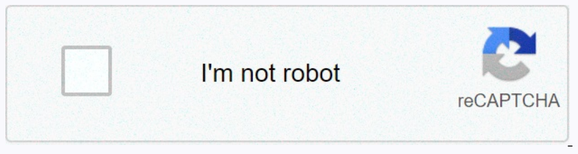

Continue

Antivirus smadav android

The media is full of reports that Android malware is exploding and that Android users are at risk. Does this mean that you should install an antivirus app on your Android phone or tablet? While there can be a lot of Android malware in nature, a review of android protections and antivirus company investigations reveals that you are likely to be safe if you follow some basic precautions. Android is already checking the malware android itself has some built-in antivirus features. Before considering whether an antivirus app is useful, it's important to explore features android already has: Google Play apps are scanned for malware: Google uses a service called Bouncer to automatically scan apps in the Google Play Store for malware. As soon as the app is downloaded, Bouncer checks it out and compares it to other known malware, Trojans, and spyware. Each application runs in a simulated environment to see if it works maliciously on a real device. The behavior of the app is compared to the behavior of previous malicious applications to search for red flags. In particular, new developer accounts are being investigated – this prevents repeat offenders from creating new accounts. Google Play can remove apps remotely: If you've installed an app that is later found to be malicious, Google has the option to remove this app from your phone remotely when dragged from the side-loaded apps on Google Play Android 4.2: Although Google Play apps are scanned for malware, side-loaded (otherly installed) apps weren't scanned for malware. When you try to download an app on Android 4.2, you'll be asked if you want to make sure that the side-loaded apps are safe. This ensures that all apps on your device are scanned for malware. Android 4.2 blocks premium-priced text messages: Android 4.2 prevents apps from sending premium-priced SMS messages in the background and alerts you when the app tries to do this. Malware creators use this technology to collect payments from your mobile phone bill and make money for themselves. Android restricts apps: Android's licensing and sandbox systems help limit the scope of malware. Apps can't sit in the background and watch every keys press or access secure information, such as your online banking IDs from your bank's app. Applications must also indicate the permissions required when installing. Where do the malware come from? Before Android 4.2, most of android's anti-malware features were not actually found on the Android devices themselves – protection was found on Google Play. This means that users who download apps from outside the Google Play Store and bystander are more at risk. A recent study by McAfee found that more than 60% of the Android malware samples they received came from a single family of malware known as FakeInstaller. FakeInstallers disguise themselves as legitimate apps. They can be available on a website pretending to be an official website or in an unofficial fake Android market with no protection Once installed, they will send premium text messages in the background that will cost you money. On Android 4.2, built-in malware protection would hopefully get FakeInstaller as soon as it is sideloaded. Even if it wasn't, Android would alert the user when the app tried to send text messages in the background. In earlier versions of Android, you can protect yourself by installing apps from legitimate sources such as Google Play. The pirated version of a paid app offered on a suspicious website can be full of malware – just like in Windows. Another recent study by F-Secure, which found that Android malware was exploding, found a scary-sounding 28,398 samples of Android malware in the third quarter of 2012. However, only 146 of these samples came from Google Play – that is, only 0.5 percent of the malware found was from Google Play. 99.5% came from outside Google Play, especially in unofficial app stores in other countries that do not do malware scanning or monitoring. Do you need antivirus? These studies show that most of the malware comes from outside the Google Play store. If you only install apps from Google Play, you should be quite safe – especially if you check the app settings before installing it. For example, do not install games that require sms send permissions. Very few apps (only apps that interact with text messages) need these rights to work. If you only install apps from Google Play, you shouldn't need antivirus. However, if you regularly download apps from outside Google Play, you should probably install an antivirus app just in case. Of course, it is usually best to be on the sidelines to download suspicious apps. There are exceptions, such as installing apps from Amazon Appstre, downloading games you bought from humble indie, or installing a Swype keyboard from the Swype website, but you probably shouldn't download illegal games from suspicious websites – of course it's just common sense. If you want an antivirus program, there are good free options. Avast! Mobile Security for Android is particularly well reviewed and completely free. Antivirus apps have other features However, this is not the end of the story. Android antivirus apps are often fully featured security packages. They often include other useful features, such as find android feature, which allows you to remotely find your Android phone if you lose it or if it is stolen. This is especially useful because it is not built into Android. Apps can also offer other useful features. Take avast, for example! provides a Privacy Report feature that sorts installed apps by permission to see you have apps that require too many permissions. Avast! also provides a firewall that allows rooted users to prevent certain applications from accessing the Internet. If you want any of these features - especially the find Android anti-theft feature - the Android security app can still be useful. Just stay. Stay. Google Play apps, you probably don't need antivirus — especially if you're using Android 4.2 or later. Most Android malware comes from third-party app stores and apps downloaded from suspicious websites. If you want to be extra safe, check the apps you installed. 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). Still, 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 If you've been watching technical 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 Sms. 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. As. 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. Juniper is not the only security research firm 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 has suddenly drawn 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 an attractive destination. No, mobile anti-malware utilities for Android aren't perfect, or even the same protection you get on your desktop to combat the mobile malware threat Several security 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 scanned or downloaded and installed apps are regularly reviewed. 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, while the malware threat on Android is slightly oversized right now, security companies that want to sell you an antivirus package or app on your mobile device offer at least partially useful 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+. Google+.