The Increasing Threat of Malware for Android Devices

6 Ways Hackers Are Stealing Your Private Data – and How to Stop Them

INTRODUCTION

If you own a smartphone running the Android operating system, like the popular Samsung Galaxy, your personal data, financial security, and privacy could be at risk.

The reason? An unprecedented rise in malware, viruses, and other threats that can collect text messages, make phone calls and send texts to premium numbers, take pictures, record from your microphone, steal your contacts, and even log your keystrokes so as to capture your passwords.

Industry watcher Juniper Networks revealed in a recent report that malware on mobile devices skyrocketed 614% from March 2012 to March 2013. And the percentage of mobile threats targeting Android grew from 47% in 2012 to 92% in 2013. It's thanks to more than 500 third-party app stores offering malicious apps, as well as malware posing as legitimate games and others apps on the official Google Play app marketplace.

And that's not all. By early October 2013, industry watcher Trend Micro had already identified more than 1 million separate threats targeting Android. And the forecast for 2014 is even bleaker.

And with nearly 60% of all new smartphones shipping with Android in the last quarter...that means million of users at risk.

What makes Android so vulnerable? Well, it has an “open” system that allows a user to download and install virtually anything. Tech-minded users like this because it allows them to customize their device. But it also opens the way to hackers who can trick everyday users into installing harmful programs disguised as legitimate apps.

Unfortunately, most people with Android devices have no idea of these threats to their security. It's not publicized or talked about in the mainstream press. It's restricted to tech circles and industry forums.

But hope is not lost. A generation of new apps, such as Secure AntiVirus for Android! are becoming available that can scan Android devices for threats, eliminate them, and then shield them from future attack. It's a lot like antivirus software for a home computer or laptop – just for smartphones.

The creators of this app are seeking to spread the word and help unsuspecting users protect their personal data. They want everyday folks to be protected. In this report, you'll find tips for:

- Identifying suspicious emails, websites, and third-party app stores
- Determining if your smartphone is already infected
- Avoiding Android viruses, trojans, phishing attacks, and other malware
- And much, much more

Enjoy the report... stay safe... and for more information on Secure AntiVirus for Android! please visit: URL

Where Android Malware Hides

Users of popular smartphones, like the Samsung Galaxy series, running the Android operating system beware. You are the target of hackers trying to steal your personal data. And Android's "open architecture," which allows users to download apps and software without restriction (a feature tech geeks love because they can customize their phone), leaves you wide open to attack.

These attacks can steal contacts, financial info, passwords, send premium SMS, take pictures...and much more.

But there are ways to protect yourself. Your first step is to install an app to screen out potential threats. It'll catch malware before it's installed and find any malware already hiding on your phone.

Your next step is to avoid the places where Android malware live:

- Third-party app stores – These are notorious breeding grounds of malicious apps. The appear to be legit.

- Fake Google Play stores – Check the domain on what you think is the official Android app store. Often hackers will set up a similar URL and load up the site with malicious apps.

- Email – Just like on your PC, phishing emails have come to mobile. The message appears to come from a trusted source, when in fact the account has been hijacked by hackers. The file attachment is a malicious app that starts to steal data as soon as you install it.

- Google Play app store – Yes, even the official app store for Android devices is not immune to the malware threat. Remember, any developer with $25 can put up an app for sale. And Google's screening process doesn't catch all the evil-doers.

So watch out for these threats. If something doesn't look right... don't assume it's okay to download.

How to Determine If Your Android Device Has Been Compromised by Malware

It's not widely known outside of industry experts and those in the know when it comes to mobile technology, but smartphones running the Android operating system, like Samsung's popular Galaxy series, are extremely susceptible to malicious hacker attacks.

Experts have detected more than 1 million threats to Android devices already in 2013 in the form of malware, viruses, trojans, and more. And these devious programs, created by hackers, have the appearance of regular apps like games.

They can do significant damage by:

- Collecting text messages, call history, photos, and contacts.
- Taking pictures and recording from the microphone.
- Logging your keystrokes to figure out passwords.
- Sending text messages and making phone calls – often at great cost to the user.
- And more...

Most of the time users unknowingly download these programs to their devices. But there are ways to protect yourself from these threats to your personal privacy and sensitive financial information, as well as prevent having to pay out for premium texts and long-distance phone calls.

The first step is to figure out if your phone has been compromised. There are a few indicators:

1. A fast draining battery – due to the malware or virus running in the background.
2. Unusual dropped calls or strange noises.
3. Huge phone bills filled with text message and calls you didn't make.
4. An increase in data usage because the malware is uploading and downloading information.
5. Overall slow performance because the malware is using up processing power.

If you've ticked any boxes – or you're concerned about any future threats – you should download an app like Secure AntiVirus for Android!, which will scan for and eliminate any viruses. It will also protect your smartphone from future attacks by closely monitoring anything you download to your phone.

For more information on Secure Antivirus go to:
https://play.google.com/store/apps/details?id=com.pleap.av.app

Government Agencies Voice Concern about Security of Android Smartphones

You know there's a problem when the government weighs in with its opinion. And that's where the Android operating system, which runs the majority of smartphones and tablets on the market, finds itself.

In a recent report, the Department of Homeland Security and Federal Bureau Investigation (these are the big guns when it comes to security) cautioned government agencies about the dangers of using devices running Android. According to their study, the Android OS is much more vulnerable to malware, viruses, and other threats. It's subject to well over 90% of attacks on mobile devices.

These attacks can steal personal data, make phone calls and texts – often to premium numbers, log passwords, and more. Android malware poses a real threat to privacy and security.

A major cause is users running outdated versions of the Android operating system, says the report. But the widespread, worldwide use of Android is another factor. Of course, attacks can from a variety of sources. Third-party app stores are prone to hosting malicious apps. And even the official Google Play app store is not immune, with malware posing as popular legit apps.

The DHS and FBI report recommended that police, fire, and other emergency personnel take a close look at their use of Android devices.

Android Malware Hackers Driven by Profit – Not Just Mischief

Representing 80% of the smartphone market worldwide, Google's Android, which powers popular models like the Samsung Galaxy series, is the hands-down most-used operating system in the world.

But what most of those millions of users don't know is that Android lacks security features to protect them from hackers seeking to steal from them through viruses and other malware. In fact, according to a new report from security firm F-Secure Threat, 77% of Android malware was profit-driven. And with 96% of all malware targeting Android specifically... that's millions of users at risk around the world. Although Europe and North America currently is where most of these “money stealing” malware attacks target.

In some cases, “bots” installed on smartphones by unsuspecting users steal bank log in information and send them back to the hackers who created the malicious programs. In other cases, the malware takes control of the smartphones SMS sytem to send texts to premium numbers controlled by the hacker, with the charges going to the user. The average “hacked” SMS case cost the user more than $10.

One particularly sneaky trick involved hackers first stealing the contacts from smartphones. They would then send all the contacts an invitation to a fake membership website that cost money to join. Thinking the invite was from a friend, many users actually signed up and paid to join.

Android Malware Now Cloaked in Email

The issue of malware has long been an under-the-radar problem in the Android community. And though Internet security experts have noted that Android is subject to well over 90% of malware attacks and there were more than 1 million malware identified so far in 2013, most users of smartphones with that OS not even aware there are malicious programs out there. Even fewer know the extent to which this malware can steal personal and financial information and cost the user money by:

- Sending premium texts and making phone calls
- Logging keystrokes to steal passwords
- Recording text messages and listen to voicemails
- Taking pictures and recording with the microphone
- Swiping contact lists
- And more

In the past, hackers and identity thieves focused on tricking users into installing their malware in the form of malicious apps on thirty-party app stores and the official Google Play store. But according to researchers at Kaspersky Labs, they now they have a new plan of attack: email. And it looks an awful lot like the phishing and virus-laden emails you get in your inbox from time to time.

It works like this:

1. You receive an email from what appears to be a trusted source. But hackers have infiltrated that account and then sent the malicious email to that contact list.
2. The email has a file attachment with a name related to something the sender does. (For example, if they were an accountant, it might say 2014 Tax Instructions.)
3. In reality, it is an Android Package file, which you can recognize because of the extension .apk.
4. Opening the email, opens an Android application and ask you to install it on your phone.
5. Once you install it, the app starts collecting personal data from the phone and sending it back to the identity thieves, including contacts, call logs, geo-location, your phone number and model, and more.

A targeted attack by email on your smartphone, which, by the way, would have no affect if you opened it on your PC. Not unexpected given the tactics success in stealing private information on PCs. But it's something you can avoid if you pay attention. Never install apps you receive by email without triple-checking their source, even from supposedly trusted contacts. And it's also a good idea to have an anti-virus app installed on your smartphone to screen out any threats that make it past you.

Four Easy Ways to Protect Yourself from the Threat of Android Malware

The year isn't even out and already mobile security experts Trend Micro have identified more than 1 million malware, viruses, and other threats released on unsuspecting users of smartphones with the Android operating system.

These threats pose great danger to personal and financial security, as well as privacy, because they can:

- Collect text messages, voicemails, and contact lists
- Log keystrokes to determine passwords
- Record from the microphone and take photos
- Make phone calls
- And much more

Some of this malware can cost you immediately too. Some malicious program hijack phones to send premium text messages – at an average cost of $10 per affected device.

But you can do something do something about it. Here are four ways you can protect yourself from the increasing danger from Android malware:

Make Sure You Have the Latest Version of Android

Yes, waiting for your phone to download the latest operating system update can be inconvenient. But you should definitely upgrade your operating system regularly. Security does improve with each new version – at least protecting you from previously identified threats.

Install Apps Only From Reputable Sources

Although the Google Play marketplace has not totally eliminated hackers who manage to offer malicious apps for download to unsuspecting users, it is safer than third-party app stores. A recent study found that more than 500 of these “unofficial” app stores had malicious apps.

Often these dangerous programs will look identical to legitimate apps. Yet, running in the background are programs that serve adware that clogs up your processor and slows down your phone... send premium text messages at cost to you... steal your contacts and log in info... and much more.

So stick to the Google Play store... and still watch your back.

Watch Out for Apps that Ask for Unusual Permissions

When you download an app and are installing it make sure the permissions it asks for match its purpose. If it doesn't, that could be a sign that it's malware. For example, a game shouldn't need access to your contacts...or be able to send a text.

Install Anti-Malware Software or App

This is really the only nearly fool-proof way of protecting yourself.

If you already suspect your phone might be “hacked,” an anti-malware program will scan your device and eliminate the threat. And it will protect you in the future by alerting you to anything you're trying to download that doesn't look right.

Android Malware Hijacks Legitimate Apps

Viruses, trojans, adware, and other malware have been in the bane of the Android operating system since the beginning. These malicious programs have infected millions of devices running Android, which account for the majority of smartphones on the market today.

There are some places where malware is known to live: third-party app stores, torrent sites for downloading pirated content, and phishing emails. But now security researchers have discovered another way ingenious hackers can infect an Android smartphone and steal personal and financial data from users, as well as send premium texts (at cost to the user), make phone calls, listen to voicemails, steal contacts, and more.

The malware actually hijacks real, legitimate apps, including popular games like Angry Birds, that are available on the official Google Play store. Once the user downloads it, the hijacked app behaves exactly as it should. But in the background, the hacker can do anything he wants with the phone. And all he had to do was add some code to app's command and control software using an Android software development kit.

This is just the latest iteration in the malware threat to Android devices. More than 1 million threats to Android have already been identified so far in 2013. And analysts see even more growth in malware for 2014.

Luckily this latest threat can still be stopped... if users have an anti-malware app on their device that can screen for and eliminate threats. Big name anti-virus software companies have gone mobile. But many users prefer to use apps from smaller developers, including the highly-rated Secure Antivirus, which was recently-upgraded. For more information, go here:
https://play.google.com/store/apps/details?id=com.pleap.av.app