How to be safe, find trusted apps, & avoid viruses.
PocketPermissions
A guide for those new to Android.

By Patrick Cousins

Founder / Developer
Lost Packet Software

Intro

This guide aims to provide the basic info most people want to know about the security of their phones, and when to download, and when not to download applications from the Android Market.

It's my hope that this will help people make more informed decisions and be safe about their application usage, privacy, and data. It is my firm belief that Android is a fundamentally safe platform. With some common sense, diligence, and the right knowledge of the potential threats, users can rest assured and enjoy their devices more thoroughly.

While most of these tips will apply to any of the new app stores and markets now available for Android, this guide is written specifically for Google's original Android Market.

Also, while this guide attempts to be as comprehensive as possible, there may be errors or misjudgments, or just opinions that are subjective. Please read it with the idea in mind that it's just a part of the information you may want to consider when downloading your apps. **Deciding what to download is ultimately up to you, and that's the most important thing you'll need to remember.**

I am also an Android developer. I wanted to write this in the interest of full disclosure.

*You can read more about me or my apps (**Listables** and **BlueMuze**) on my site:*

http://alostpacket.com/

You can also contact me through the Market or my website with any thoughts you have on this guide.

Background about Android

The first thing when understanding the security of your phone is to know a little bit about what makes it tick. Android is a 'lite' version of Linux with most applications that you download from the market written in Java.

This is important to know because it means Android is very unlikely to ever get a 'virus' in the traditional sense. Part of the reason is because Linux is a fairly secure operating system that protects various parts of itself from other parts. This is similar to how Windows has admin accounts and limited user accounts. Because of this protection, applications downloaded from the market do not have access to anything by default. You must grant them permission for each activity they want to perform when they are installed. This is a very important point which we will address a bit later. Also due to some bad choices by Google, there are a few exceptions to this rule that we'll talk about in the permissions section.

Nevertheless, while Android is very unlikely to get a 'virus', that does not mean you are completely safe from 'malware', 'spyware', or other harmful types of programs.

Types of Dangerous Programs

The most common threats from Android applications are:

1) When the app tricks the user into giving it permissions it does not need to do its job.

2) When the app hides malicious code behind legitimate permissions.

3) When the app tricks the user into entering in personal information or sensitive data (such as a credit card number).

There are various ways malicious developers (also known as hackers or crackers) accomplish this. We'll briefly define each kind just to have a common understanding of the terms.

Malware

Malware generally is an all-encompassing term used to describe any harmful program. This includes spyware, viruses, and phishing scams. Sometimes the older term 'virus' is used in this context, but malware is now considered more accurate.

Spyware

Spyware is used to describe software or applications that read your information and data without you actually knowing it and reporting it back to some unknown third party for nefarious purposes. Oftentimes this includes keystroke loggers to steal passwords or credit card information. Some people include certain types of Advertising tracking in this category (sometimes called Adware, see below). However that's a much larger debate we wont cover here.

Phishing

Phishing and spyware are closely related. They work on a similar principle: tricking the user and sending user information to a 3rd party to steal it. The difference with phishing however, is that the application (or website) will pretend to be from a trusted source to try and 'trick' you into entering in your details. Contrastingly, spyware would try to hide itself from being known to the user. One way to think about the difference is that phishing is masquerading while spyware is hiding, but the end goal of stealing your data is the same.

An example of this would be an app or website pretending to be affiliated with your bank or Paypal or your email provider (Gmail, Hotmail, Yahoo). However it can, and does, include any service where someone might want to steal your identity or password.

There have been known successful phishing attacks related to at least one bank on Android.

Virus

The definition of virus used to be more all-encompassing. These days that term has been replaced by malware. Virus is more typically used to describe a specific type of software that takes control of your operating system and either damages it, or uses it for its own purposes. An example might be when a virus sends emails to everyone in your email address book. Again this is the type of program least likely to be a problem for Android.

Trojan Horse

A trojan horse is really just a specific type of virus. It merely refers to the idea that the app pretends to be something useful or helpful or fun for the user while actually causing harm or stealing data. This term is often used to describe spyware and phishing attacks as well.

Adware

Adware is typically a bit of a grey area. Sometimes this is also called nuisance-ware. This type of application will often show the users an excessive amount of advertising in return for providing a service of dubious quality to the user. However, this type of program can often be confused with legitimate ad-supported software, which shows a mild to moderate amount of advertising while providing a useful service that the user wants. Because it can be hard to tell the difference, there exists a grey area from most anti-virus companies as to how to handle adware.

Warez

This is a term you'll sometimes hear referring to 'pirated' or unlicensed software. Often warez forums and web sites will offer "free apps" or "apks" (Android Package).

Don't be fooled by these sites, and do NOT download these files and load them to your phone. These files are stolen from the real developers by unscrupulous people who have no regard for the work put into apps by the developers, or the law. Oftentimes they will even try making money off of the advertising on their "warez" forums. They are profiteers that do the entire Android community a great disservice, and hurt the developers. Furthermore, this is very often the most popular 'vector' (method) of attack that malware writers use. Some go as far as stealing apps and putting them on the Android Market itself under different names.

If you are a user who cannot access the paid Android Market, there are alternatives these days. The most trustworthy markets (in my opinion) are the following:

- Android (Google) Market
- Amazon AppStore
- SlideMe
- Archos AppsLib
- AndAppStore (possibly)
- Verizon's Market (not sure if this is live yet)
- Motorola's Market (not sure if live or where, might be focused on Latin America)

Other than these markets, I would not advise anyone to download and install an app from anywhere else.

However there are a few exceptions related to open source. These are places that independent developers can upload free and/or open source apps. They don't guarantee your safety (nothing does) but they are ***not*** warez sites and are much more likely to be safe.

Open source or free apps: (very likely safe, not warez)
- XDA Developers
- Googlecode
- GitHub

How to Protect Yourself

There are no full-proof ways to avoid all bad situations in the world. But, any sane person with a reasonable head on their shoulders knows that a few good habits can keep you safe for a long, long time in whatever you do. Here are a few tips I have learned from many years as a professional software developer and from reading many Android forums that have many people smarter and more knowledgeable than I about Android.

Read the comments in the Market

This should go without saying. Before you download any applications, be sure to read the comments. Don't just read the first three either, click through and see what people are saying. This can also help you understand how well an app works on your particular phone (and your particular version of Android). Comments should also be read EVERY time you update an app.

It's also important to note that bad apps can sometimes "game" the comments and ratings. There are some unsavory services that provide thousands of fake comments for apps and they are probably more common than you think. See the section on **The Community** for more on identifying these types of fake comments.

Check the Rating

Any app that fails to maintain above 2.5 stars is likely not worth your time. If you are brave enough to be one of the first few to download an app, this does not apply to you. Nevertheless, almost all good apps have between 3 and 5 stars. To me, this is just a general rule to *help* find quality apps.

Check the permissions

There are many things an app can do to, and for, your phone. But anything an app can do is told to you when you download and install it. Before you download and install an app, you will be shown a list of permissions the application is requesting. **Read them**. Try your best to understand them in terms of what the application is supposed to do for you. For example, if you download a game of checkers, and the Market warns you that it wants to be able to read your contacts, you should think twice and probably not download it. There is *no sane reason a game of checkers needs to know your friend's phone numbers.*

In the Permissions section you can read a list of some of the most commonly used permissions. The list explains how important they are, what they do, and notes some examples of apps that might legitimately need the permission. This should help you get a basic understanding of what to allow, and when to skip, an app.

Check the developer's website

Make sure the developer has a website and not just some blog. This is often a good indication of quality as well as safety. If the developer cares about their app they will likely have a relatively nice looking website (or, if they are open source, a site on Google Code or something similar). Note: sites on Google code are NOT verified or approved by Google. However, open source is *usually (but not always)* more likely to indicate a safe application.

NOTE: This is not a definitive indicator if a developer is good or bad, just one more piece of information you can use. There are a lot of exceptions to this particular rule, as a lot of good developers might not have anything more than a blog, and a lot of bad developers could just point to a nice looking site they have no affiliation with. However, the developer's website can be helpful just as an extra piece of information you can use in making your decision about the developer or app.

Updating applications is the same as installing them fresh

Each time you update an application on your phone, you should use the same diligence as if you were installing it for the first time. Reread the permissions to see that it is only asking for what it needs and no more. Reread the comments to see if anything has changed in the opinions of the users and to see if it still works for your phone. If you see that an application says Update (manual) next to it, that means the developer has changed the permissions that they are requesting. This is not necessarily a bad thing -- but it should indicate that you should pay a bit closer attention to the permissions and re-evaluate them as needed.

The community

If you are still unsure, ask around -- the community is your anti-virus

If you see an app you want, but it seems to be asking for more permissions than it should, or its comments and ratings are mediocre, go ahead and ask around about the app. You will often find dozens of people who know the answers and another whole bunch wishing to know the answers to the same questions. Good places to ask include Android enthusiast web sites and forums.

I can't stress this point enough. This is the best part about Android. The community is usually the first to identify any malware or dangerous programs, and is the best resource for finding quality apps.

Beware the Sockpuppets, Shills, and Spammers

However, like anything, don't believe everything you read. Someone who comes into a forum telling you an app is the "best" may be what's referred to as a sockpuppet or shill. I tend to be wary of people with low post counts on forums, or who have unreasonably high praise for what seems to be a simple app, or anyone using the word "best" in a forced context.

Now these people are not all bad, some may just be excited, or not speak English as their first language. But it's common for sockpuppets to use the term "best" to try and get better search rankings on Google. Saying things like "Best Android App" or "Best GPS."

Other tell-tale signs include when a spammer mentions software for iPhone or other platforms without any focus on Android in their post/comment. Another is when it seems like the post is just out of context or overly general (think about how horoscopes are made for everyone to relate to them). I often get spam on my blog that says things like "best blog post! love your writing style, you put things in perspective for me" which makes no sense when my blog was about my new app.

This is a fine line and very much a grey area. Sometimes it can be very hard to tell if someone is a spammer. If you see a post or comment in the Market or on a forum that you suspect is spam, report it to the website or Market, don't reply and start an argument.

These tips also apply to the comments about apps. There are sometimes people who are paid to rate and comment about an app. The key to spotting this is again all about context. If an app has not been on the market for very long and has thousands of great comments it should raise an eyebrow. If the comments are all general like "best app" that is another good indicator. Again it's hard to tell for sure, but you should always look with a skeptical eye at comments. It's also to be expected that the developer themselves (and maybe a handful of friends) would rate an app well, that's normal and not something to be concerned about. However, when you see an overwhelming number of questionable comments, you should tread carefully.

Posting your own comments

After you have downloaded an app you can post your own comments. The comment will be visible to all other Android users but it will only show your first name. To do this go into the Market and press **[menu]** then **[downloads]**. You should see five empty stars at the top which you can tap to rate the app. Once you have rated the app you should see an option to add a comment under the stars.

Being a good user

While this guide is about security, I think it's important to point out how to be a good user too. Android is a community and stems from open source and will only ever be as good as both its developers and its users.

So, if an app is crashing on you, try emailing the developer before uninstalling and posting an angry comment. Anything you post in the market will stay even if you have uninstalled the app, and you could do serious harm to a developer's reputation if you post very negative comments.

If you think the developer just made a mistake, or didn't support your phone, work with them. If they are unhelpful, then you can consider giving them a bad rating. This is especially true for free apps in the market. Remember that you, as a user are not "entitled" to perfect free apps. Most developers do not have Google's engineering and QA team backing them up and even Google makes mistakes.

And while it's frustrating when things don't work, imagine how frustrating it is when you put long hours into something but make a mistake -- and then because of that mistake you can never fix the damage done by a rude commenter.

What does Google do to protect us?

Unfortunately at the moment, not a lot. They do police the market to a small extent and investigate any reports of malware. However, on at least 2 occasions they identified several instances of malware (called DroidDream) and remotely uninstalled the applications from users' phones. The was also an instance of a phishing app that pretended to be from a particular bank and was removed when discovered.

Nevertheless, the Market is not like the Apple App Store or Amazon AppStore, there is no screening of applications before they are published. There are no draconian procedures or lengthy approval processes that developers have to go through to publish applications. All that a developer needs to do is to 'digitally self sign' the application before posting it. This helps Google track any developers with ill intent, but it's just a way to manage malware *after* it is discovered.

Permissions

When you install an application the Market will tell you all of the permissions it needs to function. These are important to read as it can give you an idea if the application is asking for permission to do more than it needs. While some legitimate apps often ask for more permission than they need, it should at least raise an eyebrow when deciding if an application is safe and of good quality.

NOTE: there are also some backwards compatibility decisions Google has made that will grant apps targeting 1.5 or earlier two permissions you may never see requested. It is my belief this is a security hole, but not a large one. The permissions are **Read Phone State and Identity** and **Write/Delete files from the SD.** I will elaborate on those below.

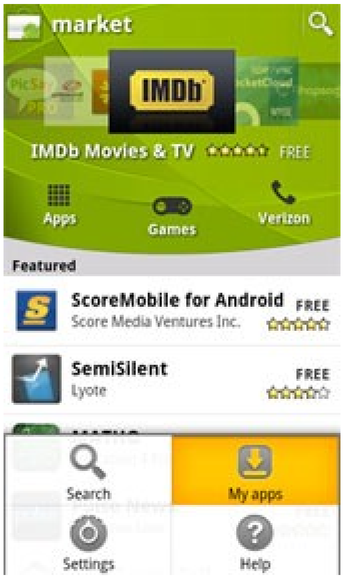
To see the permission given to an application after installation open the Market app and follow these steps:

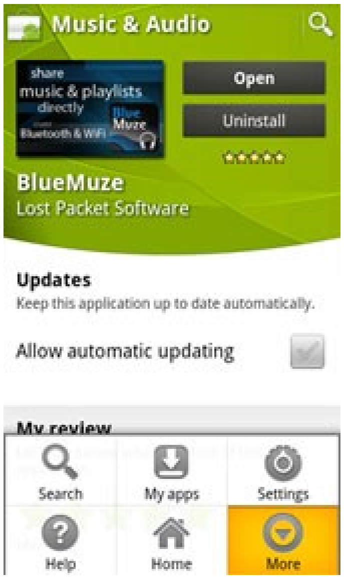
---

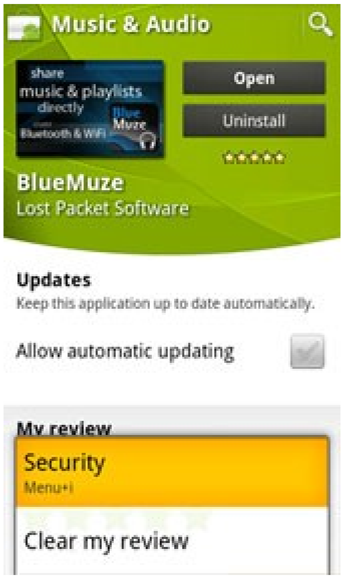
1) Press **[menu]** then **[downloads]** or **[my apps]**

2) Then select the app, press **[menu]** again, then **[More]** (skip to step 3 if you don't see a [More] option)

3) Then tap **[security]**.







⚠ Make phone calls

Services that cost you money

This permission is of moderate to high importance. This could let an application call a 1-900 number and charge you money. However, this is not as common a way to cheat people in today's world as it used to be. Legitimate applications that use this include: Google Voice and Google Maps.

⚠ Send SMS or MMS

Services that cost you money

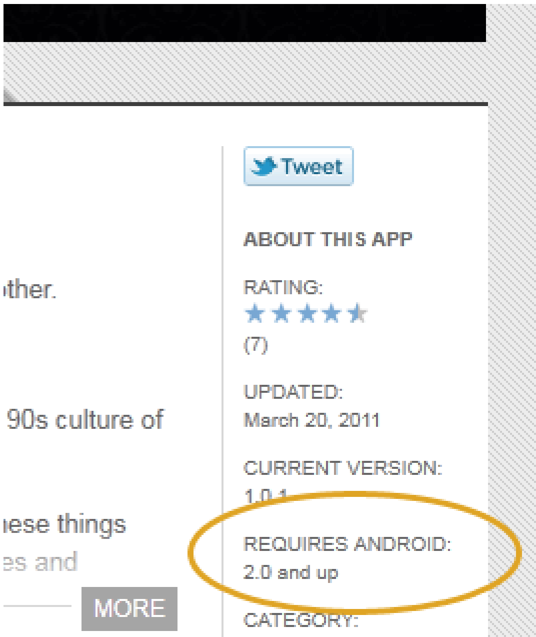
This permission is of moderate to high importance. This could let an application send an SMS on your behalf, and much like the phone call permission, it could cost you money by sending SMS to for-pay numbers. Certain SMS numbers work much like 1-900 numbers and automatically charge your phone company money when you send them an SMS.

⚠ Modify/delete SD card contents

Storage

This permission is of high importance. This will allow applications to read, write, and delete anything stored on your phone's SD card. This includes pictures, videos, mp3s, documents and even data written to your SD card by other applications. However, there are many legitimate uses for this permission. Many people want their applications to store data on the SD card, and any application that stores information on the SD card will need this permission. You will have to use your own judgment and be cautious with this permission knowing it is very powerful but very, very commonly used by legitimate applications. Applications that typically need this permission include (but are not limited to) camera applications, audio/video applications, document applications

WARNING: Any app targeting Android 1.5 or below (possibly 1.6 as well) will be granted this permission BY DEFAULT and you may not ever be warned about it. It is important to pay attention to what version of Android an app is targeting to know if this permission is being granted. You can see this on the Market website in the right hand column.



ither.

90s culture of

iese things
es and

ABOUT THIS APP

RATING:
★★★★★
(7)

UPDATED:
March 20, 2011

CURRENT VERSION:
1.0.1

REQUIRES ANDROID:
2.0 and up

CATEGORY:

⚠ Read contact data, write contact data

Your personal information

This permission is of high importance. Unless an app explicitly states a specific feature that it would use your contact list for, there isn't much of a reason to give an application this permission. Legitimate exceptions include typing or note taking applications, quick-dial type applications and possibly social networking apps. Some might require your contact information to help make suggestions to you as you type. Typical applications that require this permission include: social networking apps, typing/note taking apps, SMS replacement apps, contact management apps.

⚠ Read calendar data, write calendar data

Your personal information

This permission is of moderate to high importance. While most people would consider their calendar information slightly less important than their list of contacts and friends, this permission should still be treated with care when allowing applications access. Additionally, it's good to keep in mind that calendar events can, and often do contain contact information.

⚠ Read/write Browser history and bookmarks

Your personal information

This permission is of medium-high importance. Browsing habits are often tracked through regular computers, but with this permission you'd be giving access to more than just browsing habits. There are also legitimate uses for this permission such as apps that sync or backup your data, and possibly certain social apps.

⚠ Read logs / Read sensitive logs

Your personal information / Development Tools

This permission is of very high importance. This allows the application to read what any other applications have written as debugging/logging code. This can reveal some very sensitive information. There are almost no reasons an applications needs this permission. The only apps I might grant this permission to would be Google apps. The name of this permission recently changed as it came to light how important and dangerous this permission can be. Both the old name and category and the new name and category are listed above.

⚠ Read phone state and identity

Phone calls

This permission is of moderate to high importance. Unfortunately this permission seems to be a bit of a mixed bag. While it's perfectly normal for an application to want to know if you are on the phone or getting a call, this permission also gives an application access to 2 unique numbers that can identify your phone. The numbers are the IMEI, and IMSI. Many software developers legitimately use these numbers as a means of tracking piracy though. This permission also gives an application to the phone numbers for incoming and outgoing calls.

WARNING: Any app targeting Android 1.5 or below (possibly 1.6 as well) will be granted this permission BY DEFAULT. And you may not ever be warned about it. It is important to pay attention to what version of Android an app is targeting to know if this permission is being granted. You can see this on the Market website in the right hand column.

(see image above)

⚠ Fine (GPS) location

Your location

While not a danger for stealing any of your personal information, this will allow an application to track where you are. Typical applications that might need this include (but are not limited to) restaurant directories, movie theater finders, and mapping applications. This can sometimes be used for location based services and advertising.

⚠ Coarse (network-based) location

Your location

This setting is almost identical to the above GPS location permission, except that it is slightly less precise when tracking your location. This can sometimes be used for location based services and advertising.

⚠ Create Bluetooth connection

Network Communication

Bluetooth (Wikipedia: Bluetooth) is a technology that lets your phone communicate wirelessly over short distances. It is similar to Wi-Fi in many ways. It itself is not a danger to your phone, but it does enable a way for an application to send and receive data from other devices. Typical applications that would need bluetooth access include: Sharing applications, file transfer apps, apps that connect to headset out wireless speakers.

⚠ Full internet access

Network Communication

This is probably the most important permission you will want to pay attention to. Many apps will request this but not all need it. For any malware to truly be effective it needs a means by which to transfer data off of your phone; this is one of the settings it would definitely have to ask for.

However, in this day and age of cloud computing and always-on internet connectivity, **many, many legitimate applications also request this.**

You will have to be very careful with this setting and use your judgment. It should always pique your interest to think about whether your application needs this permission. Typical applications that would use this include but are not limited to: web browsers, social networking applications, internet radio, cloud computing applications, weather widgets, and many, many more. This permission can also be used to serve Advertising, and to validate that your app is licensed. (Wikipedia article on DRM).

⚠ View network state / Wi-Fi state

Network communication

This permission is of low importance as it will only allow an application to tell if you are connected to the internet via 3G or Wi-Fi

⚠ Discover Known Accounts

Your accounts

This permission is of moderate-high importance. This allows the application to read what accounts you have and the usernames associated with them. It allows the app to interact with permission related to that account. An example would be an app that was restoring your contact, would discover your Google account then send you to Google's login screen. It doesn't actually get to see your password, but it gets to work with the account. This is also legitimately used by applications to add contacts to your accounts, such as dialer replacements and contact managers/backup/sync/etc.

⚠ Manage Accounts

Your accounts

This permission is of high importance. This allows the application to manage the accounts on your phone. For instance it would be used by a service like Facebook to add an account to your accounts list. It seems at this time unclear if this permission allows an app to delete accounts.

⚠ Use Credentials

Your accounts

This permission is of high importance. This will allow an application authorization to use your accounts. They do this typically by giving what's called an AuthToken depending on what account you use (Google/Facebook/Yahoo/Last.fm/Microsoft/etc.). It's not as scary as it sounds however, it does typically protect your password from being seen by the application. However, it's still a very important permission you should give only with great caution.

⚠ Read/modify Gmail

Your messages

This permission is of high importance. Few apps should need access to your Gmail or email account. Email is also a prime method for managing accounts with other companies and services. For example, someone with control over your email could request a new password from your bank. While this is the worst case scenario, and there are various legitimate uses for this permission, it's still best to treat all email related permissions with extreme care.

⚠ Install Packages

System tools

This permission is of critical importance. This allows an application to install other applications on your system. This can be exploited by virus writers to install adware and malware on your system without your knowledge. It is a very, very dangerous permission and should almost NEVER be granted to a typical app. The only legitimate uses for this permission are for Market-like apps such as the Amazon AppStore or the Android Market.

⚠ Prevent phone from sleeping

System tools

This is almost always harmless. Sometimes an application doesn't expect the user to interact with the phone directly, and therefore may need to keep the phone from going to sleep. Many applications will often request this permission. Typical applications that use this are: Video players, e-readers, alarm clock 'dock' views and many more.

⚠ Modify global system settings

System tools

This permission is pretty important but only has the possibility of moderate impact. Global settings are pretty much anything you would find under Android's main 'settings' window. However, a lot of these settings may be perfectly reasonable for an application to change. Typical applications that use this include: volume control widgets, notification widgets, settings widgets, Wi-Fi utilities, or GPS utilities. Most apps needing this permission will fall under the "widget" or "utility" categories/types.

⚠ Read sync settings

System tools
This permission is of low impact. It merely allows the application to know if you have background data sync (such as for Facebook or Gmail) turned on or off.

⚠ Restart other applications

System tools
This permission is of low to moderate impact. It will allow an application to tell Android to 'kill' the process of another application. However, any app that is killed will likely get restarted by the Android OS itself.

⚠ Retrieve running applications

System tools

This permission is of moderate impact. It will allow an application to find out what other applications are running on your phone. While not a danger in and of itself, it would be a useful tool for someone trying to steal your data. Typical legitimate applications that require this permission include: task killers and battery history widgets.

⚠ **Automatically start at boot**
System tools

This permission is of low to moderate impact. It will allow an application to tell Android to run the application every time you start your phone. While not a danger in and of itself, it can point to an applications intent.

⚠ **Control Vibrator**
Hardware controls

This permission is of low importance. As it states, it lets an app control the vibrate function on your phone. This includes for incoming calls and other events.

⚠ **Take Pictures & Video**
Hardware controls

This permission is of moderate importance. As it states, it lets an app control the camera function on your phone. In theory this could be used maliciously to snap unsuspecting photos, but it would be unlikely and difficult to get a worthwhile picture or video. However, it is not impossible to make malicious use of cameras.

Privacy

Wi-Fi

One of the things to remember when trying to keep yourself safe is to be very careful with public Wi-Fi. Whenever you connect to the internet through a public Wi-Fi, you should never use any website that requires a password to sign into. The danger here is because you have no idea who is connecting you to the website. A good analogy would be like trying to mail a letter to your friend by giving it to a stranger in the street. For more info read: Man-in-the-middle attack(Wikipedia). There is also a risk that applications may be transmitting data in the background over that Wi-Fi connection about you without encrypting it. This is also true of any applications over any internet connection however. And while there are some good ways to secure your phone, I personally don't use any public Wi-Fi at all. This may be seen as extreme in some circles, but I believe it to be safest route (although somewhat limiting).

SD Cards

There isn't much to say about SD cards except that all users should remember that they are not a safe place to store personal information. This can be something as simple as a backup/export of your contacts.

The reason the SD card is not safe is that nearly all applications can read any file they want from the SD card. Most personal info such as contacts is stored internally in protected databases however, so this shouldn't be a huge concern for most people, but it's helpful to keep in mind.

GPS and Network Location

There is a lot of information online and in various books about why letting yourself be tracked has potential consequences. However, there are a lot of useful features that apps can provide with location tracking information. You should treat location tracking with care and be sure to give it only to parties your trust. Google Maps would be a great example of this.

Advertising and location tracking

There is a trade-off that some people will consider making with regards to location tracking. Some advertisers would like to have location information on you in order to show you local advertisements and coupons. In exchange, you get free use of an app such as a game. This is a decision you will need to make for yourself. I personally would not make this trade off, but some people very knowledgeable about security are very comfortable making it.

Anti-virus

The efficacy of anti-virus apps on Android is a controversial subject on even the best of days. Needless to say, there are some very differing opinions on the necessity of having anti-virus software protecting your phone. Both sides of this debate have some credible and respectable reasons for their choice, so I will try and present both sides as objectively as I can. In full disclosure though, I personally do not use anti-virus on my phone. That's a personal choice I made. Plenty of security experts whom I respect do chose to use anti-virus on their phones. So ultimately this will be a choice that is yours alone to make and not something where you should take cues from other people. That said, here are the pros and cons of each side as best as I know them.

One thing to remember though, is that each side may have some irrational or sensational arguments. These stem from either a sense of emotional justification or a vested interest in selling software. Put simply, neither side of the debate is above bad arguments and unintentional or intentional faulty logic.

Benefits

- Will protect you from all past threats
- May protect you from a future threat
- Often can have additional features for privacy and data protection
- May have features to protect your phone if it is lost or stolen

Drawbacks

- May waste system resources like battery and memory
- It's hard to protect from future/unknown threats
- Can potentially cause serious harm to the OS (very rare but not unheard of)
- May provide a false sense of security and encourage risky behavior

Last updated: June 7, 2011

For more info see http://alostpacket.com/