C

Computer Virus: How It Spreads, Signs, Removal, and Prevention

Learn what makes malware a computer virus, how file, macro, and boot infections spread, how viruses differ from worms and Trojans, and how to recover.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 How a computer virus spreads
02 Common virus categories
03 Virus vs. worm vs. Trojan
04 How do I know if my computer has a virus?
05 Immediate response
06 Removal challenges
07 Safe recovery
08 Prevention
09 Do modern computers still get viruses?

A **computer virus** is malware that replicates by inserting its code into another file, program, document, or system area. When infected content runs, the virus can execute its payload and seek new hosts.

People often use “virus” for all malware, but ransomware, spyware, Trojans, and worms have distinct behaviors. Correct terminology helps responders understand propagation and recovery.

01 How a computer virus spreads

A virus needs a host and an opportunity for infected content to run or be shared. It may modify executable files, document templates, boot structures, or scripts. Distribution can occur through removable drives, network shares, email attachments, unofficial software, and shared repositories.

02 Common virus categories

- **File infector:** inserts code into executable files.
- **Macro virus:** uses an application’s macro language and infected documents or templates.
- **Boot-sector virus:** targets startup structures or boot code.
- **Multipartite virus:** infects more than one type of host.
- **Polymorphic virus:** changes parts of its representation to complicate detection.

03 Virus vs. worm vs. Trojan

A worm spreads automatically between systems without attaching itself to a host file. A Trojan relies on disguise or another delivery method and does not self-replicate by definition. A virus replicates through infected host content. A campaign can deliver one category using another.

04 How do I know if my computer has a virus?

Possible indicators include repeated detections across unrelated files, unexpected file-size or hash changes, corrupted applications, disabled security tools, removable-drive artifacts, and infection returning after partial cleanup. Performance problems alone do not prove a virus.

05 Immediate response

1. Disconnect affected devices from networks and shared storage.
2. Stop using removable media and shared executable repositories.
3. Preserve representative samples, detections, hashes, and logs.
4. Scan connected systems and media with updated security tools.
5. Protect sensitive accounts from a known-clean device.

06 Removal challenges

A file-infecting virus may modify many legitimate programs. A security tool can sometimes disinfect a known variant, but cleaning may damage files or leave an uncertain state. Reinstall applications from original signed sources. Rebuild the operating system when core files or security components are affected.

07 Safe recovery

Restore documents and data from verified backups, but avoid restoring unknown executables or scripts. Patch the system, rotate exposed credentials, and monitor for renewed detections before reconnecting to shared resources. Investigate the original source so another device or repository does not reintroduce the infection.

08 Prevention

Use supported software, official downloads, application control, least privilege, updated endpoint protection, and safe macro settings. Restrict removable media and write access to software shares. Keep offline or immutable backups and test restoration.

09 Do modern computers still get viruses?

Yes, although many current attacks are classified as Trojans, ransomware, stealers, or loaders rather than classic viruses. File infectors such as Sality illustrate why the category still matters, especially in legacy or weakly controlled environments.

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