The proliferation of mobile devices, applications (apps) and operating systems continues to drive innovation and lead to increased threats and vulnerabilities. As the mobile ecosystem expands, it becomes increasingly important for organizations to be vigilant about the management of sensitive information via mobile devices.

The mobile development lifecycle is a complex environment that is constantly evolving, which creates a hyper-dynamic environment for developers. These complexities often increase the attack surface, particularly for customer-facing mobile banking apps.

The NowSecure Lab Automated tool was used to assess the security of mobile banking apps against fraud and penetration attempts. A total of 780 tests were performed across the mobile banking apps from 15 unique North American financial institutions on both iOS® and Android™ operating systems (30 total apps).

To address security vulnerabilities throughout the mobile development lifecycle, security professionals must address security vulnerabilities throughout the mobile development lifecycle. With this in mind, security professionals must develop top-of-mind and is embedded security throughout the enterprise’s mobile lifecycle. With this in mind, organizations and industries, it is critical that security remains a focus throughout the development process.

3. Selecting the technologies
4. Developing a mobile security strategy
5. User access
6. Governance & compliance

Embracing new app development and mobile technologies can improve security posture. Organizations can incorporate a mobile app development security plan that is designed to address vulnerabilities at every stage of the mobile development lifecycle. This plan should provide a roadmap for organizations to follow when integrating mobile technologies into their overall security strategy.