Raymond Ng
IS 3423 – Network Security
Lab 3: Host Hardening
April 12th, 2023

For this lab, I will be hardening my hosts (personal computers). I will be working on a Windows machine.

Part A

Password Hardening

Changing Default Password on Routers

Changing default passwords on routers is an essential security measure that helps harden the host and protect my network from unauthorized access. Changing the default password helps protect my router and network from unauthorized access by potential hackers, who often target default settings on devices to gain control. Moreover, a strong, unique password can prevent unauthorized users from making changes to my router's settings or accessing sensitive information. Further, changing the default password ensures that only authorized users have access to my network and its devices, allowing for better monitoring and control.

Conversely, users may find it challenging to remember new, complex passwords. This could lead to password resets or writing down passwords, which can create security risks. Changing default passwords on multiple devices may take time and effort, especially for inexperienced users or large organizations with numerous routers. Properly managing and storing passwords can be challenging, and poor password management practices can lead to security vulnerabilities. Users may need to reconnect devices to the network after changing the router's password, which can be inconvenient.

Despite the disadvantages, the benefits of changing default passwords on routers far outweigh the risks. It is crucial to use strong, unique passwords and follow good password management practices to maintain the security of my network and devices.

Encryption Hardening

Enable Hard Drive Encryption

Hard drive encryption is a method used to secure data on a storage device by converting it into a format that is unreadable without the correct decryption key. Normally, when I access my data it's through Windows and has the usual protections associated with signing into the operating software (Microsoft, 2023). If a malign user wanted to bypass those Windows protections, he/she could open the computer case and remove the physical hard drive. Then by adding my hard drive as a second drive on a machine they control, they may be able to access my data without needing my credentials. However, if my drive is encrypted, when they try to use that method to access the drive, they'll need to render a decryption key to access anything on the drive. Without the decryption key the data on the drive will appear obfuscated (Microsoft, 2023).

In addition to the abovementioned, encryption ensures that only authorized individuals can access the data on the hard drive. This is particularly important in case of theft or unauthorized access. Moreover, if a data breach occurs, encrypted data is significantly more difficult for attackers to access and exploit, reducing the potential damage. Further, encryption helps maintain the privacy of personal or sensitive data, protecting against identity theft and other malicious activities.

Encryption and decryption processes can cause some performance overhead, potentially slowing down system operations (Wright & Zadok, 2003). However, modern hardware and encryption algorithms have minimized this impact. Additionally, implementing and managing encryption solutions can be complex, especially for non-experts. Misconfiguration or mistakes can result in data loss or reduced security (De Groot, 2023). If encryption keys are lost or damaged, it can be extremely difficult or even impossible to recover the encrypted data. Regular backups and secure key management are essential to avoid this risk.

Overall, the benefits of hard drive encryption often outweigh the disadvantages, particularly in environments where sensitive data is stored. However, it is crucial to properly implement and manage encryption solutions to maximize security and minimize potential risks.

Registry Hardening

Secure Registry (Guest and User Account) Privileges

Securing registry privileges is vital in maintaining a safe and secure computing environment. It involves implementing access control measures to protect registry keys and values from unauthorized access and modification (Microsoft, 2021). Registry privileges can be secured for both guest and user accounts.

Restricting access to the registry can prevent unauthorized users from making modifications that could lead to system instability, data breaches, or malware infections. Moreover, by securing registry privileges, sensitive data stored in the registry is protected from unauthorized access, helping to maintain the privacy and integrity of the information. Further, limiting registry access can reduce the risk of unintended or malicious modifications that could result in system crashes or other issues (Rosencrance, 2023).

Restricting registry access may prevent users from making legitimate modifications to the system or applications, potentially hindering their ability to troubleshoot or customize settings. Additionally, implementing security measures for registry access can increase the complexity of the system configuration, making it more challenging to manage and maintain. Incorrectly implementing registry security measures can result in unintended consequences, such as users being unable to access necessary resources or system instability.

Network Hardening

Disable Remote Access to a Computer

Disabling remote access can reduce the attack surface, making it more difficult for hackers to infiltrate a computer system. This can help protect sensitive information and prevent unauthorized access or control. Additionally, disabling remote access can possibly mitigate potential attackers, denying them the ability to exploit vulnerabilities in remote access protocols, reducing the risk of unauthorized access to the system (Babu, 2022).

Disabling remote access can make it more challenging for administrators to perform tasks such as system updates, troubleshooting, and maintenance remotely, potentially increasing the time and effort required to manage the system. Users may need to access their computers remotely to complete tasks or access resources. Moreover, disabling remote access can create challenges for users who rely on remote access to maintain productivity and efficiency. Disabling remote access can limit the ability of these users to collaborate effectively and securely (Bhardwaj, 2022).

Web Browser Hardening

Managing/Disable Cookies

Cookies are small text files stored on a user's device by web browsers to remember information about the user and their preferences (Kaspersky, 2023). While cookies can offer several benefits, there are also reasons to disable them. Disabling cookies can protect user privacy by preventing websites from tracking user activity and collecting personal information (Dodt, 2020). Disabling cookies can help prevent unintentional data sharing between different websites or third-party trackers, reducing the risk of data breaches. Cookies can sometimes be used to exploit security vulnerabilities or spread malware.

From a previous class I know cookies help websites remember user preferences, such as language, login information, and site-specific settings. Disabling cookies can lead to a more generic browsing experience, requiring users to re-enter their preferences each time they visit a site. Moreover, disabling cookies can result in the loss of convenience features such as automatic logins, saved shopping carts, or site-specific customization, which may affect the user experience and make browsing less efficient. Further, some websites rely on cookies for essential functionality. Disabling cookies can cause these sites to function improperly or not work at all.

Operating System Hardening

Update and Patch Operating System

From a previous operating systems course–prerequisite to this course—I learned that one of the most important advantages of operating system updates is that they often include security fixes and patches. These updates can help protect my computer or device from vulnerabilities that could be exploited by hackers and other malicious actors. Moreover, operating system updates can improve the stability of your device, fixing bugs and issues that could cause crashes and other problems. Further, operating system updates can ensure that your device is compatible with the latest software and hardware, preventing compatibility issues that could cause problems down the line.

From my experience working in IT support for Apple I’ve learned that operating system updates can also create compatibility issues with older software or hardware that may no longer be supported. Some operating system updates can negatively affect performance, causing slowdowns and other issues. In some cases, operating system updates can cause data loss, especially if there are issues with the installation process.

Overall, while operating system updates can have some disadvantages, the benefits often outweigh the drawbacks, especially when it comes to security and stability. However, it's important to be cautious when installing updates and ensure that you have backups of your important data in case something goes wrong.

Audit/Logging File Hardening

Set Up Firewall Profiles

Setting up firewalls provides protection against unauthorized access to my network, or in this case, my host (Prakash, 2023). More importantly, firewalls can prevent hackers and other malicious actors from accessing my network and stealing sensitive information. Firewalls can also be used to monitor network traffic and detect suspicious activity. This can help me identify potential security threats and take action before they cause damage.

Firewalls can be complex to set up and configure, especially for users who are not familiar with network security concepts. This can make it challenging for individuals with limited IT resources to implement and maintain a firewall. Moreover, firewalls can sometimes generate false positives, blocking legitimate traffic and disrupting normal operations (ITL, n.d.). This can be frustrating for users and can lead to productivity issues. Firewalls can sometimes impact network performance, especially if they are not configured correctly. This can result in slow internet speeds and other issues that can negatively impact productivity.

Application Hardening

Disable Unneeded Services

Disabling unneeded services can improve the performance of your computer, as it reduces the number of background processes that are running. This can help your computer run faster and more smoothly, especially if you have a limited amount of RAM or processing power. Moreover, from a previous operating systems course, I learned that disabling unneeded services can also improve the security of your computer, as it reduces the number of potential attack vectors that can be exploited by hackers and other malicious actors. This can help prevent data breaches and other security incidents.

Disabling some services can cause some functionality loss, as certain features and applications may depend on these services to function properly. This can be especially problematic for users who rely on specific software applications that require specific services to be running. Additionally, disabling necessary services can also cause compatibility issues with certain software applications or hardware devices, especially if these applications or devices require specific services to be running. Disabling services can also create security risks, as it can make it more difficult to manage and secure my computer. Disabling a service(s), coupled with lack of familiarity with the service, may disengage a critical service that is required for security purposes.

Anti-Virus Hardening

Install and Updating an Antivirus

Anti-virus software is that it provides protection against viruses, malware, and other types of malicious software from infecting the host (CISA, 2019). Anti-virus software can detect and remove these threats before they can cause damage to your computer or steal your sensitive information. Most anti-virus software providers release regular updates to their software to stay up-to-date with the latest threats and vulnerabilities, providing additional protection against new and emerging threats.

From experience, some anti-virus software can impact the performance of your computer, especially during scans or updates. This can result in slow internet speeds and other issues that can negatively impact productivity. Anti-virus software can sometimes generate false positives, identifying legitimate software or files as malicious and removing them (Martens, 2023). This can be frustrating for users and can lead to data loss and productivity issues. Further, while anti-virus software can provide protection against viruses and malware, it may not provide comprehensive protection against other types of threats, such as phishing attacks or social engineering scams.

Physical Hardening

Limit the Physical Access of a Host

Limiting physical access to host machines improves the physical security of your network. By restricting physical access to host machines, you can prevent unauthorized users from accessing sensitive data or tampering with hardware. Moreover, restricting physical access to host machines can reduce the risk of hardware failure due to accidental damage or tampering, prolonging the life cycle of my hardware and reduce the risk of downtime or data loss. Limiting physical access to host machines can also simplify the management of my network, as it reduces the number of users who have physical access to critical systems and data.

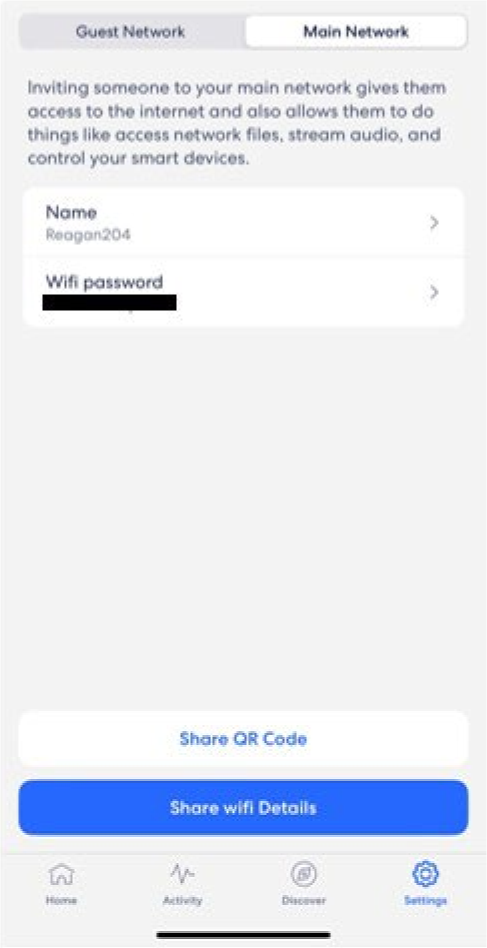
In a business setting, limiting physical access to host machines can sometimes reduce productivity, especially if users need physical access to perform their job duties. This can be a particular issue for users who need to work on hardware or perform maintenance tasks, like IT folks. Moreover, from experience, limiting physical access to host machines can also increase the complexity of a network, leading to outcomes such as establishing additional procedures and policies to manage physical access. This can be a challenge for IT teams who need to balance security needs with user satisfaction. Finally, limiting physical access to host machines can sometimes be met with resistance from users, especially if they feel that their access is being unfairly restricted.

Part B:

Password Hardening

Changing Default Password on Routers

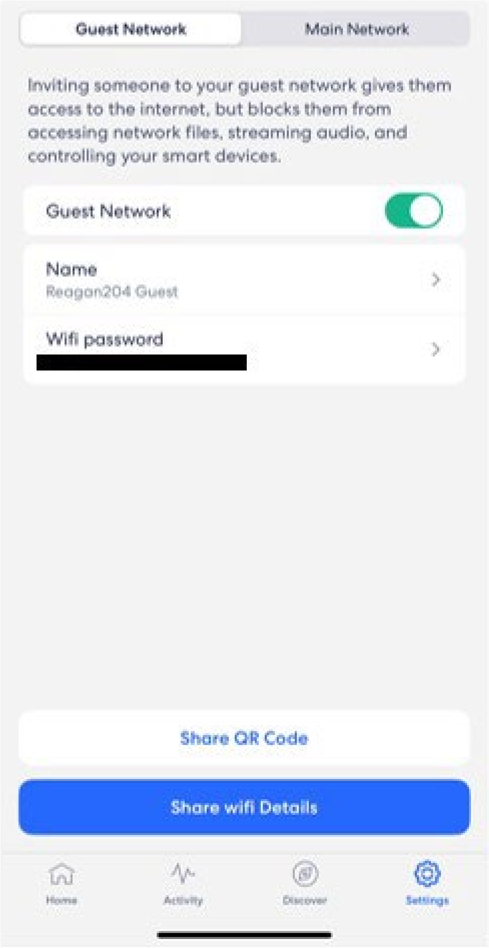
I use a third-party router product called EERO, which extends the Wi-Fi network and creates a Wi-Fi mesh ecosystem in my home. I have created a separate Wi-Fi password for myself (Main Network) and my guests (Guest Network). The passwords are alphanumeric combinations with special characters that I change monthly. I have obfuscated/redacted the password for privacy reasons in the screenshots below.



Inviting someone to your main network gives them access to the internet and also allows them to do things like access network files, stream audio, and control your smart devices.

Name
Reagan204

Wifi password
[redacted]



Inviting someone to your guest network gives them access to the internet, but blocks them from accessing network files, streaming audio, and controlling your smart devices.

Guest Network ●

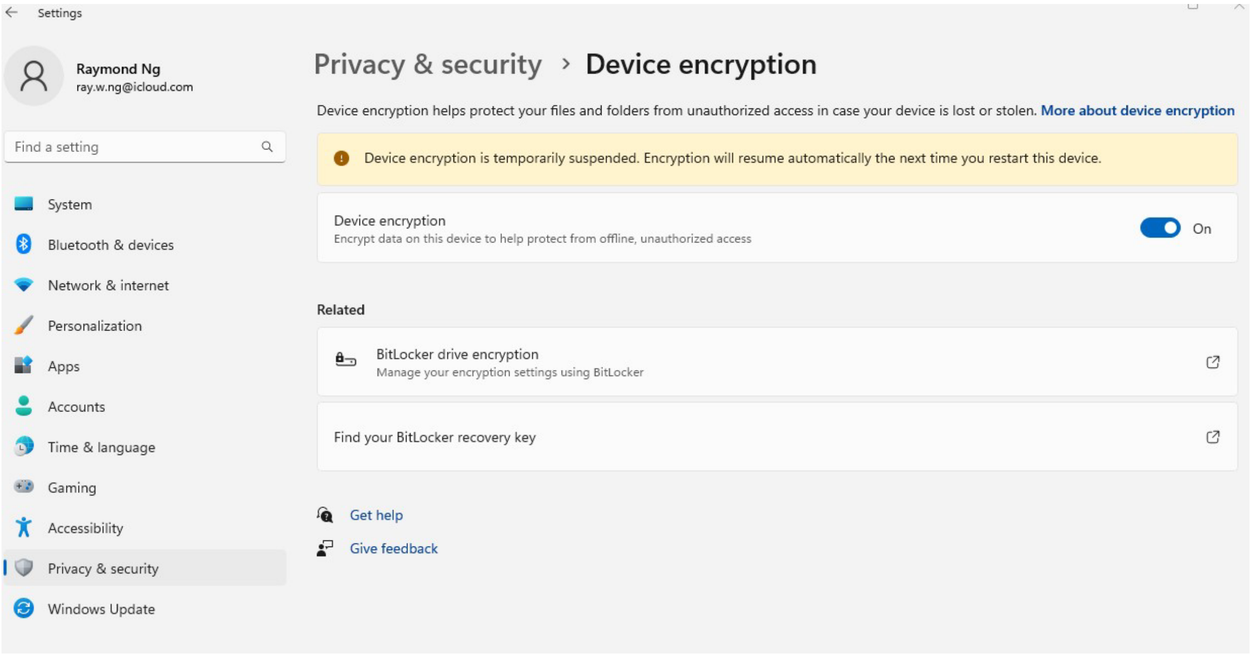
Name
Reagan204 Guest

Wifi password
[redacted]

Encryption Hardening

Enable Hard Drive Encryption

To enable ‘Device Encryptio’n on my Windows PC. I opened ‘Settings’. Clicked on ‘Privacy & security’ and turned on the ‘Device encryption’.



Privacy & security > Device encryption

Device encryption helps protect your files and folders from unauthorized access in case your device is lost or stolen. More about device encryption

Device encryption is temporarily suspended. Encryption will resume automatically the next time you restart this device.

Device encryption
Encrypt data on this device to help protect from offline, unauthorized access — On

Related

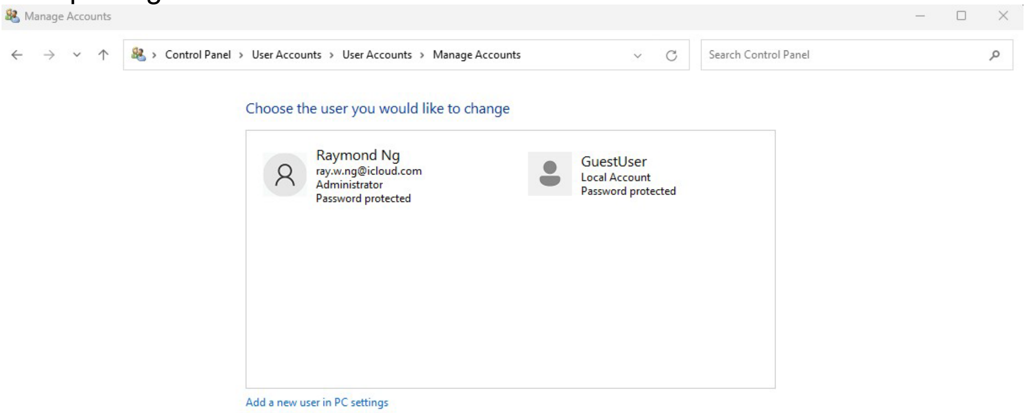
BitLocker drive encryption
Manage your encryption settings using BitLocker

Find your BitLocker recovery key

Registry Hardening

Secure Registry (Guest and User Account) Privileges

To secure the registry for Guest and User account privileges. I went to the Control Panel, clicked User Accounts>>Manage another account. I have two Accounts on this PC, mine with Administrator privileges and a Guest account.


Manage Accounts
Control Panel > User Accounts > User Accounts > Manage Accounts
Search Control Panel

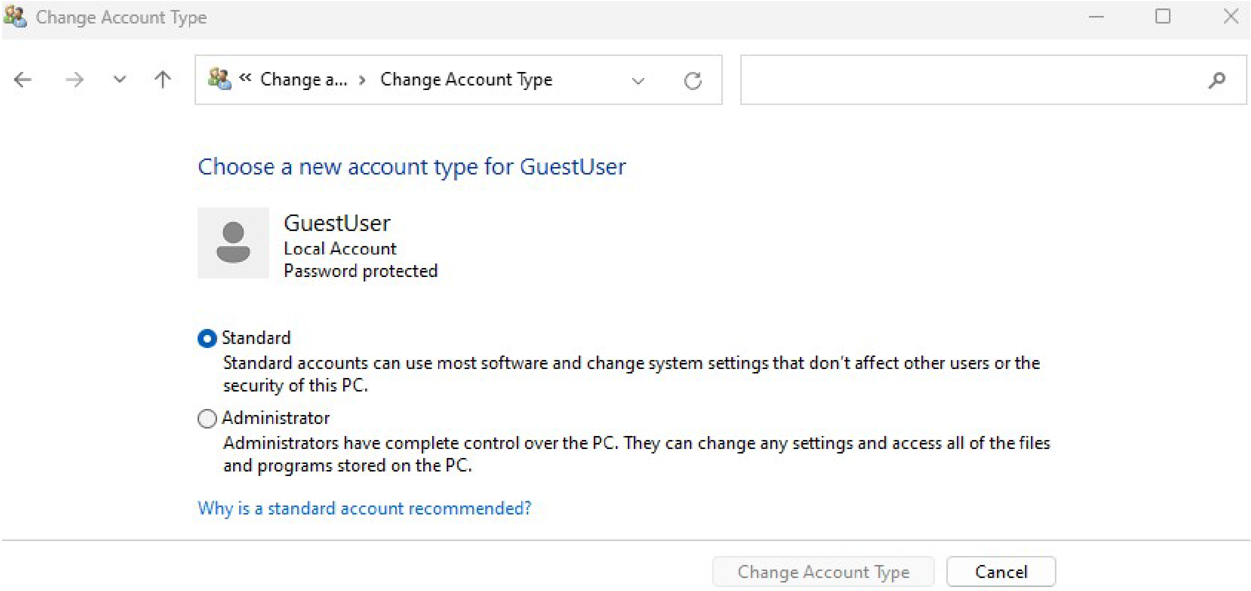
Choose the user you would like to change

Raymond Ng
ray.w.ng@icloud.com
Administrator
Password protected

GuestUser
Local Account
Password protected

Add a new user in PC settings

Next, I clicked on ‘Manage Accounts’ >> ‘Change an Account’ >> ‘Change Account Type’. I changed the GuestUser to ‘Standard’ access/privileges because it will allow the user to use most software and change system settings without affecting the existing security of my PC.



Choose a new account type for GuestUser

GuestUser
Local Account
Password protected

● Standard
Standard accounts can use most software and change system settings that don't affect other users or the security of this PC.

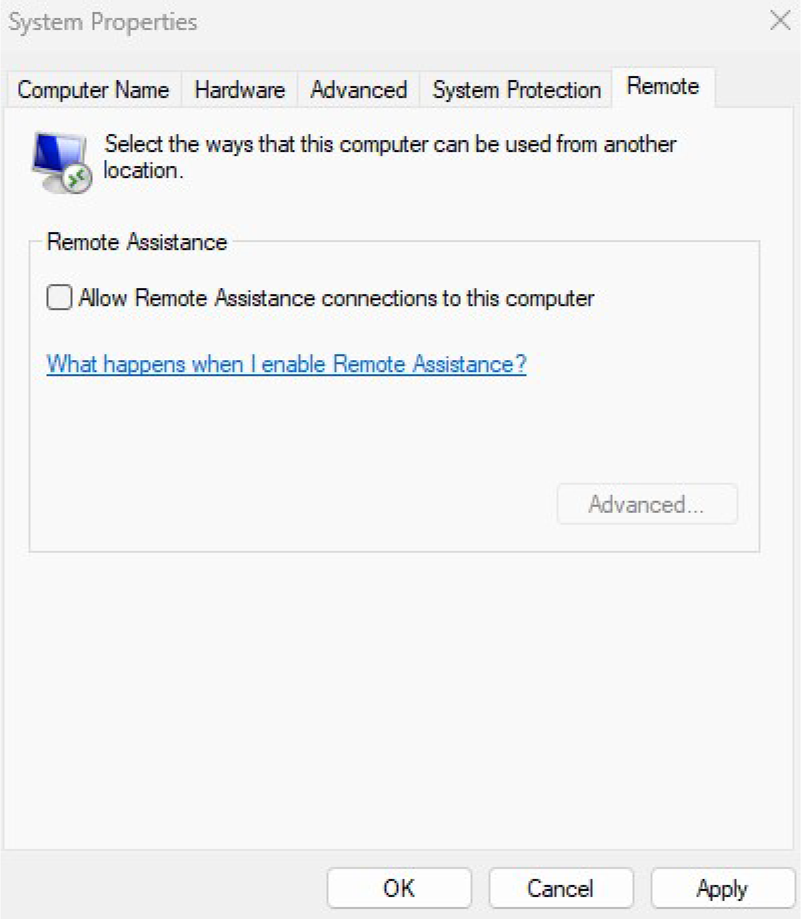
○ Administrator
Administrators have complete control over the PC. They can change any settings and access all of the files and programs stored on the PC.

Why is a standard account recommended?

Network Hardening

Disable Remote Access to a Computer

To disable 'Remote Assistance' on my PC, I went to 'System Properties' and unchecked the box 'Allow Remote Assistance connections to this computer', and clicked 'Apply'.



Select the ways that this computer can be used from another location.

Remote Assistance

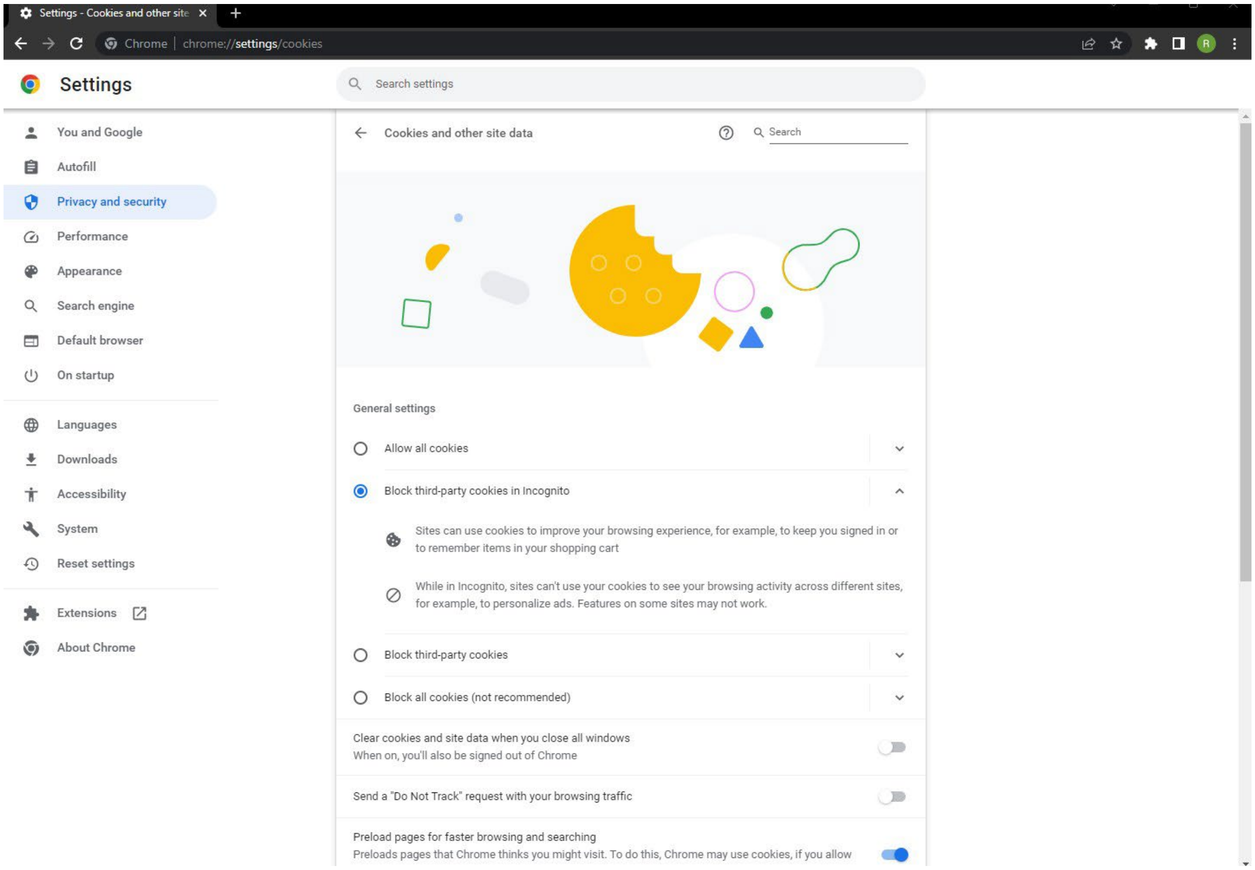
□ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Web Browser Hardening

Managing/Disable Cookies

To manage/disable cookies in Google Chrome, I clicked ⋮ button in the upper right corner of the browser window. Next, I clicked on ‘Privacy and security’ >> ‘Cookies and other site data’. Here, I clicked the option to ‘Block third-party cookies in Incognito’. I will not be permanently ‘Block all cookies’ because some websites use cookies to improve user experience, i.e. keeping me signed into and/or remembering items in my online shopping cart.



Cookies and other site data

General settings

○ Allow all cookies

● Block third-party cookies in Incognito

Sites can use cookies to improve your browsing experience, for example, to keep you signed in or to remember items in your shopping cart

While in Incognito, sites can't use your cookies to see your browsing activity across different sites, for example, to personalize ads. Features on some sites may not work.

○ Block third-party cookies

○ Block all cookies (not recommended)

Clear cookies and site data when you close all windows
When on, you'll also be signed out of Chrome

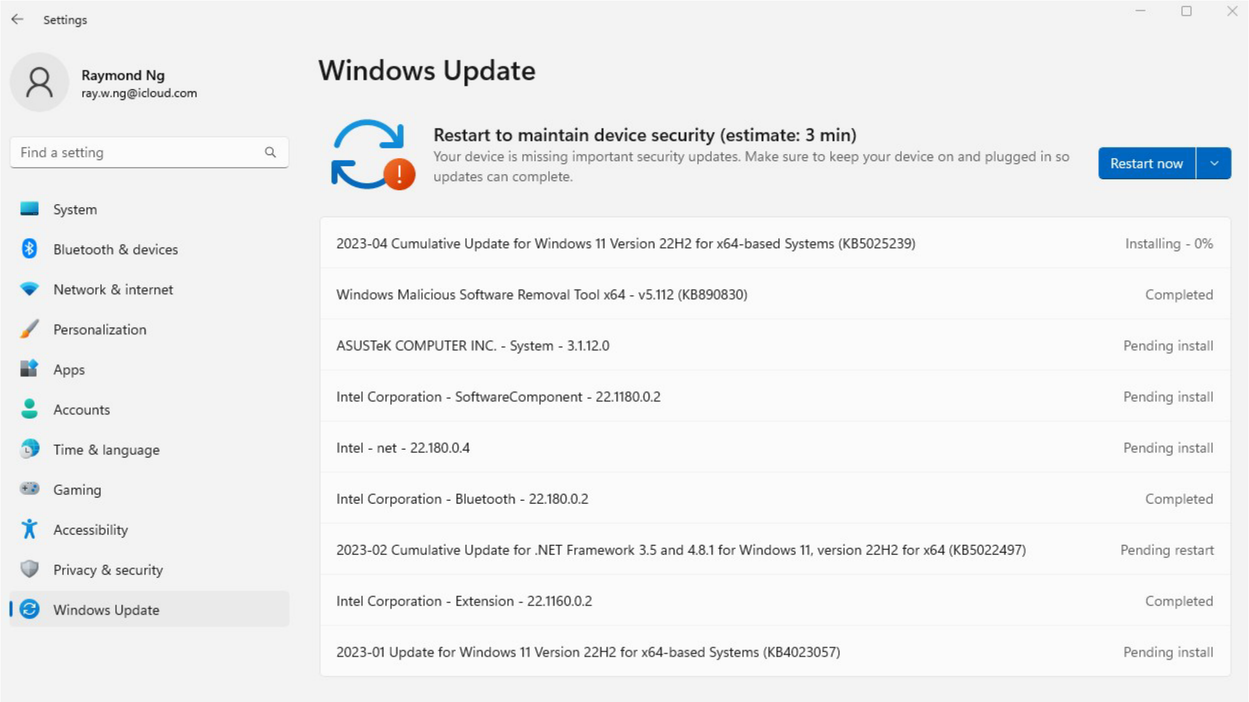
Send a "Do Not Track" request with your browsing traffic

Preload pages for faster browsing and searching
Preloads pages that Chrome thinks you might visit. To do this, Chrome may use cookies, if you allow

Operating System Hardening

Update and Patch Operating System

To ensure my PC's software is up-to-date. I went to 'Settings' >> 'Windows Update'. Next, I clicked 'Check for updates'. In the screenshot below my PC began performing all necessary updates.



Windows Update

Restart to maintain device security (estimate: 3 min)

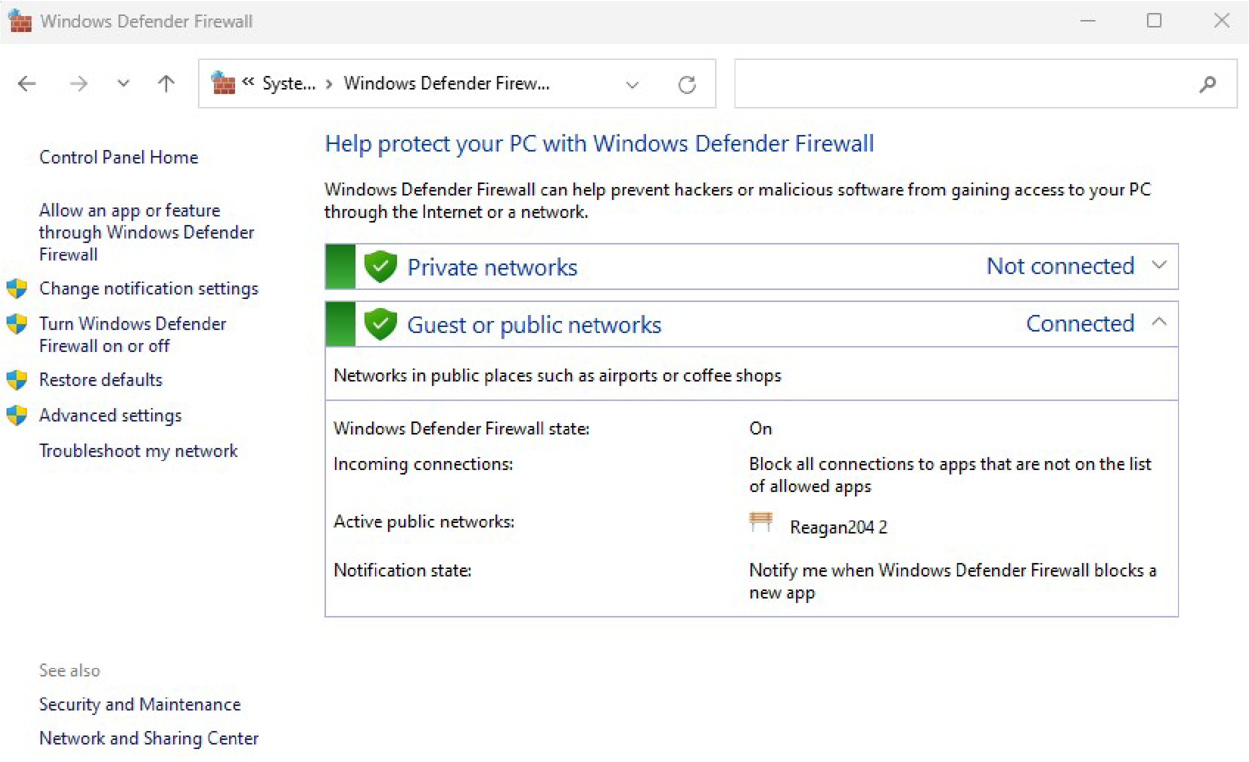
Your device is missing important security updates. Make sure to keep your device on and plugged in so updates can complete.

2023-04 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems (KB5025239)	Installing - 0%
Windows Malicious Software Removal Tool x64 - v5.112 (KB890830)	Completed
ASUSTeK COMPUTER INC. - System - 3.1.12.0	Pending install
Intel Corporation - SoftwareComponent - 22.1180.0.2	Pending install
Intel - net - 22.180.0.4	Pending install
Intel Corporation - Bluetooth - 22.180.0.2	Completed
2023-02 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 22H2 for x64 (KB5022497)	Pending restart
Intel Corporation - Extension - 22.1160.0.2	Completed
2023-01 Update for Windows 11 Version 22H2 for x64-based Systems (KB4023057)	Pending install

Audit/Logging File Hardening

Set Up Firewall Profiles

To enable my PC’s Firewall (Windows Defender), I opened the ‘Control Panel’. Next, I clicked on ‘System and Security’ >> ‘Windows Defender Firewall’.


Windows Defender Firewall
« Syste... › Windows Defender Firew...
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

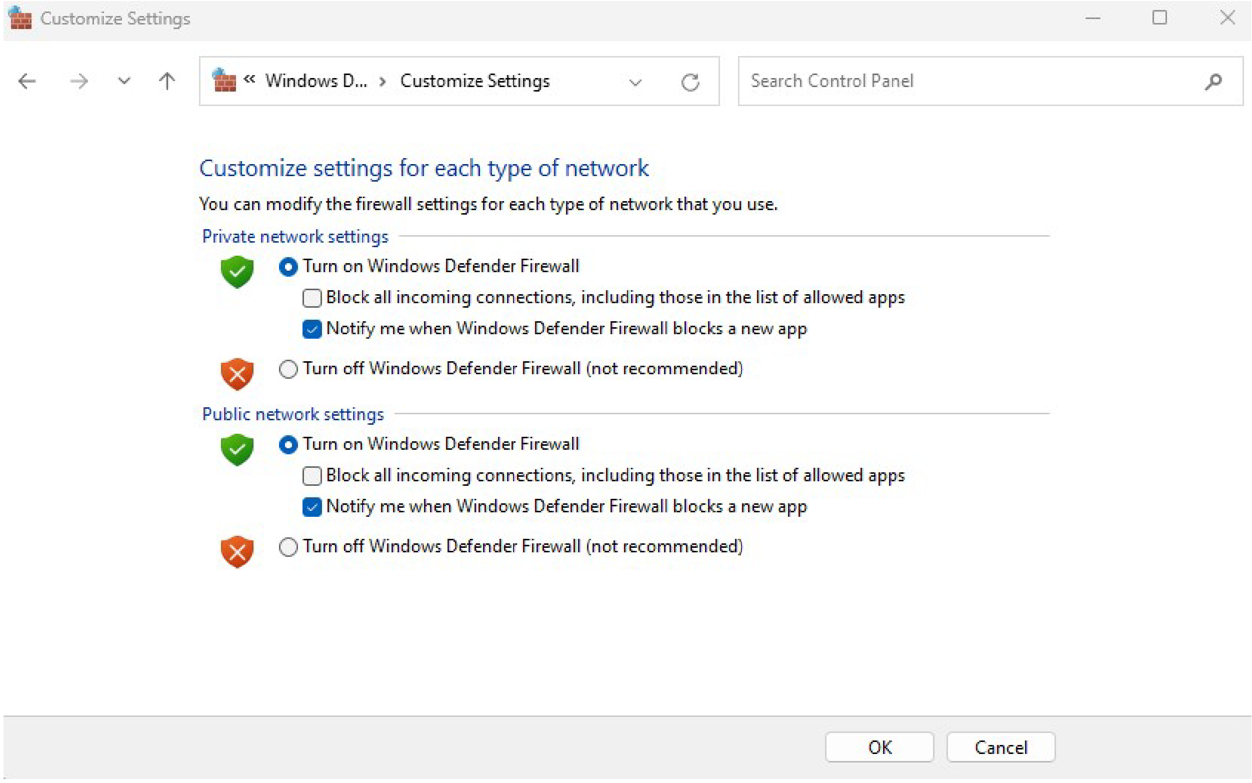
Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Reagan204 2
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Next, I clicked on ‘Turn Windows Firewall on or off’. My Windows Defender Firewall was already on for both ‘Private network settings’ and ‘Public network settings’. Additionally, I left the ‘Notify me when Windows Defender Firewall blocks a new app’ function checked.



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Public network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

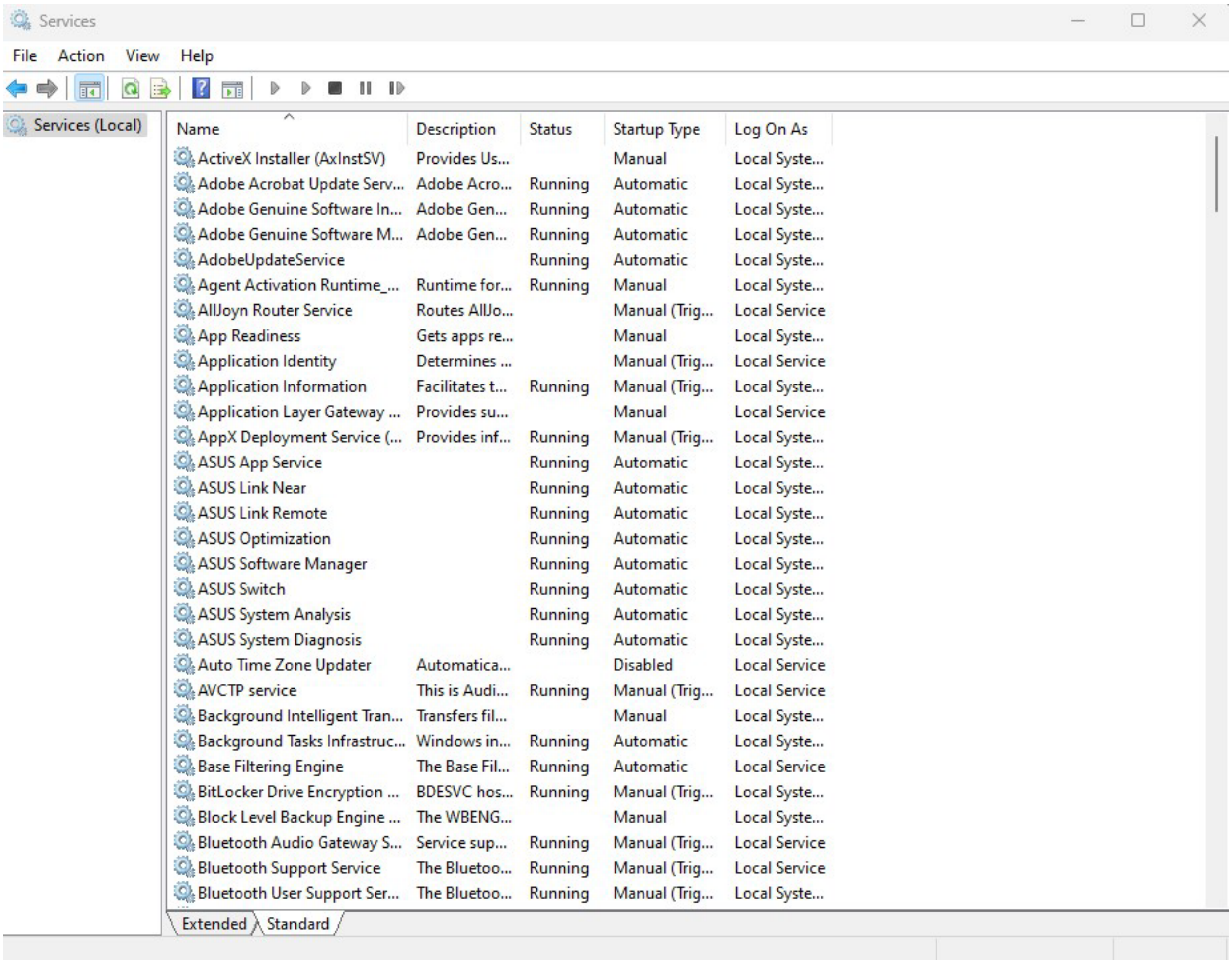
☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Application Hardening

Disable Unneeded Services

To disable/stop any services/applications from running on my PC I can simply go to the ‘Settings’ application. Here, I can stop and pause any service/application running.



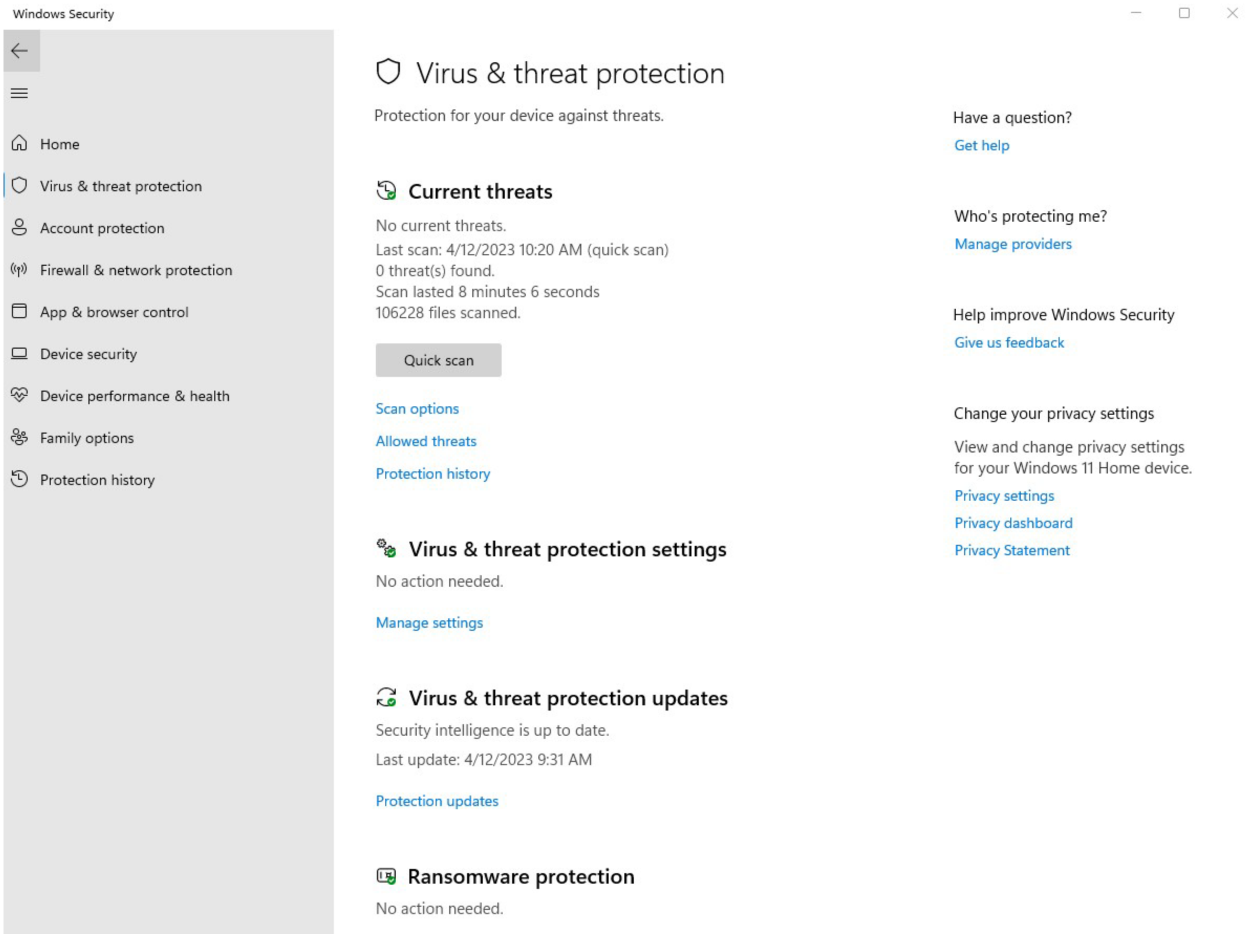
Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
Adobe Acrobat Update Serv...	Adobe Acro...	Running	Automatic	Local Syste...
Adobe Genuine Software In...	Adobe Gen...	Running	Automatic	Local Syste...
Adobe Genuine Software M...	Adobe Gen...	Running	Automatic	Local Syste...
AdobeUpdateService		Running	Automatic	Local Syste...
Agent Activation Runtime_...	Runtime for...	Running	Manual	Local Syste...
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Local Service
App Readiness	Gets apps re...		Manual	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
AppX Deployment Service (...	Provides inf...	Running	Manual (Trig...	Local Syste...
ASUS App Service		Running	Automatic	Local Syste...
ASUS Link Near		Running	Automatic	Local Syste...
ASUS Link Remote		Running	Automatic	Local Syste...
ASUS Optimization		Running	Automatic	Local Syste...
ASUS Software Manager		Running	Automatic	Local Syste...
ASUS Switch		Running	Automatic	Local Syste...
ASUS System Analysis		Running	Automatic	Local Syste...
ASUS System Diagnosis		Running	Automatic	Local Syste...
Auto Time Zone Updater	Automatica...		Disabled	Local Service
AVCTP service	This is Audi...	Running	Manual (Trig...	Local Service
Background Intelligent Tran...	Transfers fil...		Manual	Local Syste...
Background Tasks Infrastruc...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
BitLocker Drive Encryption ...	BDESVC hos...	Running	Manual (Trig...	Local Syste...
Block Level Backup Engine ...	The WBENG...		Manual	Local Syste...
Bluetooth Audio Gateway S...	Service sup...	Running	Manual (Trig...	Local Service
Bluetooth Support Service	The Bluetoo...	Running	Manual (Trig...	Local Service
Bluetooth User Support Ser...	The Bluetoo...	Running	Manual (Trig...	Local Syste...

I did not need to disable/stop any services for this lab because I had already done so for another class. However, if need to disable any programs I can visit the Settings app to stop/disable services/applications.

Anti-Virus Hardening

Install and Updating an Antivirus

To check my PC’s ‘Virus & threat protection’, I opened up ‘Windows Security’. Next, I clicked on ‘Virus & threat protection’. Here I observed that my existing antivirus is active and up-to-date.



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 4/12/2023 10:20 AM (quick scan)
0 threat(s) found.
Scan lasted 8 minutes 6 seconds
106228 files scanned.

Virus & threat protection settings

No action needed.

Virus & threat protection updates

Security intelligence is up to date.

Last update: 4/12/2023 9:31 AM

Ransomware protection

No action needed.

Have a question?

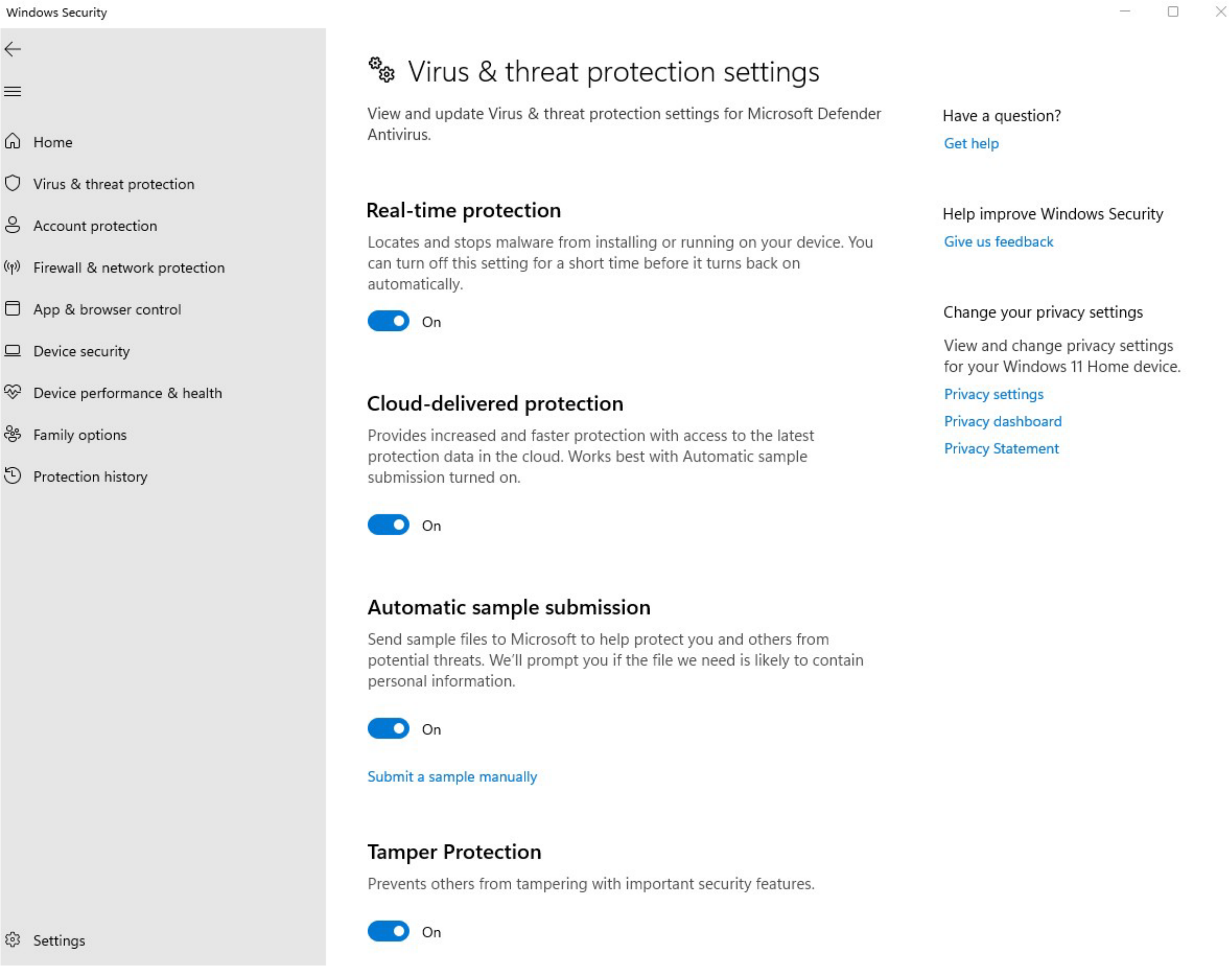
Who's protecting me?

Help improve Windows Security

Change your privacy settings

View and change privacy settings for your Windows 11 Home device.

Next, I clicked on ‘Manage settings’ under ‘Virus & threat protection settings’. Here, I ensured all the necessary functions (protections) were on.



Windows Security

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

On

Submit a sample manually

Tamper Protection

Prevents others from tampering with important security features.

On

Have a question?

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 11 Home device.

Privacy settings

Privacy dashboard

Privacy Statement

Physical Hardening

Limit the Physical Access of a Host

My computers are safeguarded in my home office, inside my house that is persistently monitored by smart security cameras. Moreover, I am the only one that has access to my computer system, and they are all password protected. I do not share access with anyone. Not even my spouse. Below is a snapshot of my home office setup.

References

Babu, S. (2022, November 26). *How to Prevent Remote Access Trojan Attacks and Stay in Control of Your PC*. Retrieved from https://www.makeuseof.com/how-to-prevent-remote-access-trojan-attacks/

Bhardwaj, P. (2022, September 8). *What Are the Risks of Remote Computer Access?* Retrieved from https://www.makeuseof.com/remote-access-risks/

Cybersecurity and Infrastructure Security Agency (CISA). (2019, September 27). *Understanding Anti-Virus Software*. Retrieved from https://www.cisa.gov/news-events/news/understanding-anti-virus-software

De Groot, J. (2023, February 8). *What is Data Loss Prevention (DLP)? Definition, Types & Tips*. Retrieved from https://www.digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

Dodt, C. (2020, July 7). *Cookies: An overview of associated privacy and security risks*. Retrieved from https://resources.infosecinstitute.com/topic/cookies-an-overview-of-associated-privacy-and-security-risks/

National Institute of Sandards and Technology (ITL). (n.d.). *An Overview of Issues in Testing Intrusion Detection*. Retrieved from https://www.govinfo.gov/content/pkg/GOVPUB-C13-12311f1b97702aad61bee4378916ab9e/pdf/GOVPUB-C13-12311f1b97702aad61bee4378916ab9e.pdf

Kaspersky. (2023). *What are Cookies?* Retrieved from https://www.kaspersky.com/resource-center/definitions/cookies

Martens, B. (2023). *What Are Antivirus False Positives & How to Fix Them in 2023?* Retrieved from https://www.safetydetectives.com/blog/what-are-antivirus-false-positives-how-to-fix-them/

Microsoft. (2021, January 7). *Registry Key Security and Access Rights*. Retrieved from https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry-key-security-and-access-rights

Microsoft. (2023). *Device encryption in Windows*. Retrieved from Microsoft.com: https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d

Prakash, M. (2023, January 29). *What is Firewall and How does it Work?* Retrieved from https://www.knowledgehut.com/blog/security/firewall-in-cyber-security

Rosencrance, L. (2023). *10 types of security incidents and how to handle them*. Retrieved from https://www.techtarget.com/searchsecurity/feature/10-types-of-security-incidents-and-how-to-handle-them

Wright, C., & Zadok, E. (2003, September 24). *Cryptographic File Systems Performance: What You Don't Know Can Hurt You*. Retrieved from https://www.filesystems.org/docs/nc-perf/index.html