

Forum:[Hack Forums](#)

Thread: [Identifying Signs of Malware and Virus Attacks on a Personal Compute](#)

R5N3T - December 10, 2025, 6:28 pm

What are the common signs that indicate a personal computer might be infected with malware, viruses, or other cyber threats?

Null State - January 25, 2026, 3:26 pm

If your PC's acting weird, slow, random pop-ups, strange apps, or weird browser redirects — that's a red flag.

R5N3T - January 26, 2026, 2:51 am

My computer had an issue. Every time I copied a Bitcoin address and pasted it, the address changed to a different one. Luckily, I always double-checked before sending. I've now reinstalled my computer. Friends, please be careful and always verify the Bitcoin address before sending.

WinGV - January 26, 2026, 3:23 am

(Jan 26, 2026 03:51 AM)tuyulperang Wrote: [\[CITE\]](#) My computer had an issue. Every time I copied a Bitcoin address and pasted it, the address changed to a different one. Luckily, I always double-checked before sending. I've now reinstalled my computer. Friends, please be careful and always verify the Bitcoin address before sending.

You can check the list of process trying to identify if there's anything weird/unknown. But the process could be injected in another one if the attackers know their stuff. For persistence you should check your registry Run entries for anything unusual. Also WMI events, or scheduled tasks. But a rootkit could be even at deeper level (though I doubt it would be the case for a simple clipboard hijacker). The best thing to do when you know your computer has been compromised would be to go with a fresh install. Even though it might be a bit overkill for most of the malwares, you don't wanna take risks, especially if you deal with cryptos.

Forget my curiosity but, when your wallet address was replaced, how did you notice it ? Were all the characters different or were there first/last few similar ? Did you check the whole address or just the first/last few ?

R5N3T - January 26, 2026, 6:37 am

I didn't want to take any risks, so I went straight ahead and did a fresh reinstall.

C00dZero - January 27, 2026, 4:24 am

If the clipboard isn't working properly, you probably have a keylogger or wallet spoofing.

R5N3T - January 28, 2026, 9:32 am

(Jan 27, 2026 05:24 AM)C00dZero Wrote: [\[CITE\]](#) If the clipboard isn't working properly, you probably have a keylogger or wallet spoofing.
I thought so too.

habeotron - March 24, 2026, 6:39 pm

You can check the list of process trying to identify if there's anything weird/unknown.

DeathPenalty666 - March 24, 2026, 8:38 pm

for rat/botnet/loader and most remote control tool just looking for tcp/udp traffic help a lot. cmd

netstat -n then arrow up and enter do this for a while and you see most connection, sync sent is dead rat looking for remote server, look for all ip to see what it link to.

Rat and most remote tool are very easy to detect, they all link to a ip. Advanced tool may use tor for data exfill or control and may be harder to detect. Soon as you have a suspicious ip you can get many detail and mess with them a lot xD. One dude tried to rat a flash crypto tool and i had 3 new ip in my list, he got his 3 vps under heavy ddos hahaha.

Alway check startup app, from task manager or even other folder for this. Make sure all ink used if there is are legit. And best one, NEXT TIME you format setup esxi as main os. If at anytime you have doubt you can load a snapshot from a previous time when it was safe, run many vm at same time, manage every connection and security and if you need a fresh machine you have one in 2min and can run up to 4 os at same time :)

whitehatlord - April 3, 2026, 8:25 pm

The computer running slowly, or having suspicious things happening on accounts is a very big sign.

R5N3T - April 3, 2026, 8:43 pm

(Apr 3, 2026 08:25 PM)whitehatlord Wrote: [\[CITE\]](#) The computer running slowly, or having suspicious things happening on accounts is a very big sign.

The problem has been solved, but thanks anyway