KASPERSKY FRAUD PREVENTION SDK FOR MOBILE

Kaspersky Fraud Prevention SDK for Mobile is comprehensive solution to protect mobile banking apps running under Android™, iOS® and Windows Phone. It combines Kaspersky Lab's market-leading IT security technologies to protect customers' account information, secure communications with the bank and ensure that there are no threats lurking on the mobile device used for mobile banking.

Kaspersky Fraud Prevention SDK for Mobile is highly flexible, enabling the bank to translate its user experience seamlessly onto its customers' mobile devices while offering them reliable protection against fraud.

Kaspersky Fraud Prevention SDK features five key areas of functionality to stop account takeovers, malware injections and other attacks before they can do any harm:

MALWARE SCAN AND REMOVAL

A clean, safe device is essential for safe banking operations. Even before a banking app is uploaded, Kaspersky Fraud Prevention SDK makes sure that the working environment is free of malware and vulnerabilities that might compromise security.

THREATS

- Malware infecting a device, before or after the banking app is uploaded

PROTECTION

- Before installing the main application a full malware and vulnerability scan detects any potential threats and enables them to be deleted. If the user refuses to remove detected malicious code, it is recommended that the banking app is blocked
- The Anti-Virus component protects the device in real-time and can perform on-demand scans of any installed software

RISK DETECTION

To ensure the working environment is safe before accessing the banking app, Kaspersky Fraud Prevention SDK checks for any risks associated with the device and its Internet connection.

THREATS

- Rooted or 'jailbroken' devices, and the presence of unofficial or obsolete versions of firmware that have unpatched vulnerabilities
- Untrusted Wi-Fi networks
- Apps that are, or could be malicious

PROTECTION

- Special components check for escalated user privileges on the device and verifies that all firmware is running in its most up-to-date version
- Wi-Fi Safety Analysis confirms that the user is connected to a trustworthy Wi-Fi network
- Risk Detection alerts the banking application to the presence of any dangerous or suspicious apps. The app can then warn users and help them to delete the suspect software. If the suspicious program is regarded as 'high risk' the banking app can be blocked until the danger is removed from the device
- Device Fingerprinting allows the banking app to analyze key information about the device (IMEI, IMSI, location, phone number, etc) within its own Anti-Fraud systems

MOBILE BROWSER PROTECTION

Most online banking operations require Internet access – and that means they need mechanisms that can secure the exchange of data between the user device and the online banking system.

THREATS

- Phishing and compromised sites
- DNS spoofing – a 'man-in-the-middle' attack that redirects traffic to the attacker's server
- Interception and modification of information between the mobile device and the infrastructure using fake certificates or compromised Wi-Fi channels

PROTECTION

- URL and Web Filtering components check the resource's reputation against a cloud-based database. The Web Anti-Virus component checks the body of the webpage for any malicious code. Unsafe resources are blocked and the user is notified
- DNS Checker confirms that this domain matches the bank's trusted IP address. If there is any discrepancy the banking session is terminated and the user is alerted to the problem
- The Certificate Validation component confirms the authenticity of the connected server. Wi-Fi connections are checked to ensure that they are encrypted

DATA AND SMS PROTECTION

Any online banking system needs to share important information with its users. This data can be vulnerable when it is sent from the bank to the user, or from the user to the bank. Kaspersky Fraud Prevention SDK offers protection against this.

THREATS

- Spyware that records keystrokes and transmits this information to cybercriminals, potentially allowing access to log-in credentials
- Interception and falsification of SMS messages between the bank and the user, allowing cybercriminals to access sensitive information or manipulate a transaction
- Malicious apps that can access important data on the user's device

PROTECTION

- Secure keyboard and secure input fields are used to protect the entry of all sensitive data
- Secure SMS recognizes and intercepts any messages from the bank. The messages can be deleted from the inbox and securely stored elsewhere
- Secure Storage provides a protected area to store sensitive data

SELF DEFENSE

Built-in features ensure that malware cannot interfere with the running of Kaspersky Fraud Prevention SDK.

THREATS

- Attempts to unload IT security software from the device, leaving it vulnerable to attack
- Modifications to the SDK-based application's resources or binary code
- Outdated antivirus databases leave the device open to attack from malware that was discovered after the last update

PROTECTION

- Kaspersky Fraud Prevention SDK includes a mechanism that prevents malware from blocking its protection technologies
- There are five key means of preventing modifications:
  - Applying the digital certificate of the SDK-based application, and running an integrity check
  - Re-launching the application if it is stopped
  - Protecting the main application in real time
  - Detecting injection methods
  - Disable debugging mode
- The updater tool refreshes antivirus components at least once every 24 hours, and ensures they are up-to-date before using the banking application

Kaspersky Lab also offers full support during the implementation process. Our professional services team is on hand to advise on how best to roll out Kaspersky Fraud Prevention – SDK, ensuring installation can be managed swiftly and smoothly.

March 15/Global

KASPERSKY lab