Avast free antivirus android test

I'm not robot

reCAPTCHA

Continue

I'm not robot

reCAPTCHA

Avast is no stranger to game security - it has made one of the most famous Windows apps for decades. Did he successfully switch to an Android phone? Let's find out. Avast decides to tackle mobile, but does it still come out on top? If you've ever used an antivirus - and let's be honest who didn't - you'll be happy to see a big, orange button scan. This is the central point of the Avast interface, and will be your first step using the app. On the test phone, untouched by antivirus scanning so far, the scan was acceptably fast (about 25 seconds), despite a slight lag of 3 - 5 seconds before the start. After scanning the work, a list of problems appeared, which Avast found problematic. None of them were worried, especially since 2 of the 3 problems were simply that the Avast function was not enabled. Less experienced users may feel that such warnings may indicate mobile security issues, but this is unlikely. If the difference between the problem and the proposal is clear, it will eliminate this confusion. Once you've taken all the steps you deem appropriate, you'll find the rest of the features that the app offers, either by scrolling down the results page or accessing the list in the menu on the left. Some of these features are slightly interesting: if you choose a premium package (the default freemium app), you can remove ads. You can also include anti-theft measures, scan new files uploaded to your computer, block sensitive photos in storage, and take steps to measure and improve Wi-Fi speeds. Tweak that the app scans when it performs a general antivirus scan, and set it up to scan on a regular basis of your choice. Although there are many options, none of them are innovative. They're similar to what you'll find in other apps. In addition, many of these features are available on your phone (malware scanning, download scanner, app information, theft management, etc.). Another problem found with the app is that the features are not the same type that users may find confusing. To give an example, some of them are standard Avast features (not problematic), others need more resolution before they can work, and some are actually different Avast applications that need to be downloaded separately. Offering them everything in an undifferentiate list increases the chances that inexperienced (and not very inexperienced) users will click on unwanted product pages and come across annoying resolution solutions. Avast Antivirus for Android is not the most beautiful of the apps to use. Given that this is a freemium product, ads can be expected. that is not acceptable as intrusive these ads. There are ads from third parties and for other Avast services, and they are all sneaky designed to look just like bona fide app features. It would be easy to Click one. It's hard to take terrible security warnings for your phone seriously when there's spam-looking used car advertisements in just millimeters! Where can you run this program? This version of Avast is for Android phones. It is also available for other platforms including Windows and iPhone. Is there a better alternative? Your opinion about antivirus applications is likely to be shaped by how much they are needed. If you think they are a valuable addition to your security repertoire, then Avast is one option. There are others like Kaspersky Internet Security for Android, but, in terms of security, they are all similar in efficiency. Preferences for one over the other are likely to be aesthetic and depend on what you have used - or used - on other platforms in the past. Avast was not a pleasant app to use. It was a strange experience - it offered everything you would expect from an antivirus, comes from a reputable developer, and worked quickly and smoothly, but seems packed to make the user experience so unpleasant it detracts from its functionality. Should you download it? No. Avast Antivirus for Android is ad-ridden, confusing, and potentially unnecessary. If you want a mobile antivirus, check out competing apps like Kaspersky or Bitdefender to see if it offers the best user experience. With the rise of malicious threats on Android, it definitely makes sense to use an antivirus app, but unfortunately, a new study shows many security apps have pathetic detection rates, so you need to choose wisely. Here are the ones that perform best. If you watched the news tech headlines last week, you've probably heard that Android... More than 41 Android virus scanners were inspected against 618 types of malware. Nearly two-thirds of them identified less than 65% of these types of malware, making them unsuitable or unreliable for your mobile security, the firm writes. The top 7 apps, those with green boxes on the chart above, are: Avast, Dr. Web, F-Secure, Ikarus, Kaspersky, zoner, and Lookout. Using one of these apps, the report says, means you don't have to worry about malware protection. If you have a favorite app that has done badly on the AV-Test report (full PDF test here) it may not mean that it is completely useless if it has features such as remote lock and wipe or backup data, and there are problems in testing for active malware threats (AV-Test is used only by the most well-known malware families detected between August and December 2011). However, if wondering what kind of antivirus app to use on Android, this independent test offers some recommendations. Test: Malware protection for Android - March 2012 AV-Test via CNET Screenshot: David MurphyIf something is free, especially if it's complicated something, or what you'll probably have to pay for for familiar sayings are often true: You are a product. This is one of the reasons why you are always advertised over the internet. Search engines, email services, messaging platforms or other apps and services that you represent cost money, and companies have to somehow recoup this (and profits). That's why I think you should reconsider using the free Avast antivirus product. As a joint message from Motherboard and PCMag, a subsidiary of Avast, Jumpshot, recently discovered, it draws data from Avast's antivirus users and sells it to advertisers, who can then combine it with other data they have about your activities to keep track of you in great detail. According to the Article Motherboard: Avast collects data from users who choose in and then provides that Jumpshot, but several Avast users told Motherboard they didn't know Avast sold browsing data, raising questions about how reported that consent. Data obtained by Motherboard and PCMag include Google searches, location searches and GPS coordinates on Google Maps, people visiting LinkedIn companies, particularly YouTube videos, and people visiting sites. From the data collected, you can determine what date and time an anonymous user visited YouPorn and PornHub, and in some cases what search term they entered on a site and what specific video they watched. Although the data does not include personal information such as usernames, it still contains a plethora of specific browsing data, and experts say it may be possible to deanonymize some users. Avast got nailed last year after security researcher Vladimir Palant discovered that the company's browser extensions were sending your browser's web history straight to Avast. As a result, Google, Mozilla and Opera removed a number of Avast extensions from their additional directories until Avast cut out the abusive behavior. As Avast PCMag recently said: We have completely ceased the practice of using any data from the browser extension for any other purpose other than the main security engine, including exchange with Jumpshot. Screenshot: David MurphyTo Avast's (small) credit, the company provides users with a fairly obvious screen surge when asking users to share their data. However, as PCMag correctly notes, this screen does not detail what companies can combine this data with other information they have about you to create a fairly accurate profile of who you are and what you do. Users are also not given any instructions to delete data that you have already shared with Avast/Jumpshot (if possible). Similarly, Avast sets out which services collect and present your data in its tiny font privacy policy, which people probably don't read. This includes: Cleaning the browser is a module inside the Desktop Antivirus (Windows), which checks the browser extension of most browsers, browsers, to identify malicious extensions and suggests removing them. The browser is cleaned up by default. You can opt out of processing cookie data (internal ID (GUID), product version, time information, original browser, cookie domain, cookie name, cookie value) for trend analysis purposes, Avast therefore provides this dataset from the free version of this product to allow Jumpshot to create products and services. For more information, please see our consent policy. Web Shield scans data that is transmitted when you browse the Internet in real time to prevent malware from being downloaded and run on your computer. By default, Web Shield is configured to provide optimal protection when you turn it on. If the Web Shield feature is active and you choose to process data (internal ID (GUID), the product version, time information, devoid of URLs (if not cached), carefully selected aspects of certain pages without identifiers, selected requests) for trend analysis purposes, Avast therefore provides this data set in a stripped and de-identified form from the free version of this product to allow Jumpshot to create services. For more information, please see our consent policy. I've already installed Avast. Now what? If you're not doing anything, I recommend tightening up Avast's settings (through the Settings menu) and visiting the Personal Privacy section. Inside there, uncheck every version of Avast offers: Screenshot: David MurphyHonestly, I'd go ahead and uninstall Avast completely, because you don't really need a third-party virus scanner on your desktop or laptop-at least not on Windows 10. The free antivirus app baked into your operating system, Windows Defender, is powerful enough and doesn't pack data about everything you do and sells it to third parties. If you need a little more firepower, you can also install a separate anti-malware application like Malwarebytes (whose privacy policy you can read here). Stay on top of it though, in case any future policy changes push Malwarebytes more into tracking and selling territory than a useful anti-am security application. It never hurts to be skeptical. (I'm also a fan of Malwarebytes' Adwcleaner, if you need extra help to clean up the filled system.) Otherwise, you can also test an open source virus and a malicious scanner like ClamAV. I can't make any promises about his privacy, but as an open source project, it's at least more transparent about what it does than other third parties As for Mac users, the general convention is to shrug and smile at your Windows-Macs brothers for not getting viruses after all. Right? Not exactly. Macs can get hit by viruses and malware; it's just rarer. Less rare, perhaps, if you don't have common sense what it is and click on or download anything and everything you see online. If you are you and don't try to install things that sound weird, or provide system permission for anything that asks it out of nowhere, you should be fine. Keep your system updated with the latest security patches, grab Malwarebytes, and run a strong ad blocker in your browser. Ignite Malwarebytes it every now and then to give yourself a quick inspection against malware and other crap, but you probably don't need a more comprehensive antivirus scan setup than this. A what.