# Are Banking Systems Vulnerable To Security Issues?

Mobile app security is one of the biggest concerns faced by the financial sector, and this vulnerability has led banks to experience theft of funds.

## Why bank should be bothered?

Yes, this is a great hassle and bank applications, although every mobile banking application must go through an acceptable level of security.

And you should know that clients are mostly affected by these security issues, due to unauthorized access to user data. You should know that almost 76% of mobile banking issues come up without any physical interference to the device. This means the information from the banking apps is at the risk and can leave the users' data exposed to some malicious activities without any prior information given.

## Banking applications; prone to experience security issues

As we all know that Android apps are more vulnerable to security hassles, as this OS involves insecure deep link handling. The development process on Android experiences more freedom of implementation, compared to iOS. It has been observed that the server sides of mobile banking applications consist of 54% of security hassles, and each mobile bank has 23 server-side vulnerabilities.

These server-side vulnerabilities are experiencing around 43% security issues in business logic. And this issue further attracts hackers to get sensitive user information and brings fraud.

In this context, the user credentials are more prone to the security attack, also it has to be taken into consideration that users must avoid jailbreaking or rooting their devices, and they must download applications only from official stores.

This ensures to avoid any suspicious activity from any unknown links from SMS and chat messages, and always install the latest updates for OS and mobile applications.

*Olga Zinenko from Positive Technologies stated, "Banks are not protected from reverse engineering of their mobile apps. Moreover, they give short shrift to source code protection, store sensitive data on mobile devices in cleartext, and make errors allowing hackers to bypass authentication and authorization mechanisms and bruteforce user credentials. Through these vulnerabilities, hackers can obtain usernames, account balances, transfer confirmations, card limits, and the phone number associated with a victim's card."*

*He has also mentioned, "We urge that banks do a better job of emphasizing application security throughout both design and development. Source code is rife with issues, making it vital to revisit development approaches by implementing SSDL practices and ensuring security at all stages of the application lifecycle."*

## Conclusion

Mobile app security is the concern, which has to be addressed at every possible level. However, not every mobile app builder can address this issue, but a **leading mobile app development company** like Techugo can well-handle these issues. Each of our apps is successful due to the incredible features and functionalities that have been integrated well in the solution, to provide a seamless experience to the users.

Get in touch with us today and help your business flourish out of bounds.