Smartphone Viruses Are Real: How To Stay Protected

by Joel Lee

The last thing you want is a latent Trojan that sits in the background and steals all of your sensitive data. Think you're safe from a smartphone infection? I wouldn't be too sure. Viruses are most prevalent on PC platforms, yes, but these past few years have proven that smartphone viruses are real. Are you safe?

Considering how integral smartphones now are to everyday life, it's scary to think how much damage can be done by malware – and sometimes all it takes is one lapse in judgment to become infected. Keep reading to find out what these infections could do to you, how to detect them, and how to shield yourself from them.

The Worst Smartphone Malware Attacks

(Image credit: Shutterstock)

Smartphone malware infections might seem like a recent concern, but the first attack goes back nearly a full decade. How bad can malware be?

The first notable attack was on Symbian OS, the world's most popular smartphone operating system prior to Android's rise to fame in 2010. The Cabir worm was a proof-of-concept virus in 2004 that could spread to other phones through Bluetooth. The constant scan for Bluetooth devices reduced battery life, but otherwise it was harmless.

Then, in 2005, Symbian phones were hit by the Commwarrior virus. This too was relatively harmless, but it proved that viruses could spread through MMS (text messages with images, videos, or sounds). Prior to this, mobile attacks were localized due to the limited range of Bluetooth. With Commwarrior, distance was no longer a limit.

As Android exploded in popularity, it became the target of malware developers. The **Gingermaster Trojan** exploited a security hole in the Gingerbread version of Android, allowing the virus to elevate itself to superuser permissions. With unfettered access, Gingermaster gathered phone data and sent it off to a remote address for collection.

This particular virus is a good example of why Android app permissions are important and the potential dangers of rooting Android.

And if you thought iOS was immune to viruses, think again. Although Apple tries to maximize app security by exercising strict control over the App Store, some things can slip through.

The **Ikee worm** exploited a vulnerability in jailbroken devices and spread using the SSH protocol. Fortunately, it was harmless and only replaced the wallpaper with a photo of Rick Astley. However, it did prove that iOS wasn't as virus-proof as some defenders had claimed.

Symptoms of Smartphone Malware Infection

(Image credit: Shutterstock)

Perhaps the most dangerous aspect of malware is its stealthy and deceptive nature. For as long as you remain in the dark, malware can sit back and do its thing. It's only when you know you're infected that you can take the proper steps towards removing the threat. So, how can you tell if your phone has been infected by malware?

Decreased battery life is a huge signal that should always raise a red flag. It won't always mean an infection – it could be as simple as a buggy app that's hogging a lot of CPU – but it should make you suspicious. Malware is always trying to collect information, always tapping into data streams, and always attempting to spread, and all of those processes make your phone work overtime.

Again, battery drain is not always a sign of something malicious. If you're having issues with it, check out these tips for extending Android battery life.

Decreased performance. In the same vein as the battery life sign above, malware tends to slow down your phone's speed. You only have so much processing power. When malware is constantly running in the background, it leaves even fewer resources for the rest of your apps. In most cases, you should notice the performance hit.

Interrupted calls and apps. Malware is invasive and it often likes to interfere with running processes in order to snoop and pull information to which it might not normally have access. The result is that calls might unexpectedly drop (especially when malware tries to reroute them) and apps might unexpectedly crash. If these problems start occurring out of the blue, you may be infected.

There are some other yellow flags that could raise suspicions, but these are major warnings that you shouldn't ignore.

Mobile Security With Safe Habits

(Image credit: Shutterstock)

If you suspect malware on your phone, there are a few antivirus tools you could use to diagnose and remove the infections. It may seem unnecessary but not using antivirus app is one of the most common smartphone security mistakes. Better to be safe than sorry.

Some recommended apps include:

- **360 Security (Free,** Android **&** iOS**)**: This wonderful app not only scans for actual infections but also for vulnerabilities in your system. It's also equipped with automatic protection to ease your mind. On top of malware defense, 360 Security is even useful for anti-theft protection, power saving, and blocking unwanted calls and texts.
- **Avira Mobile Security (Free,** Android **&** iOS**)**: Avira has an on-demand and automatic app scanner that negates most mobile threats. It can also track your phone's location, lock it down remotely, and detect hacked emails and notify your contacts that your email has been comprised. It's light on the battery, too, so it's a good choice if you're worried about resource consumption.
- **avast! Mobile Security (Free,** Android**)**: avast! is an acclaimed antivirus app that deserves its reputation. It can scan and remove malware, but like the two apps above, it has a few extra bells and whistles on top of that: anti-theft measures, network meter, app locks, firewall, and more. The ability to schedule automatic periodic scans makes this one the most convenient option.

All in all, these three apps are all great and packed full of security features. Which one should you use? It comes down to personal preference.

Other tips that will maximize your mobile safety:

Reputable downloads only. Being reckless with downloads is essentially the same as leaving the door open and inviting every stranger into your home. Not every shady download will harm you, but eventually one will. That's not a risk worth taking. Only download apps that have gained a good reputation.

Learn the risks of rooting and jailbreaking. With our Android rooting guide and iOS jailbreak guide, it's never been easier to unlock the full potential of your phone. However, you should be aware of the risks and security issues that accompany such freedom.

Scan for issues regularly. There are times when an infection doesn't show any obvious signs. There are few feelings worse than running a malware scan for the first time in six months only to realize that you've been compromised for most of that period. Once every week is enough for most users.

If you only take away one thing from all of this, just remember that smartphone viruses are real. Be careful and vigilant whenever your phone is connected to WiFi, Bluetooth, or data. You never know when malware could find its way onto your device.

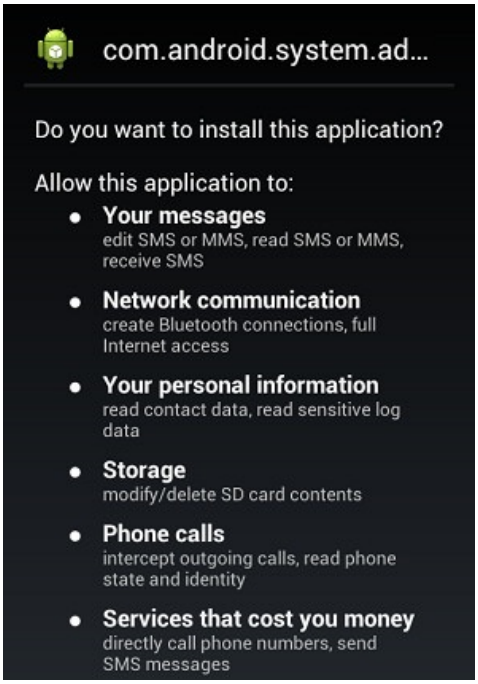
What You Really Need To Know About Smartphone Security

By Matt Smith

Your smartphone is a computer in your pocket, and it often contains just as much private data. All of your emails, location history, web history and app usage are likely accessible through the device on your pocket. This makes it well worth protecting, but the threats you should worry about extend beyond.

Viruses Exist

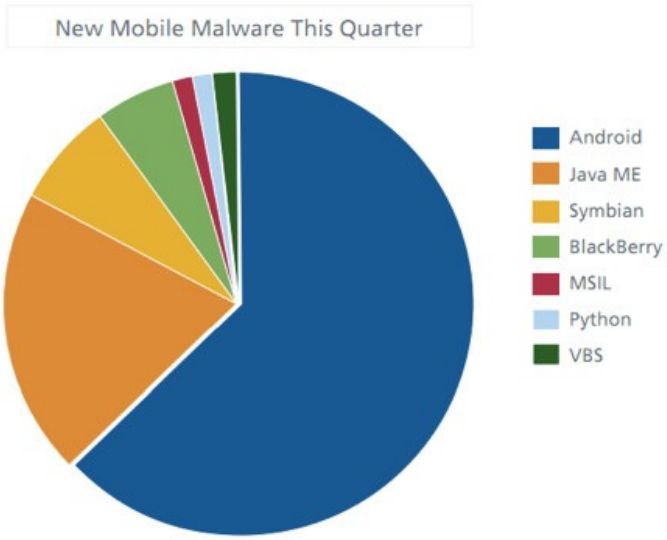
Since a smartphone is like a computer, it is vulnerable to similar security threats. Malware can be used to monitor data transferred on a phone, hijack specific data (like credit card numbers) or simply corrupt apps and generally make your life difficult. There are millions of potential threats in existence, and while most are unlikely to cross your path, the risk is higher than you might have guessed.



Smartphone viruses also emulate their PC brethren in the way they spread; anyway they can. They can arrive via text message, through a web attack that exploits vulnerabilities in your web browser, or through an exploit in your phone's networking capabilities. This is why, as is true with PCs, the advice of "just don't download a virus, dummy," doesn't always work.

No Platform Is Immune, Though Some Are Better Than Others

The operating system your smartphone runs has a significant impact on the threats you must be concerned with. Android, which is the most popular and most open, is predictably the least secure. This isn't entirely Google's fault, as it's effectively become the Windows of the smartphone world. Everyone targets Android because it offers the largest pool of potential victims.



Apple's iOS is more secure because it is more tightly controlled. The company rigorously oversees the app store, does not allow the installation of apps from any alternative source, and closely integrates the operating system with its hardware. While security flaws have been found in iOS there have been no confirmed reports of an in-the-wild virus (though there have been a few apps that behaved badly, albeit within the confines of the permissions given to them). With that said, jailbreaking your iOS device and using "unauthorized" apps opens you to a variety of potential threats.

BlackBerry viruses have been reported, though they're not particularly common, and Windows Phone has yet to fall victim to a virus. That may change, however, if the operating system becomes more popular.

Security Apps Aren't Always Worth Their Title

All of this doom and gloom is likely to send you screaming towards the nearest security app, but be careful. Not all security apps work equally well, and not all of them actually protect you.

Android users can make an informed decision about the antivirus they use by viewing the latest reports from AV Test and AV Comparatives. These organizations compare antivirus solutions by

throwing a collection of malware at each app. Established names like Kaspersky, Bitdefender and Avast! often win these contests, but some lesser-known companies like ESET and AhnLab have scored well, too.

BlackBerry and Windows Phone users, however, have no such scores to go by. Users on these platforms should play it safe and stick to apps from companies that have a proven track record in Windows and Android.

Most antivirus apps do what they say, but not all of them work equally well. AV Test's last round-up found that two entries, VIRUSfighter Antivirus Pro and Zoner AntiVirus, let through at least a quarter of all threats. These aren't unpopular apps; both of them have four-star rankings on Google Play and Zoner has been recommended over 20,000 times on Google Plus.

And then, of course, there are the inevitable fakes. In April of 2014 a new antivirus app called Virus Shield appeared with a price of $4 and rose to the top of the paid apps list. Just one problem; it didn't actually do anything. Though eventually removed, over 10,000 users downloaded it before it was taken down.

The moral of the story? Do your research and don't fall for spanking-new security apps that promise perfect security.

A Lost Phone Can Be Worse Than A Virus

Worrying about malware can keep your attention locked on just one problem, however. There's another issue that's just a disconcerting, and far more likely; the loss of your phone, either accidentally or because it was stolen.

(Image credit: Flickr)

A phone in a stranger's hands opens you to all the security issues we've already touched on. Everything stored on your phone can be accessed, from your saved credit cards to your email inbox, no virus required, and anti-virus can't do a thing to protect you.

What can protect you is preemptive action. Place a lock on your phone. Backup your data. And make sure you're aware of if it goes missing. Waiting until after your phone is already missing may be too late, so don't hesitate to familiarize yourself with your smartphone's security. The process only takes a few minutes.

Where There’s Data, There’s Risk

Keeping your phone secure is now a complex, multistage process. That’s unfortunate, but also inevitable given their expanding capabilities. Where there’s data, there will be someone who wants to obtain it, often through illegitimate means.

The good news is that all smartphone manufacturers have become wise to the problem in short order, so most modern devices offer backup, remote wipe and lock features by default. You’ll also find that there’s a wide variety of effective antivirus solutions, some of which are absolutely free. While certainly worth a bit of worry, smartphones are still easier, and less expensive, to protect than a PC.

Hopefully that remains true in the future.

Ten Common Smartphone Mistakes That Expose You To Security Risks

By Kihara Kimachia

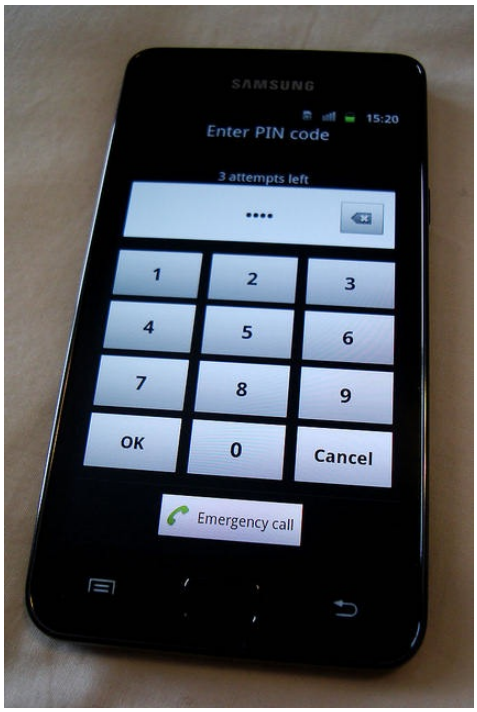
The smartphone has evolved into an integral part of life. Think about it, how many times do you use your phone for some task in single day? Numerous times I suppose. Yet, for a device that is so important, I am often shocked by the mistakes people make on their smartphones and unnecessarily expose themselves to security risks.

The following is a run-down of ten of the most common smartphone mistakes.

Not Locking That Phone

It may be a tad irritating to have to enter a screen lock password every time you want to use your phone but this is one of the easiest ways to prevent unauthorized access and/or use of your phone. While tech savvy villains can crack any screen lock security with time, implementing this measure provides you with at least some basic form of security that will prevent most people from accessing your phone.

The best type of screen lock is a PIN or password. Avoid screen lock patterns which can easily be hacked. Set the phone to lock the screen after one minute of being idle.



(Image credit: Flickr)

Joining Public Wi-Fi Networks

Public Wi-Fi networks may be cheap but they are also a major security risk. Information sent over public Wi-Fi networks is visible to anyone on the network if they know how to view it. Hackers can easily steal your information and remotely access your device. If you must use a public Wi-Fi network, connect to the Internet using a VPN. VPN stands for Virtual Private Network and is a method to connect to websites securely even on public networks. Otherwise, use your mobile data network.

Not Using An Antivirus & Other Security Software

Many people don't realize that a smartphone is actually a computer and is still prone to the same malware risks. They will go to great lengths to make sure they have the latest and most up-to-date antivirus for their PC but have zero protection for their smartphone. According to the Journal of Information Systems Technology and Planning, over 96% of smartphones do not have pre-installed security software. Few smartphone users go to the trouble of installing antivirus and other security software.

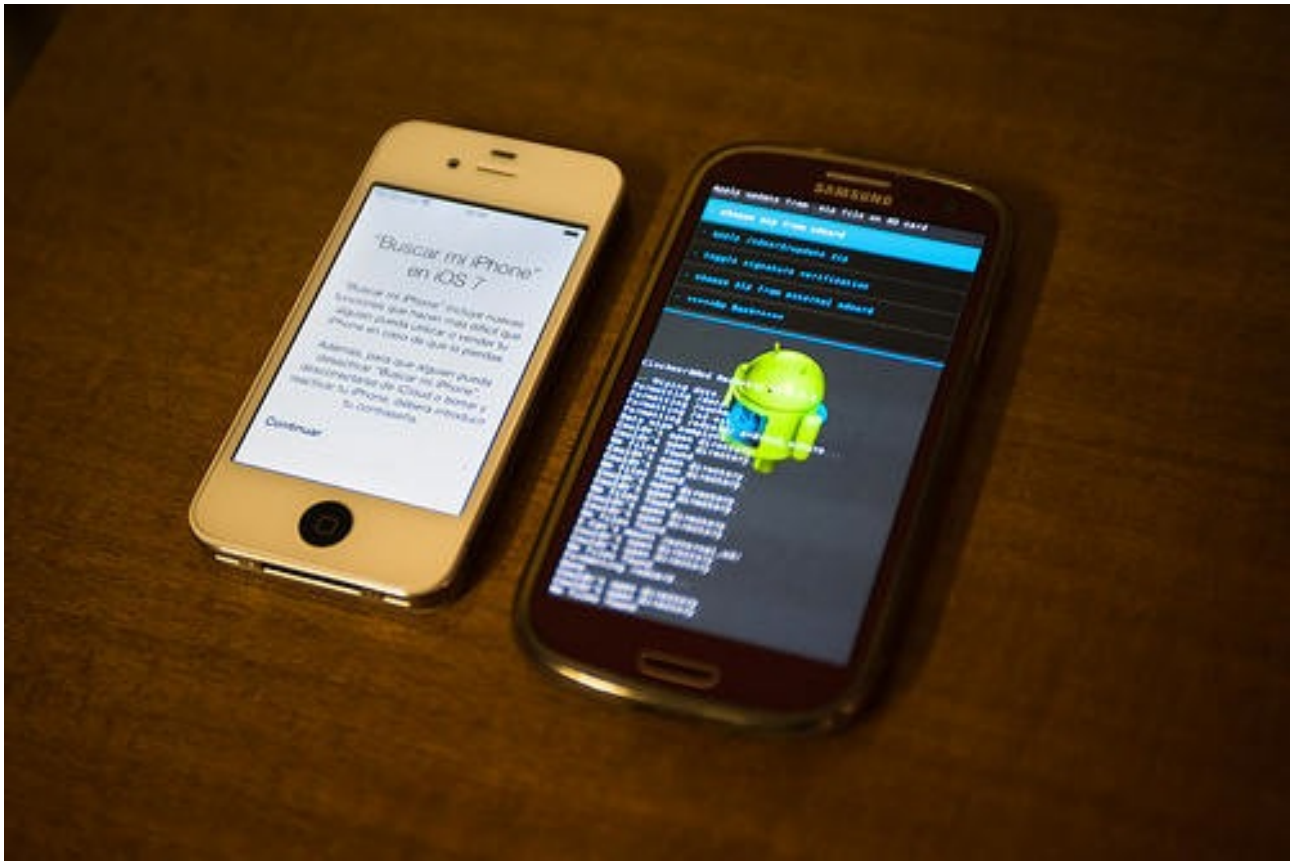
Some good free antivirus software for Android phones include; Bitdefender, AVG and Avast. Apple says their iPhones are practically impermeable to malware but only time will tell.

By installing an antivirus on your smartphone, you also avoid transferring a virus to your computer via USB which is a common problem these days. In addition to that, it is also a good idea to install antitheft software that prevents access to your phone after it has been stolen. An application such as Prey wipes your data remotely if your phone is stolen.

To track your phone using GPS, you can also install an app such as Where's My Droid for Android or Find My iPhone for iPhones.

Forgetting To Install Those Updates

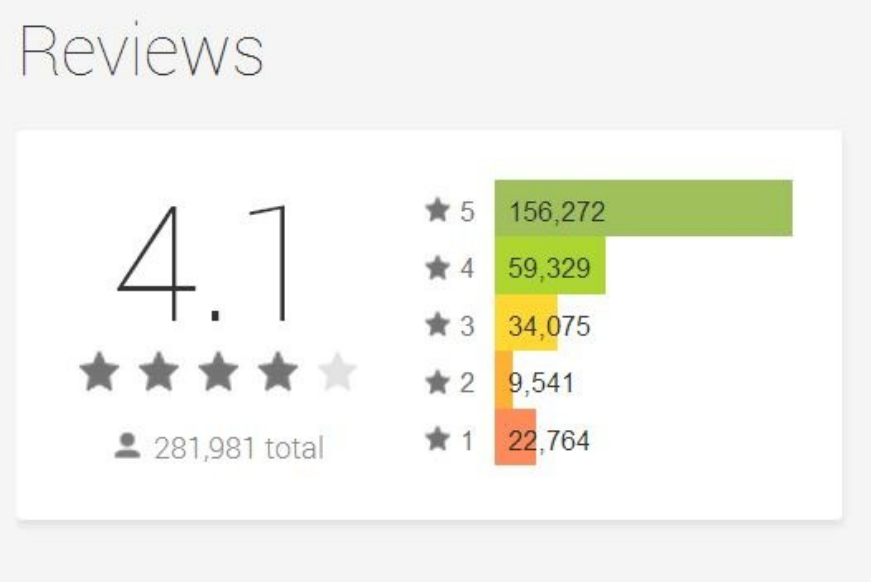
Smartphone manufacturers and app developers regularly issue software updates to improve functionality and to patch security gaps. In general, you should accept updates to your phone's operating system as soon as you are notified. The same goes with apps running on your phone. Make it a habit to regularly update the software running on your smartphone.



(Image credit: Flickr)

Not Verifying Your Apps

Few people verify apps before they download and install them. By verify, I mean checking to see the developer's history, prior products, reviews and going online to carry out some basic research before installing an app. Many smartphone users download and install apps that come packaged with malware that gives a remote hacker root access. The problem is mainly with Android phones due to the relaxed rules required to host an app in the Play Store. iPhone users are safer due to Apple's closed wall policy.



Simply Tapping On Links

According to RSA's cyber security experts, smartphone users are more susceptible to phishing attacks than desktop users. They tend to be less vigilant about security. It is harder to spot a fake login page on a smartphone than on a computer. Further, shortened URLs make it harder to detect illegitimate addresses. The best defense is to avoid clicking on links sent via SMS or instant messaging apps. Also, always open email links using your computer.

(Image credit: Flickr)

Jailbreaking or Rooting

I know I will get lots of flak for this from hardcore ‘jailbreakers’ and ‘rooters’ on this one. The fact of the matter is that non-rooted Android devices and non-jailbroken iPhones have security safeguards that limit the amount of access a user has to vital parts of the phone’s operating system. Jailbreaking or rooting gives you access to hidden system settings that allows you to do much more with your phone. Of course, the price you pay for that is greater security risk.

But, I am not saying you should not jailbreak or root your phone. All I am saying is that if you choose to do so, make sure you know what you are doing. If you are new to these concepts, please read our Android Rooting Guide and our article on Jailbreaking for newbies.

(Image credit: Flickr)

Not Switching Off Bluetooth

Have you heard of the terms bluejacking, bluebugging or bluesnarfing? These all describe a situation where a hacker gains access to your phone using your Bluetooth connection. Using this technique, the hacker only needs to be at least 30 feet away from you and you’ll never know what hit you. Within seconds, a Bluesnarfer can steal data such as confidential information and even login data to various sites. So, unless you are transferring or receiving a file, switch off your Bluetooth connection.

Forgetting To Log Out

If you are always logged into PayPal, Amazon, eBay and other sensitive sites where your finances are within easy reach, you might as well leave your credit card lying on the table at your local eatery. Don’t keep your phone permanently logged into such websites. Don’t check the box in the app that asks to save your username and password. It is convenient not to have to log into the app every time but it exposes you to considerable financial risk. If your phone were to be stolen, a thief would have unrestricted access to your finances and you could end up with a massive bill for things you never bought.

The same goes for a browser. If you log into sensitive sites such as mentioned above, do not give the browser permission to save your username and password. Also, make sure you clear your browser history after surfing for sensitive material. Chris Hoffman published an excellent article on how to delete your Android browser history and for the iPhone users, read "How to Delete Any and All History on Your iPhone" by Joshua Lockhart.

Storing Sensitive Data On Your Phone

I have never quite understood why some people insecurely store credit card PINs, bank online passwords, social security numbers and other such sensitive data on their phones. In the event your phone is stolen, it wouldn't take a genius to figure out that a four digit number stored as a phone contact is a PIN to one of your accounts. With a bit more digging, a clever crook can mess up your life.

The Take Away

The safeguards for all the mistakes listed here are easy and simple to implement. The problem is that many people take security for granted and assume the worst won't happen to them. Security is about 'when' you get hit not *'if'* you get hit. At the end of the day, you must take charge of your smartphone's security.