Bits & Bytes

Arkansas' Premier Computer Club

October 2019

Bella Vista Computer Club - John Ruehle Center

Highlands Crossing Center, 1801 Forest Hills Blvd Suite 208 (lower level), Bella Vista, AR 72715

Website: http://BVComputerClub.org **Email: editor@bvcomputerclub.org**

HOW TO FIND US

All meetings are on the lower level of the Highlands Crossing Center in Bella Vista. You may use entrance A on the West side or entrance C on the South side and take the elevator or stairs to the lower level. Turn left (West) to reach the General Meeting room, right for the John Ruehle Training Center. **The lower-level NE entrance is also now available again.**

MEETINGS

Board Meeting: October 14, 6:00 pm, John Ruehle Training Center

General Meeting: October 14, (2nd Monday), 7:00 pm, Community Room 1001.
Program: "Do You Need a Mesh WiFi Router?", presenter Joel Ewing. This will look at how mesh WiFi routers are different, and how they are a better solution than multiple routers or WiFi extenders in homes or buildings where consistent WiFi coverage everywhere is a problem.

Bring a guest! New Members and Guests are always welcome at the General Meeting

Genealogy SIG: October 19 (meets 3rd Saturday of the month).

MEMBERSHIP

Single membership is $25; $10 for each additional family member. Join by mailing an application (from the web site) with check, or complete an application and pay at any meeting.

HELP CLINICS

Saturday, October 5, 9am – noon

Wednesday, October 16, 9am – noon

Saturday, November 2, 9am – noon

Help clinics are a free service for BVCC club members, held in the Training Center

Bring your tower, laptop, tablet or smartphone for problem solving.

CLASSES

"Computer Security for Regular People, Part 2" – Justin Sell, Tuesday, October 15, 6:30 – 8:30 pm
Part 1 will be offered again on 3rd Tuesday in November.

"Slow PC? Let's Upgrade or Buy New" – Pete Opland, Tuesday, October 22, 9am – 11am

"Why, When and How to Backup Your C Drive" – Pete Opland, Tuesday, October 29, 9am – 11 am

Advance sign up required for each listed class: Contact Grace: email to edu@bvcomputerclub.org, text 469-733-8395, call 479-270-1643, or sign up at the General Meeting. Classes are **free to Computer Club members** and are at our John Ruehle Training Center.

Check the monthly calendar and announcements for any last minute schedule changes at http://bvcomputerclub.org .

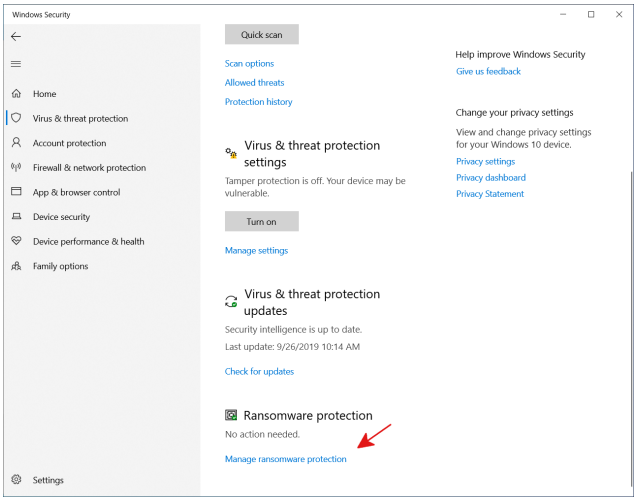
WINDOWS 10 RANSOMWARE PROTECTION

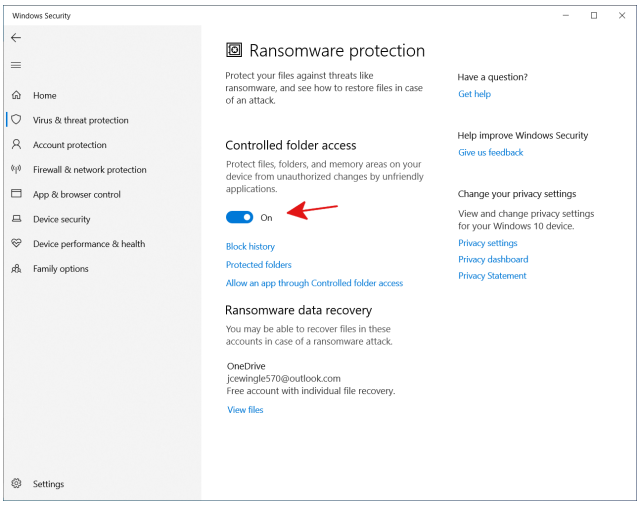
By Joel Ewing
President, Bella Vista Computer Club
October 2019 *Bits & Bytes*
http://bvcomputerclub.org

One of the prominently advertised features of Malwarebytes Premium (the non-free version) is that it provides real-time protection against ransomware attacks, the malware that encrypts all your personal files and then tries to extort money from you to get your files back.

Did you know that Windows 10 also has some native real-time ransomware protection capability, added with the October 2017 (level 1709) feature update to Windows 10? I just stumbled across it myself. I believe that Malwarebytes ransomware protection uses a sophisticated AI approach of attempting to analyze the behavior patterns of unknown programs. The Windows 10 approach is a more simplistic but potentially effective one that doesn't require sophisticated analysis: If a program is not a known and trusted program running from the appropriate file path on your computer, don't allow it to change content in folders that are defined as "protected".

By default this feature is turned off, because it is subject to false positives when dealing with software from non-Microsoft sources; and you do need to be aware when it is turned on and know how to modify its behavior if it blocks things you know are legitimate. I only learned of its existence when I encountered a failure trying to install Mozilla Thunderbird on a rare system where it was enabled.

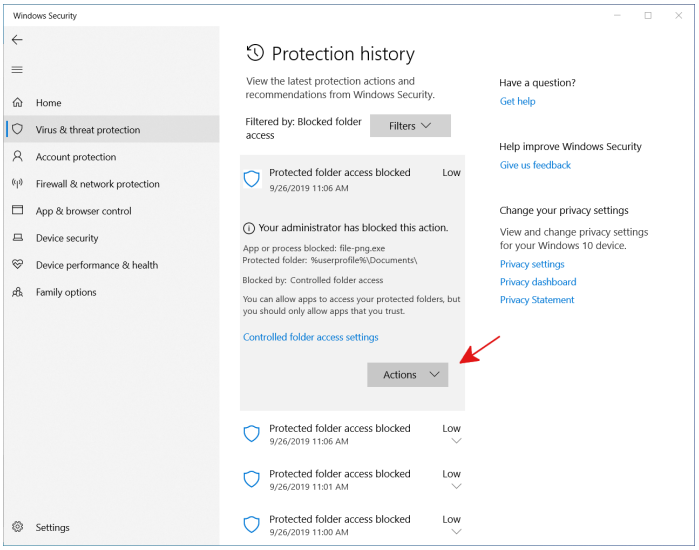




Search for "Virus" which should find "Virus & threat protection" (part of System settings) and open that. Scroll down to the bottom to find Ransomware protection and click on "Manage ransomware protection". To enable ransomware protection, toggle the "Controlled folder access" switch to "On". Once it is enabled you will see other options available that can be used to tune its behavior.

The protection works by restricting what programs are allowed update access to selected folders containing user files. By default the protected folders are your folders for Documents, Pictures, Videos, Music, Desktop, and Favorites, and the Public folders for Documents, Pictures, Videos, Music, and Desktop, as these are the folders in which most users save their personal files. If you have personal files in additional folders that need to be change-protected, additional folders may be added. All contents of a protected folder, including all sub folders and their files, are protected from change by an unknown

program. Microsoft has a built-in list of "acceptable" application programs that are allowed to change things in the protected folders, and will block attempts by "unknown" programs to alter these folders.



If an attempt to modify a protected folder is blocked, you will receive an "Unauthorized changes blocked" notification alert. From the "Ransomware protection" window under "Windows Security", you can click on "Block History" to see blocked events, and click on one of those to see the details of the failure. If you know this is in response to an action you requested from a legitimate application, from the details of the blocked event you can select "Allow on device" from the "Action" list. This will enable that program at that specific path to change all protected folders the next time the program is started. Alternatively, if you know the full path to the failing program, you can manually add it using the "Allow an app through Controlled folder access" link on the Ransomware protection window. You can also view there the programs you have added for protected folder update access.

If the failure occurs during an install of an application that is known to be legitimate, one choice is to just turn "Off" Controlled folder access, install the application, and then turn it back on. This worked to circumvent a failure during Thunderbird installation (probably caused by the install adding a shortcut to the protected Desktop). I suspect you will have this issue attempting to install any non-Microsoft application that places a shortcut on the desktop. If the application automatically checks for and installs updates, this problem may or may not repeat for each update – if it does, you probably want to use the "Allow on device" approach above for a more permanent fix.

I like the idea of turning this feature on for the added protection it provides, but even a brief usage does show that you will have to be prepared to get failures with all your legitimate non-Microsoft applications that need to save anything in these protected folders, and enable access as those failures are found – an initial pain, but I think it could be worth it in the long-run. Some applications may even require that multiple programs be enabled. I have not yet found a non-Microsoft application that by default could store into protected folders, so I would presume this is by design. While less convenient for the end user, this is a rational design choice for Microsoft since they have no control over the directory path or program names chosen by other software distributors. Those applications I've found on my Windows 10 system so far that are not enabled to change protected folders and require enabling of specific programs include:

- LibreOffice – C:Program Files\LibreOffice\program\soffice.bin
- GIMP – C:\Program Files\GIMP 2\bin\gimp-2.10.exe (changes for new release)
  For exporting images in various file formats, you will need to enable a different program for each of the major file type groups under C:\Program Files\GIMP 2\lib\gimp\2.0\plug-ins\…
  png: file-png\file-png.exe
  gif: file-gif-save\file-gif-save.exe

jpg: file-jpeg\file-jpeg.exe
ico: file-ico\file-ico.exe
pdf: file-pdf-save\file-pdf-save.exe
tiff: file-tiff\file-tiff.exe
bmp: file-bmp\file-bmp.exe
(probably others, but these are the only formats I regularly use)

- KeePass – C:\Program Files (x86)\keePass Password Safe 2\KeePass.exe
- FireFox – Blocked, but not added. Without knowing more about how FireFox handles scripts, this is one you might not want to allow since one common source of malware infection could be a rogue web site executing scripts that trick your browser into doing bad things. Without enabling FireFox, you can still download files into the "unprotected" Downloads folder.

I have some other non-Microsoft applications that I use less frequently. I suspect they will have similar problems and also require adding their programs to allow protected folder access.

Note that GIMP is unusual in that more than one program needs to be enabled for protected folders. Exporting an image in various image formats apparently invokes a secondary program, depending on the file type, to do the actual saving. That secondary program must also be allowed protected folder access in order to save exported files for those format types. The list above is incomplete, but covers the most common image formats. If you only export in a small number of image formats, those are the only ones you really need to worry about. If you export from GIMP to image types not covered above, you may need to add additional programs to the list.

Note that while the Thunderbird email client requires folder protection to be disabled during install, by default it does not need protected folder access to run, as it stores all mail related data under C:\users\<your-user-dir-name>\AppData\Roaming\Thunderbird, which is unprotected. If you have important emails saved, you may want to add that as a protected folder to protect it against ransomware also, in which case you will have to experiment to see what executables associated with Thunderbird must be allowed protected folder access. I would guess at a minimum that would be C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe, but there could be others.

It appears that the determination of whether a program is allowed to access protected folders is made at the time the program is started, not when the access is next needed. That means that if you get a failure from a program the first time you try to save into a protected folder and then enable the program to update protected folders, if the program is still running it will have to be stopped and restarted before the change takes effect. That may require you to temporarily save a file in an unprotected folder in order shut down the program without losing data you have created.

BVCC FINANCIAL OUTLOOK

The BVCC Board learned at the September Board meeting that Bella Vista Recycling is suspending payment of grant funds to non-profit organizations that supply volunteer workers at the Recycle Center, starting in mid September. The market value of recycled materials has dropped drastically because of the tariff trade war with China, which has caused China to cease purchase of recycled materials from the U.S. As a result the Bella Vista

Recycle Center is under financial stress and has minimal or no net profit to distribute among other non-profit organizations. It is the hope of the Recycle Center that this problem is temporary, but the timing of any resolution is out of their hands. It could easily be over a year before this tariff war ends, and there is no guarantee that the recycle market will recover immediately after that.

BVCC has been blessed over the last decade to have had the Bella Vista Recycle Center as a grant source. Those grant funds have subsidized the cost of maintaining our Training Center and have made it possible to offer classes and Help Clinics for free to our members for the last decade. Prior to about 2009, members had to pay modest fees for classes, with higher rates for non-members. Without some replacement for the Recycle Center grant funds, we may be forced to consider a return to that practice of requiring class fees to help fund the Training Center.

During our last fiscal year (Sept 2018 – Aug 2019) our Training Center provided 177 student contact hours in classes and served 85 members at Help Clinics. During that same 12 months, if we had not had any grant funds from the Recycle Center, we would have had a deficit of $3,854.48. That rate of loss will put us out of business in three years. We need some combination of alternative grant sources (no promising prospects found so far), outright financial donations, more members, and/or a return to the practice of a decade ago of charging for classes or Help Clinic usage to help defray the cost of maintaining the Training Center, which costs us slightly over $6,600 annually just for rent and fixed expenses.

Joel Ewing, BVCC President