!

All you have to do is highlight all the words then press ***Ctrl, Shift, G*** together and bingo, Microsoft does it all for you.

Microsoft will give you these figures:

Number of pages	Number of words
Total characters (no spaces)	Total characters (with spaces)
Number of paragraphs	Number of lines.

Very clever.

How Antivirus Software works.

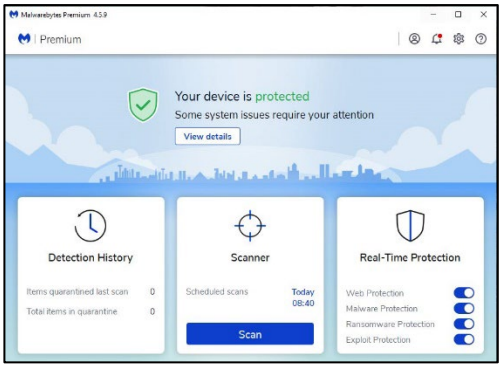
How-To Geek

Everyone accepts that Antivirus programs are essential on computers that connect to the internet, but have you ever wondered how they work.

An antivirus program is an essential part of a multi-layered security strategy, even if you're a smart computer user, the constant stream of vulnerabilities for browsers, extensions and the operating system itself make antivirus protection important.

On-Access Scanning
Antivirus software runs in the background on your computer, checking every file you open. This is generally known as on-access scanning, background scanning, resident scanning, real-time

protection, or something else, depending on your antivirus program. On a PC, when you double-click an EXE file, it may seem like the program launches immediately, but it doesn't. Your antivirus software checks the program first, comparing it to known viruses, worms, and other types of malware. Your antivirus software also does "heuristic" checking, checking programs for types of bad behaviour that may indicate a new, unknown virus.



Antivirus programs also scan other types of files that can contain viruses. For example, a .zip archive file may contain compressed viruses, or a Word document can contain a malicious macro. Files are scanned whenever they're used, for example, if you download an EXE file, it will be scanned immediately, before you even open it.

It's possible to use an antivirus without on-access scanning, but this generally isn't a good idea, viruses that exploit security holes in programs wouldn't be caught by the scanner. After a virus has infected your system, it's much harder to remove. (It's also hard to be sure that the malware has ever been completely removed.)

Full System Scans.

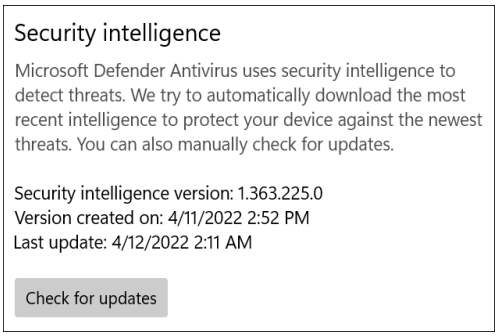
Because of the on-access scanning, it isn't usually necessary to run full-system scans. If you download a virus to your computer, your antivirus program will notice immediately, you don't have to manually initiate a scan first.

Full-system scans can be useful for some things, however. A full system scan is helpful when you've just installed an antivirus program, it ensures there are no viruses lying dormant on your computer. Most antivirus programs set up scheduled full system scans, often once a week. This ensures that the latest virus definition files are used to scan your system for dormant viruses. These full disk scans can also be helpful when repairing a computer. If you want to repair an already-infected computer, inserting its hard drive in another computer and performing a full-system scan for viruses (if not doing a complete reinstall of Windows) is useful. However, you don't usually have to run full system scans yourself when an antivirus program is already protecting you, it's always scanning in the background and doing its own, regular, full-system scans.

Virus Definitions

Your antivirus software relies on virus definitions to detect malware. That's why it automatically downloads new, updated definition files, once a day or even more often. The definition files contain signatures for viruses and other malware that have been encountered in the wild. When an antivirus program scans a file and notices that the file matches a known piece of malware, the antivirus program stops the file from running, putting it into "quarantine." Depending on your antivirus program's settings, the antivirus program may automatically delete the file or you may be able to allow the file to run anyway—if you're confident that it's a false positive.

Antivirus companies have to continually keep up-to-date with the latest pieces of malware, releasing definition updates that ensure the malware is caught by their programs. Antivirus labs use a variety of tools to disassemble viruses, run them in sandboxes, and release timely updates that ensure users are protected from the new piece of malware.



Heuristics

Antivirus programs also employ heuristics and machine learning. Machine learning models are created by analysing hundreds or thousands of pieces of malware to find common attributes or behaviours. The combination allows an antivirus program to identify new or modified types of malware, even without virus definition files. For example, if an antivirus program notices that a program running on your system is trying to open every EXE file on your system, infecting it by writing a copy of the original program into it, the antivirus program can detect this program as a new, unknown type of virus.

No antivirus program is perfect. Heuristics that are too aggressive, or machine learning models that are trained incorrectly, can accidentally mark perfectly safe software as malware.

False Positives

Because of the large amount of software out there, it's possible that antivirus programs may occasionally say a file is a virus when it's actually a completely safe file. This is known as a "false positive." Occasionally, antivirus companies even make mistakes such as identifying Windows system files, popular third-party programs, or their own antivirus program files as viruses. These false positives can damage users' systems, such mistakes generally end up in the news, as when Microsoft Security Essentials identified Google Chrome as a virus, AVG damaged 64-bit versions of Windows 7, or Sophos identified itself as malware.

Heuristics can also increase the rate of false positives. An antivirus may notice that a program is behaving similarly to a malicious program and erroneously identify it as a virus. Despite this, false positives are fairly rare in normal use. If your antivirus says a file is malicious, you should generally believe it. If you're not sure whether a file is actually a virus, you can try uploading it to VirusTotal (which is now owned by Google). VirusTotal scans the file with a variety of different antivirus products and tells you what each one says about it.

Detection Rates

Different antivirus programs have different detection rates and both virus definitions and heuristics contribute to the discrepancies. Some antivirus companies may have more effective heuristics and release more virus definitions than their competitors, resulting in a higher detection rate.

Some organizations do regular tests of antivirus programs in comparison to each other, comparing their detection rates in real-world use. AV-Comparitives regularly releases studies that

compare the current state of antivirus detection rates. The detection rates tend to fluctuate over time, there's no one best product that's consistently on top. If you're really looking to see just how effective an antivirus program is and which are the best out there, detection rate studies are the place to look.

Testing an Antivirus Program

If you ever want to test whether an antivirus program is working properly, you can use the EICAR test file. The EICAR file is a standard way to test antivirus programs, it isn't actually dangerous, but antivirus programs behave as if it's dangerous, identifying it as a virus. This allows you to test antivirus program responses without using a live virus.

The older I get, the more clearly I remember things that never happened

JPG vs JPEG: Are they the same thing?

If you've used a computer, digital camera, or smartphone long enough, you've likely seen files with either JPG or JPEG extensions in them. But are they the same thing? What's the difference?

Well, not a lot, they're just two abbreviations for the same image format.

"JPG" and "JPEG" are two file extensions that refer to the exact same digital image format. JPEG is an abbreviation for "Joint Photographic Experts Group," which is a tech industry group that created the JPEG image format widely in use in digital cameras, social media, and on the web.

The JPEG format originated in 1992. At that time, most of the world's personal computers ran the Microsoft MS-DOS operating system, which only supported three-letter file extensions (borrowed from CP/M). As a result, JPEG files gained the extension "JPG" on MS-DOS and early Windows platforms. Meanwhile, the Apple Macintosh platform had no such limitation, so JPEG files often carried the .JPEG file extension there.

Today, both Windows and macOS can handle the full .JPEG file extension and most apps understand and open both .JPG and .JPEG files equally. So, if you have files with either extension that open properly in an image viewer or editor, there's no need to make any changes on your part.

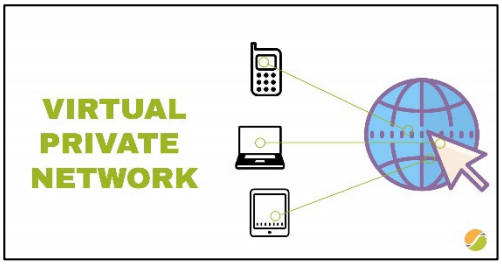
Can I convert JPEG to JPG?

Since JPEG and JPG files are the exact same image format, no conversion is necessary to turn a JPG file into a JPEG, or vice-versa. Instead, all you need to do is rename the image file and change the file extension. For example, if you have a file named “IMAGE.JPEG”, and you’d rather have “IMAGE.JPG”, use the rename feature in your operating system to edit the “IMAGE.JPEG” file name and remove the “E” from the “JPEG” extension. You can also do the same in reverse, changing “JPG” to “JPEG”.

If you have a large number of JPEG or JPG files you want to rename, you can automate the process fairly easily both on Windows (by selecting multiple files and selecting “Rename” in the context menu) and Macs (using the “Rename Items” option in the menu bar).

The biggest joke on mankind is that
computers have started asking humans to prove that they aren’t a robot.

VPN



Many people these days use a VPN to hide their real IP address and encrypt their internet connection. There are 3 main reasons why:

- **Your browsing history is private** — A VPN hides your browsing and search history from your Internet Service Provider (ISP). The only thing the ISP can see is your encrypted traffic traveling to the VPN server.
- **You can change your online location** — Your IP address gives away your physical location. With a VPN, you can connect to a server in a different country.
- **Your internet activities are anonymous** — A no-logs VPN ensures that no one knows what you’re doing on the web.

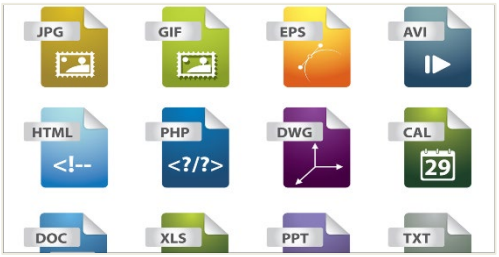
However – it can cause a problem. If you do your banking via computer and you’re connected via your VPN, your bank will connect your account details with a different IP address originating in another country (that of the VPN) and could consider there is some suspicious activity on your account – and block it.

If you consider using a VPN, let your bank know or you could be locked out.

How to make Windows show file extensions.

Windows doesn’t show file extensions by default, but you can change a single setting and make Windows always show you each file’s full file extension. This works in File Explorer on Windows 10 and Windows 11 as well as Windows Explorer on Windows 7 and Windows 8.

Why you should show File Extensions.

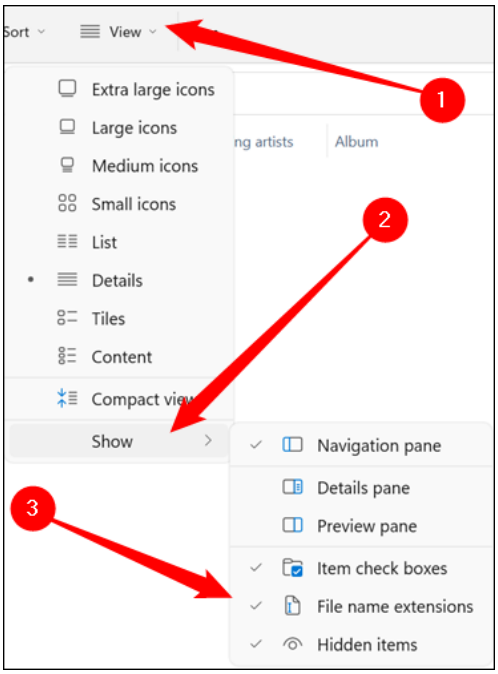


Each file has a file extension that tells Windows what type of file it is. File extensions are usually three or four digits long, but can be longer. For example, Word documents have the .doc or .docx file extension. If you have a file named Example.docx, Windows knows it's a Word document and will open it with Microsoft Word.

There are many different file extensions. Audio files may have a file extension like .mp3, .aac, .wma, .flac, .ogg, and some common image file extensions are .jpeg, .png, .gif, and .heic.

Setting Windows to show file extensions is helpful for security. For example, the .exe file extension is one of many file extensions that Windows runs as a program. If you can't see what a file's extension is, it's hard to tell whether it's a program or a safe document or media file. As an example, you may have a file named "document" that has the icon of your installed PDF reader. With file extensions hidden, there's no quick way to tell if this is a legitimate PDF document or is actually a malicious program using your PDF reader's icon as a disguise. If you had Windows set to show file extensions, you'd be able to see whether it's a safe document with the name "document.pdf" or a dangerous file with a name like "document.exe". You could look at the file's properties window for more information, but you don't need to do that if you've enabled file extensions.

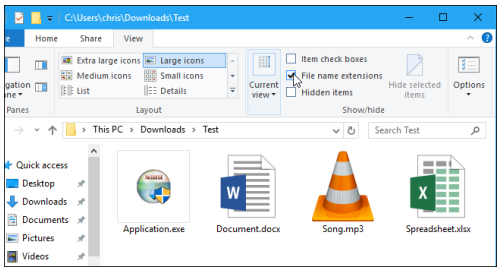
How to show File Extensions in Windows 11



Windows 11 changed the user interface for File Explorer quite a bit between Windows 10 and 11, but the option to show file extensions is still readily accessible. Click the "View" tab along the top of the File Explorer window. Mouse over "Show" at the bottom of the drop-down menu, and then click "File Name Extensions" in the sub-menu.

File extensions will then be visible for all files in all folders.

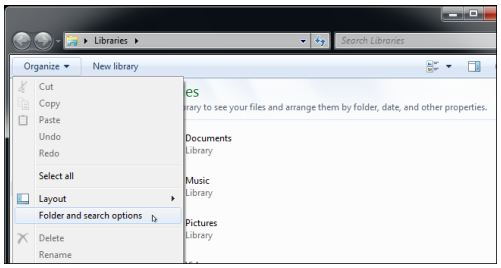
How to Show File Extensions in Windows 10 and 8



This option is easily accessible in File Explorer on Windows 10, and it's in the same place on Windows 8.

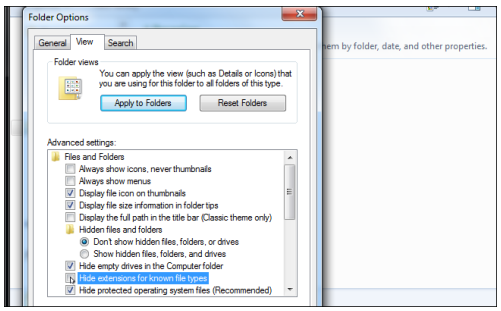
Click the "View" tab on the ribbon. Activate the "File name extensions" box in the Show/hide section to toggle file extensions on or off. File Explorer will remember this setting until you disable it in the future.

How to Show File Extensions in Windows 7



If you're still using Windows 7 (you shouldn't be) this option is a little more hidden as it's buried in the Folder Options window.

Click the "Organize" button on Windows Explorer's toolbar and select "Folder and search options" to open it.



Click the "View" tab at the top of the Folder Options window. Disable the "Hide extensions for known file types" checkbox under Advanced settings. Click "OK" to change your settings.

(This options window is also accessible on Windows 8, 10, and 11 — just click the "Options" button on the View toolbar. But it's faster to quickly toggle file extensions on or off via the ribbon.)

You can also do it via the Control Panel on any version of Windows. Head to Control Panel, in the **View By**: section, select Large Icons, then Select **File History**, then **View**, then unclick "*Hide extensions for known file types.*"

At age 20, we worry about what others think of us…
At age 40, we don't care what they think of us…
At age 60, we discover they haven't been thinking of us at all.

Picture in Picture.

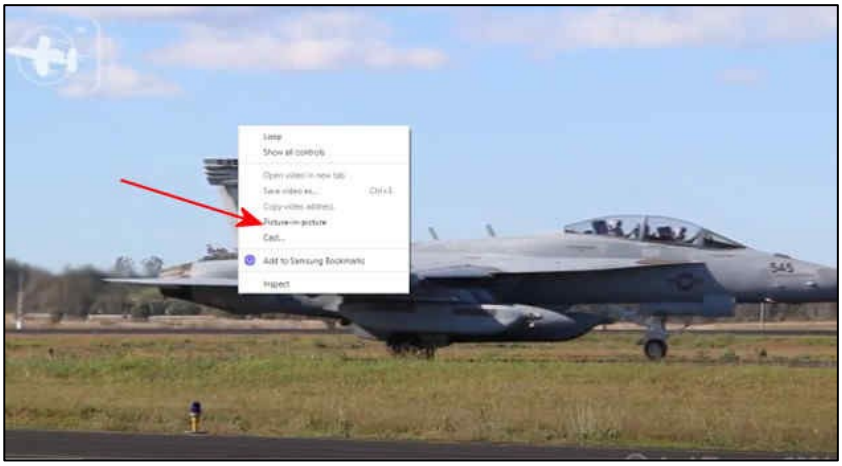
With picture-in-picture mode, you can shrink down your favourite (online) video and have it playing up on the top right edge of your screen (or anywhere really) while you continue working.

It's a very handy little trick and easy to set up though you will need to be using one of the popular web browsers like Chrome, Firefox or Edge. If, for instance you've got Kayo Sports on your computer, you can watch the footy or cricket while you work, or you can bring up a video on YouTube and watch that while you work. Here's how!

How to use Picture-in-Picture mode in Google Chrome and Microsoft Edge.

Open Chrome or Edge and open the site where your video is located. Start playing the video then right-click on the video and you will see a black menu. Do not select any option from this menu.

Right-click on the video again (outside of the black menu area) and you will see a new menu. From this menu, select "Picture in Picture."



And immediately, Chrome or Edge will detach your video and turn it into a floating window on your screen. You'll probably find it down the bottom right of your screen. You can grab it with your mouse, resize it and move it to anywhere on your screen.

When you're finished with it, hover your mouse over it and click the X top right of the video.

How to Use Picture-in-Picture mode in Mozilla Firefox.

Firefox makes it a bit easier, open the site where your video is located and start to play the video

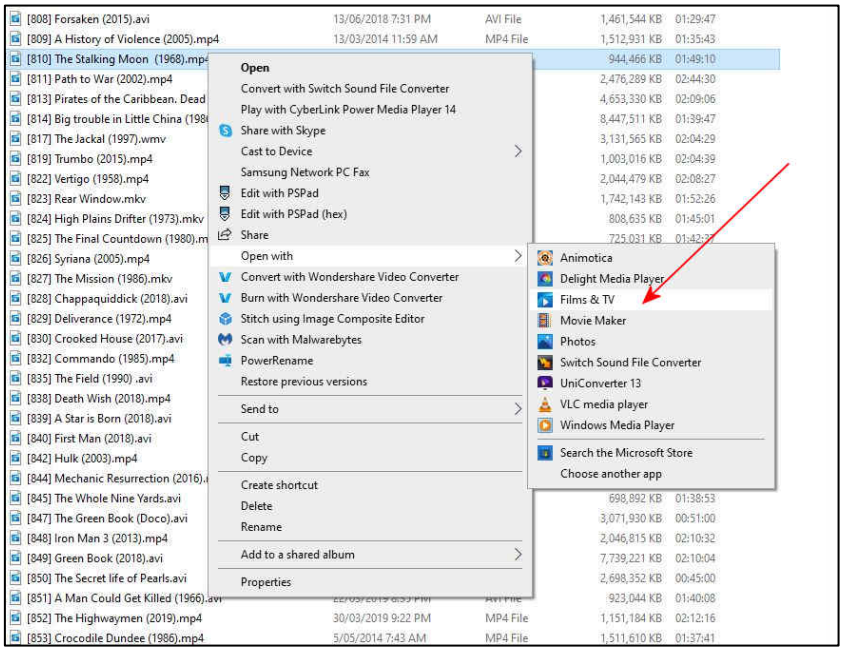
Hover your mouse anywhere on the video and you will see a square icon with an arrow in it pointing to the bottom-right corner. Click this icon and the picture-in-picture mode is activated.

You can turn it off the same way as above.

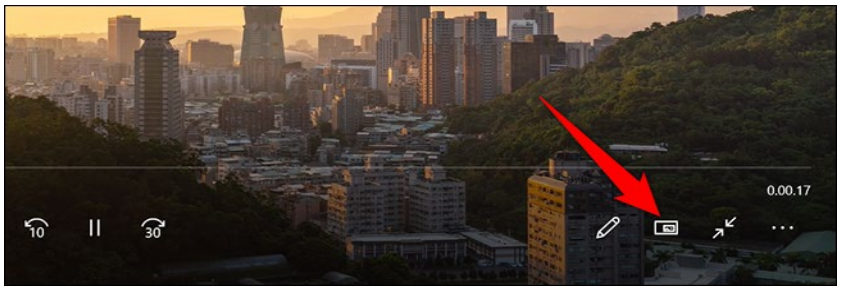
The above procedure may not work for all sites out there, Vimeo is one which will not work.

Off-line videos.

You can also watch a video stored on your computer or on a memory stick in the Picture-in-Picture mode too, here's how:



When the movie starts to play, down the bottom right hand corner of the video, click the small "Play in Mini View" icon.



This detaches your video and adds it as a floating window to the top-right corner of your screen.

Once again you can resize it and move it anywhere you want and when you're finished watching it, hover your mouse over the video and click the X at the top right.

Stop Putting Your Phone in Rice.

How-To Geek

For nearly as long as smartphones have existed, people have been putting them in rice after dropping them in water. This often-repeated “trick” to save a water-logged phone has gone too far. It doesn’t work!

Where did it come from?

The rice trick has been around forever and there’s probably a good chance you’ve done it yourself. Where did this common advice originate from? That’s an interesting question.

One of the first high-profile examples of the rice “trick” being recommended dates back to a Lifehacker post from June 2007. The claim was that dry rice “sucks up the surrounding moisture.” That same line of reasoning has been repeated ever since. The trick certainly predated smartphones, but it really caught on as more people began carrying around expensive, fragile devices that don’t play nice with water. People wanted to know what to do when they dropped their phone in water and the rice trick filled that need.

Why It Doesn’t Work

The harsh truth about putting a wet phone in rice is — it does absolutely nothing. Rice does not have magical moisture-wicking powers. You might as well just put the phone in a completely empty bowl. Rice does have some ability to absorb water from wet things, but it’s very weak. But that’s not the real problem, even a strong desiccant such as silica gel can’t get at the most damaging liquid, which is on the inside of the phone.

Sometimes, if the water didn’t penetrate the phone too much, leaving it powered off and giving it time to dry out will save it. People end up thinking it was the rice that did something when in reality it was simply leaving the phone alone for a while that did the trick.

To make matters worse, rice can actually accentuate the water damage in some cases. The fine rice "dust" can get into the ports and mix with the water to create a paste-like substance that's harder to remove.

How to Save a Wet Phone

The key to saving a wet phone is not necessarily to just wait for it to dry. That may work if you're lucky, but it's much more effective to actually remove as much water as possible as quickly as possible. Simply allowing it to dry will leave behind all the conductive stuff in the water. If your phone has been submerged in water, the immediate first step is to power it off. Don't try to power it on if the water turned it off. Then you should remove anything that can be removed. This includes cases, the SIM card tray, microSD card tray, and the battery (if it's even removable).

Next, you can go the low-tech route and use a fan or compressed air to blow the water out of the ports, however, that won't do anything for water that's inside the phone. To remove that water yourself, you'll need to open it up. From there, you can scrub it with 90%+ isopropyl alcohol or set it in front of a fan.

Leave the rice for dinner.

Basic Computer Security:
How to protect yourself from viruses, hackers and thieves

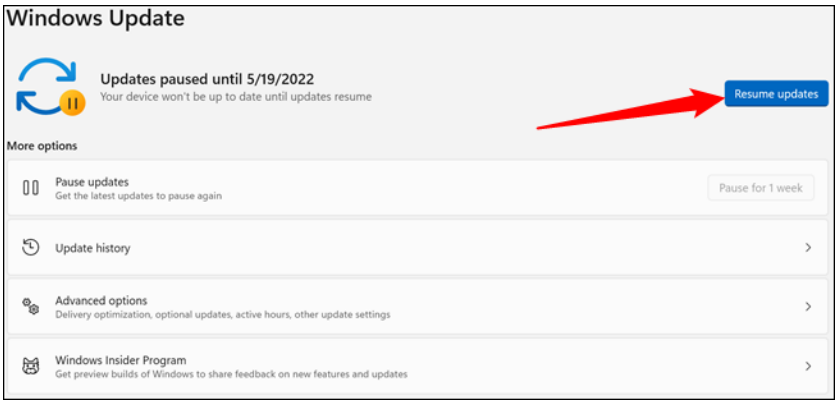
People often think of computer security as something technical and complicated and when you get into the nitty-gritty, it can be — but the most important stuff is actually very simple. Here are the basic, important things you should do to make yourself safer online.

Don't delay automatic updates

All the software applications we use every day are likely riddled with security issues. These security issues are constantly being found, whether we're talking about Windows, Microsoft Edge, Mozilla Firefox, Google Chrome, Adobe's PDF Reader, Microsoft Office — the list goes on and on.

These days, a lot of operating systems and programs come with automatic updates to close these security holes. No longer do you need to click a button or download a file to update your software; it'll update itself in the background without any input from you.

Some people like to turn this off for one reason or another. Others will delay it for weeks. Maybe you don't like that Windows restarts after installing an update, or maybe you just don't like change. But from a security perspective, you should always leave automatic updates on.



If you have turned off automatic updates previously, for any of your software programs, we suggest you turn them on right now.

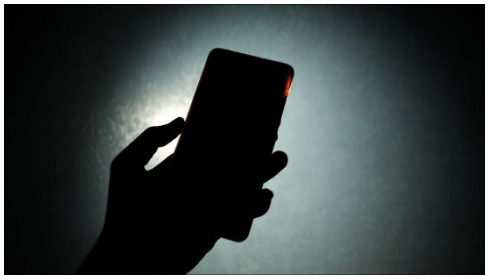
Keeping your computer up-to-date is the number one way to keep it safe against online threats. Microsoft provides updates for Windows and associated Microsoft products (Defender, Office, etc) on the second Tuesday of each month. Apple doesn't have a regimented schedule, but they also regularly provide updates. These updates not only fix bugs, but they patch security holes, so the only way to protect yourself against the latest known vulnerabilities is by updating. Malicious attackers are always looking for unpatched systems they can attack and automatic updates keeps you off the list of low hanging fruit.

Use Antivirus and Anti-Malware

It seems like every couple of years an article will come out saying one antivirus is the absolute best. Three more will follow saying three others outperformed the first. On top of these, some security expert will write an article saying antivirus is no longer relevant and you're dumb if you use it.

Let's set the record straight: you should be running antivirus, even if you're careful on the web. Which one? It's up to you, though when it comes to free, simple, and good, there's nothing wrong with using Microsoft Defender. It's built into Windows, it updates automatically with the Windows Update utility, it has a minimal impact on performance and it's free. To be effective, an antivirus application need to integrate with the operating system on a very deep level. Who better to know the internals of Windows than the people who built it? Plus, it won't try to sell you other products or inject other features you don't need, like some antivirus programs do.

Stop using Flashlight Apps.



Flashlight apps were once a clever tool inspired by everyone having a smart phone in their pocket. Those days are long gone, though. You shouldn't be using flashlight apps anymore. Here's why and what you should use instead.

It might be hard to believe, but camera flashes haven't always been included on smartphones. Apple didn't add an

LED flash until the iPhone 4 in 2010. Even after it became more common for phones to include flash, iOS and Android didn't have built-in "flashlights" for a while.

What Is a Flashlight App?
There are two distinct types of flashlight apps. The first type existed primarily before phones included a flash next to the camera lens. These apps would simply crank up the display brightness and show a blank white screen. It was a surprisingly effective way to get some light in a dark space.

The second type of flashlight app uses the flash on the back of the phone. They simply turn the flash on or off. This is an even better way to illuminate a dark space. While both types of flashlight apps technically perform the function they're advertising, there are some major concerns you may not know about.

The Problem with Flashlight Apps

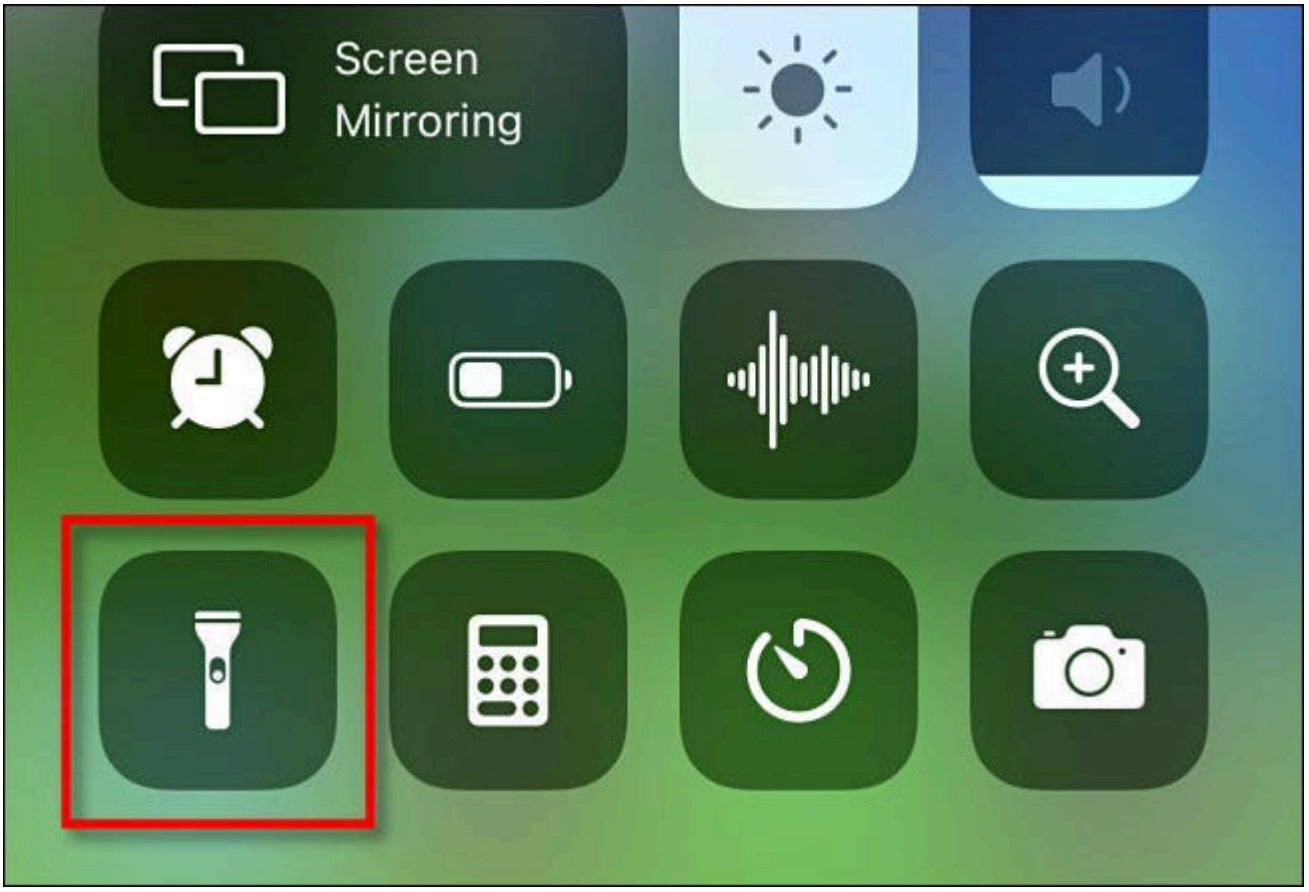
A flashlight app is designed to do one thing—provide light. Some have extra features like strobe lights and different colours to choose from, but at the core, these are very simple apps. That is precisely what makes them easy to not think twice about. The reality is many of these flashlight apps have been found to abuse unnecessary permissions. It's been a bigger problem on Android, but there have been some malicious iPhone flashlight apps too.

Back in 2019, Avast looked at around 1,000 flashlight apps found on the Google Play Store. Over a quarter of those apps were requesting between 50 to 77 permissions. These were things like recording audio and reading contacts, which are certainly not needed by a flashlight.

M

The scary thing is several of these apps had over one million downloads. Who would suspect such behaviour from an app that is supposed to be so simple? Thankfully, both the iPhone and Android now have got much better permissions controls.

What to Use Instead



Thankfully, it's no longer necessary to use any type of flashlight app. Android devices and iPhones now have built-in toggles to turn on the flash. There's nothing to install or worry about permissions being abused.

On the iPhone, you'll find the flashlight toggle on the lock screen and Control Centre for quick access. You can even adjust the brightness. With the Shortcuts feature, you can even launch the flashlight by tapping the back of the iPhone.

Over on Android, the flashlight (torch) can be found in the Quick Settings panel. Android phones all have slightly different interfaces, but to open the torch on a Samsung Galaxy device, you swipe down from the top of the home screen. This unveils a menu of shortcut icons, in which you should find the torch. You can add an icon to your home screen to tun the "torch" on if you like, here's how:

You do this with a very basic app from the Google Play Store called Flashlight Widget by David Medenjak. Why this app? After all, there are dozens of different torch/flashlight apps in the Google Play Store that promise the same thing, however, this one doesn't ask for any unnecessary permissions, so it isn't a front to harvest data from your phone.

N

When you install this tiny app, you'll be presented with a screen that asks if you want to Add to Home screen. Tap Add and a small power button icon will appear somewhere on your home screens. You can drag and drop the icon to somewhere convenient.

Smartphones have improved a lot over the years. Many problems that were solved by third-party apps don't exist anymore. Flashlight apps are a relic from days gone by. Let's leave them there.

Oh, and if your phone's flash doesn't cut it, real torches still exist and you can get excellent small ones from $2.00 shops everywhere.

O

This page left blank.