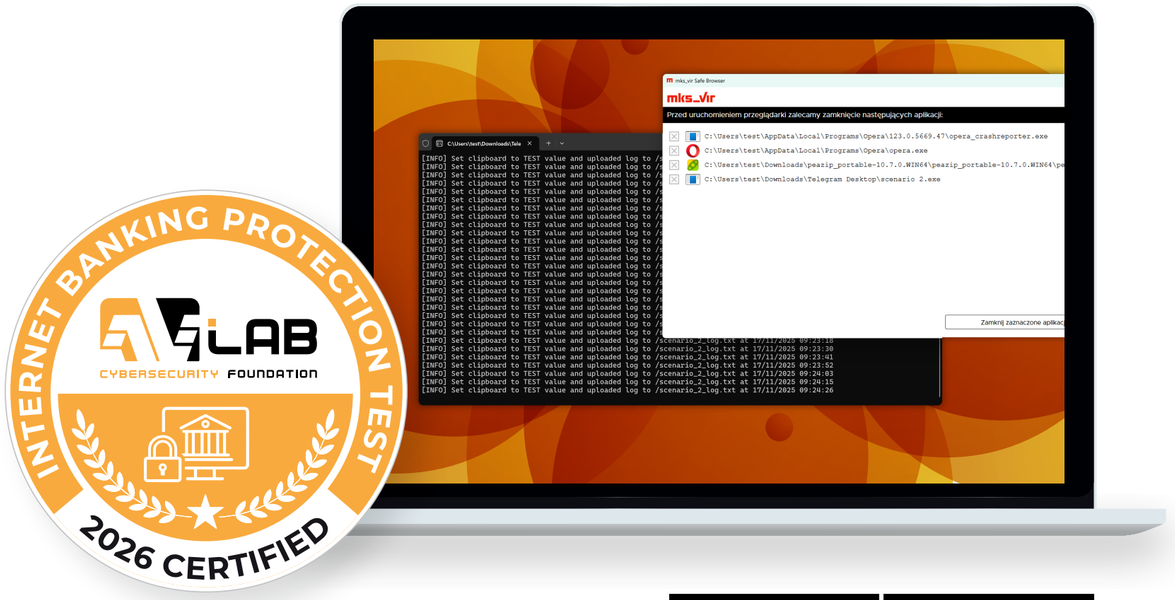
Analysis of modules for protection of online banking and payments

2026

mks_vir

MKS_VIR Internet Security + Safe Browser



Thanks to the Safe Browser module, the entire MKS_VIR package achieves an extremely high level of security during banking and payment operations, significantly minimizing the risk of data interception. Safe Browser works in close integration with the other modules of the mks_vir package, which continuously monitor system security, process activity, and attempts to access memory. This allows it to block unauthorized processes attempting to intercept the keyboard, clipboard, screen, or perform network operations.

Safe Browser uses a process whitelisting mechanism: before launching the browser, the module analyzes all active processes in the system and displays a list of potentially dangerous items to the user. This allows the user to manually close suspicious programs, such as remote access tools, PowerShell scripts, or other background applications that start with the system. This allows you to customize the environment to meet the more restrictive requirements of working with financial data. This design makes Safe Browser an additional, controlled layer of security, reducing the risk of malware activity in the system when performing online transactions.

Configuration:	Default	Hardened
CLIPBOARD HIJACKING	✓	
CLIPBOARD SWAPPING	✓	
KEYLOGGER SIMULATION	✓	
SCREEN CAPTURE	✓	
FILE DISCOVERY & EXFILTRATION	✓	
REMOTE CONTROL DETECTION	✓	
RANSOMWARE-LIKE ACTIVITY	✓	
REBOOT EXECUTION SIMULATION	✓	
SOCIAL ENGINEERING SIMULATION	✓	

The “Internet Banking Protection Test - 2026” certificate is awarded once the conditions are met.

The certificate confirms full compliance with AVLab's guidelines for the implementation of a virtual environment or a dedicated online banking protection module. The certification process involves a series of simulated attack scenarios that reflect the real-world techniques used by cybercriminals. The tests evaluate the effectiveness of protection against system clipboard hijacking, keyboard logging, malicious screen capture, data exfiltration, and attempts to remotely access the user's desktop.

In addition, the software's response to ransomware activity, manipulations in the file system and the creation of artifacts in the system (registry, Autostart, Task scheduler) are checked, aimed at simulating persistence maintenance after a system restart. The tests also include an assessment of resistance to click-to-compromise social engineering attacks.

Obtaining the certificate means that the security suite effectively protects against the takeover of online banking sessions and meets the high requirements set by AVLab in terms of financial transaction protection.