# Security Features

**Strong Hack-proof Code:** Mobile apps are highly vulnerable to malware attacks and data breaches and this mandates that developers pay extra attention to write a robust code that is free from backdoors which in turn could be infringed by hackers.

**Use the Latest Cryptography Techniques**: Most widely used cryptographic protocols and algorithms such as MD5 and SHA1 are insufficient as per modern security standards. Therefore it is better to use state-of-the-art encryption APIs such as 256-bit AES encryption combined with SHA-256 for hashing.

**Require Data Validation / Integrity Checks:** Most secure applications will require a username to login. You should control that input so that it will only accept valid usernames.

**Disable Debug Code:** Debug code is often used during the development process to help developers test for errors and figure out what is causing them. Once the app is in production, however, it should be disabled. If left in, and a hacker gains access to the debug clause, they will be able to see how the application is handling input and users moving around the app. This can translate into a roadmap for them to the best way to exploit the app.

**Ensure Data Security during Transit and Storage:** The biggest challenge posed to mobile app security is that mobile apps have to connect with external networks. They connect to internet via Wi-Fi, cellular networks, VPN, non-encrypted networks, and so on. This has to be given special consideration by developers and precautions should be taken to encrypt data during transit. All the critical user information like login details, passwords, personal info should be encrypted. The data should be stored in encrypted data containers and any unnecessary data should not be stored within phone memory at all

**Don't Log Sensitive Data :** Be sure to review what your application is logging and ensure that you're not storing sensitive information, including usernames, passwords, or account numbers, that a hacker could access.

**Sanitize Background Image:** If you navigate away from your banking app and it takes a screen shot of your account information, a hacker could get this info. Sanitizing the background image means that you put a static image in the place of a live screenshot.

**Restrict Clipboard Access:** Hackers will always go to the clipboard data to see what information they can glean to make their job easier, like usernames and passwords. You can restrict the ability to store anything on the clipboard from your app.

**Test for Vulnerabilities:** When a hacker attempts to exploit a mobile application, their goal is to identify and exploit vulnerabilities in either the mobile application or any backend web services / infrastructure of the application in order to gain access to the system and /or sensitive data, so it's important that the engagement includes both.