

9 steps to clean a virus-infected Windows PC

CyberGuardLab is an independent comparison site. We may earn a commission on paid links; buying nothing is valid.

Recover files first, then clean or reset. Microsoft Defender Offline is the built-in deep scan. A reset is often cleaner than stacking paid suites. Buying nothing after a reset is valid.

1. Back up files - do not treat the copy as clean. Copy Documents, Desktop, Pictures. Safer: pull the drive or use a live USB. Scan the copy on a healthy PC.
2. Disconnect from the network.
3. Restart in Safe Mode (Shift+Restart).
4. Run Microsoft Defender Offline from Windows Security, Scan options.
5. Use one on-demand scanner, not three.
6. Uninstall leftover trials and junk so Defender can run.
7. Check the browser for a hijack.
8. Change passwords from a clean device. IdentityTheft.gov if a SSN may be exposed.
9. Reset Windows if the infection returns.

Sources: Microsoft Defender Offline (Support + Learn), Microsoft remove-malware help, IdentityTheft.gov. Reddit r/techsupport thread is community discussion only.

CyberGuardLab.com key points | August 21, 2026