

Continue

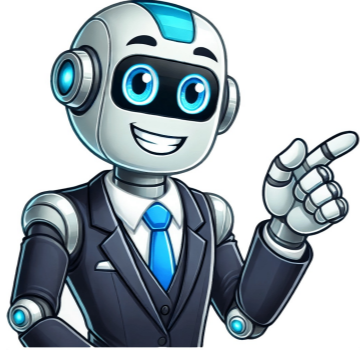


Image: Shutterstock.com / solarseven A lot of attention gets spent on the best paid antivirus suites, but free antivirus solutions are worth talking about, too. Not only is a solid option built into Windows, but the same antivirus engines that power paid third-party software power the gratis versions, too. So if you see a free alternative to a paid version you like, you can safely assume the antivirus protection level is similar—save for any specific malware types the free version doesn't cover. The difference is the number of features available to you. To create this list of the top free antivirus programs, we looked at the top mainstream antivirus suites for Windows and selected the ones that offer a free version, as not all of them do. Then we looked at how well these suites performed in third-party detection tests. We also made sure they weren't resource hogs, because software that slows down your PC is a pain in the rear, even when it's free. In the end, our selection came down to these top free antivirus suites. Avast One is a very highly rated antivirus program. With the free version of this suite you can run all the various virus scans. Most of the key Avast protections are also available, such as scanning new files added to your system, watching for malicious behavior from installed programs, a web browsing shield, and an email shield. Avast Free even allows you to inspect your network and see the devices currently connected to your home router. Avast Free uses a so-called smart scan to look for a variety of problems including browser threats, outdated apps, viruses and malware, and "Advanced issues" such as whether your webcam is protected from hijacking and the status of your firewall. However, the trick with those advanced issues is that to supposedly fix them, you need to start paying for the Avast One suite (about \$50 per year for new subscribers). What you don't get for free is phishing protection, the sandbox to separate suspicious files from your system, webcam shield, password protection, a sensitive data shield, identity protections, VPN, and PC utilities. It does, however, provide basic ransomware protection. As an alternative to Windows Security, Avast is surprisingly useful in its free version and is one of the most flexible options around. Bitdefender's free antivirus may have gotten a makeover, but its premise remains the same—a laser focus on guarding your PC from viruses and other malware, including web threats. You can run a quick scan or full scan, as well as create your own custom scans. VPN access is included as well, but free users are limited to just 200MB of bandwidth. And...that's it for features. Everything else is kept under lock and key until you upgrade to a paid subscription. No password managers, PC tools, or additional ransomware defenses. It's malware scanning and that's it. Well, almost it. Bitdefender's free edition includes anti-phishing safeguards—if you create a Bitdefender account to enable the app's full protection. What distinguishes Bitdefender is its high rating from independent security organizations, with some of the highest detection rates for malware whether you're online or off. So even though it's light on features, it's heavy on the most important quality you need in free antivirus. Avira Free includes antivirus protection, a basic password manager, file shredder, and a free VPN with an allowance of 500MB per month. It's not as full featured as Avira Prime, but it'll do for a free suite. The free version scans your PC, and offers real-time protection for your desktop. But it lacks protection from web threats and email threats, as well as additional ransomware protection for your device. It also lacks the improved PC cleanup feature for clearing out old files in the Pro version. Installation with Avira is easy, though it does prompt you to install its secure browser (completely optional), and automatically adds its Safe Shopping browser extension to already-installed browsers on your PC, like Microsoft Edge. Avira still uses more than one application for its features, with the most notable being Avira System Speed up for PC utilities and Avira Phantom VPN. If you want a free suite that splits its attention across a wider set of features, rather than concentrating on malware protection, this is the software to look at first. Finally, we come to Microsoft's built-in security solution. Once upon a time, we wouldn't even consider Windows Security (previously known as Windows Defender) for an article like this. Times have changed, however, and Windows Security is equaling the competition in terms of results from third-party testing houses. Windows Security is very good. There are third-party options that have better detection capabilities based on independent tests, but so long as you're not visiting sketchier places on the internet, you'll stay protected. Windows Security is active by default in Windows 10 and 11, and it works in the background ensuring you're protected from threats. Read our full Windows Security review As you can see, there are several capable free antivirus programs for you to choose from. Still, we feel it's important to point out what you don't get when you opt for a free solution. Email protection, for example, is typically a paid feature—and something that people who are extremely active in a desktop email program might care about. Also missing from the free suites are enhanced security features such as file protection (to ward off ransomware attacks), a sandboxed area for opening suspicious files, a sandboxed browser for shopping protection, an enhanced firewall, monitoring for malicious behavior from installed programs, webcam monitoring, and a password manager. Identity monitoring and other privacy services like a VPN usually require a paid subscription, too. If, however, you're only looking for basic antivirus protection that scans your PC and alerts you when there's a problem, then one of these suites will do the job without costing you a cent. 1. Maybe, but probably not. To ensure that there is no malware or other threats present, antivirus software scans files and programs on your computer. The longer the time frame between each scan, the more files they will need to check. These more intensive scans may have some noticeable effects on your computer speed. Therefore it's recommended that you do more frequent scans or even run them at night so it doesn't affect your computer usage. While antivirus software can have some impact on the speed of your computer, it's most likely not the only thing—or even the most prominent. Other factors such as unnecessary startup and background programs, insufficient RAM, or even undiagnosed malware can have more drastic effects on your computer speed than a simple antivirus scan. 2. Ideally, your antivirus software will quarantine and clean the infected files for you. However, this largely depends on which antivirus program you're using. In general, the antivirus will send a warning to you and try to quarantine the infected file in order to keep it from spreading. Once it has isolated the threat, the software will give you the option to remove the infection or delete the file altogether. 3. A full scan performs a comprehensive and thorough check of your whole system. It usually checks your system memory, startup programs, system backup, email databases, hard drives, and any removable storage drives. A quick scan only checks a few key areas including startup programs, system memory, and boot sectors. It may not detect all malware, but it can usually give you an idea if your computer has a virus. We recommend doing a full scan once per week ideally when you're not using your computer (such as late at night). A quick scan can be done anytime but it's usually only necessary if you notice suspicious activity on your PC. The Forbes Advisor Small Business team is committed to bringing you unbiased rankings and information with full editorial independence. We use product data, first-person testing, strategic methodologies and expert insights to inform all of our content to guide you in making the best decisions for your business journey. Our team analyzed 15 antivirus providers with 27 factors such as transparent pricing, ransomware protection, anti-phishing security, access to customer support and customer ratings to organize this list of the seven best free antivirus services. All ratings are determined solely by our editorial team. Learn More Learn More Yes, for Windows, Mac, Android and iOS Removal only, not prevention Learn More Yes, with Microsoft 365 subscription Think of antivirus software as a personal digital bodyguard. It's there to guard your computer around the clock, keeping an eye out for intruders that could ruin your day. These unwelcome guests are often known as malware—nasty stuff such as viruses, worms, trojans, ransomware and spyware. Each has its own sneaky methods and nasty intentions, but your digital bodyguard is trained to catch them in the act. Modern antivirus software goes beyond just bodyguard duties, acting more like a whole security team. It monitors your emails, filters out suspicious ones, keeps a vigilant eye on your internet browsing and blocks any malicious websites before they can do any harm. Some even have the skills to provide anti-phishing protection, helping you avoid online scams designed to steal your personal information. In the world of antivirus software, more features often mean better protection. It's free, so it must be a good deal, right? Well, not always. Yes, some free programs can give you basic protection, but they might not give you the full security coverage you need. Consider the fact that cyber threats are always evolving—the bad guys never sleep. Paid antivirus software typically offers regular updates and cutting-edge features, which help you keep pace with these ever-changing threats. Free antivirus software can also come with some unwanted extras. Annoying ads, a sluggish computer and even privacy issues can tag along. Certain no-cost programs have been discovered selling user data to outside parties, which is a serious privacy violation. And, let's not forget the most important thing—the level of protection offered by your chosen software. Free software can sometimes fall short when faced with complex cyberattacks. As cybercriminals get smarter, the software needs to outsmart them, and free versions might not have the muscle to do that. While free antivirus software can work for simple needs, a paid version may be the better option if you're a frequent internet user and value your privacy. Always do your research before choosing any antivirus software—your digital safety is worth it. The most important feature of any antivirus is protection from a wide range of threats. These include viruses, malware, ransomware, spyware and phishing. Of course, the best free antivirus software will be available for all of your device types, so you are protected whether you are using your Windows desktop or your iPhone. Additionally, it's also worth considering the price for premium antivirus plans in case you decide you want to further increase your security in the future. Those with affordable feature-rich plans will be your best bet to easily grow with. Threat Protection Features An antivirus software is like a fortress against cyber threats—the more features it has, the better it can defend your system. Different antivirus software may protect against different types of threats, but a comprehensive one should cover viruses, malware, ransomware, spyware and phishing attacks. The most crucial features to look for include: Real-time protection: This is like having a 24/7 security guard for your device. It continuously monitors and prevents potential threats from damaging your system. File scanning: Regular scanning of files and folders is a must-have feature, as it can detect and eliminate hidden threats. Browser protection: Given the internet's vast landscape, ensuring safe browsing is paramount. This feature warns of or blocks dangerous websites, links and downloads. Email protection: Since phishing attacks often come via email, this feature will screen your inbox for any suspicious activity. Threat Removal Features While protection is essential, equally important is the ability to remove threats that somehow bypass your defenses. Threat removal involves the antivirus software identifying, isolating and eliminating the threat from your device. Some advanced features to consider include: Automatic quarantine: This feature isolates the detected threat from the rest of your system to prevent it from causing damage until it's removed. Threat repair: Some software can fix any changes made by the malware, restoring your files or system settings back to their original state. Post-attack report: A detailed report following a threat removal provides insights into the attack and how it was dealt with, enhancing your awareness about your system's vulnerabilities. Performance Impact Antivirus software is a bit like a marathon runner—it needs to be robust, but also efficient so as not to slow down your system. Some antivirus software can consume significant system resources, leading to slower device performance. Look for software that promises lightweight operations or has a "gaming mode" to minimize disruptions during intensive tasks. Upgradability and Add-ons The ability to scale up your security with your needs is a handy feature. Many free antivirus solutions offer premium upgrades that provide more comprehensive protection. Here are a few popular add-ons: Password managers: This tool generates, stores and auto-fills complex passwords across your accounts, enhancing your online security. VPNs: A virtual private network encrypts your internet connection, preventing hackers from intercepting your data. System performance tools: These tools optimize your device's performance by clearing unnecessary files and streamlining processes. Wi-Fi monitoring: This feature checks your Wi-Fi network for vulnerabilities that hackers could exploit. Antivirus software is a critical layer of security for your digital life. The choice between free and paid options depends heavily on your individual needs and concerns. Here are some points to consider. When To Consider Free Antivirus Software Free antivirus software can be an excellent choice for users with basic security needs. If you primarily use your device for light activities such as browsing, streaming content or checking emails, free software might provide adequate protection. If you're not protecting your devices now, a free antivirus tool is a necessary step to take before investing in paid offers. Free antivirus allows you to understand how such software works and determine your specific needs without making an upfront investment. When To Consider Paid Antivirus Software If you're a heavy internet user, regularly access online banking, store sensitive information on your device or work from home, consider investing in a paid antivirus solution. These offer more comprehensive protection, and typically include additional features such as: Advanced threat protection: Paid antivirus software usually offers superior protection against various threats, including zero-day exploits and ransomware. Multidevice coverage: If you own multiple devices or have a family that needs protection, paid plans often allow you to cover multiple devices with a single subscription. Customer support: Many paid options include 24/7 customer support, which can be crucial if you encounter complex security issues. Additional features: Paid antivirus often includes valuable extra features such as parental controls, VPNs, password managers and system optimization tools. Free antivirus software is sufficient for minimal internet use and those on a tight budget. However, for comprehensive protection, especially if you handle sensitive data or own multiple devices, a paid antivirus solution can provide peace of mind with enhanced security features. Amid an escalating cybersecurity climate, consumers are taking a more discerning approach to their software choices. One name often brought into the mix is the Russian cybersecurity firm, Kaspersky Lab, which has long been recognized for its robust antivirus capabilities. Once again, the U.S. government is scrutinizing the firm. The Department of Commerce is reportedly considering enforcement action against Kaspersky, escalating from a previous ban that restricted federal government use of its software. This move comes amid a backdrop of intensifying concerns around Russian cyberattacks, particularly following Russia's invasion of Ukraine. Allegations against Kaspersky, suggesting possible ties to the Russian government, are not new. Such claims, which date back to 2017, suggest that the company could potentially provide a back door for cyber-espionage activities. As a result, many users, especially within the U.S., have become wary of installing Kaspersky's software on their devices. Kaspersky Lab continues to deny these allegations, maintaining that it operates independently of any government influence. And it's worth noting that, despite the geopolitical controversy, Kaspersky's antivirus products remain highly rated for their efficacy in threat detection and removal. Therefore, when considering Kaspersky as an antivirus solution, it's essential to weigh its technical merits against the potential geopolitical risks. While its software is often lauded for superior protection, the looming question of trust and data safety remains. Users are urged to stay informed about these developments when choosing an antivirus solution. In the world of cybersecurity, the trust between a user and their antivirus provider is paramount. When this trust is broken, it can be nearly impossible to regain. This is the challenge with AVG and Avast, two popular antivirus solutions owned by the same parent company, Gen Digital. In the past, these two companies were mired in controversy. The trouble began when Avast's Online Security browser extension was found to be gathering an excessive amount of user data, far beyond what was necessary for the extension to function. This included users' location, search history, gender, age and even personal shipping information. The allegations escalated when it was discovered that this data was sold to corporate clients through a subsidiary of Avast named Jumpshot. This practice raised serious ethical questions and landed Avast and AVG in hot water with privacy advocates. Following public outcry and investigations by security experts and journalists, Avast shut down Jumpshot in early 2020 but the damage was done. The discovery of these unethical business practices led to the removal of AVG and Avast from many recommendation lists, despite their previously solid reputations in the antivirus market. Since then, Avast and AVG have undergone significant changes to restore user confidence and ensure that privacy isn't compromised. They have closed down the data-aggregating subsidiary, Jumpshot, and have received certifications from data privacy advisors such as TrustArc. Avast and AVG have also committed to working closely with privacy experts to responsibly manage users' data. Today, both AVG and Avast claim to no longer pose a privacy threat to users, and they continue to provide robust virus protection. However, their past actions serve as a stark reminder that choosing an antivirus goes beyond considering its technical merits. Users must also consider the company's ethical stance and practices, and whether they can trust it with their sensitive data. In this case, despite improvements, the shadow of past missteps continues to hang over AVG and Avast, highlighting the importance of a strong ethical framework in cybersecurity companies. To identify the best free antivirus software, we've developed a comprehensive methodology involving the evaluation of various antivirus solutions against a weighted set of categories. Each software solution was assigned a score in each category, and these scores were then used to calculate a product's total score, with a possible maximum score of five stars. Pricing (10%): This category assessed the cost-effectiveness of each antivirus solution. We evaluated the availability of a free trial or free option, the starting price for paid plans and the highest price tier. Affordability, the diversity of pricing plans and the set of features provided at each price point were all factors in scoring this category. This category contributed to 10% of a product's total score. General Features (30%): We evaluated each product on several key features that are essential for a good antivirus solution. These include malware protection, identity protection, firewall, email security, PC cleaner, file shredder and two-factor authentication. Each feature was scored on its implementation, effectiveness and user-friendliness. This category accounted for 30% of a product's total score. Additional Features (20%): Beyond the essential features, this category involved evaluating additional features that significantly enhance the functionality of an antivirus solution. These include anti-spam measures, password protection, encryption, ransomware protection, whether a VPN is included, whether a password manager is included and phishing protection. The availability and quality of these features significantly influenced this score. This category made up 20% of a product's total score. Ratings and Reviews (10%): Making up 10% of the total score, this category involved a thorough analysis of user reviews and ratings on trusted platforms such as Trustpilot, G2 and Capterra. We specifically sought out products with a rating of 3.5 or above on these platforms, considering both the score and the number of reviews. This highlighted antivirus solutions that users found reliable, effective and user-friendly. Expert Score (30%): The final category, contributing to 30% of a product's total score, involved our own expert evaluation. Here, we reviewed each antivirus solution for its unique or standout features, assessed its overall value for money, considered its popularity among users and evaluated its ease of use. The aim of this category was to identify antivirus solutions that offered something extra beyond the basics, whether that be innovative features, exceptional value or superior user experience. Free antiviruses are good at protecting your devices from a wide range of threats. However, they typically don't include some of the more advanced features that come with paid options. Microsoft Defender is technically no longer free. Microsoft has recently shifted its policy and the software doesn't come preinstalled with Windows anymore. Now, users need to buy it separately. Although it provides good protection, other antivirus software in the market offers more extensive coverage, which includes features, such as identity theft protection, a VPN and password manager. All devices that connect to the internet are vulnerable to viruses and other threats. That's why it's important to have some form of antivirus protection on all of your devices—even Apple products. Yes, you can. It's important to be careful about which emails you open and never click on any links or attachments unless you're absolutely sure they're safe. Many email clients, such as Gmail, will pre-scan attachments before you open them and alert you to potential threats. While Macs are less likely to be affected by viruses than PCs, they're not immune. It's still important to have some form of antivirus protection on your Mac in addition to other security measures. Signs that your device may be infected include slow performance, unexpected pop-ups and new programs that you didn't install. If you suspect your device has a virus, it's important to scan it with an antivirus program as soon as possible. While today's leading antivirus services offer helpful features, the truth of the matter is that it's not enough to keep you fully protected. Human error is responsible for a large number of security breaches for both private individuals and businesses. Using common sense when it comes to password usage, deciphering phishing scams and other tools are essential when it comes to keeping your information secure. No, antivirus software cannot stop hackers. However, it can detect and remove any malicious software that hackers may have installed on your computer without your knowledge. In addition, antivirus software can also help to protect your computer from being hacked in the first place by identifying and blocking any suspicious activity. 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 the license permits. You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation. No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material. The Motorsport Images Collections captures events from 1895 to today's most recent coverage. Discover The CollectionCurated, compelling, and worth your time. Explore our latest gallery of Editors' Picks.Browse Editors' FavoritesExperience AI-Powered CreativityThe Motorsport Images Collections captures events from 1895 to today's most recent coverage. Discover The CollectionCurated, compelling, and worth your time. Explore our latest gallery of Editors' Picks.Browse Editors' FavoritesExperience AI-Powered Creativity