AV-TEST CYBERSECURITY FOUNDATION



Analysis of modules for protection of online banking and payments

amtso
The cybersecurity industry's testing standard community

MEMBER

Test of a banking mode in modern antivirus solutions

Dec. 2025

Table of contents

I Why does online payments protection matter?

II Methodology

III Test scenarios overview

IV Tested security suites – basic information

V Detailed results

VI Conclusions from the test

VII Certyficate

I

Why does online payments protection matter?

Dedicated online payment modules are designed to protect users' finances and personal data from cybercrime. They enhance the security of banking services and online transactions, offering reassurance that money and sensitive information are safe. Using solutions recommended by the AVLab Cybersecurity Foundation can significantly reduce the risk of a successful cyber attack.



Most modern antivirus software for Windows 11 and macOS comes with basic online banking and payment protection as standard. This usually includes anti-phishing, anti-malware, anti-keylogger and anti-screenlogger technologies, as well as blocking untrusted applications and scripts and detecting changes to DNS servers. However, some developers go the extra mile. They create a special module that protects the operating system during online payments and other important, confidential operations.

The main objective of our test was to evaluate the effectiveness of these dedicated modules in defending against online banking attacks, regardless of the initial protocol or vector employed by cyber attackers. To conduct our analysis, we developed malicious software and simulated an attack scenario in which the attacker aimed to steal information from a device protected by antivirus software while the dedicated online banking protection mode was active. If such a secure environment was unavailable, we used the full potential of the solution by applying hardened settings.

For this test, we chose to simulate a delivery attack via the Telegram messenger. This involved sending the victim a malicious file disguised as a trusted application from a ”familiar contact” (for example, a beta version of a new game supposedly sent by a friend). Similar attacks can be carried out using any messenger. This method of delivering malware bypasses the browser and some basic protective measures, giving attackers a slight advantage but also offering a clearer view of the interaction between malware and security technology.

II

Methodology

The methodology was developed in accordance with the Anti-Malware Testing Standards Organisation's guidelines*.
This ensures that all developers are treated equally and given sufficient time to review the provided logs and verify the results.

amtso
The cybersecurity industry's testing standard community

*https://www.amtso.org/amtso-ls1-tp168



All tests were conducted on a Windows 11 25H2 computer with either the default or hardened security settings activated. This standard configuration reflects the setup typically used by home and office users.

We created malicious files and downloaded them to the system via different methods: a common instant messaging service and a less popular protocol [1,2]. This differs from threats that go through browsers or email. With the banking mode or the browser running in the background, the task for the tested solutions was to detect and stop an attack at any stage: before it was launched, once it had started or once a connection had been established to a hacker controlled server.

[1] https://www.kaspersky.com/about/press-releases/kaspersky-uncovers-global-telegram-malicious-campaign-targeting-fintech-users

[2] https://ffnews.com/newsarticle/fintech/kaspersky-detected-a-new-remote-access-trojan-targeting-financial-institutions-through-skype-messenger/

We followed the scenario below

1. We are attempting to inject and activate malware in the system. The antivirus solution is running in the background, either with the default settings or with the settings described in the post-test report.

2. This activates the module that protects online payments. Depending on the solution being tested, protection can be activated in two ways: automatically when a user accesses a bank's website, or manually by the user.
If such an environment was unavailable, we used Opera and the online banking website.

3. Observe how the protection solution reacts and what information the attacker was able to obtain.
Repeat this step for all test scenarios.

4. Draw own conclusions and evaluate the product on its own merits.

Test scenarios overview

We used the .NET language to simulate the operation of malware that can perform specific tasks, such as keylogging, clipboard swapping, taking screenshots and transmitting data and logs to a server controlled by testers, to verify that the malware is functioning correctly. During this time, the antivirus software ran in the background with the default settings, unless otherwise specified in the report. We also activated special settings to protect browsers or bank modes used for online banking. We tested how well these features could stop hackers from stealing data in this mode and recorded the results for each one.



Clipboard Hijacking Simulation
Evaluate the effectiveness of security software in identifying attempts to intercept and transfer sensitive data copied to the system clipboard.



Clipboard Swapping Simulation
Test how well the protections respond when malicious actors replace clipboard content (e.g. payment or crypto addresses) and attempt to exfiltrate it.



Keylogger Simulation
Evaluate the effectiveness of input-capture techniques by simulating real keylogging behaviour and gathering user data.



Screen Capture Simulation
Check whether security products can detect repeated attempts to take screenshots of the desktop or bank mode and transmit them externally.

File Discovery and Exfiltration Simulation
This simulates an adversary listing a directory and attempting to copy any found files to an external location.

Remote Control Detection
Measure the visibility of the RustDesk remote control tool when it is running on endpoints, and how it interacts with the user's desktop.

File System Tampering (Ransomware-like Activity)
Simulate ransomware behaviour by encrypting files, creating ransom notes and altering timestamps.

Reboot Execution Simulation (Registry, Startup, Scheduled Tasks)
Create typical AutoStart artifacts in the system registry, the startup folder, and the Task Scheduler to test their detection as persistence mechanisms. Also, verify their presence and functionality after rebooting the system.

Click-to-Compromise Social Engineering Simulation
Create a phishing scenario in which a fake system prompt tricks the user into executing code, thus testing social engineering defenses rather than exploiting real vulnerabilities.

All scenarios are harmless simulations that are run in a controlled environment to produce artifacts that are typical of malicious techniques. Additionally, some attacks may not be detected as typical malware by the manufacturers of the tested solutions. This does not mean that attackers cannot exploit legitimate tools to achieve malicious goals on users' computers.

Scenario and short description	Expected artefacts	User Impact	What user would see?	Mitre Phase	Transfer Data to External Server	Mitre ID
Clipboard Hijaking Simulation	Saved clipboard logs on the FTP server	High	No visible symptoms (background process).	Collection	Yes	**T1115** Clipboard Data
Clipboard Swapping Simulation	Log with modified clipboard as evidence	Medium	Users might notice that the copied address is different when pasting.	Collection, Credential Access	Yes	**T1115** Clipboard Data
Keystroke Capture Simulation	Keystrokes recorded in the log	High	No visible symptoms (background activity).	Collection, Input Capture	Yes	**T1056.001** Input Capture: Keylogging
Screen Capture Simulation	Screenshots taken	Medium	No visible symptoms (screenshots taken silently in the background).	Collection, Screen Capture	Yes	**T1113** Screen Capture
File Discovery & Exfiltration Simulation	Log with actions on files	Medium	Potential impact (loss of data) only visible after the fact; no on-screen indication during the activity.	Discovery, Exfiltration	Yes	**T1083** File and Directory Discovery **T1048** Exfiltration Over Alternative Protocol
Remote Access & User Activity Visibility	Available user desktop preview	Low	Users may notice an active remote session or someone controlling the desktop.	Command & Control	n/a	**T1219** Remote Access Software
File System Tampering & Ransomware-like Activity	Renamed files, encrypted files	High	Visible changes to files and directories may look like ransomware activity.	Impact	n/a	**T1486** Data Encrypted for Impact
Persistence Artefact Simulation (Registry, Startup, Scheduled Tasks)	Added actions to AutoStart (HKCU\Run, Task Schedule, Startup folder, and log with completed tasks)	Medium	No visible symptoms at creation time; AutoStart artefacts added silently in the background.	Persistence	n/a	**T1547.001** Boot or Logon AutoStart Execution: Registry Run Keys/Startup Folder **T1053** Scheduled Task/Job
Click-to-Compromise: Social Engineering Simulation	Test files, HKCU key, outbound beacon, process entry and alerts.	High	A fake system or installer window with a prompt to click and install.	Initial Access, Execution	Yes	**T1204** User Execution

Basic information on tested security suites

The test began on 3 November 2025 and ended on 23 December 2025. Throughout this period, we used the latest software versions.
Not all packages had a special banking mode; however, those that did not were able to access their full potential through the use of hardened settings, which provided a clearer picture of the capabilities of a given solution.



Sophos Home was excluded from testing because it was found that the software does not have any additional mechanisms or hardened settings that could be of practical use in the tested scenarios.

Manufacturer name	Special module
AVAST Premium	Bank Mode
BITEDEFENDER Total Security	Safe Pay
COMODO Internet Security Pro	Secure Shopping
ESET Home Security Premium	Safe Banking & Browsing
F-SECURE Total	Bank Mode
G DATA Internet Security	-
KASPERSKY Plus	Safe Money
MICROSOFT Defender	-
MKS_VIR Internet Security	Safe Browser
NORTON 360	-
QUICK HEAL Total Security	Safe Banking
TREND MICRO Maximum Security	Pay Guard

In addition, the tests were conducted both on default settings, which reflect the most common configuration and typical end-user behavior, and on hardened settings, which present the full protection potential of a given solution after conscious security configuration.

The tables with the results use a clear assessment of the effectiveness of the attack scenario, regardless of the classification of the sample itself. A scenario marked as “attack successful (X)” means that the simulated attack achieved its technical goal, e.g., data interception, banking session manipulation, remote access, or persistence, even if the sample used was not classified as malicious by the product in its default configuration.

On the other hand, the designation “attack blocked (V)” indicates that the protective mechanisms effectively prevented the attack from achieving its goal, regardless of whether the block occurred at the prevention, behavioral detection, memory protection, or environment isolation stage.



Settings of the tested solutions

No additional settings are required for the following package

In the case of F-Secure, mks_vir and Quick Heal, the lack of hardened configuration in selected test scenarios was due to the fact that the product effectively blocked the simulated attack with its default settings or did not offer additional modules or configuration mechanisms whose activation could significantly increase resistance to a given type of simulated threat.

Hardened settings applied

Avast

To achieve better protection results, it was necessary to enable: “Protection -> Firewall -> Ask”, “Protection -> Core Shields -> Enable Hardened Mode”.

eset

We considered the following settings: “Protection -> All as Aggressive,” “Advanced heuristic/DNA signatures enabled,” “Network access protection -> Ask for profile”, “HIPS -> Notify when changes occur in Startup application”, “Eset Folder Guard”. However, only the interactive mode firewall allowed us to block the sending of stolen data from the computer to the server controlled by the tester.

norton

Firewall from “Smart Mode” to “Ask” or “Block” – it prevents applications without a digital signature and with very low popularity from connecting to hosts that may be controlled by hackers.

Bitdefender

For additional control over network traffic, we used: “Firewall -> Settings -> Alert mode”. Lack of additional significant features that could increase the flexibility of protecting the threats used.

G DATA

To get the maximum potential of the software, we used manual rules for the firewall: "Firewall – Disable Autopilot".

Windows Defender

Windows 11 25H2 was reinstalled to activate Smart App Control (On), but this did not apply to attacks that did not originate from a browser, although they retained ZoneID for files downloaded from instant messengers. Additionally, we used a Windows firewall to obtain maximum protection settings for specific scenarios: “Windows Defender Firewall -> Advanced Security -> Outbound Rules -> Add New,” as well as protected folders for better protection against ransomware: “Windows Security -> Protected Folders -> Add Folder.”

COMODO

To block malicious actions in one scenario, we used HIPS on default settings with a “Settings -> Configurations -> Comodo Proactive Security policy”.

kaspersky

We applied the following settings: “Security level -> Extreme”, “Safe Money -> On Screen Keyboard”, “Security settings -> Firewall settings -> Application network rules -> Deny” and “Security settings -> Intrusion Prevention -> Trust group for applications not included in other groups -> Untrusted”. The last option (Intrusion Prevention) in particular is the most intelligent, as it enables the product's settings to be adjusted automatically, not just the firewall rules. Users should also experiment with the “High Restricted” setting, where the application can be launched but will be controlled by the behaviour detection engine and will not be able to perform any network activities.

TREND MICRO

We used hardened protection for better results: “Protection Level -> Hypersensitive”, “Folder Shield -> (Add Desktop)” as protected folders.

Results

The table contains information about the settings at which a given attack scenario was blocked.

- Test passed – default settings
- Test passed – hardened settings
- Test not passed

*	Clipboard Hijacking	Clipboard Swapping	Keylogger Simulation	Screen Capture	File Discovery and Exfiltration	Remote Access and User Activity Visibility	Ransomware -like Activity	Persistence Artifact Simulation	Social Engineering Simulation
AVAST Premium	⊕	⊕	✓	✓	⊕	✓	⊕	✓	✓
BITDEFENDER Total Security	⊕	✗	✓	✓	⊕	⊕	✓	✓	⊕
COMODO Internet Security Pro	✓	✓	✓	✓	⊕	✓	✓	✓	✓
ESET Home Security Premium	⊕	✗	✓	⊕	⊕	⊕	⊕	⊕	⊕
F-SECURE Total	✓	✓	✓	✓	✓	✓	✓	✓	✓
G DATA Internet Security	✓	✗	✓	✓	✓	⊕	✓	✓	⊕
KASPERSKY Plus	⊕	⊕	⊕	✓	⊕	⊕	✓	✓	⊕
MICROSOFT Defender	⊕	✗	⊕	⊕	⊕	✓	✗	✗	⊕
MKS_VIR Internet Security	✓	✓	✓	✓	✓	✓	✓	✓	✓
NORTON 360	⊕	✓	⊕	✓	⊕	⊕	✓	✓	⊕
QUICK HEAL Total Security	✓	✗	✓	✓	✗	✓	✓	✓	✗
TREND MICRO Maximum Security	✗	✓	✗	✗	✗	✗	✓	✓	✗

*Test results reflect attack outcome, not malware classification.
Security suites were initially tested in their default configuration. If specific protections were disabled by default, they were enabled to evaluate the feature. When detection did not occur under default settings, alternative configurations were tried.

VI

Our conclusions from the test

The observations based on the test raise concerns even in the case of those solutions that received the maximum rating and passed certification.

01

There are situations in which, despite the correct delivery of a sample to the system with the ZoneID=3* attribute, antivirus software protection mechanisms are not always able to detect 0-day files that do not have a digital signature. This applies in particular to samples that are not very popular in a given manufacturer's telemetry ecosystem, such as files prepared specifically for testing purposes. In such cases, it is not the classification of the file itself that is decisive, but the actual user impact and whether the simulated attack allows the attacker to intercept data, manipulate the session, or gain unauthorized access.

02

Not every sample or technique used in testing needs to be classified as classic malware in the signature sense. In many scenarios, legitimate system tools, operating system functions, or mechanisms commonly available in the user environment are used. Therefore, the key evaluation criterion is not the classification of the sample itself, but the actual impact on the user (User Impact) and whether the simulated attack achieves the attacker's technical goal – such as intercepting credentials, manipulating an online banking session, gaining remote access, or exfiltrating sensitive information. For this reason, scenarios in which the product does not respond to something “non-malicious” are treated as a successful attack, regardless of the classification decision of the antivirus engine.

03

Additionally, with default settings, security solutions often fail to effectively filter network traffic generated by the aforementioned zero-day files with low or no reputation (EXE executable files). In practice, this means that outgoing communication from a PC may not be blocked if the sample has not been previously observed in the manufacturer's cloud or has only been seen on one or two test devices, making it impossible to clearly classify it as malicious at the early detection stage. This is an ideal situation for this type of testing.

*https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms537183(v=vs.85)

04 We would like to draw end users' attention to the need to use more manual or restrictive firewall modes or HIPS modules. Automatic settings are usually designed to minimize the number of alerts and interference with the user's daily work, which unfortunately often comes at the expense of security. In practice, this means that network traffic or other actions generated by executable files with zero or low reputation may be allowed. As a result, it becomes possible to intercept the contents of the system clipboard, take screenshots, collect keylogger activity data, and exfiltrate it to a server controlled by a potential attacker – in testing, firewalls often failed with default settings regardless of the manufacturer (usually, for a 0-day sample, outgoing traffic is allowed to limit the number of alerts and match the default settings of a given solution to a large group of users, which affects security). As part of the tests, the extracted data from the systems was sent to a server controlled by the Testers).

05 As tests confirm, special banking modes in many cases limit the effects of potential malware running in the background. Sometimes, malicious code is unable to function properly in an isolated environment. For example, anti-keylogger mechanisms encrypt the characters entered, rendering the intercepted keylogger useless to the attacker, while attempts to hide malware and survive a restart can be detected by specialized modules (e.g., HIPS in ESET) that monitor autostart mechanisms and notify the user of unauthorized changes.

06 The banking mode with default settings has been best developed in F-Secure, mks_vir, and Comodo solutions. These three products use several preventive methods, including an isolated environment (similar to a sandbox) designed for critical operations such as online payments. However, the differences do not end there, because F-Secure uses automatic blocking of all network traffic outside the browser used for banking, while mks_vir reveals processes running in the background and requires the user to make an informed decision to close them by displaying appropriate alerts. In these cases, these are strictly preventive mechanisms that effectively limit the attack surface and work well in practice.

07 In solutions without this mode, packet protection may be limited if the manufacturer has not implemented additional preventive mechanisms, such as blocking all network traffic on banking websites (except for browsers or trusted applications). As tests have shown, banking mode clearly outperforms standard mode, in which similar restrictions on applications with unknown reputations do not apply.

After testing the solutions indicated in the report, we informed their manufacturers about the results and shared our recommendations regarding the hardening of protection. We also recommended the development of additional mechanisms for detecting the malware used in this edition of the study.

VII

Certificate

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.



Avast

AVAST Premium + Bank Mode



Avast Bank Mode provides isolation during financial transactions. When activated, it creates a virtual desktop that shares only the absolutely necessary drivers for the keyboard, mouse, screen, network, and disks with Windows. This architecture minimizes the attack surface, as the banking environment runs completely separately from the main operating system.

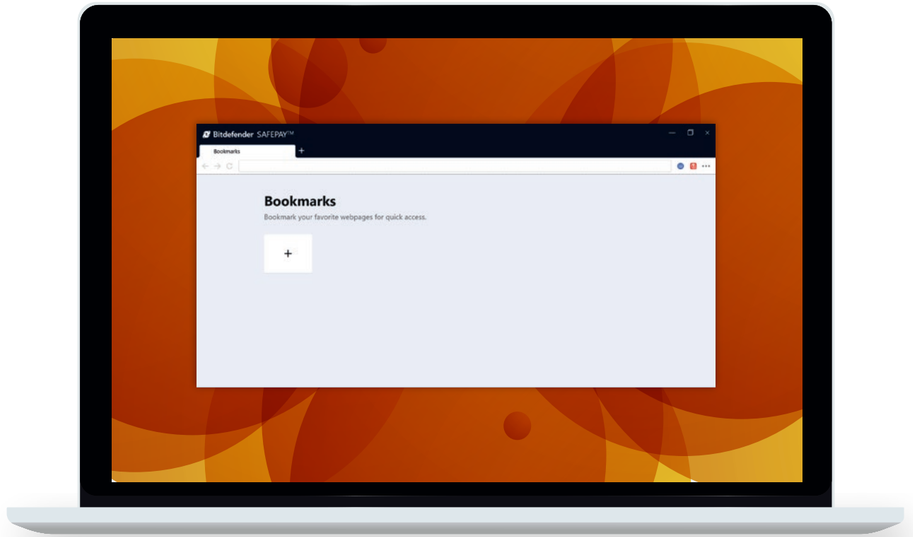
As part of its additional layers of protection, Avast uses CyberCapture technology, which analyzes unknown or potentially dangerous files in real time. Files with unverified reputations are blocked and sent to the Avast Threat Labs cloud for manual analysis, reducing the risk of infecting the system with new malware variants.

The isolated Bank Mode is complemented by the other modules of the Avast suite. In practice, this means that even if the operating system were partially compromised, the dedicated banking mode maintains an isolated environment that limits attacks on login credentials, session manipulation, or network traffic interception.

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	✓	

Bitdefender

BITDEFENDER Total Security + Safe Pay



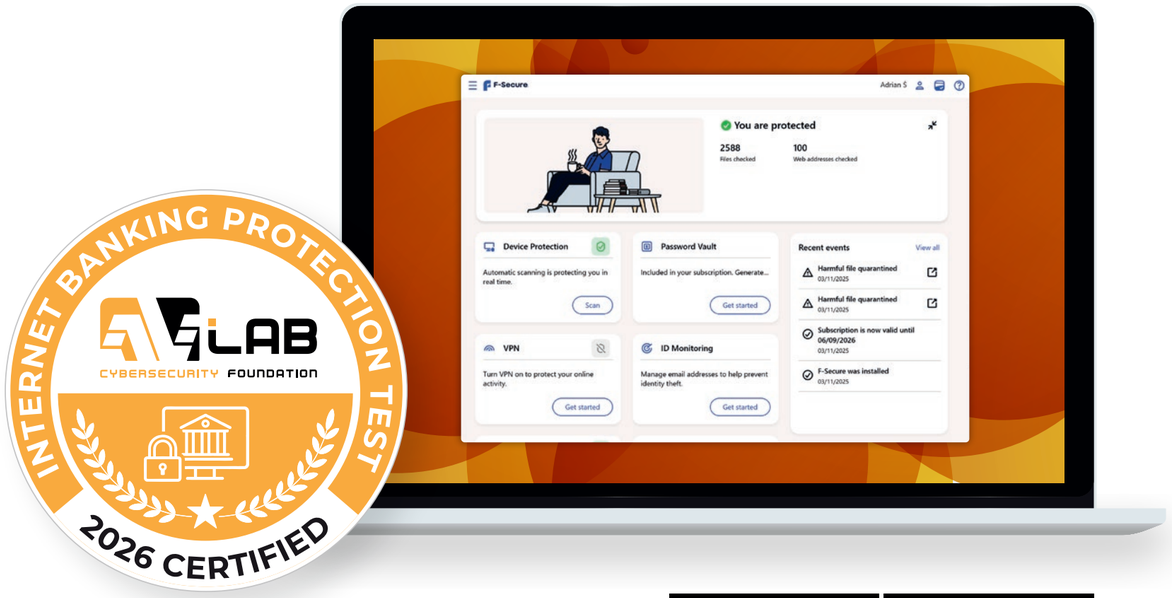
Bitdefender SafePay is a specialized, isolated browser designed to protect online banking, online payments, and sensitive data processing. When launched, SafePay creates a separate, virtual environment that provides real-time protection against fraud, phishing, and malware designed to capture keystrokes and take screenshots. Users can freely switch between the secure SafePay environment and the Windows desktop system without unnecessary resources overhead and without compromising user experience.

The SafePay mechanism theoretically prevents unknown processes or applications from interfering with the isolated browser environment. In practice, this environment is designed to act as a barrier against banking Trojans, keyloggers, and man-in-the-browser attacks.

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		✓

COMODO

COMODO Internet Security Pro + Secure Shopping

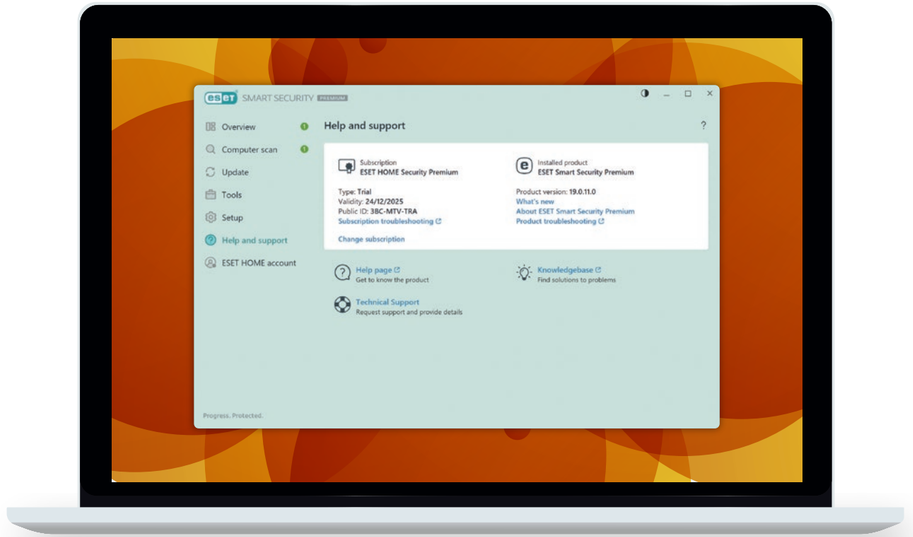


Secure Shopping technology provides multi-layered protection for online banking and shopping sessions by launching the browser in an isolated environment that effectively separates the protected session from the operating system.
This separation prevents other applications from injecting code into the browser process, intercepting input data, or interfering with its memory. The module protects the user against keyloggers, banking Trojans, and screenloggers by blocking keystroke logging and screen capture attempts during an active session.

Another important element of protection is HIPS, which monitors process behavior and controls attempts to modify key areas of the system, such as AutoStart mechanisms, process memory, and APIs. The preventive layer is complemented by Comodo containerization and the VirusScope mechanism, which analyzes application behavior in real time. This makes it possible to detect and neutralize unknown threats based on their activity, rather than just signatures, which significantly increases the effectiveness of financial session protection.

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	✓	

ESET Home Security Premium + Safe Banking & Browsing



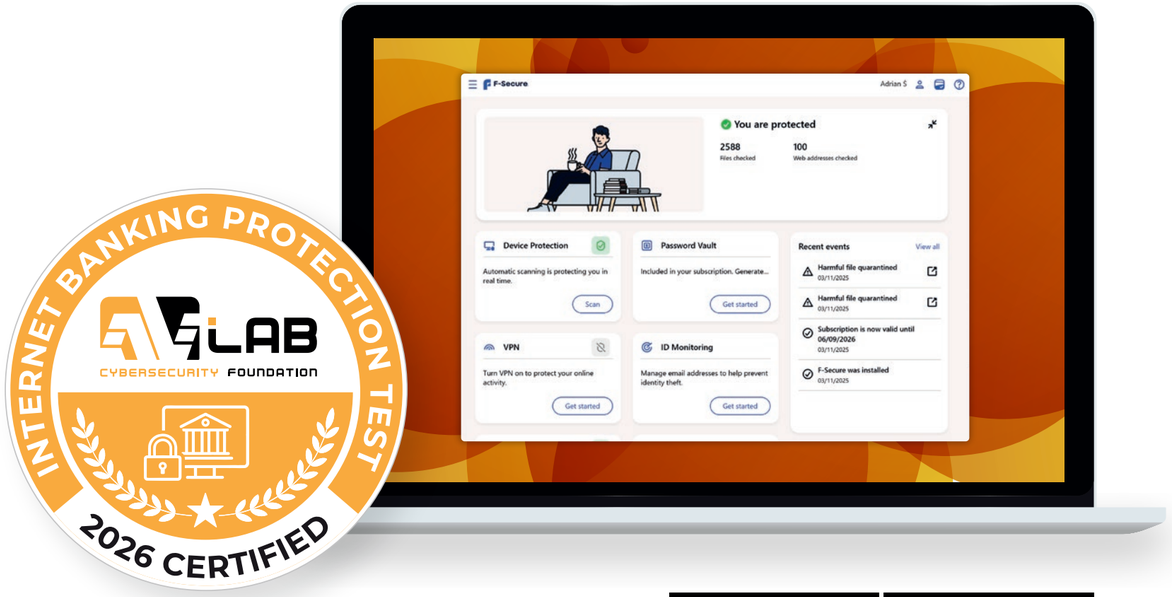
ESET is provided with a Safe Banking & Browsing module, which adds an increased level of protection when performing financial transactions and logging into services containing sensitive data. The mechanism launches the browser in “secure” mode, isolating the browsing process from the rest of the system and preventing interference from potentially harmful applications. Additional protection against keyloggers, screen scrapers, and browser process memory manipulation is also used.

This special module works with other layers of the package, including an advanced detection engine based on behavioral analysis, exploit blocking, and network protection. TLS/SSL traffic is also protected, which allows for the detection of fake certificates and prevents redirection to fake bank websites. As a result, ESET creates an environment that corresponds to the concept of a secure banking session: isolated, constantly monitored, and resistant to data interception techniques, while fitting into a multi-layered model of protection against network threats and targeted attacks.

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		✓

F-Secure

F-SECURE Total + Banking Protection



Secure Banking Features:

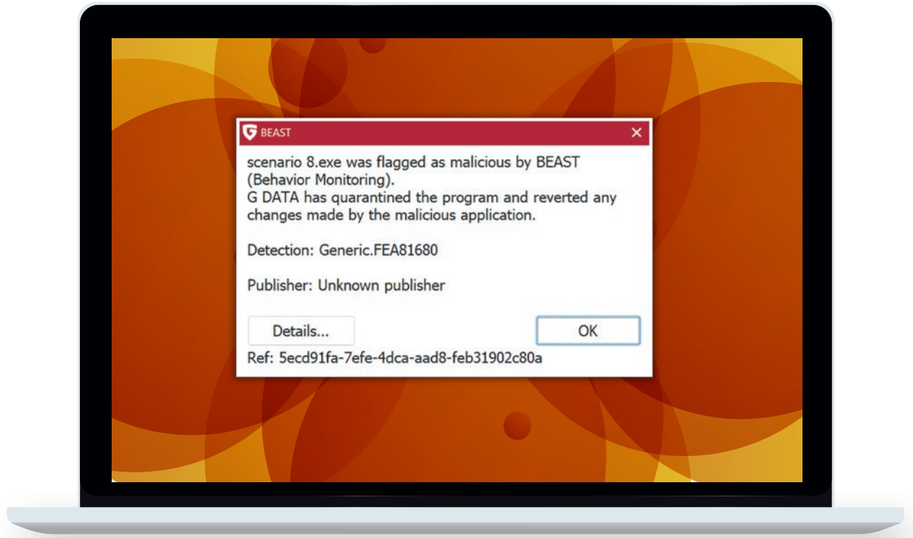
F-Secure uses a multi-layered protection system that combines real-time behavioral monitoring, cloud-based reputation analysis, and dedicated security features for online transactions. During active Banking Protection mode, the software automatically applies additional safety measures when the user visits a banking website or performs an online payment. All untrusted or unknown applications including command-line tools and scripting utilities are disconnected from the Internet to prevent unauthorized access or data exfiltration.
The clipboard is also cleared after each banking session to eliminate any residual sensitive information.

When a file is launched for the first time, F-Secure verifies its safety via the Security Cloud file reputation service. If its reputation cannot be confirmed, DeepGuard begins to monitor the process behavior in real time and automatically blocks suspicious or malicious activity typical of zero-day attacks.

Furthermore, Remote Access Blocker prevents remote-control fraud attempts, such as scams where attackers impersonate “technical support” agents and request victims to grant remote access to their devices during banking sessions. Additionally, the Shopping Protection feature enhances security during online purchases by showing notifications for trusted and suspicious e-commerce websites, helping users avoid phishing stores and fraudulent domains.

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	✓	

G DATA Internet Security



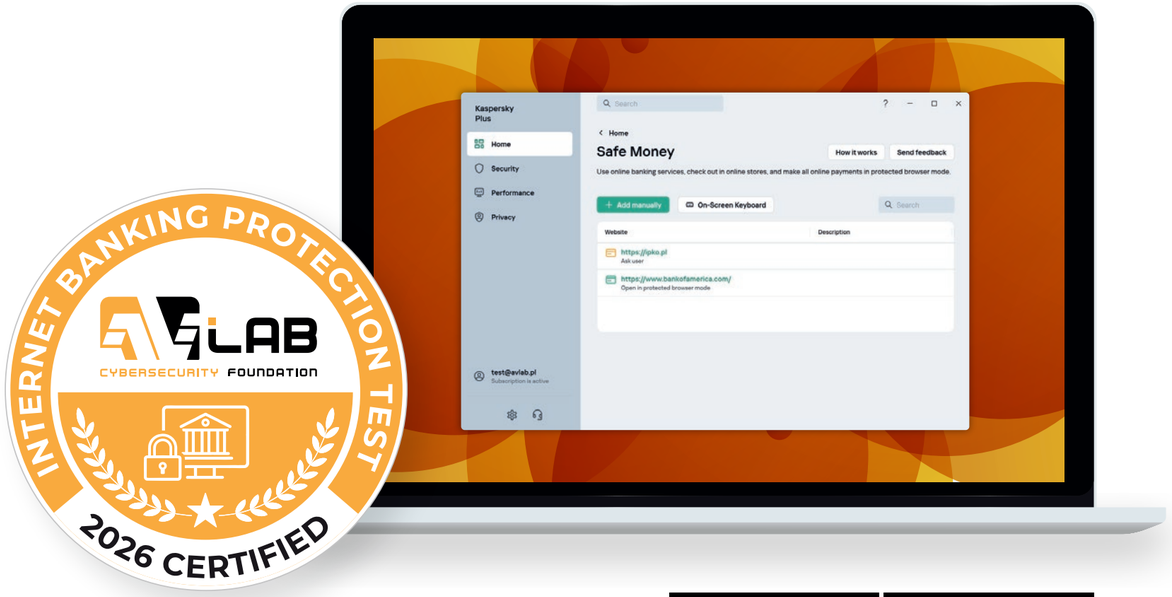
G DATA offers advanced protection when banking and online shopping. A key element in this regard is the G DATA BankGuard module, which protects the browser against manipulation by banking Trojans, both known and new, not yet known in the signature databases. BankGuard works by checking the authenticity of the web libraries used by the browser to prevent the browsing process from being infected or tampered with. In addition, the Web Protection module blocks malicious websites and protects login and financial information by monitoring network traffic and identifying phishing.

G DATA Internet Security can be recommended as part of a multi-layered online banking session protection package, although it is worth noting that it is not a special isolated “secure browser” dedicated only to financial transactions, but rather an advanced module within the overall security package.

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		✓

kaspersky

Kaspersky Plus + Safe Money

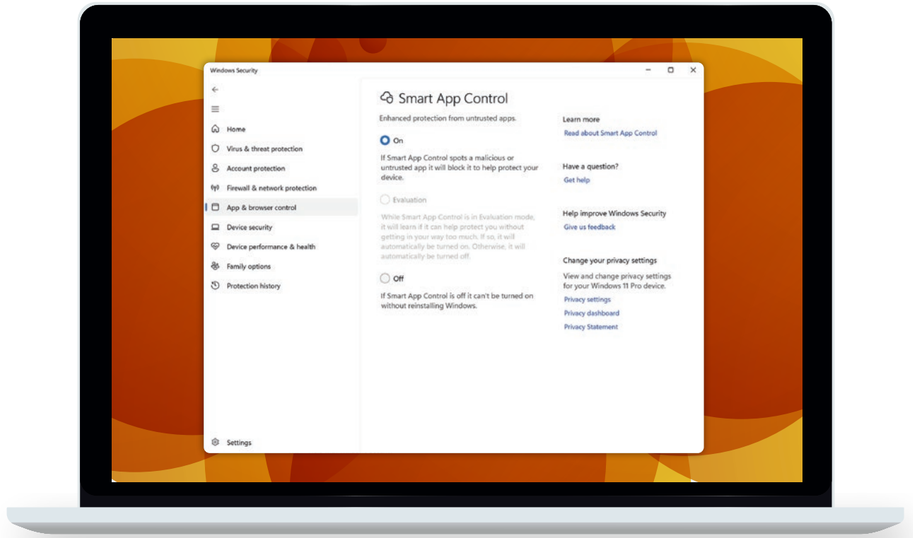


Kaspersky with Safe Money offers comprehensive protection for online banking sessions and Internet payments by launching the browser in a special, isolated container. This makes it difficult to inject malicious code, manipulate browser memory, or load unauthorized add-ons. HIPS mechanisms block attempts by malicious software (e.g., rootkits, malicious modules) to interfere with banking operations. A virtual keyboard protects against keyloggers, minimizing the risk of passwords and payment card details being intercepted. Safe Money also checks the authenticity of visited websites by verifying URLs and SSL/TLS certificates to prevent phishing or MITM attacks.

A key element is the Kaspersky Security Network, a reputation-based security cloud that analyzes the behavior of files, modules, and connections in real time. Thanks to this, Safe Money can immediately block suspicious processes, libraries loaded into the browser's memory, and servers with a bad reputation. KSN also detects anomalies in HTTPS traffic and known C&C servers used by banking Trojans. Safe Money provides layered security because it protects against traditional malware, banking Trojans, phishing, and advanced attack techniques such as MITB and MITM.

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		✓

MICROSOFT Defender



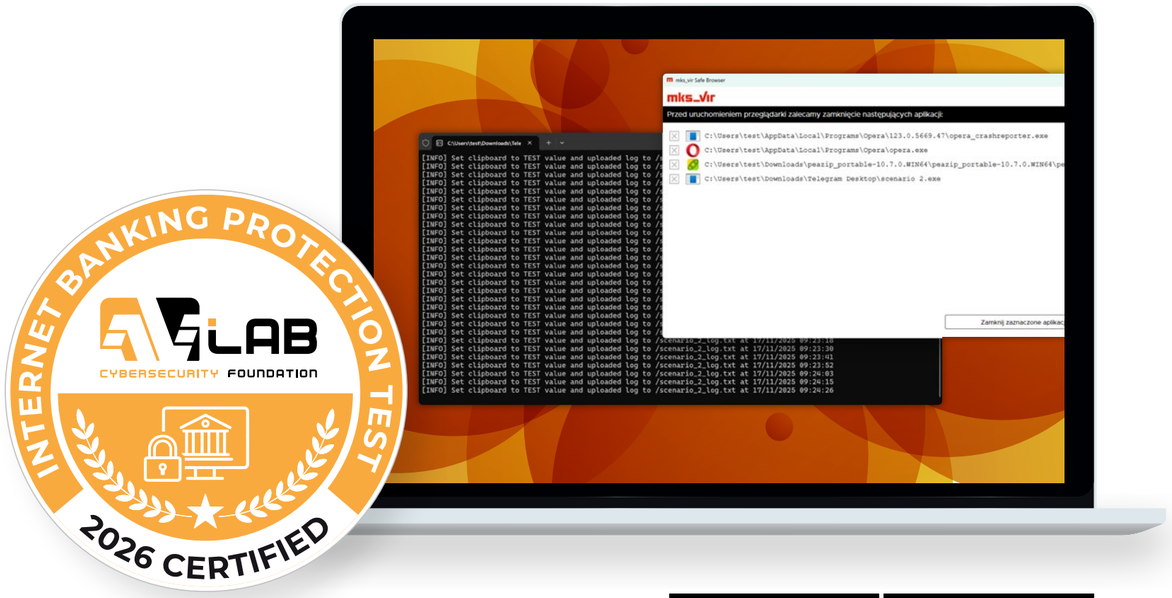
Microsoft Defender does not offer a dedicated banking mode or an isolated browser for financial transactions, but it does protect online banking sessions through a set of system-wide security mechanisms. In tests, Smart App Control was activated, which operates in preventive mode and blocks applications with unknown reputations or those that do not meet Microsoft's trust criteria from running before they can perform any actions on the system. However, this protection does not apply if malware has entered the system through a route other than the browser, which is the biggest drawback of this technology and also its weak point.

The overall protection of the package is based on a combination of application control, cloud reputation, and behavioral mechanisms that limit the ability to run tools used in attacks. This is complemented by Network Protection and SmartScreen features that block access to phishing sites and malicious network resources. However, it should be emphasized that this protection does not provide full isolation or systemically block screen capture, clipboard, or input data in a manner comparable to dedicated banking modes. The effectiveness of Microsoft Defender in this regard depends mainly on preventively blocking the launch of a threat, rather than separating the financial transaction environment.

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		✓

mks_vir

MKS_VIR Internet Security + Safe Browser



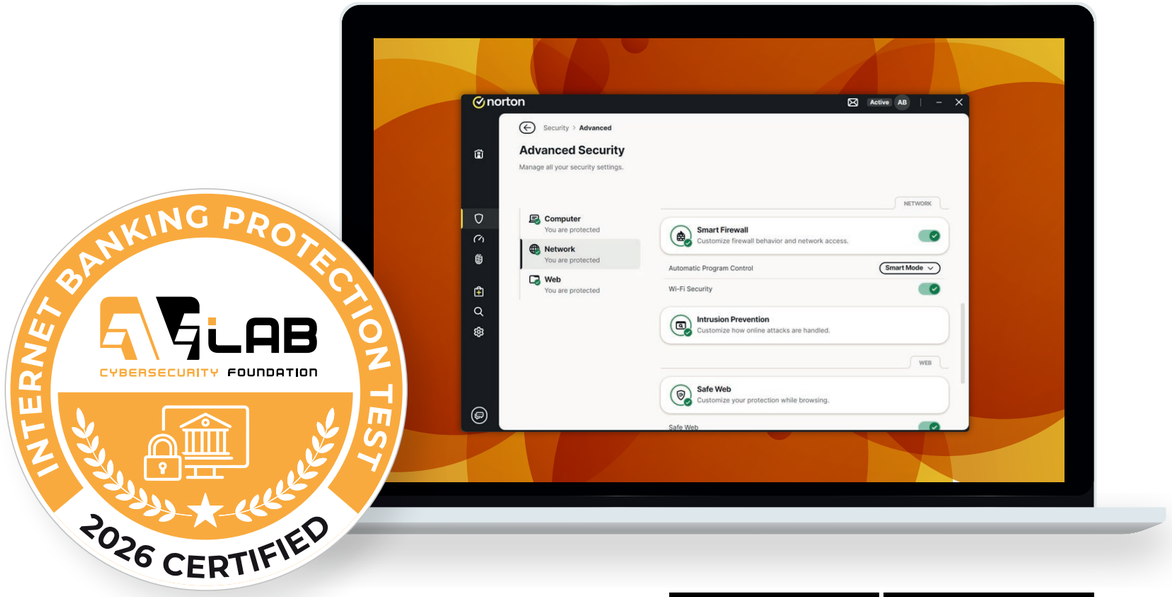
Thanks to the Safe Browser module, the entire MKS_VIR package achieves an extremely high level of security during banking and payment operations, significantly minimizing the risk of data interception. Safe Browser works in close integration with the other modules of the mks_vir package, which continuously 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	✓	

norton™

Norton 360



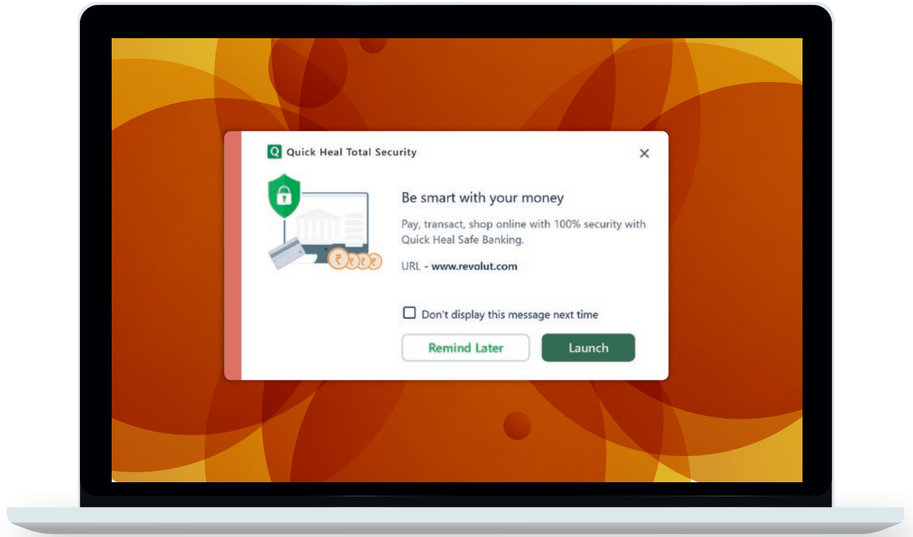
Although Norton 360 does not have a dedicated module for performing critical financial operations in Windows, the software provides effective protection for online sessions through alternative mechanisms. The sandbox feature enables you to run potentially malicious files in an isolated environment, while the real-time scanner detects malicious scripts that exploit legitimate system tools such as CMD, PowerShell or WMI. A firewall with a reputation system and intrusion detection provides an additional layer of protection, blocking suspicious encrypted connections and network attacks. Norton Safe Web protects users from fake banking websites and phishing attempts, while the behavioral protection system detects keyloggers and attempts to intercept login credentials. Consequently, Norton 360 offers robust, multi-layered protection for online banking sessions.

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		✓

Quick Heal®

Security Simplified

QUICK HEAL + Safe Banking

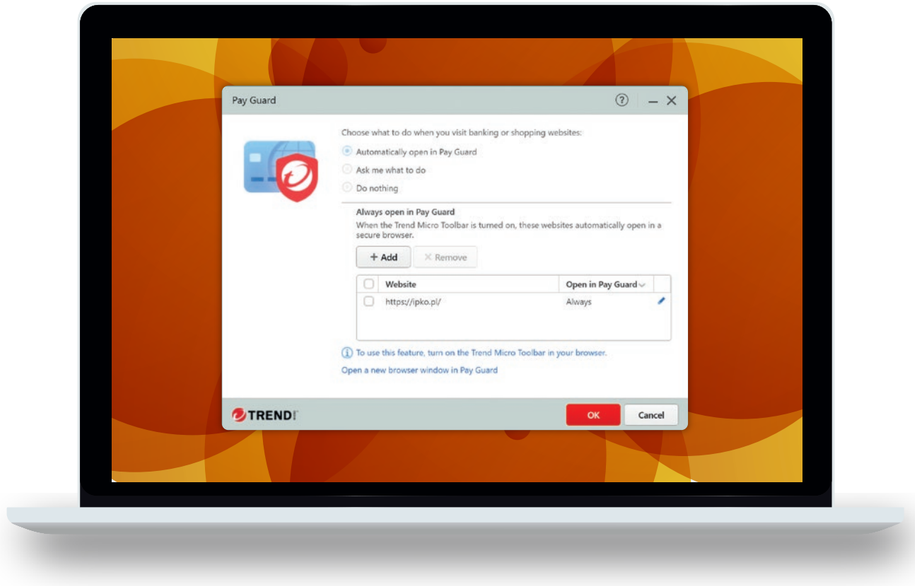


Quick Heal provides multiple layers of protection to secure your online banking sessions, combining isolation mechanisms and network traffic analysis. The Safe Banking module enables your browser to run in a special mode that effectively separates its processes from the rest of the operating system. This prevents keyloggers, screen loggers and other tools from intercepting session data from the operating system. As the virtual environment is isolated from the host, potentially malicious processes running on the system cannot access data entered in the protected browser.

Protective mechanisms also shield the device from manipulation of network settings, including DNS address spoofing, to prevent users from being redirected to fake banking or payment portals. Quick Heal also monitors the security of visited websites in real time, verifying them for phishing attempts, suspicious certificates, SSL/TLS manipulation and network layer abuse. Any unauthorized connections are blocked before data can be stolen.

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	✗	

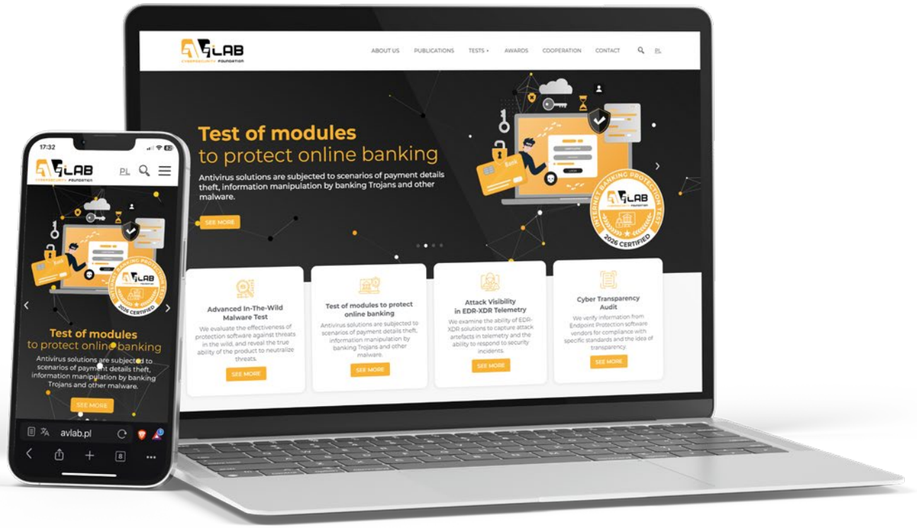
Trend Micro Maximum Security + Pay Guard



Trend Micro contains the Pay Guard module, which provides a kind of isolated environment for financial transactions and logging into banking services. Once activated, the browser operates in a separate layer, reducing the risk of attacks, code injection, or session modification. As part of its multi-layered protection, Pay Guard verifies visited URLs and SSL/TLS certificates, blocking fake bank websites and phishing sites before the user enters any login details.

The protection is complemented by Trend Micro's anti-exploit module, which monitors browser processes and prevents the exploitation of vulnerabilities to take control of the banking session. Thanks to its integration with the other components of the package, Pay Guard (theoretically) maintains a high level of security even in the event of zero-day threats or unknown types of malwares.

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	✗	



To learn more about the collaboration, please visit the webpage, where you can also read the results of recent editions.

CHECK OUR WEBSITE

We also conduct tests of other types:

Attack Visibility in EDR-XDR Telemetry

We examine the ability of EDR-XDR solutions to capture attack artefacts in telemetry and the ability to respond to security incidents.

Advanced In-The-Wild Malware Test

We evaluate the effectiveness of protection software against threats in the wild, and reveal the true ability of the product to neutralize threats.

Cyber Transparency Audit

We verify information from Endpoint Protection software vendors for compliance with specific standards and the idea of transparency.

For more information, please visit our website: https://avlab.pl/en/internet-banking-protection-test



How do we test in details?

- **Preparation of Windows-based attack scenarios relevant to banking online environments.**
- **Validation of the test setup and execution of simulated attacks.**
- **Analysis of detection and attack visibility.**
- **Assessment of automated response actions, including sandbox-isolation, blocking, and remediation.**
- **Manual verification of incident handling and technical review of results.**

Why is it worth having the certificate?

- Join a group of vendors certified by an independent organization.
- Test your product safely in a controlled environment.
- Receive feedback and improve the effectiveness of your security solution.
- Demonstrate to potential customers that your solution meets reputable, independent security standards.
- Use the certificate for marketing purposes, such as displaying it on your website or promoting your company in industry publications.

INTERNET BANKING PROTECTION TEST
AV LAB CYBERSECURITY FOUNDATION
2026 CERTIFIED

AVLab
CYBERSECURITY FOUNDATION

The AVLab Cybersecurity Foundation is an independent organization dedicated to protecting privacy and security on the Internet.

We are part of the CTF (Cyber Transparency Forum) and provide independent assessments of cybersecurity vendors' systems. We are a member of AMTSO (Anti-Malware Testing Standards Organization), which works to improve the transparency, objectivity and quality of testing. Also, we are a member of MVI (Microsoft Virus Initiative) in this matter as well.

We build awareness of users in the field of digital protection.
We issue opinions, technical analyzes and tests of IT solutions in the field of cybersecurity.
Our strongest assets include thorough and detailed reviews, preparation of reports related to privacy and endpoint protection, and in particular, security tests that make us recognizable all over the world as one of the most trusted and popular testing laboratories.

To learn more about other opportunities for cooperation,
please refer to our full offer and contact us: kontakt@avlab.pl

amtso
The cybersecurity industry's testing standard community
MEMBER

www.avlab.pl