Lab *03* – Potential Hardening Techniques

David Murillo Santiago
Professor Valecha
IS-3423
28 November 2023

INTRODUCTION

In this lab, I aim to enhance the security of my Windows machine by implementing ten distinct host hardening techniques. These measures include incorporating AdBlockers, forcing logoff when inactivity/logon hours expire, enabling Hard Drive Encryption (BitLocker), updating, and patching the operating system, turning off Secondary Logon Services, closing unused ports and services, enabling Windows Notifications for Events, disabling default Windows services, installing, and updating an antivirus, and limiting the physical access of a host.

PROCESS

(Part A) Step *1: 10 Hardening Techniques*

I chose to strengthen my device security by implementing the following 10 hardening techniques:

1. Use AdBlockers or Pop-Up Blockers

Ad-blockers are software tools designed to improve the online experience by blocking unwanted ads on web pages. Although they are widely used for this purpose, they also strengthen your computer's security, to the point that the FBI even recommends their use. ad-blockers reduce the risk of inadvertently clicking on malicious ads, providing an added layer of security against malware and phishing attacks. These extensions also block ads in search results, protecting users from malicious campaigns impersonating legitimate brands. Additionally, they enhance privacy by preventing tracking tools embedded in ads from collecting user data. Because ad-blockers filter all pop-up advertising, websites may require you to disable ad-blocking as they earn money from displaying ads. Therefore, users should consider the impact on content creators and publishers who rely on ad revenue when employing these tools.

2. Force Logoff when Inactivity/Logon Hours Expire

Implementing an automatic logoff after user inactivity feature is a vital security measure. Force logoff reduces the risk of unauthorized access when a system is left unattended. Similarly, auto logoff after specified logon hours reinforces access restrictions, lowering the risk of unauthorized access during restricted time periods and ensuring compliance with company access policies. One downside to this feature is users may become frustrated as they have to login every time after briefly stepping away from the computer.

3. Enable Hard Drive Encryption (BitLocker)

Enabling hard drive encryption strengthens your device security, especially in the case that your device is stolen or has been accessed by malicious actors. The way it works is the contents of the hard drive go through an encryption process where only the users with the right password can access the information. One disadvantage of encrypting your hard drive with a password is if the password is forgotten. Good password management is required as forgetting the password will likely result in the loss of the data.

4. Update and Patch Operating System

Updating your Operating System is an important hardening activity as the system updates include security patches for found vulnerabilities. Checking for updates regularly is an important security measure to protect yourself from vulnerability exploitation. Although updating your devices is important, one disadvantage of frequent updates is it may create application compatibility issues until the application developers too release an update.

5. Turning Off Secondary Logon Services

Disabling the Secondary Logon service is a security move involving the shutdown of a Windows service responsible for running processes with alternative credentials. Because this service allows users to execute programs with different credentials, it poses a security risk if exploited. Turning off Secondary Logon Services mitigates privilege escalation threats and unauthorized access. However, one downside of turning the service off is some applications rely on this service, leading to compatibility issues.

6. Close Unused Ports and Services

Closing unused ports and services is a fundamental step in computer hardening. Ports are communication endpoints that allow data to be transmitted between a computer and external networks. By closing unused ports, you minimize potential points of entry for cyber threats. Closing unused pots is important to limit your attack surface, but one must be careful when closing ports as closing the wrong one may impede network traffic and cause Network issues.

7. Enable Windows Notifications if Events.

Windows notifications offer real-time alerts which encompass software updates, system warnings, and security events. By enabling notifications, users can become immediately informed of new updates that are released. One downside to enabling notifications is information overload. A user may become fatigued from constant alerts and begin to ignore them all together. Therefore, it is important to prioritize the important notifications.

8. Disable Default Windows Services

Windows defaults various services, some of which are nonessential for specific users. By deactivating unnecessary services, users improve system security as the unused services will no longer have access to the machine. One disadvantage of disabling services is if you accidentally disable the wrong service, you may affect the functionality of your device. Therefore, it is important to research the service you are disabling prior to disabling it.

9. Install and Update an Antivirus

Installing anti-virus software helps defend against various threats such as viruses, Trojans, spyware, and ransomware. Anti-virus software offers continuous detection and behavioral analysis and also remove threats. Although anti-virus software can be helpful, some of them are signature based, meaning they rely on known identifiers of specific malware. If the malware is new and its signature has yet to be identified, it is unlikely the anti-virus would detect the malware.

10. Limit the Physical Access of a Host

Limiting the physical access of a host is a fundamental practice in computer security. It involves restricting direct interaction with the actual hardware, such as servers, desktops, or laptops. This prevents unauthorized tampering with the system, stealing sensitive data, or introducing malicious software. While it enhances protection, strict limitations on physical access can create inconvenience for legitimate users who may require direct access for tasks like maintenance, upgrades, or troubleshooting.

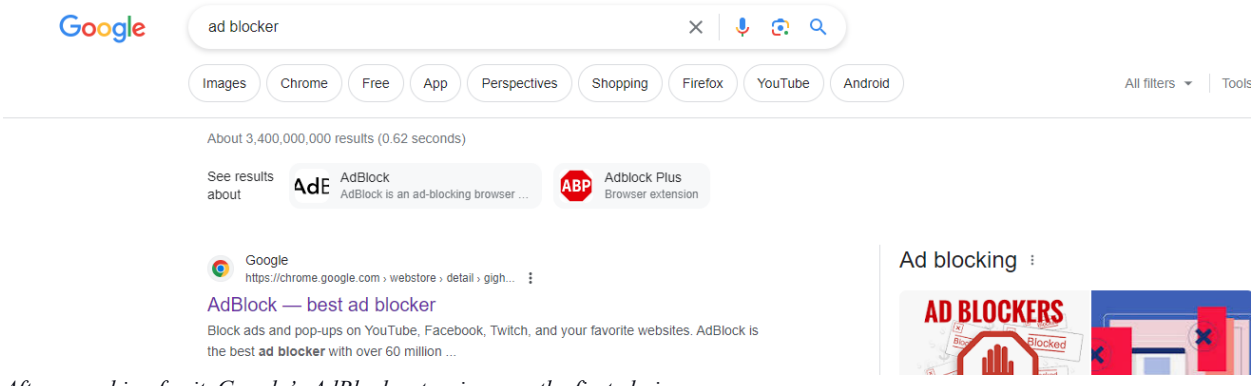
(Part B) Step *2: 10 Hardening Techniques*

1. Incorporating AdBlockers

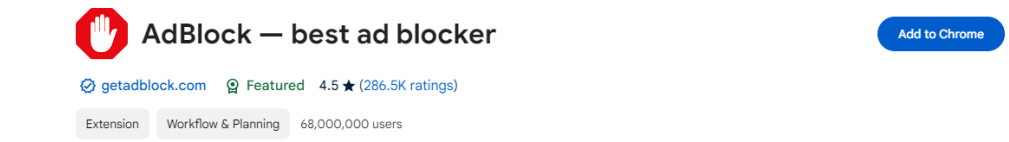
I will download Google's ad-blocker to help block pop-up ads and third-party tracking.

Step 1: *Google AdBlock*

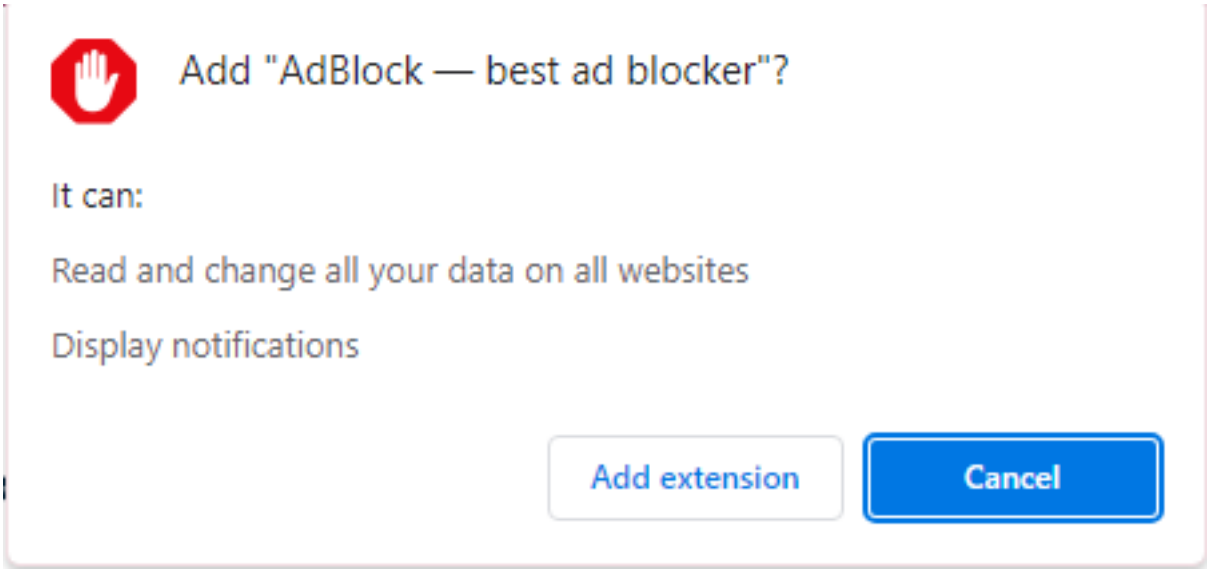
To begin, I searched up AdBlocker on Google, to look for the Chrome extension 'AdBlocker.'



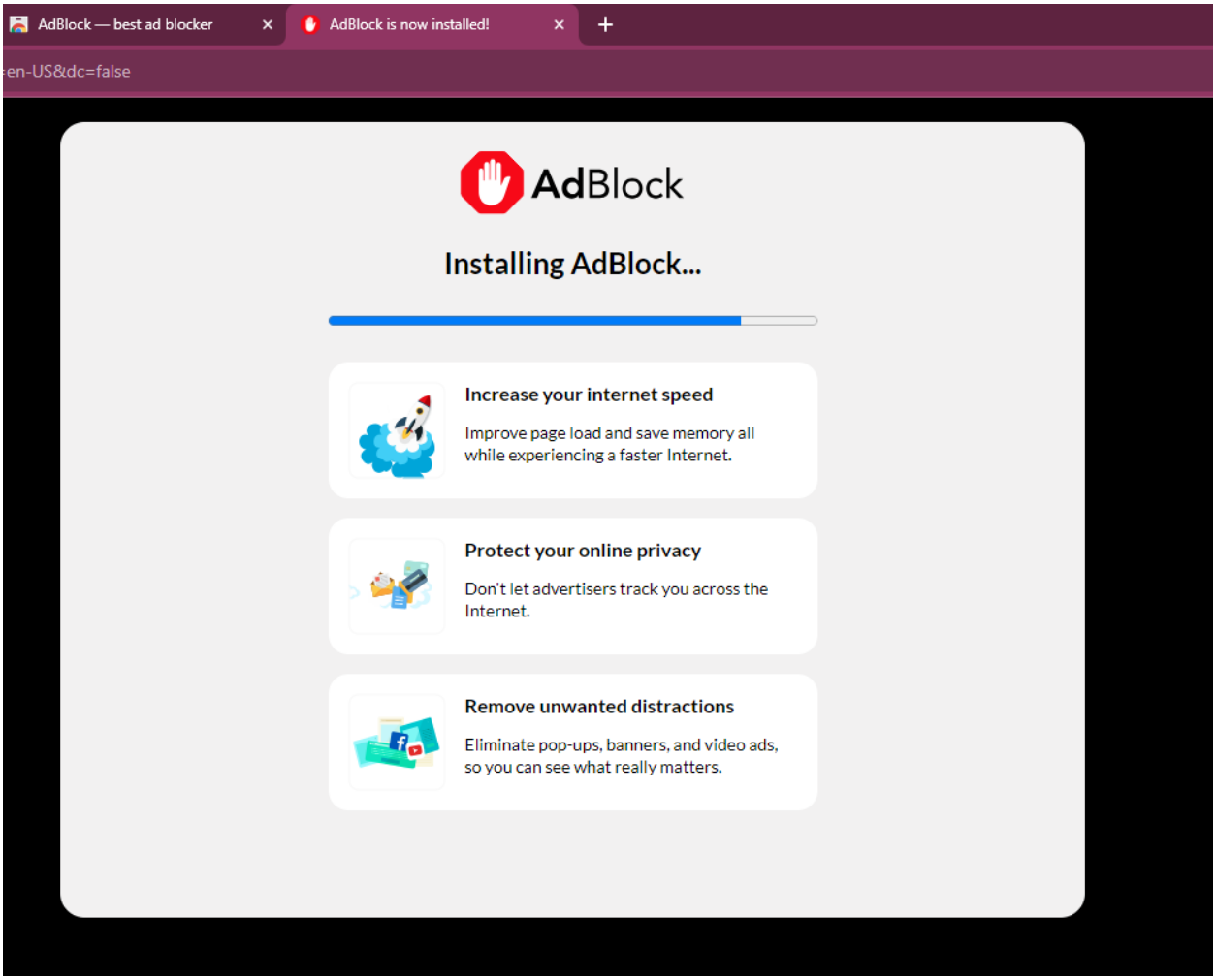
After searching for it, Google's AdBlock extension was the first choice.



Next, I entered the website and clicked 'Add to Chrome' to download the extension.

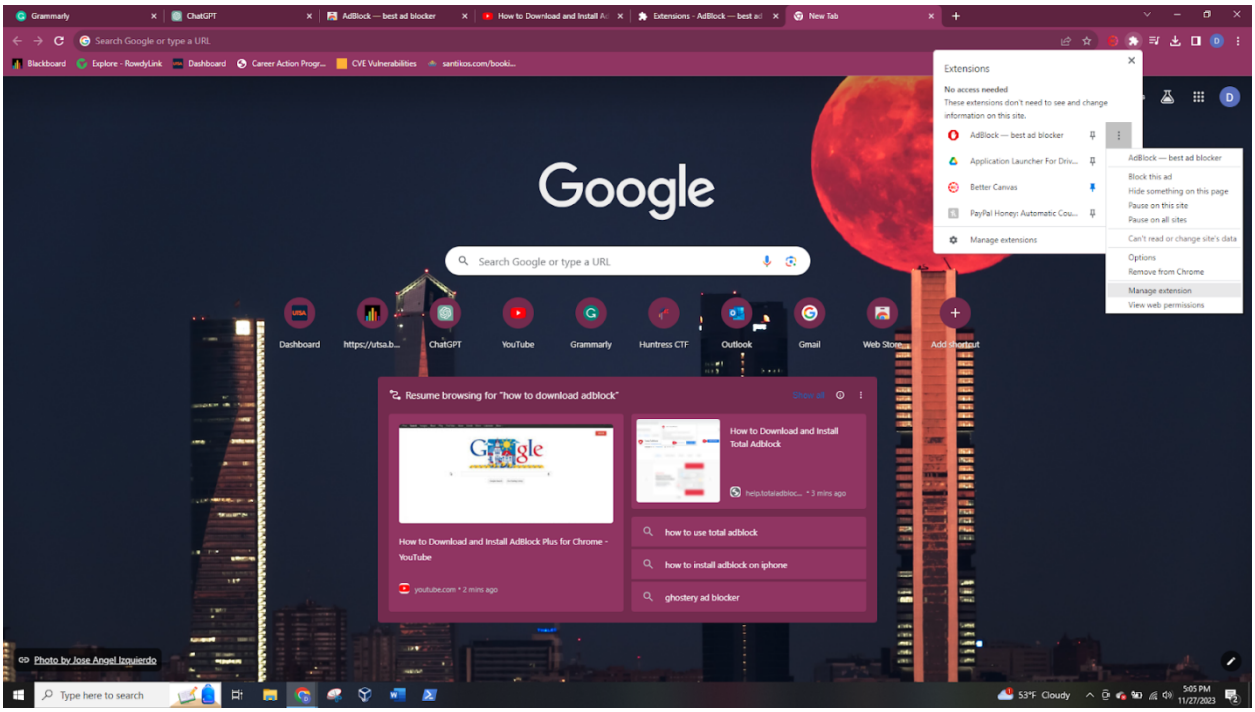


Next, I clicked "Add extension.'

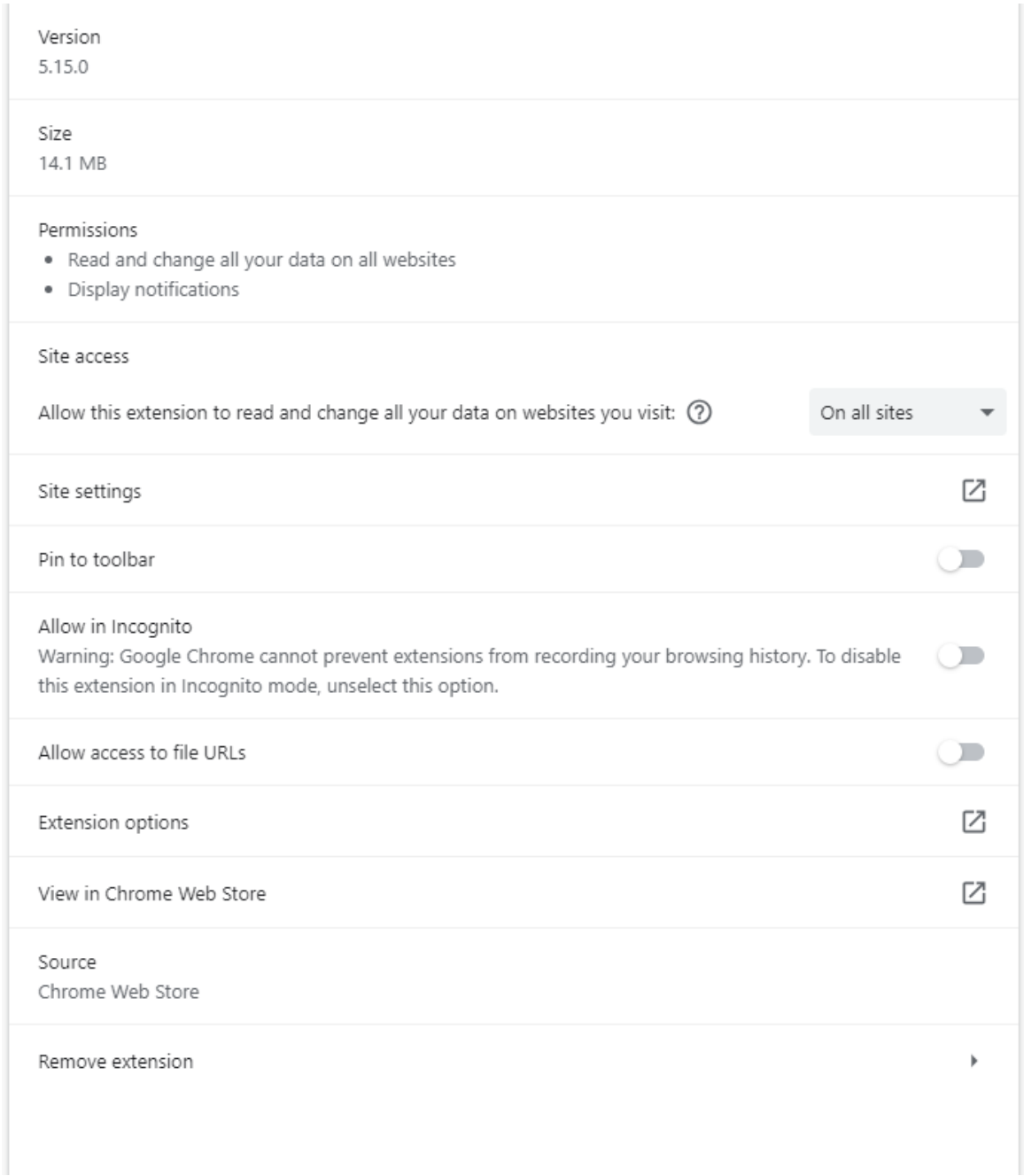


Next, the extension was downloading and when it fully downloaded, it took me a to a page which asked me to donate. Once it fully downloaded, I closed the donation page because the extension is free.

Now that the extension is fully downloaded, I wanted to analyze the settings.

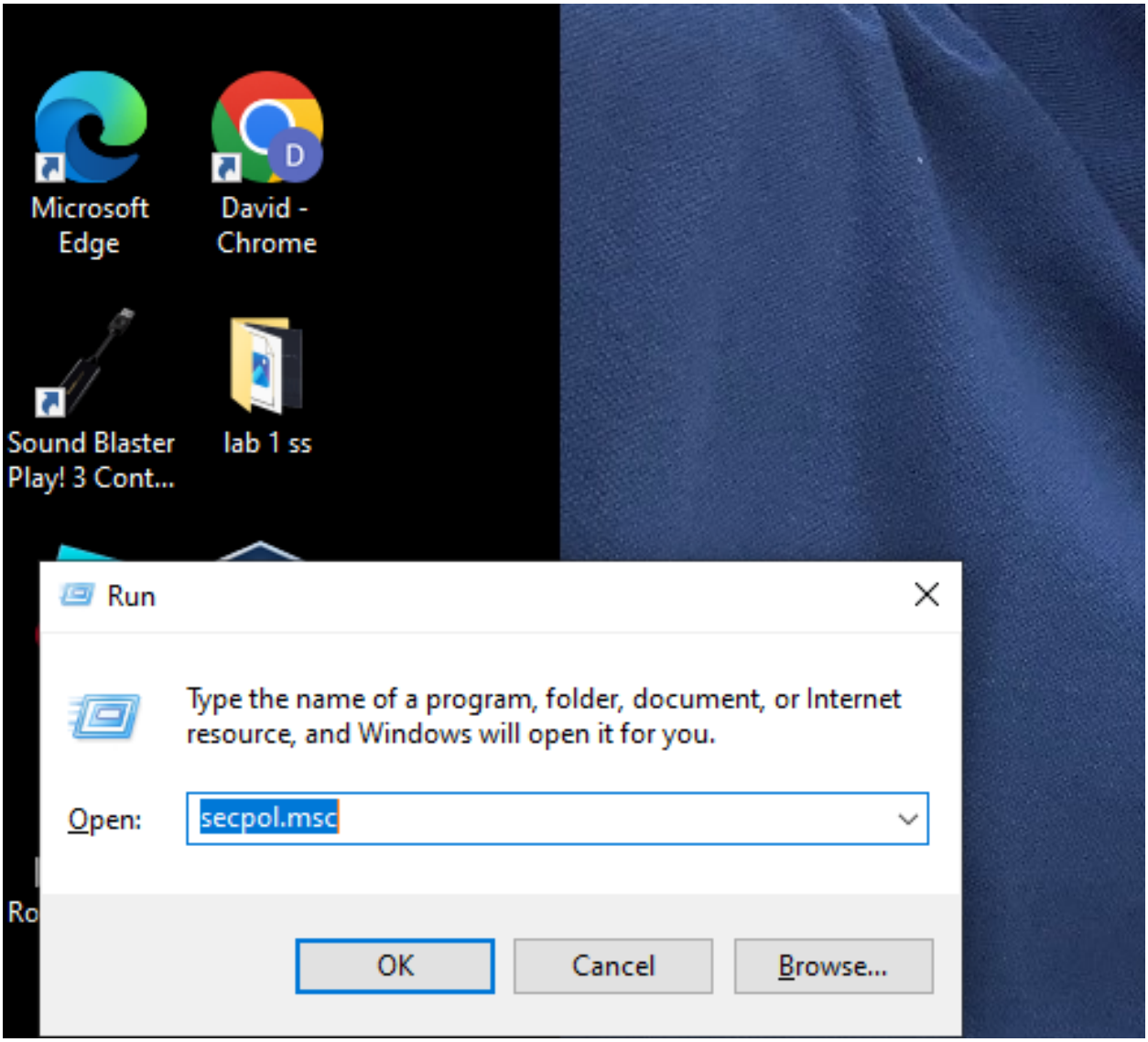


To analyze the settings, you click on the 'puzzle' icon and then the 3 dots besides 'Ad Block.' Next, you click on 'Manage Extension.'

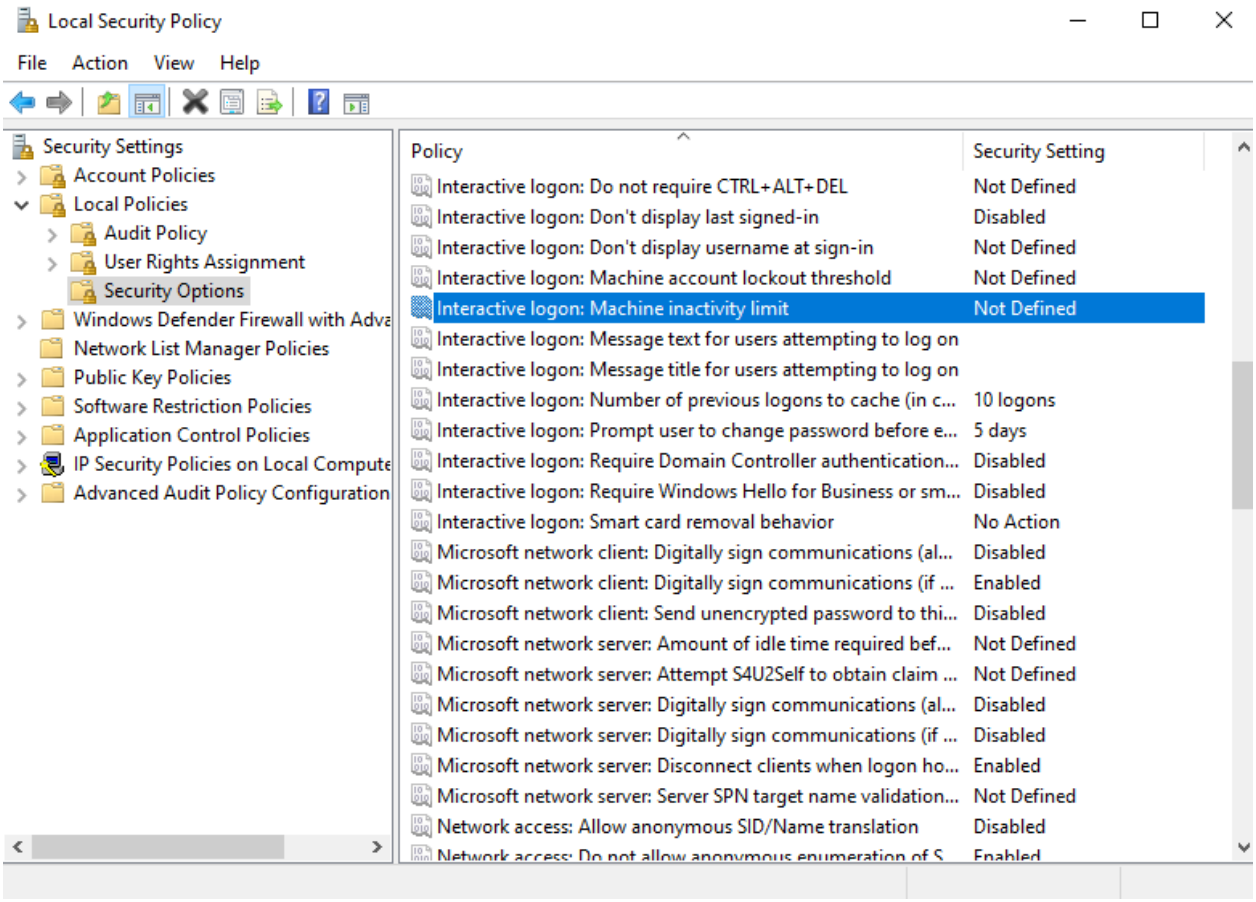


In the settings you could choose whether you want the AdBlocker to work on all sites, specific sites, or whether you want it to continue working on Incognito mode.

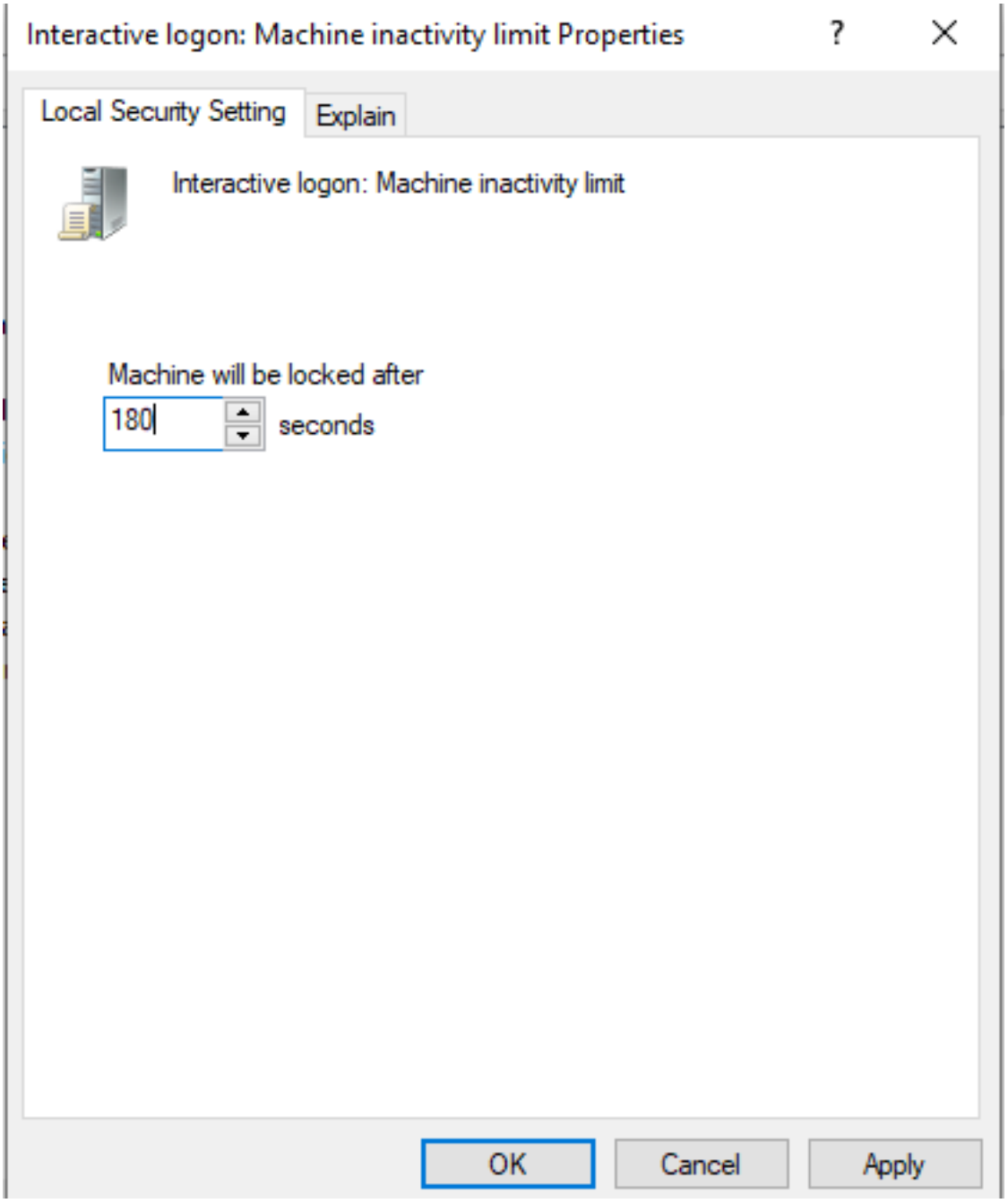
2. Forcing logoff when inactivity/logon hours expire



First I used the window key + r shortcut to bring up the run line. Once the run line comes up, I entered 'secpol.msc' to bring the security policies for my local machine.



Next, I expanded the 'Local Policies' and clicked 'Security Options' and I looked for 'Interactive logon: Machine inactivity limit.'

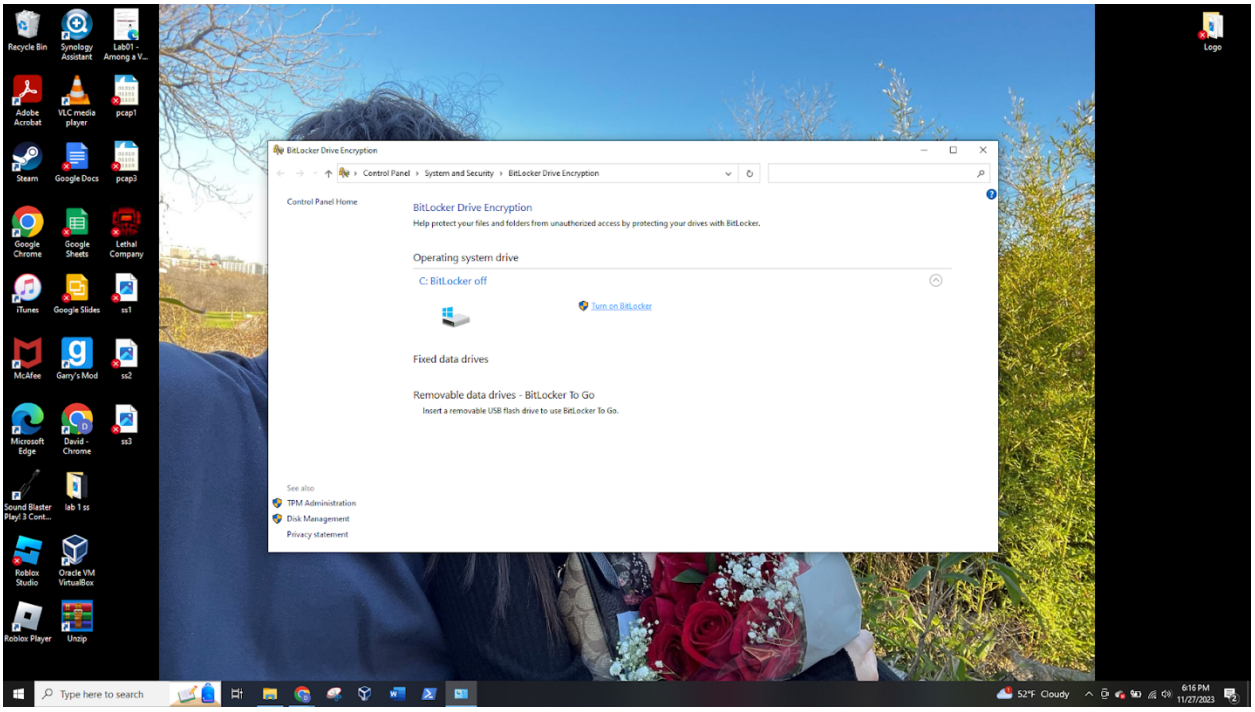


Next, I set the machine to lock after 180 seconds in order to ensure the machine is locked after being inactive for 3 minutes.

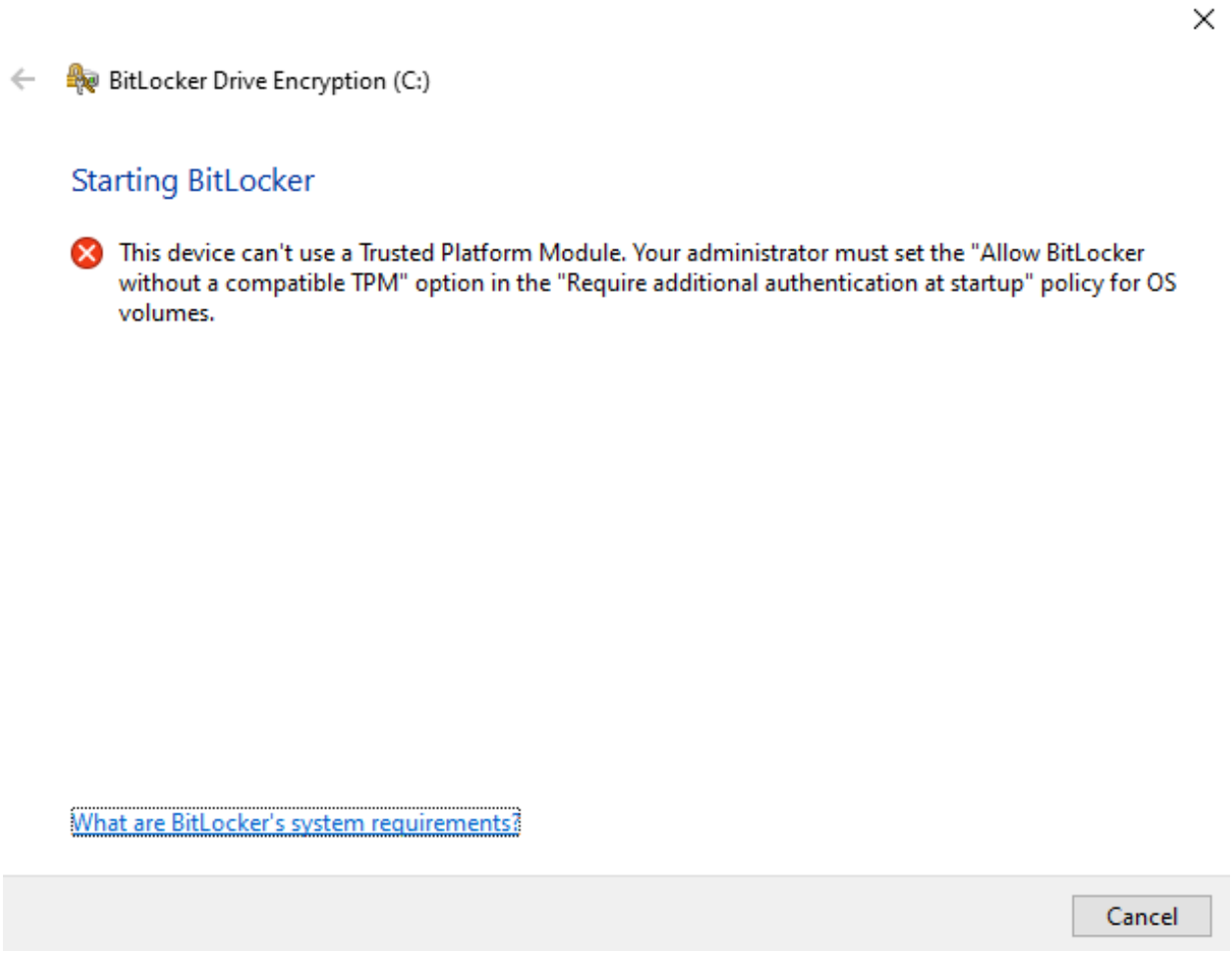
Next, I clicked and apply in order to apply the security changes.

3. Enabling Hard Drive Encryption (BitLocker)

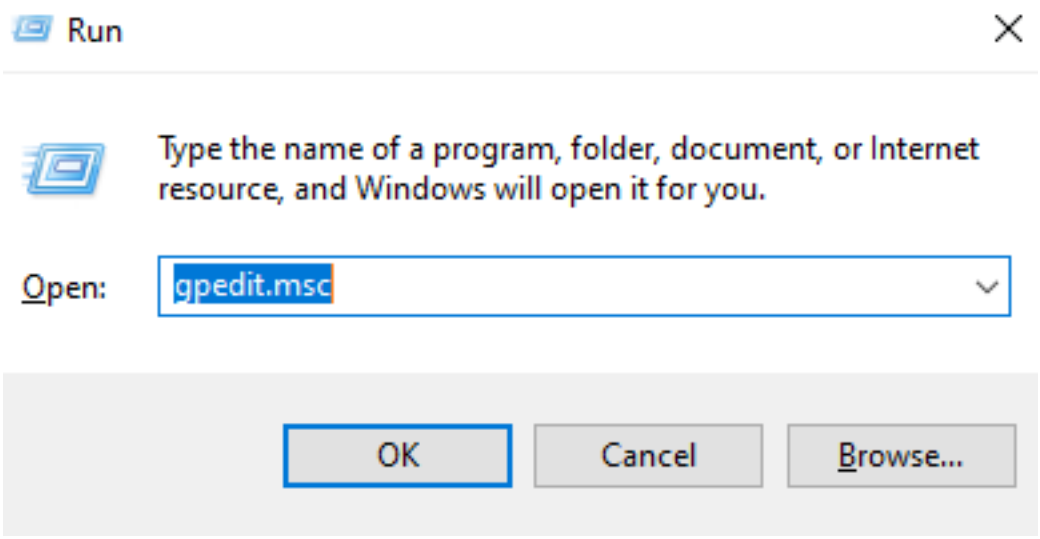
First, I searched for BitLocker on the Windows search bar and I clicked on "Manage BitLocker."



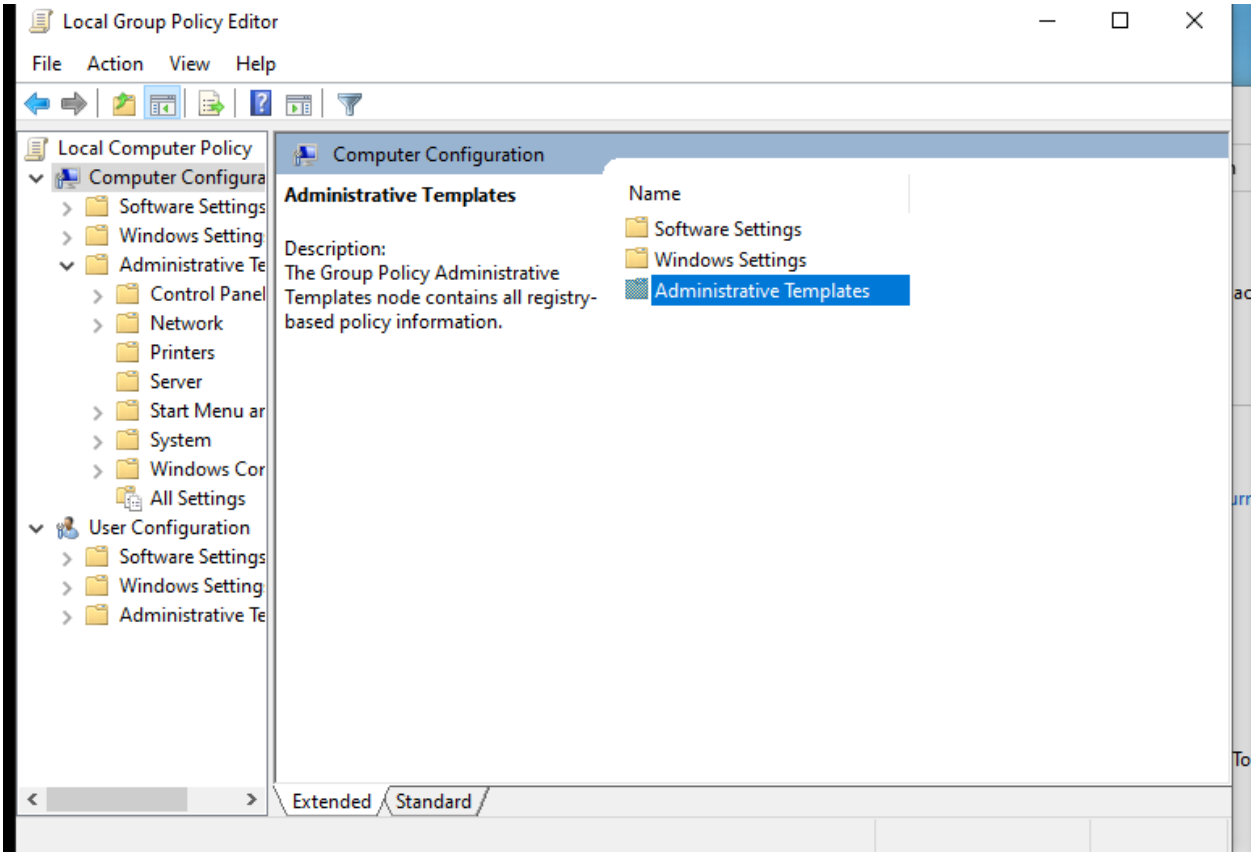
Next, I clicked on the shield that says "Turn on BitLocker."



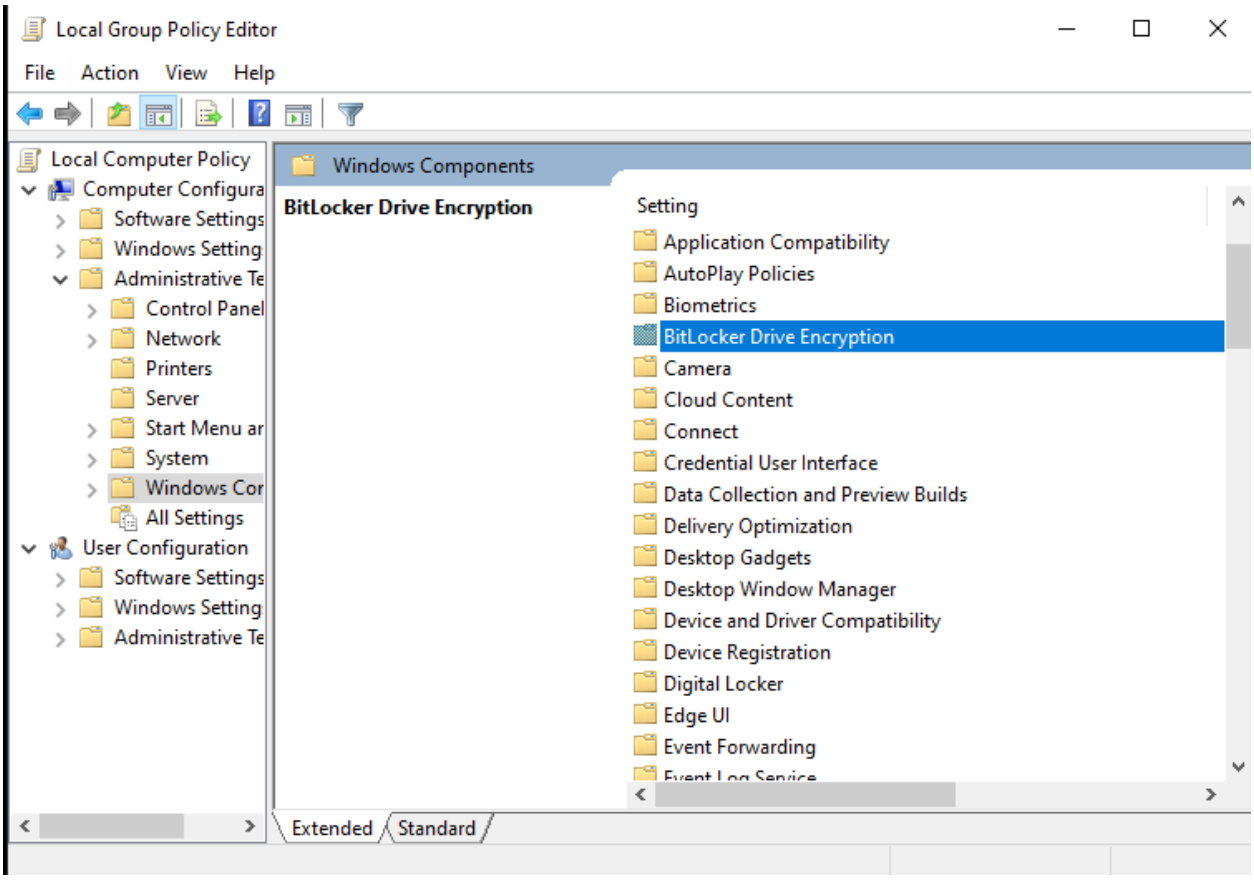
Next, I got this error which stated that I need to have the administrative account enable BitLocker without a compatible TPM option.



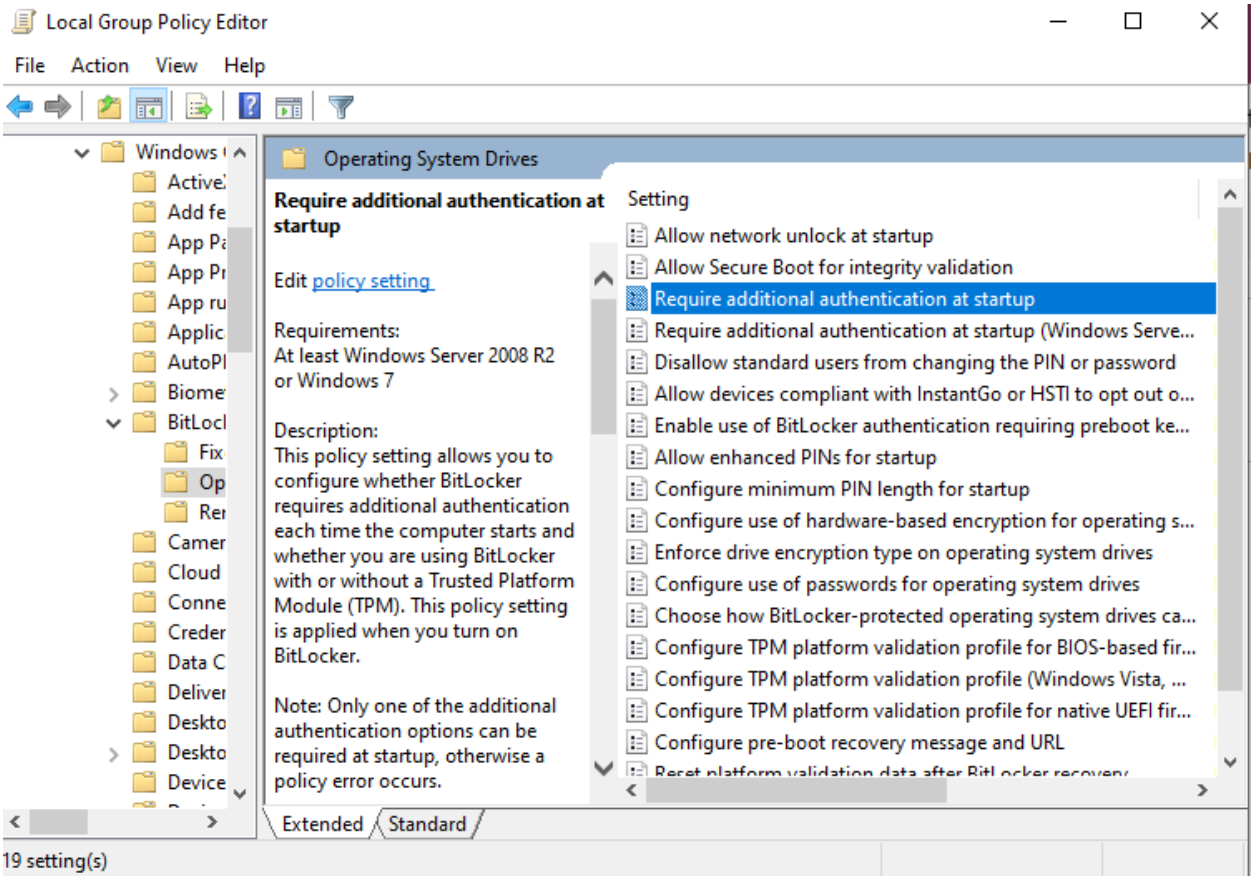
To fix this error, I opened the run line and searched 'gpedit.msc' to open the Local Group Policy Editor.



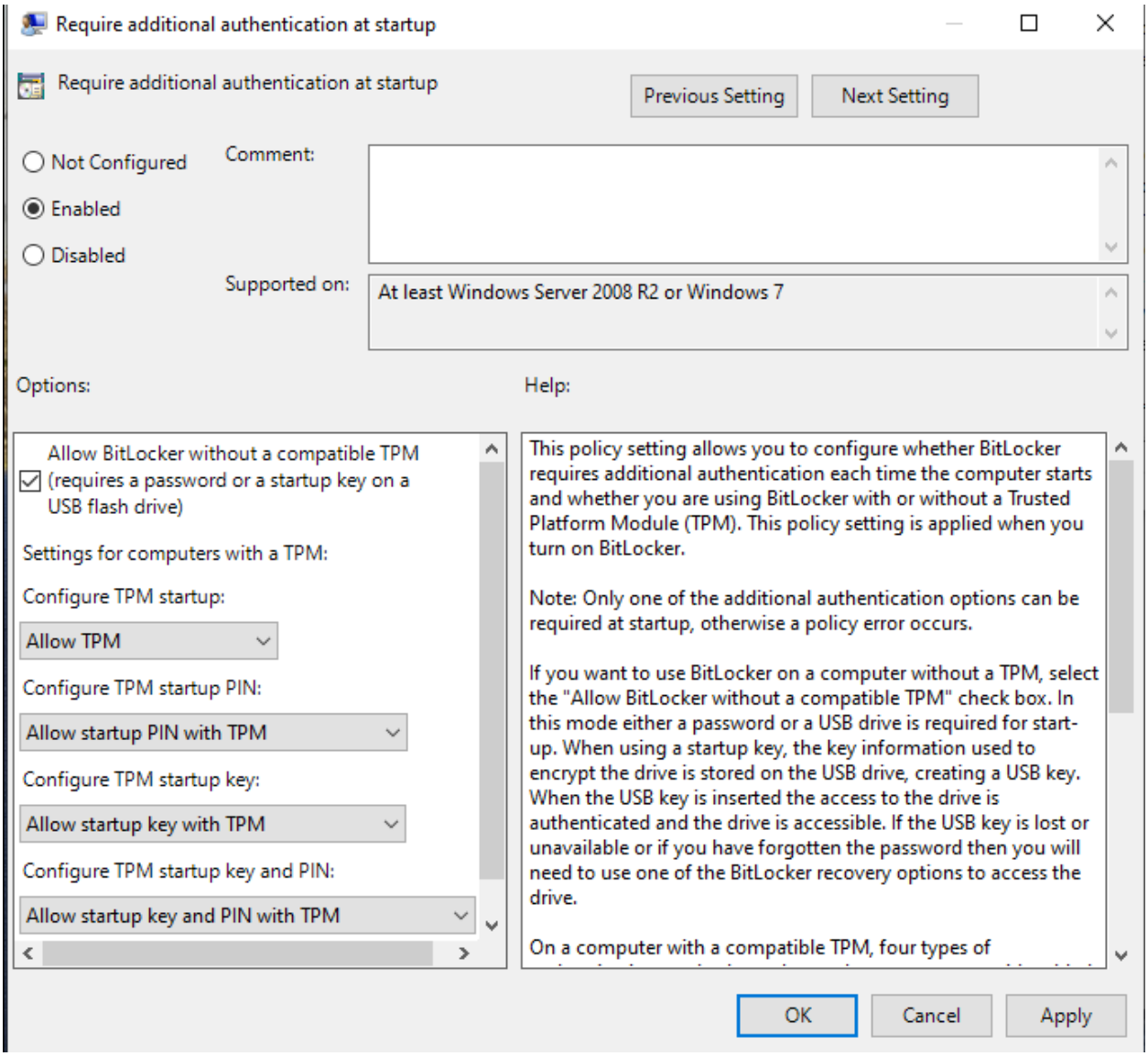
Next, I clicked on "Computer Configuration" and "Administrative Templates."



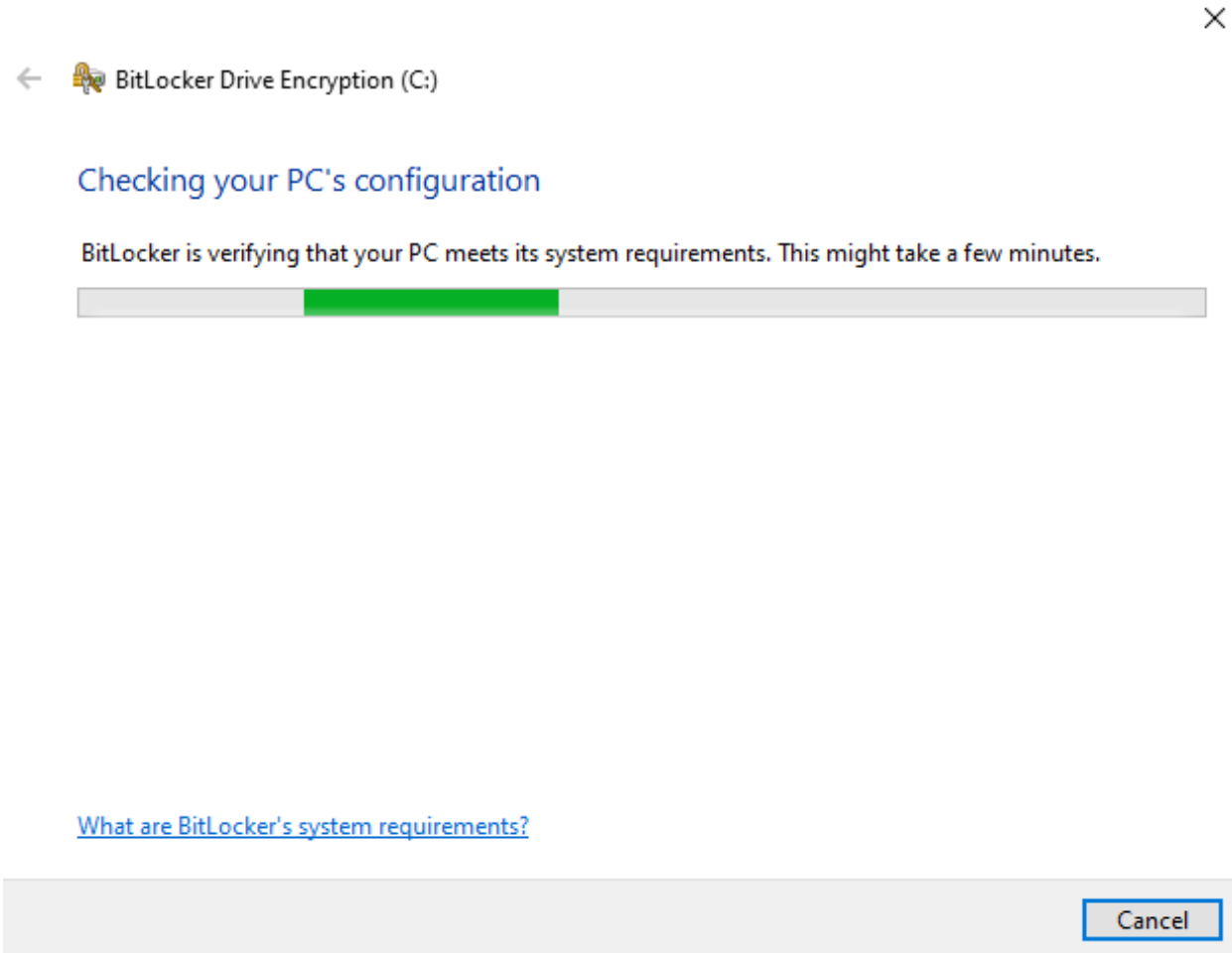
Next, I clicked on Windows Components and BitLocker Drive Encryption.



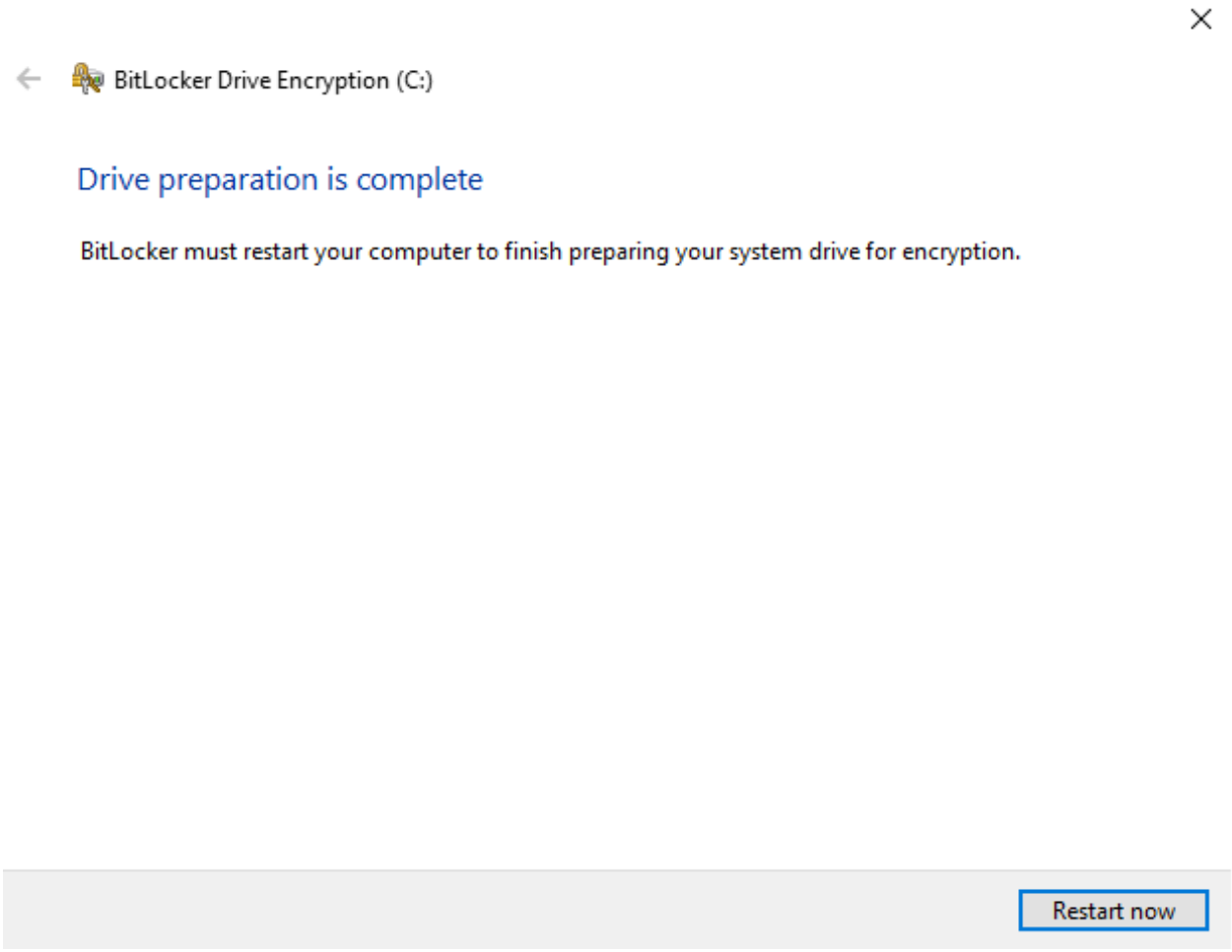
Next, I clicked on "Operating System Drives" and then I clicked on "Require additional authentication at startup."



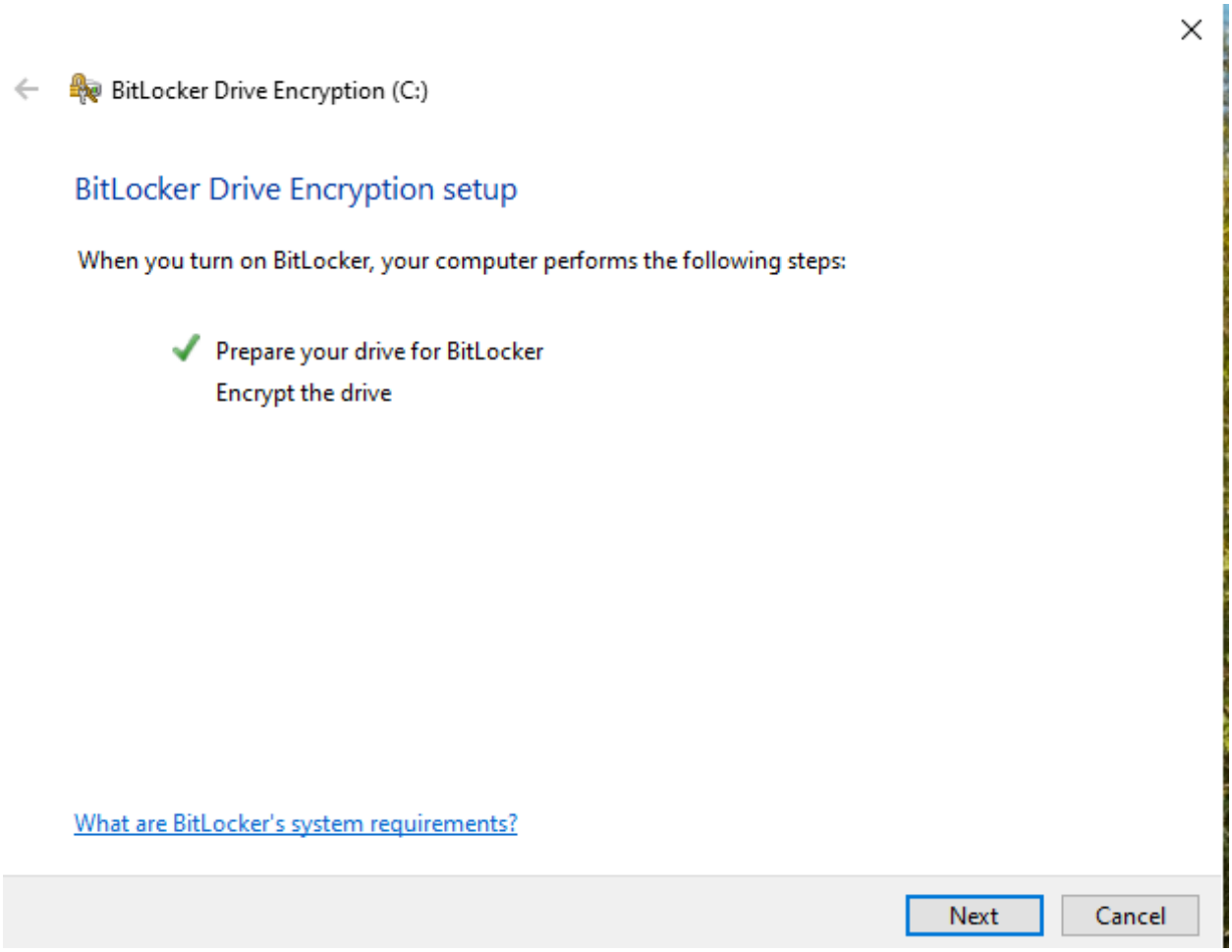
Once on "Require additional authentication at startup," I clicked 'enable' and then applied my changes.



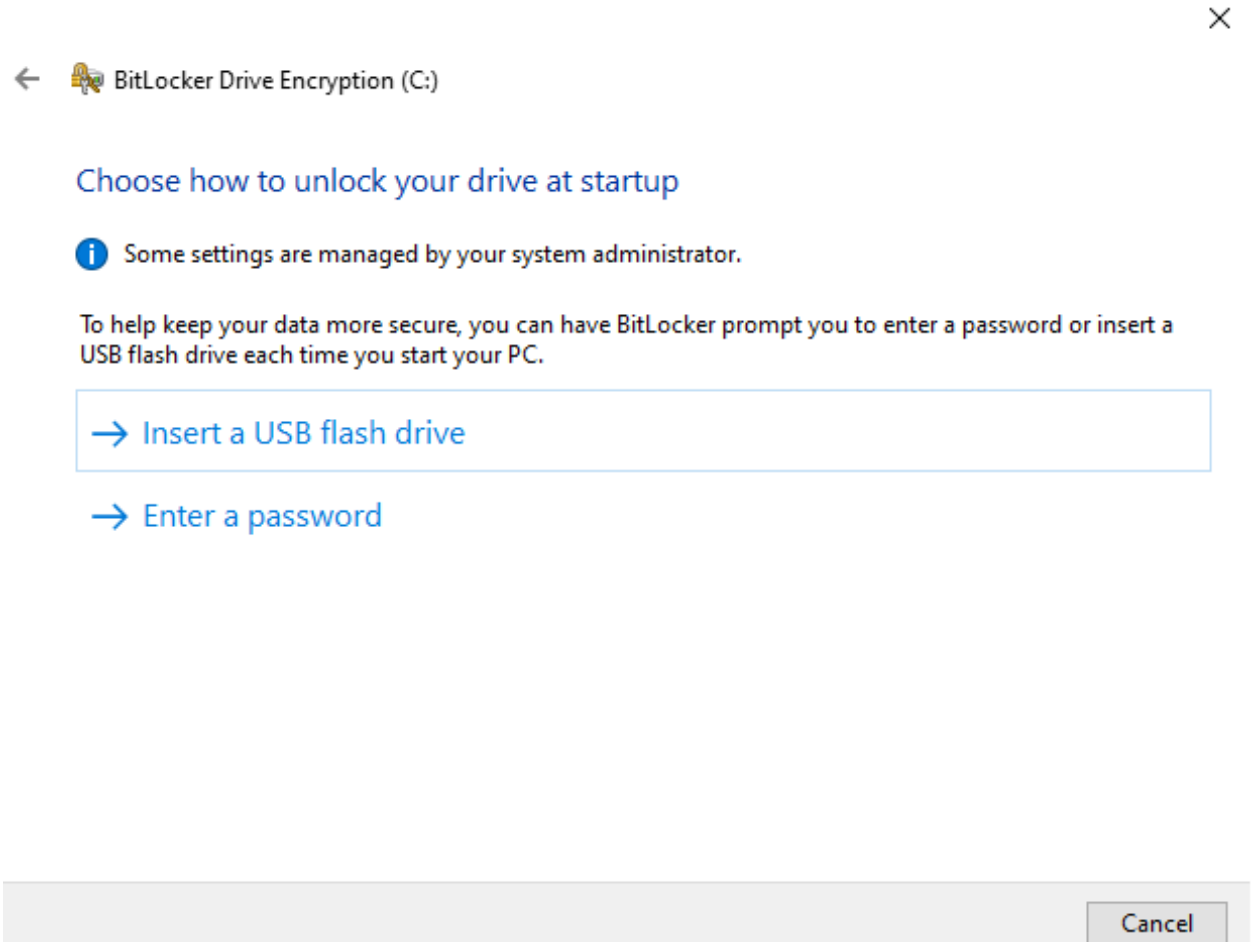
Next, I went back to turn on "BitLocker" by clicking on the shield icon.



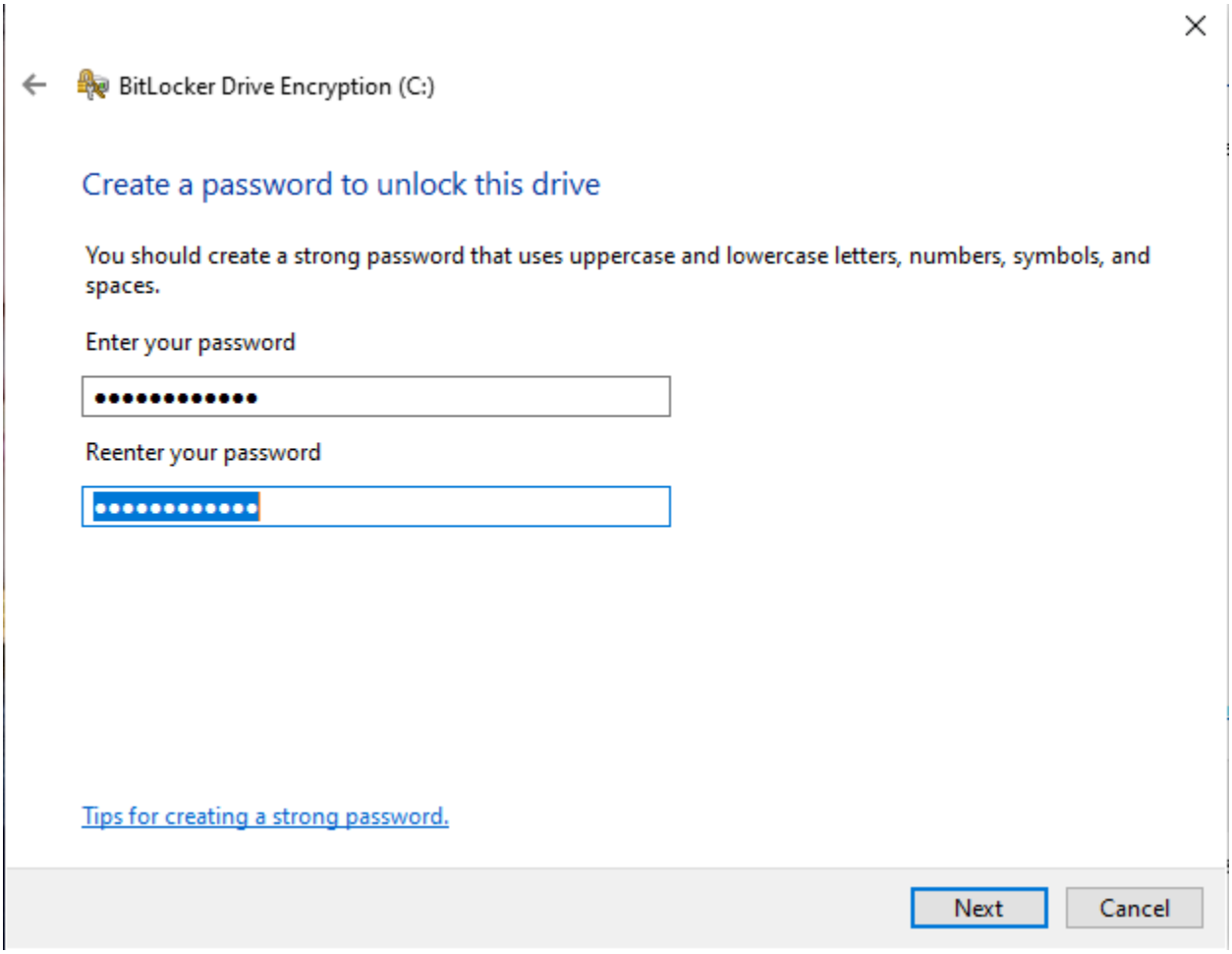
Next, BitLocker asked me to restart my device.



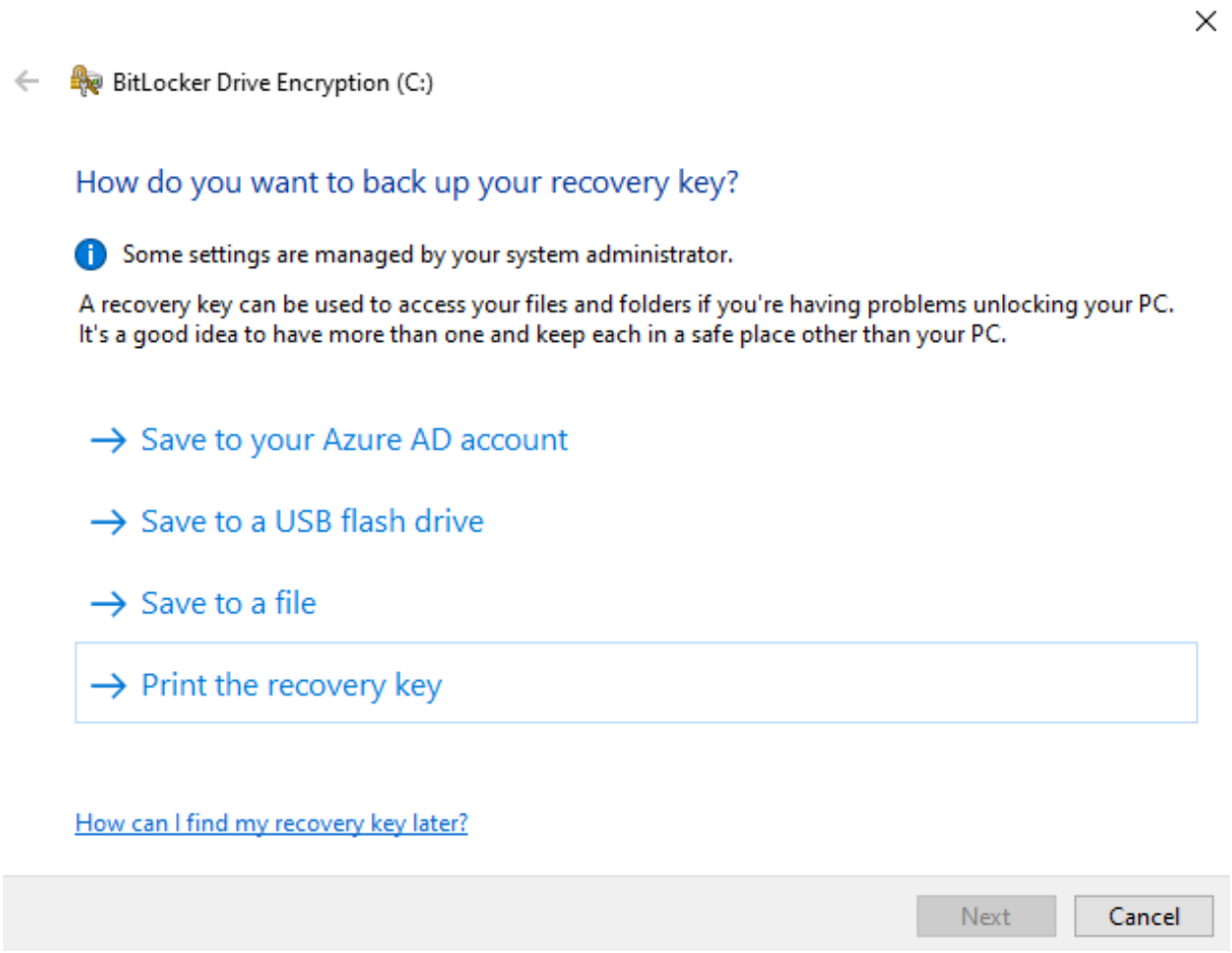
Once I restarted my computer, this screen popped up and I clicked next to encrypt the drive.



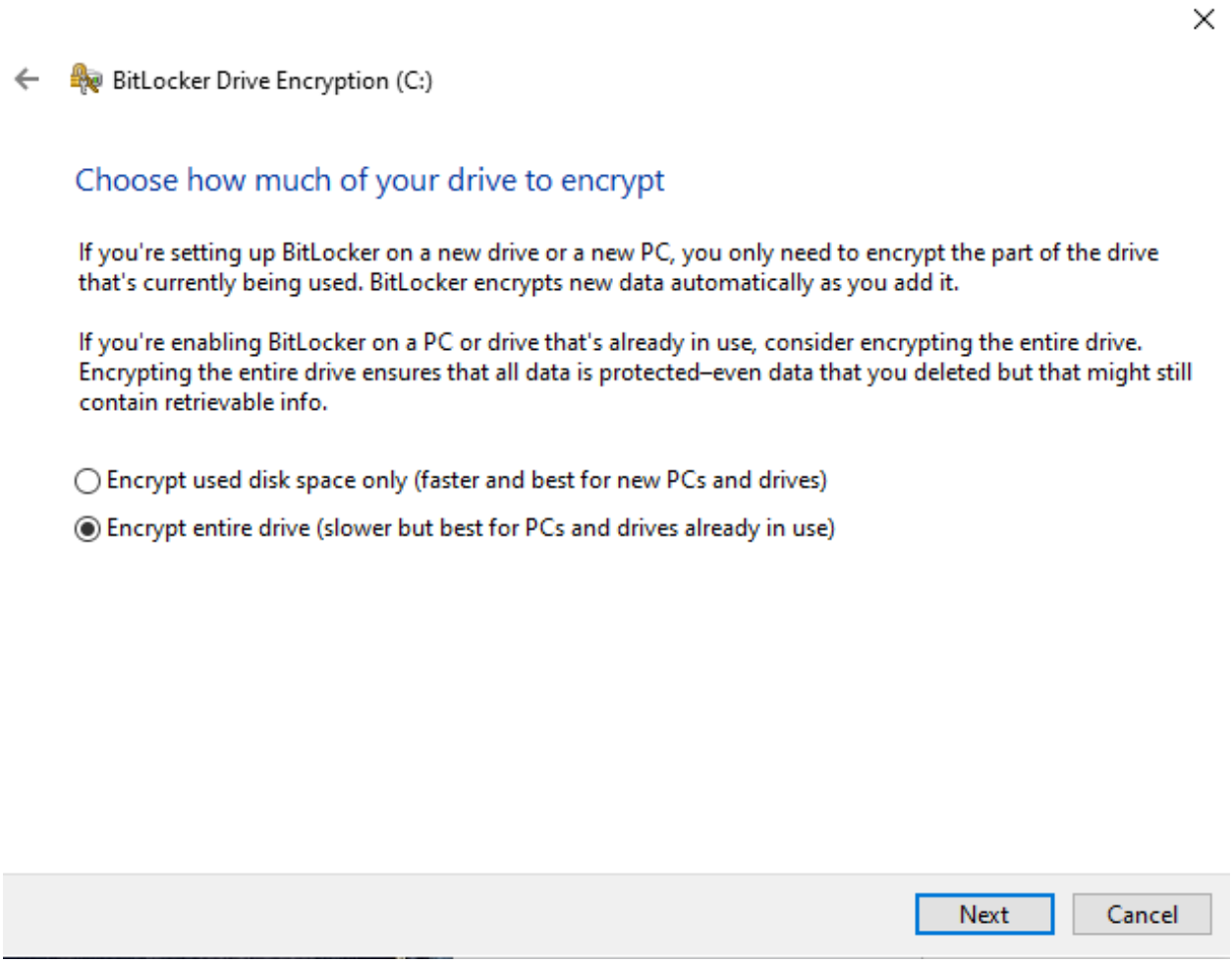
I chose to encrypt the drive with a password.



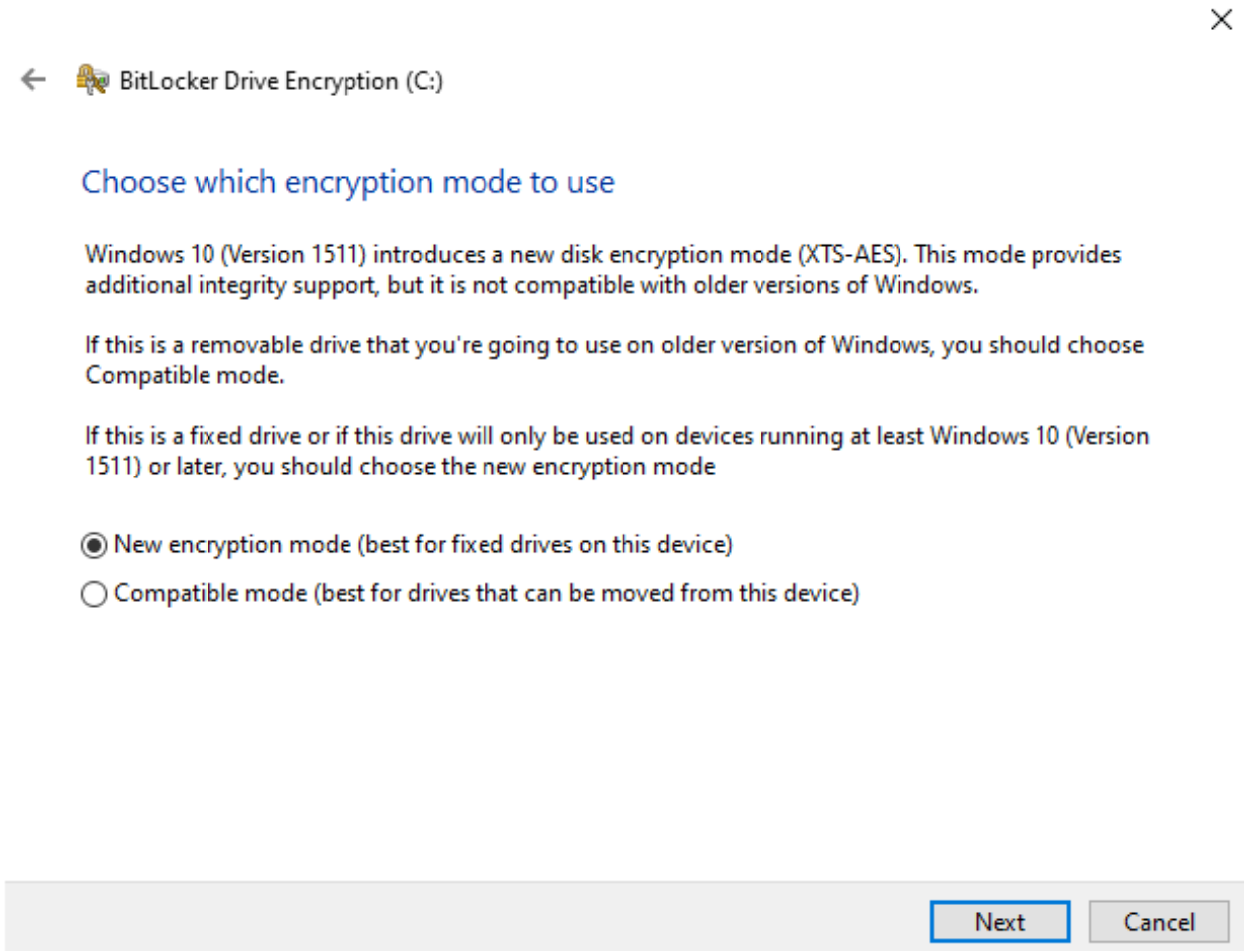
I chose a safe password that used a combination of capital letters and numbers and special characters.



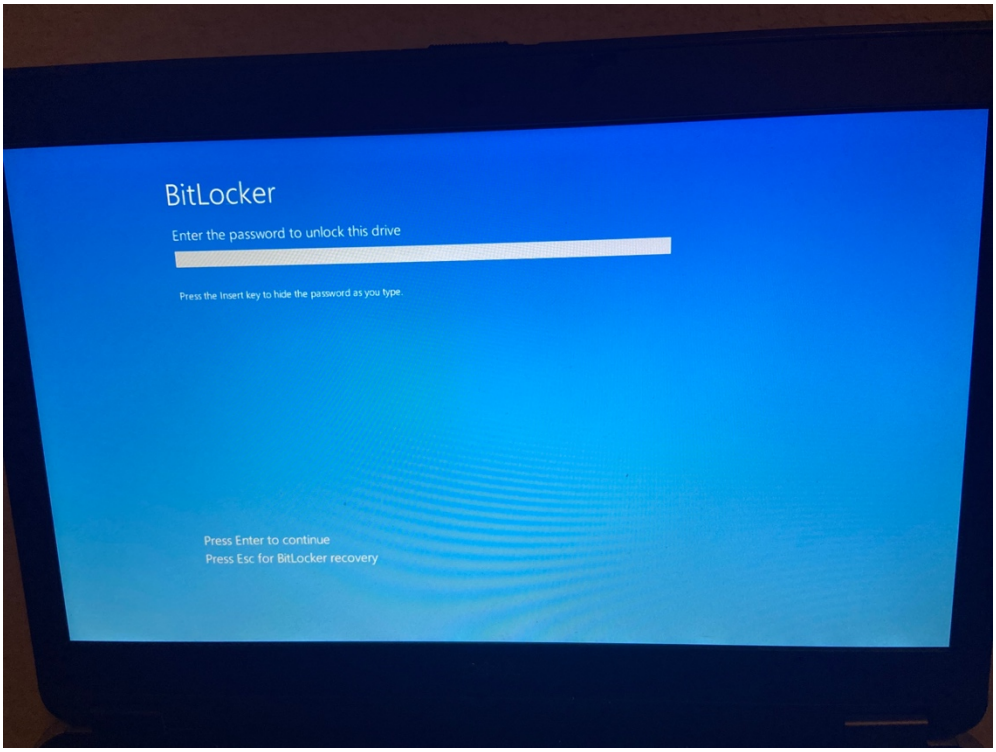
Next, I chose to print recovery key so I could keep a copy saved in my lockbox in case I forget the password.



Next, I chose to encrypt the entire drive because this PC is already in use.

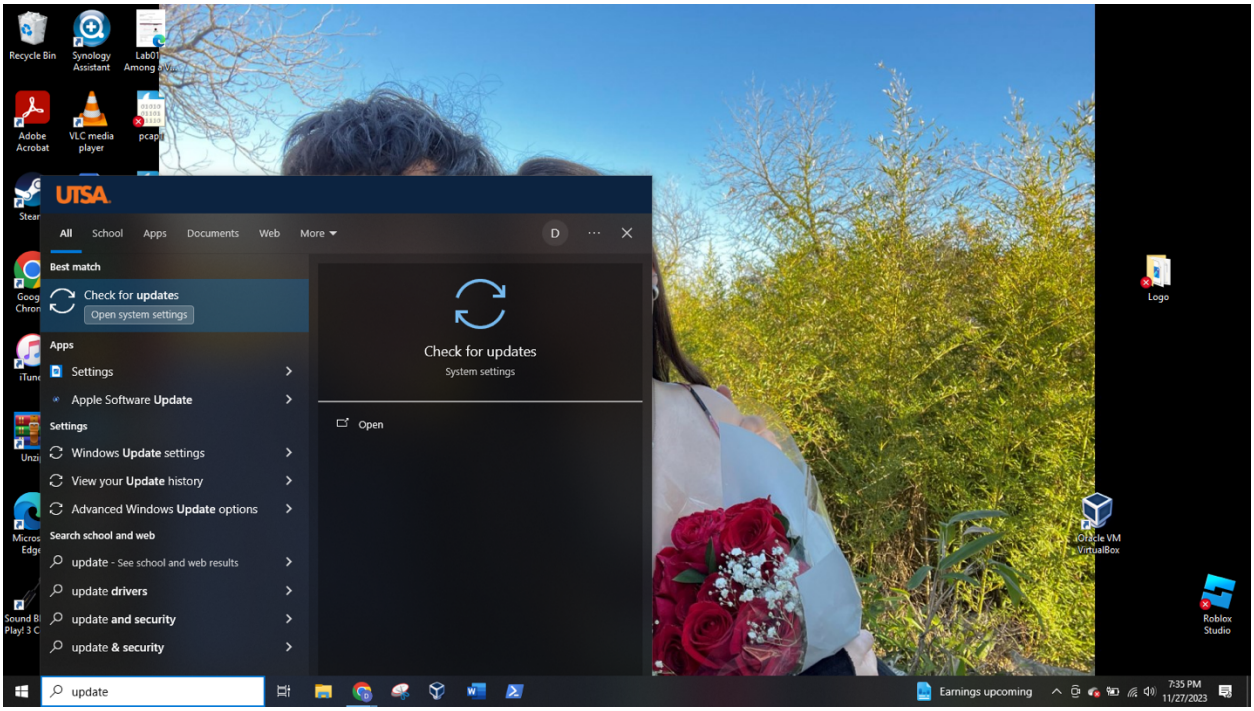


Next, I used the 'New encryption mode' because my drive is fixed to my device.

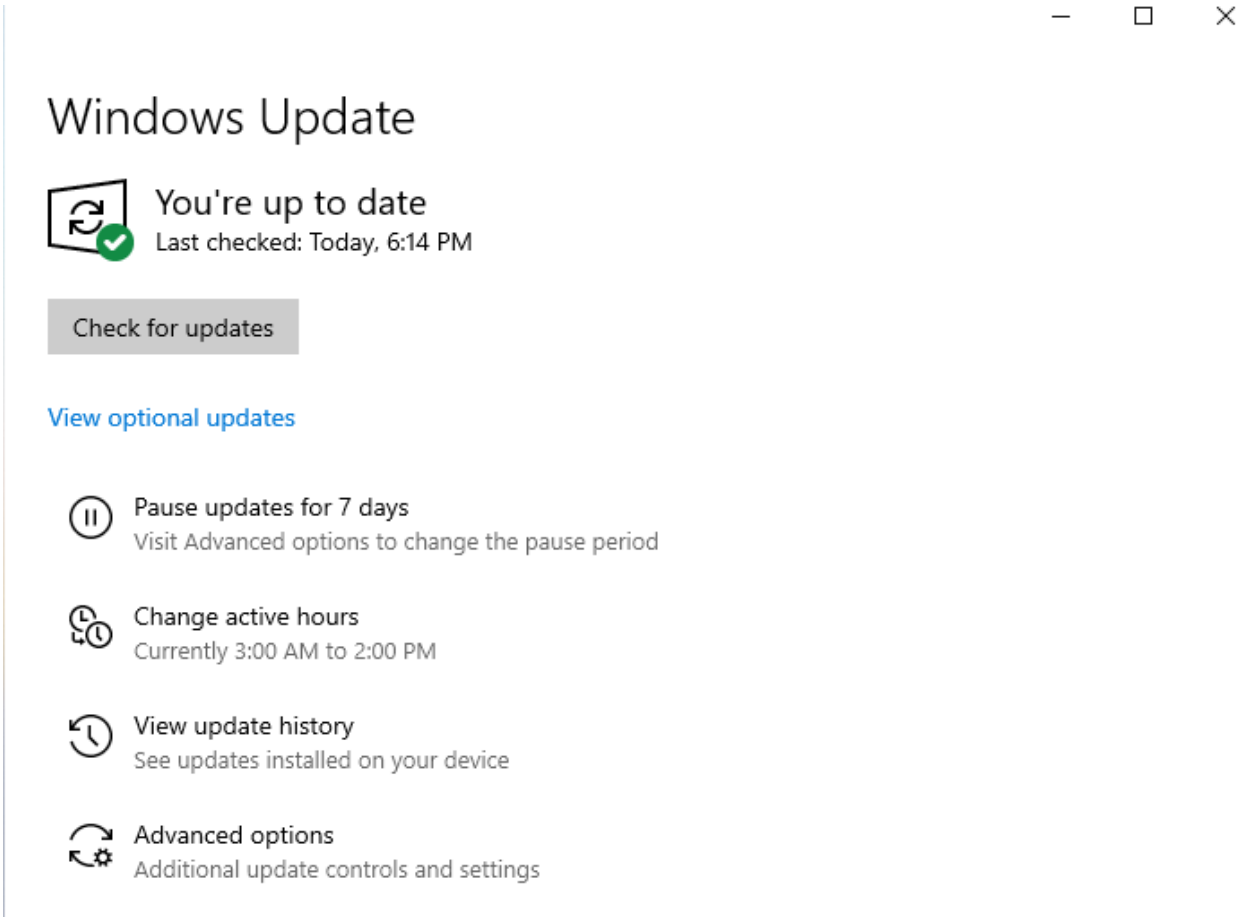


Finally, I restarted my computer to finalize the set-up of BitLocker. Once the device rebooted, I was able to verify that BitLocker was turned on as I was prompted to enter the BitLocker password to access the hard drive.

4. Updating and patching the operating system



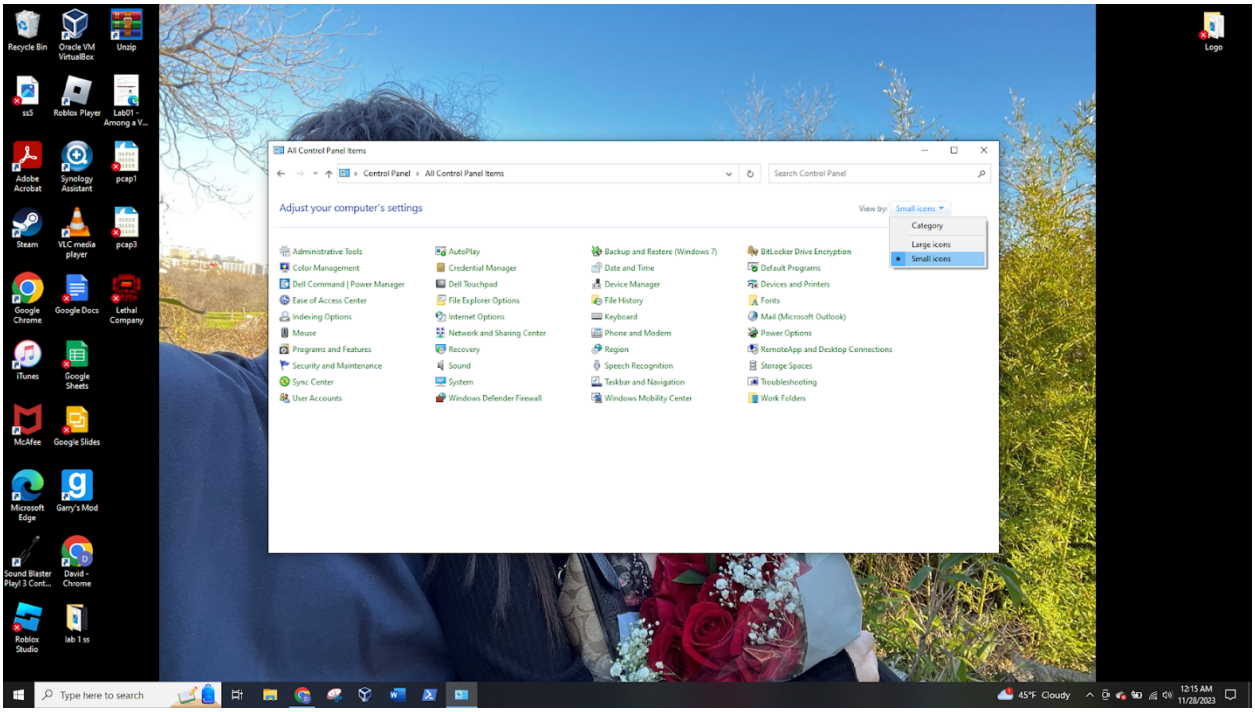
To update the OS, search 'update' on the Windows search bar and select 'Check for updates.'



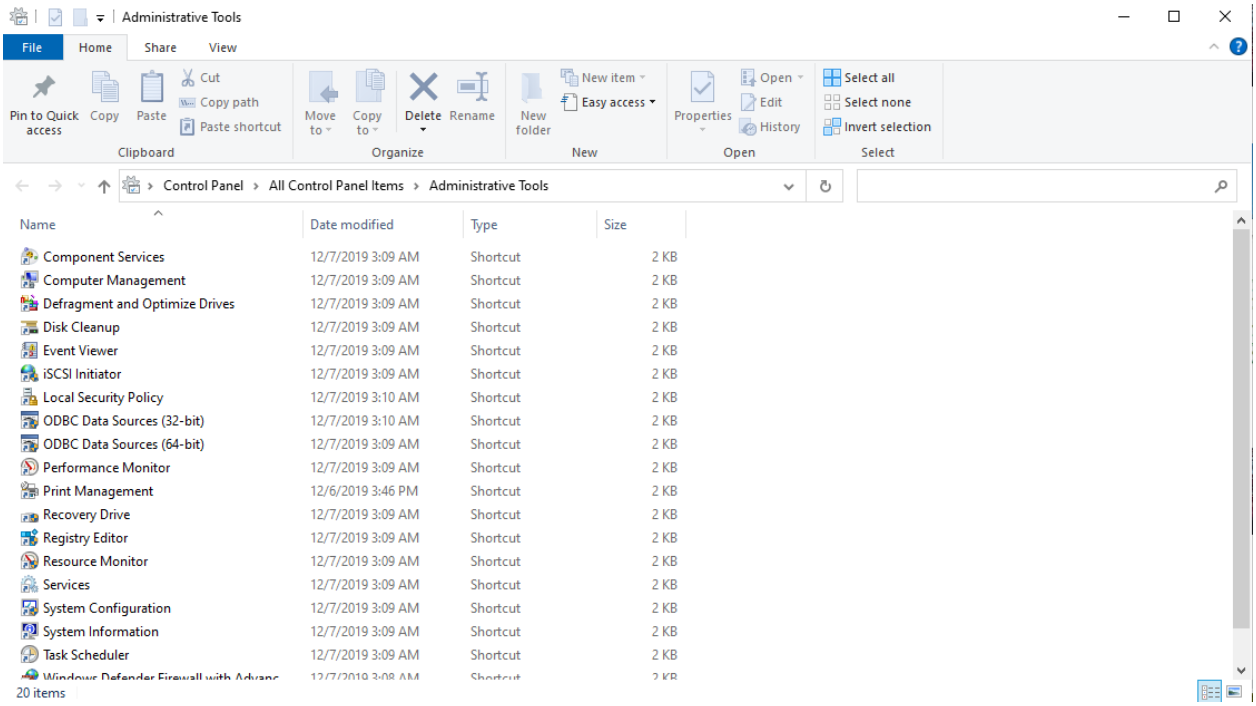
Once here, you can view if an update is available or if your device is up to date. You could also select 'View optional updates' if you'd like. My device is already up to date to there are no more patches or updates I could download.

5. Turning off Secondary Logon Services

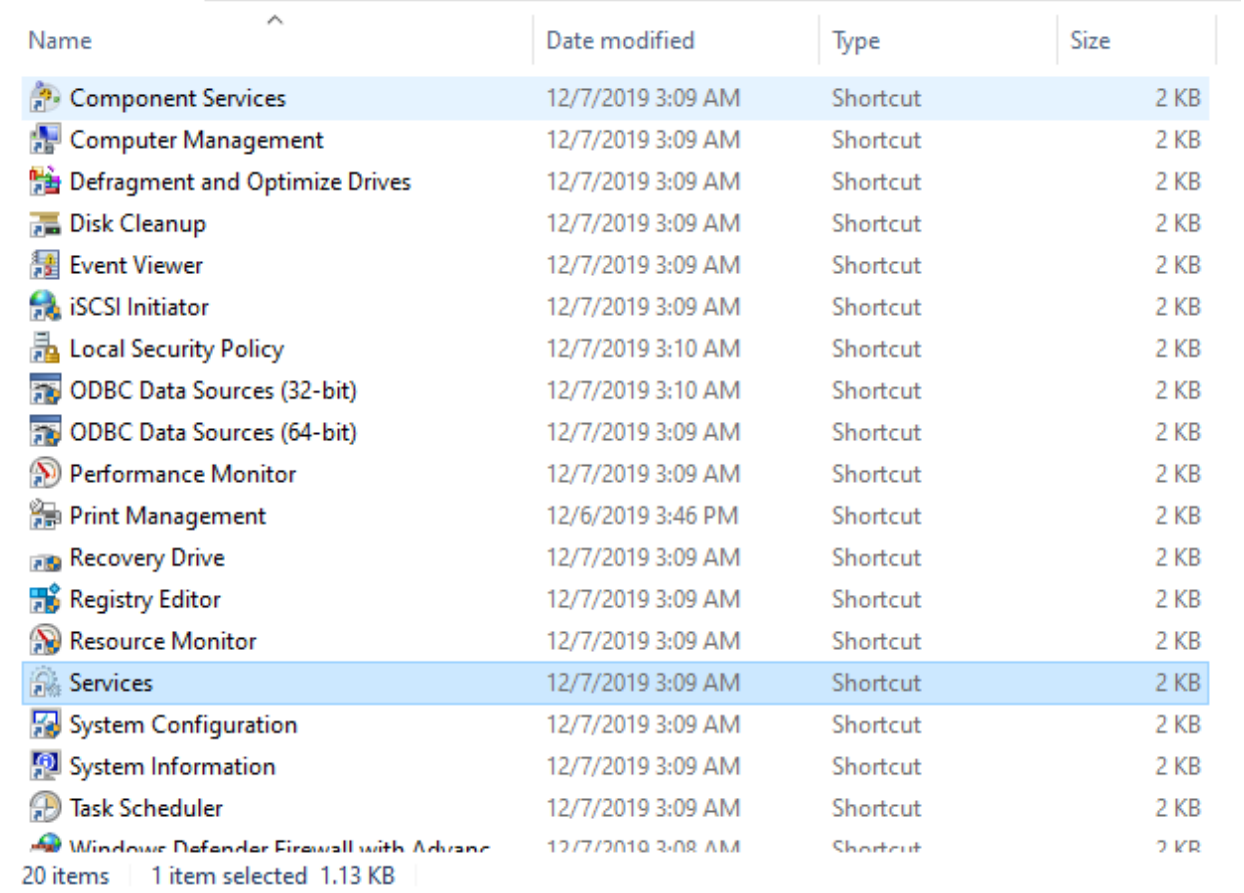
To begin, I searched for and opened the 'Control Panel.'



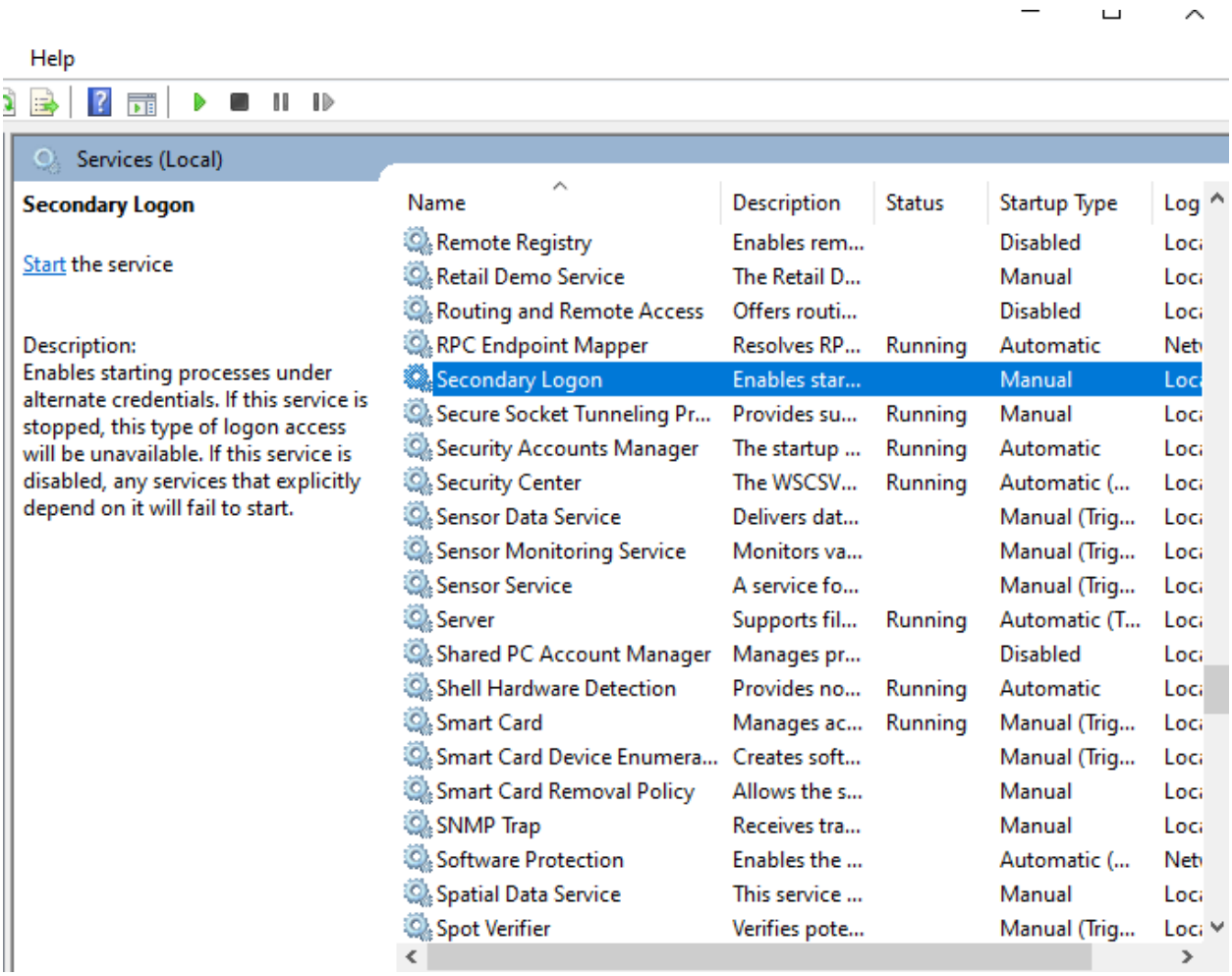
Next, I filtered the panel by 'small icons.'



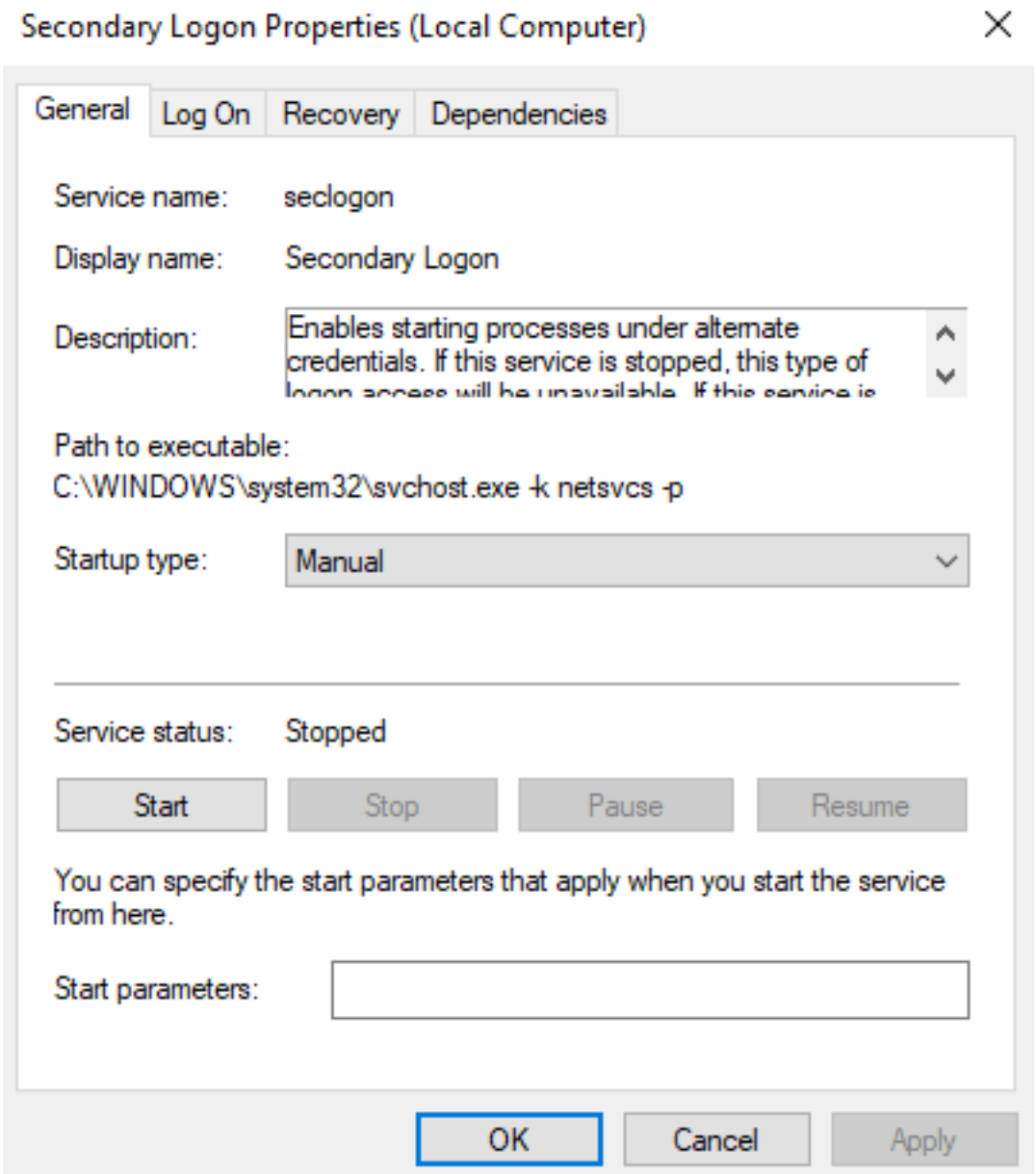
Next, I selected 'administrative tools.'



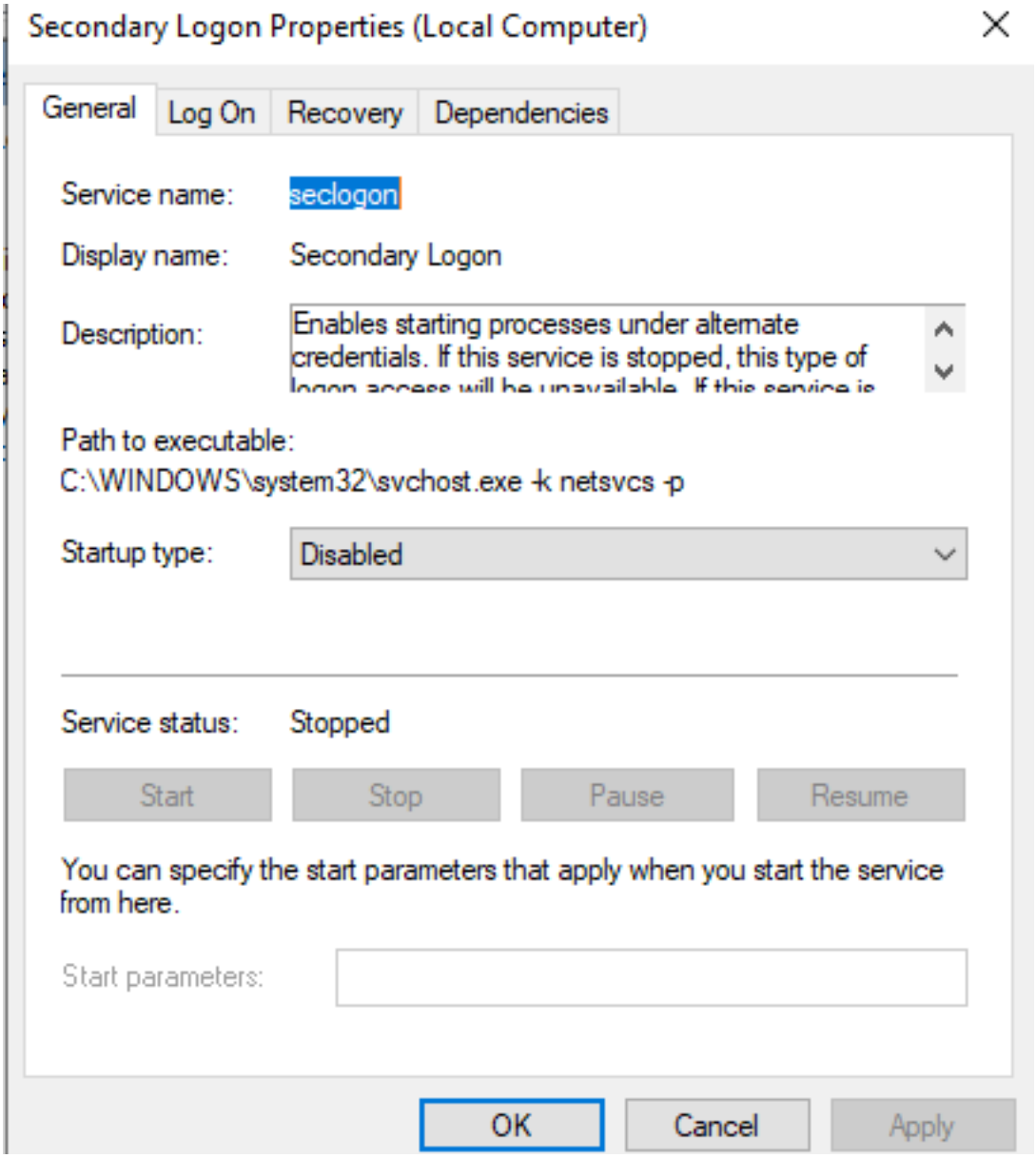
I then selected services.



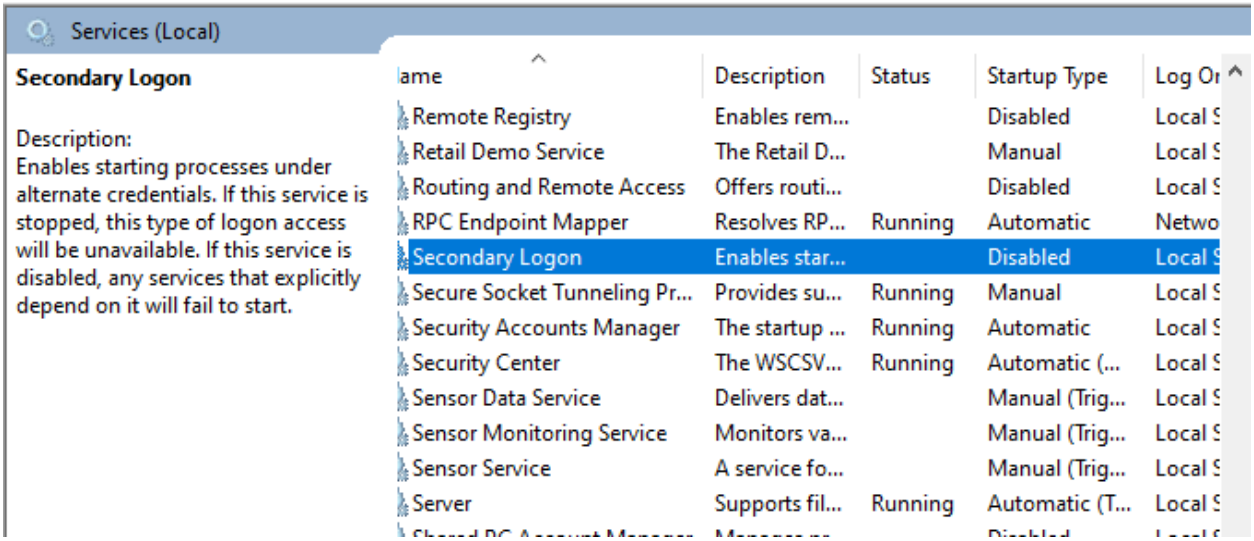
Next, I looked for "Secondary Logon."



Next, I right clicked on "Secondary Logon" and selected "Properties." After, I selected where it says "Manual" next to "Startup type" and I changed it to disabled.



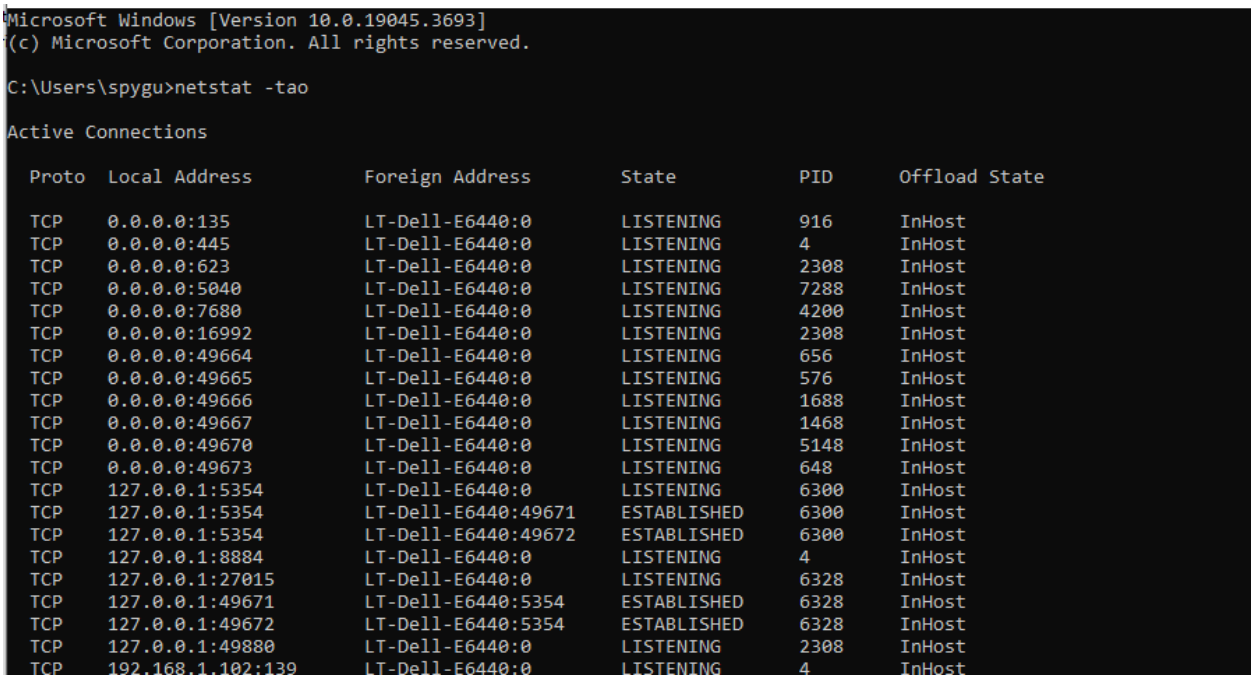
Once Secondary Logon was disabled, I clicked apply and then OK.



After selecting apply, you could see under "Startup Type" that "Secondary Logon" was successfully disabled.

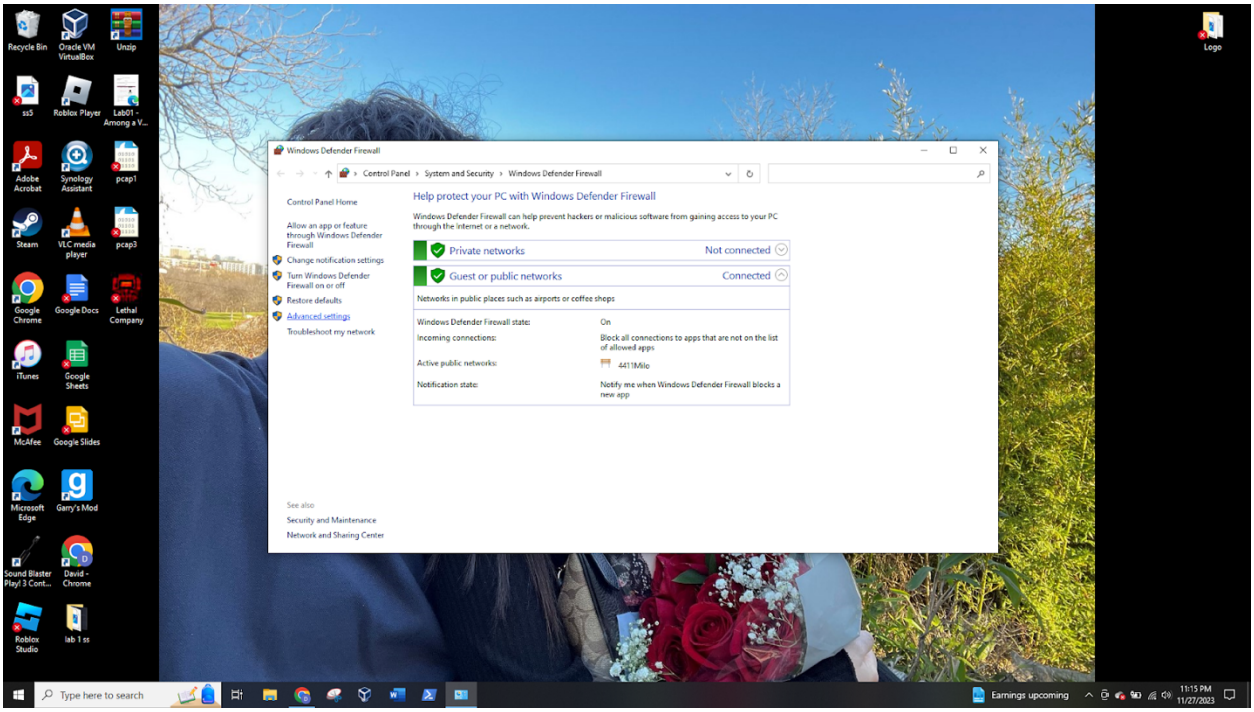
6. Closing unused ports and services

In order to reduce your attack surface, you should close unused ports. One feature that I never use is RDP, a protocol which allows for remote access of your machine. This feature has been exploited repeatedly over the years; therefore, I will close the port associated with this feature. According to CIS's article, RDP uses port 3389; therefore, I will close port 3389.

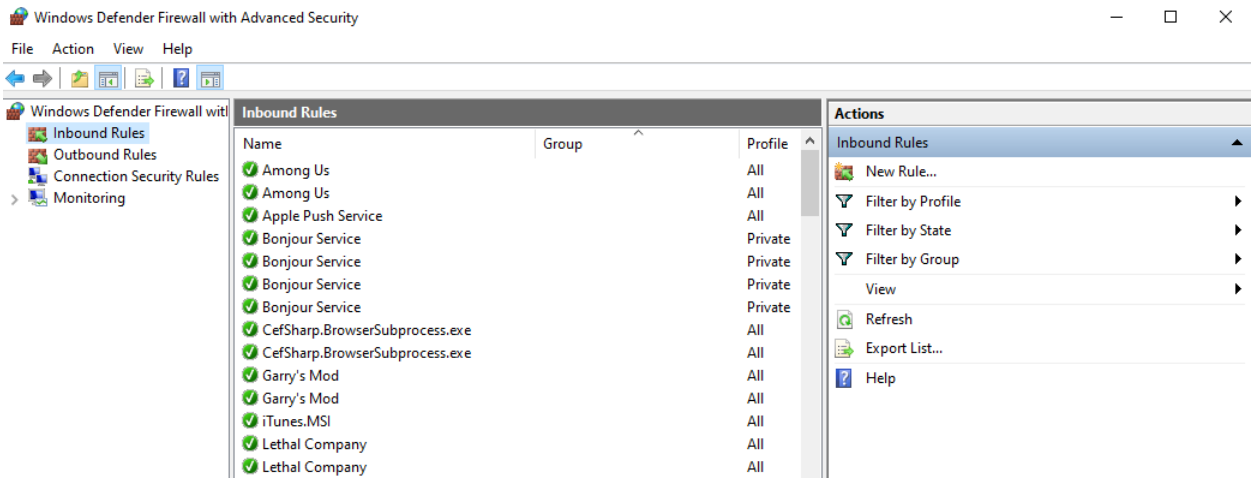


To view both the open and ports in use, I entered 'netstat -tao' in the terminal. By viewing your machine's port activity, you will be able to better understand which ports you need and which you could turn off without issue.

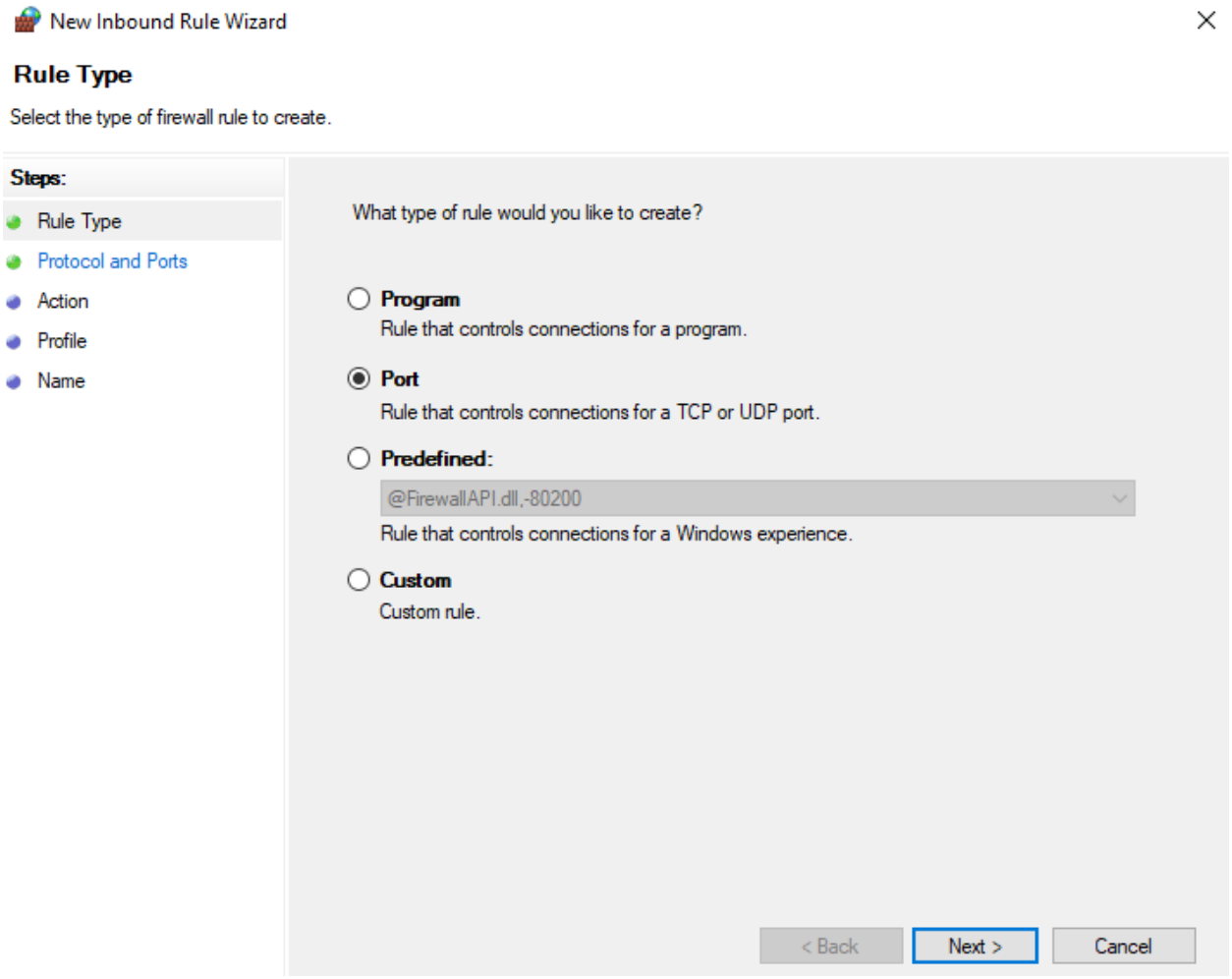
Next, I searched for and opened 'Windows Defender.'



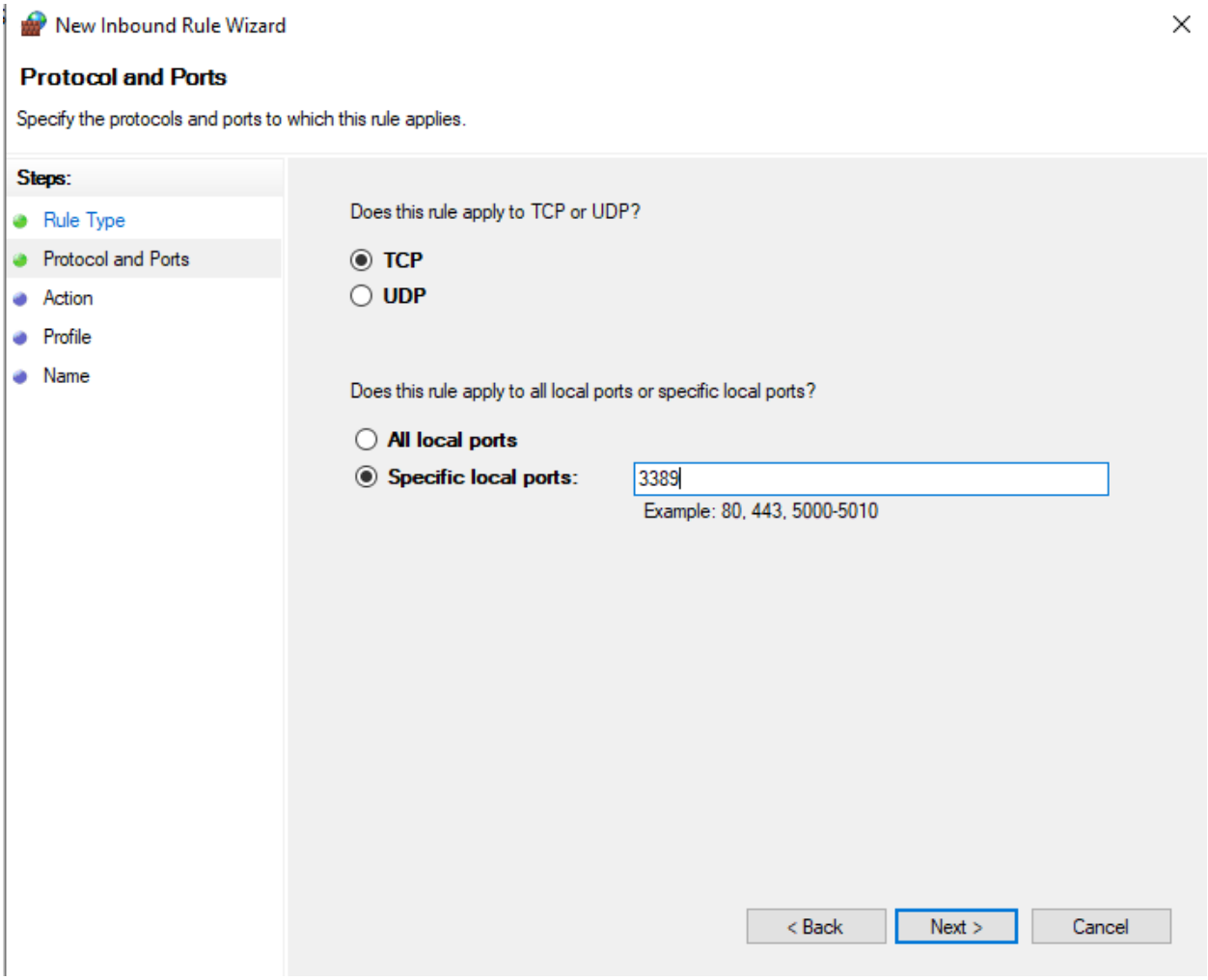
Next, I selected 'Advanced settings' on the left side of the 'Windows Defender Firewall.'



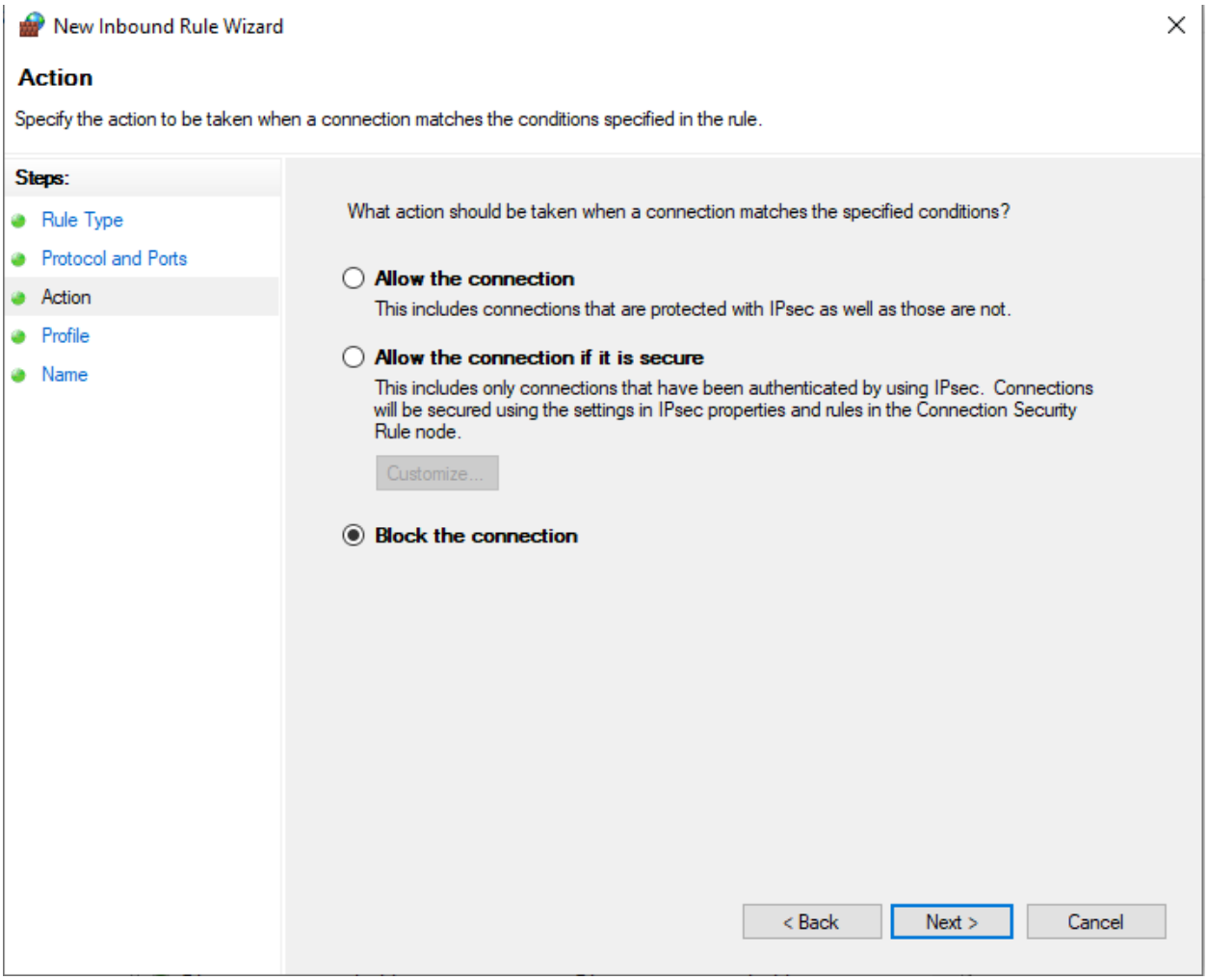
Next, I selected 'Inbound Rules' and 'New Rule.'



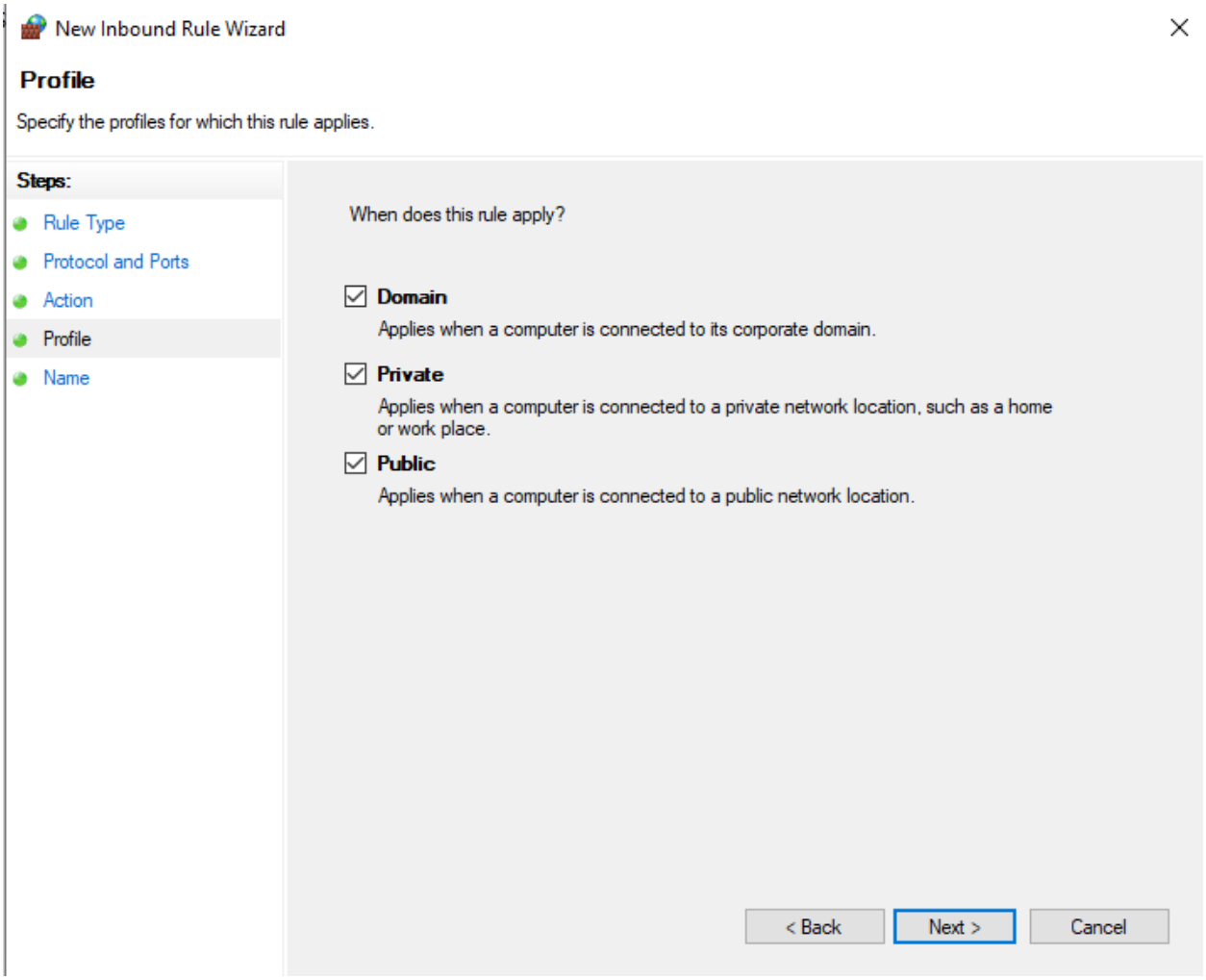
I created a new rule, and I selected "Port" to ensure the firewall rule I create disables the RDP port.



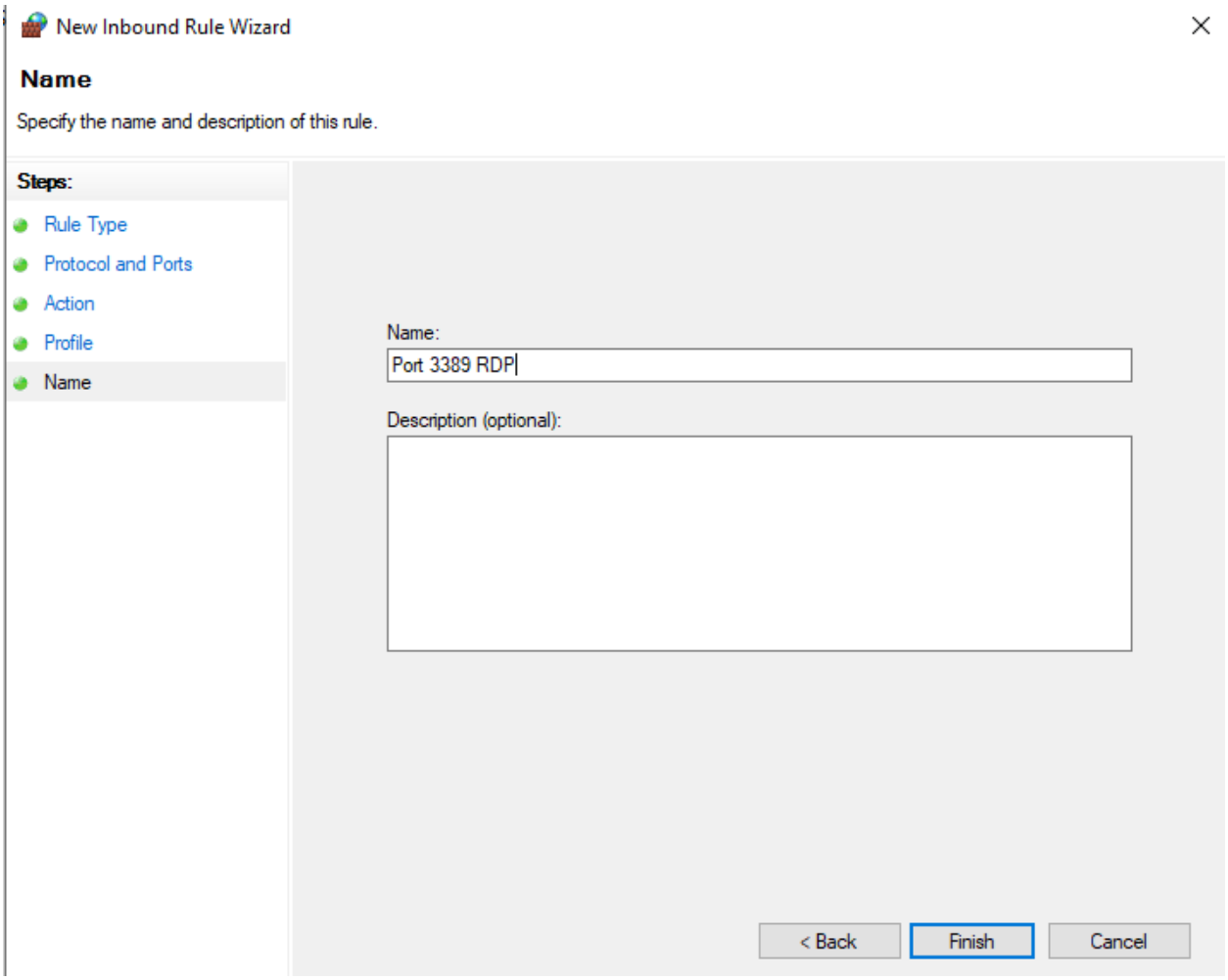
RDP uses TCP port 3389.



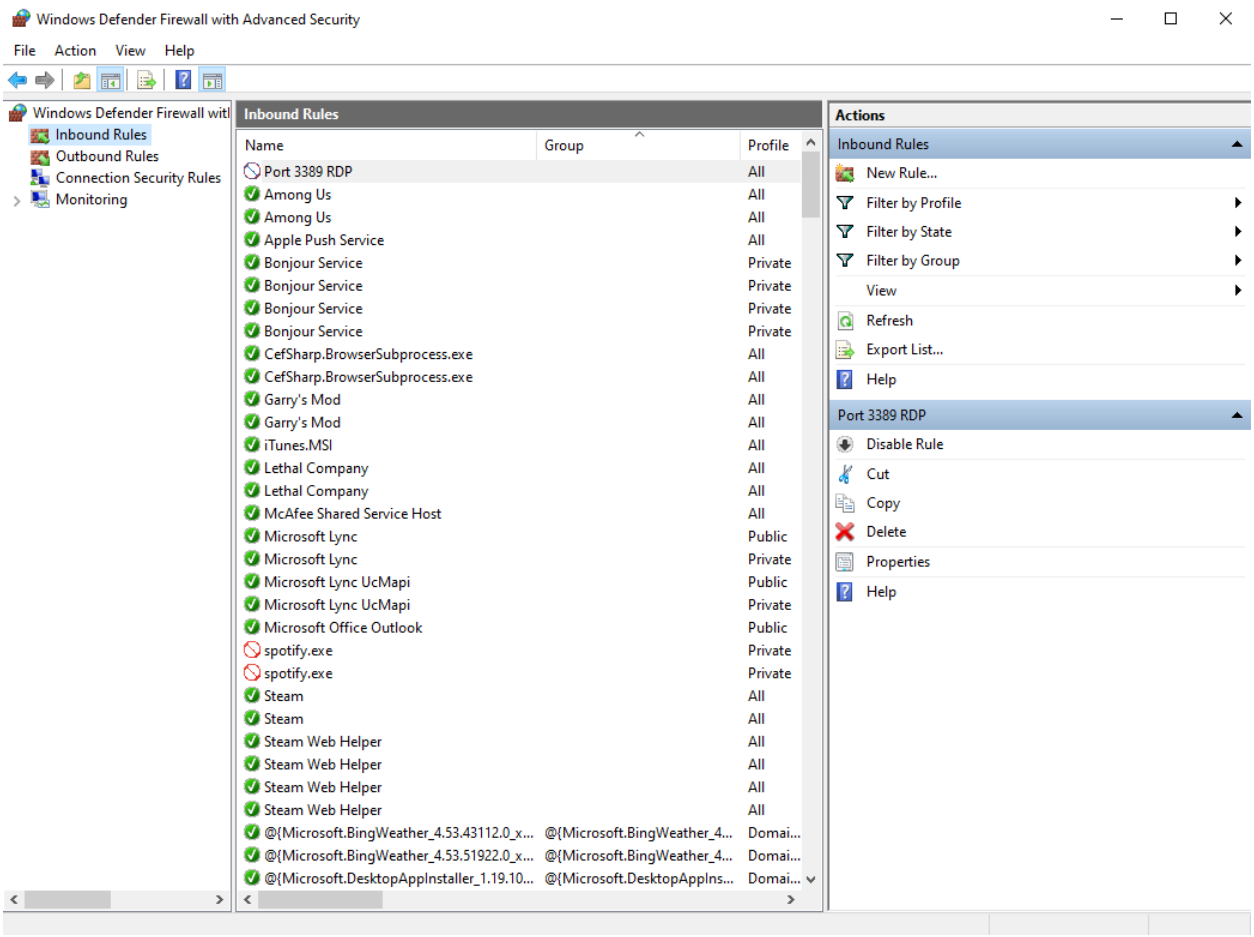
Next, I selected 'Block the connection.'



Next, I made sure this rule applied to all domain, private, and public networks.



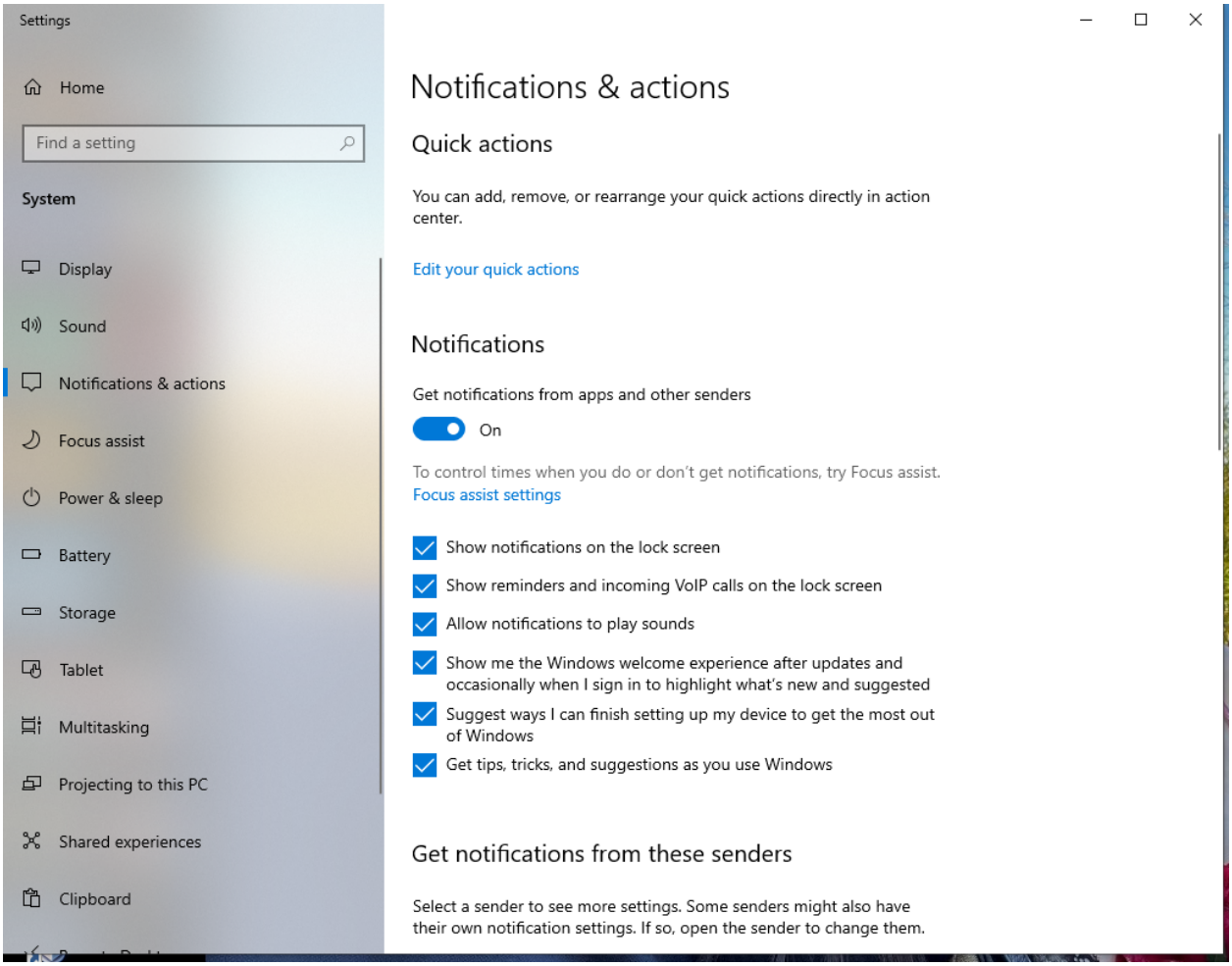
Next, I named the rule "Port 3389 RDP" and clicked "Finish" to complete the process of blocking the port.



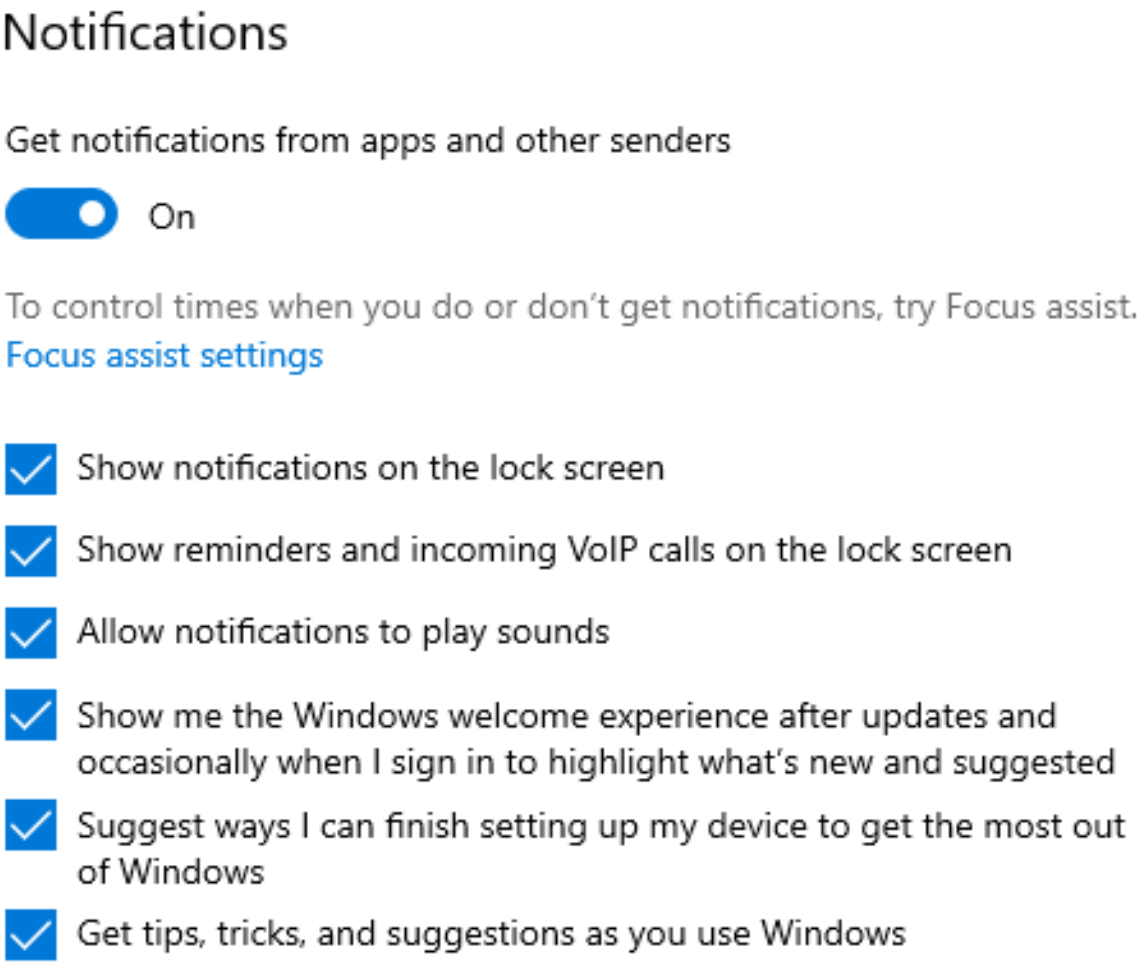
Once I selected "Finish," I was able to view my new rule at top of the 'Inbound Rules.'

7. Enabling Windows Notifications for Events

To check Windows event notifications, select the message icon at the bottom right of the screen and, on the right, all the notifications will appear.

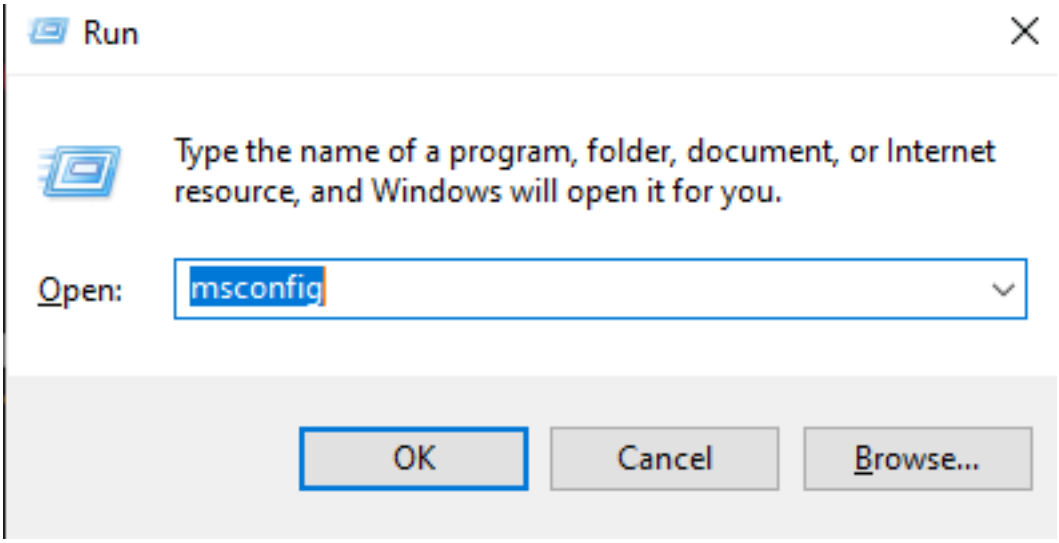


If your notifications are turned off, you can turn them on by going on system settings and then selecting 'Notifications & actions."

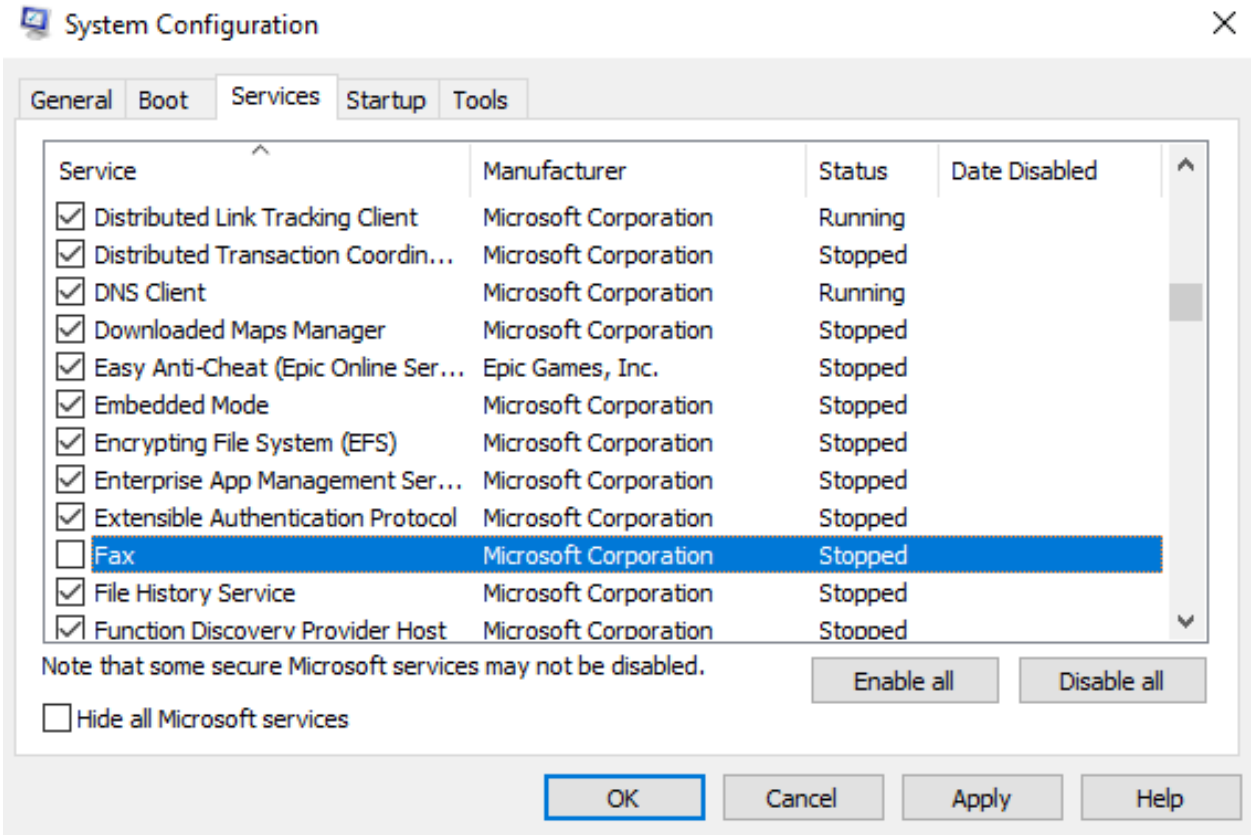


Once here, you can alter your notifications settings based on what you would like to receive notifications over. More specifically, you could choose which apps you would like to receive notifications from or where you would like to display notifications.

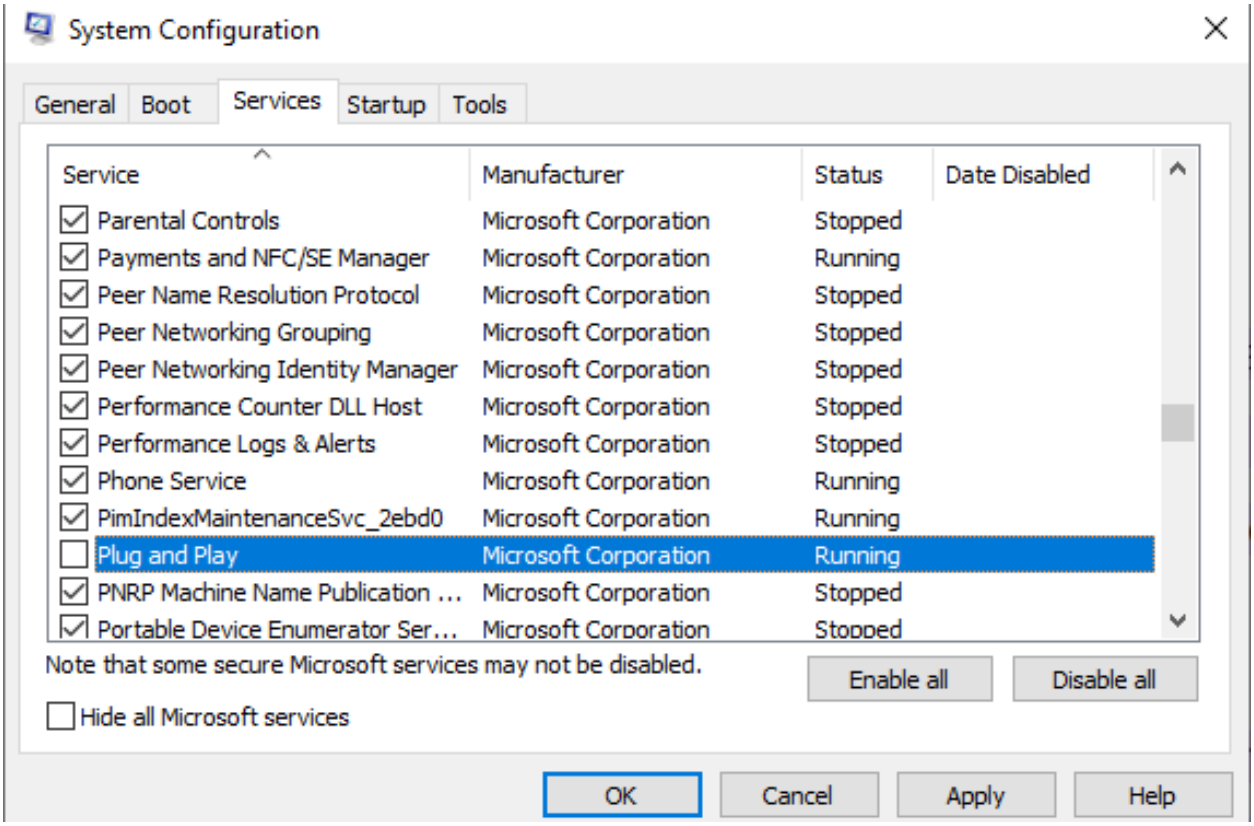
8. Disabling default Windows services



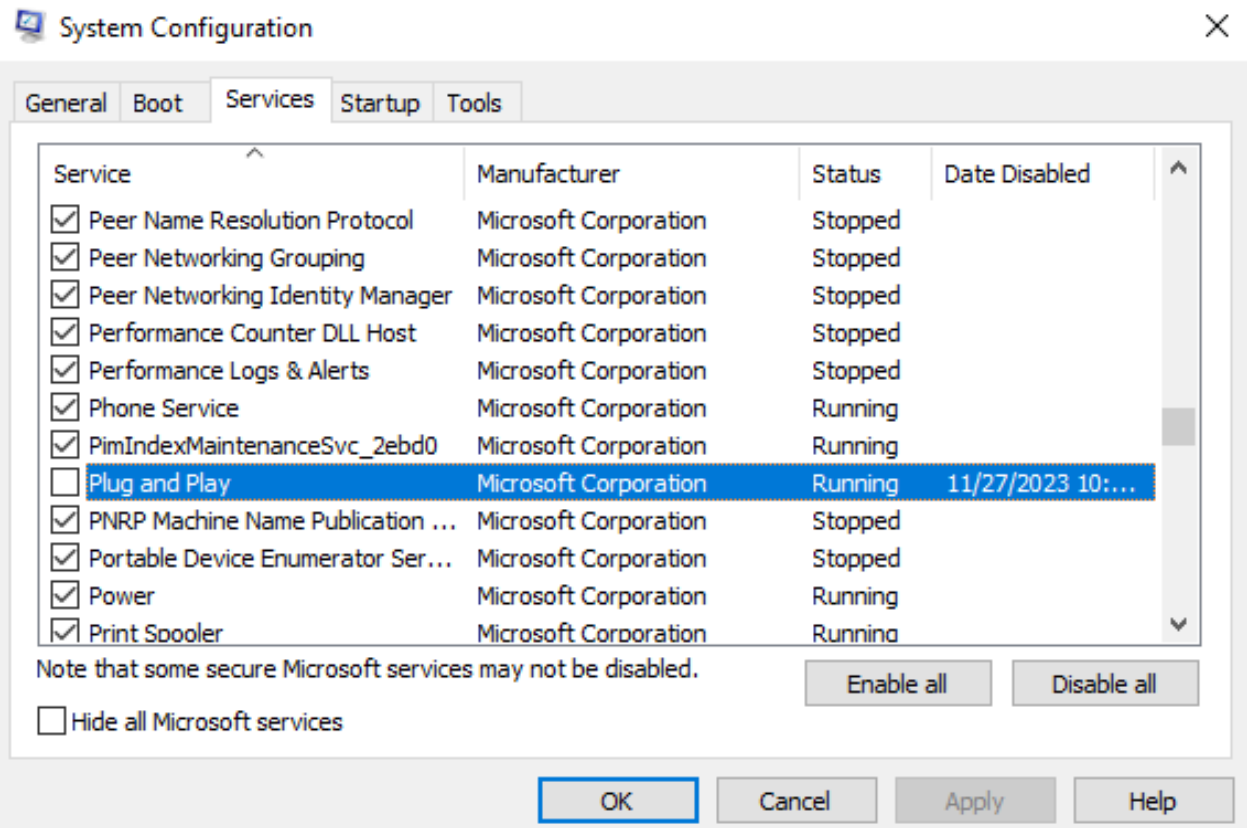
To disable default windows services, I first opened the run line by using the win + r shortcut, and I entered 'msconfig.'



Next, I selected services and began unchecking all the services I wanted to disable.

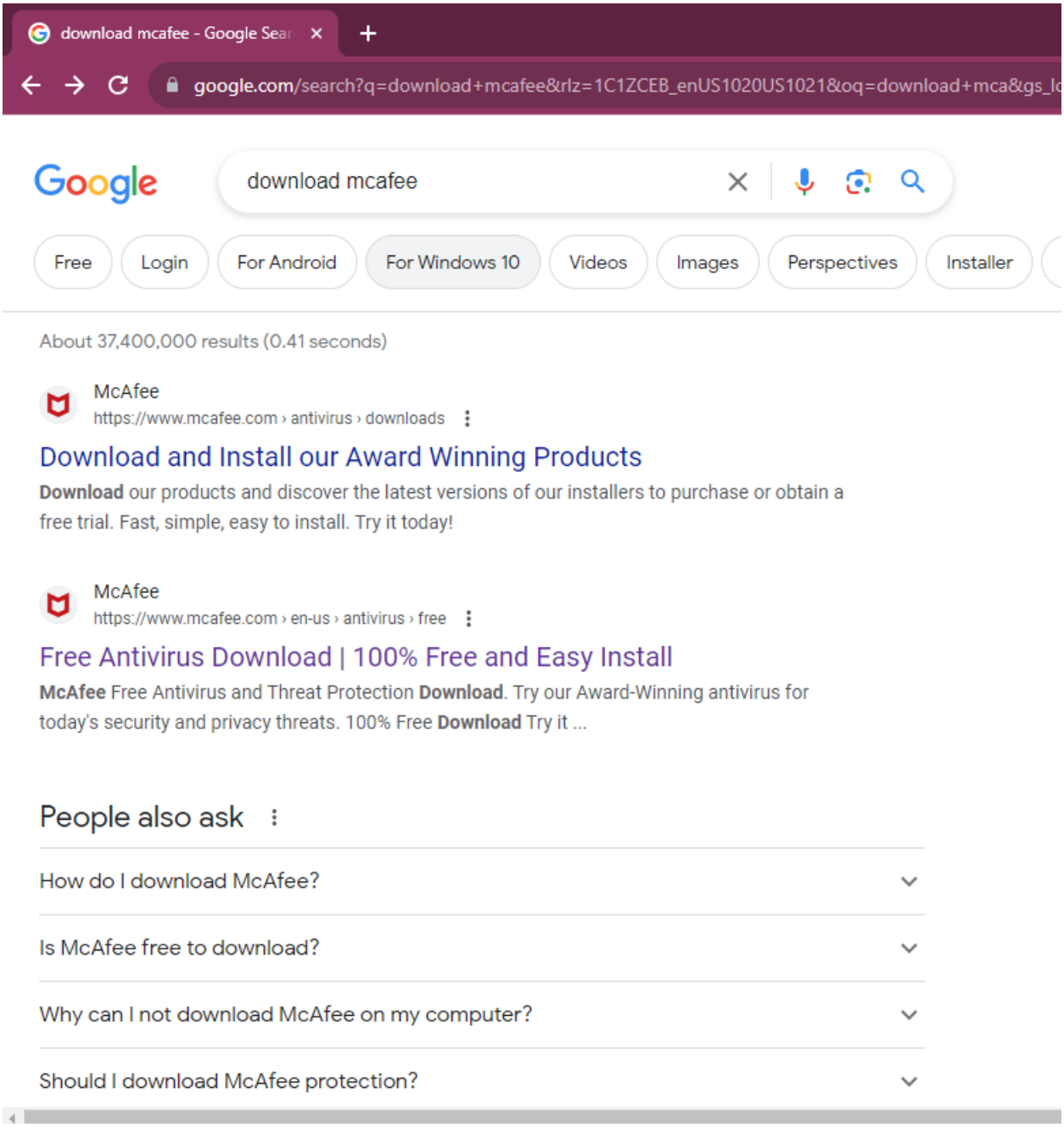


I also disabled Plug and Play as this service is an immense security risk. If left enabled, if you were to plug in a malicious USB, the services would automatically execute its contents on your computer.

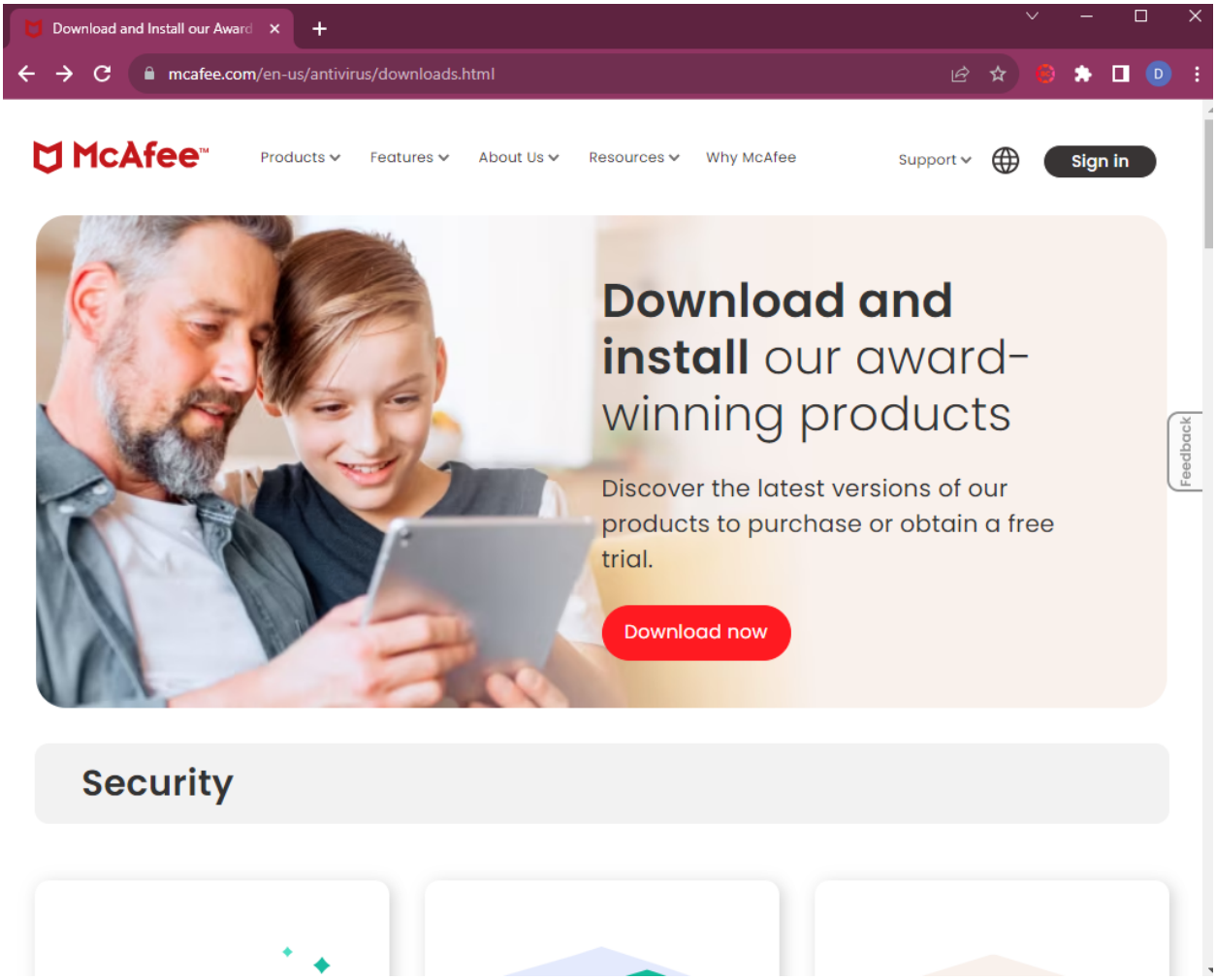


Finally, I clicked apply and you could see that the service was successfully disabled as there is now a date beside the service under 'Date Disabled.'

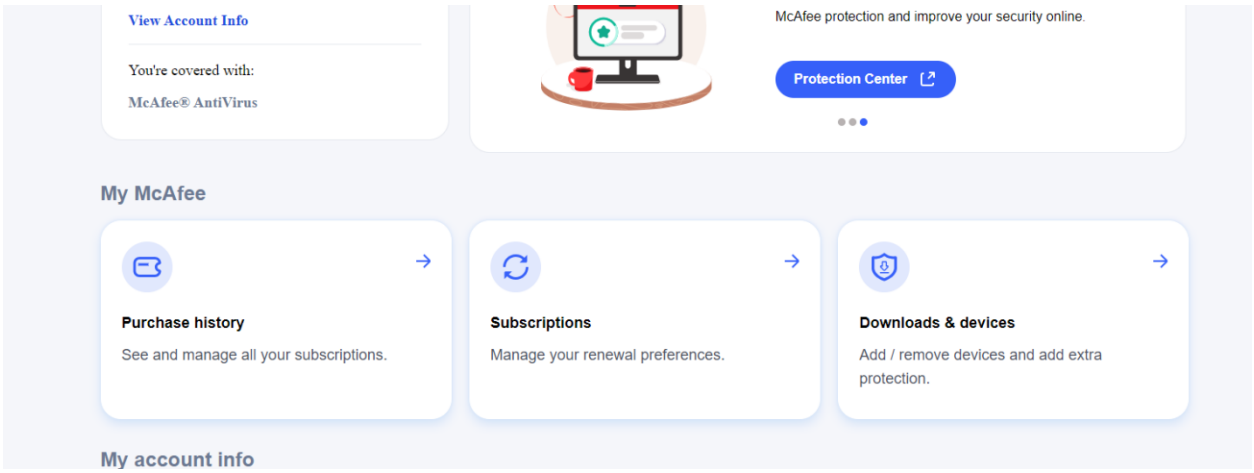
9. Installing and updating an antivirus



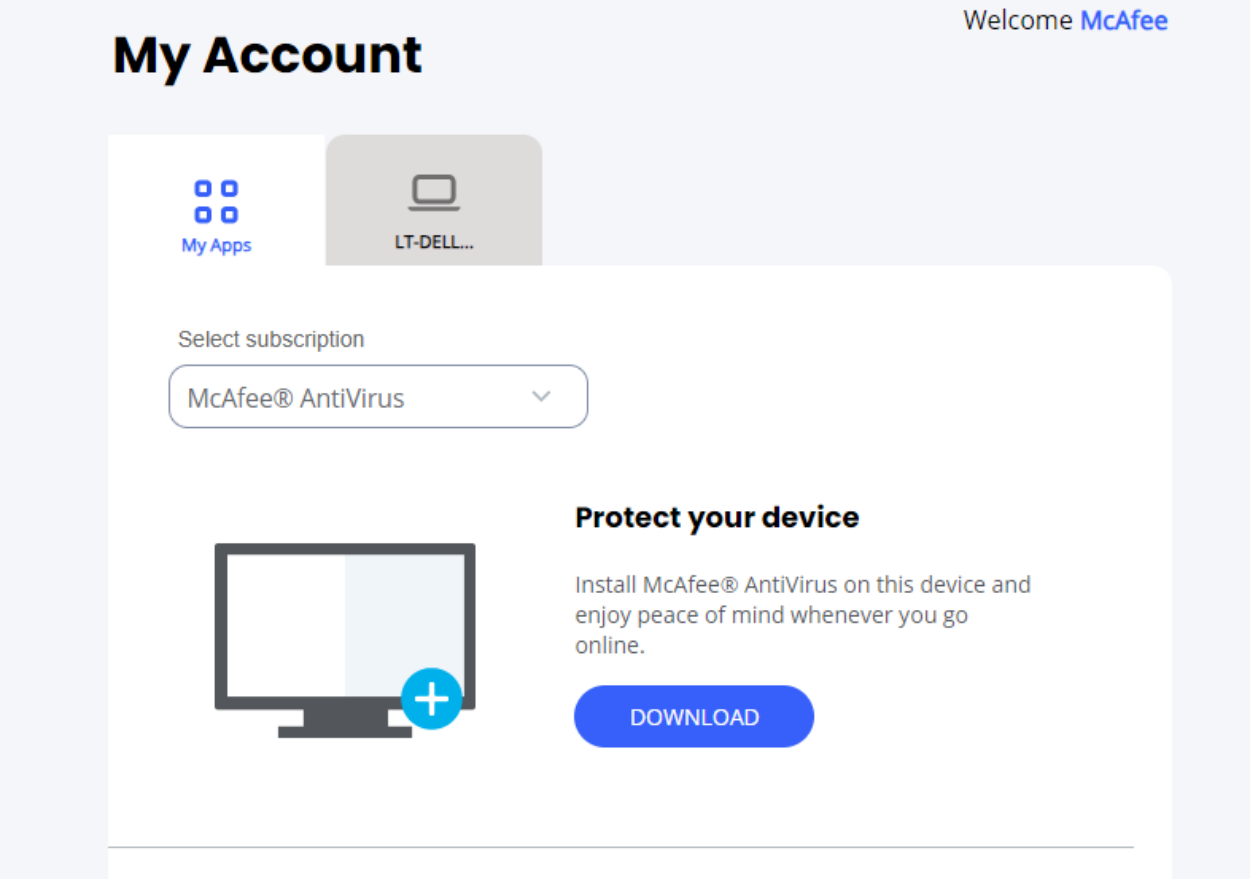
I chose to download McAfee as I am already paying for a McAfee subscription. To begin, I searched up 'download McAfee' and I selected the first search result.



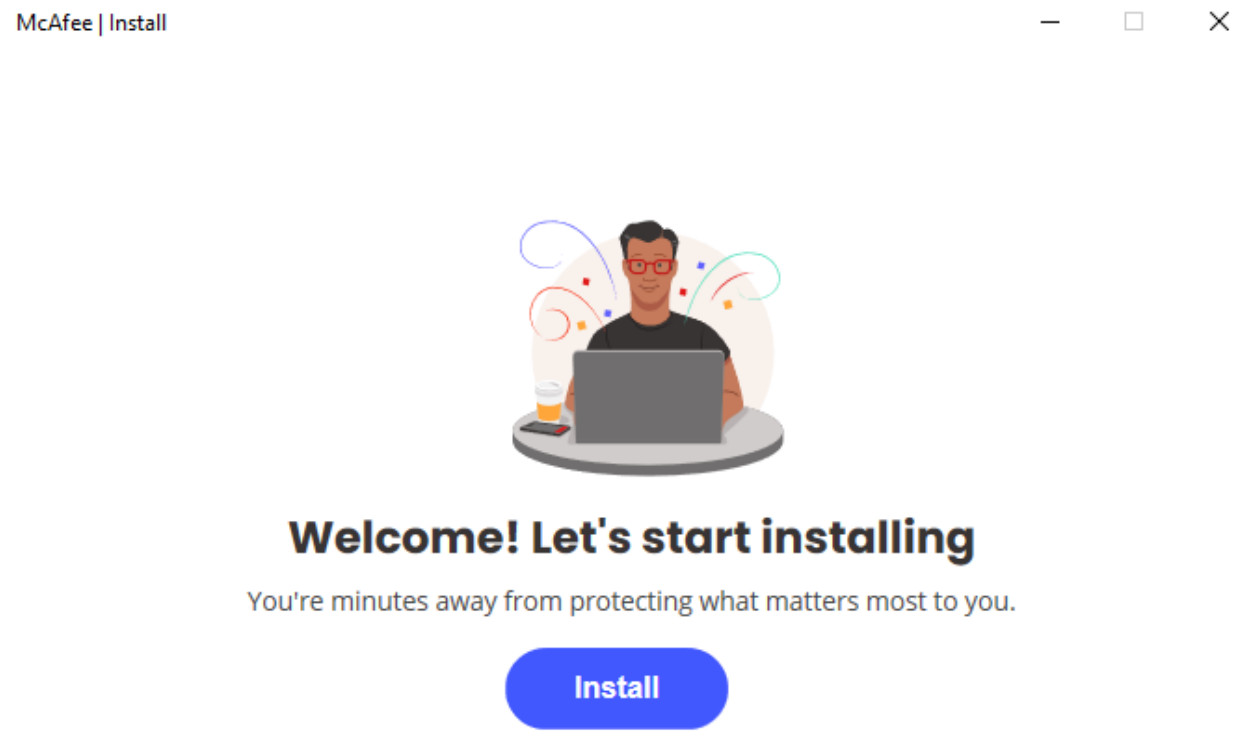
Next, I clicked on "Sign in" to sign into my account.



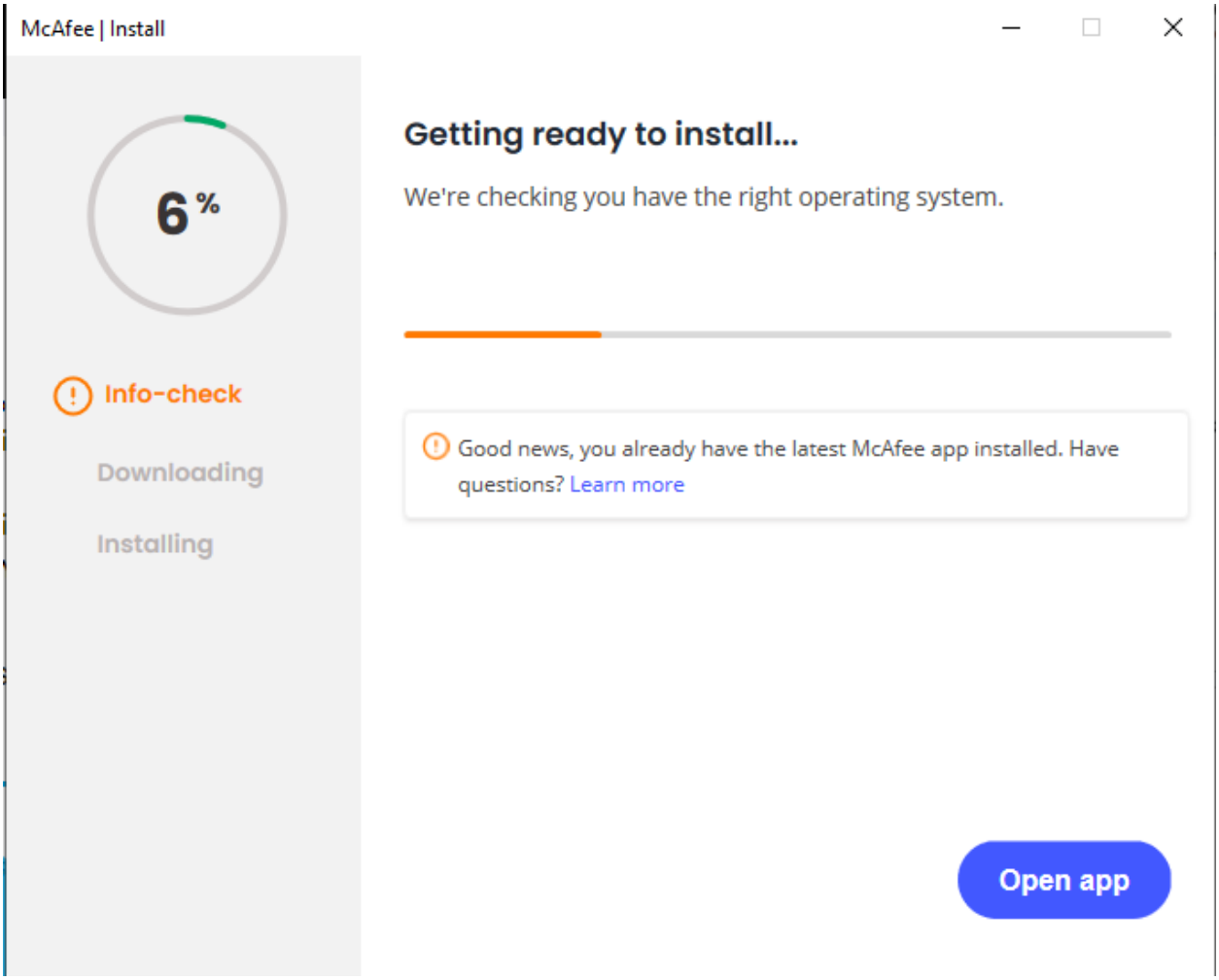
Once signed in, I selected "Downloads and devices."



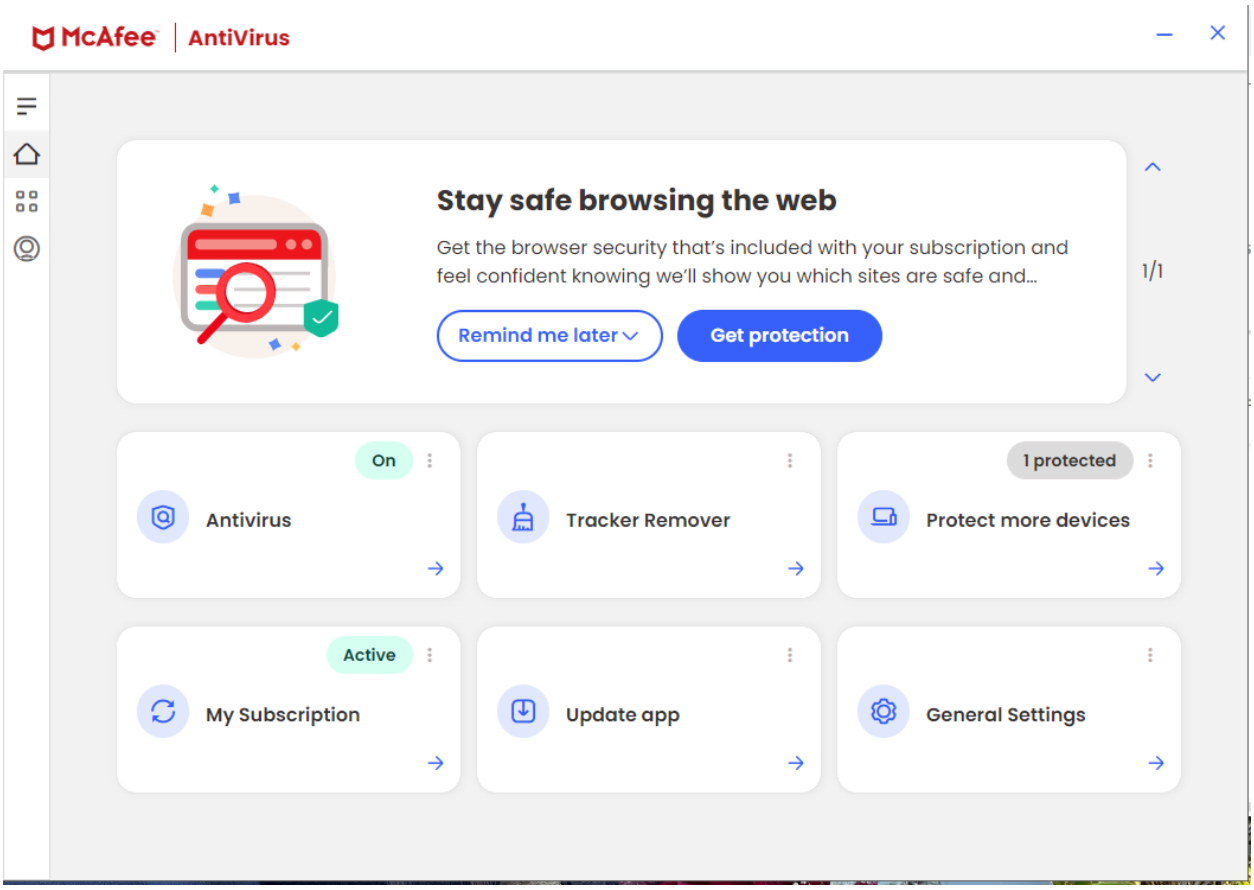
Once on 'Downloads and devices,' I clicked Download.



Next, the anti-virus began installing.



Screenshot of McAfee installing onto my Desktop.



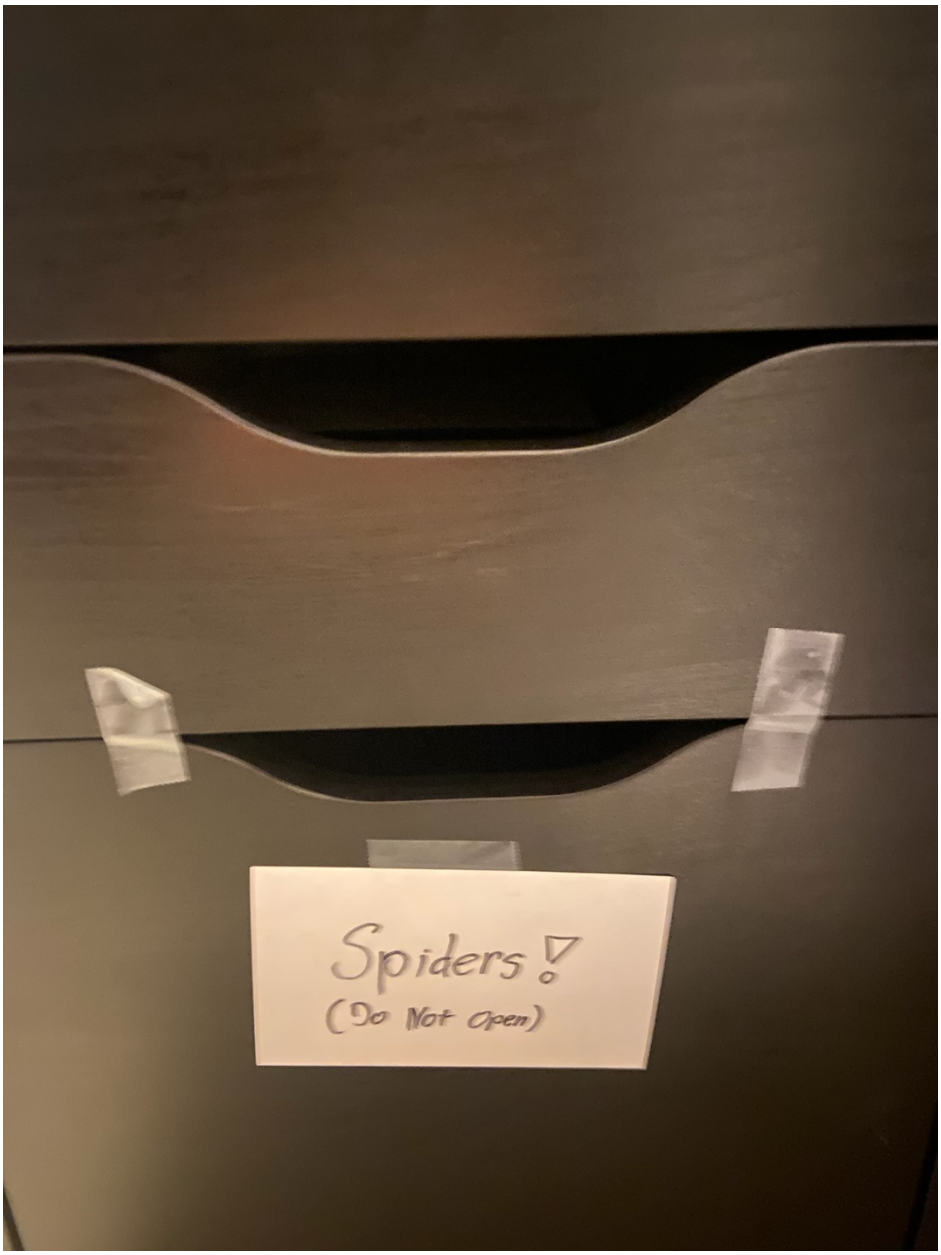
Finally, I installed McAfee and I successfully have an antivirus on my device.

10. Limiting the physical access of a host

I've already limited physical access to my device as I have both a BIOS password and a profile password. I will further limit physical access to my machine by hiding my device while the computer is inactive.

Normally I keep my device sitting on my table even when inactive.

To limit physical, I will place my laptop inside my cabinet while it is inactive.



Once inside a safe place, one could use a lock or other deterrent to safeguard your device.

LIMITATIONS/CONCLUSION

In this lab, I adeptly implemented 10 hardening techniques that bolstered my computer's security. The hardening techniques I implemented included incorporating AdBlockers, enforcing logoff upon inactivity or when logon hours expire, enabling Hard Drive Encryption (BitLocker), updating and patching the operating system, deactivating Secondary Logon Services, closing unused ports and services, enabling Windows Notifications for Events, deactivating default Windows services, installing and updating an antivirus, and restricting the physical access of a

host.

REFERENCES

TechCrunch: ‘Even the FBU says you should use an ad blocker’ https://techcrunch.com/2022/12/22/fbi-ad-blocker/#:~:text=This%20holiday%20season%2C%20consider%20giving,or%20extorting%20money%20from%20victims.
I used this website to become more knowledgeable on ad-blockers and how they could be used to harden your machine.

4Sysops: ‘Automatically log off idle users in Windows.’ https://4sysops.com/archives/automatically-log-off-idle-users-in-windows/
I used this website to learn more about Force log off and how I could add that feature onto my computer.

Professor K: ‘Disable Windows 10 Automatic Logoff for Inactivity’ https://www.youtube.com/watch?v=eDuGWGiawfQ&ab_channel=ProfessorK
I used this website to find the Automatic Logoff for Inactivity.

Microsoft: ‘Turn on device encryption.’ https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838#:~:text=Turn%20on%20standard%20BitLocker%20encryption,-Sign%20in%20to&text=In%20the%20search%20box%20on,is%20available%20for%20your%20device.
I used this webpage to learn more about BitLocker and how to use it on my device.

LinkedIn: ‘What are the benefits and risks of updating to the latest OS version? https://www.linkedin.com/advice/1/what-benefits-risks-updating-latest-os-version
I used this article to learn a little more on the risks of updating to the latest OS.

Tech Wonders: ‘Disable the Secondary Logon Service to Prevent Starting Processes Under Alternate Credentials.’ https://www.tech-wonders.com/2009/08/disable-secondary-logon-service-to.html
I used this article to learn more about Secondary Logon and how to disable it.

SuperUser: ‘How do I close ports that I don’t need in Windows 10?’ https://superuser.com/questions/1686740/how-do-i-close-ports-that-i-dont-need-in-windows-10
I used this webpage to understand how to close unused ports on Windows.

Microsoft: ‘Change notification settings in Windows.’ https://support.microsoft.com/en-us/windows/change-notification-settings-in-windows-8942c744-6198-fe56-4639-34320cf9444e
I used this webpage to learn how to change my notification settings on Windows.

Windows Report: ‘Windows 10 Services You Can Safely Disable & How to Guide.’ https://windowsreport.com/disable-windows-services/
I used this website to research default services, which ones I could disable, and how to disable them.

FTC: ‘Physical Security.’ https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/physical-security
I used this web page to learn about the importance of physical security.

Chrome Web Store: ‘AdBlock’ https://chromewebstore.google.com/detail/adblock-%E2%80%94-best-ad-blocker/gighmmpiobklfepjocnamgkkbiglidom?pli=1
I downloaded this ad-blocker.

JR Tech & Software: ‘What Happens When You Disable All Windows Services?’ https://www.youtube.com/watch?v=J5o7IZGh9I8
I used this video to learn how to disable default enabled services.

NordVPN: ‘Should UPnP be enabled or disabled?’ https://nordvpn.com/cybersecurity/glossary/upnp/#:~:text=Enable%20UPnP%2DUP%20to%20require,at%20the%20cost%20of%20convenience.
I used this website to determine whether I should disable plug n play on my device.

CIS: ‘Security Primer – Remote Desktop Protocol’ https://www.cisecurity.org/insights/white-papers/security-primer-remote-desktop-protocol
I used this website to learn about the security risk posed by RDP and which port I could disable to mitigate the risk.

Win10User: ‘Windows 10: How to Start or Stop Secondary Logon Service.’ https://www.youtube.com/watch?v=ho3p75xGtJ8
I used this website to learn how to stop secondary logon on Windows 10.