Norton™ by Symantec

GOOD, BAD, AND SNEAKY: DO YOU REALLY KNOW WHAT YOUR APPS ARE DOING?

Apps are fun, productive, and free, but they can also hit you with hidden costs and bad behavior. Stop reacting to the risks and start a new proactive approach to your mobile protection.

Contents

Introduction 3

Bad apps are just that 4

Grayware can be risky, too 6

Norton Mobile Insight never sleeps 7

Data: The more you have, the more you know 8

Advanced, proactive protection is needed in today's app-happy world 9

Boldly go with the Norton solution 9

Today, smart mobile devices have become ubiquitous. Globally, nearly 1.8 billion people, or one quarter of the world population, own a smartphone.[1] As mobile device use grows, so does app use.

Smartphone owners around the world now spend 86 percent of their time using apps and just 14 percent on the Web.[2] Globally, the average number of installed apps is 26 per phone, and among the top 10 countries, it's more than 35.[3]

Apps enable freedom by allowing you to do the same things on your mobile device as on your PC—and in new and different ways, as we move toward the Internet of Things. For example, you can already use apps to control the temperature in your living room, turn the lights on before you get home, and keep your home safe from intruders.

Apps make things happen. If your phone is the vehicle, apps are the steering wheel, the gas pedal, and the turn signal. They're also the key that opens the door to all the information your mobile device holds—and all the information you might be storing in the cloud.

Cybercriminals have taken note. Your personal information is worth money, and hackers are increasingly using tried-and-true tactics (such as fake apps and ransomware) to target mobile devices. And they're not the only ones. Money-hungry app developers are also after your personal information. Their goals are not necessarily illegal. They may simply be trying to insert targeted ads in your notification bar. But their methods can present risks.

Given that there are so many parties interested in getting at your private information, it's more important than ever that you know what your apps are doing and take steps to keep your mobile devices safe.

Simply locating and locking a lost or stolen phone is not enough these days. Yes, these reactive protection measures are important safeguards. But the new imperative is proactive security. This means protection not only against outright malicious apps that steal money and personal data but also protection that empowers you to make informed decisions about the potential risk of apps you download—and whether that free app is worth the final cost.

Mobile protection now demands a fresh, pre-emptive approach, so you can confidently unlock and enjoy all the benefits of our app-centric world.

[1] "Worldwide Smartphone Usage to Grow 25 Percent in 2014," *eMarketer* (June 11, 2014), www.emarketer.com/Article/Worldwide-Smartphone-Usage-Grow-25-2014/1010920.

[2] "Apps Solidify Leadership Six Years into the Mobile Revolution," *Flurry* (April 1, 2014), www.flurry.com/bid/109749/Apps-Solidify-Leadership-Six-Years-into-the-Mobile-Revolution#.VH5uBmctDIU.

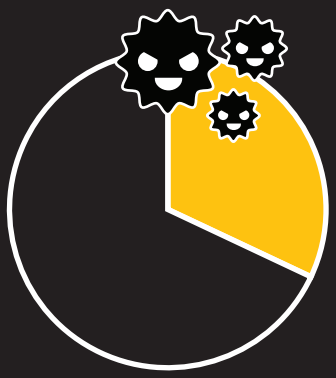
[3] *Our Mobile Planet*, www.think.withgoogle.com/mobileplanet/en/.

Bad apps are just that

Most consumers tend to regard mobile apps with the same naivete that they viewed desktop application software 10 or 15 years ago. They install mobile apps with little or no thought given to the risks they may pose; and they install a lot more of them because it's one simple tap to download.

Apps (especially free ones) are very good at telling you what benefits they provide, but they don't tell you their real costs. These costs can come in the form of hidden threats and other potential risks. Apple makes it tough to stumble across malicious apps by sandboxing its iOS operating system combined with tight controls around what gets into its iTunes® app store. But the open nature of the Android™ operating system can be more easily manipulated to cause threats and potential risks.

The Symantec Internet Security Threat Report found that mobile malware in 2013 was developed almost exclusively for the Android OS, with 32 percent of those apps stealing a user's personal information.[4]



More than 75 percent of all mobile apps fail basic security tests, performing a variety of risky or malicious behaviors.[5]

Symantec recorded a 69 percent rise in mobile malware instances between 2012 and 2013.

[4] "2014 Internet Security Threat Report," *Symantec*, www.symantec.com/security_response/publications/threatreport.jsp.

[5] "Gartner Says More Than 75 Percent of Mobile Applications Will Fail Basic Security Tests Through 2015," *Gartner* (September 14, 2014), www.gartner.com/newsroom/id/2846017.

It's easy to see why mobile apps are appealing to hackers. The user base is growing fast and the amount of information attainable once a malicious app is in place is significant. And hackers are getting better, as hackers always do. They're learning and sharing, and their attacks are getting more sophisticated. Cybercriminals are bringing their trusty PC tactics (such as phishing, fake software, and ransomware) to mobile devices.

In one fake-app scam, phishers offered a bogus app that claimed to deliver free cellphone minutes. The offer was available only if a user entered login credentials and forwarded the offer to 10 friends. The scam was aimed at exponentially increasing the number of victims, stealing credentials, and harvesting other personal data.

Another fake app copied exactly the real app of Mizrahi Bank, one of the largest banks in Israel. Hackers uploaded it to the Google Play™ store and unsuspecting bank customers downloaded it. When they opened the app and entered their login information, the app nabbed their user IDs. The app then deviously sent an error message and instructed customers to reinstall the bank's real app, which would then work fine. Most customers never had a clue their user IDs had been stolen.

Another recent threat is Android.Simplocker, a ransomware Trojan delivered through a fake app. Once installed on your device, it encrypts (or locks) files, then displays a fake alert from the FBI claiming illegal pornographic content has been found on your device. You're then instructed to pay a $300 "fine" through a payment service called MoneyPak to unlock your files.

Quick Guide to Malicious Apps

More than 20 percent of the 15 million apps analyzed to date by Norton software are malicious apps. They come in a variety of forms.

Tracking apps collect text messages and call logs, track GPS coordinates, record calls, and snatch photos and videos from devices. The 2014 Norton Report showed the volume of user-tracking threats increased in 2013 from 15 percent to 30 percent.

Stealing apps collect device-specific and user-specific data, such as device information, configuration data, and personal content.

Infection apps run traditional malware functions, such as installing backdoors and downloaders that give hackers access to your device.

Reconfiguration apps elevate privileges or modify settings in the operating system, which can open the door to attackers.

Money-theft apps use short-code, premium-rate text-messaging numbers. Then hackers create malware that sends text messages to those numbers from infected devices. The users get a bill from their carriers and the hacker gets the money.

Two-factor theft apps can intercept a text message from your bank, carrying a one-time authentication code, which could give hackers access to your bank account.

Grayware can be risky, too

The line between legitimate software and malware is not clearly drawn. There is a class of apps called *grayware* that occupies the murky middle ground. Working in this middle ground are many nonmalicious developers who find it easy to persuade users to download potentially risky apps that expose information and content, often by using the lure of a "free" app.

Grayware apps don't contain malicious code but can still compromise your privacy and afflict your device with ads and all sorts of other annoying behavior. A common type of grayware called mobile adware, or *madware*, includes apps that display ads in a phone's notification bar, replace the dial tone with voice ads, or, worse, expose private data, such as phone numbers or user account information.

You might be able to spot a lot of these risks if you have a fair degree of technical knowledge and you carefully read the long list of app permissions you're agreeing to when you download the app from the Google Play store. But that's not always the case. Even if you do read the permissions, you still won't know all the actual behaviors of the app.

Norton research shows that more than

60 percent

of Android apps contain adware or other grayware.

Once installed, grayware might track your location or monitor your Web browsing and sell the information to marketers. In many cases, an app has a reasonable excuse for collecting some sensitive data, but usually you're not aware of the behavior and probably would not be comfortable sharing certain personal information with that particular app. Take, for example, an app that collects your phone number as a unique ID from your device and sends it over the network without encryption. Suddenly your phone number is available to marketers and scam artists virtually anywhere.

Or an app may present a potential privacy risk by collecting information that seems unreasonable, given the app's purpose. For example, why should a weather app need to access your contacts or calendar information?

Equally common are apps that drain your battery, hamper device performance, or suck down data from the network and drive up your bill. These apps are not technically grayware, but they are certainly annoying. Many of them run surreptitiously in the background. Do you notice your battery life shrinking the longer you own your device? Apps could be the cause. Are your data charges unexpectedly high? Again, apps. Many do a lot of downloading even when they're not open.

Norton™ Mobile Insight never sleeps

You trust Norton™ technology on your PC. We apply the same cutting-edge technology, deep research capabilities, and global intelligence resources to securing your mobile device.

Most of today's mobile-security products provide basic protection. We go the extra mobile mile to deliver technology that fully protects you against malicious and irritating apps. We leverage our 30 years of security expertise and the world's largest threat database to keep you safe against Android app threats.

All the Android app data we collect through Norton Mobile Insight—by constantly crawling more than 200 app stores and compiling app information from the Norton Community Watch network—is entered into our processing pipeline and run through a robust set of tools to identify those that pose problems.

First, we perform static analysis, which includes extracting basic data such as the app title, the developer's signature, and the list of permissions, which are usually presented at the time of downloading an app and can be excessively long.

Then we dig deeper into the app's code to see what sensitive application program interfaces (APIs) will be called. For instance, is the app calling APIs to read your phone number and other private information and then accessing the Internet? The interrogation doesn't stop there. We find out if the app is localized. Does it install without putting an icon on the launcher? This information provides important clues to the safety of the app.

Next we perform important dynamic analysis, which delivers an unprecedented view into app privacy and information leakage. We run every app through an instrumented Android emulator, making the app think it is operating in the real world. For example, if an app collects and sends device information or personal information off the device in the background, it could be going to an unwanted third party.

We do this analysis in an intelligent, automated way by exercising real usage flows and features. Many of our competitors simply infer mobile app behaviors and report risks based on app permissions without actual testing, which can lead to inaccurate information or false alarms reported to the user.

Leading Protection for Mobile

Norton Mobile Insight is a dynamic system that constantly downloads and analyzes new or updated Android apps from more than 200 app stores, including Google Play, to generate unique, ongoing app intelligence. We analyze more than 30,000 new apps every day and have analyzed more than 15 million apps to date.

Norton Community Watch is a vibrant network of millions of users who allow us to collect anonymous metadata and performance data from apps running on their Android devices, including many previously unseen app files. Leveraging this community data and performing real-time analysis gives Norton Mobile Insight another way to understand an app's behavior once it is installed, as well as the risks involved in keeping it on your device. In fact, 25 percent of the known apps analyzed by Norton Mobile Insight are collected from Norton Community Watch only, which means we're analyzing and learning about many apps not distributed via app stores.

Security Technology and Response (STAR) is a global team of security engineers, virus hunters, threat analysts, and researchers who provide the underlying security technology, content, and support for all our security products, including mobile. These experts are our eyes and ears, surveying the threat landscape day and night to keep you safe.

Data: The more you have, the more you know

The Norton solution brings the significant advantage of Symantec™ Data Analytics Platform (SDAP), one of the rare systems powerful and nimble enough to stay on top of the enormous growth in cyberthreats, mobile and otherwise.

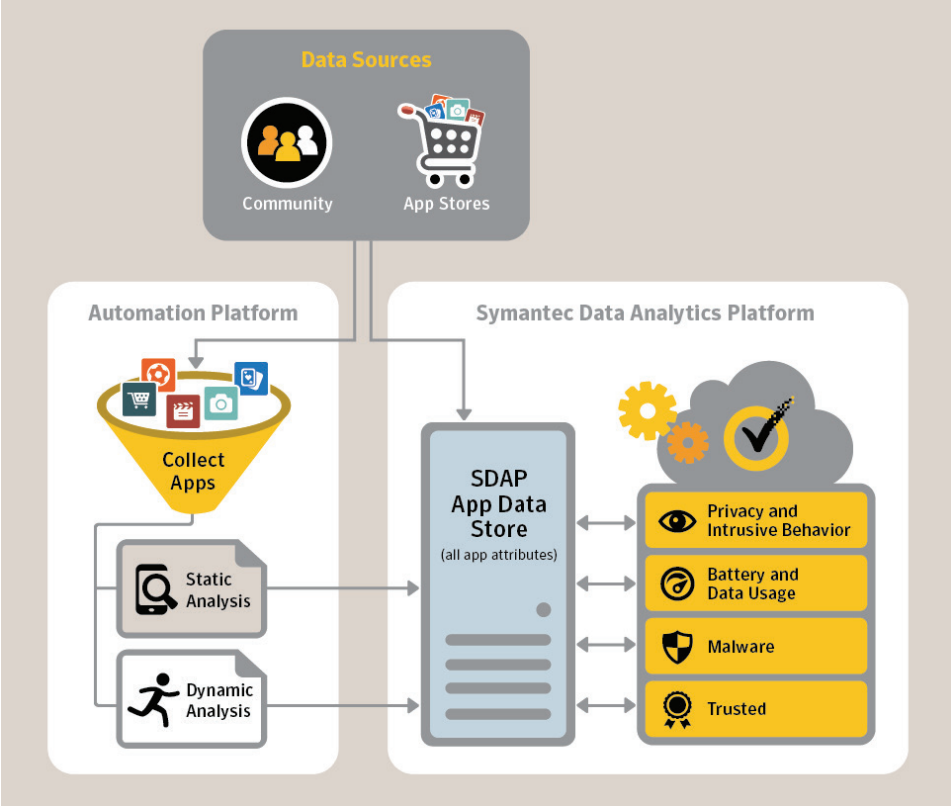
SDAP is a massive, always-expanding database that houses all of our security data. Our mobile data includes around 1.6 trillion individual pieces of data. That's a lot. But that's what is necessary to protect your device from mobile threats.

All of the app data we collect—from application behaviors to application stability and performance details—is processed by SDAP. This data includes information on how the app performs in the real world, how many people in Norton Community Watch have used it, what app stores it is in, and how many people have downloaded it.

We analyze all the data and then we discern whether the app is malicious. Norton Mobile Insight has processed more than 15 million apps to date and processes 30,000 new apps every day. It detects the features and patterns that signify malware, it checks apps for suspicious privacy and intrusive behavior, and it examines their battery and data usage.

And it's constantly getting smarter, as the threat landscape changes. It learns and evolves based on the new data it collects. For example, it knows that malware apps tend to be smaller than nonmalicious apps because malware developers typically do not spend time refining their creations.

Norton Mobile Insight then cross-references all this information against hundreds of other data points to see if the app is malware and sets a confidence level for the security of the app. It recognizes elements inherent to malware that an attacker can't easily change, such as code patterns, techniques for performing malicious behaviors, and the status of the developer's reputation in the community.



Norton Mobile Insight: A dynamic, 'living' intelligence system

Advanced, proactive protection is needed in today's app-happy world

Now it's easy to protect all of your devices with one Web-based subscription service. Norton Mobile Security, powered by Norton Mobile Insight technology, is designed to save you time and take the guesswork out of identifying apps that contain risks.

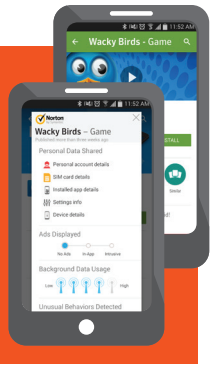
The key to Norton Mobile Security is an app-scanning feature called App Advisor. App Advisor provides proactive protection by letting you automatically scan apps from the Google Play store *before* you download them (on Android 4.0 or later, or Android 4.2 or later on Samsung devices). It tells you if apps contain malicious code or if they come with privacy risks, intrusive behavior, or high battery or data usage. It also automatically scans your previously downloaded Android apps or apps installed outside of an app store for these same risks and enables you to remove them if you choose.

In one simple step, you can easily make informed choices about Android apps. You can decide when a particular app is worth the "cost."

Norton Mobile Security also provides other proactive protection components for you and your Android devices, such as Web Protection to shield you from fraudulent websites designed to steal your personal information and money.

It also includes remote device-recovery protection for your Android devices and Apple® iPhone® and iPad® devices so you can find them fast. You can even save your contact information and restore it in case of loss or theft.

The key to Norton Mobile Security is an app-scanning feature called App Advisor.



Boldly go with the Norton solution

Mobility is integral to your busy, connected life. But increasing reliance on these small computers—your mobile devices—makes it imperative that you recognize mobile security risks and take steps to protect yourself.

We also offer Norton mobile protection technologies as part of our cross-platform Norton Security, Norton Security with Backup, and Norton Small Business product subscriptions. These three subscriptions provide you, your family, and your business with tailored protection for your PCs, Mac® computers, and Android and iOS devices with one easy-to-use, comprehensive solution—anytime, anywhere.

Visit us on Google Play to experience all of the advanced, proactive protection features of a Norton Mobile Security Premium subscription free for 30 days. You'll just need to create a Norton account, no credit card required. After the trial period ends, you can upgrade to Premium or keep using the free features.