Like any other application, Mobile apps also need our attention from the security perspective. They are as vulnerable to cyber threats such as malware, phishing, pharming, etc., as web applications. These threats get even harder to counter in case of rooted or jailbroken mobile devices. It would not be correct to assume that attacks on such mobile devices will always be successful, especially when they have security measures in place. However, the fact is that they will not hamper the motivation of a dedicated attacker. Implementing basic security controls, such as installing antivirus on your mobile devices, is not always enough to keep the hackers away. It needs regular mobile app security testing, along with other mitigation means, to overcome threats.

Before we look into how we can mitigate threats to our mobile apps, let us first consider the motivation for hackers behind reversing and tampering with mobile apps.

The first thought that probably comes into your mind is that hackers do it to gain access to your sensitive data, or to develop a better understanding in order to build their own malicious replica of your device, or perhaps, to modify the code in order to bypass authentication and other controls. All these possibilities are correct. But there is another motivation behind these attacks which may not cross a common person’s mind. Advanced apps naturally have complex coding and logic flows involved, which interact with their IT infrastructure in backend. Laying hands on a single app can put the reigns in hacker’s control and set the entire IT assets of the app owning organization at risk. This is the real motivation why many hackers intend to modify or reverse mobile apps code.

***How can we Mitigate Threats to our Mobile Applications?***

An attack to reverse, tamper or debug an app can be made ineffective with the help of concrete mitigation steps. Let us look at some of those:

* Fumbling an application code makes it very difficult for the attacker to understand the meaning and flow of the code, thus making the hacking process further hard for them.
* Encrypting all app files, assets and resources, making it harder for hackers to access them. In case the code gets tampered with, it will still not allow a modified app to run.
* Creating a debugger app to mitigate reverse engineering when connecting an app to debugger.
* Making mobile app security testing a part of application development process.

All security professionals need to consider assessing their organization’s security posture and proactively take mitigation steps to reduce the probability of security threats to mobile apps.