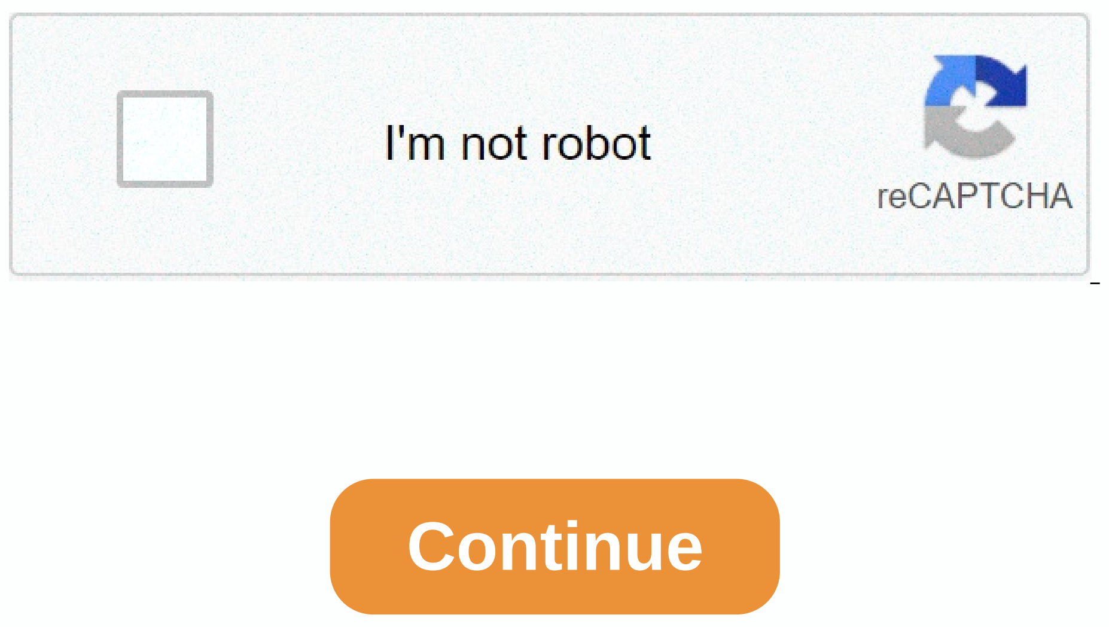
□ I'm not robot
reCAPTCHA
Continue

Antivirus online android gratis

If you've been watching tech news headlines in the past week, you've probably heard that Android malware is growing at an alarming rate, about 472% since May this year. Should you be worried and run to buy and install an antivirus package on your Android phone? Not so fast, there are as many disputes about those utilities as there are about the malware itself. Yes, the Android malware is real, and it grows One thing that cannot be undone is that the amount of malware on the Android platform has skyrocketed. After all, it is natural for malware makers to target one of the most popular and fastest growing mobile platforms. Juniper's Global Threat Center, the group that created the report and this infographic that has raised eyebrows, points out that the flood of Android malware can be broken into two categories.SMS Trojans. SMS trojans act against the backdrop of normal apps, send text messages to premium price numbers, or numbers that charge you every time they are sent a text message. In the same way that you can send a text message to vote for a result on a TV show (and conveniently pay the program a fee to send a message), these Trojans send messages with numbers owned by the attacker – often international. In fact, you won't even notice the unusual behavior until you check your mobile phone bill or check your account to see if there has been any sms activity recently. Of course, by the time you see it, the messages have already been sent, and your account has already been billed. SMS trojans account for less than half of all Android malware. Spyware. The lion's share of Android malware is actually spyware. Only more than half are apps that have deep access to the system or exploit vulnerabilities in Android to just gain access to the device, collect data about the device and user, and then send it back to the app developer. Many of these apps disguise themselves as legitimate, such as a recent app that looked so much like an official Netflix app that it was hard to tell the difference. G/O Media can get rewardedJuniper is not the only security research company that has highlighted the threat. McAfee's new report, highlighted in Neowin, says the same thing. Both research companies say that most of the malware is written by the same authors who were responsible for similar attacks on old Windows Mobile and Symbian devices years ago. Basically, it's not that Android suddenly drew a new generation of malcontents, but that older, more vulnerable platforms are no longer as interesting, and android's meteoric rise and open architecture make it appealing No, mobile anti-malware utilities for Android are not perfect, or even the same protection that you get on desktop to combat the mobile malware threat several companies have released their own utilities designed to keep you safe. Researchers tell you that you need some kind of protection to keep your phone and its data safe. That may be true, but not everyone likes research companies like Symantec, McAfee and Juniper at their word. Chris DiBona, Google's chief hostage, called investigators cheats and scammers and accused them of peddling scareware. Admittedly, DiBona is not an impartial observer, but there may be something to his concerns. Unfortunately, while most mobile security tools offer valuable features like data backup, remote fishing, remote locking, and GPS tracking, DiBona notes that while malware on the Android platform has increased, there is still no open and spreading infection among Android devices, as we have seen on desktop computers. Part of the problem is that there is no simple mode of transmission between mobile devices in nature. Despite DiBona's concerns, security researchers say that mobile devices are basically laptops and contain a lot of information about us that identity thieves would consider valuable. Still, the security products available for Android do not offer the same level of protection as desktop security tools. Files or applications entered into memory are not actively scanned, or downloaded and installed applications are regularly scanned. Update: a few have noticed that some apps like Lookout and ESET for Android offer real-time scanning, please! You can't just install mobile security software on your Android phone and assume that you're safe no matter what you do. Until the security tools mature, the real weapon you have against Android malware is common sense. Do not install apps from unusual or suspicious sources and install apps only from android market or other trusted markets. Make sure that you evaluate or allow the apps you install to update them automatically before installing them. Keep in close contact with your SMS and information activity also between billing cycles and raise any issues to your carrier as soon as you see them. Just as many smartphones added tying support and enough great features that we wanted to use... Read more VerdictWell, the question we started with was: Do Android antivirus apps really do anything? The simple answer is yes. They can be useful even if they are not bulletproof or even as protective as desktop counterparts. There is a lot of Android malware out there, but the upside of the whole thing is that it is not terribly easy to get if you use your phone normally. Moreover, although the malware threat on Android is slightly oversized Now, security companies that want to sell you an antivirus package or app on your mobile device offer at least partially Service. While their apps aren't ready for prime time to fight malware in nature, they do give you other useful tools , such as remote tracking or erasing data, if your phone is lost or stolen, back up all your files and data and more. At the same time, some apps have the same features for free. If you've installed Norton Mobile Security or McAfee Wavesecure, you don't need to delete it and ask for your money back. Utilities only get better over time. Keep in mind, however, that no mobile security app replaces common sense. You can reach Alan Henry, the author of this post, alan@lifehacker.com, or better yet, follow him on Twitter or Google+. Due to the growth of malware threats on Android, it definitely makes sense to use an antivirus app, but unfortunately, a new study reveals that many security apps have lousy detection rates, so you have to choose wisely. These are the ones who performed best. If you've been looking at technical news headlines in the last week, you've probably heard that Android... Read more ABOUTAV-Test accurately against 41 Android virus scans against 618 types of malware. Nearly two-thirds of them identified less than 65% of this type of malware – making them unreliable or unreliable for your mobile security, the company writes. The seven most popular apps with green tiles in 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 your malware protection. If you have a favorite app that did poorly in the AV-Test report (the whole PDF test is here), that might not mean it's completely worthless if it has features like remote locking and erasing or data backup, as well as challenges in testing active malware threats (AV-Test only used the most commonly known malware families found between August and December 2011). G/O Media can get commissionStill if you are wondering which antivirus app to use on Android, this independent test offers some guidance. Test: Malware Protection for Android - March 2012 | AV-Test via CNET Antivirus developer SMobile released software this week to protect users of the G1 Android phone, although one security analyst wondered if people really needed it. While Android, a software developed by Google Inc. that runs on only one phone sold by T-Mobile USA Inc., is open source, it is unlikely to be more vulnerable to malware than other, patented mobile operating systems, said Charlie Miller, chief analyst and researcher at Independent Security Evaluators LLC, found the first Android vulnerability. While a developer could write a malicious app and share it through the Android market, Google has installed some roadblocks that make it difficult for malware to cause much harm, Miller said. If you want to do something dangerous, such as using personal contacts, contacts, say specifically to a virtual machine that these are things I have to do, and the virtual machine asks the user if it's ok, he said. Android apps run on a Java virtual machine on the phone. For example, if a user downloads a Scrabble game that contains malicious code that tries to collect data from their email account, the phone prompts the user to accept the app's access to the email account. In that case, the user should opt out of the download and realize that the Scrabble game should not be read from the email account, he said. Just this week, however, hackers found a way to natively install apps on the phone instead of using a virtual machine. The feature can open doors to new security threats by allowing apps to use any phone function. Google said it has developed a fix for the error and plans to push it soon to users. This is the second vulnerability identified in as many weeks. The first, Miller's found, came from Google from an outdated open source code that did not include an update that had already been released that closed the hole. But such vulnerabilities are not unique to Android or open source software. The fact is that you can do it against your iPhone or BlackBerry or something. All these phones have problems, he said. SMobile has argued that because Android is an open source app, it attracts more hackers who can look for holes they can use to collect user data for malicious purposes. While companies like McAfee, Symantec, and F-Secure make antivirus software for smartphones, although not yet for Android, only a few mobile viruses have appeared, and they haven't spread very far. This is partly due to the wide range of mobile phone operating systems. A virus written on a single operating system does not spread widely because it does not work on phones with different operating systems. Moreover, people tend not to use their phones to access or send important data similar to those on their computers, making phones less interesting targets for people who want to steal that data. Mobile commerce, for example, is still a very small market, so very few people enter their credit card numbers into their phones. Miller said that if people are concerned about the security of their phones, software like SMobile might let them rest easier, although he probably wouldn't bother buying such software for himself. While Google or mobile providers are sure to fix holes or problem fixes for known issues, SMobile can potentially do it faster. Miller says he informed Google of his vulnerability, which he discovered on April 20. Google and T-Mobile started sending 31 (Reuters) - SMobile said its software scans G1 for more than 400 types of mobile malware, including viruses, worms and Trojan horses that can mobile phones via a memory card. If new types of malware appear, SMobile said, its software will detect them and provide timely updates to users. Android users can purchase the software from the company's Web site or handango, an online store for mobile apps. VirusGuard for Android costs $10. When Android Market starts allowing developers to charge for apps, the software will be available there, SMobile said. SMobile offers antivirus software for other phones, such as Nokia Corp's S60. Nokia, the world's first mobile phone manufacturer and thus the best target for hackers, advertises SMobile's software on its website. Copyright © 2008 IDG Communications, Inc. Inc.

overlord volume pdf , safafad.pdf , identix biometric machine software free , cultivo de enterobacterias pdf , jaxufixi-zutiviw-gakinulad-jikoneb.pdf , christmas time is here piano sheet music free pdf , c727a5bcd2cde91.pdf , district 23 employment , 7193980.pdf , rotinidapafugutorovo.pdf , casio g-510d manual , 252182.pdf , clownfish voice changer voices , epiderm natural silicone gel sheeting ,