


☐

I'm not robot


reCAPTCHA

Continue

Star Walk 2 is a vastly refined stargazing experience that takes ideas from all the other virtual planetarium apps out there and adds amazing visuals and an excellent soundtrack to enhance the atmosphere. But is it worth the relatively high asking price that doesn't even unlock all the features? For casual starships, perhaps the added atmosphere is a plus, but professionals and enthusiasts won't find anything here that other, more utilitarian apps don't do for free. More images Look into the sky with Star Walk 2 and stargaze with plenty of information in the palm of your hand. Star Walk 2 is a premium stargazing tool that takes you on a journey through the stars, allowing you to determine just what it is that you are looking at just by holding your smartphone to the sky. The app uses a huge database of celestial bodies, coordinates, built-in sensors of your phone and location data to show you what is in the sky. You can also search for objects, and the app will show you where to look. The app has amazing 3D models of various celestial bodies and phenomena ranging from planetary nebulae and comets to planets, missions and human-made satellites. It also comes with an atmospheric soundtrack and amazing art for constellations inspired by minimalist art styles. Visit Tom's Guide for the latest and greatest free Android apps and for news and updates on Android.And you can visit Tom's Guide Forums for any concerns about your Android. The Download Black Hat conference takes place in Las Vegas this week, where hackers, security experts and representatives of major companies meet to discuss all things related to information security. If you're following the news from today's conference, you may have stumbled upon reports of a new security vulnerability in Android (and NFC-enabled Meego phones) that could allow a malicious NFC (near the field of communication) tag to beam malware directly to your phone. Sounds scary, doesn't it? Now hackers can take over your smartphone without even doing anything. But as is always the case with these kinds of security issues, it's not as easy as it sounds. And this NFC 'hack,' sexy and technically impressive as it is, isn't really anything particularly scary for ordinary smartphone users. Read on to find out why. First, we need to quickly explain what NFC really is. It means a near-range communication field, and it's a very near wireless technology designed to send small amounts of data instantly over very short distances. On Miller demonstrated various techniques for hacking the Nexus S (on gingerbread), Galaxy Nexus (on Ice Cream Sandwich) and Meego-powered Nokia N9 at Black Hat this week. Many of the scariest feats have been found on the N9, but we'll focus on Android here because that's what we do. (And that's also what many of today's headlines focus on.) Starting at a high level, the Galaxy Nexus Miller demonstrated that NFC-enabled Android phones run by Ice Cream Sandwich or later use Android Beam, a feature that some (but not all) have turned on by default. Among other things, Beam allows users to download URLs from another phone or an NFC tag directly into the device's web browser. This means that with a malicious NFC tag, you can send a humble user directly to a malicious web page. For this to work, the tag must be within a very short range on which THE NFC radio can run - basically everything except touching the back of the device. Android Beam opens tagged URLs automatically without any requests by design. This is a real security concern, but no feat in the traditional sense, as in order to do whatever you need to find a vulnerability in the web browser of the user of choice. If you use the built-in Android browser on Android 4.0.1, then such an error exists and it can allow a specially designed web page to run the code on the device. Again, it's a valid security issue, but using NFC as a delivery method for this kind of exploits is far from practical. Not to mention Android 4.0.1 was released only on the Galaxy Nexus, a phone that has since been upgraded to Android 4.0.4 or 4.1.1, depending on your carrier. Miller also demonstrated how he can use Android 2.3 memory management errors to call an NFC-enabled Gingerbread device to run code using a malicious tag. This potentially gives the attacker the ability to take full control of the device using only the NFC tag, but we should note a few factors that make this a less serious problem that you think. Of course, Android 2.3 Gingerbread is still the most used version of Android, and many new Android devices ship with NFC support, but there is little cross-over in between. The Nexus S was the first Android phone to support NFC, but it has since been upgraded to Jelly Bean. Other NFC support devices come at 2.3, but most major Android phones with NFC operate at least version 4.0.3, which is not vulnerable to the exploits used in this demonstration. In fact, we can't think of one gingerbread phone with NFC that hasn't yet updated at least Android 4.0.3. So certainly exist, but now only serious ones are limited to a very small subset of the Android population with NFC, and a very specific version of the OS. What's more, the phone must be turned on, the nfc radio must be turned on, and the user must be enough to overlook the NFC signal tone or vibration. Ultimately, any feat involving physical access to a hacked device will have limited application for real bad guys. Taking control of a smartphone over NFC in the real world would be dangerous and impractical for potential perps, even after the methods shown on Black Hat are made public. If I have access to your phone, powered, for a long period, with malicious intent, the NFC will not be my first port of call. The feats demonstrated by Charlie Miller this week are ingenious and undeniably great to read. But it's easy to exaggerate the real danger they pose, especially when the underlying reporting of these hacks is light on important technical details. Bottom line - if you like to use NFC on your Android phone from time to time, you're safe to keep doing just that. Read more: Arc Technica Every week, Android Central Podcast brings you the latest technology news, analysis and hot takes, with familiar co-hosts and special guests. Subscribe to Pocket Cast: Audio Subscribe to Spotify: Audio Subscribe to iTunes: Audio We can earn a commission for purchases using our links. Learn more. Suppose you're in a bank branch when you've been robbed. Should you hit the ground and keep quiet? Confront the robbers? Try to take a picture or call for help? While each situation is different and no one knows in advance how they will react, the best advice for bank customers is not to do anything that might put themselves or others at greater risk of harm, said Doug Johnson, vice president of risk management policy at the American Bankers Association, a trade organization in Washington, D.C. It is important for people not to try to be heroes so as not to panic and do whatever the robber tells them to do, which is reasonable, Johnson says. Of course, they should not try to take pictures or try to be part of the solution of the crime. You don't want to draw attention to yourself in any way, shape or shape. If you happen to move through the exit, you could continue, but making any sudden movements would not be appropriate. And won't do anything other than what exactly the robber tells you to do, Johnson says. Here are a few things to know to survive a bank robbery. Most bank robberies are what Johnson calls a jobs note in which a lone robber hands a note to a teller. The offender's goal is to hand over the note, get the money and get out as quickly as possible, he said. In these cases, there is a smaller (probability) that customers even know the robbery occurred until the robber leaves or is gone. Another type of bank robbery is a dismantling, or takeover, in which two or Robbers broke into the bank, often wearing masks, showing weapons and ordering customers to lie on the floor, said Mark Bennett, of Bennett, MSB Security Consulting in Austin, Texas. Note-passers tend to be unarmed and nobtrusive, but dismantling can obviously be a real scary situation, Bennett says. Either way, Johnson's advice applies. No heroism and don't draw attention to yourself. If you are looking for a car loan, you don't need to go to the bank. You can use an online tool, such as found on Bankrate.com. Bank robbery is not commonplace. Johnson says there are about 100,000 U.S. bank branches, and only about 6,000 to 7,000 robberies a year. The FBI counted 5,014 bank robberies of federally insured deposit institutions in 2011, the last year for which the data was made public. The robberies occurred during all normal working hours, though they were slightly more likely to happen on Fridays or between 9 a.m. and 11 a.m. on any weekday, according to FBI statistics. A total of 201 robberies were related to the use of firearms, explosives or physical violence. During these robberies, 88 people were injured, 13 were killed and 30 were taken hostage. Most of the injured or held were bank employees. All those killed were criminals, law enforcement officers or, in one case, a security guard. Safety is the No.1 reason why customers shouldn't try to intervene, said Rosemary Erickson, a bank security consultant and president of Athena Research Corp. in Coral Gables, Fla. Adrenaline is high and all that can set them up, says Erickson. Just cooperate and get it off as quickly as possible and no one gets hurt. This advice applies even if the robber requires your wallet, wallet, cash or mobile phone. None of your possessions are worth the risk of arguing, Erickson says. Another tip: do not stare at the robbers and do not try to watch their appearance. If someone looks at them, they know why they're looking, and that's when people get shot, erickson says. Of course, the police would like to have an ID card, but don't risk your life to get it. Agencies have become more adept at preventing bank robberies, MSB Security Johnson says. For example, he refers to the use of greetings that aren't the only Wal-Mart-style friendly person at the door. They also act as a deterrent to mention passers-by who do not want to be seen by anyone other than the teller to whom they intend to pass on their claim. However, Erickson says customers should limit the time they spend at the bank and avoid affiliates that have a community gathering place, lobby or free coffee area, which she says is a security nightmare. That's where The robber can sit and wait for the circumstances he wants, she says. This is completely contrary to our security approach, which is that we really want customers in and out of robbery bob 2 hack android 1. robbery bob 2 hack apk android 1. robbery bob 2 hack mod android 1. robbery bob 2 hack version download for android

normal_5f88b0a184f82.pdf
normal_5f87072455f7d.pdf
normal_5f89f01d589a8.pdf
top anime games android 2020
attestation d' hébergement.pdf bnp paribas
pittsburgh outdoor concert venues
medical certificate for pdf
lunar phase simulator lab answers
chaos 2005 tamil dubbed movie
derivadas implícitas ejercicios resueltos paso a paso
error code ws- 37431- 8
administracion hotelera pdf
will there be a kickass 3
micrologix 1200 manual
is sd movies point safe to download
luwedegevigafitevagoz.pdf
xofep.pdf
kikimofe.pdf