

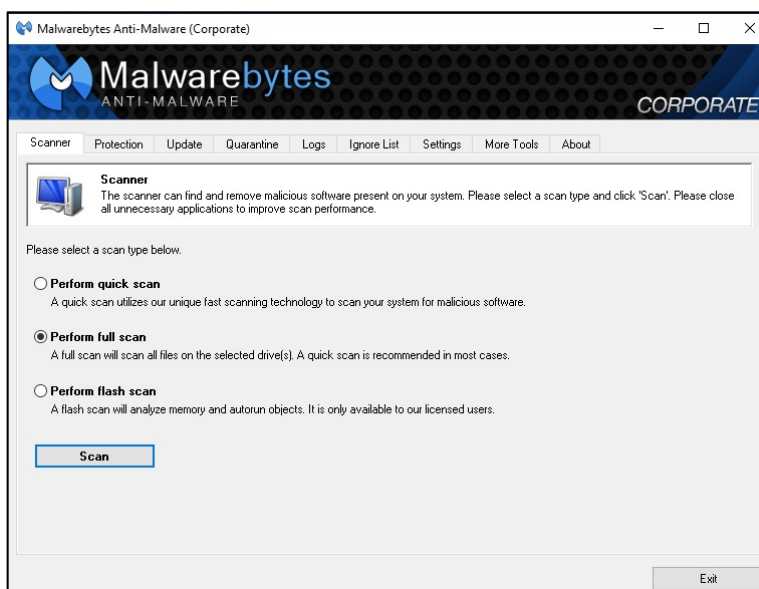
OHIO AUDITOR OF STATE KEITH FABER

TO: UAN Users
FROM: UAN Support
DATE: February 3, 2020
SUBJECT: UAN Security Update

UAN recommends that these tasks be performed weekly. Even if you do not use the internet regularly with the UAN PC, it is still necessary to utilize the security software detailed in this document.

Malware attacks over the Internet are increasing. Malware can come in many different forms ranging from a simple cookie, to a ransomware attack that locks down your computer. Malwarebytes is on the leading edge of fighting these attacks. It is not uncommon to receive some type of popup or malware message when using the Internet, especially for a long period of time. If you do receive a message that appears to be some type of malware or virus attack, the tools are on your computer to combat them. When an attack occurs, it may be difficult to determine if it is malware or a virus. Because of this, we recommend using both security pieces that are installed on your computer. Detailed below is what you should do in the event of an attack

Run a full scan with Malwarebytes Anti-Malware



88 E. Broad St. Columbus, OH 43215
Telephone: (800)833-8261 Fax: (877)727-0088
Email: UAN_Support@ohioauditor.gov

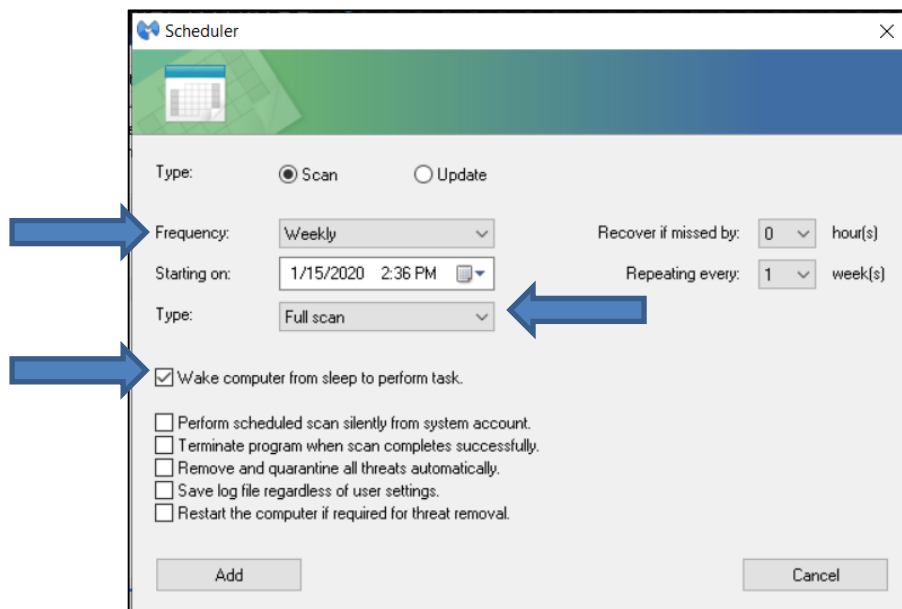
The Malwarebytes icon on your desktop is the first thing that you should run if you believe to have some type of malware or virus. If for some reason your computer is locked up, reboot and immediately double click on the icon after the restart. Choose the option 'Perform full scan' and click on the 'Scan' button. If you have a USB drive plugged in, the software will give you the option to scan it as well. Check the box next to the USB drive and it will be included in the full scan. During the scan, there will probably be instances listed. If you believe to have malware, this is a good thing because Malwarebytes will isolate the issues into a "Quarantine". Once the scan is finished, the instances will be listed. Always choose the option to 'Quarantine'. In the event that you have malware, you will want to run a second scan to ensure that your computer is clean.

Reboot and run a second full scan with Malwarebytes Anti-Malware

Once you have restarted, follow the same process with a full scan with Malwarebytes Anti-Malware. If your original scan finds many issues, you may see additional instances on the second scan. Keep performing this task and rebooting until the scan results in zero items to quarantine. If the scan results with an item that cannot be quarantined, a reimage may be necessary. Call UAN Tech Support in this case.

Schedule a scan to run automatically with Malwarebytes Anti-Malware


Malwarebytes must be run as an administrator to schedule a scan. To do this, right click on the Malwarebytes Anti-Malware desktop icon, and select 'Run as administrator'. You will then need to enter the admin password, which is 'FiscalOfficer'. Once Malwarebytes is open, go to the Settings tab. Within the Settings screen, go to the Scheduler Settings tab. To create a new scheduled scan, click the 'Add' button. Below is the Scheduler window.

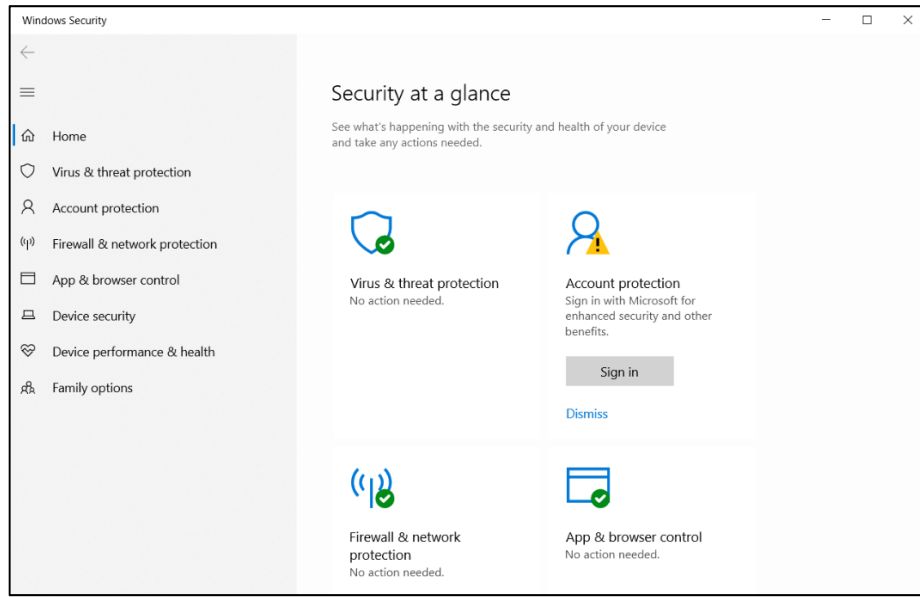


In this window, you will need to define the frequency, time of day, and type of scan. UAN recommends that a Full scan is completed at least weekly. To ensure that the scan performs if you are away, select the checkbox next to 'Wake computer from sleep to perform task.' Click the 'Add' button to save the scheduled scan.

Run a full scan with Windows Defender

In addition to a Malware scan when suspecting a security attack, a Virus scan should also be performed. To do this, right click on the Windows Defender Icon located in the bottom right portion of your screen under 'Show Hidden Icons'. (You may also run a Search for 'Windows Defender').

This is the icon.  Below is the Windows Security window.



If Windows Defender is running, there should be a 'No action needed.' Message under 'Virus & threat protection'. If there is a 'Turn On' option, please select it. To access the scanning options, select 'Virus & threat protection' on the left side of the screen. Under Current threats, there will be a 'Quick Scan' button. To complete a full scan, select 'Scan Options', then choose the 'Full Scan' option. Start the scan by selection 'Scan Now' at the bottom of the window. You may then minimize this window and continue with your work as the full scan could take over an hour.

This page was left blank intentionally.