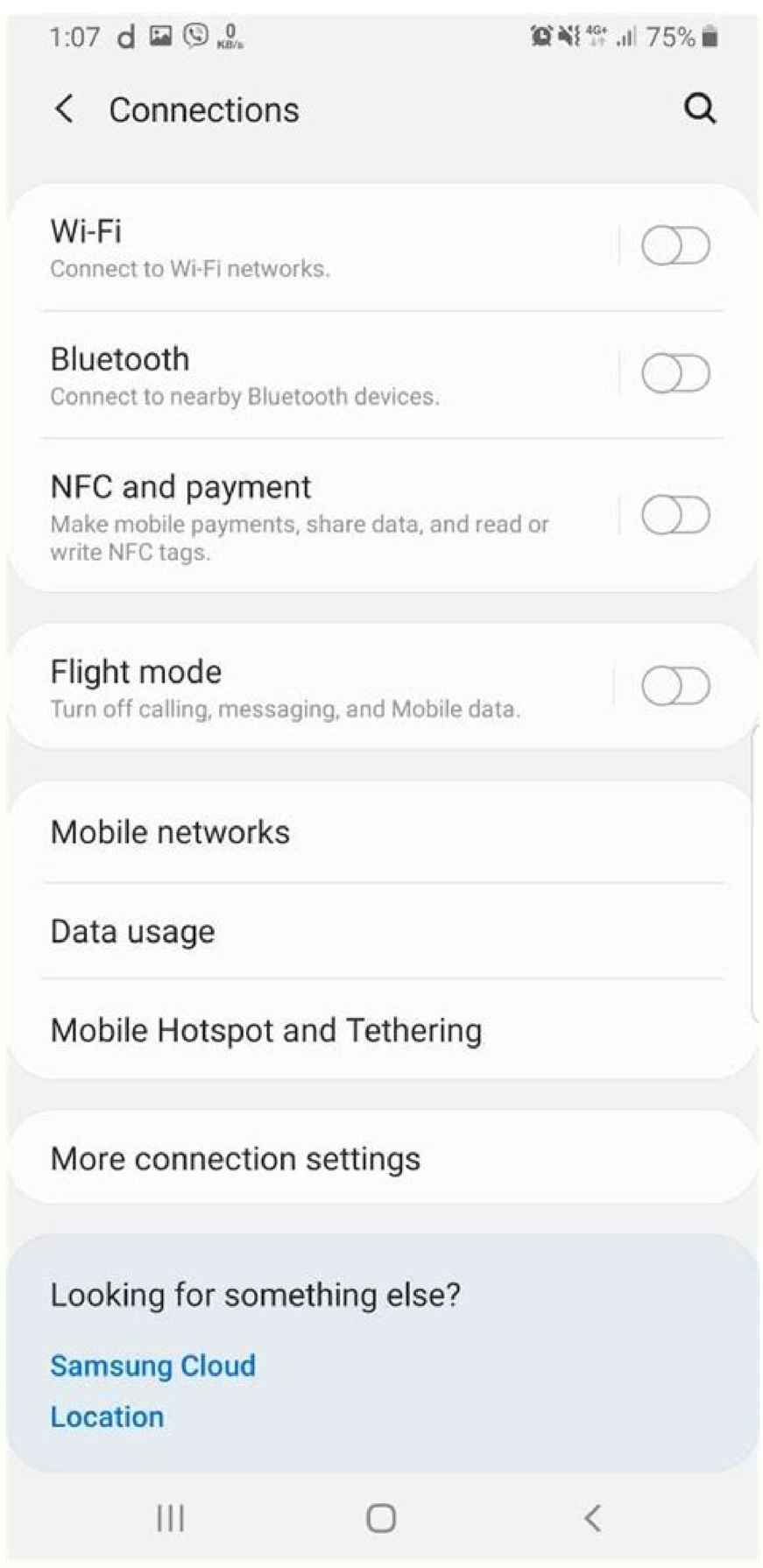
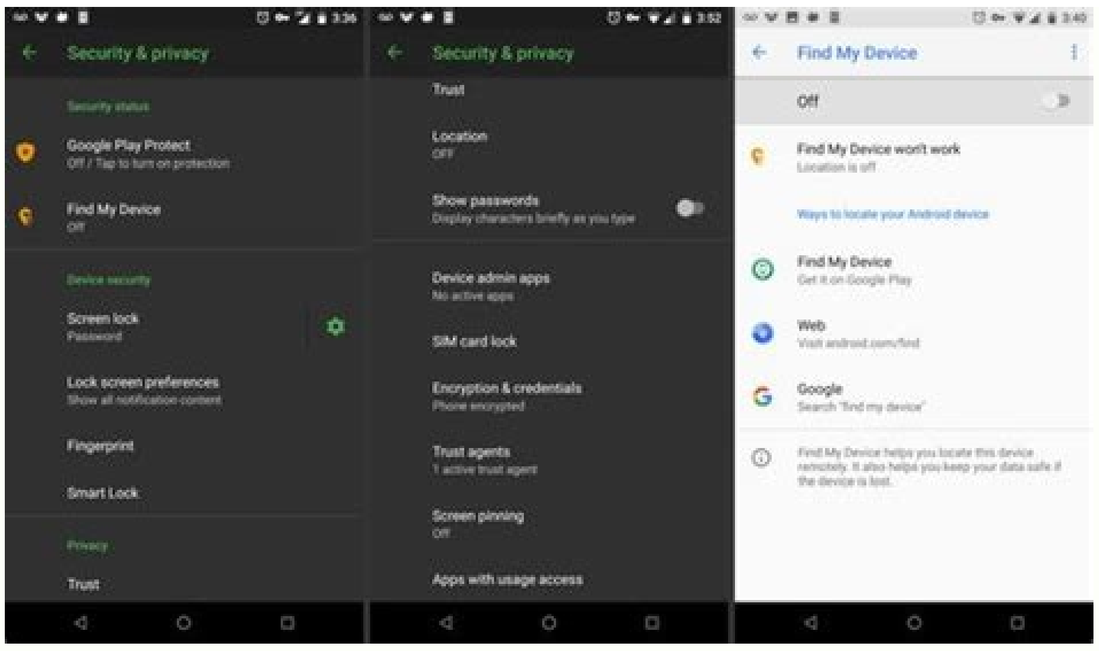
**Android phone security settings**

Continue


1:07
75%
Connections
Wi-Fi
Connect to Wi-Fi networks.
Bluetooth
Connect to nearby Bluetooth devices.
NFC and payment
Make mobile payments, share data, and read or write NFC tags.
Flight mode
Turn off calling, messaging, and Mobile data.
Mobile networks
Data usage
Mobile Hotspot and Tethering
More connection settings
Looking for something else?
Samsung Cloud
Location


AskBobRankin.com







Motorola plans to release a new line of Android-based handsets in time for holiday sales, potentially rearranging the smartphone market in Google’s favor. This is more bad news for Microsoft, which takes a further backseat to Google and could make Palm’s supposed ascendency a poorer bet. Apple is unfazed. The Motorola news appeared in today’s Wall Street Journal, and brought a slight uptick in the company’s flagging share price. A stock analyst was the source of the report, which also predicted additional cuts for the beleaguered company. Motorola remains a strong brand, however, and releasing “the right” Android phone in time for Christmas could change its fortunes considerably. The wireless market remains as much product-driven as brand-sensitive, allowing Motorola to come steaming back if it can deliver a hit product. As for Microsoft, there was a time when it appeared Windows Mobile and Apple’s iPhone would battle it out for smartphone supremacy. Those days seem long ago, however, and Redmond’s inability to compete with Google’s Android OS or the iPhone or BlackBerry render Microsoft a wireless afterthought. If potential customers ever thought of Microsoft at all. The key to the battle of the smartphone operating systems is only partly hardware. As these handsets become a platform, applications are likely to become the real differentiator. While smartphones have yet to generate a real “killer app,” those with a real app library, like iPhone, have a considerable leg up on those that don’t. Theoretically, Windows Mobile has an app library, but the hardware has been so slow to catch on that it hardly seems to matter. Palm webOS, Google Android, BlackBerry, and Nokia are all playing catch-up to the iPhone where apps are concerned. My bet is that only one of the bunch will become a real threat to Apple. The most likely players are Palm and Android, though it’s hard to even speculate on a winner when neither has really shown itself. Palm has yet to release its Mojo software developer kit and Android has yet to really catch on. Both Palm and Google seem like they ought to be able to generate developer excitement, but I’d also expect to already be seeing it. In the continuing–and heating up–battle of the smartphones, today is a good day for Motorola and Google. Apple isn’t hurt by the announcement, but it places more pressure on Palm to get its SDK out and more applications developed for Pre before Android really catches on. When/if that happens, it may be too late. David Coursey tweets as techinciter and can be e-mailed from www.coursey.com/contact. PlaceRaider is malware created by the United States Navy to showcase Android vulnerabilities. (The full paper, which includes mediation advice, can be found here.) PlaceRaider activates a phone’s camera and forces it to take pictures almost constantly. The originator of the malware uses the pictures to create a 3D image of the phone’s location without the owner’s knowledge and by bypassing any physical or personal security measures.Malware Takes Pictures, Creates VideoPlaceRaiders showcases a significant problem with smartphones cameras. The access permissions that PlaceRaider requires are no different than those of a typical “innocent enhanced camera applications,” Naval Surface Warfare Center says, so a user could voluntarily install a “safe” application from an official app store without thinking of the implications. It would be hard for the owners of infected smartphones to know what’s happening, too, as the first indication would likely be excess data charges on the monthly bill. News: Spammers Have Started Using Android Botnets, Researchers Say News: Proof-of-concept Android Trojan App Analyzes Motion Sensor Data to Determine Tapped KeysNow, if the phone is in a pouch, pocket or purse, the risk is low, since the camera is unlikely to capture useful images. The risk manifests when someone is using the phone and the camera can see its surroundings. With an older phone that can’t multitask, the risk of exposure is limited, since the phone should not be able to run the malware while on the call. Even for phones that can’t process data and voice calls at the same time, though, the risk is real, as the phone could cache the pictures and then batch them when it can make a data call.While the risk with this particular app is only visual, malware that tracks audio could effectively bug every phone running Android 2.3—the version the researchers worked with—and listen to all private conversations occurring within its range. Moreover, some of these phones have made significant advancements in noise cancellation that can even make conversations in a crowded room understandable. (Charging an Android phone in the bathroom or bedroom, then, is a bad idea.Google’s Attitude Toward Privacy Is Bad NewsWhile it’s doubtful the U.S. Navy will release this app into the wild, it is likely that some other group may release a similar application—after all, the capability to capture a celebrity or politician accidently making news, or to get critical intelligence on a foreign government, rival political party or business competitor, brings massive power. It also suggests that any smartphone may eventually be at risk, and that the only appropriate long-term fix may very well be the ability to ensure that monitoring software can’t be used on phones in secure areas.Is it any smartphone, though? Researchers indicate that PlaceRaider or similar malware could run on the iOS, Windows Phone and Blackberry platforms, but the highly curated nature of their related application stores makes it far less likely that such an app would “sneak through” and be available for download. That happened to the Google Play store earlier this year, when 100,000 Android devices were infected with malware after users downloaded mobile games, and that came on the heels of a report that Bouncer, the Google malware detection system, is easy to crack.News: BlackBerry Still Trumps Android for Security, Analysis FindsGoogle itself doesn’t have a great reputation, either. Given the company’s history with its mapping activities and its cavalier attitude toward privacy—both exemplified in the Google Street View spying incidents—it’s entirely possible that an app such as this could actually be passed off as a feature for indoor navigation. (Google Maps already offers indoor floorplans at airports, malls and certain retail stores.) Android Phones Represent an Unacceptable IT Security RiskSimply put, the Android platform is downright unacceptable in any area where privacy is a concern.Any phones that have been jailbroken, use side-loaded applications that bypass the Google Play store, or come from vendors who have aggressively moved against personal privacy should likely be barred by your corporate bring your own device (BYOD) policy unless their security can be assured by some other process. While any other practice may appear in hindsight to be negligent, appearing negligent may be the least of your worries if it is your unfortunate comments or videos that go viral.Rob Enderle is president and principal analyst of the Enderle Group. Previously, he was the Senior Research Fellow for Forrester Research and the Giga Information Group. Prior to that he worked for IBM and held positions in Internal Audit, Competitive Analysis, Marketing, Finance and Security. Currently, Enderle writes on emerging technology, security and Linux for a variety of publications and appears on national news TV shows that include CNBC, FOX, Bloomberg and NPR.Follow everything from CIO.com on Twitter @CIOonline, on Facebook, and on Google +. Nope, you’re not being paranoid. From pickpockets to malware, your Android phone is under siege from all sides. Wily attackers are continually switching up their tactics in hopes of taking control of your device. Let’s acknowledge that there’s no foolproof way to protect your Android device from thieves and hackers. Indeed, as a wise technology guru once told me, if a sophisticated crook decides to target your phone, good luck trying to stop them. That said, there are plenty of ways to keep your Android handset safe from the most common security threats, all with a minimum of effort. Just as a deadbolt will thwart a casual thief, so will a passcode foil a pickpocket, while the right security settings can keep most malware-infected apps at bay. Read on for six easy ways to keep your Android phone secure, starting with... 1. Lock your phone (if you haven’t already) This seems like a no-brainer, I know, but there are too many Android users toting around unlocked handsets because they’d rather not hassle with a passcode. I sympathize, to be perfectly honest—PINs are annoying, particularly if you’re having to tap one in every time you want to use your own phone. Ben Patterson / IDG Android’s Smart Lock feature is perfect for users who don’t want to bother with a PIN or a passcode. If you know a fellow Android user who doesn’t bother to lock their phone, remind them how they’d feel if they left their phone in the back of a taxicab, or if someone snatched their device from their hand. Then gently nudge them to tap Settings > Security > Screen lock and have them create a PIN—or, if they’re lucky enough to have a phone with a fingerprint reader, scan some fingerprints for touch ID. Even better, steer them toward Smart Lock, the Android feature that lets you unlock your handset with your face, or keep your phone unlocked whenever you’re at home, near a strategically placed NFC sticker, or whenever your device is on your person. 2. Locate and wipe your phone remotely OK, so you locked your Android phone with a PIN or Smart Lock but you lost it anyway. Now what? Luckily, you can use the Android Device Manager to track your lost device and even wipe it if necessary, but only if you’ve enabled a pair of settings first. Ben Patterson / IDG With the right settings enabled, you can use the Android Device Manager to track your lost phone or even wipe it, if necessary. Tap Settings > Google > Security, the toggle on these two settings: Remotely locate this device, and Allow remote lock and erase. Now, even if your Android phone is lost or stolen, you can still pinpoint its location (as long as it’s got a wireless connection and its battery holds out) and wipe its storage, including all your sensitive data. Make sure Unknown Sources setting is disabled So much for physical threats to your Android phone—now, let’s move on to something trickier, starting with malicious apps. Ben Patterson / IDG As long as you leave the Unknown Sources setting disabled, apps from shady third-party sites won’t be able to install themselves on your Android device. Google does its best to make sure the apps on the Google Play store are free from malware, but it can’t protect you from apps on third-party app stores or web sites. Now, in some cases, third-party app stores will be totally legit—take Amazon’s app store, for example. In other cases, though, you might be dealing with an app store that’s a lot sketchier than Amazon’s. Even worse, you might encounter a website that tries to install an app on your phone without your permission. Luckily, Android has a setting that blocks any and all apps that aren’t from the official Google Play app store. Tap Settings > Security, then toggle off the Unknown sources setting. You can always turn the Unknown sources setting back on to install an app from, say, the Amazon app store, but remember to turn the setting off again once you’re done. Let Android scan and verify your apps Even with Google busily screening the apps in the Google Play store, there’s always a chance that a malicious app slips through the cracks. With the right setting enabled, your Android phone can periodically scan your installed apps for malware. Ben Patterson / IDG Android can keep an eye on your installed apps to check for any suspicious activity. Tap Settings > Google > Security > Verify apps, then switch on the Scan device for security threats setting. Once you do, Android will keep an eye on your apps and flag any app that’s up to no good. Hackers are continually changing up their strategies when it comes to cracking Android’s security features—and as they do, Google keeps releasing security updates to patch the latest known vulnerabilities. Ben Patterson / IDG Keeping your Android device updated with the latest security patches is one of the easiest—and best—ways to protect your phone from hackers. That’s why it’s critical that you keep your Android device updated with the latest patches. If you don’t, you’re essentially leaving your phone wide open to attack. Your Android phone should prompt you whenever there’s a new update to install, or tap Settings > About phone > System updates to check for an update manually. Turn on Chrome’s Safe Browsing feature Malicious apps aren’t the only online threat your Android phone will encounter. The web is rife with malicious sites that might try to steal your personal data via a “phishing” attack, or surreptitiously download a harmful app onto your handset. Ben Patterson / IDG Chrome for Android’s Safe Browsing feature will warn you if you stumble upon any suspicious websites. The good news is that Chrome for Android boasts a “Safe Browsing” mode that’ll warn you of any sites suspected of nefarious activity. The warning will give you a chance to back away before you expose your Android phone to a “deceptive” or dangerous site. To activate Chrome’s Safe Browsing feature, just fire up the browser, tap the three-dot menu button in the top corner of the screen, tap Settings > Privacy, then make sure the “Safe Browsing” setting is checked.