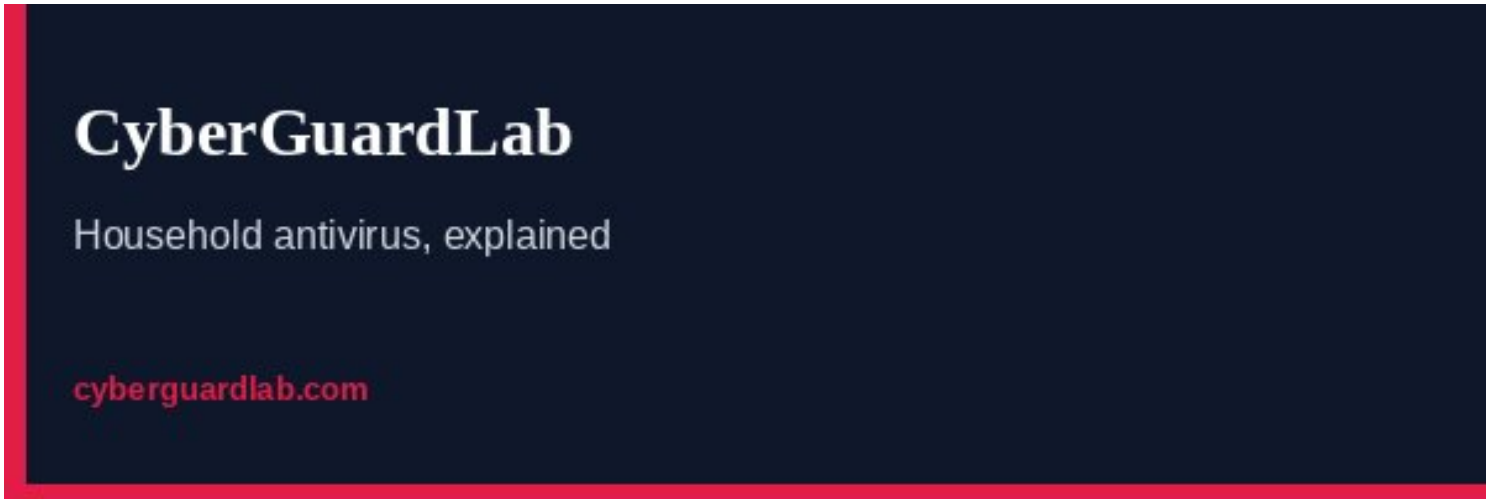

How to use Windows Sandbox to open a risky file

https://cyberguardlab.com/blog/windows-sandbox-risky-file

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.

Windows Sandbox is a temporary, disposable Windows environment (available on supported Pro/Enterprise/Education editions) where you can open a suspicious attachment or installer with less risk to your main system-closing Sandbox discards its state. Enable it via Windows Features, copy the file in, inspect, then close without keeping the sandbox. This how-to is about Sandbox for risky files-not BitLocker, not a keep-files reset, and not hijacker cleanup after you already ran malware on the host.

1. Requirements and limits

Sandbox needs a compatible Windows edition, virtualization enabled in firmware, and enough RAM/disk. It is not on typical Home SKUs. Sandbox reduces risk; it is not a guarantee against every escape technique. Prefer deleting obvious malware without opening it. Never enter banking passwords inside Sandbox while testing unknown software.

Forum posts sometimes say to turn off antivirus inside Sandbox for "accurate" malware tests. For home users inspecting a random attachment, leave protections on; your goal is safe triage, not malware research. If the file is clearly unwanted, delete it without opening.

2. Sandbox vs neighboring tools

Approach | Best for | Not for

Windows Sandbox | One-off look at untrusted files on Pro+ | Daily browsing as your only defense

SmartScreen / Defender | Blocking known-bad downloads on the host | Replacing judgment on every attachment

BitLocker | Disk theft protection | Isolating a live malware sample

Keep-files reset | Repairing a already-infected OS | Routine file preview

3. Steps: enable Sandbox and open a risky file

* Confirm edition: Settings -> System -> About-look for Pro/Enterprise/Education. Home users should scan on the host with Defender or use a separate spare PC instead.
* Enable virtualization in BIOS/UEFI if Windows Features gray out Sandbox (OEM docs vary).
* Open Turn Windows features on or off, check Windows Sandbox, OK, reboot.
* Download or save the suspicious file to a normal folder on the host (do not run it yet). Prefer keeping the original in quarantine until inspected.
* Start Windows Sandbox from the Start menu. Copy-paste or drag the file into the Sandbox window (clipboard/file share as your build allows).
* Inside Sandbox only, open the file with appropriate viewers. Watch for unexpected network installers or macros-close Sandbox immediately if behavior is hostile.
* Do not copy "cleaned" mystery executables back to the host as trusted. If you need the real document, obtain a re-sent

copy from the sender through a verified channel.
* Close Sandbox to wipe the environment. On the host, delete the risky file and run a Defender scan. A trusted primary suite such as Norton or Bitdefender can supplement-avoid stacking full suites. TotalAV, McAfee, and Avast are other on-site comparison options.

4. If you opened the file on the host by mistake

* Disconnect from networks if ransomware behavior appears; power off if encryption of files starts.
* Run Defender full scan; review Protection history.
* Change passwords from another device if credential theft is possible.
* Escalate to Reset this PC - Keep my files if the host remains unclean.
* Do not call phone numbers from fake virus screens-see fake BSOD support scam.

FAQ

Is Sandbox available on Windows 11 Home?

Generally no. Microsoft documents Sandbox for Pro/Enterprise/Education with virtualization support.

Does closing Sandbox always delete malware remnants on the host?

Sandbox state is discarded, but the original file on the host remains until you delete it. Never assume the host copy is safe to run.

Can I use Sandbox instead of antivirus?

No. Keep real-time protection on the host. Sandbox is an isolation tool for inspection.

Is this the same as a virtual machine I keep forever?

No. Sandbox is disposable by design. Persistent VMs need their own hardening and snapshots.

If you still want a paid suite

Avoiding how to use Windows Sandbox to open a risky file does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

* Microsoft Learn: Windows Sandbox
* Microsoft Learn: Windows Sandbox configuration
* FTC: Malware
* CISA: Understanding and protecting against malicious code

Also read

* How to turn on BitLocker on a Windows home PC
* How to reset Windows 11 while keeping your files
* How to turn on SmartScreen for apps and files
* How to spot a fake Windows blue screen support scam
* How to check a download before opening an EXE