|  |  |
| --- | --- |
| **TO:** | UAN Users |
| **FROM:** | UAN Support |
| **DATE:** | June 22, 2017 |
| **SUBJECT:** | UAN Security Update |

Windows Defender has replaced Symantec Endpoint Protection as the anti-virus software package on the UAN Dell Latitude 3570 and the OptiPlex 3040 PCs. In addition to the anti-virus software, Malwarebytes is installed as the Anti-Malware package *(Anti-Ransomware, Anti-Exploit, and Anti-Malware)*.

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**



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. 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.

**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. 



Under ‘Scan options:’ choose ‘Full’ and click ‘Scan Now’. This scan will go through every file on your computer, and run tests differently than Malwarebytes. This should take a considerable amount of time longer than the Malwarebytes Scan. During this scan, you may minimize the window and continue with your work. If the scan does result in an instance of a virus, first choose the option to Delete or Remove. Sometimes if a critical file has been infected, only a ‘Quarantine’ option is available. This is okay to do and as long as the result is successful, you can continue on with your everyday work.

**View the ‘Windows 10 Security for UAN Clients’ Video on the UANLink webpage**

This video will take you through updating both Security packages, and will show you how to schedule an automatic scan at certain intervals.

**View the free cyber security training video after logging in to Profile Login**

The Auditor of State has made this available to all UAN clients. This is a very informative video that goes in depth with one of the leading security experts in the world.

