Choose any OS (Windows or Linux) and do hardening on it (You need to identify 7 items, Explain it and configure it)

Configuration of operating system and removing unnecessary applications to minimize the computer's exposure to threats is called OS Hardening.

Importance of OS hardening: Removal of attack vectors and freezing the computer's attack surface to reduce security risks. The main goal is to limit the security weaknesses and vulnerabilities which can be used by the attackers to attack.

Windows Hardening performed on Windows 11.

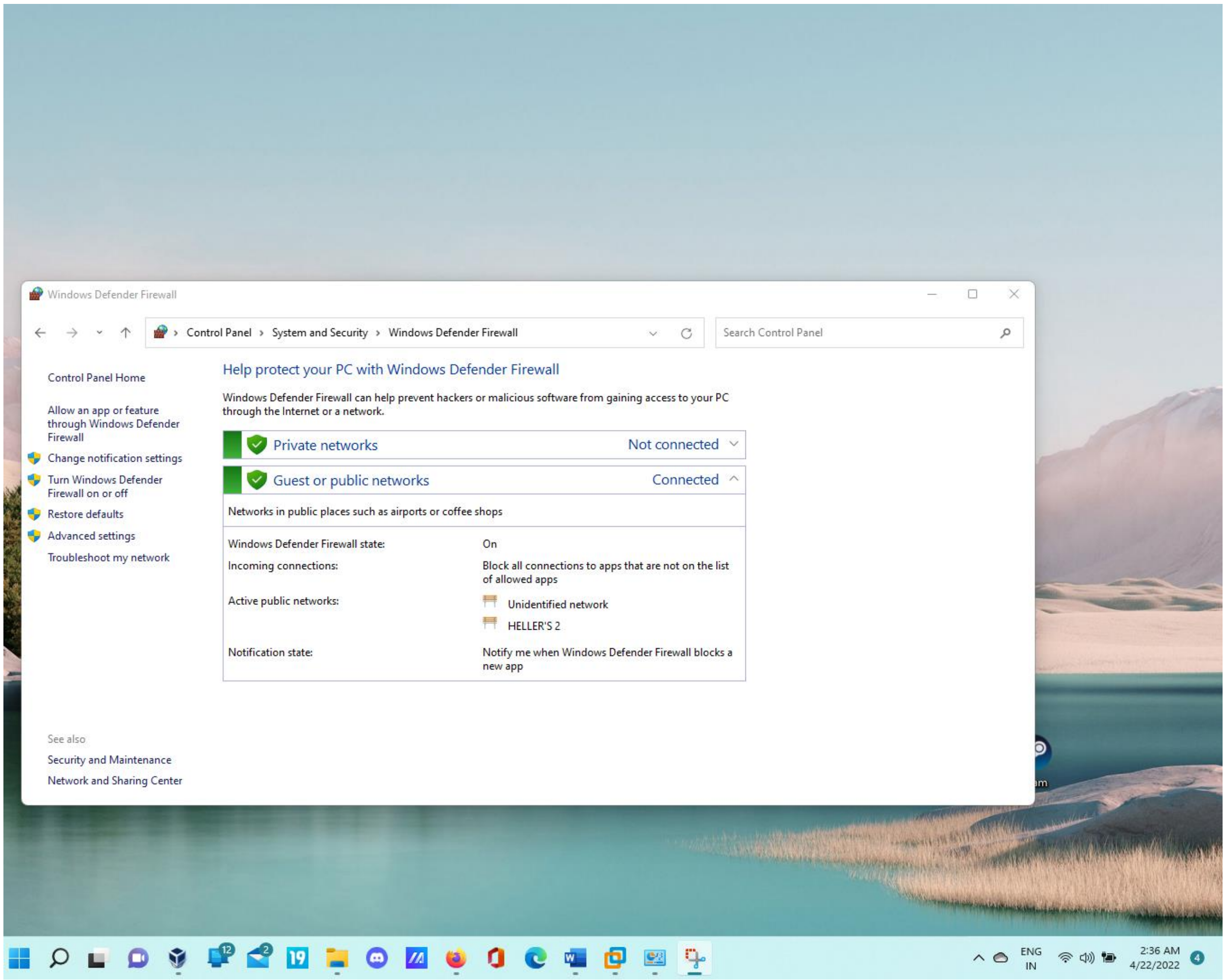
1 Turn on Firewall.

Firewall is an already installed network security system whose main purpose is to shutout unauthorized access to or from your network.

Whenever the firewall is active it will examine all the messages entering or leaving the intranet and allow it to drop or pass depending on the security criteria.

To Turn on Firewall:

Click on Search box-> Control Panel-> System and security-> Windows Defender Firewall.



Windows Defender Firewall
Control Panel > System and Security > Windows Defender Firewall
Search Control Panel
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
ENG
IN
2:36 AM
4/22/2022

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:	Unidentified network HELLER'S 2
Notification state:	Notify me when Windows Defender Firewall blocks a new app

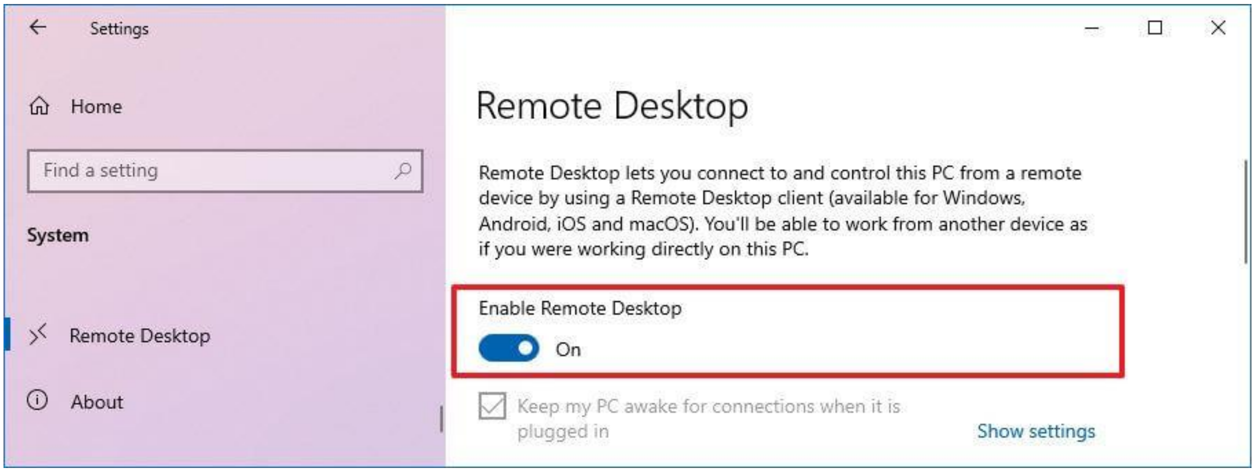
2 Disable Remote Access:

The process in which any computer can connect to my computer remotely over a network is called Remote Access. Once gaining the access the person will be able to perform any function he can. He can install malware or even stole your personal data.

To disable Remote Access

Click on Search button->Remote Desktop settings-> Disable Remote Desktop

Note: Windows 11 home does not support Remote Desktop but below is the image in which it explains how to enable disable Remote Desktop.



Remote Desktop

Remote Desktop lets you connect to and control this PC from a remote device by using a Remote Desktop client (available for Windows, Android, iOS and macOS). You'll be able to work from another device as if you were working directly on this PC.

Enable Remote Desktop

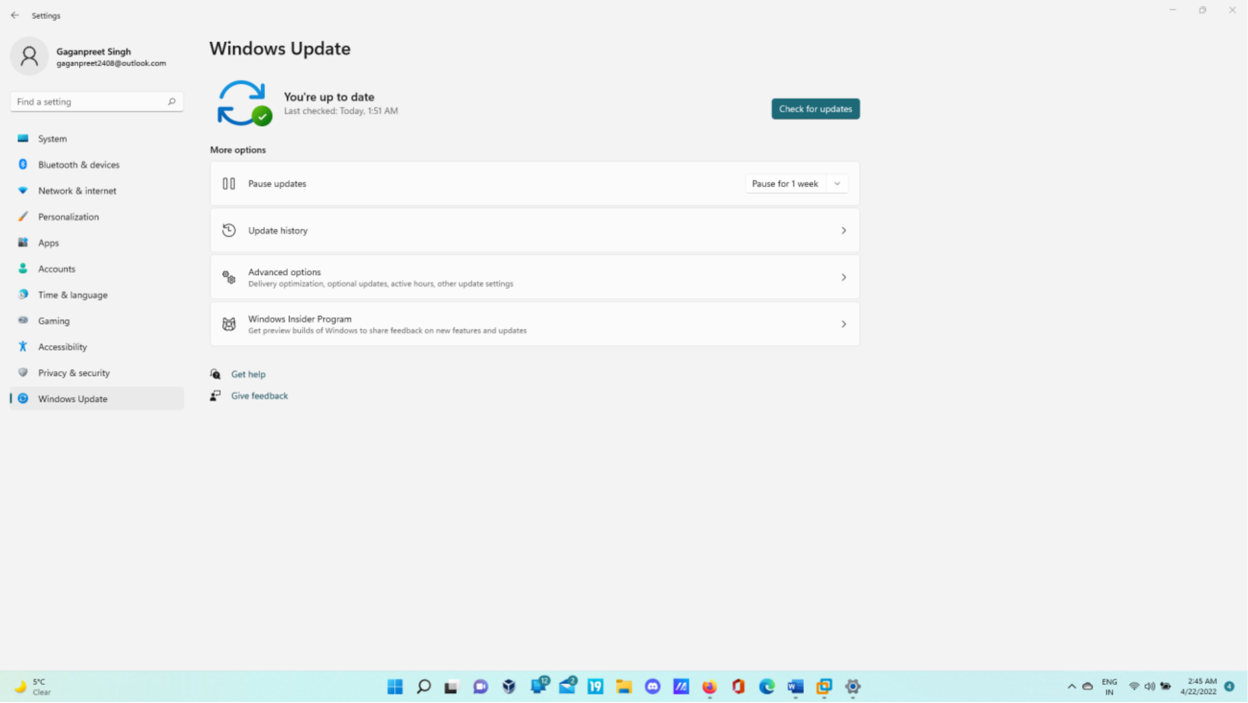
● On

☑ Keep my PC awake for connections when it is plugged in

3 Operating System auto-updates Enabling

Always keep this feature enabled, whenever patches are released, it would always increase your OS Security.

- To navigate to windows update-> Search settings-> Navigate to windows update
- Click on Check for updates and install any updates.



Windows Update

You're up to date
Last checked: Today, 1:51 AM

More options

Pause updates — Pause for 1 week

Update history

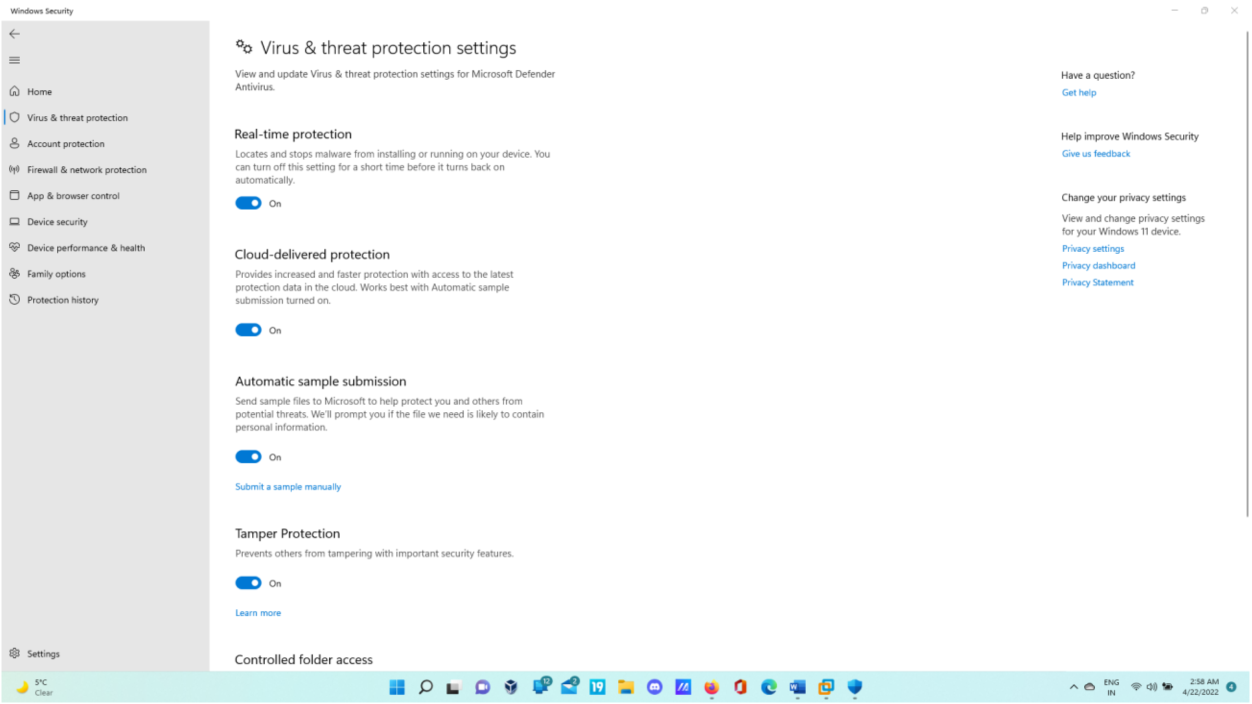
Advanced options
Delivery optimization, optional updates, active hours, other update settings

Windows Insider Program
Get preview builds of Windows to share feedback on new features and updates

4 Enable Antivirus tools

Our system is at risk from viruses and malwares, which we can stop by enabling Windows Defender. This is inbuilt in your windows.

- Navigate to Virus and Threat Protection under Windows Security and turn on Real time protection, cloud-delivered protection, automatic sample submission and tamper protection as shown in the image below.



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

Learn more

Controlled folder access

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 device.

Privacy settings
Privacy dashboard
Privacy Statement

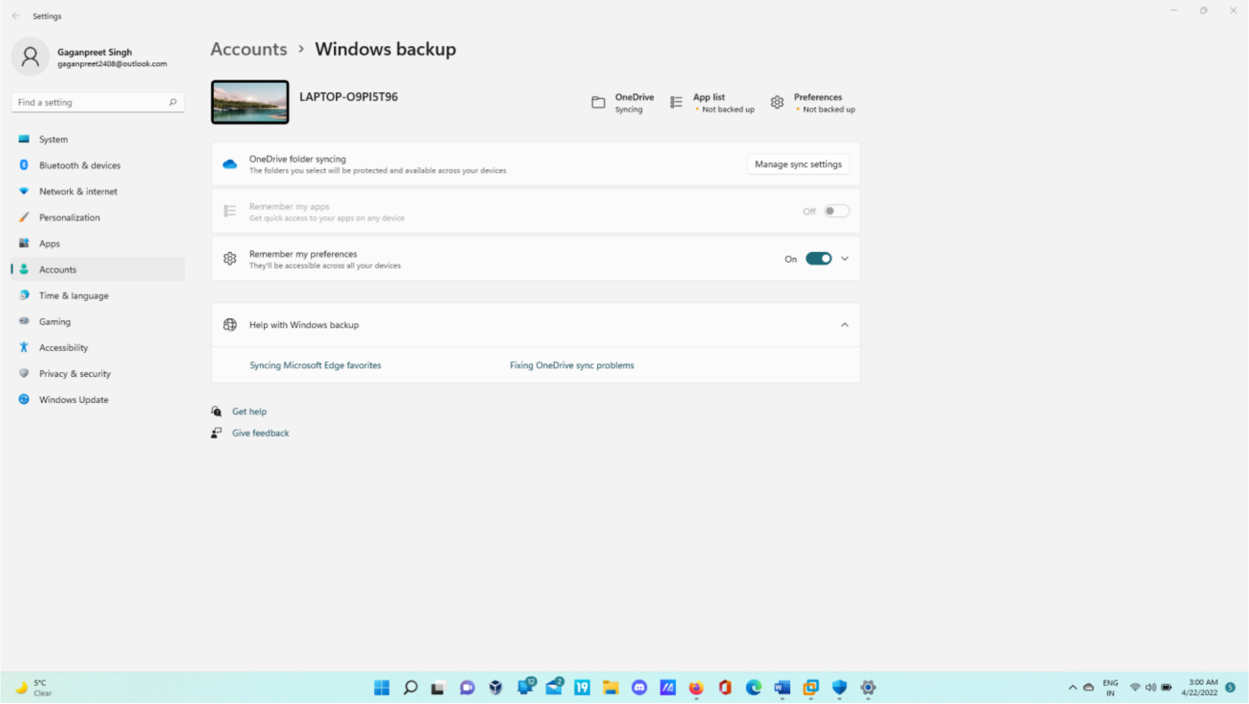
5 Enable File backups

To prevent loss of sensitive and critical data during hardware failures one must enable file backups:

There are 3 ways we can perform backups:

- Backup to the cloud
- Recovery drives creation which can be used to restore system if some mishap happens.
- File history to help backup important and sensitive files

To backup files to the cloud navigate to windows backup under accounts in settings tab and select the files or folders you need to backup.



Accounts › Windows backup

LAPTOP-O9PI5T96

OneDrive: Syncing — App list: Not backed up — Preferences: Not backed up

OneDrive folder syncing
The folders you select will be protected and available across your devices

Remember my apps — Off
Get quick access to your apps on any device

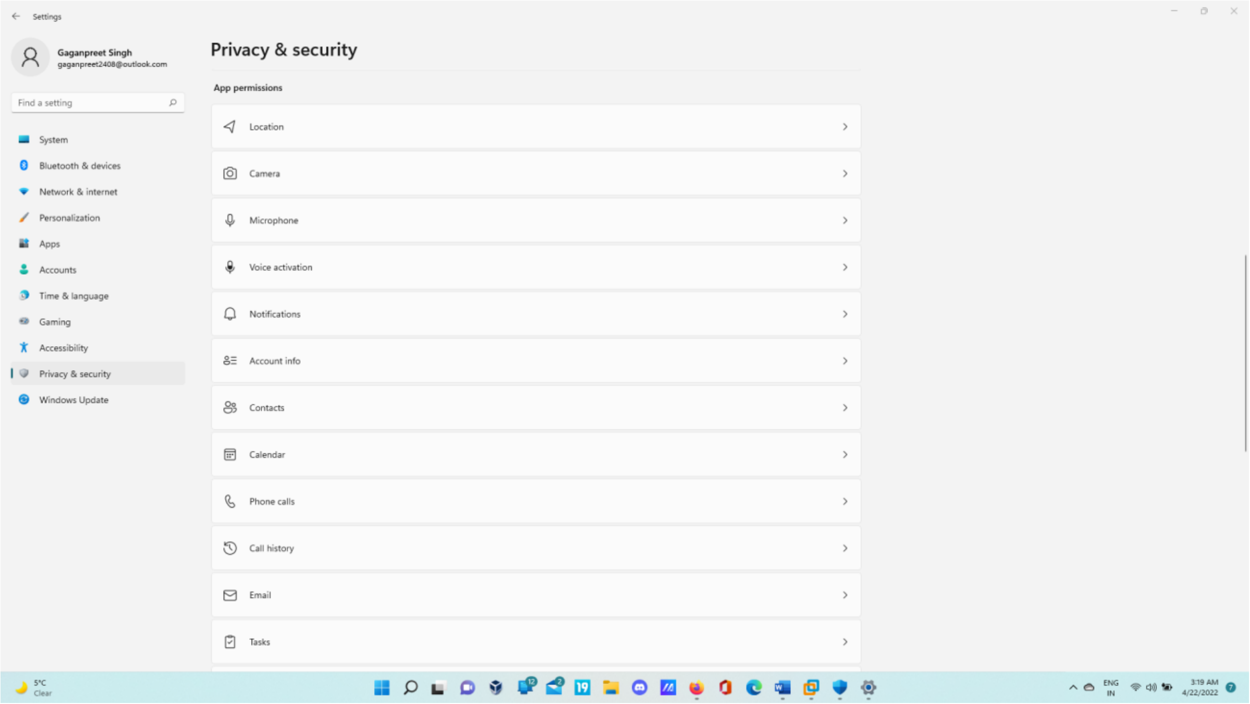
Remember my preferences — On
They'll be accessible across all your devices

Help with Windows backup
Syncing Microsoft Edge favorites
Fixing OneDrive sync problems

6 Manage Application Permissions

To check which application is using permissions of camera, location and microphone is necessary. Unwanted apps can tack the locations and provide data to untrusted sources. Make sure only trusted and necessary apps have the correct access.

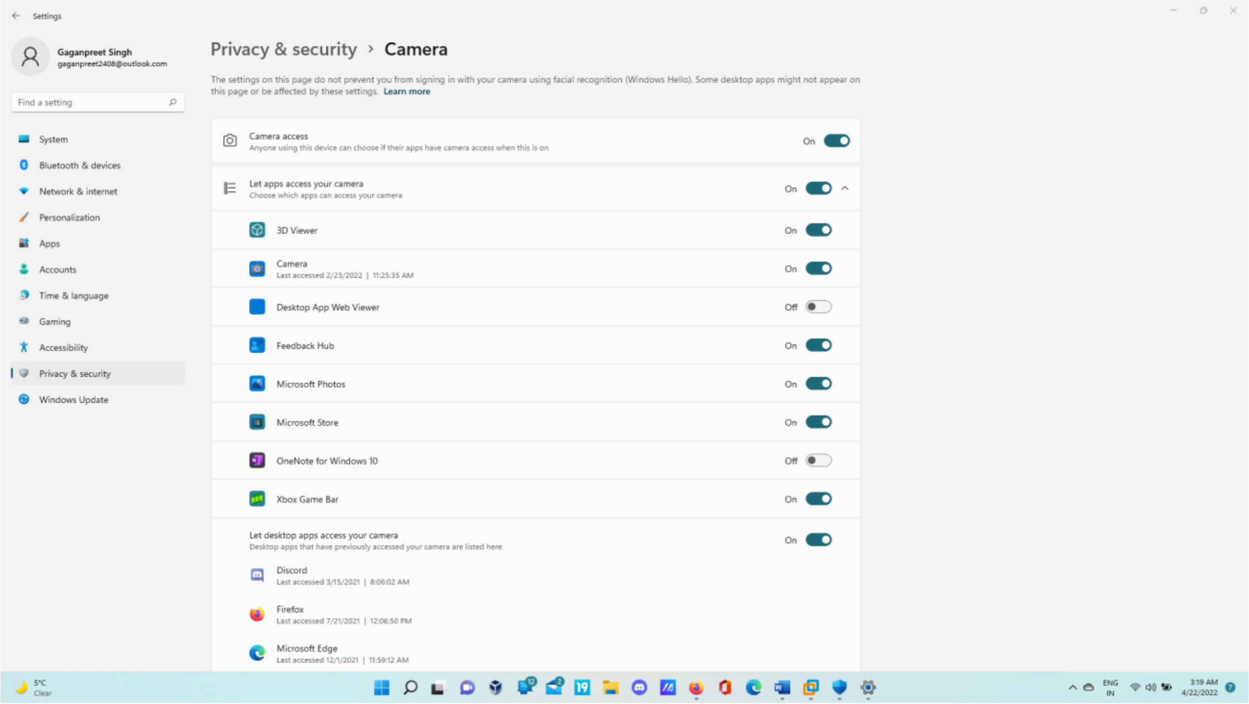
To manage application preferences, Navigate to Privacy and security and scroll down to permissions. Select which permission you want to change access for a application or software.



Privacy & security

App permissions

- Location
- Camera
- Microphone
- Voice activation
- Notifications
- Account info
- Contacts
- Calendar
- Phone calls
- Call history
- Email
- Tasks



Privacy & security › Camera

The settings on this page do not prevent you from signing in with your camera using facial recognition (Windows Hello). Some desktop apps might not appear on this page or be affected by these settings. Learn more

Camera access
Anyone using this device can choose if their apps have camera access when this is on — On

Let apps access your camera
Choose which apps can access your camera — On

3D Viewer	On
Camera Last accessed 2/23/2022 | 11:25:35 AM	On
Desktop App Web Viewer	Off
Feedback Hub	On
Microsoft Photos	On
Microsoft Store	On
OneNote for Windows 10	Off
Xbox Game Bar	On

Let desktop apps access your camera
Desktop apps that have previously accessed your camera are listed here — On

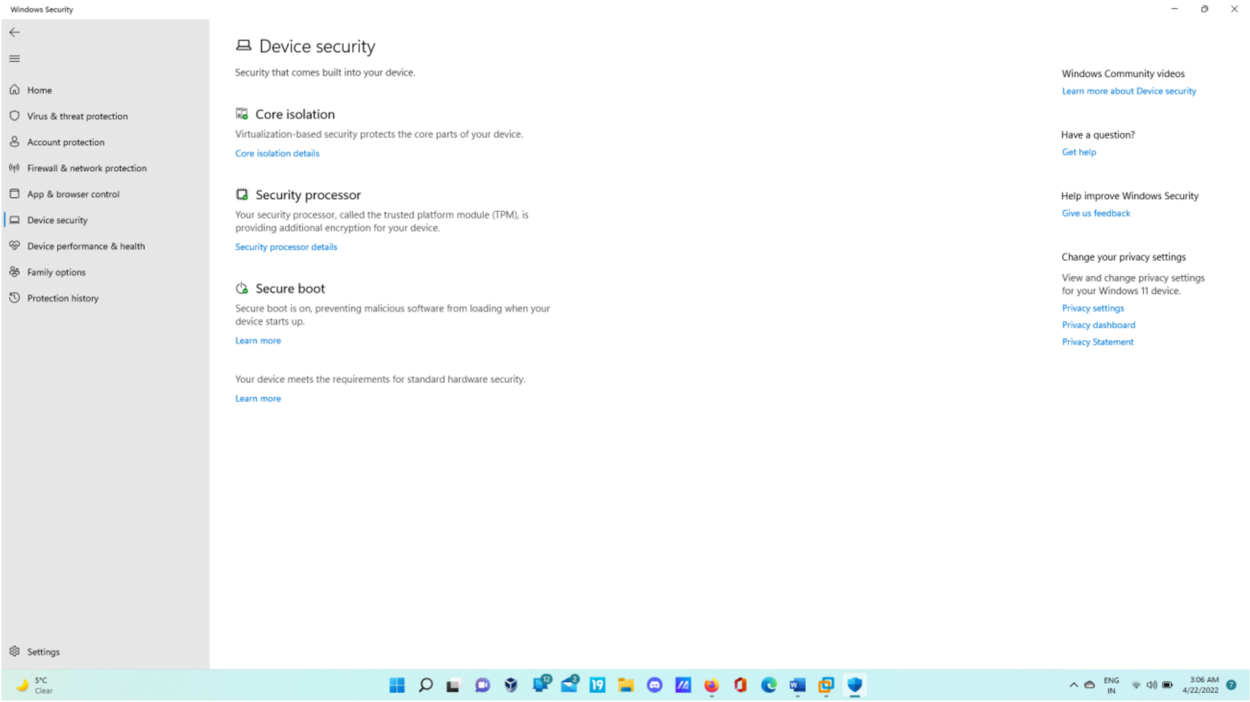
Discord
Last accessed 3/15/2021 | 8:06:02 AM

Firefox
Last accessed 7/21/2021 | 12:06:50 PM

Microsoft Edge
Last accessed 12/1/2021 | 11:59:12 AM

7 Secure Boot

Secure boot stops any malicious code runs when your system is starting up. It is a security standard. Make sure it is on in your Security tab.



Device security

Security that comes built into your device.

Core isolation

Virtualization-based security protects the core parts of your device.

Core isolation details

Security processor

Your security processor, called the trusted platform module (TPM), is providing additional encryption for your device.

Security processor details

Secure boot

Secure boot is on, preventing malicious software from loading when your device starts up.

Learn more

Your device meets the requirements for standard hardware security.

Learn more

Windows Community videos

Learn more about Device security

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 device.

Privacy settings

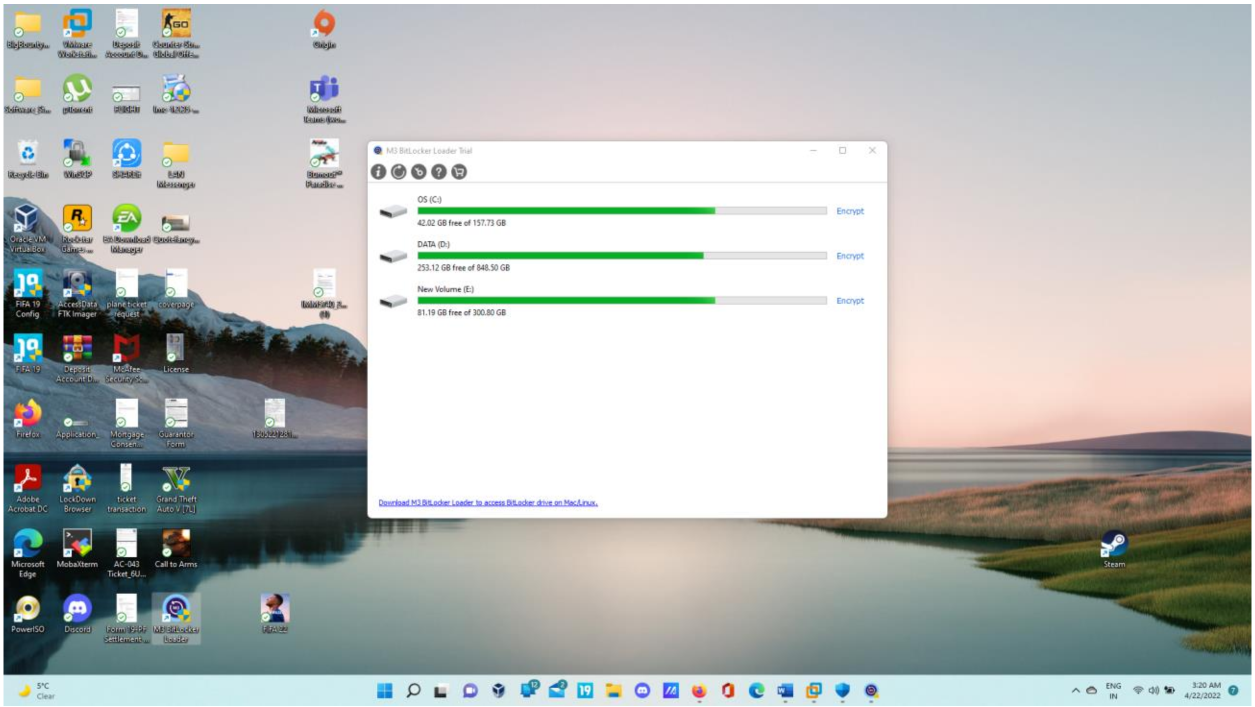
Privacy dashboard

Privacy Statement

8 Turn on Encryption

Encryption is a technique in which we can lock our data with a key and no one would be able to access it without the key. Only the authorized users will be able to change, view or delete data. In windows 11 we can perform disk encryption with the help of BitLocker tool which is free.

Unfortunately, Windows 11 home does not support BitLocker but you can encrypt your files using M3 BitLocker Loader application to encrypt your files.



M3 BitLocker Loader Trial

OS (C:)
42.02 GB free of 157.73 GB
Encrypt

DATA (D:)
253.12 GB free of 848.50 GB
Encrypt

New Volume (E:)
81.19 GB free of 300.80 GB
Encrypt

Download M3 BitLocker Loader to access BitLocker drive on Mac/Linux.