EARLY WARNING SYSTEM

Secure Bank

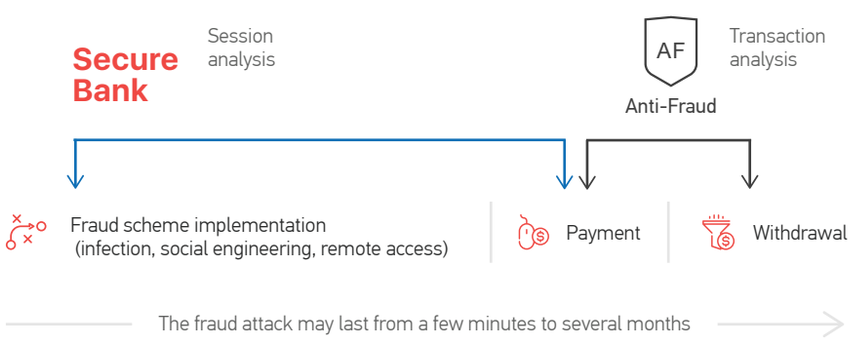
PROACTIVE FRAUD DETECTION

Secure Bank detects fraudulent activity in real time without installation of any additional software on client devices:

- Malicious injections in online banking pages
- Phishing attacks and social engineering
- Unsanctioned remote access to client's devices to conduct transactions on his/her behalf
- Banking Trojans designed to automatically create payment orders or replace banking credentials and payment amounts
- Intrusions through Zero-day vulnerabilities
- New malware versions

Modern cybercrime tools (remote connections, web injects to automate e-banking manipulations, Trojans intercepting SMS messages) make traditional client protection tools ineffective.

Standard Anti-Fraud Systems do not identify fraud preparation on the client's side. They do not activate until the transaction is executed and leave little time for decision making.



Secure bank eliminates "blind spots" in online payment security by detecting fraud attempts when logging into online banking.

Saves your money

Prevent crimes with early fraud detection

No equipment investments to cover the entire client base required

Reduce expenses for processing false positives and calls to clients

Strengthen your reputation

Increase the security level of your online banking systems and improve their attractiveness

Enhance clients' confidence in the bank by notifying them on infections and attacks

Reduce reputational risks by lowering the number of IT security incidents

UNIQUE THREAT DATA SOURCES

High-tech infrastructure designed to collect threat data enables us to monitor new fraud tactics and timely update indicators of compromise.

THREAT INTELLIGENCE

Group-IB leverages data on compromised accounts to prevent theft caused by both infected devices and data theft resulting from hacker attacks.

FORENSICS

Group-IB's Computer forensics laboratory analysts provide us with information on the most advanced malware targeting our clients.

MACHINE INTELLIGENCE

By processing large behavior data sets, machines detect malicious anomalies. Group-IB analysts select those related to fraud preparation and execution and employ machine learning to detect unknown fraud indicators.

Currently protecting over 50 mln banking clients

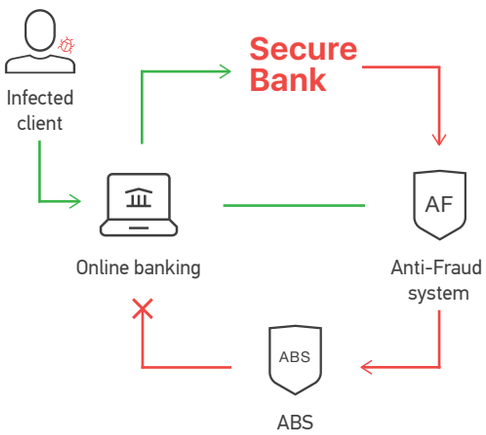
HOW SECURE BANK WORKS

DATA COLLECTION

The JavaScript module runs together with the webpage without any involvement from the customer. The scripts' functions are not noticeable to the bank's client.

The module monitors for any injection attempts on online banking pages, collects client device identification data and monitors for signatures of malicious activity on the client side.

The anonymized data is transmitted over a secure channel to Secure Bank server infrastructure.



The script does not slow the page loading speed.

DATA PROCESSING

To correlate and classify the data obtained, Group-IB uses accumulated and daily updated information from unique sources.

If fraud is detected, Group-IB immediately informs the bank security service.

The API can be used for direct integration with bank security infrastructure including notifications and established response procedures in real time.

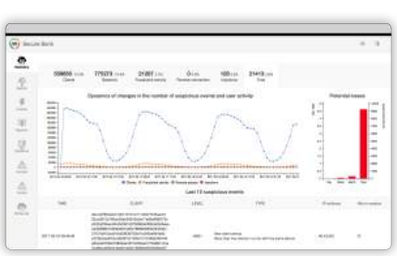
SECURE BANK CAN PROTECT YOUR BRAND

For theft of user credentials and bank card data, fraudsters create fake bank sites. Many of these are simply copies of original resources.

As soon as the first user enters the phishing resource, the module informs the Secure Bank system on the domain name of the website, which is detected by the module.

Secure Bank transfers the domain name detected to 24/7 CERT-GIB emergency response team, which will promptly block the phishing resource upon your confirmation.

MAXIMUM CONVENIENCE



Detailed information on each suspicious session is available in the web interface.

Cloud interface

All information on suspicious sessions is available in the web interface.

Documented API

Convenient integration with fraud monitoring systems and IT infrastructure.

Informative reports

Visualized statistics by periods and event types enables the client to track changes in attack dynamics and nature.

Threat Intelligence enrichment

Our team reverses malware daily to provide fresh updates to the system and accordingly protect you from the newest threats and changes in pre-existing attack patterns.

READY FOR INTEGRATION WITH:

Online Banking Platform

BSS

R-Style Softlab

Anti-Fraud

SAS

FRAUDWALL

RSA

Intellinx Insider Threat Intelligence

SIEM

QRadar®

ArcSight An HP Company

WAF

POSITIVE TECHNOLOGIES

CONTACT US

to test Secure Bank

+7 (495) 984 33 64

sb@group-ib.com

LEARN MORE

about fraud prevention with Secure Bank

sb.group-ib.com

MEET GROUP-IB

one of 7 world's best threat intelligence providers according to Gartner

www.group-ib.com