

## Clean an Infected Computer

Stephanie Obodda - 2026-06-19 - Comments (0) - Antivirus and Malware

### Some Ways a Computer Gets Infected

- Responding to a phishing email
- Failing to keep your anti-malware definitions current
- Clicking on a seemingly innocuous web site for a free widget while a malicious script runs in the background
- Using an anonymous thumb drive you found in the airport and installing its keylogger software
- Opening an attachment from a long lost uncle you didn't know you had (and actually don't)
- Not disabling your web browser's function to automatically run scripts (check its security configuration and set to "high")

### Signs a Computer is Infected

- It begins to run slowly
- Task manager indicates 100% utilization
- Firewall is asking permission to allow unknown programs access to the Internet
- There are unknown processes and programs at start up
- Policy changes were made without your knowledge
- There are visible configuration changes
- Some programs no longer work
- You begin to get pop-ups

### Tools for Your Toolbox

- [Ad-Aware](#) (*Lavasoft - for personal home use only, Windows*)
- [Spybot Search & Destroy](#)
- [SpyWare Blaster](#) (*Windows*)
- [Rootkit Buster](#) (*Windows*)
- [RUBotted](#) (*automated scanning for Windows*)
- [Hijack This](#)
- [Trend Micro Anti-Ransomware Tool](#)
- [Belarc Advisor](#)
- [Microsoft Baseline Analyzer](#)
- [Malwarebytes](#) (*IT Service Desk recommendation - non-Brown owned computers only*)

- [Mac Malware Guide](#)
- Flash or CD-run antivirus tool

#### Steps to Disinfect

1. Remove the machine from the network
2. Turn off the system restore
3. Clean out the temporary files using *Disk Clean-up*
4. Run the following apps: *Ad-Aware*, *Spybot S&D*, *SpyWare Blaster* and *HijackThis*
5. Run your system's antivirus tool plus a non-resident antivirus tool
6. Reconnect to the network
7. Run *Belarc Advisor* and then run *MS-Baseline Analyzer*
8. Take actions as needed, including turn on system restore
9. Afterwards, change all passwords and monitor online banking, credit cards, etc.

#### Summary

The best defense is sometimes your best offense as well:

- If you use a firewall, keep it on
- Keep all your system tools up-to-date
- Consider using automatic updates
- Read everything that comes from ISG
- Use common sense!