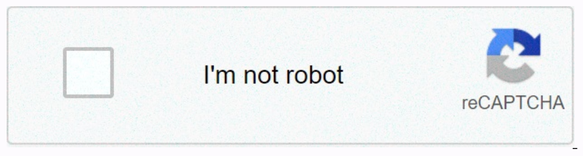

Continue

Gooz io hack

An iOS App Store weather app called UVLens this morning sent out highly inappropriate pornographic notifications to all its users, suggesting that the app may have been hacked or otherwise compromised in some way. There are dozens of complaints from users on Twitter who received a notification that was in no way weather related and was explicit enough to shock users who received it. UVLens is a simple application designed to provide hourly UV predictions for those who are concerned about their exposure to the sun. It is a general use application and it is quite possible that it could be downloaded by children due to its 4+ age rating. UVLens appears to have sent out a notification to all its users due to the volume of tweets, and one person said that when they tapped the incoming notification, they tried to open a secondary window. MacRumors has been alerted to the problem by editor Mitchel Broussard, who has been using the app for more than a year. Before today, the app worked well and sent out no inappropriate content to users. We've never seen reports of an app sending out such notifications before, so it's quite unusual. Apple doesn't seem to have a solid reporting system in place for cases like this, as we found out after the announcement came out. UVLens has not yet commented on the situation. There's a Report a problem website to report problems with recently purchased iOS apps, but it doesn't work with older apps you've purchased that are suddenly being troubled. There's no app-specific outline button in the App Store, no option when 3D touches apps on start, and no clear support path to alert Apple to problematic apps. We contacted developer UVLens and more people posted complaints on Twitter so the app can be removed from the App Store or repaired in the near future. For now, customers who have installed UVLens will probably want to remove the app because it's not clear what's going on and if there has been a breach of any kind. Update: UVLens sent out another notice, apologizing for the explicit push notification. The company says it was not from the UVLens team and is being investigated. Update 2: UVLens tells MacRumors that a third-party push notification service that it uses has been compromised, allowing the sender of spam to send out inappropriate notifications over the network, including users of UVLens. UVLens says measures have been taken to prevent this from happening again and no software application has been compromised. Yet once again demonstrating the ingenuity of software hackers, two iOS devs have taken the second generation Apple TV and created a hack that allows them to run iOS applications through a device via an emulator. Their hope is that Apple will take note and be forced to create an app store that is usable in the device. Steve Troughton-Smith and Nick TheMudkip worked together on a jailbroken Apple TV code called MobileX, which takes advantage of the fact that the device is essentially iOS device under the hood. The new Apple TV, which features an A4 chip as well as a modified version of iOS 5, has the power to run apps seamlessly in an emulator. In videos demonstrating MobileX in action, the duo had Facebook, Angry Birds and YouTube running on their TV screens, as well as Cydia, a rogue app store for jailbroken devices. A video of the hack in action is embedded below. Before you go rushing to download a hack package to get some Angry Birds action on your TV, here's the bad news: Troughton-Smith says they're not releasing the hack to the public just yet. He does, however, say the team is giving away the right software libraries so the devs app can optimize their code for use with the Apple TV remote control. While apps aren't optimized using the libraries above, you can control the action on the screen using the Mac Magic Trackpad. Although this workaround sounds feasible, it can slow application performance down because it connects over a VNC connection. Simply put, trackpad must connect to the middle finger to talk to applications running in the emulator. I admire the fact that the team aims to achieve the lofty goal of being the catalyst that forces Apple to release the Apple TV app store. I think they will have their wish, but not because of the hack they created. With rumors of an all-in-one Apple TELEVISION set continuing to fly around, an app store dedicated to iOS-giving option TVs is most likely already in the works. It would also not be surprising if the upcoming iPad 3 could connect to these new display devices in more than just airplay display mirroring capacity. As you recall, Apple runs its App Store with an iron fist. And it will be a cold day in Cupertino in front of the company ... IOS and iPadOS 14.3 are here and seem to be safe to download. At least I didn't notice any major news about... There are many apps you can use to find gadgets in iOS 14. Don't go looking for a word... iOS 14.2 is here, and while it's not a crazy-gigantic update for your device, there are still a few fun features... In a perfect world, we could download apps from a centralized, secure app store on our phones, and these apps would... I like the many improvements Apple has made to messages in iOS 14 and iPadOS 14 - pinned conversations, nested replies,... Although the feature has been around for some time, many people used running iOS 14 to trick out... I don't facetime much, but I've often been accused of not appearing present in various video chats because... Update 9/21/20 3:00 p.m.: Well, that was fast! Gmail for iOS app update that brings it to version 6.0.200825... Tired of Safari on your iPhone or iPad? You can install many other great alternatives from the App Store-not... Apple today released iOS 13.7. Update your device and you'll now be able to see if your state supports... Is your iPhone screen looking for sick lately? Software Software can only be the medicine it needs. We'll be the first to say that worrying about someone who knows if you've read their text message is a bit... The Neirfy/Shutterstock iPhone has gained a reputation as a security-focused device thanks (in part) to Apple's iron grip on the ecosystem. However, no device is perfect when it comes to safety. So, can your iPhone be hacked? What are the risks? What it means To Hack iPhone Hacking is a free term that is often used incorrectly. Traditionally, it refers to illegally gaining access to a computer network. With respect to your iPhone, hacking can refer to one of the following: Access private information stored on your iPhone. Monitor or use your iPhone remotely without the owner's knowledge or consent. Change how your iPhone works with additional soft-or hardware. Technically, anyone guessing your passcode could constitute hacking. Installing monitoring software on your iPhone so someone can spy on your activities may also be something you would expect a hacker to do. There is also jailbreaking, or the act of installing custom firmware on the device. This is one of the more modern definitions of hacking, but it's also widely used. Many people have hacked their own iPhones by installing a modified version of iOS to remove Apple restrictions. Malware is another problem that's hit the iPhone before. Not only were apps in the App Store classified as malware, but zero-day exploits were also found in Apple's web browser, Safari. This allowed hackers to install spyware that circumvented Apple's security measures and stole personal information. Justin Duino Jailbreaking space moves fast. It's a constant game of cat and mouse between Apple and tweakers. If you keep your device up to date, you are most likely safe against any hacks that rely on the jailbreaking method. However, that's no reason to keep your guards down. Hacking groups, governments and law enforcement agencies are interested in finding ways around Protecting Apple. Any of them could discover a breakthrough at any time and not inform Apple or the public. RELATED: Can My iPhone or iPad Get a Virus? Your iPhone cannot be used remotely apple will not allow anyone to remotely control the iPhone via remote access apps like teamviewer. While macOS comes with a virtual network computing (VNC) server installed that allows the mac to be remotely controlled, if you enable it, iOS doesn't. This means you can't control someone's iPhone without jailbreaking it first. There are VNC servers available for jailbroken iPhones that allow this feature, but stock iOS is not. iOS uses a robust system of permissions to give an app explicit access to specific services and information. The first time you install a new app, you'll often be prompted to give location or camera permissions to your iOS camera. Apps literally can't access to this information without your express consent. There is no available on iOS, which provides full access to the system. Each application is quarantined, which means that the software is disconnected from the rest of the system in a safe sandbox environment. This prevents potentially harmful applications from affecting the rest of the system, including restricting access to personal information and app data. You should always be careful about the permissions you grant to the app. For example, an app like Facebook wants access to your contacts, but it doesn't require it to work. Once you grant access to this information, the application can do whatever it wants with this data, including uploading it to a private server and saving it forever. This may be in violation of apple developer and App Store developer agreements, but it's still technically possible for an app to do so. While it's normal to take care of attacks on your device from criminal sources, you're probably at greater risk of handing over your personal information to a secure app that's simply politely asked. Check your app permissions regularly for iPhone, and always think twice before agreeing to app requests. RELATED: 10 Easy Steps to Better iPhone and iPad Security Apple ID and iCloud Security Your Apple ID Account (which is your iCloud account) is probably more susceptible to external interference than your iPhone. Like any online account, many third parties can get hold of your credentials. You probably already have two-factor authentication (2FA) turned on on your Apple ID. Still, you may want to make sure by going into settings > [Your name] > password and security on your iPhone. Tap Turn on two-factor authentication to set it up if it's not already enabled. In the future, whenever you sign in to your Apple ID or iCloud account, you'll need to enter a code sent to your device or phone number. This prevents someone from signing in to your account even if they know your password. Even 2FA is prone to attacks of social engineering, however. Social engineering was used to transfer a phone number from one SIM card to another. This could hand the would-be hacker the last piece of the puzzle for his entire online life if he already knows his main email password. This is not an attempt to scare you or make you paranoid. However, it proves how something can be hacked if given enough time and ingenuity. You shouldn't worry too much about these things, but be aware of the risks and remain vigilant. What about iPhone Spy Software? One of the closest things to a hack to affect iPhone owners is so-called spy software. These applications prey on paranoia and fear by inviting people to install monitoring software on devices. These are marketed to concerned parents and suspicious spouses as a way to track someone else's iPhone activity. These apps can't work in iOS stock, so they require your device to be jailbroken first. The iPhone opens for the next security and potential app compatibility issues, as well as some app apps work on jailbroken devices. Once the device is jailbroken and a monitoring service is installed, people can spy on individual devices from web control panels. This person will see every text message they send, details of all calls and received, and even new photos or videos caught with the camera. These apps won't work on the latest iPhones (including XS, XR, 11, and the latest SE), and for some iOS 13 devices, only a tethered jailbreak is available. They've fallen from grace because Apple is so hard to jailbreak recent devices, so they pose little threat within iOS 13. However, it won't stay that way forever. With each great jailbreak development, these companies start marketing again. Not only is spying on a loved one questionable (and illegal) jailbreaking someone's device also exposes them to the risk of malware. It also void any warranty he or she might leave. Wi-Fi can still be vulnerable No matter which device you're using, unsecured wireless networks still pose one of the biggest threats to mobile device security. Hackers can (and do) use the man at the center of the attacks to set up fake, unsecured wireless networks to intercept traffic. By analyzing this transmission (known as packet sniffing), the hacker may be able to view the information you send and receive. If this information is unencrypted, you can keep passwords, login information, and other sensitive information. Be smart and avoid using unsecured wireless networks and be mindful whenever you use a public network. For maximum peace of mind, encrypt your iPhone traffic with a VPN. Vpn.