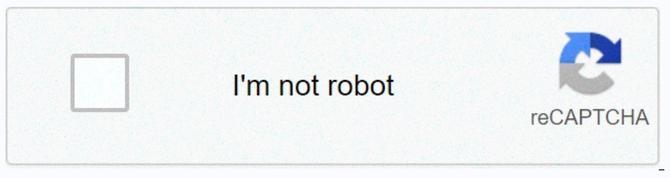

Continue

Authentication app apk

As many of you know, installing an Android app is a simple, simple process – you open the Play Store, find the software you need, and press the big green install button. However, Android apps also come in the form of packages that are installed manually, not through Google's App Store. These packages have a . APK file extension, and their practical use are numerous. For example, you can save offline backups of apps as APKs. Even if the app in question is pulled out of the Play Store (like what happened to Flappy Bird), it can still be installed from an APK file. It also uses APKs when sideloading apps on smartphones that run forked Android versions because they are not included with the Play Store client. Think the Amazon Kindle Fire or the Nokia X phone. So where do you get APKs from? While they can be downloaded from the Internet, the safest way is to extract Android installation packages directly from an Android device. Keep in mind that the method described here only works for free applications! Paid apps are protected from extraction for obvious reasons. In addition, apps that download additional data during installation (see figure #5) cannot be used when installed by an extracted APK. Apps that download additional files after they are installed should work properly. With this out of the way, here's how to turn your own Android apps into APK installation files. On an Android device, open the Play Store and download the apps you've extracted. Download APK Extractor. It is a free and easy-to-use application. Open APK Extractor and tap any app you want to extract. Press Long to select multiple apps. The APK files are stored in a folder on the device's memory. (By default, Apks is extracted.) That's pretty much everything! The extracted APKs can now be copied to another Android smartphone or tablet and installed using a file manager such as Astro or ES File Explorer. SUBSCRIBE TO OUR NEWSLETTER! As technology advances, hackers' ability to access our personal accounts and information has also increased, potentially putting us at risk of becoming victims of identity fraud or worse. As a result, Internet security is becoming increasingly important, and many services such as Google are now taking additional steps to protect consumers' private data. Google Authenticator is an app that uses two-step verification software to keep your information safe by requiring an additional level of identification before it is access to your accounts. Instead of simply entering a password when you sign in to Google apps on the go, Google Authenticator generates a random six-digit code that you need to enter to sign in when you have two-factor verification active. If you want to use Google Authenticator to protect your Google apps, learn how to do this. Check out the products mentioned in this article:MacBook Pro (starting at Best Buy at €1,299.99)Microsoft Surface Pro X (starting at Best Buy)iPhone 11 (from $699.99 at Best Buy) Galaxy S10 (starting at Best Buy from $899.99)How to set up Google Authenticator 1. Download the Google Authenticator app from the Google Play Store to your Android device or app store on iPhone. 2. While you've signed in to your Google Account on your PC or Mac, click the small icon with your photo in it in the top right corner of your screen and click Manage your Google Account. 3. In the menu on the left side of the screen, click Security, and then scroll down to the Sign in to Google.4 header. Click 2-step verification to enable the option. You will then be prompted to re-enter your Google account password to continue. Enable 2-step verification. Jennifer Still/Business Insider 5. Under Set up alternative second step, in the Authenticator app option, click Set up. Click Set up. Jennifer Still/Business Insider 6. Select whether you have an Android or iPhone, and then click Next. 7. Open the Authenticator app on your mobile device and tap Start Setup. On your mobile device, tap Start Setup. Jennifer Still/Business Insider 8. Tap Scan Barcode on your phone and then scan the code displayed on the computer screen. Scan the code with your mobile device. Jennifer Still/Business Insider 9. After scanning the code, your Authenticator app automatically starts displaying a randomized six-digit code. On the computer screen, click Next, and then type the six-digit code that appears in the Authenticator app on your phone. 10. Click Done to confirm the verification. You'll now be set up with Google Authenticator and can sign in to your Google Account using the app. Related cover of How To Do Everything: Tech: Get the latest Google stock price here. Insider receives a commission when you buy through our links. Photo: ShutterstockTech 911Tech 911Do you have a technical question that keeps you on the map at night? We would like to answer it! E-Mail-david.murphy@lifehacker.com with Tech 911 in the subject line. I stirred up a bit of host this week when I suggested that people should switch from Google Authenticator to another two-factor authentication app on Android. I recommended Authy, but that's just because I use it and find it incredibly convenient. Not only does it prohibit you (and other apps) from taking screenshots of it, but I appreciate the extra verification security built into Authy (and the options you have to get the security of your 2FA keys, even if you use more controversial features, such as the ability to quickly sync your 2FA keys with other devices you own). But Said, there are also many other great 2FA apps – 1Password comes to mind if you don't mind paying for it (and you should do it if you don't have a password manager yet). Better yet, use a hardware token for all the accounts you can use instead of your smartphone. I don't care what you use; Me and many others, like Authy, but you are welcome to use whatever authenticator app works best for you. Do you feel overwhelmed? You shouldn't be, but it's seem to process a lot if you are not particularly savvy with technology or two-factor authentication. As Lifehacker reader Jenny writes: I'm reading your article about 2FA apps, and I need a little guide, please, if you don't mind? I'm just semi-techie and most of it thanks to the nice people on Reddit. This week I turned on Google 2 Factor Authentication for my Reddit signon and still can't really get the spin out how it works. Now you say it's not safe, and I should switch to Authy, right? How do I do this? If I delete the Google sign from my phone, will it confuse my Reddit sign? Or will it change automatically? And when I go to Authy, can I put it on my tablet so that if something happens to my phone, can I still get into my accounts? And if I swap with Authy, should I delete the Google one from my phone before or after downloading and turning on the Authy? Any guidance you could give me would be greatly appreciated! Have a wonderful day, and thank you for all the work you put into informing all of us out here! Let's go over the basics! First is the simple version of how 2FA protects your accounts. You set up 2FA on a website or service and link it to an app (in this case). This app has a rotating number. When you sign in to the website or service, you need to access the app and provide that rotating number to verify that you are you and not a hacker who got your login and password in their hands. The protection comes from the idea that while your credentials can easily be stolen in different ways, the chances are very slim – if not infinite – that an attacker will also be able to guess this particular number (or with fallow force), which changes approximately every 30 seconds. Just last week, Instagram confirmed reports that it is changing its account security setup to read more this is slightly different than when a website or service gives you a number that you then need to enter during the login process. This is called two-step verification, and although it's better than nothing, it's less secure than 2FA because it's easier for an attacker to swap your phone number or jog in other ways—intercept your messages, including those login requests, and have a field tag. It is much more difficult for an attacker to gain physical control over the device you use for two-factor authentication, so the latter is preferred. Now to your question. Honestly, you're probably okay if you stay with Google Authenticator because it's better than no one at all to use. As long as you don't download shitty malware or random apps to your device—often the same thing—it doesn't matter that Google Authenticator allows screenshots (from the time I wrote this). If you want to be super safe, you can wait or switch to another authenticator app like Authy. Here's how I'd do it with Reddit: Use Google Authenticator to sign in to Reddit, as you would normally disable two-factor authentication. Would. David MurphyTurn it back on and set it up with Authy instead of Google AuthenticatorThat's. You must repeat this process for each website or service where you have enabled 2FA and linked it to Google Authenticator. It is an annoying process, but it should not take very long; and at least you have a list of all the sites that need to be customized as you can see them in the Google app. Once you have swapped all your accounts in Authy and can confirm that you can sign in to them using Authy's codes, delete Google Authenticator. However, to share Authy codes across devices, the process is much simpler. Install the Authy app on any other device you want to use for 2FA. Then jump into the Authy app on your original device and drag its settings. Tap Devices below and enable Allow Multi-Device. Screenshot: David MurphyThen, sign in to Authy on your second device with all the credentials it requires – your phone number, I think, or the first device. Once you have set it up and see that all your 2FA codes are synchronized, go back to your original device and turn off the Allow Multi-Device setting. The new device you just configured will continue to work, but no one else can sync your account to another device until you reverse this switch. Sounds weird, doesn't it? As much as we try to promote the importance of this security measure, a... Read moreNormally, 2FA apps need to perform the process described earlier to sync an account with authenticator apps on multiple devices: sign in to your accounts and temporarily disable 2FA, re-set up and scan the provided QR code (or whatever) with the authenticator app on each device. Otherwise, there is usually no way to simply add a new device and have it synchronized. Authy is the exception, which is also a source for some of its controversies – although convenient, this feature theoretically makes it easier for an attacker to gain access to all your 2FA combinations if you haven't prevented them from doing so by disabling it. I like the convenience, but I can see how this would be a sticking point for people who want an authenticator experience as safe and as private as possible. If you are, Authy may not be the best pass. Do you have a technical question that keeps you on the market at night? Tired of fixing your Windows or Mac? Looking for tips on apps, browser extensions, or utilities to accomplish a specific task? Let us know! Tell us in the comments below or email david.murphy@lifehacker.com. david.murphy@lifehacker.com.