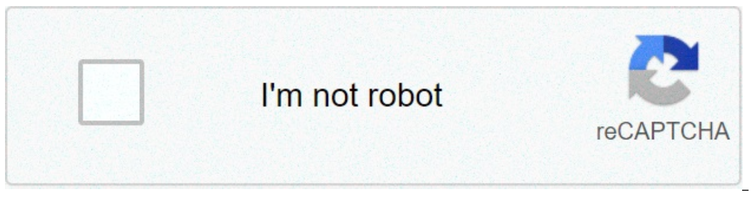

Continue

Reset iphone without lock screen passcode

If you have smartphones or tablets with fingerprint scanners, being able to access your devices with touch or swipe is a wonderful convenience. On the other hand, this simplicity makes it easy to forget your password and PIN number. This is a problem if your phone or tablet requires a PIN on the lock screen. However, there are multiple ways to remotely unlock Android. These instructions apply to most Android devices manufactured by Samsung, Google, Huawei, Xiaomi and others. Samsung Find My Mobile option works only with Samsung phones. Lifewire There are several ways to remotely unlock Android when you can't get past the lock screen. To get access to Android, reset your PIN or password remotely, wind up your phone to change settings, or reset your phone. The Google Find My Device web app has for years enabled users to change their lock screen PIN. It's not an option anymore. Now it's only possible to use Find My Device to locate your phone or tablet using the web or other device and send a message to the screen in case someone finds your lost device. This doesn't mean you won't be able to remotely unlock Android. It just means it's not going to be that easy. You still have options. If you own a Samsung Android phone or tablet, and if you have registered a device in a Samsung account, you are in luck. Use Samsung Find My Mobile to reset your lock screen. To enable remote unlocking on Android with

Samsung Find My Mobile: Go to Settings on your device. Choose Lock Screen and Security. On some Samsung devices, you may need to choose security or biometric and security protection. Choose Find My Phone. Choose Add account and sign in to your Samsung account. Turn on the remote controls. To unlock your device, go to the Samsung Find My Mobile website and sign in. Choose Unlock. Screen lock information on your device is deleted. This could be the pattern, PIN, password, or biometrics you originally set. If you're using an older version of Android, especially Android 4.4 KitKat or older, the lock screen reset option is built into the lock screen itself. Simply enter the wrong pattern or PIN five times and you will see forget the pattern or forgot the PIN message. Select a message and sign in to your Google Account to reset your lock screen. One of the easiest ways to reset the lock screen is to use the special commands available with Minimal ADB and Fastboot. The catch is that this method works only on rooted Android phones. This advanced feature edits the database on your phone where the lock screen PIN is stored. If you're not familiar with Android cheerleading or uncomfortable working with Minimal ADB and Fastboot, skip this option. If you've never used this tool before, take some time to learn all about setting up minimum ADB and Fastboot and connecting to your phone using USB After following the instructions to enable USB correction of document documents and you have a window open with minimal ADB commands, enter adb devices to confirm that you are connected to your phone. Enter the adb shell and select Enter. Enter the following commands one line at a time. Select Enter at the end of each line. cd /data/data/com.android.providers.sq update system set value=0 where name='lock_patte update system set value=0 where name='lockscreen.lockedout Restart phone and lock screen will be reset. If nothing else works, you have a last resort to recover your device. You'll need to delete the device and start over. The downside of this is that you will lose all the data and files that are stored on it. The upside is that you won't have to buy a new phone or tablet. It is possible to make a factory reset in recovery mode if you can't get past the lock screen. However, the faster and simpler method is to use Google Find My Device to completely delete your device. Turn on the device. In your web browser, go to the Google Find My Device website. Select the Android device you're currently locked from. In the left panel, select Delete Device. In the delete device pane, read the alerts, and then select Delete Device. You may be prompted to sign in to your Google Account before starting the deletion process. After deleting your phone or tablet, it automatically restarts. The next time you start your device, sign in to your Google Account and set it up like you did when you first bought it. Thank you for telling us! Tell us why! Author: Adrian Grahams Not all iPhone apps work well with screen rotation, and some apps don't rotate because they're designed to work specifically in landscape or portrait mode. If you don't think the screen in the iPhone app is turning, the screen lock may be in place. Turn off screen rotation lock on your iPhone from the status bar at the bottom of the Start screen. Double-press the Home button under the iPhone screen to display icons for recently used apps in the status lower bar. Swipe the status bar from left to right until you see the screen lock icon, which is a padlock inside the circular arrow. Tap the screen lock icon to turn off the screen lock. The lock icon will disappear and the screen rotation should be unlocked. Press the Home button again to return to hide the status bar. An app you know allows you to rotate your screen, such as the Calculator app, has been launched. Rotate your iPhone to make sure the calculator screen also rotates. If the screen moves as expected, you have successfully removed the lock. If the screen stays locked, press and hold down the On/Off key, and then swipe the Slide to Power Off tab to turn off your iPhone. Press the On/Off button to turn on your iPhone. With iOS 12 and iPhones that have Touch ID, you can still bypass iPhone screen and trick Siri into getting into a person's phone. The detour is the same as it was in earlier versions of the operating system: Press the home button using a finger that is not associated with fingerprint authentication, prompting prompting to wake up. Tell Siri: Mobile data. Siri then opens mobile data settings where you can turn off cellular data. As was the case before, anyone can do it. It doesn't have to be the person who trained Siri.By also excluding mobile, you cut off Siri's access to mobile networks. You will receive an error that says: Siri is not available. You are not connected to the Internet. But you don't care about this error because you've already bypassed the iPhone lock screen. However, if the device is on a Wi-Fi network, this connectivity will remain. Other privacy loopholes remain for Touch ID devices with iOS 12Still problem for iPhones that have Touch ID: Anyone can use Siri to read your new/unread text messages, send text messages, send emails, and see your latest phone call. To do this, again encourage Siri to wake up with a finger that is not associated with phone authentication. Then say Read messages, and Siri will read all unread text messages from the lock screen. Say: Send a text message [person's name], and Siri will allow you to dictate the message and send it. Say: Show me recent calls, and Siri will show your latest phone call. Say: Send an email in the [person's] name, and Siri will allow you to dictate the email and send it. Apple patches privacy holes on the phones of the iPhone X series Apple has patched a privacy loophole with the iPhone X series phones, which all use Face ID to unlock the phone. There is no way to force Siri to activate on these devices and allow non-owners to access text messages, phone call logs, emails or other apps. Furthermore, future iPhones will have Face ID. Touch ID, while still supported on iPhones up to the iPhone 8 series, won't be included on new devices. Lock your privacyUntil Apple patches a privacy hole on iPhones that have Touch ID - or until you can upgrade to an iPhone X Series device - the best option is to disable Siri from the lock screen. ----------Update for iOS 11S iOS 11, you can still bypass the iPhone lock screen and trick Siri into getting into a person's phone. The bypass is the same as it was in an earlier version of the operating system: Press the home button using a finger that is not associated with fingerprint authentication, prompting Siri to wake up. Tell Siri: Mobile data. Siri then opens mobile data settings where you can turn off cellular data. As was the case before, anyone can do it. It doesn't have to be a person who Siri.By and turn off Wi-Fi, you cut off their connectivity access. You will receive an error that says: Siri is not available. You are not connected to the Internet. But you don't care about this error because you've already bypassed the iPhone lock screen. Other privacy loopholes remainAlso is still a problem: Anyone can use Siri to read your new/unread text messages send text messages and see your latest phone call. To do this, again encourage Siri to wake up with a finger that is not associated with phone authentication. Phone. Say: Read messages, and Siri will read all unread text messages from the lock screen. Say: Send a text message [person's name], and Siri will allow you to dictate the message and send it. Say: Show me recent calls, and Siri will show your latest phone call. Facebook's privacy loophole closedApple closed the loophole that allowed you to order Siri to post on Facebook. Now, she tells you she can't do it and gives you a button to open Facebook. You must enter a passcode for the device to open the application. Lock your privacyUntil Apple patch a hole that allows you to bypass the lock screen and allows you to command Siri, the best option is to disable Siri from the lock screen.----------iOS 10.3.2Apple has not yet patched the hole allowing you to bypass the iPhone lock screen. From iOS 10.3.2 (and beta version 10.3.3), you can still trick Siri into entering the iPhone.It like this: Press the home button using a finger that is not associated with fingerprint authentication, prompting Siri to wake up. Tell Siri: Mobile data. Siri will then open mobile data settings where you can turn off cellular data. Anyone can do this – it doesn't have to be the person who trained Siri.By also turn off Wi-Fi, you cut off their connectivity access. You will receive an error that says: Siri is not available. You are not connected to the Internet. But you don't care about this error because you've already bypassed the iPhone lock screen. Not only can someone trick Siri into turning off mobile data, but they can trick her into reading unread text messages and posting on Facebook - a major privacy issue. To do this, again encourage Siri to wake up with a finger that is not associated with phone authentication. Then say Read messages, and Siri will read all unread text messages from the lock screen. Or say: Post on Facebook, and Siri will ask you what you want to post on Facebook.We tested this with iPhone 7 staff, with someone other than the owner of the iPhone giving the commands. Siri let a person make him at home. While we wait for Apple to patch the hole, your best option is to disable Siri from the lock screen.----------iOS 9 screen lock bypass vulnerabilityThere are more bypass vulnerabilities that could allow an attacker to get past the passcode lock screen on Apple devices with iOS 9.Details for four different attack scenarios were revealed by Vulnerability Lab. It is worth noting that the attacker would need physical access to the device in order to perform this; this, said, the advice says hacks were successfully executed on iPhone models 5, 5s, 6 and 6s as well as iPad models Mini, 1 and 2 with iOS 9 versions 9.0, 9.1 and 9.2.1.Security researcher Benjamin Kunz Mejri, who about a month ago discovered a different method for disabling lock screen codes on iOS 8 and 9, revealed flaws. The Vulnerability Lab has released a proof-of-concept video showing more new ways to locally locally bypass the iOS 9 code and gain unauthorized access to the device. Local attackers can use Siri, an event calendar, or an available hourly module for an internal request to connect a browser to the App Store that is able to bypass the coupe's passcode or fingerprint protection mechanism, according to the post. Attacks exploit vulnerabilities in the App Store, Buy multiple tones or time channels of watch connections, event calendars, and the Siri user interface. There are four attack scenarios explained in the discovery and shown in the proof-of-concept video; each starts on an iOS device with a locked passcode. The first scenario involves pressing the Home button to activate Siri and asking it to open a nonexistent app. Siri replies that you don't have such an app, but it can help you search for it on the App Store. Tapping the App Store button opens a new restricted browser window. Select the update and open the last app, or double-click the Home button to make the task slide appear. Swipe towards the active task on the front screen and this bypassed the passcode lock screen on iPhone 5, 5s, 6, and 6s models. The second scenario is similar, first pressing the Home button for two seconds activate Siri, and then ask to open the watch app. Switch to the world clock in the module below and tap the image for the Weather Channel LLC network; if the weather app is deactivated by default, a new restricted browser window will open that has App Store menu connections. Click the update and open the last app, or double-tap the Home button to get an overview of the task slides. Swipe towards the active front screen and voila — the passcode lock screen bypassed again; it reportedly works on iPhone models 5, 5s, 6 and 6s. The third attack scenario works on iPad models 1 and 2, but basically follows the same steps as the second scenario to bypass the passcode and gain unauthorized access to the device. The fourth way around a lock screen passcode involves forcing Siri to open by pressing the Home button and asking it to open the Events/Calendar app. An attacker could tap the Information of Weather Channel link located at the bottom of the screen next to the Tomorrow module. If the weather app is deactivated by default, a new restricted browser window opens with links in the App Store. Tap the update and open the last app, or double-click the Home button to update the slide overview of the task. Swipe to select the active front screen, and the code on the lock screen is bypassed. Although Apple's security team was reportedly notified on January 4, there are no specified dates in the vulnerability detection timeline for Apple's response or patch development. Vulnerability Lab suggested the following temporary solution for users to harden device settings: Deactivate siri module settings menu Also deactivate the Event Calendar without a code to disable the Weather Channel LLC nudging feature. Deactivate in next step step control panel with timer and world clock for disarming exploitation. Activate the weather app settings to prevent redirection when the module is disabled by default in the event calendar.