Continue

Please wait while your request is being verified... Securing Windows 11 involves a few straightforward steps to protect your computer from threats. Start by keeping your system up-to-date with the latest updates, enabling built-in security features like Windows Defender, and setting up robust account passwords. Also, adjust privacy settings for better control over your data. By following these steps, you will enhance your computers security, ensuring your personal information and files are safe. Securing your Windows 11 system is crucial to protect your data from cyber threats. Heres a step-by-step guide on how to do just that. Make sure Windows 11 is always updated with the latest security patches. Updating Windows ensures that you have the latest security features and bug fixes. To check for updates, go to Settings > Update & Security > Windows Update. Click on Check for updates and let Windows do its magic. This simple action can prevent many security vulnerabilities. Turn on Windows Defender to safeguard your system against viruses and malware. Windows Defender is a built-in antivirus program that provides real-time protection. To enable it, navigate to Settings > Update & Security > Windows Security > Virus & threat protection. Ensure that all protection settings are on. Windows Defender will continuously monitor your system for threats. Create robust passwords for your accounts to prevent unauthorized access. Use a mix of letters, numbers, and symbols to create strong passwords. Avoid using easily guessed information like birthdays. Consider using a password manager to generate and store passwords securely. Strong passwords are your first defense against hackers. Customize privacy settings to control what information is shared. In Settings > Privacy & Security, you can manage what data apps can access and what information is shared with Microsoft. Review these settings to ensure youre not oversharing. By tweaking these settings, you enhance your privacy and control over personal information. Use BitLocker to encrypt your data for added security. BitLocker encrypts your hard drive, making it difficult for unauthorized users to access your files. To activate it, go to Control Panel > System and Security > BitLocker Drive Encryption, and follow the instructions. This feature is especially useful for laptops and other portable devices. Once youve completed these steps, your Windows 11 system will be much more secure. You can rest easy knowing that your personal information and files are better protected. Regularly back up important files to prevent data loss in case of a breach. Avoid clicking on suspicious links or downloading unknown attachments. Use a reliable VPN for secure internet connections. Set up two-factor authentication for your accounts if available. Regularly review and remove unused apps and software. Its important to check for updates regularly, ideally once a week. Automatic updates can also be set to ensure you never miss critical security patches. Windows Defender offers decent protection for most users, but adding an additional layer of security with third-party antivirus software can be beneficial. A strong password is typically at least 12 characters long and includes a mix of uppercase and lowercase letters, numbers, and symbols. BitLocker is available in Windows 11 Pro, Enterprise, and Education editions. It is not available in the Home edition. Go to Settings > Privacy & Security > App permissions to review and adjust what information each app can access. Keep Windows Updated. Enable Windows Defender. Set Strong Passwords. Adjust Privacy Settings. Activate BitLocker. Securing Windows 11 is not only about keeping your system running smoothly but also about safeguarding your digital life from potential threats. Whether youre surfing the web, downloading your favorite apps, or storing sensitive information, these security measures act like a virtual fortress around your data. Think of it as building a moat around your castle. Regular updates and Windows Defender are your first line of defense. Strong passwords act like the castles drawbridge, while privacy settings and BitLocker provide added layers of protection. In todays digital world, threats are as common as mosquitoes on a summer night. But by following these steps, youre swatting them away before they even get close. Keep your system updated, stay aware of potential threats, and regularly review your security settings. For further reading, consider exploring Microsofts Advanced Threat Protection features or third-party security tools that complement Windows Defender. Staying informed and proactive will ensure that your digital life remains secure in the ever-evolving world of technology.Matthew Burleigh has been writing tech tutorials since 2008. His writing has appeared on dozens of different websites and been read over 50 million times.After receiving his Bachelors and Masters degrees in Computer Science he spent several years working in IT management for small businesses. However, he now works full time writing content online and creating websites.His main writing topics include iPhones, Microsoft Office, Google Apps, Android, and Photoshop, but he has also written about many other tech topics as well.Read his full bio here.On Windows 11 (and 10), the "Windows Security" app provides a user-friendly interface and tools to manage common security features. For example, the experience includes the Microsoft Defender Antivirus, which offers real-time protection for your computer and data against viruses and many other kinds of malware.You can also manage the Microsoft Defender Firewall to block intruders from sneaking in. With the account protection settings, you can monitor the device's performance and health, as well as your account and sign-in information, and you can access even more advanced features to keep everything a little more secure.In this how-to guide, I will explain the steps to start using and perform everyday tasks with the security app to keep your system and data safe from malware and hackers.You may like Windows Security vs. Microsoft Defender AntivirusBefore diving into this guide, you must understand the difference between "Microsoft Defender Antivirus" and "Windows Security."Windows Security is an app that offers a unified interface for viewing the status and managing security features, such as antivirus, firewall, performance, and others.On the other hand, Microsoft Defender Antivirus is the default anti-malware engine that offers real-time protection against many forms of malware, including viruses, spyware, ransomware, and hackers.Also, when you install another third-party antivirus, the system will disable the Microsoft Defender Antivirus automatically, but this will not affect the functionality of the Windows Security app. In the same way, disabling Microsoft Defender Antivirus or Microsoft Defender Firewall will not disable Windows Security.All the latest news, reviews, and guides for Windows and Xbox diehards.How to navigate Windows SecurityWindows Security is a straightforward application. You can open it from the Start menu or double-clicking the shield icon from the notification area in the Taskbar.(Image credit: Mauro Huculak)On the "Home" page, you can view the security status of the different protection features available by default on Windows 11 and 10. You can also see alerts of any action that needs to be taken to keep your computer secure.The shield icon in the notification area can also alert you when an action needs to be taken. If there is more than one alert, only the most severe warning will appear. Also, if you right-click the app icon, you'll have access to actions, such as quick scan, download updates, adjust notifications, and access the dashboard.(Image credit: Mauro Huculak)Windows Security includes eight areas of protection that you can manage and monitor:Virus & threat protection: This section houses the Microsoft Defender Antivirus settings. It allows you to monitor malware protection, scan the device for threats, launch an offline scan, and set up the advanced anti-ransomware feature.Account protection: Allows you to see how to protect your identity on Windows 11 or 10.Firewall & network protection: This feature lets you monitor network connections and configure various Microsoft Defender Firewall settings.App & browser control: This section includes the settings to help you protect your device and data from malicious code hidden in apps, files, and websites.Device security: This area provides hardware-level security features, such as Core isolation and Security processor, to protect your computer from certain attacks.Device performance & health: This section displays your computer's health and performance report.Family options: This area offers easy access to manage your devices and kids' online experience using a Microsoft account.Protection history: This section gives you quick access to the latest actions and recommendations from the security feature.How to scan computer for malware using Microsoft Defender AntivirusWindows automatically updates and scans the device for malware regularly, but you can perform different scans manually.Quick virus scanA quick scan happens fast and only scans the parts of the system where malware is known to hide.To start a virus scan with Microsoft Defender, use these steps:Open Windows Security.Click on Virus & threat protection.Click the Quick scan button.(Image credit: Mauro Huculak)Once you complete the steps, under the "Current threats" section, you'll find any detected threats, as well as the time it took to complete the scan and the number of scanned files.If you suspect that a virus is still on your computer, you should try to perform a full scan.Full virus scanA full virus scan takes longer, but it makes sure to check every file, folder, and application.To start a full virus scan with Microsoft Defender, use these steps:Open Windows Security.Click on Virus & threat protection.Click the Scan options option under the "Current threats" section.(Image credit: Mauro Huculak)Select the Full scan option.(Image credit: Mauro Huculak)Click the Scan now button.After you complete the steps, you can continue using the device, while the antivirus will perform a full scan to detect any potential malware.Custom virus scanIf you only want to scan a particular folder or location, the Windows antivirus includes an option to complete a custom scan.To perform a custom virus scan, use these steps:Open Windows Security.Click on Virus & Threat Protection.Click the Scan options option under the "Current threats" section.(Image credit: Mauro Huculak)Select the Custom scan option.(Image credit: Mauro Huculak)Click the Scan now button.Select the location to be scanned.Click the Select Folder button.Alternatively, you can just right-click on Windows 10 (or shift + right-click on Windows 11) a drive, folder, or file and select the "Scan with Microsoft Defender" option from the context menu to perform a custom scan.Offline virus scanSometimes, if you're dealing with a tough virus or another type of malware, the antivirus software may be unable to remove it while the operating system is running. If so, you can use Microsoft Defender to perform an offline scan. When using this feature, the computer will restart automatically in the Windows Recovery Environment (WinRE) and perform a full scan before the operating system starts.To start an offline virus scan, use these steps:Open Windows Security.Click on Virus & threat protection.Click the Scan options option under the "Current threats" section.(Image credit: Mauro Huculak)Select the "Microsoft Defender Offline scan" option.(Image credit: Mauro Huculak)Click the Scan now button.Click the Scan button.Once you complete the steps, the device will restart and boot into a standalone version of the Microsoft Defender Antivirus, which will scan the entire machine. If malicious code is detected, it will be removed or quarantined automatically.After the scan, the device will restart, and you can view a report in the Windows Security app.How to view protection history using Microsoft Defender AntivirusMicrosoft Defender Antivirus also includes an area that you can view the latest protection actions and recommendations.To view protection history, use these steps:Open Windows Security.Click on Virus & threat protection.Click the Protection history option.(Image credit: Mauro Huculak)Click the "Filters" drop-down menu and select the history you want to review, including:Recommendations.Quarantined items.Cleaned items.Blocked actions.Severity.After you complete the steps, a report will be generated with items that have been removed, cleaned, or are still waiting for action.How to temporarily disable Microsoft Defender AntivirusIt's not recommended to use a device without malware protection, but sometimes, the antivirus can prevent you from installing an app or update. If so, you can temporarily disable the antivirus to complete the installation.To disable Microsoft Defender Antivirus on Windows, use these steps:Open Windows Security.Click on Virus & threat protection.Click the Manage settings option under the "Virus & threat protection settings" section.(Image credit: Mauro Huculak)Turn off the "Real-time protection" toggle switch.(Image credit: Mauro Huculak)Once you complete the steps, you can perform tasks that may conflict with the antivirus. If you don't re-enable the antivirus, it'll restart automatically the next time you reboot your computer.How to enable anti-ransomware using Microsoft Defender AntivirusMicrosoft Defender Antivirus includes a feature known as Controlled folder access, designed to monitor and protect your data against ransomware attacks and unwanted changes from malicious programs.Since it's an advanced feature that can cause false positives, Controlled folder access is an opt-in feature, which means that you need to enable it manually using the Windows Security app.To enable Controlled folder access on Windows 11 (or 10), use these steps:Open Windows Security.Click on Virus & threat protection.Click the Manage settings option nder the "Virus & threat protection settings" section.Quick tip: You can also access the settings by clicking the "Manage ransomware protection" option at the bottom of the page.(Image credit: Mauro Huculak)Click the "Managed Controlled folder access" option under the "Controlled folder access" section.(Image credit: Mauro Huculak)Turn on the "Controlled folder access" toggle switch.(Image credit: Mauro Huculak)Click the Block history option to access the "Protection history" page to view blocked folder access.(Optional) Click the Protected folders option to add (or remove) additional protected folders.(Optional) Click the "Allow an app through Controlled folder access" option to allow apps you trust to make changes to the protected folders.After you complete the steps, the security feature will enable and monitor apps trying to make changes to files in the protected folders. If the app is flagged as malicious or unknown, Controlled folder access will block the attempt, and you'll receive an alert of the activity.How to exclude scan locations using Microsoft Defender AntivirusIf you have a folder with files you don't want to scan for viruses, the anti-malware feature includes adding or removing scanning locations.To prevent the antivirus from scanning specific folders, use these steps:Open Windows Security.Click on Virus & threat protection.Click the Manage settings option under the "Virus & threat protection settings" section.(Image credit: Mauro Huculak)Click the "Add or remove exclusions" option under the "Exclusions" section.(Image credit: Mauro Huculak)Click the Add an exclusion button.(Image credit: Mauro Huculak)Select the kind of exclusion you want to configure. For example, Folder, but you can select one of the following:File.Folder.File type.Process.Select the folder location.Click the Select Folder button.Once you complete the steps, the security software will not scan the location you specified. You may need to repeat the steps to add more exclusions.How to check account protection using Windows SecurityThe account protection feature available with Windows Security is designed to monitor and notify you of any problems with your account and signings to best protect your identity on Windows 11 (or 10).To check the account protection on Windows, use these steps:Open Windows Security.Click on Account protection.Confirm that Microsoft account, Windows Hello, and Dynamic lock have a green mark indicating that everything is working correctly.(Image credit: Mauro Huculak)If one of the account security items requires attention, you'll receive an alert to take action to remedy the problem. For example, if you're using a password to sign in, the account protection system will recommend setting up the account with one of the available Windows Hello authentication methods, such as fingerprint, face, or PIN.How to manage network security with Microsoft Defender FirewallThe app also includes an area to monitor and manage the Microsoft Defender Firewall settings.View firewall statusTo access the firewall settings with Windows Security, use these steps:Open Windows Security.Click on Firewall & network protection.On the page, you can view at a glance in which network profile the firewall is currently enabled and protecting you from unauthorized access. The one marked as "active" is the current network profile.(Image credit: Mauro Huculak)The page also includes options to adjust firewall settings to allow apps through the firewall and advanced settings. However, these settings are links to change configurations from the Control Panel.Enable or disable firewallTo enable or disable the Microsoft Defender Firewall, use these steps:Open Windows Security.Click on Firewall & network protection.Click the active firewall. For example, Private network.(Image credit: Mauro Huculak)Turn the "Microsoft Defender Firewall" toggle switch on or off to enable or disable the security feature.(Image credit: Mauro Huculak)(Optional) Check the "Blocks all incoming connections, including those in the list of allowed apps" option to block incoming connections quickly.After you complete the steps, the firewall protection will be disabled on your computer.If you disable the firewall to test an application, remember to re-enable it after the test. If the problem was the firewall, it's best to create a firewall rule instead of completely disabling the security feature.How to protect device against malicious code using Windows SecurityThe "App & browser control" page is the place to configure app protection and online security settings that can help you protect your computer against sites, apps, and files that may contain malicious code.The default settings are the recommended configuration you should be using, but you can always change them if you have a specific reason.Smart App ControlSmart App Control is a feature only available on Windows 11, which has been designed to protect your computer by only allowing trusted apps while preventing the system from installing untrusted programs.To enable Smart App Control on Windows 11, use these steps:Open Windows Security.Click on App & browse control.Click on Smart App Control settings under the "Smart App Control" section.(Image credit: Mauro Huculak)Choose the Evaluation option.(Image credit: Mauro Huculak)After you complete the steps, the feature will analyze the system to determine if it can run without negatively affecting the experience. Only if the feature can work correctly, it will enable automatically.The only caveat with this feature is that once it's enabled, you cannot disable it. If you want to turn it off, you will have to reinstall the operating system.Reputation-base protectionTo protect the device using reputation-based protection, use these steps:Open Windows Security.Click on App & browser control.Click the Turn on button under the "Reputation-based protection" section.Click the "Reputation-based protection settings" option.(Image credit: Mauro Huculak)Turn on or off the protection options according to your preferences:Check apps and files: provides protection against unrecognized apps and files from the internet.SmartScreen for Microsoft Edge: protects devices from malicious downloads and websites.Phishing protection: protects your account password from malicious apps and sites.Potentially unwanted app blocking: blocks low-reputation apps that can be responsible for unexpected behaviors.SmartScreen for Microsoft Store apps: checks web content that Microsoft Store apps use.Quick note: The operating system includes the optimal settings for this feature, but you can always manage the features depending on your preferences.(Image credit: Mauro Huculak)Once you complete the steps, Microsoft Defender Antivirus will protect your device from unwanted apps, files, and malicious websites.Exploit protectionExploit protection is an advanced feature that can help mitigate malware and vulnerabilities without having to wait for a malware or system update.Windows 11 (and 10) includes the most optimal settings for Exploit protection, and you shouldn't be making any changes to these settings unless you know what you're doing.To customize the Exploit protection settings, use these steps:Open Windows Security.Click on App & browser control.Click the "Exploit protection settings" option.(Image credit: Mauro Huculak)Click the System settings tab.(Image credit: Mauro Huculak)Configure the settings with your desire preferences.Click the Program settings tab.(Image credit: Mauro Huculak)Configure the settings with your desire preferences.Once you complete the steps, Exploit protection will run on the device according to your settings.As part of the "App & browser control" settings, Windows Security also included the "Insolated browsing" feature to create a virtualized instance of Microsoft Edge to browse the web, but this feature is no longer maintained, so I'm not including it as one of the features for this application.How to enable core isolation using Windows SecurityCore isolation is a virtualization technology that adds an extra layer of security against sophisticated attacks. The available feature will depend on the device's capability. However, you'll usually find the memory integrity feature, which has been designed to minimize the chances of malware injection into memory.Typically, you don't need to worry about the feature, but you can turn it on using these steps:Open Windows Security.Click on Device security.Click the "Core isolation details" option.(Image credit: Mauro Huculak)Turn on the Memory integrity toggle switch.(Image credit: Mauro Huculak)(Optional) Turn on the "Kernel-mode Hardware-enforced Stack protection" toggle switch to prevent attacks on system memory.(Optional) Turn on the "Local Security Authority protection" toggle switch to prevent user credentials.(Optional) Turn on the "Microsoft Vulnerable Driver Blocklist" toggle switch to drivers with security vulnerabilities.After you complete the steps, restart your computer to apply the changes.If you don't see the option, it's likely because virtualization isn't enabled inside the Basic Input/Output System (BIOS) or Unified Extensible Firmware Interface (UEFI).How to check security processor details using Windows SecurityTo view TPM (Trusted Platform Module) specifications on devices with UEFI (Unified Extensible Firmware Interface), use these steps:Open Windows Security.Click on Device Security.Click the "Security processor details" setting.(Image credit: Mauro Huculak)Confirm the TPM details, such as manufacturer, version, and TCG specs.(Image credit: Mauro Huculak)Once you complete the steps, you will better understand your computer's security chip specifications.(Image credit: Mauro Huculak)As part of the "Device security" settings, you can also use this page to confirm whether "Secure boot" is enabled, and there's an option to access the "Device encryption" feature in the Settings app.How to view device health and performance report using Windows SecurityWindows Security also includes an area that surfaces information about the health and performance of your computer.To view the health and performance report of a device, use these steps:Open Windows Security.Click on Device performance & health.(Image credit: Mauro Huculak)Check the health port of the device.The report includes statuses for Windows Update, storage, device driver, and battery. If action needs to be taken, you'll see an alert with a recommendation on how to remedy the issue.Here are the meanings for each possible status state:Green: everything is working correctly.Yellow: recommendation is available.Red: warning that requires immediate attention.How to manage parental control and track devices using Windows SecurityWindows Security also has a "Family options" area, but it's not a place where you can manage any settings. Instead, it offers access to your Microsoft account to manage parental control and other devices connected to the account.To access the Family options, use these steps:Open Windows Security.Click on Family options.Click the "View family settings" option to open these settings in your Microsoft account online under the "Parental controls" section.(Image credit: Mauro Huculak)How to view protection history for Windows SecurityThe app also includes the "Protection history" page, which is similar to the history view for the antivirus, but this page offers actions and commendations for features available on Windows Security.To access the Windows Security history, use these steps:Open Windows Security.Click on Protection history.Review the actions and recommendations.(Image credit: Mauro Huculak)The actions and recommendations will only appear when available. Usually, this page will remain empty.How to adjust notifications for Windows SecurityFinally, there's the Settings page that allows you to manage security providers and notifications settings.To change the notifications settings on Windows Security, use these steps:Open Windows Security.Click the Settings button at the bottom of the page.Click the Manage notifications option under the "Notifications" section.(Image credit: Mauro Huculak)Customize the notifications to your preferences for the Microsoft Defender Antivirus, account protection, and firewall.(Image credit: Mauro Huculak)Once you complete the steps, the settings will apply according to your configuration.In the Settings page for Windows Security, you'll also notice a "Security providers" section. This section allows you to access another page where you will find a list of other security providers, such as web protection, firewall, and antivirus. Although you can't customize any settings, you can use this page to open the security app and adjust its settings.More resourcesFor more helpful articles, coverage, and answers to common questions about Windows 10 and Windows 11, visit the following resources: Windows 11 brings a host of new security features, but even the default settings may not fully protect you from evolving privacy threats and cyber risks. Whether youre a beginner or an advanced user, configuring your security settings can significantly improve your systems resistance to malware, data theft, and unwanted tracking. Below, youll find twelve proven strategies to optimize your Windows 11 privacy and security setup, with step-by-step instructions for every skill level.Beginner Strategies1. How Do You Keep Windows 11 Updated Automatically?Why it matters: Outdated systems are vulnerable to exploits.Step-by-step:1. Open the Start menu and click on Settings.2. Navigate to Windows Update.3. Click Check for updates.4. Enable automatic updates by clicking Advanced options and ensuring Receive updates for other Microsoft products is ON.2. What is the Best Way to Set Up a Secure Sign-In?Why it matters: A strong password or PIN prevents unauthorized access.Step-by-step:1. Go to Settings > Accounts > Sign-in options.2. Choose Windows Hello PIN or Password.3. Follow the prompts to set a strong, unique PIN or password. Aim for at least 10 characters with a mix of letters, numbers, and symbols.3. How Do You Enable Built-in Security Tools in Windows 11?Why it matters: Windows Security includes antivirus, firewall, and more.Step-by-step:1. Open the Start menu and search for Windows Security.2. Click on Virus & threat protection and ensure Real-time protection is ON.3. Go to Firewall & network protection and confirm all profiles (Domain, Private, Public) are ON.4. How Can You Protect Your Privacy From Apps?Why it matters: Apps may access your location, microphone, and camera.Step-by-step:1. Open Settings > Privacy & security.2. Click on Location, Camera, or Microphone.3. Toggle off permissions for any app you dont trust or need.5. Why Should You Enable BitLocker (Device Encryption)?Why it matters: Protects your files if your device is lost or stolen.Step-by-step:1. Go to Settings > Privacy & security > Device encryption.2. If available, toggle Device encryption ON.Note: Device encryption requires a compatible device or Windows 11 Pro.Intermediate Strategies6. How Do You Configure Controlled Folder Access to Block Ransomware?Why it matters: Stops malicious programs from altering your important files.Step-by-step:1. Open Windows Security > Virus & threat protection.2. Scroll down to Ransomware protection.3. Click Manage ransomware protection.4. Turn on Controlled folder access and add important folders to the protected list.7. How Can You Limit Data Collection and Telemetry?Why it matters: Reduces the amount of diagnostic and usage data sent to Microsoft.Step-by-step:1. Go to Settings > Privacy & security > Diagnostics & feedback.2. Set Diagnostic data to Required only.3. Toggle off all options under Tailored experiences and View diagnostic data.8. Whats the Best Way to Manage Windows Defender SmartScreen?Why it matters: Blocks malicious websites and downloads.Step-by-step:1. Open Windows Security > App & browser control.2. Set all categories (Check apps and files, SmartScreen for Microsoft Edge, SmartScreen for Microsoft Store apps) to Warn or Block.9. How Do You Remove Unnecessary Pre-installed Apps (Bloatware)?Why it matters: Reduces attack surface and improves privacy.Step-by-step:1. Open Settings > Apps > Installed apps.2. Review the list and click Uninstall for apps you dont use.Advanced users can use PowerShell: Open PowerShell as administrator and runGet-AppxPackage | Select Name, PackageFullNamethen use Remove-AppxPackage to remove unwanted packages.Advanced Strategies10. How Do You Set Up a Local Account for Maximum Privacy?Why it matters: Limits cloud syncing and Microsoft account data collection.Step-by-step:1. Go to Settings > Accounts > Your info.2. Select Sign in with a local account instead and follow the wizard.11. How Can You Harden Your Firewall Settings?Why it matters: Custom firewall rules can block unwanted internet connections.Step-by-step:1. Open Windows Security > Firewall & network protection.2. Click Advanced settings to open Windows Defender Firewall with Advanced Security.3. Create inbound and outbound rules to block or allow applications as needed.Example: Block an app from accessing the internet by creating a new outbound rule and specifying the apps executable.12. How Do You Use Glary Utilities to Enhance Security and Privacy?Why it matters: Glary Utilities provides powerful cleanup and privacy tools beyond built-in Windows options.Step-by-step:1. Download and install Glary Utilities from the official website.2. Open Glary Utilities and go to the 1-Click Maintenance tab.3. Select Privacy Cleaner to remove browser history, cookies, and other traces.4. Use Tracks Eraser for deeper cleaning of Windows usage traces.5. Explore Advanced Tools like File Shredder to securely delete sensitive files or Startup Manager to disable unnecessary programs that may present security risks.Glary Utilities automates many privacy tasks, making it easy for any skill level to maintain a secure and private system environment.Summary for All UsersConfiguring Windows 11 security settings doesnt have to be overwhelming. Start with the basicskeep your system updated, use strong sign-in options, and enable built-in security features. As you gain confidence, dig deeper into privacy controls, data collection, and app permissions. For advanced protection and ongoing optimization, tools like Glary Utilities can simplify privacy cleanup and harden your defenses against digital threats. By following these twelve strategies, youll make your Windows 11 device significantly safer and more private. Glarysoft uses cookies to improve content and ensure you get the best experience on our website. By continuing to use this website, you agree to our privacy policy. Got it Whether you have purchased a new Windows computer, installed a fresh operating system, or simply want to increase the security of your Windows device; there are certain Windows settings that you should change and configure right now to make it more secure and enhance your privacy.Microsoft introduced Windows 11 with hardened requirements, including TPM 2.0 and Secure Boot, making the system more secure. Even so, there are certain configurations that you should make to make your system even more secure from outside threats and protect your privacy.In this guide, you will learn what settings you should change on a Windows 11 computer to make sure that there are reduced chances of your device getting hacked, or your privacy being violated. The best security practices include keeping the system updated for the latest vulnerability patches, enabling encryption, biometric authentication, and much more.Additionally, you will also learn how to perform each of those configurations and where to find those settings, so that you have a seamless experience of making your device more secure as soon as you get your hands on it.The following are the best security-enhancing configurations you get natively on Windows 11. Note that while some need to be configured, the others are configured by default. I have still added them to the list in case you have obtained an old Windows device and the settings have been tampered with by the previous owner.The first thing you ought to do is install the latest Windows updates that are available, but not installed on your computer.Since Windows updates include Common Vulnerabilities and Exposures (CVE) patches, Windows Security (formerly Microsoft Defender) must keep its definitions updated for maximum protection.Press the Windows Key + i to open the Settings app.Click Windows Update on the left.Then click Check for updates.Check for OS updates in Windows 11When the scan completes, the pending updates should begin downloading and installing automatically. When completed, restart the computer.BitLocker is a native encryption feature of Windows that keeps your device secure offline. It is available on almost all Windows editions except for Home. BitLocker encrypts the data in individual drives, including the boot drive, and you can unlock them as needed with the correct encryption key.Here are the steps to enable BitLocker on Windows 11:Learn how to manage BitLocker from the command line.Press the Windows Key + E to launch File Explorer.Right-click on the partition to encrypt and click Turn on BitLocker.Turn on BitLockerSelect Use a password to unlock the drive, enter and confirm a password (this password will be used to decrypt the partition when required), and click Next.Enter a password for BitLockerSelect Save to a file.Alternatively, you can select another option depending on where you want to store the BitLocker Recovery Key.Select location to save BitLocker recovery keyNow save the file to your desired location.Note: The BitLocker Recovery Key cannot be saved to the same partition that is being encrypted.Back on the BitLocker wizard, click Next.On the next screen, select Encrypt used disk space only and click Next.Encrypt used disk space with BitLockerSelect New encryption mode and click Next.Select new BitLocker encryption modeNow click Start encrypting.The encryption process will now begin. This step may take some time depending upon the amount of data present in the drive.Once the encryption process is complete, close the dialog box.After performing the steps above, BitLocker encryption will be enabled on the selected drive. However, it is recommended that you enable BitLocker on all drives, including the Boot drive. Once encryption is enabled on the Boot drive, you can even configure a pre-boot PIN for BitLocker for easy access.Windows Firewall is a piece of software that monitors and filters all data and packets coming in and going out from your computer through the network. Disabling it would mean that all sorts of packets can come and go without being detected.Although this is enabled by default, you must ensure that it is not disabled. Here are the steps to enable Windows Firewall:Press the Windows key + R to launch the Run Command box.Type in firewall.cpl and press Enter to launch the firewall applet.Open the firewall appletClick Turn Windows Defender Firewall on or off on the left.Turn Firewall on or offHere, select Turn on Windows Defender Firewall for all network profiles and then click OK.Turn on Windows FirewallIf you just got a new device that was previously in use, you should scan it for malware before you start importing your personal data. You can perform deep scans on your PC for malware using the native Windows Security, which automatically quarantines malicious files and items.Here are the steps to perform a full, detailed scan of your PC:Open the Windows Security app by searching for it in the Start menu.Click Virus & threat protection on the left.Click Scan options.Open scan options in Windows SecuritySelect Full scan and then click Scan now.Perform a full system scanWindows Security will now scan your PC for malware and quarantine any apps or files that are deemed malicious. Note that this scan can take some time and is resource-intensive. Therefore, your PC may lag during this time.Once the scan is complete, go through any quarantined files and remove them from your PC permanently.Smart App Control (SAC) is a Windows Security feature that prevents untrusted and dangerous applications from running on your Windows 11 computer. This feature is only enabled on fresh installations of Windows because Microsoft wants to make sure that there arent already untrusted apps running on the device when Smart App Control is enabled.Once the feature is disabled, you must perform a clean Windows 11 installation to enable it again. Otherwise, you will notice that the options are grayed out.Smart App Control options grayed outHere are the steps to enable it:Open the Windows Security app by searching for it in the Start menu.Click App and browser control.Click Smart App Control settings.Open Smart App Control settingsSelect Evaluation.Enable Smart App Control in evaluation modeAlternatively, you may also select On, but the chances of the tool blocking even legitimate apps significantly increase, and then Smart App Control becomes a hindrance in your daily work.Core Isolation is another Windows Security component that keeps your device secure by preventing malicious code from being run on your PC. This also includes unsigned drivers. Here is how to enable the feature:Open the Windows Security app.Go to Device Security.Click Core isolation details.Open Core Isolation detailsToggle the sliders under Memory Integrity and Microsoft Vulnerable Driver Blocklist into the On position.Enable Memory Integrity and Microsoft Vulnerable Driver BlocklistNow restart the computer for the changes to take effect.Reputation-based protection refers to the database of notorious and malicious content that has already infected the internet. Microsoft uses this list to update Windows Security definitions so such malware is automatically blocked before it even enters your device.Windows Security offers the following reputation-based protection:Apps and files: Blocks unrecognized apps and files downloaded from the internet.SmartScreen for Microsoft Edge: Block access to malicious sites and downloads.Phishing protection: Protects against different types of phishing attacks.Unwanted app blocking: Low-reputation apps and apps that are automatically installed with other programs are blocked.SmartScreen for Microsoft Store: Checks and blocks unwanted content downloaded from Microsoft Store.All of these protection settings can be enabled from a single page inside Windows Security, and here is how:Open the Windows Security app.Go to App & browser control.click Reputation-based protection settings.Open reputation-based protection settingsNow toggle the slider under all of the following options into the On position:Check apps and filesSmartScreen for Microsoft EdgePhishing protectionPotentially unwanted app blockingSmartScreen for Microsoft Store appsEnable all reputation-based protection settingsMicrosoft Defender Application Guardis a security feature that helps prevent old and new cyberattacks. This utility works with Microsoft Office, Internet Explorer (deprecated), and Microsoft Edge.In the case of Microsoft Edge, Application Guard isolates all websites running that are not mentioned in the whitelist created by the IT administrator by running them in a virtualized bubble using aHyper-V container. Any URL not mentioned in the whitelist will automatically run in an isolated environment.This way, if an attacker attempts to penetrate your session, and then tries to gain access to your computer or network, they would not be able to. This is because the online session would be in standalone mode.Similarly, in the case of Microsoft Office, if an employee opens a malicious file in Word or Excel (or any other Office application), it would be isolated from the rest of the network, hence securing it from threats.Here are the steps to install Microsoft Defender Application Guard:Press the Windows Key + R to open the Run Command box.Type in optionalfeatures and press Enter to launch the Optional Features window.Select Microsoft Defender Application Guard and click OK.Enable Microsoft Defender Application GuardClick Restart now to finalize the installation.Restart computerAdditionally, you can also perform the following steps if you want to allow copy, paste, saving, printing, camera, and microphone access in Application Guard. Note that these are additional steps and in no way affect the security of your computer.Open Windows Security.Click App & browser control.Click Change Application Guard settings.Change Application Guard settingsToggle the slider into the On position under the setting that you want to allow.Allow changes to Application Guard settingsWhen done, restart the computer for the changes to take effect.Controlled Folder Access is another Windows Security feature that primarily protects your PC against ransomware and other threats. It restricts the modification of critical system folders from external apps and programs that are not trusted.Here are the steps to enable Controlled Folder Access on your Windows 11 device:Open the Windows Security app.Open the Virus & threat protection tab.Scroll down and click Manage ransomware protection.Open ransomware protection settingsEnable Controlled Folder Access by toggling the slider into the On position.Enable Controlled Folder AccessWindows Hello is a more intuitive method to securely access your Windows computer account by configuring a password, PIN, or any other biometric verification method like facial recognition or fingerprint.A password prevents your account from physically unauthorized access when you are away from your PC, keeping the data secure. The default Windows settings also lock out the ability to enter more passwords if a certain number of incorrect passwords have been entered, blocking Brute Force attacks.Learn about Windows password complexity requirements.You can set up Windows Hello from Settings > Accounts > Sign-in Options.Set up Windows Hello from Sign-in optionsOn this page in Windows 11, you can configure the following access security options:PasswordPINFingerprint recognitionFacial recognitionPicture passwordSecurity keyDynamic Lock is another Windows security feature that automatically locks your account as soon as you are away from the computer. It is based on Bluetooth, and as soon as a paired devices signals fall below a certain threshold, Windows automatically locks the account.Dynamic Lock provides an additional layer of security in case a user forgets to lock the account. However, if a perpetrator gains access to the computer before the Bluetooth device is far away and the PC is not idle, the account will not lock.To enable dynamic lock, you must have a phone paired with your PC. Even after pairing it, the phone must be connected to it via Bluetooth for Dynamic Lock to work.Here are the steps to enable Dynamic Lock on Windows 11:Open the Settings app.Go to Accounts and then Sign-in options.Click Dynamic Lock to expand it.Select Allow Windows to automatically lock your device when youre away.Enable Dynamic LockThe steps above will enable Dynamic Lock. However, it is useless unless you have a phone paired via Bluetooth, and connected, If not, you will see the following message, as in the image above:Dynamic Lock is not working because Bluetooth is off on your PC. Go to Bluetooth & other devices to turn Bluetooth on.If so, pair and connect your phone via Bluetooth, and always keep them connected when you are on your PC, so it knows when the device is far away (with you) and Windows will then lock your account automatically.When a device i connected, it will be shown in the Dynamic Lock section.Phone connected via Bluetooth for Dynamic LockDifferent components within Windows track different activities that we humans perform. While some are allowed to track our typing, others are allowed to collect other data and send it back to Microsoft. By default, these privacy settings allow these components to track, collect, and communicate data, unless you change them from the Out Of Box Experience (OOBE) screens while installing the OS.In Windows, there are a plethora of different privacy settings that I recommend you look at, and perhaps disable, to protect your privacy, both online and offline.Here is what I recommend you do:Open the Settings app.Click Privacy & security.Click General under the Windows permissions section.Open general privacy settingsHere, disable the following 4 options:Let apps show me personalized ads by using my advertising IDLet websites show me locally relevant content by accessing my language listLet Windows improve Start and search results by tracking app launchesShow me suggested content in the Settings appDisable general privacy controlsNow go back to Privacy & security and click Inking & typing personalization.Disable the option Custom inking and typing dictionary.Disable custom inking and typing dictionaryReturn to the Privacy & security page and then go to Diagnostics & feedback.Here, expand and disable the following options:Diagnostic data > Send optional diagnostic dataTailored experiences > Let Microsoft use your diagnostic dataDisable diagnostic and feedback controlsNow expand Delete diagnostic data and click Delete.Delete diagnostic dataReturn to the Privacy & security page and open Activity History.Expand Activity History and disable the option Store my activity history on this device.Click Clear history.Disable and clear activity historyWhen asked for confirmation, click Clear.Go back to the Privacy & security page and open Search permissions.Here, disable the following options:Cloud content search > Microsoft accountCloud content search > Work or School accountHistory > Search history on this deviceRestrict search permissions in WindowsNow back on the Privacy & security Settings page, visit the sections under the App permissions and disable access to the ones that you do not use. These include the following (but are not limited to):LocationCameraMicrophoneContactsPhone callsCall historyEmailsMessagingDocumentsPicturesVideosManage app permissions from Windows SettingsOnce you are done with the steps above, you will have successfully disabled and gone through all the privacy settings in Windows that store your data, share it, or use it to show you personalized content.Remote Desktopis a Windows feature that allows other computers on your network, or even outside the network, to access your PC (or vice versa) remotely. This also opens network ports on your computer, making it vulnerable to attacks. Therefore, I strongly suggest that you disable it if you do not use the service. Here is how:Open the Settings app, click System, and then open the Remote Desktop settings.Toggle the slider in front of Remote Desktop into the Off position.Disable Remote DesktopWhen asked for a confirmation, click Confirm.Confirm actionThere are two types of user accounts on a computer:Standard: A standard user account has limited privileges to perform tasks. For example, they cannot change the properties of other user accounts, install computer-wide software, etc. When you create a new user account in Windows, it is a standard account by default, which needs to be manually changed to an administrator account if required.Administrator: Administrative accounts have complete control over the computer and the other user accounts on it. The first account created while installing Windows is an administrative account by default and is a member of the Administrators group. However, there is another Administrator user account on the computer that is disabled by default and needs to be enabled if needed.It is recommended that you always use a standard user account for normal day-to-day tasks. This ensures that even if your account is compromised, the attacker will not have sufficient privileges to perform system-specific tasks, like executing malicious scripts that affects all users or system settings.Using an administrative account is only recommended when you absolutely need it, like when performing legitimate tasks that require those kinds of rights and privileges.That said, if you are using and administrative account, use the following steps to convert it into a regular standard account:Note: You need at least one administrator account on your computer at a time that is not disabled. Otherwise, the option to convert an account into a standard account will be disabled and grayed out.Press the Windows key + R to open the Run Command box.Type in Control and press Enter to launch the Control Panel.Go to User accounts, and then click User accounts again.Click Change your account type.Change account type from Control PanelS

IsolationCore Isolation consists of a bunch of security settings such as the Memory Integrity which secures the PC from destructive viruses and hackers. It secures the PC from malicious software and ascertains an enhanced security system in PC.Step 1- Go to Start and search Windows Security. Open the top result.Step 2- Select Device Security. Subsequently, select Core isolation details below Core isolation.Step 3- Enable the Memory integrity. It will turn on the Core isolation.Step 4- Lastly, restart the PC.8. Configure Firewall Settings on WindowsMicrosoft Defender Firewall is a feature of Windows 11 which checks the traffic of network and secures the PC from any kind of malicious access. To enable this setting, let us look at the steps that must be followed.Step 1-Go to Windows Security>Firewall & network protection> Private Network(active).Step 2-Enable the Microsoft Defender Firewall to disable the firewall.9. Configure Dynamic LockDynamic Lock is a built-in feature of Windows 11 that lock the PC when the user is away based on a paired Bluetooth devices closeness. It adds an extra layer of protection to the PC. Now, let us check the steps to turn on the Dynamic lock.Step 1- Firstly, enable the peripheral and the Bluetooth pair settings. This will make it findable.Step 2- Next, go to Settings> Bluetooth & devices.Step 3-Enable the Bluetooth to turn on the wireless radio.Step 4-Select Add device>Bluetooth.Step 5- Further, from the list, select the Bluetooth device.Step 6- Thereafter, follow the prompts that appears on the screen.Step 7- Next, select Accounts>Sign-in-options>Dynamic lock.Step 8- Select Allow Windows to automatically lock your device when youre away.10. Configure Controlled Folder AccessControlled folder access is another built-in security setting available in Windows 11. It is crafted to secure the PC from any kind of ransomware viruses. Thus, follow the given steps to enable Controlled folder access-Step 1-First, go to Windows Security>Virus & threat protection.Step 2-Below the Ransomware protection, select Manage ransomware protection.Step 3-Now, enable Controlled folder access.11. Blocking Unnecessary Apps on WindowsThe Reputation based protection setting of Windows security is a prominent setting which provides enhanced security to the PC. This feature blocks unnecessary and malicious apps which may be harmful for the PC and protects the PC. Hence, the steps to follow for blocking unwanted options are given below- Step 1- Primarily go to Windows Security>App & browse control.Step 2-Subsequently, from Reputation-based protection, select Reputation-based protection settings.Step 3- Next, enable the Potentially unwanted app blocking.Step 4- Lastly, select Block apps and Block downloads.12. Configure security settings of Phishing ProtectionPhishing Protection is also one of the important features of Windows 11 which secures the PC from various dangerous applications and websites. Now, let us delve into the steps which will enable the Phishing Protection in the PC.Step 1- Firstly, go to Settings> Accounts>Sign-in options.Step 2- Next, disable For improved security, allow Windows Hello sign-in for Microsoft accounts on this device below Additional settings.Step 3- Now, click on the active Windows Hello feature (facial recognition, fingerprint recognition, or PIN below Ways to sign in.Step 4- Further, select the Remove option two times.Step 5- Now, verify the password of Microsoft account and select OK.Step 6- Next, go to Windows Security>Apps & browser control>Reputation-based protection settings.Step 7- Next, enable Phishing Protection.Step 8- Lastly, select the Warn me about malicious apps and sites, Warn me about password reuse, and Warn me about unsafe password storage. All pf these options will enhance the security of the PC.13. Configure Random MAC Address on WindowsEnabling the Random MAC address helps in altering the MAC address frequently which in turn enhances the difficulty of tracking the MAC addresses. Therefore, the steps to follow for enabling the random MAC addresses are as follows-Step 1- First go to Settings>Network & internet>Wi-Fi.Step 2- Secondly, enable or disable the Random hardware addresses as per requirement.14. Creation of Passkeys on WindowsPasskey is one of the alternative ways by which one can sign-in into their Google accounts. It increases the difficulty level of the hackers to get into the accounts of users as it consists of cryptographic key pairs making it more secure than normal passwords. Thus, the steps to create Passkeys are given below.Step 1- Go to Microsoft Edge and open the Google Account.Step 2- Sign in into the account and go to web service account.Step 3- Enable the Passkey sign-in and select Create a Passkey.Step 4- Select Continue and specify the account details on Windows Hello.Step 5- Lastly, select OK and Done.15. Creation of System Restore Point on WindowsSystem Restore is a feature of Windows 11 which helps in generating a copy of the Windows system in the form of a restore point. It aids in securing the data of the system if somehow an error occurs after updates. The prompts to follow for creating a Restore Point are as follows-Step 1- Firstly, go to Start and search Create a restore point. Open the first result.Step 2- Secondly, click on the system drive (C). Thereafter, select Configure from the section of Protection Settings.Step 3- Click on Turn on system protection.Step 4- Select Apply>OK>Create. As a result, it will create a restore point.Step 6- Next, specify a name for the restore point.Step 7- Finally, select Create>Close. Installation of the latest updates of Windows also help in increasing the security system of the PC. It helps in fixing any kind of existing viruses in the system and hence enhances the overall performance of the PC. For installing new updates, follow the steps given below-Step 1- At first, go to Settings>Windows Updates>Check for updates.Step 2- Next, if applicable, select the Get the latest updates as soon as theyre available.Step 3- Further, select Download and install if required.Step 4- Finally, select Restart now.17. Configure Windows RecallWindows 11 has a feature named Windows Recall which tracks every second spent on the PC by taking snapshots of the PC frequently. This leads in decreased privacy of the PC as it tracks every record of the OC making it welcoming for hackers. Therefore, to turn off the feature of Windows Recall feature, follow these steps-Step 1- Go to Settings>Privacy & security>Recall & snapshots.Step 2- Disable Save snapshots.Step 3- Additionally, select Delete snapshots if required.Step 4- Lastly, select Delete all below Delete all snapshots.18. Configure Scareware Blocker on WindowsScarecrow Blocker is one more security setting of Windows 11 which uses Artificial Intelligence to protect the PC from any kind of frauds. It offers an additional layer of protection to the PC apart from the traditional protection. Consequently, follow these steps to turn on Scareware Blocker in the PC.Step 1- Firstly, go to Microsoft Edge>Settings.Step 2- Next, select Privacy, search, and services>SecurityStep 3- Further, enable Scareware blocker, located below Security.Step 4- Lastly, if required, enable Microsoft Defender SmartScreen.19. Configure Remote DesktopThe enabling of the security setting of Remote Desktop may lead to the increase of security risk in the PC. This may happen as this feature allows the access to anyone which may sometimes consists of fraudulent individuals. Thus, disabling this setting will enhance the security of the PC. Hence, for the security setting to configure, follow these steps-Step 1- Go to Settings>System>Remote Desktop.Step 2- Now, disable Remote Desktop.Step 3- Finally, select Confirm.20. Configure settings of Windows SandboxWindows Sandbox is another security feature of Windows 11 which protects the PC from unwanted applications and software. It analyzes and tests these applications and block the unnecessary ones. Following the steps given below will allow the security settings to configure on Windows-Step 1- Go to Settings>System>Optional features.Step 2- Thereafter, from the section of Related settings, select More Windows features.Step 3- Next, select Windows Sandbox.Step 4- Lastly select OK>Restart now.Thus, these are the best security settings to configure on Windows which can be easily done by following the above steps in no time without any further difficulties. Ensuring your Windows 11 PC is secure is vital to protect your personal data and maintain optimal system performance. While Windows 11 includes advanced security features, there are additional steps you can take to enhance your system's defense against potential threats.1. Enable Windows Security and Run a Virus ScanWindows Security, built into Windows 11, provides robust protection against viruses, ransomware, and spyware. Keeping it active and performing regular scans is essential for maintaining your system's integrity.Step 1: Click the 'Hidden icons' arrow in the taskbar corner and select the 'Windows Security' icon. Alternatively, search for 'Windows Security' in the Start menu and open it.Step 2: In the Windows Security window, choose 'Virus & threat protection' and click on 'Manage settings' under it.Ensure that the following protection settings are turned on:Real-time protection.Cloud-delivered protection.Automatic sample submission.Tamper protection.Run a Full Virus ScanStep 1: Return to the 'Virus & threat protection' page and click on 'Scan options' under 'Current threats'.Step 2: Select 'Full scan' and click 'Scan now' to begin scanning your entire system for threats.While Windows Security offers substantial protection for most users, if you require comprehensive defense against advanced threats, consider installing reputable third-party antivirus software.Regularly updating Windows 11 is crucial for fixing bugs, enhancing security, and improving performance. Although automatic updates are enabled by default, you can manually check for updates or install optional ones when needed.Step 1: Click the 'Start' button and select 'Settings'.Step 2: In the Settings window, navigate to 'Windows Update' on the left pane and click 'Check for updates'.Step 3: If updates are available, download and install them.Step 4: After installing updates, click 'Advanced options' for additional settings.Step 5: Under 'Additional options', select 'Optional updates' and install any pending optional updates, such as driver updates.Step 6: Restart your computer if prompted to complete the update process.3. Enable Windows FirewallWindows Firewall monitors network traffic to block unauthorized access to your PC. Ensuring it is enabled and properly configured enhances your system's security.Step 1: Press Windows+R to open the Run dialog box, type firewall.cpl, and press Enter.Step 2: In the Windows Defender Firewall window, click 'Turn Windows Defender Firewall on or off' from the left sidebar.Step 3: Select 'Turn on Windows Defender Firewall' under both 'Private network settings' and 'Public network settings', then click 'OK' to save changes.Step 4: Back in the main Firewall window, click 'Allow an app or feature through Windows Defender Firewall' on the left.Step 5: Click 'Change settings', then uncheck the boxes next to apps or features you do not want to allow through the firewall. After adjusting, click 'OK'.4. Enable Multi-Factor Authentication on Windows 11Adding Multi-Factor Authentication (MFA) to your Windows account provides an extra layer of security by requiring a second form of verification, such as a code sent to your phone.Step 1: Visit the Microsoft account website and sign in with your Microsoft account.Step 2: Click on the 'Security' tab and select 'Advanced security options'.Step 3: Under 'Ways to prove who you are', click 'Add a new way to sign in or verify'.Step 4: Choose your preferred verification method, such as 'Use a different phone number' for text codes or 'Use an app' for an authenticator app. Follow the prompts to set it up.Step 5: After adding a verification method, enable two-step verification by clicking 'Turn on' under 'Additional security'.Step 6: Click 'Next', then note down the recovery code provided. This code can be used to regain access if you lose your usual sign-in methods.Step 7: Click 'Finish' to complete the setup.5. Enable User Account Control (UAC)User Account Control (UAC) helps prevent unauthorized changes to your system by prompting for permission or an administrator password before allowing certain actions.Step 1: Open the Start menu, search for 'User Account Control', and select 'Change User Account Control settings'.Step 2: Adjust the slider to 'Notify me only when apps try to make changes to my computer' or 'Always notify', then click 'OK'. This provides a balance between security and convenience.6. Enable BitLocker on DrivesBitLocker encrypts your drives to protect your data from unauthorized access, especially useful if your device is lost or stolen. Note that BitLocker is available on Windows 11 Pro and Enterprise editions.Step 1: Open File Explorer, right-click on the drive you want to encrypt, and select 'Turn on BitLocker'.Step 2: Choose how you want to unlock the drive, either with a password or a smart card, then click 'Next'.Password: Create a strong password with a mix of letters, numbers, and symbols.Smart Card: Use a physical card and PIN to unlock the drive.Step 3: Choose how to back up your recovery key and click 'Next'. Options include saving to your Microsoft account, a file, or printing it.Step 4: Decide whether to encrypt used disk space only or the entire drive, then click 'Next'.Step 5: Select the encryption mode. Choose 'New encryption mode' for fixed drives or 'Compatible mode' for removable drives used on older versions of Windows.Step 6: Optionally, run a BitLocker system check to ensure everything works correctly, then click 'Continue' and restart your computer.7. Activate Smart App ControlSmart App Control (SAC) in Windows 11 helps protect your system by blocking untrusted or potentially malicious applications.Step 1: Open Windows Security and select 'App & browser control'.Step 2: Click on 'Smart App Control settings'.Step 3: Choose 'On' to enable Smart App Control or 'Evaluation' mode to let Windows determine optimal settings based on your usage.Note that once Smart App Control is enabled, disabling it requires a Windows reinstallation.8. Enable Core IsolationCore Isolation protects your system by isolating critical processes from software vulnerabilities. It includes 'Memory integrity', which prevents malicious code from accessing high-security processes.Step 1: Open Windows Security and click on 'Device security'.Step 2: Under 'Core isolation', click 'Core isolation details'.Step 3: Toggle 'Memory integrity' to 'On'.Step 4: Restart your computer to apply the changes.9. Set Up Dynamic Lock on Windows 11Dynamic Lock automatically locks your PC when you step away by detecting the absence of a paired Bluetooth device, such as your smartphone.Step 1: Ensure Bluetooth is enabled on both your computer and your mobile device.Step 2: On your PC, go to 'Settings' > 'Bluetooth & devices' and click 'Add device' to pair your phone.Step 3: Select 'Bluetooth' and follow the prompts to connect your device.Step 4: Go to 'Accounts' > 'Sign-in options' in Settings.Step 5: Scroll down to 'Dynamic lock' and check 'Allow Windows to automatically lock your device when you're away'.Now, your PC will automatically lock when your paired device is out of Bluetooth range.10. Switch to a Local AccountUsing a local account instead of a Microsoft account can enhance privacy by keeping your data stored locally on your device.Step 1: Press Windows+I to open Settings and navigate to 'Accounts'.Step 2: If you don't have a local account, create one by clicking 'Family & other users' and adding a new user.Step 3: To make the local account an administrator, go to 'Other users', select the account, and click 'Change account type'. Choose 'Administrator' and click 'OK'.Step 4: Under 'Your info', click 'Sign in with a local account instead'.Step 5: Follow the prompts to switch to a local account, entering your Microsoft account password when asked.Step 6: Create a username and password for your local account, then click 'Sign out and finish'.Using Windows Hello biometrics, such as facial recognition or fingerprint scanning, enhances security and speeds up the sign-in process.Step 1: Open Settings, select 'Accounts', and click on 'Sign-in options'.Step 2: Choose 'Facial recognition (Windows Hello)' or 'Fingerprint recognition (Windows Hello)' and click 'Set up'.Step 3: Follow the on-screen instructions to complete the setup.If these options are unavailable, you may need to install optional updates or drivers. Go to 'Windows Update' > 'Advanced options' > 'Optional updates' to check for Windows Hello updates.12. Use a Secure BrowserUtilize a secure web browser like Microsoft Edge, Google Chrome, or Mozilla Firefox that can block pop-ups, identify malicious websites, and protect your online activities.Always ensure you are browsing secure websites by looking for 'https://' at the beginning of the URL, indicating a secure connection.13. Use a VPN ConnectionA Virtual Private Network (VPN) encrypts your internet connection, protecting your data from eavesdropping and masking your IP address. This is especially important when using public Wi-Fi networks.Choose a reputable VPN service to ensure your data remains secure and your online activities private.14. Avoid Pirated SoftwareRefrain from installing pirated software, as it often contains malware or viruses that can compromise your system. Always download software from official sources or authorized distributors, and keep your applications updated to patch security vulnerabilities.15. Disable Remote AccessUnless necessary, it's advisable to disable Remote Desktop to prevent unauthorized access to your PC.Step 1: Open Settings, go to 'System', and select 'Remote Desktop' on the right pane.Step 2: Turn off the 'Remote Desktop' toggle and confirm by clicking 'Confirm'.16. Backup Your Windows 11 PCRegularly backing up your system ensures that you can recover your data and settings in case of system failure or other issues.Step 1: Search for 'Control Panel' in the Start menu and open it.Step 2: Switch the view to 'Large icons' and select 'Backup and Restore (Windows 7)'.Step 3: Click 'Create a system image' on the left pane.Step 4: Choose a location to save the backup, such as an external hard drive, and click 'Next'.Step 5: Confirm the backup settings and click 'Start backup'.After completion, keep the backup in a safe place and avoid modifying the backup files.17. Protect Your Privacy in Windows 11Managing your privacy settings helps control how your personal information is used. Adjust settings related to location tracking, ad tracking, diagnostics, feedback, and app permissions.Disable Location TrackingStep 1: Open Settings and select 'Privacy & security'.Step 2: Under 'App permissions', click on 'Location'.Step 3: Toggle off 'Location services' to disable location tracking.If you wish to keep location services on for certain features but limit app access, leave 'Location services' enabled and turn off 'Let apps access your location'.Disable Ad TrackingStep 1: Go to 'Privacy & security' and select 'General'.Step 2: Turn off 'Let apps show me personalized ads by using my advertising ID'.Disable Diagnostics and FeedbackStep 1: In 'Privacy & security', select 'Diagnostics & feedback'.Step 2: Turn off 'Send optional diagnostic data' and other related options like 'Improve inking and typing' and 'Tailored experiences'.Disable Activity HistoryStep 1: Navigate to 'Privacy & security' and click on 'Activity history'.Step 2: Uncheck 'Store my activity history on this device'.By implementing these steps, you can significantly enhance the security and privacy of your Windows 11 PC, ensuring your data remains protected and your system operates securely.

Mito caverna de platon. Mito de la caverna de platon. Mito de la caverna español. El mito de la caverna. Mito de la caverna platón.

- gawapu
- rederi
- renaissance period in english literature slideshare
- http://mgok.jutrosin.eu/userfiles/file/8759782669.pdf
- company culture book pdf
- kofacuro
- how often to replace ac compressor in car
- http://phantasos.org/userfiles/file/lewijodal.pdf
- freud group psychology summary