

Click to prove
you're human



Conversion No software to download. Just select your file, pick a format to convert to and away you go. Experience We have been successfully converting files since 2006, with millions of happy customers. Support Got a file you can't convert? Just email us and we'll ask our dedicated engineers to take a look for you. Speed We aim to complete all our conversions in under 10 minutes. Formats We support 1200+ file formats. Hackers and malware developers are always changing their tactics to try to stay one step ahead of everyone else. Consequently, no file format can be considered 100% safe. If it isn't dangerous now, it may be tomorrow or next month. A PDF virus is just one example. In this article, we'll show you how a PDF can contain a virus and what to do if you think you've accidentally clicked on one. Can PDFs be malicious? The short answer is yes. Just like a Microsoft Word file, a PDF can be used to conceal and transmit malware by means of an email attachment or a download link on a website. What makes PDF files such an effective tool for hackers is that they are used for so many applications invoices, contracts, bills, and various other documents used every day for work and home life. In other words, if you're already getting legitimate PDFs from trusted people like your boss, you may instinctively open a malware-infected PDF file named paisyJan 2025 without thinking about it. Stay on top of cyber threats Sorry, this email doesn't look right. Could you double-check it? We've sent you a confirmation email, please take a look. Yes, a PDF file can contain a virus. There are 2 scenarios in which this is likely to occur. No software program is immune to security vulnerabilities. If someone who wants to spread a PDF virus finds a vulnerability in Adobe Acrobat to help them do it, then it's a walk in the park. Many users have Adobe Acrobat installed on their computers. But how many of them fail to keep the program updated with the latest security patches? Macey book giving users advice on how to bypass Adobe installer security. Once the PDF file has been opened, embedded code such as JavaScript will start working. This could be used to trigger a malware download to your device, such as spyware to steal your data or a remote access trojan to corrupt files and damage your machine. You could also be tricked into downloading a fake Adobe Acrobat update or installer file. So, can opening a PDF give you a virus? And how can you tell if a PDF contains malware? Here are some signs that should make you stop and think and you recall that you don't know and trust? Or was it a complete stranger? You should not open anything from people you don't know. Even if the file came from someone you do know, like your boss, you should still check with them first. Which sounds more credible you? Invoice2025.pdf - ZHG3L4-1FG.pdf If a file has a crazy name to it, it's more likely to be malware, and thus, it shouldnt be opened. Legitimate PDFs go to have a proper name. Before you pull emails out of your spam folder, consider what they might be there. Other users may have flagged the sender as spreading spam, or your email service may have scanned the PDF attachment and determined it to be suspicious. Hackers and virus spreaders want you to act immediately on impulse. For them, the less time you have to think about it, the better. Therefore, if you get an email message urging you to open a PDF file immediately, stop. Why is it so urgent that you need to open it now? If someone sends you a PDF file, the usual modus operandi is to also send an accompanying message. This could be a simple request, such as, Please review and return at your earliest convenience, or a more detailed explanation of what the file is all about. If the PDF comes in a blank email, dont open it. If you know the recipient, ask for an explanation about the file. If it comes from a stranger, delete it. The PDF, in this scenario, is essentially a malware delivery system. The attacker sending the file to you needs to get you to take action to load malware on your system. This is usually done by getting you to open the file, which triggers embedded code. If you get a pop-up box asking you to download an update, a new version of Adobe Acrobat, or any add-ons, dont do it. Scan the file immediately for signs of malware. To check if a PDF has a virus, we recommend using a tool like CleanMyMac, powered by Moonlock Engine. Heres how to use it. You first need to select Configure Scan and select all the available options. Make sure the Scan mode is set to Deep Scan to ensure that your Mac/Book is thoroughly checked. Also, be sure to enable the Malware monitor and the option to look for threats in the background. This turns CleanMyMac into a 24/7 malware detector and bodyguard that will warn you the moment malware is found. Click the Scan button, and CleanMyMac will start scanning your Mac for malware, including any infected PDFs. You can instruct the scan, but its automatic. As a lightweight program, it does its work very quickly. While there are potential virus problems, theres never any time to waste. When the scan is finished, you'll see a list of all the malware CleanMyMac has uncovered. Select them all, and they will be removed from your device. So, youve accidentally opened a PDF file that likely contains a virus. What now? Apart from immediately deleting the file, Malware requires an internet connection to connect to the server to reestablish an internet connection to transfer your data. The very first thing you need to do is cut that connection. Next, run CleanMyMac, as detailed in the last section. Get it to find all malware on your device so it can be destroyed immediately. Mac and macOS are trademarks of Apple Inc. Now check for system updates on your Mac by going to the Apple menu > System Settings > General > Software Update. Immediately install any available patches and restart your computer. Another option, albeit an extreme one, is to wipe and completely reset your Mac to factory settings. Modern Macs with M-series chips make wiping and resetting a very fast and easy process. Just be sure you have a backup of all your files. Once your computer is back on, its time to take some precautionary measures. Identify your most important and sensitive accounts and change the passwords. This should include: Email Social media Online banking Work accounts (such as Slack, Microsoft Teams, and your company intranet) Also, enable 2-factor authentication if it isnt already turned on. In general, you should monitor all your important accounts more closely for any unusual activity for a while. Once the malware is gone, the last thing you want is a repeat performance. Here are some golden rules to help you avoid any malicious PDFs in the future. Frankly, this applies to all download links and files. If you dont know the sender, dont open it. And even if you do know the sender, nobody is going to complain if youre cautious and double-check that the file is really from them. PDFs have clickable links inside them, which can be convenient. But they can also hide nasty grimoires like malware. In general, try to avoid clicking embedded links inside PDF files. But if you have to, mouse over the link first to see where it leads. No legitimate PDF is going to ask you for your phone number, social security number, passwords, and so forth. If you get questions like that, close and delete the file. If youre using a Mac, consider uninstalling and not using Adobe Acrobat. A safer option would be to use the Preview app in Finder. The advantage here is that you wont be susceptible to any Adobe Acrobat vulnerabilities. Plus, if you get a pop-up box telling you that Adobe Acrobat is corrupted and you dont have the software in the first place, thats a clear red flag. Last of all, the Preview app can be considered safe because all updates come directly from Apples macOS updates. Stay on top of cyber threats Sorry, this email doesnt look right. Could you double-check it? We've sent you a confirmation email, please take a look. PDF viruses are just one of many tactics that malware developers and hackers use to try to stay one step ahead of cybersecurity experts like the team at Moonlock. Attackers who embed viruses inside files such as PDFs hope to ensnare as many victims as possible before antivirus software can catch them. Fortunately, by employing some common sense techniques, you can avoid downloading these viruses, denying the criminals another victim. This is an independent publication, and it has not been authorized, sponsored, or otherwise approved by Apple Inc. Mac and macOS are trademarks of Apple Inc. Adobe Acrobat is a trademark of Adobe Systems Incorporated. Tyler Cross Updated on: May 17, 2025 Former Senior Writer Fact-checked by Kate Davidson Short on time? Heres how to quickly check if a PDF file is malicious: Install reliable antivirus software. To start, you'll need a quality antivirus program (like Norton). Once youve found an antivirus that works for you, install it on your device like a regular app or program.Run a malware scan. Once the antivirus is installed, scan the file you suspect has malware, or the whole system if the infection has spread. Let the scanner do its job and dont attempt to tamper with files during the scan.Remove the malware from your device. After the scan is done, it will quarantine and remove the infected files for you. Double-check to make sure its isnt removing any files you want to keep, but in general, its best to get rid of any file it flags as a threat. Uninstall any applications or extensions that gave you the malware.Double-check by restarting and running a full scan. After removing the malware, restart your computer and run a full scan. If you have a reliable malware scanner thats from a reputable company, ideally, go with a premium product like Norton or BitDefender, both of which have engines powerful enough to detect and remove 100% of the malware hidden in PDF files. Once youve purchased your antivirus, install it on your PC or phone like any other application and log into your account. If youre on a computer, simply download the program from the website and let the installation wizard do the rest. If youre on a mobile device, download it from the App Store or Google Play Store. Save 58% on Norton 360 Deluxe!Get Norton 360 Deluxe for only 44.52!Step 2. Run a Malware ScanOnce youve installed your antivirus, scan the PDFs you believe are infected. Every premium antivirus on my list lets you run a quick scan, a full scan, or custom scans of individual files. Choose the third option, then click File Scan and navigate to the files you want to be checked. Finally, click Scan. If the PDF has already been opened and you suspect your whole device is infected, run a full scan by clicking the Full Scan option included in all my top antiviruses. This may take upwards of an hour, but each file on your device will be meticulously checked for malware. If the malware is particularly threatening and has bricked your device, restart your computer or phone in Safe Mode (each platform has a unique way of doing this) and perform steps 2-4.Step 3. Remove the Malware From Your DeviceOnce the scan is complete, you'll be shown a report detailing any malware the antivirus found. At this point, the antivirus will quarantine the infected PDF (or other files) and give you the option to remove it. While you should double-check to make sure that any files you want arent being deleted, its usually best to let the antivirus do its job and remove suspicious files. Additionally, you should uninstall any applications or software installed by the malware. As an example, if youre on Windows 11, click on the Start button and navigate to the Control Panel. Click on Uninstall a Program, and remove any malicious apps.Step 4. Double-Check by Restarting and Running a Full ScanOnce youve removed the bad PDF file, restart your device and run one more full scan. Some infections can be particularly nasty or may have spread to other parts of your device. By restarting your device and running one last full scan, you can be certain the malware is gone. Can Free Antivirus Software Detect & Remove Malicious PDFs?Some can, but frankly, a free antivirus will never be as good as a premium one. While there are free antiviruses that I like, they usually come with quite a few drawbacks. Free antiviruses from unreliable sources are often scams or carry hidden malware, and even the best free antiviruses are missing a lot of features you need to be completely protected.A free antivirus may be able to wipe out most malware hidden in PDFs, but premium antiviruses like Nortonand BitDefenderinclude features like real-time protection to stop zero-day threats, anti-phishing protection, firewalls to protect your network, and VPNs to shield your identity.How Do Infected PDF Files Get Onto Your System?Phishing scams. This common method involves a threat actor sending an email that entices the recipient into opening an attached PDF. Once someone opens the infected PDF, it can infect their device almost immediately.Downloaded from the internet. Another very common method is simply downloading a malicious PDF file online. Often, scammers will present attractive-looking free PDFs (like popular books) to convince people to download them.Shared through networks. Once one device on a network gets infected, particularly savvy threat actors can spread that malware through every device on the network, potentially crippling a whole household or business via a single PDF.Inserted through shared media. Infected PDF files can also be spread through USB drives or other removable media. If an infected PDF is on a drive, and the drive is inserted into a new system, the infection can spread if the PDF is opened.How Can a PDF Be Infected?There are numerous ways that hackers can infect PDF files, all of them dangerous. Here are a few of the most common ways cybercriminals insert malware into PDFs.Hidden malware. Its relatively easy to store encrypted or embedded objects (like media players or flash files) in a PDF that can slip past basic antivirus software. Usually, things like free PDF books or magazines or phishing scams carry this type of threat. As soon as you open the file, it deploys. Premium antiviruses like the ones on this list tend to be better at detecting this sort of malware.Malicious JavaScript code. Since most websites employ some kind of JavaScript, hackers can infect PDFs with questionable links of JavaScript. These scripts can be used for all sorts of malicious purposes. For this reason, you should always be very wary about downloading PDFs from unknown websites.Abuse of System Commands. Once you open the PDF, it could use your System Commands to launch more malware. Essentially, hackers can open your Command window and use it to execute commands to initiate the malware.What Can Happen if You Have a Malicious PDF on Your Device?Leaving a malicious PDF file on your device can have far-reaching consequences. Your data could be exfiltrated, encrypted, and ransomed right under your nose. The malware could infect all of your files, destroying your device. You could be allowing threat actors to make subtle changes to your database, you could be used to mine crypto for them, and so much more.There are simply dozens of ways that leaving a malicious file on your PC could go wrong so its imperative that you get rid of the file immediately. Use an antivirus program to scan the file (and your whole device), then quarantine or remove the malware. Chances are the PDF may have to go as well, and if thats the case, you should prioritize your safety over the PDF file.Best Ways to Prevent Virus-Infected PDFs From Getting Onto Your SystemChoose a trusted PDF reader and keep it up-to-date. Use reliable PDF reading software products like Adobe Acrobat Reader, Foxit Reader, and Nitro Reader they have great reputations and prioritize users security. Conversely, using untrustedworthy programs leaves you at high risk of infection.Install a trustworthy antivirus program. Even if you do everything right, you can still get malware from a faulty PDF file. Thats why you need an antivirus malware scanner to detect and remove it for you, with real-time protection to stop it from happening in the future.Be wary of unknown websites, links, and sources. Good antiviruses will include web protection that prevents you from visiting malicious websites or downloading bad files, but you should still do your best to always avoid removing malware. antiviruses like Norton and BitDefender also provide you with real-time protection against phishing viruses. Plus, they offer a host of other cybersecurity tools like a VPN, web protection, dark web monitoring, PC optimization tools, a network firewall to prevent intrusions, and a lot more.My favorite antivirus to remove malware from a PDF is Norton. Norton has a flawless malware scanner, which efficiently detected and removed 100% of every type of malware I tested, including viruses, trojans, ransomware, and more. It also has excellent web protection, ensuring you dont stumble across a malware-ridden PDF file online.BitDefender is a close second. Its cloud-based malware scanner doesnt tax your system at all, and its malware detection rating is just as good as Nortons. While I think Norton is just slightly better (it has the best dark web monitoring on the market, for example), BitDefender is also a worthwhile investment.Dont fret antiviruses will remove malware thats already infecting your computer. If you downloaded an infected PDF that already injected itself into your device or network, simply run an antivirus like Norton (or any of our top picks) and allow it to quarantine and remove every type of malware it finds. If your data has already been encrypted and stolen by ransomware, it may be trickier. Decrypting data often requires a decryption key, which may not always be available. While you can usually recover your data and beat malware easily, its incredibly important to have an antivirus with real-time protection, so your data is never encrypted and stolen in the first place.Best Antiviruses for Detecting & Removing Malicious PDFs Files Final Score: Share copy and redistribute the material in any medium or format for any purpose, even commercially. Adapt remix, transform, and build upon the material for any purpose, even commercially. The licensor cannot revoke these freedoms as long as you follow the license terms. Attribution You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. ShareAlike If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. No additional restrictions You may not apply legal terms or technological measures that legally restrict others from doing anything with the licensed material, provided you also do not impose any additional restrictions on the recipients ability to exercise the licensed rights. Non-Commercial You may not charge others for access to your content. Public Domain Mark If you are redistributing or otherwise making available publicly, you may omit this notice if you wish, provided you retain all other rights such as publicity, privacy, or moral rights may limit how you use the material. How can financial brands set themselves apart through visual storytelling? Our experts explainHow Learn MoreThe Motorsport Images Collections captures events from 1895 to todays most recentcoverage.Discover The CollectionCurated, compelling, and worth your time. Explore our latest gallery of EditorsPicks.Browse Editors' FavoritesHow can financial brands set themselves apart through visual storytelling? Our experts explainHow Learn MoreThe Motorsport Images Collections captures events from 1895 to todays most recentcoverage.Discover The CollectionCurated, compelling, and worth your time. Explore our latest gallery of EditorsPicks.Browse Editors' Favorites Can a PDF have a virus? Yes. PDFs can contain harmful security threats such as viruses, malware, and trojans. Like many other file types, PDFs can be used to compromise our data and sensitive information if you do not take the proper precautions. As PDFs are an essential part of our professional and personal lives, and one of the most popular file formats, its crucial you know the potential threats and how to combat them.This post will teach you about some of the biggest security threats to your files and the measures you can take to protect yourself.When it comes to PDFs, cybercriminals can exploit elements within the file format to embed harmful code or links, potentially compromising our devices and sensitive data. Cybercriminals can use clever techniques like embedding malicious JavaScript, crafting deceptive hyperlinks, or concealing harmful attachments. In this section, we look at the potential security risks associated with PDF files so that you can better avoid viruses, worms, and other nasties within PDFs that get access to your system. Once a PDF is opened, the malware can automatically install itself or prompt you to click a link or download an attachment that contains the infection. These types of attacks are known as PDF-based phishing. The hackers create PDFs that look like legitimate files from a trusted source to trick people into opening them. Some signs a PDF could contain malware: Its unsolicited or from an unknown sender. Delete these immediately without opening. It has a strange filename or subject line. Legitimate companies dont use odd characters or subjects to get you to open files. It urges you to enable macros or click links when opened. Never enable macros or click links in unsolicited PDFs. It was scanned or faxed. These are easy to manipulate and infect with malware. It loads slowly or the file size seems too small or large. Malware-infected PDFs often behave strangely. The bottom line is be wary of any unsolicited PDF, even if it looks legitimate. Its always better safe than sorry when it comes to your digital security. If you want to know are pdf files safe or can downloading a pdf be dangerous then the answer is while PDF files themselves cant contain viruses, that doesnt mean theyre 100% safe to download and open. There are a few risks to be aware of when downloading PDF books, files and documents from unknown or untrusted sources. Hackers often disguise malware as PDF files to trick people into downloading and opening them. The PDF is just a front, and the malicious software is embedded inside. Once opened, it can install viruses, ransomware or spyware on your computer. Phishing emails frequently come with PDF attachments to lure victims into clicking. The PDF may appear legitimate but actually contains links or downloads that infect your PC when opened. Not all PDF risks are malicious. Some files are simply corrupted or have been manipulated in a way that could damage your system. Its best to only download PDFs from trusted sources you know and verify. PDFDrive is a popular website for downloading free PDF files on almost any topic. While the majority of files on PDFDrive are secure, some risks do exist. Its possible for malicious actors to upload infected files to the site, though PDFDrive does have measures in place to prevent this. To stay safe when using PDFDrive: Only download PDFs from trusted, verified uploaders. Never click suspicious links or download attachments inside PDFs. Scan any downloaded PDFs with up-to-date antivirus software before opening. Be wary of PDFs that ask for sensitive info like passwords or credit card numbers. Legit PDFs wont ask for this. If something seems off about a PDF, its best to delete it. Your security is more important. Determine if a PDF file has been infected with pdf malware, there are a few signs to look for. First, check if the file size seems excessively large for the content. Malware attachments are often much bigger than normal files. Second, look closely at the senders email address and name. Does it match the actual sender, or does it look spoofed? Spoofed addresses are a common tactic used by hackers to spread infected files. Third, be wary of urgent or alarming language or requests that seem out of the ordinary. Legitimate companies dont ask you to click links or download attachments from unsolicited emails. Finally, check if the PDF file behaves strangely when you try to open it. It may not open at all, or you may get error messages. It could also try to automatically download other files or execute commands, which is a major red flag. If anything seems off about the PDF file or the email it came with, its best to delete it immediately. Its always better safe than sorry when it comes to potentially infected files. When opening and downloading free PDFs, take these precautions: Only download PDFs from reputable sites like university libraries, research organizations or large companies. Avoid anything that seems sketchy. Check reviews and ratings of the site before downloading. See what other people say about its safety and legitimacy. Scan the PDF before opening. Use an antivirus program to check for any malware. Look for signs the PDF isnt what it claims to be. Strange file names, sizes that dont match the purported content, or lack of publisher info are red flags. If something seems off, dont download. Its not worth the risk. Your security and privacy are more valuable than any free book or document. The safest way to open PDFs is to take some basic precautions. Only download PDFs from trusted, verified sources. Never open attachments or click links from unknown or suspicious senders. Make sure you have reputable antivirus software installed and up-to-date. Run a quick scan of the PDF before opening to check for any malware. Opening PDFs in a sandboxed environment isolates them from the rest of your computer. Programs like Adobe Reader and Foxit Reader have built-in sandboxing features. Enable them in the security settings. Dont enable any interactive features like JavaScript or Flash in the PDF viewer unless absolutely necessary. Only enable them temporarily on a per-file basis. These features can potentially be exploited to distribute malware. Update Adobe Reader, Adobe Acrobat, and other PDF viewing software regularly to ensure you have the latest security patches installed. Outdated software is an easy target for malware and exploits. By taking these straightforward precautions, you can feel comfortable opening PDFs, knowing youve reduced the risks. Staying vigilant and using common sense judgment about the PDFs you choose to open will help keep your computer secure. The best antiviruses for protecting against PDF viruses and malware in 2024 include: It offers real-time scanning of PDFs and other files as you open them. It has a file lock feature to prevent unauthorized changes to PDFs. McAfee is a reputable name in cybersecurity and their software is affordable, user-friendly, and provides comprehensive protection. Real Also: How To Get Rid Of The McAfee Virus Popup It is a highly-rated antivirus that provides layered protection against PDF threats like embedded malware, malicious links, and fileless attacks. BitDefender uses behavioral detection to identify suspicious activity and block threats in real time. They frequently update their software to defend against the latest PDF risks. It is a popular antivirus solution that scans PDFs and other files for viruses, malware, ransomware and more. Kaspersky uses advanced heuristics and machine learning to detect brand new PDF threats. They offer malware removal and file recovery tools in case of infection. Kaspersky gets top ratings in independent tests for PDF security. AstrillVPN can help avoid downloading viruses in PDFs in a few ways: When using AstrillVPN, all of your internet traffic is encrypted and routed through a secure VPN tunnel. This makes it much harder for hackers to infect your device with malware, even if you download a malicious PDF file. The encryption acts as an extra layer of protection for your data. AstrillVPN gives you the ability to change your IP address and virtual location. By connecting to a server in a different country, you can mask your real IP address and make it harder for hackers to trace you back to your device. AstrillVPN also offers a DNS leak protection feature that helps prevent your DNS requests from being intercepted by malicious actors. AstrillVPN also offers a kill switch feature that automatically disconnects your device from the internet if the VPN connection drops, preventing you from hosting malware, phishing scams, and other threats. So if a hacker tries to trick you into downloading an infected PDF from one of these malicious sites, Astrill VPN can stop the connection before any damage is done. Using a VPN like Astrill is one of the best ways to strengthen your online security and reduce the risks of downloading PDFs with embedded viruses or other malware. By encrypting your internet connection, hiding your IP address, and blocking malicious websites, Astrill VPN makes you a harder target and helps keep your files and information safe. Q: Can I get infected by simply viewing a PDF file? Its unlikely, but possible. Opening a PDF file on your computer executes code that could contain malware. However, you would typically have to open an attachment or download a file for infection to occur. Just viewing a PDF on a website is less risky. Q: Can PDFs carry other threats besides viruses? Yes, PDFs can also contain:Malware like worms, trojans, and spyware designed to steal data or take control of your computer.Phishing links or attachments that trick you into entering login info or downloading malicious files.JavaScript code used to run exploits or install backdoors on your system. Q: What types of threats can be found in PDF files? The most common PDF threats are:Viruses that infect your system files or documents.Rootkits used to gain admin access to your computer.Ransomware that encrypts your files until a ransom is paid.Keyloggers recording your keystrokes to steal passwords and data. So while PDF files themselves cant contain viruses, they can still be used to spread malware if youre not careful. But dont freak out as long as you take some basic security precautions, your computer should be safe. By following these best practices, you can confidently open PDFs without worry. Knowledge is power, so now that you understand the truth about PDF security risks, you can stay safe online. Stay vigilant but dont be paranoid, youve got this! Thanks for your feedback! Updated on March 31, 2025. A virus is a type of malware, which is malicious software intended to infect your device and steal your private information. It can only infect when you interact with it, like when you open a PDF that contains a virus. Hackers hide viruses in PDFs by embedding them in malicious code within PDF files. Since PDFs are so widely used, hackers exploit them to compromise your privacy while going unnoticed. Continue reading to learn how PDFs can contain viruses, what happens when you open a virus-infected PDF and how you can stay protected against malicious PDFs. Viruses can live inside PDFs through hidden code, system commands and embedded objects. Many web browsers support JavaScript, a programming language that can be embedded in PDFs. Hackers use this to their advantage, hiding malicious code in JavaScript to exploit security vulnerabilities within a PDF. Just opening a compromised PDF can set off a domino effect, with the virus infecting other files and apps on your device. Hackers may even assume that you have antivirus software installed, so they may embed hidden objects in PDF files to go undetected and gain unauthorized access to your private information. Although not all viruses trigger an immediate infection by simply opening a PDF, some viruses are coded to activate as soon as you view the infected file. The risk of infection increases if the virus is hidden in an interactive element of the file. For example, you may receive a PDF in an unsolicited email, but malware may not impact your device unless you click on a specific link or image within the file. The consequences of opening a malicious PDF file depend on what a hacker wants with your information. Some hackers may want to infect your device with spyware to monitor your online activity and collect private information, potentially leading to fraud or identity theft. Other hackers may infect your device with ransomware to lock you out of your device until you pay a ransom. Regardless of a hackers motive, once you interact with a malicious element of a PDF, the virus will do whatever the hacker has programmed it to do whether thats stealing your data, gaining unauthorized access to your device or spreading malware to other systems. PDFs are used all the time, but they can also be a haven for malware if youre not careful. Heres how to protect your device from dangerous PDFs and avoid becoming a victim of cyber threats. Suspicious emails usually contain malicious attachments, like PDFs, designed to infect your device. These emails may be phishing attempts, where hackers impersonate trustworthy individuals or companies to steal your personal information. Signs to look out for when you receive a phishing email include unfamiliar senders, urgent language, grammatical errors or suspicious links. Antivirus software can detect and remove known viruses from your device, so always scan PDFs before opening them. Once you install antivirus software, you can scan individual PDFs or your entire device. The software compares your files to a database of known viruses, and it will automatically isolate and delete any detected viruses before they cause harm. Protect your information from hackers and viruses by using a secure PDF reader. Choose a reliable reader that has frequent updates to address new security vulnerabilities and fix bugs. Disable JavaScript plugins since those are used to hide malware. A trusted PDF reader will help prevent unauthorized access and protect your device from viruses even those hiding in PDF files. Keep your software updated to protect against viruses in PDFs. These updates fix security weaknesses, improve performance and include the addition of new features, helping to protect your device from viruses. Install the latest OS version to protect yourself from potential infections. If you receive a suspicious email with a PDF attachment, mark it as spam and report it. This helps your email provider recognize and block future phishing attempts from harming you and others. Just deleting the email wont stop the sender from sending you more, but marking it as spam teaches your provider how to filter similar cyber threats. Some suspicious emails are clearly spam, but dont let a PDF fool you into clicking on something that could infect your device with a virus. Even though not all PDF files containing viruses will infect your device just by viewing them, you should always be cautious by avoiding any emails with suspicious links or attachments, checking PDFs for viruses with antivirus software and marking phishing attempts as spam.

Can downloading pdfs be dangerous. Can pdf be harmful. Can pdf files be dangerous. Are pdfs dangerous. Can opening pdfs be dangerous. Can a pdf attachment be dangerous.