Kaspersky Fraud Prevention platform: a comprehensive solution for secure payment processing

Today's bank customers can perform most of their financial operations online. According to a global survey of Internet users conducted by B2B International and Kaspersky Lab, 91% of respondents regularly use online banking services [1]. However, 62% of them encountered at least one attempted fraud or scam during the year that meant they ran the risk of losing money from their accounts.

Cybercriminals don't just threaten individuals – they also target businesses. According to CyberSource, which provides e-payment automation services, North American companies lost about $3.5 million as a result of cybercriminal activity in 2012 [2].

Most financial organisations try to protect their users from cyber-fraud by introducing multifactor authentication and transaction approval services. They also make use of encryption technologies when sharing data between an online service and a user device. Unfortunately, these measures are not always enough to prevent money being stolen – cybercriminals who specialise in financial attacks have an array of tools that help them bypass the standard protective barriers used by banks.

For many years Kaspersky Lab has researched and developed technologies for effective protection against all types of cyber-threats, including those targeting the financial sector. Using this experience, Kaspersky Lab has developed Kaspersky Fraud Prevention – a complex security solution to counter online fraud. The platform provides multi-functional protection for all the stages of an online transaction and meets regulatory requirements for transaction security.

The platform includes client applications to ensure safe online payments and a server solution that functions within the IT infrastructure of the financial organisation. Moreover, it features Kaspersky Fraud Prevention SDK – a special technology framework for building secure mobile apps, reinforced with Kaspersky protection technologies. Each transaction goes through several phases of authentication, during which the security status of the user device is closely monitored and controlled. The system notifies the bank's specialists as soon any suspicious activity is detected.

As well as protection technologies, Kaspersky Fraud Prevention offers several services, including training, reporting on financial threats, etc.

[1] Security in a multi-device world: the customer's point of view Kaspersky Lab August 2013

[2] CyberSource 2013 Online Fraud Report

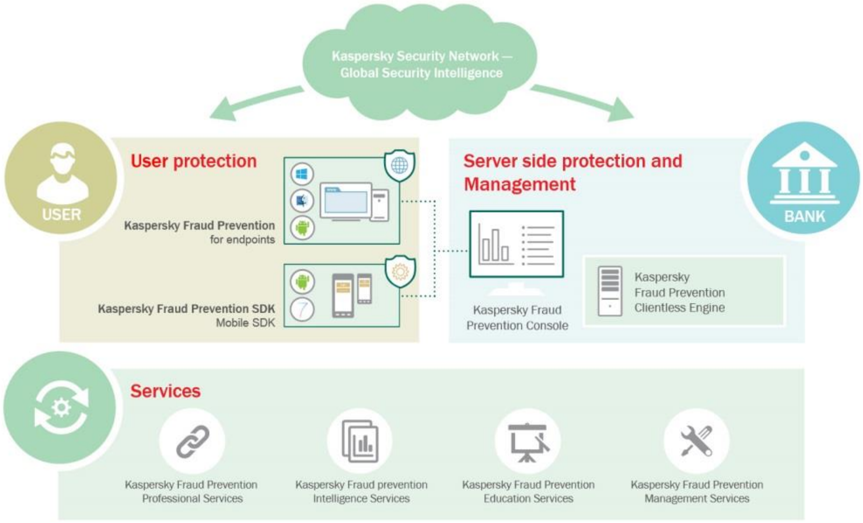
Kaspersky Security Network — Global Security Intelligence
USER
User protection
Kaspersky Fraud Prevention for endpoints
Kaspersky Fraud Prevention SDK Mobile SDK
Server side protection and Management
BANK
Kaspersky Fraud Prevention Console
Kaspersky Fraud Prevention Clientless Engine
Services
Kaspersky Fraud Prevention Professional Services
Kaspersky Fraud prevention Intelligence Services
Kaspersky Fraud Prevention Education Services
Kaspersky Fraud Prevention Management Services

Figure 1. Kaspersky Fraud Prevention components can work separately or in conjunction with each other, providing efficient multi-layered protection.

Protection for endpoints

Client devices tend to be the most vulnerable part of any online transaction. Analysis of data collected by Kaspersky Lab during financial cyber-attacks shows that it is usually the customer who falls victim to malicious activity, not the bank or payment infrastructure. As a rule, users are responsible for protecting their own devices. However, they don’t always install security solutions, or use generic antivirus products that have no dedicated defenses against complex financial attacks. Kaspersky Fraud Prevention for Endpoints, available within the Kaspersky Fraud Prevention platform, contains specific protection technologies that ensure users of online banking and e-payment services are safe.

The solution supports Windows, Mac, Android and iOS. All applications provide data protection on local devices and are able to prevent traffic being intercepted as it travels between a user and an online financial service.

If a company (a bank or payment system) plans to develop its own mobile application for Android or iOS devices, it can use Kaspersky Fraud Prevention SDK – a set of components to help create applications based on Kaspersky Lab protection technologies.

To work as effectively as possible, Kaspersky Fraud Prevention for Endpoints assumes data will be shared with the platform’s server components. The system collects statistical data from the Kaspersky Fraud Prevention console and makes it available to the bank’s specialists. This console also makes it possible to configure Kaspersky Fraud Prevention for Endpoints. This means that if a bank launches a new online payment service, the applications currently installed on user devices automatically get all the information needed to protect against a cyber-attack.

Detecting fraudulent activity

In some cases criminals can still gain access to online accounts by applying social engineering methods, for example, by fraudulently obtaining access data over the phone. However, even if this happens, the operator of a financial service can detect and block fraudulent transactions via Clientless Engine – a server component of Kaspersky Fraud Prevention.

Clientless Engine is integrated into a company's IT infrastructure and gathers data delivered from different information sources (abnormal user behavior, transaction details). The data is sent to Risk Engine – the system's central element, which carries out a risk assessment. To determine a transaction's legitimacy, Risk Engine uses the following data:

- Reports from the server antivirus module, which checks the web pages a user accesses while working with an online banking system. This component can detect malicious code embedded into a seemingly legitimate page to steal confidential information.
- User behavioral analysis during an online banking session, which can determine that operations are conducted by the account holder and not a third party. This feature generates a user profile built with a special mathematical model.
- Data collected from Kaspersky Security Network [3], including information about new cyber-threats and a database of devices with a "bad" reputation that was designed especially for the needs of financial organizations. A device can be placed in the database for a number of reasons, for example, if it is infected with malware or used to make suspicious payments.

Risk Engine receives the gathered data and the system determines whether an operation is legitimate based on a flexible set of rules. If there is evidence of illegal activity, the system uses a special interface to notify the financial organisation's specialists. They can then decide whether to approve or block the transaction.

Clientless Engine can enhance protection by receiving information from Kaspersky Fraud Prevention for Endpoints, although the server component is able to work independently from the other parts of the platform. This data sharing is useful when a financial organisation or an online store wants to protect customers without installing software on user devices.

Intelligence and education services

Along with the protection technologies introduced in Kaspersky Fraud Prevention, Kaspersky Lab offers a range of educational and analytical services:

- With **Professional Services** a financial organisation gets dedicated incident investigation and forensics performed by Kaspersky Lab's team of experts.
- **Intelligence Services** – customised reports on changes in the financial cyber-threat landscape delivered on a regular basis.

[3] Cloud-based technology in Kaspersky Security Network – Kaspersky Lab 2013

- Within the **Educational Services** program Kaspersky Lab experts provide training sessions for the staff of your financial organisation that focus on malware capable of stealing financial data.
- **Management Services Security Account Manager** – a dedicated Kaspersky Lab expert that helps resolve issues related to online banking threats.

Kaspersky Fraud Prevention benefits

Kaspersky Fraud Prevention offers a wide range of advantages to any financial organisation whose activities are linked to the processing of online transactions (banks, payment systems, etc.):

- Advanced technology to protect transactions on all types of popular computers and mobile devices;
- Fast and easy integration with existing solutions to counteract online fraud;
- Real-time access to Kaspersky Lab's extensive expertise in the field of countering financial cyber-threats.

Protecting financial online services from cyber-fraud requires effective security for transactions at all levels: from their initiation by customers to their approval by the organisation. These requirements form the basis of the Kaspersky Fraud Prevention platform: the solution uses an advanced multi-layered security system where the components work in harmony with each other to deliver maximum protection.

As a result, Kaspersky Lab's solution allows financial organisations to reduce the risk of cybercriminal incidents, and subsequent financial and reputational costs, to a bare minimum.