CASE STUDY

A Top 10 Bank in Thailand Adopts AppProtect+ Mobile App Protection Solution.

Scammers are increasingly more sophisticated in the way they get access to their victims' personal information. Most companies, including banks that are operating in a hybrid working environment, allow their employees to log into their computers from remote locations. While remote access is convenient, it also poses a threat to government agencies and financial institutions. This is because hackers can disguise themselves as IT professionals from trusted sources like banks or telecom support teams to connect, install and take control of their victims' mobile devices via Remote Control applications such as TeamViewer. In most cases, this causes personal details to be compromised.

Rooted or jailbroken devices are another major cause for concern for all mobile app service providers, as malware can bypass security controls provided by the manufacturer allowing the phone's owner or hackers full access to the system. This means users can download third-party applications not approved or qualified by either Apple or Google stores. Hence, there could be a chance that the apps installed may contain malware, Trojan horses, or viruses which runs a higher risk of having critical information stolen.

It is due to the rise of these online threats has made one of Thailand's top 10 banks look at ways to protect its mobile app from such threats and attacks. Therefore, it is paramount to ensure that their customers are protected from scammers and cyber threats, such as those mentioned above. On top of that, there was also a directive from the Central Bank of Thailand to all financial institutions to ensure that all banks' mobile apps and financial systems are secure.

The financial institution also wanted a solution that can easily integrate with its existing mobile applications as soon as possible. Additionally, it also required that the solution can be easily managed by the bank's stakeholders. For instance, no additional lines of code need to be added to shield the app.

After reviewing the available solutions in the market, the bank decided on YESsafe AppProtect+ to address the protection needs of their banking app. It prevents reverse engineering, safeguards sensitive data, and protects end-users from sophisticated malware attacks on mobile apps. It provides vulnerability detection, app protection via Runtime Application Self-Protection technology, and App Usage Information to respond to the real threat of sophisticated malware. AppProtect+ is EMVCo certified and recognized by Gartner, a leading global technology research and consulting firm.

Once the new AppProtect+ security shield is applied, the bank's financial services app will be protected against the ever-changing threat landscape while maintaining a frictionless customer experience. Upon implementation, a series of tests were done to verify that each functionality worked as expected. YESsafe AppProtect+ went through a series of stringent tests to ensure the bank's financial app is protected to fight against threats, including:

- Malware attacks
- Vulnerabilities related to rooting, jailbreaking, or emulation
- Debugger and Block Java connection
- Code or framework injection
- Application repackaging and app integrity breaches
- Overlay attacks
- Screenshot detection
- Man-in-the-app and man-in-the-middle scenarios

With YESSAFE AppProtect+, apps can also run securely on rooted or jailbroken devices.

As more users shift from computer to mobile in search of information and services, we see an apparent growing trend in mobile attacks. Businesses are being put at risk for regulatory compliance violations, stolen user data, and, more importantly, loss of user trust, bringing irreparable damage to brand reputation.

AppProtect+ stays abreast with the ever-evolving malware attacks and is continuously updated to keep up-to-date with evolving threats. This new and updated banking app now offers its end-users improved security features without compromising performance and user experience.

Further details about i-Sprint's products are available at *www.i-sprint.com.*
To reach us, please email us at *enquiry@i-sprint.com.*