## Another Very Useful Free Tool from Microsoft:
The Standalone Windows Malicious Software Removal Tool

For sometime now, I had relied on the **Malwarebytes Free Malware Scanner** to test whether a computer is infected. But that product is no longer simply a standalone virus scanner. That AV product is now a free trial offer for the entire application. This requires it be removed after scanning if that is all you want. If the application is not uninstalled, Malwarebytes will become your default AV software, and you will be asked to pay that piper. In other words, the free Malwarebytes AV scanner is now so difficult to manage, most consumers won't bother to use it.

Enter the Microsoft Malicious Software Removal Tool. Microsoft has no need to attempt to monetize your desire to scan your Windows system for malware. **Microsoft includes the full AV software in Windows.** They already got your dime.


Now, since the tool comes from Microsoft, and not Uncle Bob's Download Emporium, we can trust that no additional crapware is also installed. No need to even offer your email address; the site doesn't ask for it. Simply click the link:
https://www.microsoft.com/en-us/download/confirmation.aspx?id=9905 to download the installer.
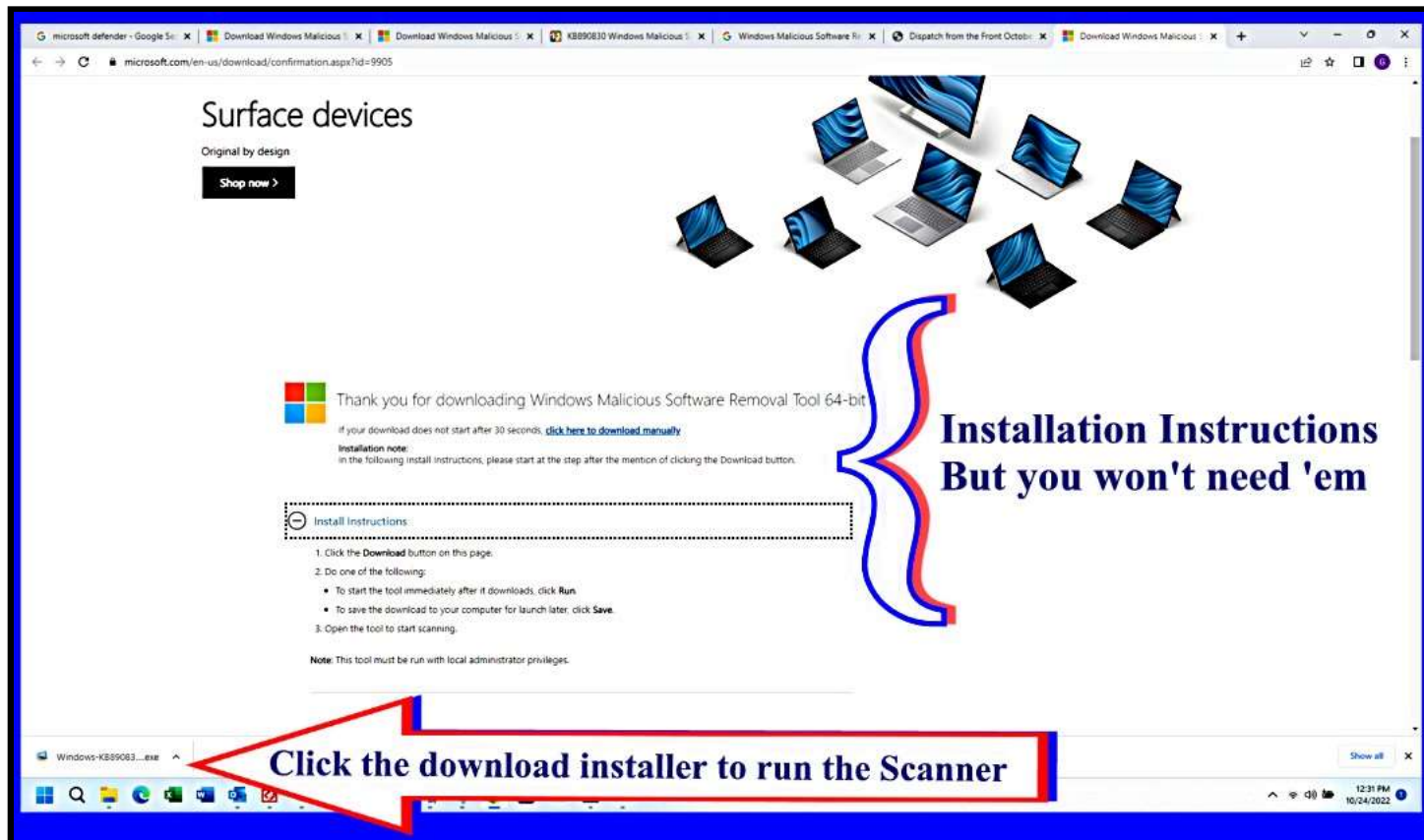
There is no extra hoop to jump through. Click the link to the page above and then click the installer. Of course, the usual User Account control will appear. Unfortunately, I can't screen dump that. Ironically, if you do chose to install and run the app, then look closely at the UA control. **The application is not a digital signed application and comes from an Unknown Source.** Kinda thing that could give one a bad reputation within the Microsoft ecosystem.

Once the installer runs, the app opens telling you what this is all about. The app is NOT a replacement for traditional anti-virus software that runs continually in the background. What makes this different is the app will quickly scan the system for malware; remove what it can remove; and report the results. Simply click Next.
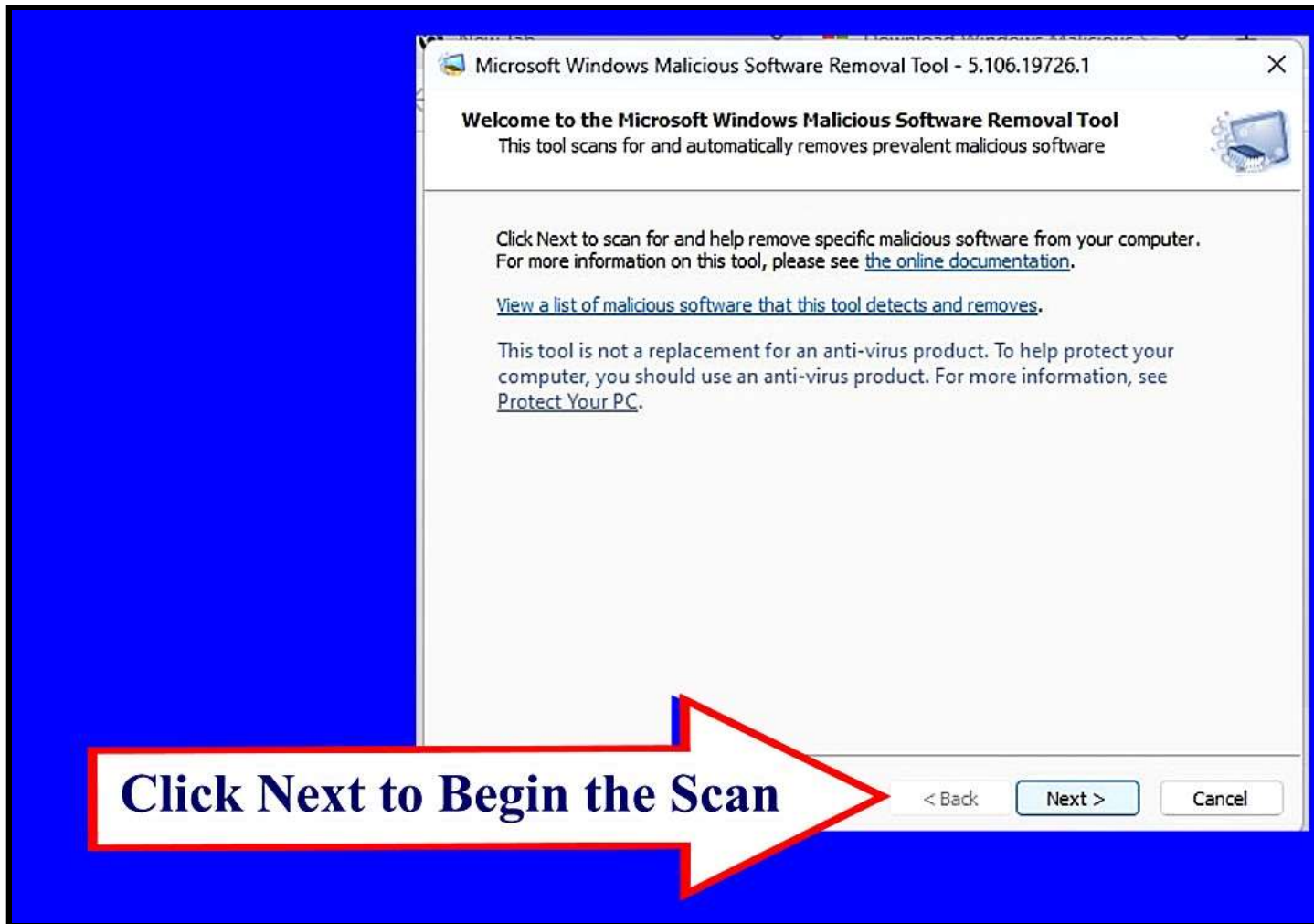
Before a scan is actually run, the app asks you what type of scan you would like to run.
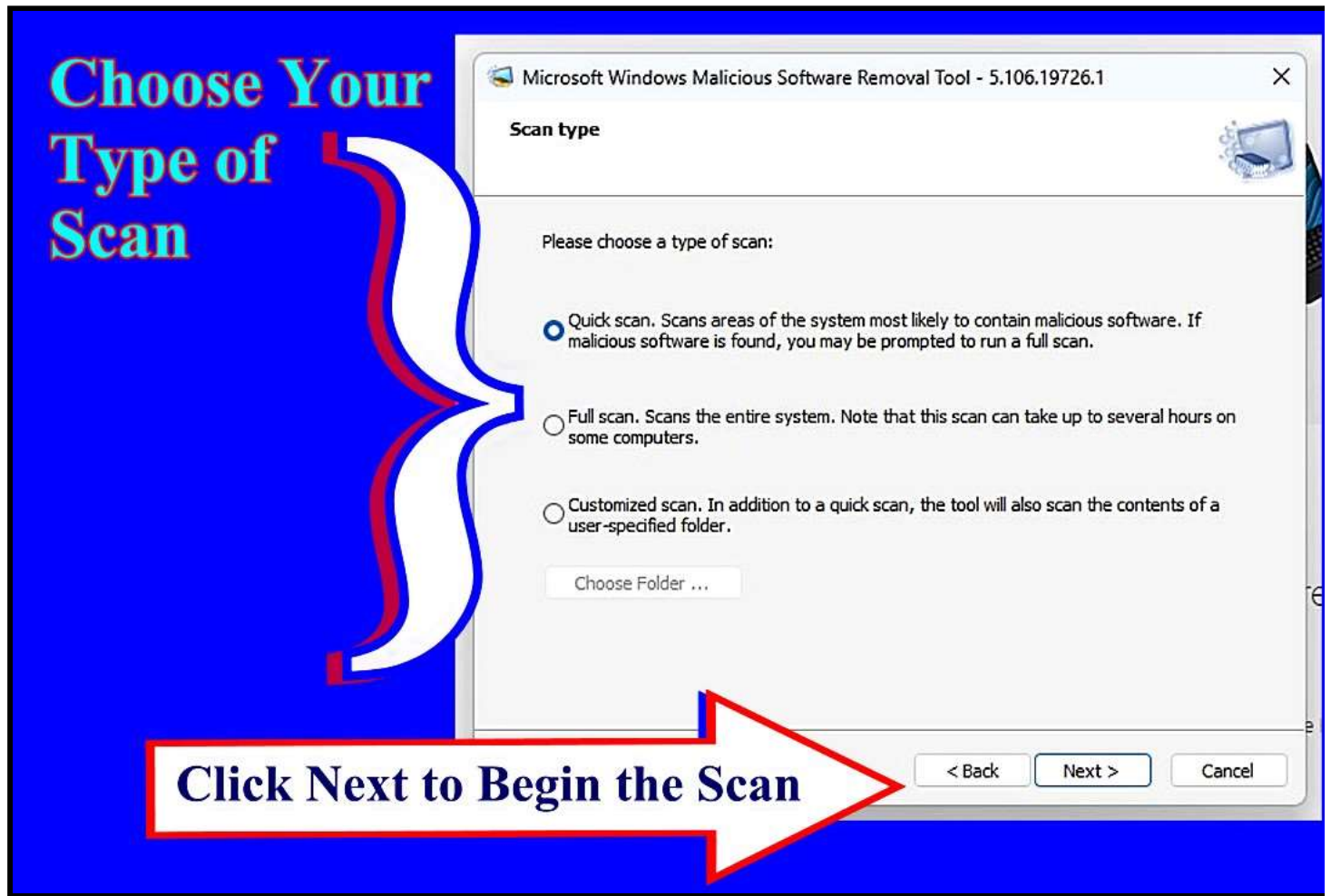
The default scan is a "Quick scan." This will scan the system files where the presence of virus would most likely be found. This is a relatively quick scan.

A **Full scan will scan the entire contents of your hard drive**. Depending on the disk size and the amount of data stored, this scan can take over an hour and could take up to several hours.

A **Customized scan** will allow you to choose which folder to scan.

Once the scan runs, the tool will display very detailed lists of the scan progress.
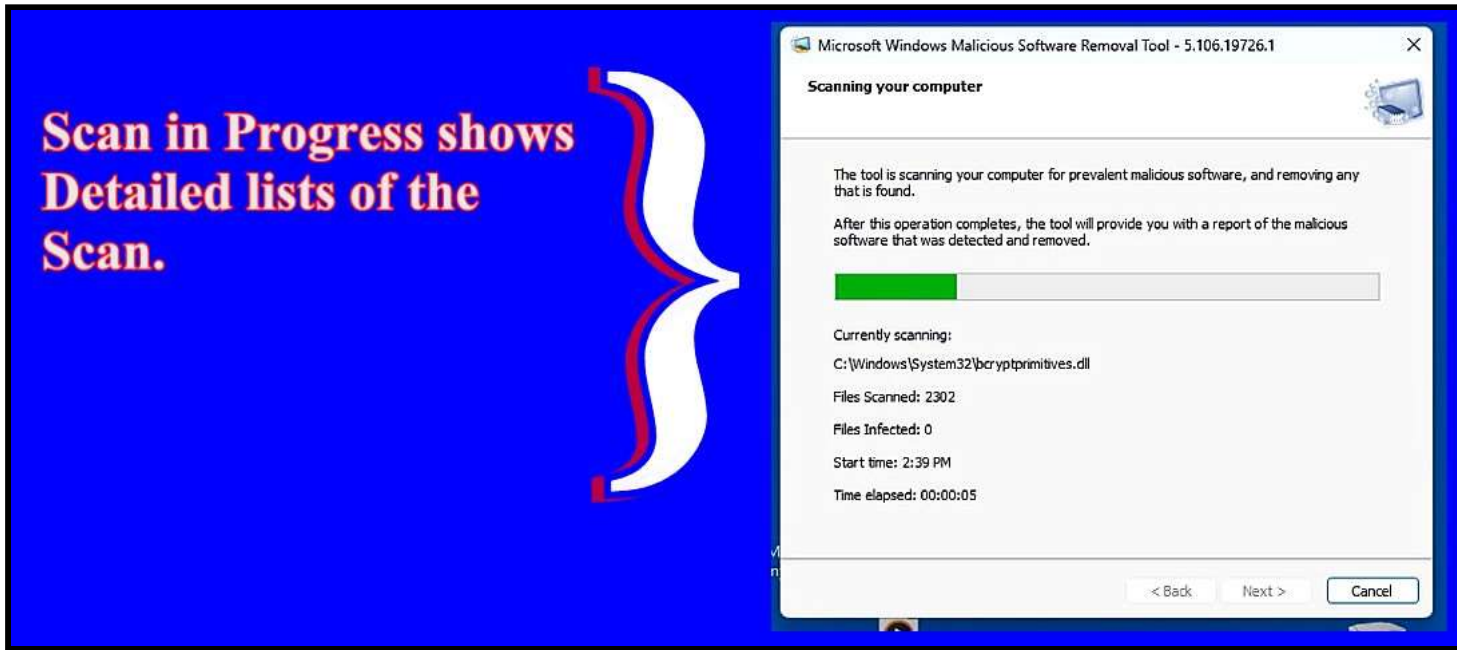
Scan in Progress shows Detailed lists of the Scan.

When the scan is finished, the app reports the results of the scan, and what removal actions were taken, if any. In this case, no malware was found.

When you click for a Detailed View, a list popups that names the types of malware that the app scanned for and what action was taken if that strain of malware was found.


Results of Scan Are displayed Once scan is Complete.

View detailed Results pops up A screen on the Right that list Types of malware Scanned for.

List of types of Malware scanned for.

One reviewer of this Windows Malicious Software Removal Tool mentioned that you can run the app again from Command Prompt. **At the command prompt, type "mrt/f".** That is, if you are into that sort of thing.
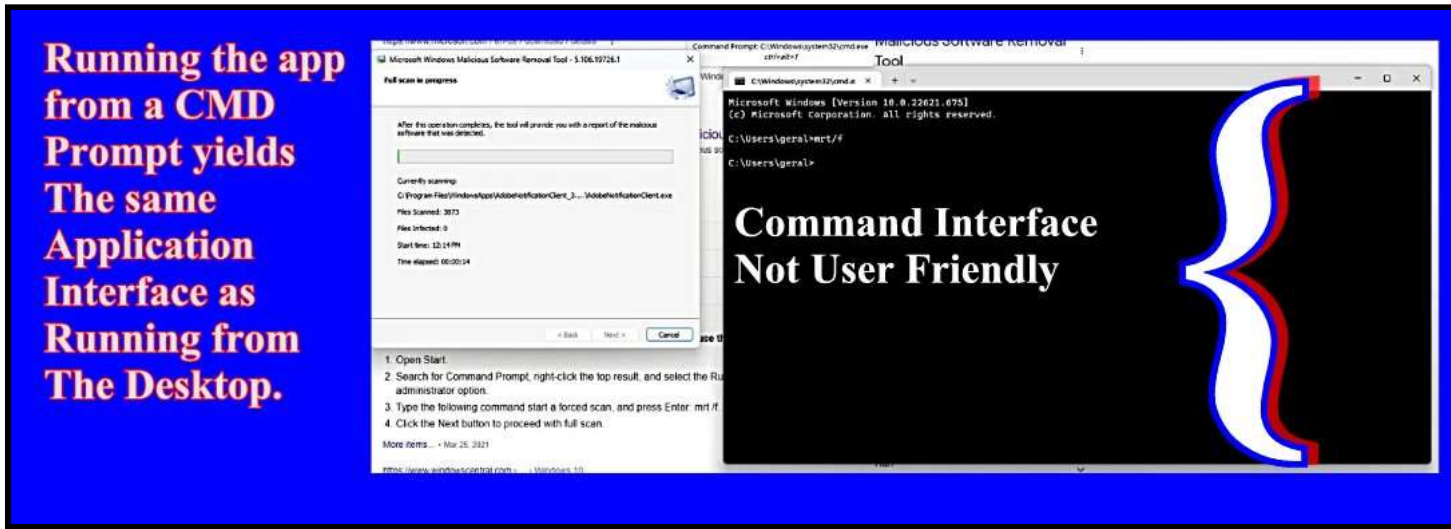
I think this is rather silly, though. Most average users don't use the RUN command to get to a CMD prompt to enter a command. Furthermore, I think it would be **best to download the most current version each time you wish to run a scan**. If you want to have the scanner handy at all times, then copy it from your Downloads Folder to the Desktop.

Use this tool whenever you have done something stupid online.
Use it when your Stupid Cousin Billy sends an email about the Conspiracy of the Day.
Use this tool after you get a Fake AV Alert popup.

Measure Twice Cut Once
— Second Frutes, John Florio, (1591)

Gerald Reiff

Back to Top

← **previous post**

next post
TBA→