HOW DO I PREVENT THIS FROM HAPPENING AGAIN?

While your computer was being serviced we installed two free programs - "**Windows Defender Security Center**" and "**Malwarebytes Anti-Malware**". Windows Defender Security Center is for removal of viruses, and Malwarebytes is for malware/spyware removal. Below are instructions for using both of these programs. If you follow these steps – *at least once a week* - you will have a much smaller chance of having to bring your computer back for infections. **BOTH PROGRAMS ARE VERY IMPORTANT TO USE, AND SIMPLY HAVING THEM ON YOUR COMPUTER IS NOT ENOUGH. EACH PROGRAM MUST BE MANUALLY UPDATED & SCANNED ONCE A WEEK!** Don't forget to be connected to the internet when running updates. It is also very important to check the 'Downloads' section of our website (www.affordablecomp.com) about once a month to see if there are new versions of these programs. Also, included on the reverse side of this flyer is a list of things to avoid all together. Make sure that **everyone** that uses your computer is familiar with this list of things to avoid, as avoiding the items on this list is **just as important** as scanning your system!

Windows Defender Security Center

1. ➔**Start Windows Defender Security Center** Double click on the **"Windows Defender Security Center"** icon located on your desktop (or click on Start and scroll down to "**Windows Defender Security Center").**
2. ➔**Get the latest updates:** Click on the '**Virus & threat protection**' option, then click on the '**Protection Updates**' option at the bottom. Now click on the grey "**Check for updates**" button. Windows Defender Security will now automatically download then install any available updates.
3. ➔**Scan your system for viruses:** Click on the **house** icon on the left. Next click on the '**Virus & threat protection**' option. Now click the "**Advanced Scan**" option. Make sure "**Full Scan**" is selected and then click the grey "**Scan now**" button. Windows Defender Security Center will now begin scanning your system. This may take some time. When the scan completes, if Windows Defender Security Center finds any infections it will display "*Threats found. Start the recommended actions*". Click the grey 'Clean Threats' button; Windows Defender Security Center will now remove the infections. Once the infections have been removed you will see a summary screen. You can now close the program by clicking the **X** button in the top right corner. Windows Defender Security Center *might* require a restart to remove the infections – if it asks to; allow your computer to restart. If Windows Defender Security Center is unable to remove any of the infections listed, or if the same infections keep showing up in future scans, then you will need to bring your computer to Affordable Computers for service. If Windows Defender Security Center displays a summary screen that says "No threats found" this means your system is clean. To close Windows Defender Security Center, simply click the **X** button at the top right corner of the window.

Malwarebytes

1. ➔**Start Malwarebytes:** Double-click on the **"Malwarebytes"** icon located on your desktop (or click on Start and scroll down to the **Malwarebytes** folder and click on **Malwarebytes**).
2. ➔**Get the latest updates:** On the right side of the window about halfway down you will see the words "**Scan Status**" – next to this you will see four icons, find the third icon over from the left that looks like a **round arrow** and left click on it. Malwarebytes will now automatically download any available updates. During this time there will be a status bar indicating the progress of the download (this may take some time). If when you click the **round arrow** icon it says *"Updates: Current"* then this means there are no new updates, and you can proceed to step three.
3. ➔**Scan your system for malware:** Click on the **"Scan"** tab (the 2nd tab down from the top at the left side of Malwarebytes). Make sure the left option **"Threat Scan"** is selected, and then click the blue **"Scan Now"** button at the bottom of the Window. Malwarebytes will begin to scan your system for possible malware infections - this may take some time. When Malwarebytes completes its scan it will show a list of all the items it found. Click on the blue **"Quarantine Selected"** button in the bottom right corner. You will screen with a summary of the scan. You may have to restart your computer when Malwarebytes finishes. If so, save and close anything you are working on and click **"Yes"** to restart your computer, otherwise click the **X** in the top right hand corner of the Window to close Malwarebytes. If your system is clean Malwarebytes will show a scan summary screen that includes *"Threats Detected: 0"* – click the **X** in the top right hand corner of the Window to close Malwarebytes.

...continued on reverse side ➘

Things to avoid all together!

Make sure that you and **everyone who uses your computer** is familiar with all of the items on the following list. Even with antivirus software, if you are not careful you will probably get infected and be back to the shop for service again!

- ➔ **do not** visit porn sites.
- ➔ **do not** download and install COUPON Printers, Programs, or surf the web looking for coupons.
- ➔ **do not** call **ANY** phone numbers that you may see on popup 'error messages' while surfing the web. *THIS IS A SCAM*. Never answer calls from companies claiming to be Microsoft, saying your computer is infected, or any 'tech support' calls similar to this. Absolutely **NEVER** let anyone remote into your computer. Do not give out your credit card information. **HANG UP THE PHONE. THIS IS A SCAM.**
- ➔ **avoid** using search engines (Google, Yahoo, Bing, etc.) whenever possible. Go directly to the website by typing the full address in the address bar (e.g. www.affordablecomp.com). Then add sites you frequent to your Favorites, and then get in the habit of using your Favorites to access these sites.
- ➔ **do not** use Google or other search engines to find tech support phone numbers (like Dell's phone number). Go directly to the company's website (dell.com) to find the phone number.
- ➔ **do not** use Google or other search engines to find sites to download programs (like iTunes, Google Chrome, etc.). Go directly to their official website (itunes.com, chrome.google.com, etc.). If you do not know what the official website is, **CALL US**, and we will look it up for you.
- ➔ **do not** visit video game cheat sites or file sharing sites/programs (Frostwire, Limewire, uTorrent, Bittorrents)
- ➔ **do not** download or install any program or utility found online that claims to optimize or enhance web performance, clean your registry or to maximize, boost, or speed up your pc.
- ➔ **do not** download **any** toolbars (this even includes Google, Yahoo, and toolbars from your ISP!).
- ➔ **do not** install more than ONE ANTIVIRUS Program. If you want to install a new AV Program, you should uninstall your current antivirus program **first**.
- ➔ **do not** click on any popup you may see online that states that "you may be infected ", not even the X to close it. If you see such a pop up you may be able to close it by Using the ALT + the F4 key, if not then try Using the CTRL + ALT + DEL (Delete) keys, all three at the same time. This opens the Task Manager which will let you see the list of applications or processes running. Try to find that pop up in the list and click END. If you cannot close it this way, then press and HOLD the power button until your computer turns off. These pop ups are trying to trick you into thinking you have a virus and if you click on it at all, even the X to close it, you could get a virus!

Subscribe to our Facebook page, Stay ahead of the viruses!

Are you a Facebook user? If so go to www.facebook.com/affordablecomp and click on '**Like**'. You will automatically receive updates and alerts from Affordable Computers Technicians about new viruses and scams to watch out for, be notified when new versions of Windows Defender Security Center and Malwarebytes become available, and get tips and tricks straight from Affordable Computers! All from the convenience of your Facebook news feed! So go ahead, become a fan of Affordable Computers today! It's 100% FREE!

To Stay Protected, Stay Updated:

At least once a month check for updates to Java, Adobe Flash, and Reader, and check for Windows updates. You can find links to these on our website (affordablecomp.com > downloads)

Need more help?

Check out our website at www.affordablecomp.com where you can download Windows Defender Security Center and Malwarebytes for your other computers for FREE via the **"Downloads"** button near the top right of the homepage. There are also other FREE useful downloads there. To reach us by phone dial 423-499-1975 in Chattanooga, 706-858-5888 in Fort Oglethorpe.

[ver 8.3.CU – 4.11.17]

AFFORDABLE COMPUTERS
sales • service • support