GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

General & Licensing

How safe will I be when using Gridinsoft Anti-Malware?

Understand what Gridinsoft Anti-Malware can reduce, what no security product can guarantee, and which habits complete a layered defense.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Jul 10, 2026	1 min

CONTENTS

In this guide

01 Keep protection effective

02 Reduce risks outside the scanner

03 Respond to warning signs

Gridinsoft Anti-Malware can reduce the risk from malicious and unwanted software, but no security product can guarantee that a computer will never be compromised. Protection depends on current detection data, enabled features, prompt action, and the way the computer and accounts are used.

01 Keep protection effective

- Keep the app and Threat List current.
- Leave the relevant real-time protection modules enabled.
- Use an appropriate scan when symptoms appear and review every proposed cleanup action.
- Quarantine uncertain files and report suspected false positives before restoring them.

02 Reduce risks outside the scanner

- Install Windows, browser, and application security updates.
- Download software from the publisher and verify unexpected installers.
- Use unique passwords and multi-factor authentication for important accounts.
- Keep offline or versioned backups and test that important files can be restored.
- Treat unexpected links, attachments, and remote-access requests as suspicious.

03 Respond to warning signs

If redirects, account alerts, disabled security tools, or unknown processes continue after a clean scan, do not assume the system is safe solely because no detection appeared. Preserve the scan result, disconnect from sensitive accounts when appropriate, and ask Support for a focused review.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com