KPMG

Defending Digital Finance: The Current State of Mobile Banking Security Among Hong Kong's Retail Banks

A new wave of cyber attacks is targeting mobile banking

- In response to the increasing prevalence of malware scams and cyber attack tactics targeting mobile banking apps, the Hong Kong Monetary Authority ("HKMA") has taken action in Q4 2023, requiring Authorized Institutions ("AIs") to thoroughly examine their mobile application security measures.
- The HKMA reiterated the security requirements outlined in the Supervisory Policy Manual ("SPM") TM-E-1 Risk Management of E-banking, specifically addressing the use of mobile devices and the implementation of soft tokens. Furthermore, banks are advised to periodically reassess their mobile security controls in response to the emergence of malware attacks that exploit legitimate features and permissions on customers' mobile devices.
- Of particular importance, the HKMA expects banks to conduct a comprehensive review and implement specific risk management measures designed to effectively mitigate the risks associated with malware scams, such as side-loaded applications and known malware applications.

Evaluation of current state of mobile banking security measures

In response to the growing concerns surrounding attacks targeting the Android platform, we conducted a market research study in February 2024. KPMG testers downloaded the Android version of 122 HK mobile banking applications directly from the Google Play Store. We then simulated activities/scripts that are also used by real-life hackers for malicious purpose, to determine if the banking apps could effectively prevent or detect the simulated malicious activities. Here are the overall results across the 122 apps:

10 apps

Deployed measures to detect potential abuse of accessibility services

9 apps

Protect users from key logging with the use of virtual keyboard, or block the keylogging services

9

Apps do not allow other apps to overlay on the banking app to prevent tapjacking

Zero Apps

disallow the presence of apps which downloaded from unofficial sources.

52%

Of apps protect users from unauhtorised screenshot / screen recording / mirroring

Based on the available statistics from February 2024, banks are working on the development and enhancement of their security measures in general. This indicates a continuous and concerted effort within the banking sector to tackle mobile security concerns and improve the overall security landscape.

Good examples of mobile security measures

Here we have consolidated a list of good examples of mobile security measures adopted by the leading banks:

Mobile Platform Security Checks

- Determining the minimum acceptable operating system version to mitigate the exploitation of vulnerabilities and overlay attacks
- Detecting root/jailbreak to mitigate unauthorised actions
- Reviewing anti-hooking risks as a defense against unauthorised modifications

Malware Safeguards

- Detecting potential malware in known harmful applications
- Detecting applications from unofficial sources (sideloaded) to identify untrusted applications **with excessive permission settings**

Abuse of Mobile App Permissions

- Detecting malicious accessibility services and keylogging to secure actions initiated by customers
- Detecting application screen/keyboard mirroring and recording to protect banking secrets
- Preventing malicious touch interactions and overlay attacks to reduce the risks of social engineering attacks

How we can help

KPMG has worked with many leading banks and security solution providers to identify mobile security risks and uplift current security measures, our services include:

01 **Comprehensive Independence Review:** review on security controls to address cyber attack threats and identify compliance gaps. Our team has extensive experience in conducting assessments on e-banking services for banks in Hong Kong.

02 **Simulated attack test cases :** KPMG maintains a list of attack test cases that could mimic real-life malicious activities to evaluate the effectiveness of your mobile security controls.

03 **In-depth understanding on current market technologies:** Through our market research data and threat intelligence insights, we could evaluate your security posture comprehensively and provide specific improvement suggestions.

04 **Transform your mobile security standards:** Provide operational remediation suggestions and work with security solution providers to uplift your mobile security posture.

Contact us

Henry Shek
Partner, Cybersecurity
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Brian Cheung
Partner, Cybersecurity
KPMG China
T: +852 2847 5026
E: brian.cheung@kpmg.com

Lanis Lam
Partner, Cybersecurity
KPMG China
T: +852 2143 8803
E: lanis.lam@kpmg.com

Gordon Chen
Manager, Cybersecurity
KPMG China
T: +852 2847 5091
E: gordon.j.chen@kpmg.com

kpmg.com/cn/socialmedia