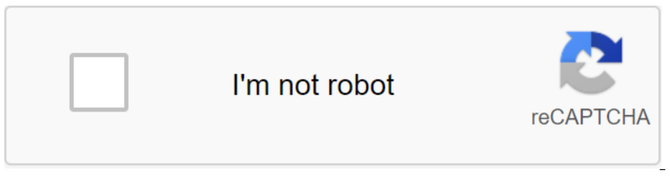
Probleme google authenticator uplay



Continue

If you want to protect your data from hackers, you should definitely use two-factor authentication, and Google Authenticator is a simple, logical choice. And now, it's finally got a feature that makes it easy to move your data from one phone to another. If you're not familiar with Authenticator, this is a mobile app that provides secondary, ever-changing code that you have to use, along with a password, to get into your online accounts such as Facebook, Gmail and Twitter. So even if a hacker somehow takes over your password (and it happens all the time), they can't get it without the code generated by Authenticator. But Authenticator has driven me crazy over the years as it was impossible to transfer my data to another phone. This meant that when you switched to a new phone, you had to go through the painful process of re-adding individual accounts to the newly installed authentic. I change phones a lot and it was a huge pain in the ass. Now, Google has updated the authentic with the ability to transfer all its data to a new phone. This process is simple, and it comes down to choosing an account and scanning the code on an old phone. In a blog post, Google noted that data is not sent to Google's servers during this transfer. In addition, if you use the transfer feature, Google will alert the user and add the event to the app log to prevent unauthorized use. SEE ALSO: This smart speaker with a Google assistant is 70% off Android Police also indicates that the app has been visually improved to look better on phones with different resolutions, and a new, blacker version of the dark theme has been added. Unfortunately, the new feature is currently only available for Android; there is no word on when it comes to iOS. You can get Google Authenticator on Google Play and Apple's App Store. You should read Matt Honan's heartbreaking story about the hacking attack and the ensuing discussion on Techmeme. Most of the story is about Amazon or Apple's security practices, but I would still advise everyone to include Google's two-factor authentication to make your Gmail account safer and less likely to get hacked. Two-factor authentication means something that you know (like a password) and something you have that can be objected to like a phone. Here's a simple video about how it works: I often hear the same questions or objections when I recommend two-factor authentication. Jeff Atwood has done a good job of debunking the common misconceptions-check your post that even photos. But here are some misconceptions that I hear, along with reality: The myth of #1: But what if my cell phone doesn't have an SMS/signal, or in a foreign country? Reality: You can install a standalone app called Google Authenticator (it's also available in the App Store) so your mobile phone doesn't need a signal. Myth #2: Ok, but how about if my cell phone works power, or is my phone stolen? Reality: You can print out a small piece of paper with 10 times the lifesaving codes and put that in your wallet. Use these one-off codes to log in even without your phone. Myth #3: Shouldn't I be bothered with an extra PIN every time I log in? Reality: You can tell Google to trust your computer for 30 days and sometimes even longer. Myth #4: I've heard two-factor authentication doesn't work with POP and IMAP? Reality: You can still use two-factor authentication even with POP and IMAP. You create a special password for a specific app that your email client can use instead of a regular password. You can revoke passwords for specific apps at any time. Myth #5: Okay, but what if I want to check how safe Google Authenticator is? Reality: Google Authenticator is free, open source, and based on open standards. Myth #6: So Google Authenticator is free and open source, but does anyone else use it? Reality: Yes! You can use Google Authenticator for two-factor authentication using LastPass, WordPress, Amazon Web Services, Drupal and DreamHost, or even use the YubiKey device. There's even a pluggable Authentication Module (PAM), so you can add two-factor authentication to any PAM-enabled application. This means you can use Google Authenticator to add two-factor authentication to SSH, for example. The last tip is to use a different password on Gmail/Google than on other services. If you reuse a password and a hacker cracks in the same company, they can use the same password to hack into your Google account. Please don't wait to turn on the 2-step check. It's not that hard and it really will protect your account. Why not set up a two-step authentication right now? Please include two-factor authentication Matt CuttsMatt Cutts is the head of Google's Webspam team. It is working to improve the quality of Google search results. Read Lifehacker's tips for setting up a two-step check here. Google has just launched a two-step check for all Google accounts, a system that makes your... Read more on April 13, 2016 2 minutes read Which brands have your loyalty and trust? According to a new study, it may not be surprising that a certain mouse has won the hearts of consumers and wallets. In its fourth annual review of brand authenticity, communications and public relations firm Cohn and Wolfe generated a ranking of the most authentic brands in the world. Related: 25 Tips for Customer Loyalty Agency surveyed almost 12,000 people in Brazil, China, France, Germany, Hong Kong, India, Indonesia, Singapore, Spain, Sweden, the United Arab Emirates, the United Kingdom and the United States and has narrowed the list of 100 companies with 1,600 brands. The study found that consumers say the brand is genuine when the company consistently delivers on what it promises, protects consumer data and respects their privacy and interacts with them with them with transparency and honesty. Related: 5 simple ways to improve customer retentionIed the old aphorism that the customer is always right still sounds true here - 69 percent of participants said that how the brand treats and treats its customers is more important than if the company were clear about its beliefs or the impact of the business on the environment. At the top of the list is a largely tech industry deal - with the usual suspects of Microsoft, Amazon and Apple - but Disney has taken the top spot. Automakers BMW and Audi cracked the top 10, as did Adidas and LEGO. Related: Improve your great idea by listening to what your customers are telling you For more information on consumer attitudes to authenticity around the world, check out the full study here. Here are the 10 most authentic brands in the world, according to a study by Cohn and Wolfe: DisneyBMWMicrosoftAmazonAppaonAudiSamAdidasLEGO Google Authenticator protects your Google account from keyloggers and password theft. With two-factor authentication, you'll need both your password and your authentication code to log in. The Google Authenticator app works on Android, iPhone, iPod, iPad and BlackBerry devices. ANSWER: What is two-factor authentication and why is it needed? We've mentioned two-factor authentication with text or voicemail in the past, but the Google Authenticator app may be more convenient. It displays code that changes every thirty seconds. The code is generated on the device, so you can use the app even if the device is offline. Activate two-step authentication go to the account settings page and log in to your Google account. In accordance with the Security Log system, click on the Go logging link. In the Password and Hang section, click 2-step check. The introductory screen displays, telling us about the 2-step check. Click Start to continue. Enter your password for your Google account and click Enter or click in. Google forces us to set up a phone check, even if we use the app. The phone number we're entering now will be our backup phone number later. You can get the code via text message or voice call. Click Try to send the code to your phone. If you set up text message notifications on your phone, you'll see a pop-up notification with a verification code. If you don't have text message notifications enabled, you can go to the text messaging app and see the verification code there. After receiving the verification code, enter it to confirm that it is working on the screen, and click next. You should see the screen telling you that it worked. Click on to Enable a two-step check. Until now, a voice or text message is the second step by default. We'll change that in the next section. Now log in from your Google account and then log back in. Back. be asked to enter the password ... ... and then you'll get a text message with a 6-digit code, just like before. Enter this code on the 2-step check screen that appears. By turning on Google Authenticator Now that we've turned on the 2-step check and plugged your phone to your Google account, we'll hiring Google Authenticator. On the 2-Step Verification page in the browser, click the Settings button under the Authenticator app. On the dialog box that displays, select the type of phone you have and click next. The Authentic Settings screen is displayed with a CD code or barcode. We have to scan this with the Google Authenticator app..... So now install the Google Authenticator app on your phone and then open the app. On the home screen authentic, click the plus sign at the top. Then click the barcode scan on the pop-up at the bottom of the screen. You camera is activated and you will see a green box. The goal is that the green box is on the qR code on the computer screen. The CD code is automatically read. You'll see your newly added Google account in the Authenticator app. Notice the code of the account just added. Once you've added an account to Google Authenticator, you'll have to enter the generated code. If the code expires, wait until it changes so you have enough time to enter it. Now go back to your computer and click the Next button in the authentic setting dialog box. Enter the code from the Authenticator app in the Set up Authenticator dialog box and click Check. Show the Done dialog window. Click Made to close it. The Authenticator app is added to the second-step check list and becomes the default. The phone number you entered earlier becomes a backup phone number. You can use this number to obtain authentication code if you ever lose access to the Google Authenticator app or reformat your device. By logging in the next time you howling, you'll need to provide the current code from the Google Authenticator app, just as you provided the code you received in a text message earlier in this article. Creating and printing Google backup codes offers printed backup codes that you can log in to, even if you lose access to both the mobile app and your backup phone number. To set up these codes, click the Settings button under the backup codes in the alternative step setting section. Save the backup codes the dialog box displays with a list of 10 backup codes. Print them out and keep them safe - you'll be locked out of your account Google if you lose all three authentication methods (your password, check codes on your phone, and backup codes). Each backup code can only be used once. If the backup codes have been compromised in any way, click Get New Codes to create a new list of codes. Now you'll see backup codes in the list under the second step on the 2-step 2-step Screen. Creating two-step authentication of application-specific passwords breaks down email customers, chat programs and everything else that uses the password of your Google account. You'll have to create a password for each application that doesn't support two-way authentication. Back to the security screen in the system in the system, click the App password button to match the password and log in to the method. On the app's password screen, click the list to drop out of the Select app list. Choose from select app dropout list. We chose Others so we could customize the app's password name. If you choose Mail,

Calendar, Contacts or YouTube, select your device from the Select Device list. If you've chosen Another select from select application drop-off list, Select's drop-off list is missed. Enter the name of the app for which you want to create a password and then click generate. The app's dialog password window is displayed with the app's password, which can be used to customize Google's apps and account programs, such as email, calendar, and contacts. Enter the password provided into the app, not the standard password for that Google account. When you're done entering your password, click The Made button to close the dialog window. You don't need to remember this password; You can always create a new one later. All the app password names you've created are listed on the App's password screen. If your app's password is compromised, you can revoke it on this page by clicking the Recall button next to the app's name on the list. On the security screen, login and Log-in are listed on the login screen. You can click on App passwords again to create new passwords or undo existing ones. These passwords provide access to the entire Google account and skip the two-factor authentication, so keep them safe. The Google Authenticator app is open source and is based on open standards. Other software projects, such as LastPass, have even started using Google Authenticator to implement their own two-factor authentication. ANSWER: How to make LastPass even safer with Google Authenticator you can also customize Google's new code without two-phase authentication for your account if you don't want to enter the code. Code.