# Chapter 15
# Importance of Information Security and Strategies to Prevent Data Breaches in Mobile Devices

**Maulik Desai**
*Swinburne University of Technology, Australia*

**Swati Jaiswal**
https://orcid.org/0000-0001-9671-534X
*SKNSITS, India*

## ABSTRACT

*Mobile devices have upgraded from normal java-based phones whose basic functionality was calling, messaging, and storing contact information to a more adaptive operating system like Symbian, iOS, and Android, which have smart features like e-mail, audio player, camera, etc. Gradually, everyone started relying more and more on these mobile devices. This led to an increase in the number of cell phone hackers. Common ways that a hacker gets access to your phone is via phishing, shoulder surfing, piggybacking, etc. There are countermeasures to this like bookmarking your most visited sites, using VPN, using encryption algorithms. Data theft and identity theft are a new concern for today's user; this chapter is to educate the end user of different ways in which their privacy can be invaded via a mobile phone. This chapter will help the researchers to know the mindset of a cell phone hacker and what are the potential damages that can be caused by them and strategies to prevent them.*

## INTRODUCTION

Smartphones have been around for ages now. The best thing about them being the mobility that they offer and how one can use them anywhere that suits them. In 2017 around 1.54 Billion smartphones were sold worldwide this includes, smartphones that had operating system as (Android, Symbian, Windows,

DOI: 10.4018/978-1-7998-1005-6.ch015

iOS, etc.) which is a significant increase in number from last year which was 1.49 Billion smartphones. The smartphone industry is booming like never before to give a frame of reference in 2012 just 5 years before this the number of smartphones sold were 680 million and today the number is almost thrice. Smartphone was helping end users to accomplish complex task at just the reach of their hand but it also came in with an unknowing alarming issue that is data breach and Information leakage. Initially, the hackers were persistent on breaching the data on desktop only but as they found out that more and more users are shifting to the world of smartphone they, started targeting the unknown world of smartphone.

The hackers started finding Breach in the system using third party application. The common thing among all this smartphone is that they have the application store of their own. Hackers can simply add a new application on the application store and once you download and install it the Virus can be multiplied (worm virus). This is happening because smartphone is becoming the most preferred platform for using the Internet medium. As soon as you are connected to an internet source in the form of Wi-Fi or 2g or 3g internet, you are vulnerable. If you are using, public Wi-Fi more than often, than chances are there that your information is already compromised and you can't do anything about it. According to the report created by cheetah, one in every five virus-infected phones is from India. This is an alarming rate at which this is turning out.

As quoted in the Paper "*Emerging security threats for mobile platforms*."

*Smartphones are also vulnerable to malware, which are malicious programs designed to run on infected systems without their owners' awareness. While users are keen on downloading apps from app markets, this provides hackers a convenient way to infect smartphones with malware. For example, they would repackage popular games with malware and distribute them in the app markets. Very often users are attracted to download the infected apps. A recent survey reported that 267,259 malware-infected apps have been found, among which 254,158 reside on the Android platform. It also suggested that the number of malware in apps has increased by 614 percent since 2012. There are also a variety of other ways for mal- ware to infect targets. Some malware is dis-guised as the macros of files. Some are installed through certain known vulnerabilities existing in a network device or mobile platform. Some are installed in victims' smartphones when they click a multimedia messaging service (MMS) message or open an email attachment. In any case, malware can cause serious issues relating to information security and data privacy, with severe repercussions for users and even organizations. In this chapter we first discuss the potential threats to the information security in smartphones. We discuss the way we can prevent them from happening and the techniques that can be used to implement it (Delac G et al., 2011).*

## Common Types of Malware

- **Expander:** This type of programs is used to make a purchase on the victims' phone bill without him/her knowing about those ill-legal purchase and finally, will come to know about this after the end of their billing cycle.
- **Worm:** This type of virus multiples, itself and spread to the devices that are connected with it. Worms can be harmful because they might be given destructive instructions. They can be transmitted using SMS or MMS, they don't require any action from the user, they are slow and difficult to detect.
- **Trojan:** The require user command to execute itself. They are quick and can cause a serious damage to the mobile OS and even harm some personal data.