Two anti-malware topics (for Potpourri)

What's the best anti-malware for Windows 7? (or Windows 8.1)

What are all the Software Security Settings in Windows 10?

presented by Gary Patrick 1/15/2020
Lexington Computer & Technology Group
with assistance from Bob Primak on audience questions

[slideset revision 12/17/19]

A recent question posed to the Reader's Forum on the AskWoody.com website was:

What's the best Free Anti-virus for Windows 7?

My takeaway, from reading the responses:

1) Respondents suggested (in alphabetical order):

Avast, AVG, Bitdefender, Kaspersky, Microsoft Security Essentials, and Panda. (Avast Free is the top-rated product by Consumer Reports).

2) Several comments about Avast and AVG say they've gotten bloated with extra features

- their marketing model is to add features some of which they try to sell to the user <Sinclair>
- one can dial these extras back <Sinclair>

3) Opinions how these 3rd party anti-virus products will be affected by Windows 7 end of support.

- MS Security Essentials likely to cease definition updates <geekdom>
- Avast and the others likely to continue signature updates.

Here was the actual wording starting the discussion on the Ask Woody Website Readers' Forum:

Reader <Nibbled by Ducks> asked: “With [end of support life for] Win 7 coming up, does anyone have a decent FREE AV going past EOL. I'm on a tight budget, and Avast/AVG (same company) has been getting some bad press lately… “

Replies:

by <Sinclair>: “I would stick with Avast as they still have one of the best AV that works well under Windows 7. The recent bad press has been a lot of old news and hype for attention-grabbing headlines. The newly claimed https scanning has not materialized and looks so far to be a feature from five years ago. That was well documented at the time it was added and has an off switch.

If you know Avast and understand how to work the menus and settings then it's perfectly usable.

With Avast you know they have a habit of adding new modules and settings with every new update. Their earnings model [depends] on getting and selling user data. But you can dial that back and opt out on a lot of that in the settings. You just have to keep an eye out for it.

As with any other AV. Sometimes Windows updates, browser updates or updates to the AV itself can interact badly with the AV software. What is meant to keep your system safe and healthy then destroys it. This is always a risk when using an AV but given the complexity of it all hardly surprising.

Alternatively you could use Windows' own Anti Virus, Windows Defender as this is not bad either." [But, in Windows 7 or 8.1 "Windows Defender" is actually MS Security Essentials, definitely not as good protection as Windows Defender in Windows 10.]

Avast and AVG merged several years ago, but continue to issue their separate products.

Avast bought Piriform (the source of CCleaner) a couple of years ago; Avast got a black eye because subsequently there was an interval of CCleaner versions that were found to contain malware, beginning with version 5.31. CCleaner 5.30 was pure, and the malware contamination was eliminated by the time of version 5.36. (2017)

More comments on specific products: <respondent's id handle>

Avast,
by <TonyS> “Avast has gotten too large and unwieldy for me.”
by <DaveYVR> “not as aggressive with messages; I have disabled by default some features that would muck up your system restore points if enabled. So I may gravitate back to Avast. (from Panda)
I have learned recently that their free version collects data from you.”
by <tonyl> (opinion): they won’t abandon you for some time yet. The program might stop getting updates after a year or two, but the definitions won’t stop”
Avast Free 2019 is Consumer Reports' top-rated free product.

AVG by <anonymous> “good luck with AVG since the 1990’s.
not as good as it was 10 years ago as it is more intrusive, less user options, and more telemetry but I think I have a handle on that.
If you have a 3rd party firewall you can block all the outbound telemetry and snoopyness too, and still get the definition updates”
by <Charlie> in AVG forum: September had a problem with prompts to Restart the Computer every couple of days, but another update seems to have fixed the problem.
AVG Free 2019 holds 3rd place in Consumer Reports testing.

Bitdefender, by <PKCano> “Very little impact on the system.”
It is in 2nd place in 2019 testing by Consumer Reports.

Kaspersky, by <Alex5723> “has a free version with limited settings”
by <Larry B> “You do get popups offering you to use their servers for VPN, but limits the amount of free traffic. I just decline.”

Panda Dome,
by <GoneToPlaid> I use Panda Dome on all of my computers.
As a sanity check to make sure that Panda hasn’t missed anything, I manually run the free version of Malwarebytes from time to time.
free version provides extremely good protection:

- includes a really good firewall.
- it was never affected by the patches for Meltdown, and it was
- never affected by any of the more recent Windows updates which have caused problems for many other AV vendors.

by <DaveYVR> free version recently become very aggressive on the pop-ups near my system tray. answered by:
<GoneToPlaid> “It is easy to turn off the popup notifications”
<Larry B> Too many false positives with Panda Dome. I went with Kaspersky free version.

All of the Anti-virus products mentioned above (except Panda Dome, for which I had no coverage) have very good test results in my November 28, 2018 report to this group (but with a lower ranking for Microsoft Security Essentials).

I also made a recommendation it's a good idea to add an anti-ransomware product.

The next slide is an updated Consumer Reports Test Results Chart for 2019 Free Anti-virus products.

Their top-rated for-pay Internet Security Suites are: Bitdefender and ESET (tie scores = 78), Avast (76), Norton 360 Deluxe and AVG (tie scores = 75).

Consumer Reports scores for ESET, Avast, and AVG are much improved over 2018 versions (refer to my November 28, 2018 presentation slides).

Consumer Reports 2019 Test Results on Free Anti-virus Software (CR online, not in magazine issues)

Tested in Windows 10

Last year's score and a comment added:

Overall Score	Brand & Model / Price	Protection	On access	On demand	Ease of use	Messages/Interface	Help	Anti-malware	Use of resources
Free Anti-Malware Programs									
OVERALL SCORE 77	**Avast** Free Antivirus - 2019 Recommended Price: $0.00 — 2018: 72; Protection and Help improved over last year.								
OVERALL SCORE 74	**Bitdefender** Antivirus Free Edition Recommended Price: $0.00 — 2018: 75; Protection has declined from "Excellent" last year; Help still poor.								
OVERALL SCORE 74	**AVG** Free Antivirus - 2019 Recommended Price: $0.00 — 2018: 69; Now has same back-end protection engine as Avast (owns AVG).								
OVERALL SCORE 67	**Avira** Free Antivirus - 2019 Recommended Price: $0.00 — 2018: 71; Slight decline in judgment of use of resources.								
OVERALL SCORE 66	**Kaspersky** Free Antivirus - 2019 Recommended Price: $0.00 — 2018: 64; Improvement in Anti-malware protection this year.								
OVERALL SCORE 58	**Microsoft** Windows 10 - Defender - 2019 Price: $0.00 — 2018: 61; Decline in judged effectiveness of "on demand" scanning, to "fair."								
OVERALL SCORE 53	**ZoneAlarm** Free Antivirus 2019 Price: $0.00 — (not tested last year)								
OVERALL SCORE 47	**Sophos** Home Free Price: $0.00 — (not tested last year)								

References:
the AskWoody Forum: https://www.askwoody.com/forums/topic/any-good-free-avs-out-there-for-win-7/?mc_cid=5ea474ced4&mc_eid=c3d7529d95

AskWoody Forum post about AVG:
https://www.askwoody.com/forums/topic/avg-free-upgrade-in-2019/
(comments about feature bloat, data mining, and how to mitigate it)

Link to Gary Patrick's report on Anti-malware Test Results a year ago:
Go to LCTG.toku.us, and scroll down to November 28, 2018.
Slides #6-9, 13, 14, & 20 give pertinent test results for free AV products
Slide #21 gives a Consumer Reports test results chart for 2018 Internet Security Suites, with information on specific extra product features.
Slides #22-23 give a summary of Overall Recommendations.

A walkthrough of Security Settings, Windows 10

based upon an article by Lance Whitney, in
AskWoody Plus Newsletter, Issue 16.32.0, 9/09/2019,
and Microsoft Corp. Product Support pages.

To begin, on the Windows 10 Desktop,
Select Start > Settings > Update & Security > Windows Security

The main Windows Security screen in Windows 10:

- a list of "Protection areas," each with a status indicator
- checkmarks in green circles that show everything is good
- “Open Windows Security” button is a bit redundant — it takes you to a slightly more detailed security window.)

Figure 1. The opening screen for Windows Security gives you a quick system status.

Click on “Virus & threat protection,”
then look under "Current threats" for the “Scan options” link, to click.
The window in Figure 2 will open;
You are presented with four choices:
Quick scan, Full scan, Custom scan, or Windows Defender Offline scan.

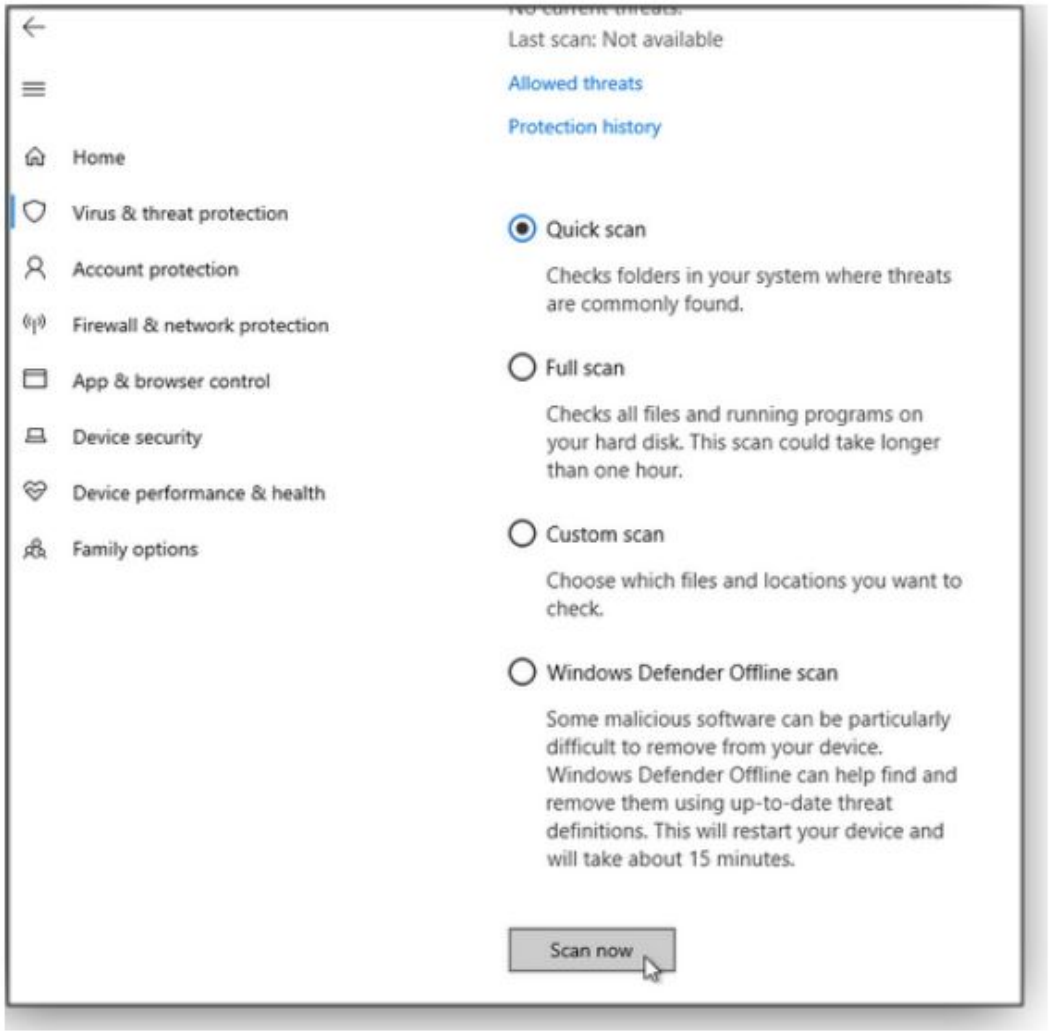


Figure 2. As with any good anti-malware app, Windows Security offers several types of scans.

Quick scan: Typically this should suffice; it checks all folders and files that are likely to harbor infections.

Full Scan: You might run a Full Scan if the quick scan doesn't turn up anything but you still suspect there's a virus in the system.

Custom scan: helpful if you wish to scan a specific area, such as an external drive or mapped network drive.

Windows Defender Offline: This scan option addresses the issue that Malware can be quite adept at hiding on your PC — while Windows is running.

- The solution is to boot up the machine with a basic operating system and run a malware scan from within that other OS (Linux, for example).
- This lets the anti-malware software look deep into the installed version of Windows.
- It's about the only effective way to find and remove viruses such as rootkits.

Invoking Defender Offline (see next slide for more info) uses this trick. It will reboot your system and then run its anti-malware tools from a specialized and separate version of Windows.

Before you use Windows Defender Offline,

- You typically need administrator rights on the PC on which you plan to run Windows Defender Offline.
- make sure you save any open files and close all apps and programs.

You'll be prompted that you're about to be signed out of Windows.

Then your PC should restart. Windows Defender Offline will load and perform a quick scan of your PC in the recovery environment. When the scan has finished (after about 15 minutes), your PC will automatically restart to Windows.

If you experience a Stop error on a blue screen when you run the offline scan, force a restart and try running a Windows Defender Offline scan again. If the blue-screen error happens again, contact Microsoft Support

To see the Windows Defender Offline scan results:

Select Start , then select Settings > Update & Security > Windows Security > Virus & threat protection .
On the Virus & threat protection screen,
(In an up-to-date version of Windows 10) Under Current threats, select Scan options, then select Threat history.

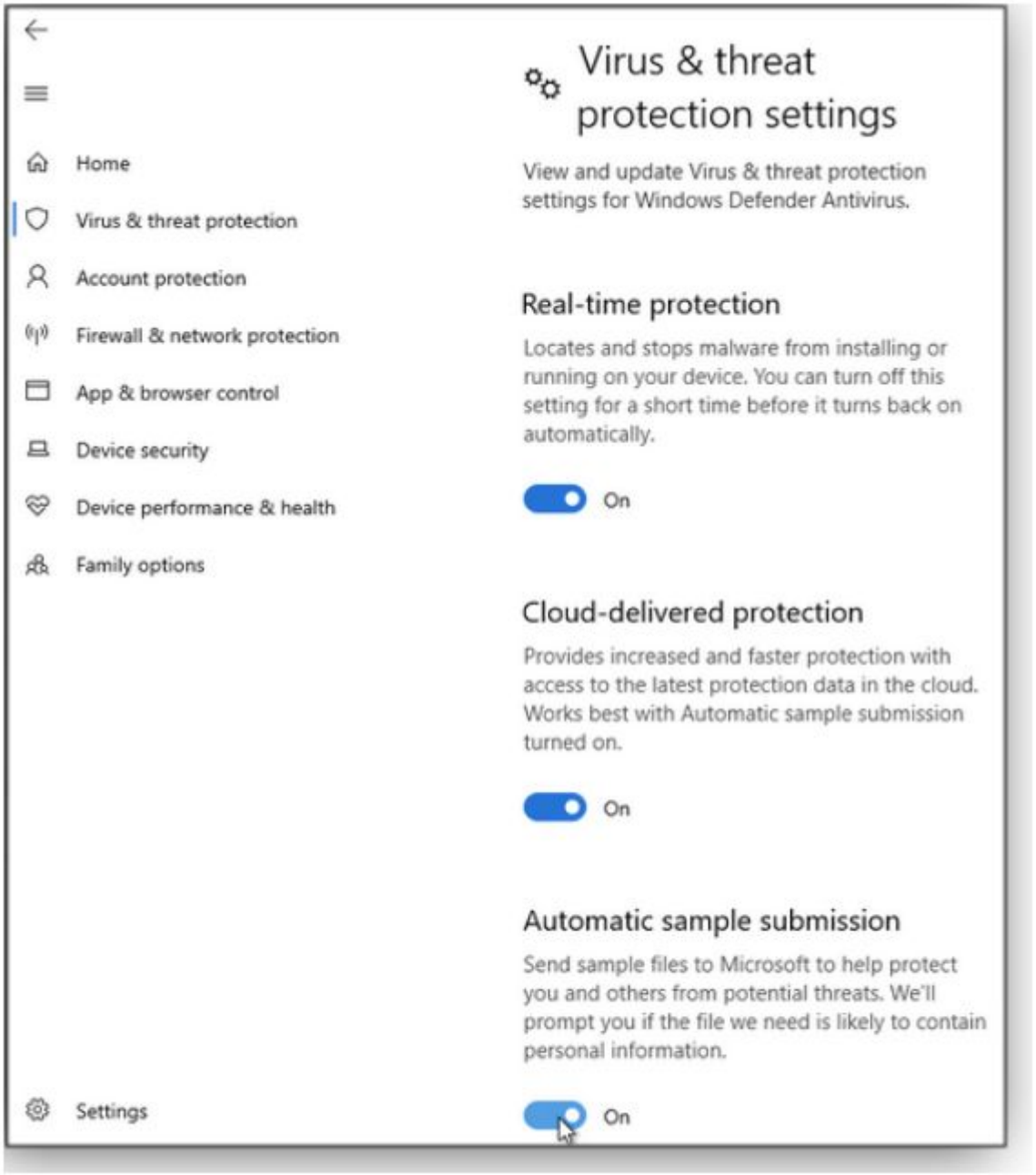


Figure 3. In the *Virus & threat protection settings* window, ensure that the first three options are enabled.

I think Tamper Protection status (discussed next) is suppose to show in this window (?) under "Manage Settings"

but it was introduced in Windows Update 1903, so won't show under previous Updates..

Tamper Protection blocks attempts by malicious apps to modify Windows Defender Antivirus settings through the registry.
(including real-time protection and cloud-delivered protection).

(Its status shows if you select Virus & threat protection,
then under Virus & threat protection settings, select “Manage settings.”)

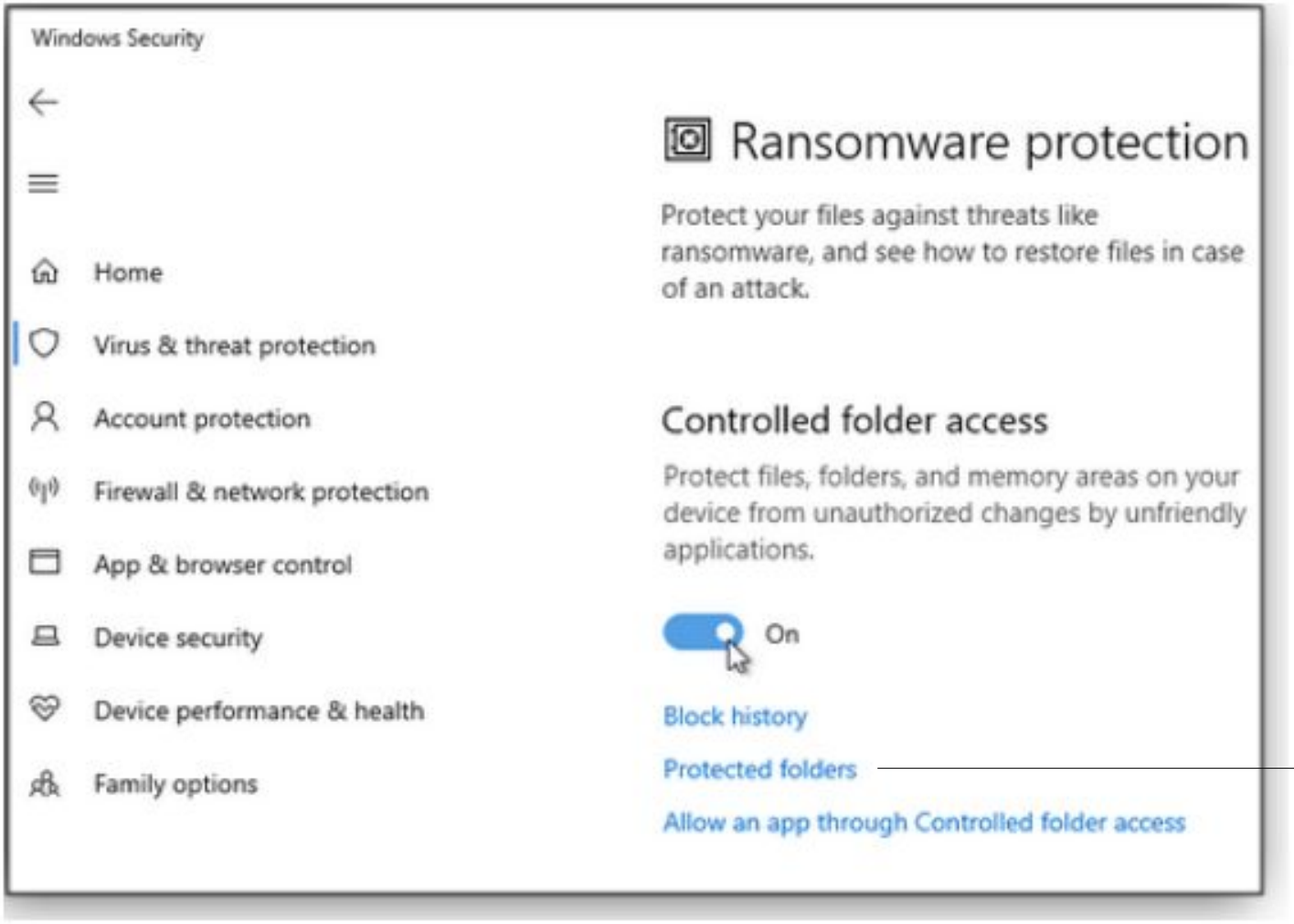
Tamper Protection is on by default, affecting the following controls:

- if you're an administrator on your computer, you can still change settings in the Windows Security app. However, other apps can't change these settings.
- but, you won't be able to turn off the Windows Defender Antivirus service by using the DisableAntiSpyware group policy key.

If you turn Tamper Protection off, you will see a yellow warning in the Windows Security app under Virus & threat protection.

(To help ensure that Tamper Protection doesn’t interfere with third-party security products or enterprise installation scripts that modify these settings, go to Windows Security and update security intelligence to version 1.287.60.0 or later. Once you’ve made this update, Tamper Protection will continue to protect your registry settings and will log attempts to modify them without returning errors).

Next up, Controlled Folder Access should also be enabled:
Prevents malicious programs from changing system and personal-profile files and folders.
Click on the Manage Controlled Folder Access link (which opens the Ransomware protection window, Figure 4) and flip the switch to "On"



see next slide

Figure 4. The *Controlled folder access* option prevents malicious apps from making unwanted changes to Windows files, folders, and memory.

Clicking the “Protected folders” link lets you see what's protected.

If "Controlled folder access" proves too aggressive and blocks a desirable (and safe) app, you can select the “Allow an app through Controlled folder access” link (Figure 4) and add it to an exceptions list

Under “Controlled folder access,” select “Manage Controlled folder access.” Switch the “Controlled folder access” setting to On or Off.

Explanation: Controlled folder access in Windows Security reviews the apps that can make changes to files in protected folders. Occasionally, an app that is safe to use will be identified as harmful. This happens because Microsoft wants to keep you safe and will sometimes err on the side of caution; however, this might interfere with how you normally use your PC. You can add an app to the list of safe or allowed apps to prevent them from being blocked.<fromMS>

Now return to the “Virus & threat protection settings” screen.

The next option — Exclusions — lets you add files or folders that you don't want scanned by Windows Defender. The only items you should need to enter are legitimate files, folders, file types, or processes that Windows Defender incorrectly flags as malicious.

The final Notifications settings control where and how you're notified of certain security events. To check current settings and make changes, click the Change notification settings link. By default, every option should be enabled — I recommend leaving them that way.

Next, go back to the main Virus & threat protection screen. Windows should automatically keep your security software updated. To manually download new virus signatures, click the link under Virus & threat protection updates and then select the “Check for updates“ button (see Figure 5).

About automatic anti-virus updates, and manual updating:

Figure 5. You can be sure you have the latest virus information by clicking *Check for updates* in the *Protection updates* window.

The final major option under Virus & threat protection is Ransomware protection. (You've already seen this screen — it was enabled when you turned on Controlled folder access).

- - - -

All current versions of Windows 10 include an option to set up OneDrive (on a Microsoft server) as a backup location, in case any of your important files is corrupted or lost due to malware. (Whether you use OneDrive or another service, you should always have local and online backups of your critical files and documents.)

Finally, you'll want to check out the other Windows Security categories,

- Account protection,
- Firewall & network protection,
- Device security,
- and others.

But if you do nothing else, at least review your Virus & threat protection settings — it's a solid step toward protecting yourself, your computer, and your critical files.

References:

Windows Defender Offline:
https://support.microsoft.com/en-us/help/17466/windows-defender-offline-help-protect-my-pc?mc_cid=5ea474ced4&mc_eid=c3d7529d95