**Improve security in your Windows 11 OS.**

In the history of the evolution of Microsoft Windows, the Windows 11 edition is the most secure version. It contains many system improvements and many new security-focused features. Indeed, Microsoft integrates many security features into Windows to protect its users against computer threats, to meet security standards, and to maintain user trust. Here are some essential configurations to improve security for your Windows 11:

1. **Keep your PC updated:**

By keeping your PC updated in Windows 11, you can ensure that your device is running the latest security patches, bug fixes, and feature updates. Keep your device up to date to avoid potential security vulnerabilities and ensure the best performance and user experience.

Follow the steps to keep your PC updated:

1. Open "Settings" app, go to the "Windows Update" option.
2. Click on the "Check for updates" button to see if there are any updates available for your PC.
3. If there are any updates available, click on the "Download and install" button to install them.
4. Restart your PC (if necessary) after installation by clinking "Restart now" button.
5. Turn on automatic updates (optional) by clicking on the "Advanced options" link in the Windows Update settings and toggling on the "Automatic (recommended)" option under "Choose how updates are installed".
6. **Set up a password for your user account.**

Set up a strong password for your user account to keep your personal and sensitive data secure. It's important to choose a password that is at least 8 characters long, includes a mix of uppercase and lowercase letters, numbers, and symbols, and is not easy to guess or remember. Additionally, avoid using the same password for multiple accounts and change your password periodically to keep it secure.

The steps below are for local accounts (without a Microsoft email).:

1. Open Windows Settings app.
2. Go to the "Accounts" section.
3. Look for "Sign-in options" and click.
4. Create a new password: Under the "Password" section, click on the "Change" button to create a new password. If you don't have a password set up already, you may need to click on the "Add" button first.
5. Enter your current password: If you have an existing password, you'll need to enter it first to continue.
6. Enter a new password in the "New password" field and confirm it in the "Reenter password" field.
7. Add a password hint (optional): You can add a password hint to help you remember your password, but make sure it's not too obvious.
8. Click on "Next" and "Finish": Follow the prompts to finish setting up your new password.

If you are using a Microsoft account to login, you can change the password via your Microsoft account settings.

1. **Configure Windows Hello for fingerprint or facial recognition features if applicable.**

Windows Hello is important to allow you signing in to your device quickly and securely using biometric authentication. If you are using PIN instead of fingerprint or face recognition, it is important to keep your biometric data secure by using a strong PIN and not sharing your device with others.

Follow the steps to configure Windows Hello in Windows 11:

1. Check if your device is compatible: To use Windows Hello, your device must have a compatible camera or fingerprint reader. You can check if your device is compatible by going to the Windows 11 Settings app, clicking on "Accounts", then "Sign-in options" and checking if Windows Hello is available.
2. If your device is compatible, open Windows 11 Settings app, click on "Accounts", then "Sign-in options". Under "Windows Hello and security keys", click on "Set up" under "Face recognition", "Fingerprint", or "PIN" and follow the prompts to set up the desired method.
3. After setting up Windows Hello, you can use it to sign in to your device. From the sign-in screen, select the Windows Hello option that you've set up (face, fingerprint, or PIN), and follow the prompts to sign in.
4. **Enable two-factor authentication if applicable.**

Enabling two-factor authentication (2FA) in Windows 11 adds an extra layer of security to your account by requiring a second form of verification in addition to your password. This helps prevent unauthorized access to your device and personal information. Always keep your 2FA verification method secure, use a strong password et do not share your smartphone or email with others.

Here is how to enable 2FA in Windows 11:

1. Set up a Microsoft account which is necessary to enable 2FA in Windows 11. If you do not have one already, go to the Microsoft account sign-up page and create one.
2. Set up 2FA for your Microsoft account: Go to the Microsoft account security settings page. Click on the "Security" tab, then click on "More security options" and follow the prompts to set up 2FA.
3. Enable 2FA for Windows 11: Open the Windows 11 Settings app, click on "Accounts" and select "Sign-in options". Under "Windows Hello and security keys", click on "Add" under "Two-factor authentication (2FA)" and follow the prompts to set up 2FA.
4. Use 2FA to sign in to Windows 11: After setting up 2FA for Windows 11, you will be prompted to enter a verification code in addition to your password when signing in. You can receive the verification code via email, text message, or through an authenticator app on your smartphone.

Top of Form

1. **Enable Windows Security**

Windows 11 include Windows Security, an antivirus protection built by Microsoft for Windows operating system. By enabling Windows Security which continually scans for malware (**mal**icious soft**ware**), viruses, and security threats, you keep your device safe and protect it from attacks. Make sure Windows Security is enabled and up to date for a better experience with Windows 11. Follow the steps to set up Windows Security:

1. Open the Windows Security app. To find the app, search for "Windows Security" in the Start menu.
2. Click on "Virus & threat protection" in the sidebar.
3. Click on "Manage settings" under "Virus & threat protection settings."
4. Here, you can turn different types of protection on or off, such as Real-time protection, Cloud-delivered protection, and Automatic sample submission.
5. To allow Windows Defender to scan and remove potentially unwanted apps, turn on the "Potentially unwanted app blocking" toggle.
6. If you want to exclude a specific file or folder from being scanned, click on "Add or remove exclusions" and then click on the "+ Add an exclusion" button.
7. You can also customize the Windows Defender Firewall settings by following the steps described in the next section “Configure Windows Firewall”.
8. Once you have made the desired changes to Windows Defender, close the Windows Security app.
9. **Configure Windows Firewall**

Follow the steps to configure Windows Firewall.

1. Open the Windows by searching for it in the Start menu.
2. Click on "Firewall & network protection."
3. Click on the network profile you want to change the settings for (e.g., Public network, Private network, or Domain network).
4. Scroll down to the "Windows Defender Firewall" section and click on "Advanced settings."
5. In the "Windows Defender Firewall with Advanced Security" window, you can manage inbound and outbound rules for the selected profile.
6. To create a new rule, click on "Inbound Rules" or "Outbound Rules" in the left pane, then click "New Rule" in the right pane.
7. Follow the prompts to configure the new rule, including selecting the program or port to allow or block, the action to take (allow or block), and the profile(s) to apply the rule to.
8. To modify an existing rule, right-click on the rule and select "Properties." You can then modify the rule settings as needed.
9. Once you have finished configuring the firewall settings, click "OK" to save the changes.
10. **Use a third-party antivirus.**

Windows 11 comes with built-in antivirus software called Windows Security, which provides basic protection against viruses, malware, and other threats. However, you may want to use a third-party antivirus software for additional features and more robust protection. Choose a reputable antivirus software and keep it up-to-date to ensure that it's providing the best possible protection for your device. You have a choice between many antivirus software options available for Windows 11, such as Kaspersky, Norton, McAfee, Avast, Bitdefender, etc. Choose, install and enable it on your device following the steps given by the antivirus software provider.

1. **Use a standard user account.**

A standard user account has limited privileges. It is very important to use a standard user account prevent accidental system changes and protect your device against malwares. The admin account should be used only for administration needs. A standard user account can be set by using a Microsoft account or not.

If you have a Microsoft Account, or a configured phone number, follow the steps below:

1. Click on the Start menu and select Settings.
2. In the Settings window, click on Accounts.
3. In the Accounts window, click on Family & other users.
4. Under the Other users section, click on Add account.
5. Select Standard user from the dropdown menu.
6. Enter the email address or phone number of the user you want to add and click Next.
7. Follow the prompts to set up the account, including creating a password and setting up security questions.
8. Once the account is set up, you can switch to it by clicking on the Start menu and selecting the account name from the list of users.

If you do not have a Microsoft Account or you do not need to use a Microsoft account, follow the steps below:

1. Open the Settings app.
2. Click on "Accounts" from the list of options.
3. Click on "Other users" in the left-hand menu.
4. Click on the "Add account" button under "Other users" on the right-hand side.
5. Click on "I don't have this person's sign-in information" at the bottom.
6. Click on "Add a user without a Microsoft account" at the bottom.
7. Enter a username, provide a password for the new account, set up the security questions and then click on "Next". After this step, the account is created as a local account by default.
8. Click on the account name and choose whether the new account is a standard user or an administrator account.
9. Click on "Finish" to create the new account.
10. **Enable User Account Control.**

After enabling UAC, you will be prompted to confirm any actions that could potentially affect your system. This helps prevent unauthorized changes to your computer and keeps your system more secure.

To enable User Account Control (UAC) in Windows 11, follow these steps:

1. Search for "UAC" into the search bar and click on "Change User Account Control settings" from the search results.
2. Move the slider to the position you want. There are four settings to choose from:
   * Always notify me when: This is the most secure setting and will notify you every time an app tries to make changes to your computer.
   * Notify me only when apps try to make changes: This is the default setting and will notify you only when an app tries to make changes to your computer.
   * Notify me only when apps try to make changes (do not dim my desktop): This setting is the same as the previous one, but it will not dim your desktop when a UAC prompt appears.
   * Never notify me: This is the least secure setting and should only be used by advanced users who understand the risks of turning off UAC.
3. Once you have selected the setting you want, click "OK" to save the changes. You may be prompted to enter your administrator password or confirm your choice.
4. **Use Dynamic Lock**

Dynamic Lock is a Windows 11 feature that automatically locks your computer when you walk away from it with your phone or other Bluetooth device you have configured for this purpose. Here's how to configure Dynamic Lock:

1. Make sure your computer and Bluetooth device are paired. Go to Settings > Devices > Bluetooth & devices and make sure your device is listed and connected.
2. Go to Settings > Accounts > Sign-in options and scroll down to the "Dynamic lock" section.
3. Check the box next to "Allow Windows to detect when you're away and automatically lock the device."
4. Choose the device you want to use for Dynamic Lock from the drop-down menu.
5. Adjust the "Dynamic Lock threshold" to the desired time. This is the amount of time your device needs to be out of range before your computer is automatically locked.
6. Click "Save" to apply the changes.
7. **Encrypt your drives.**

Encrypting your drives can help keep your data safe and secure from unauthorized access. Once the encryption process is complete, you will need to enter your password or insert your smart card whenever you want to access the encrypted drive. This will ensure that only authorized users can view the data stored on the drive.

Here are the steps to encrypt your drives using the built-in encryption tool called BitLocker:

1. Open File Explorer and right-click on the drive you want to encrypt.
2. Select "Turn on BitLocker" from the context menu.
3. Choose the type of encryption you want to use - either "Encrypt used disk space only" or "Encrypt entire drive". The latter option is more secure, but it will take longer to complete.
4. Choose how you want to unlock the drive. You can either use a password or a smart card.
5. Choose where to store the recovery key. This key will be used to unlock the drive in case you forget your password or lose your smart card. You can either save it to your Microsoft account, save it to a file, or print it out.
6. Click "Start encrypting" to begin the encryption process. This can take several hours to complete, depending on the size of your drive and the type of encryption you chose.
7. **Encrypt specific data using Encryption File System**

Windows 11, like its predecessors, includes support for the Encrypted File System (EFS) feature, which allows users to encrypt individual files or folders on their computer. This feature is particularly useful for protecting sensitive data from unauthorized access in case a device is lost or stolen. Once the file or folder is encrypted, only the user who encrypted it or a designated recovery agent can access it. It's important to note that if you lose the encryption key or the associated certificate, you may not be able to access the encrypted data.

To encrypt a file or folder using EFS in Windows 11, follow these steps:

1. Right-click on the file or folder you want to encrypt and select "Properties" from the context menu.
2. Click on the "Advanced" button in the General tab of the Properties window.
3. Check the box next to "Encrypt contents to secure data" and click OK.
4. If the file or folder is in use, you will be prompted to close any programs or windows that are using it.
5. Click OK again to confirm that you want to encrypt the file or folder.
6. **Enable Trusted Platform Module**

Trusted Platform Module (TPM) is a hardware-based security feature that helps protect your device from attacks. To enable TPM in Windows 11, follow these steps:

1. Check if your device has a TPM chip: Open the Device Manager, look for the Security devices or Trusted Platform Module category. If you see a TPM chip listed, skip to step 3. If not, your device may not have a TPM chip, or it may be disabled in the BIOS/UEFI settings.
2. Enable TPM in the BIOS/UEFI settings: If your device has a TPM chip, you need to enable it in the BIOS/UEFI settings. Restart your device and enter the BIOS/UEFI settings by pressing a key (usually F2, F10, or Del) during startup. Look for the TPM setting and make sure it's enabled.
3. Enable TPM in Windows 11: Once you've enabled TPM in the BIOS/UEFI settings, you need to enable it in Windows 11. Open the Windows Security app, click on the "Device security" option in the right pane.
4. Click on the "Security processor details" option. If you see a message that says, "This PC doesn't meet the hardware requirements for using the security processor," your device may not have a TPM chip or it may not be enabled in the BIOS/UEFI settings.
5. If your device meets the requirements, click on the "Security processor details" option again, and then click on the "Security processor troubleshooting" option. Follow the on-screen instructions to complete the TPM setup process.
6. **Enable Secure Boot**

Secure Boot is a feature that helps prevent unauthorized software and operating systems from loading during the boot process. Once you've enabled Secure Boot in Windows 11, you can be confident that your device will only load authorized software and operating systems during the boot process, which helps prevent malware and other security threats.

Here's how to enable Secure Boot in Windows 11:

1. Check if your device supports Secure Boot: Secure Boot requires a device with UEFI firmware that supports the feature. You can check if your device supports Secure Boot by restarting your device and entering the BIOS/UEFI settings. Look for the Secure Boot option in the settings. If it's not available, your device may not support Secure Boot.
2. Enable Secure Boot in the BIOS/UEFI settings: If your device supports Secure Boot, you can enable it in the BIOS/UEFI settings. Restart your device and enter the BIOS/UEFI settings by pressing a key (usually F2, F10, or Del) during startup. Look for the Secure Boot option and make sure it's enabled. The location of the Secure Boot option may vary depending on the device and BIOS/UEFI version.
3. Save and exit the BIOS/UEFI settings: Once you've enabled Secure Boot, save the changes and exit the BIOS/UEFI settings. Your device will restart and Secure Boot will be enabled.
4. Verify that Secure Boot is enabled: To verify that Secure Boot is enabled, open the System Information app by pressing Windows key + Pause/Break or by searching for "System Information" in the Start menu. Look for the "Secure Boot State" option in the System Summary section. If it says "On," Secure Boot is enabled.
5. **Scan your PC frequently**

If you are not using a third-party antivirus software, open Windows Security, click on “Virus & threats protection” and Scan your PC. If you are using third-party antivirus software, open the software and follow the on-screen instructions to scan your PC.

1. **Enable find my device feature**

To use this feature, your device must be connected to the internet and have location services enabled.

To enable the Find my device feature in Windows 11, follow these steps:

1. Open the Settings app, Click on the “Privacy & Security” option in the left pane and then "Find my device".
2. In the Find my device section, toggle the switch to the "On" position to enable the feature.
3. If prompted, enter your Microsoft account password to verify your identity.
4. Once enabled, you can locate your device by signing in to your Microsoft account on another device and navigating to the "Find my device" section.
5. **Use a password management system**

Using a password manager is a great way to keep track of all your passwords and ensure that they are strong and secure. Here's how to use a password manager:

1. Choose a password manager software between many password manager software options available such as LastPass, 1Password, Bitwarden, Dashlane, Kaspersky Password manager, etc. A good password manager should not be free.
2. Download and install the password manager software on your Windows 11 computer.
3. Open the password manager app and create a strong master password. This password will be used to encrypt all your other passwords, so make sure it's strong and unique.
4. Add your passwords: Start adding your passwords to the password manager. You can usually do this by clicking a button or selecting an option to add a new password. Enter the website or app name, username, and password, and the password manager will save it for you.
5. Use the password manager: Whenever you need to log in to a website or app, the password manager will autofill your login credentials for you. You can also generate new, strong passwords for each account and save them in the password manager.
6. Sync your passwords across devices: Most password managers have a sync feature that allows you to access your passwords on multiple devices. Make sure you set up this feature if you plan to use the password manager on your phone or tablet.
7. **Use a VPN**

Configuring a VPN (Virtual Private Network) in Windows 11 is a straightforward process. Follow these steps to do it:

1. Open the Settings app, click on the "Network & internet" option in the left pane.
2. In the Network & internet section, select the "VPN" option from the left menu.
3. Click the "Add a VPN connection" button, enter the VPN connection details, including the server address, VPN type, and authentication method. This information will be provided by your VPN provider.
4. Click on "Save" to save the VPN connection.
5. Once the VPN connection is created, you can click on it and select "Connect" to connect to the VPN.
6. If prompted, enter your VPN username and password to authenticate the connection.
7. You can also adjust the VPN settings by clicking on the "Advanced options" button.

You can choose to install a VPN directly by installing a VPN software on your Computer. The VPN software provider should provide the instructions for installing and using the VPN.

1. **Use Local Security Policy to configure and manage security policies.**

The Local Security Policy in Windows is a powerful tool that allows you to configure security settings on your local computer. It provides a way to manage and enforce security policies that can help protect your system from various threats. Note that the Local Security Policy is only available on Windows 11 Pro, Enterprise, and Education editions. If you are using Windows 11 Home edition, you will not have access to this tool. It is important to be careful when modifying security policies as incorrect configuration can potentially cause issues with your system's security or functionality. Therefore, it's recommended to make changes only if you know what you are doing or under the guidance of an expert.

Here are the steps to access the Local Security Policy in Windows 11:

1. Press the Windows key + R to open the Run dialog box.
2. Type "secpol.msc" and press Enter. This will open the Local Security Policy console.
3. From here, you can navigate through the different categories to view and configure various security policies, such as account policies, audit policies, user rights assignment, and more.
4. To modify a policy setting, double-click on the policy to open its properties. You can then enable or disable the policy or change its configuration as needed.
5. Take time to search, read and understand the meaning of each element available in Local Security Policy Editor before you make any changes.

In conclusion, there are many tools for security features in Windows. There are many books available for security features in Windows 11. You need to be an expert windows administrator or enhance your Windows skills to master all of them. Those described in this document are what you can use to configure and enforce security features in Windows 11. You can configure all of them for secure experience with the Windows operating system or choose some of them according to your needs.