Just running an Anti-Virus program is no longer enough. You need to periodically scan with bootable media to be sure that you have not been infected.
Malware can evade antivirus

No matter how good the anti-virus product you have installed is, there is always a piece of malicious code that can subvert it.

- NO product is perfect
- Malware can subvert antivirus
- Zero days are more common
- Signatures are not always accurate
ONCE YOU ARE INFECTED....

ANTIVIRUS SOFTWARE IS ALSO COMPROMISED AND MAY BE SUBVERTED
You cannot be certain

It is best to use different products when choosing a bootable antivirus product. This way, the signature sets will be different to those you are already using.

This increases the chance of detection significantly.

Scan often

Scan from trusted media

Use different products

Update regularly
**Make sure you reboot the system**

**Rebooting IS essential.**

If the hard drive is compromised, you cannot trust the system to run as you would expect. This includes anti-virus software. Malware can infect and subvert any process – including the anti-virus software designed to stop it.

- **USB**
- **CD/DVD**
- **NOT THE Hard drive**

As long as it boots separately.
Think on This...

Of the last 120 systems we tested that have been running for more than a month using up to date anti-virus signatures...

ONLY 2 did not have at least 1 instance of Malware and some systems had up to 80 separate infections...

Are you different!

When did you test last?
MALWARE CAN HOOK INTO SYSTEM FILES
IT CAN RUN UNDETECTED EVEN WITH UP TO DATE ANTIVIRUS SOFTWARE
Think just how many new instances of malicious code are being written each and every day.

Think that these have to be detected and analyzed BEFORE a signature can be written to detect and stop them.

If you are infected before the signature is detected, you may remain infected even when the signature is released.
BE SECURE

- Use AntiVirus Software
- Update and install Signatures
- Scan the system offline
- Use different Products
Operate system based AntiVirus Software

Use different products

Defense in depth

Update the disk and signatures just before you scan

Change products from time to time
USING A RANGE OF DIFFERENT ANTI-VIRUS BOOT DISKS ALSO INCREASES THE RANGE OF MALWARE YOU CAN DETECT.

NO PRODUCT CAN FIND EVERYTHING
Memory resident Malware often gets past even the best anti-virus systems. Scanning using an up to date bootable CD or USB stick can find malware that will reside in memory and bypass anti-virus programs.

Scanning periodically, is a way to ensure that you not only remain protected from casual threats, but find those that have managed to bypass your defences.
The malware front is constantly changing and is becoming more sophisticated.

Just because you have not seen an infection reported does not mean you are safe.

New malware is becoming common and it being released faster than signatures are written to detect it.

It is not when you are infected, but are you already infected?
Scanning takes time and should be planned

DO NOT interrupt the scan. You need to leave the computer scanning.

A boot scan can take a long time on large drives or older systems, and if there is malware, it can be even slower...

Once the scan is complete you will have a far better chance of no longer having any malicious code on your system.

Once the scan is complete, you can restart your computer and continue work.
MAKE IT A HABIT

SCAN OFFLINE FROM BOOT MEDIA AT LEAST ONCE A MONTH
Scan on a regular basis

In scanning your system on a regular basis, you maximize the chances that you will find and contain any malware on your system BEFORE it does too much damage.

More, it is NEVER too late.

The damage done by malware is ongoing. As soon as you remove it, the better your security will be.

The lower your losses will be.
There are options

With all products, there are many options and finding the right one for your organization is a matter of personal choice.

Many of these boot anti-malware products (such as Dr.Web) are freely made available for download and use.

Even Microsoft has released their own product.  
(https://connect.microsoft.com/systemsweeper)
WHAT EXCUSE DO YOU HAVE NOT TO SCAN YOUR SYSTEM FOR MALWARE TODAY!

Reboot on a trusted anti-malware disk NOW!