Mobile Security: How Smartphone Increase the Risk of Personal Privacy Threats?

digitalmarketingtrends.in/mobile-security-how-smartphone-increase-the-risk-of-personal-privacy-threats/

Angela Smith July 18, 2018

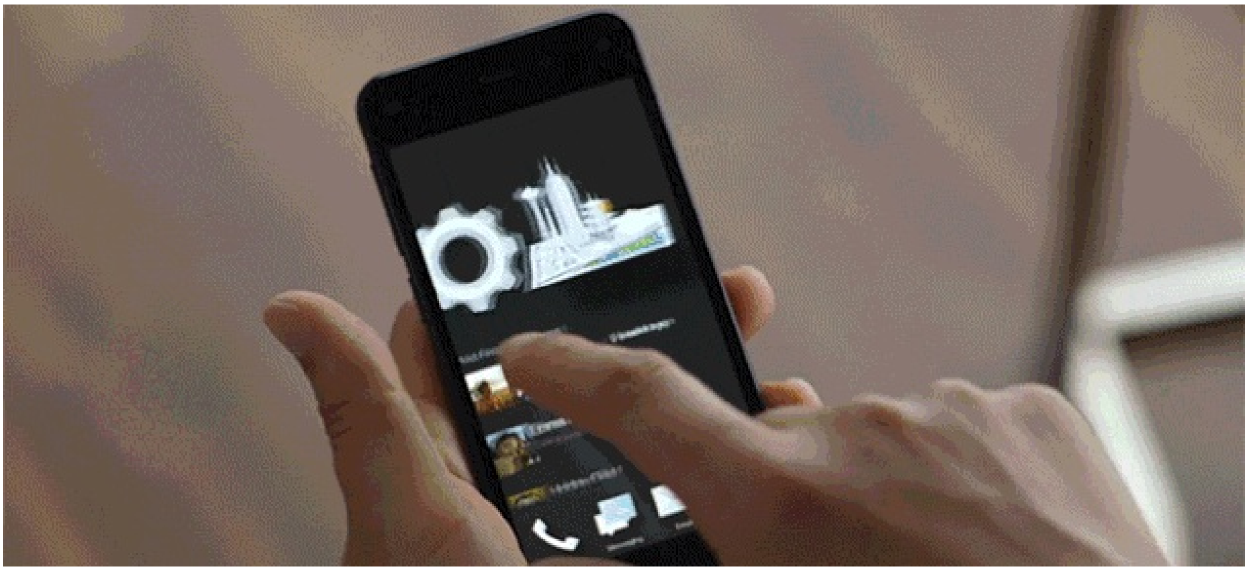
Mobile Security: How Smartphone Increase the Risk of Personal Privacy Threats?
(90%) Votes

MOBILE SECURITY: HOW SMARTPHONE INCREASE THE RISK OF PERSONAL PRIVACY THREATS?
[dmt]

> **Smartphones are the best tech –creatures in the contemporary world and everyone has owned their cell phone running with different operating systems such as Android, IOS and plenty of others alike.** 😎

You may have seen young kids and teens have their individual mobile phone devices and they used it all day long. It means people no matter what their ages are such as children, teens, adults and older ones have to have cell phones devices.

Because smartphones have become a need of the hour and everyone has to make calls, text messages, shared media files such as photos and videos and use of social messaging apps have become very common activity connected to the internet.



There are tons of free apps including social networking apps are available, but with plenty of type's vulnerabilities and malicious codes that can get access to personally identifiable information data that is been used for advertisement and even for marketing purposes. However, there are many other dangerous apps that can ruin your personal privacy via device sensors, camera microphone, and others. These apps can put your privacy at stake and can work as a GPS location tracker, steal confidential data, gallery stored photos and calls.

Major Types of personal Privacy threats via Smartphones

Threats via SMS

The SMS or text messages can become more vulnerable and it is one of the most popular choices for programmers that are black hat hackers all across the world. You may have received flying messages that usually promote some kind of services. These types of messages being received on your smartphone or android and IOS devices may put you in real trouble because it might be from smishing. The particular terms usually used for phishing attacks that can be sent on your smartphone through SMS and it can steal the confidential data of your smartphone to the fullest and Smishing can be earned with the help of return message and even through prompted to call a number where information is being recorded. All the recorded information could be very handy in order to create a fake bank account.

Wi-Fi & Bluetooth security risks

You may have got free or open Wi-Fi hotspot and people usually want to use free things without paying the single penny. All these types of things can become risky in terms of stealing personal data from your cell phones, passwords, credit card, data and plenty of other handy –identifiable information. If you are used to of using free Wi-Fi stuff, then now own wards you need to ignore this kind of networks until and unless they belong to the well – reputed businesses. However, if you are using the hotspot on your cell phones of android or IOS device then you need to protect your password. However, after a couple of days, you should change the hotspot feature. However, there is another vulnerability that is WAR Texting, in which smartphones connected car system can be tracked via sniffing the codes that can be sent through the phone to the car. You may lose your car at the end of the day.

Related articles: What happens when smart devices record a crime?

Passwords being used on a cell phone device, whether you have used it for protection, setting up on Bluetooth, then you need to change these passwords after some days. Because these passwords could be cracked and you may have to lose many things stored in your smartphone.

Location-based threats

Wireless networks, cell phones GPS location trackers and other location-based tools for smartphones and tablets are not less than blessing these days. But on the other hand, it can put your personal privacy and at stake to the fullest. Therefore, smartphone users have to take care of their devices because their location-based tools can put their privacy in real trouble and someone can easily track your GPS location. Out of all location-based vulnerabilities are geotagging and you further need to remove or disable all these kind of tools from your cell phone device in order to keep your location a secret.

Rouge Apps can breach personal privacy: A real Threat

There could be some rogue apps on any kind of platform. However, when it comes to android it usually has seen and on IOS, windows phone such apps are unlikely to be permitted to be listed. However, it would be trouble for you if you have already installed it on your smartphone. Therefore, a user should install the apps from the trusted platforms such as Android apps need to be installed from android play store and on iPhone apps need to be installed from iPhone play store and Voice Verse.

Related articles: Coming of Age: Marketing Trends to Capture the Millennial Generation

Installed apps can remotely view surroundings of your smartphone. Over the year's number of threats has detected on Android cell phone devices and people have lost the secret or private information from the android cell phone device within in minutes. However, android backups are possible with the help of data backup software for androids.

Conclusion:

Over the last few years, the smartphones vulnerabilities have increased in terms of personal privacy threats. Therefore, a user needs to have backups for the personal confidential information and they should protect their smartphones from malware, rogue apps and from other tools that can steal your private information. 😉