For more information about best practices, see the Apple Support article Security and your Apple ID.

To set up or manage your Apple ID, go to the Apple ID website.

If you forgot your Apple ID or password, see the Recover your Apple ID website.

Make sign-ins safer and easier

Sign in with passkeys on iPhone

Passkeys give you a simple and secure way to sign in without passwords by relying on Face ID (supported models) or Touch ID (supported models) to identify you when you sign in to supporting websites and apps.

Intro to passkeys

Based on industry standards for account authentication, passkeys are easier to use than passwords and far more secure.

A passkey is a cryptographic entity that's not visible to you, and it's used in place of a password. A passkey consists of a *key pair*, which—compared to a password—profoundly improves security. One key is public, registered with the website or app you're using. The other key is private, held only by your devices. Through the use of powerful, industry-standard cryptography techniques, this key pair helps ensure a strong, private relationship between your devices and the website or app. A passkey has these additional characteristics and conveniences:

- It's always strong and never guessable by a hacker.

- It's linked only with the website or app it was created for, thereby protecting you from getting tricked into using a passkey to sign in to a fraudulent website or app.

- Your iPhone stores the passkey in iCloud Keychain, so it's available on other devices where you're signed in with your Apple ID (iOS 16 or tvOS 16 required).

- It's end-to-end encrypted in iCloud Keychain, so no one—not even Apple—can read it.

- The private key never leaves your devices, so it can't be leaked from websites or apps.

- There's nothing about it that you have to create, guard, or remember.

- You can use AirDrop to securely share a passkey with someone else.

- You can use a passkey on your iPhone to sign in to an account on non-Apple devices.

Draft

Passkeys on iPhone require that you use iCloud Keychain. If you don't have iCloud Keychain turned on when you try to save a passkey, you'll be asked to turn it on. Passkeys also require that two-factor authentication is enabled for your Apple ID.

Note: Passkeys are an industry-wide security standard, and many websites and apps are quickly adding passkey support.


Save a passkey for an account

Depending on the website, browser, or app, saving a passkey to your iPhone and iCloud Keychain usually consists of steps similar to these.

1. On your iPhone, do one of the following:

   - *For a new account:* On the account sign-up screen, enter an account name.

   - *For an existing account:* Sign in with your password, then go to the account management screen.

2. When you see the option to save a passkey for the account, tap Continue.

   Your passkey is saved.
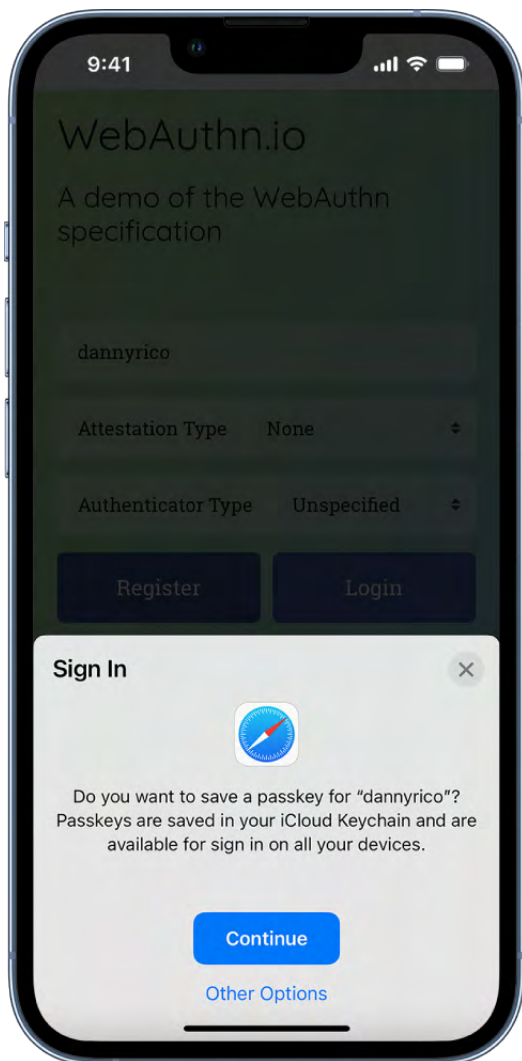
Note: If you want to save your credential to an external security key or to a different device not associated with your Apple ID, you may be able to select Other Options, Save on Another Device, or similar (instead of Continue). Then tap Continue and follow onscreen instructions.

Save a passkey to your iPhone while using a computer or device that's not your own

While using a device that's not associated with your Apple ID (such as a computer at a public library, internet café, or friend's house), you can save a passkey to your iPhone (and iCloud Keychain) instead of to the other device. Saving a passkey to your iPhone usually consists of the following steps:

1. On the other device, do one of the following:

   - *For a new account:* On the account sign-up screen, enter an account name.

   - *For an existing account:* Sign in with your password, then go to the account management screen.

2. When you see the option to save a passkey for the account, select Other Options, Save on Another Device, or similar (instead of Continue).

3. Tap "Save a passkey on a device with a camera" or similar, then follow the onscreen instructions to display a QR code on the screen.

4. Use your iPhone camera to scan the QR code.

Sign in to an account on your iPhone with a passkey

Depending on the website, browser, or app, signing in with your passkey usually consists of steps similar to these.

1. On the sign-in screen for the website or app, tap the account name field.

2. Tap the account suggested at the bottom of the screen or near the top of the keyboard.

3. If your iPhone has Touch ID, follow the onscreen instructions to verify your identity. Otherwise, Face ID verifies your identity.

Note: If you want to sign in on your iPhone using a passkey that's stored on a different device that's not associated with your Apple ID, you may be able to select Other Options (or similar) instead of Continue. Then follow the onscreen instructions.

Sign in on a different device with the passkey stored on your iPhone

iPhone stores your passkeys in iCloud Keychain, so they're automatically used when you're signed in with your Apple ID on another device (iOS 16 or tvOS 16 required).

However, if you use a device that's not associated with your Apple ID, you can still sign in to an account by using the passkey stored on your iPhone. Signing in usually consists of the following steps:

1. Use the other device to go to your account sign-in screen.

2. On the sign-in screen, tap the account name field.

3. Tap "Other options," "Passkey from nearby device," or similar, then follow the onscreen instructions to display a QR code on the screen.

4. Use your iPhone camera to scan the QR code.

Sign in with Apple on iPhone

With Sign in with Apple, you can sign in to participating websites and apps with your Apple ID. You don't need to create and remember new passwords, and your account is protected with two-factor authentication.

Sign in with Apple is designed to respect your privacy. Websites and apps can ask only for your name and email address to set up your account, and Apple won't track you as you use them.

Set up or upgrade an account to Sign in with Apple

When a participating website or app asks you to set up or upgrade an account, do the following:

1. Tap Sign in with Apple.

2. Follow the onscreen instructions.

Some apps (and websites) don't request your name and email address. In this case, you simply authenticate with Face ID or Touch ID (depending on your model), then start using the app.

Others may ask for your name and email address to set up a personalized account. When an app asks for this information, Sign in with Apple displays your name and the personal email address from your Apple ID account for you to review.

To edit your name, tap it, then use the keyboard to make changes.

To specify an email address, do one of the following:

- *Use your personal email address:* Tap Share My Email.

  If you have multiple email addresses associated with your Apple ID, choose the address you want.

- *Hide your email address:* Tap Hide My Email.

  This option allows you to receive email from the app without sharing your personal email address. When you choose this option, Apple creates a unique, random email address for you, and any email sent from the app to this address is forwarded to your personal address.

After you review your information and choose an email option, tap Continue, authenticate with Face ID or Touch ID (depending on your model), then start using the app.

Sign in to access your account

After you set up an account with a website or app using Sign in with Apple, you typically don't need to sign in to it again on your iPhone. But if you're asked to sign in (for example, after you sign out of an account), do the following:

1. Tap Sign in with Apple.

2. Review the Apple ID that appears, then tap Continue.

3. Authenticate with Face ID or Touch ID (depending on your model).

Change the address used to forward email

If you chose to hide your email address when you created an account and you have more than one address associated with your Apple ID, you can change the address that receives your forwarded email.

1. Go to Settings > [*your name*] > Name, Phone Numbers, Email > Forward To.

2. Choose a different email address, then tap Done.

Review or change Sign in with Apple settings for websites and apps

1. Go to Settings > [*your name*] > Password and Security.

2. Tap Apps Using Your Apple ID.

   All apps using Sign in with Apple appear in a list.

3. To change a setting for an app, choose the app, then do any of the following:

   - *Turn off forwarding email:* Turn off Forward To. You won't receive any further emails from the app.

   - *Stop using Sign in with Apple:* Tap Stop Using Apple ID. You may be asked to create a new account the next time you try to sign in with the app.

Sign in with Apple also works on your other devices—iPad, Apple Watch, Mac, Apple TV, and iPod touch—where you're signed in with the same Apple ID.

To sign in from an Android app, a Windows app, or any web browser, tap Sign in with Apple, then enter your Apple ID and password.

Sign in with Apple requires two-factor authentication for your Apple ID. This protects your Apple ID, your app accounts, and your app content.

For more information, see the Apple Support article What is Sign in with Apple?.

Automatically fill in strong passwords on iPhone

When you sign up for services on websites and in apps, you can let iPhone create strong passwords for many of your accounts.

iPhone stores the passwords in iCloud Keychain and fills them in for you automatically, so you don't have to memorize them.

Note: Instead of requiring you to sign in with passwords, participating websites and apps support these alternatives:

- *Sign in with Apple:* Lets you use your Apple ID to sign in, and limits the information shared about you. See Sign in with Apple on iPhone.

- *A passkey:* Lets you use Face ID or Touch ID to securely sign in without using a password. See Sign in with passkeys on iPhone.

Create a strong password for a new account

Depending on the website or app, creating a strong password and saving it to iCloud Keychain usually consists of steps similar to these.

1. On the new account screen for the website or app, enter a new account name.

   For supported websites and apps, iPhone suggests a unique, complex password.

2. Do one of the following:

   - *Choose the suggested password:* Tap Use Strong Password.

   - *Edit the suggested password:* Tap Other Options, tap Edit Strong Password, tap the password text field, then make your changes.

     To copy the password so you can paste it into , double tap the password field, tap Select All, then tap Copy.

   - *Get a different strong password:* Tap Other Options, tap Edit Strong Password, then tap the suggested password.

- *Get a strong password consisting of only numbers and letters:* Tap Other Options, then tap No Special Characters.

- *Get a strong password that's easy to type:* Tap Other Options, then tap Easy to Type.

- *Make up your own password:* Tap Other Options, then tap Choose My Own Password.

3. To later allow iPhone to automatically fill in the password for you, tap Yes when you're asked if you want to save the password.

Note: In order for iPhone to create and store passwords, iCloud Keychain must be turned on. Go to Settings ⚙ > [*your name*] > iCloud > Passwords and Keychain.

Automatically fill in a saved password

Depending on the website or app, signing in with your saved password usually consists of steps similar to these.

1. On the sign-in screen for the website or app, tap the account name field.

2. Do one of the following:

   - Tap the account suggested at the bottom of the screen or near the top of the keyboard.

   - Tap 🔑, tap Other Passwords, then tap an account.

   The password is filled in. To see the password, tap 👁.

To enter an account or password that isn't saved, tap ⌨ on the sign-in screen.

Prevent iPhone from automatically filling in passwords

Go to Settings ⚙ > Passwords > Password Options, then turn off AutoFill Passwords.

Change weak or compromised passwords on iPhone

When you create and store your own passwords for websites and apps, iPhone automatically identifies common weaknesses (for example, if they're easily guessed or used multiple times). iPhone can also securely monitor your passwords and alert you if they appear in known data leaks.

Change a weak or compromised password

1. Go to Settings ⚙ > Passwords > Security Recommendations.

   If an account has a weak or compromised password, a message explains the problem.

2. Tap an account.

3. Tap the Password field, then tap Copy Password, so you can paste it where it's requested—for example, when you create a new password and you're asked to enter your old password.

4. Tap Change Password, then change your password on the website or in the app.

   If the website or app allows you to upgrade to Sign in with Apple, you can take advantage of the security and convenience of that feature. If you aren't given the upgrade option when you change your password, many accounts allow iPhone to automatically create a strong password that you don't have to remember.

Note: If iPhone warns you about a password for a website or app that's no longer available, you can remove its account from your iPhone and iCloud Keychain. Go to Settings ⚙ > Passwords, then swipe left on the account.

Hide a security recommendation

You can hide a security recommendation so that you don't have to continue reviewing it if you're unable to address it.

1. Go to Settings ⚙ > Passwords > Security Recommendations, then tap an account.

2. In the Security Recommendation section, tap ✕, then tap Hide.

To view the recommendation later, go to Settings > Passwords > Security Recommendations, scroll to the bottom of the screen, then tap Hidden Security Recommendations. To reshow all security recommendations, tap Reset Hidden Security Recommendations.

Turn detection of compromised passwords on or off

iPhone can monitor your passwords and alert you if they appear in known data leaks.

Go to Settings ⚙ > Passwords > Security Recommendations, then turn Detect Compromised Passwords on or off.

Draft

View your passwords and related information on iPhone

You can view and copy passwords, add notes like security question reminders, and more with the encrypted account information stored on iPhone. iCloud Keychain securely keeps this information up to date across all your approved devices.

View and copy a password for an app or website account

1. For an account that uses a password, do one of the following:

   - Say something like: "Show me my passwords." Learn how to use Siri.

   - Go to Settings 🔘 > Passwords.

   - On a sign-in screen, tap 🔑.

2. Tap an account, then tap the Password field.

3. To copy the password to use elsewhere, tap Copy Password.

View and copy a password for a Wi-Fi network
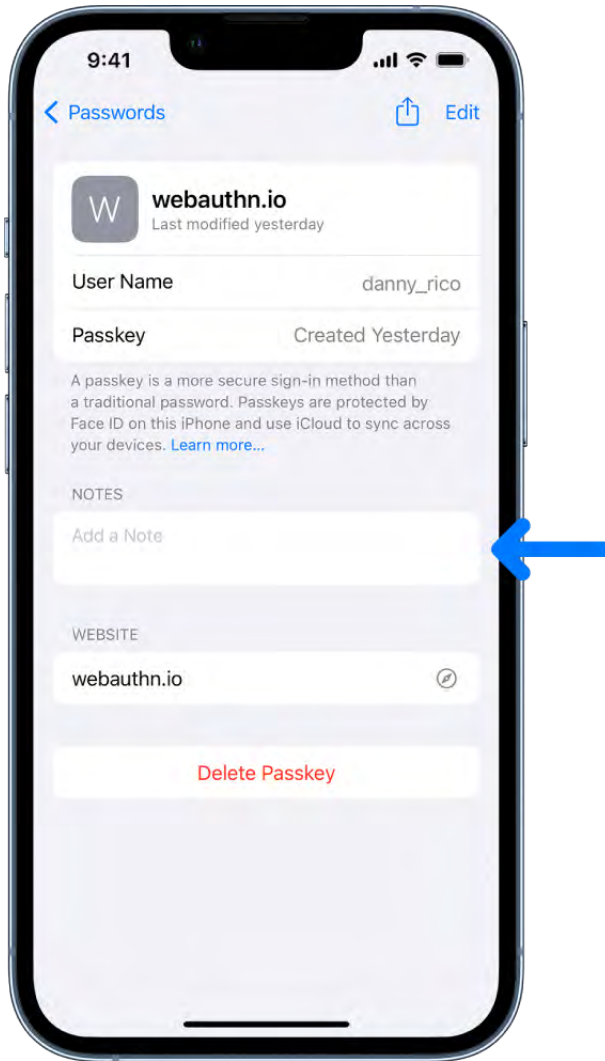
1. Go to Settings 🔘 > Wi-Fi.

   If you're connected to a Wi-Fi network, it's name appears at the top of the screen. To see a list of all saved Wi-Fi networks, tap Edit at the top right.

2. Tap ⓘ next to a network name.

3. Tap the Password field.

4. To copy the password to use elsewhere, tap Copy.

Add notes for an account with a passkey or password

You can securely keep notes about recovery key information, security questions, PIN numbers, and similar details.

1. Go to Settings 🔘 > Passwords, then tap an account.

2. Tap Add Notes, enter your text, then tap Done.

To view the notes later, go to Settings > Passwords, then tap the account. To update the notes, tap Edit (at the top right), then tap the Notes field.

Go to the website for an account

1. Go to Settings ⚙ > Passwords, then tap an account.

2. Do one of the following:

   - Tap ⊘.

   - Tap the website URL, tap Copy Website, then paste the URL into the address field of your browser.

Remove an account from your iPhone and iCloud Keychain

Go to Settings ⚙ > Passwords, then swipe left on the account.

For example, you might want to remove the account for a website or app that's no longer available.

Note: This action doesn't remove the account from the website or app where you created it.

Remove a passkey or password from your iPhone and iCloud Keychain

1. Go to Settings ⚙ > Passwords, then tap an account.

2. Tap Delete Password or Delete Passkey.

Note: This action doesn't remove the passkey or password from the website or app where you created it.

Share passkeys and passwords securely with AirDrop on iPhone

Use AirDrop to securely share passkeys and passwords for app and website accounts with someone using an iPhone, iPad, or Mac.

Note: To show someone the password you saved for a Wi-Fi network, see View and copy a password for a Wi-Fi network.

Check the AirDrop requirements

Compared to sharing other types of information, AirDrop has more stringent requirements for sharing passkeys and passwords.

- iCloud Keychain must be set up on your iPhone.

- The person you're sharing with must be in your contacts list in the Contacts app, and they must be listed with the email address they use for iCloud.

- You must be in the other person's contacts list in the Contacts app, and you must be listed with the email address you use for iCloud.

Send a passkey or password

To share with someone on iPhone or iPad, ask them to open Control Center and allow AirDrop to receive items. To share with someone on a Mac, ask them to allow themselves to be discovered in AirDrop in the Finder.

1. On your iPhone, go to Settings ⚙ > Passwords.

2. Tap the account you want to share.

3. Tap ⬆, then select the device or profile picture of the person you want to send the passkey or password to.

Receive a passkey or password

1. If you haven't already done so, allow AirDrop to receive items.

2. When you receive a request to accept a passkey or password from someone else, tap Accept.

The passkey or password is saved to your iPhone, where you can view its information and let iPhone automatically fill it in on the sign-in screen for the account. The passkey or password is also saved to your iCloud Keychain, so you can use it on other devices where you're signed in with your Apple ID.

Make your passkeys and passwords available on all your devices with iPhone and iCloud Keychain

Use iCloud Keychain to keep your website and app passkeys and passwords, credit card information, Wi-Fi network information, and other account information up to date across all your approved devices and Mac computers (iOS 7, iPadOS 13, OS X 10.9, or later required). iCloud Keychain is secured with 256-bit AES encryption during storage and transmission, and its data cannot be read by Apple.

iCloud Keychain can also keep the accounts you use in Mail, Contacts, Calendar, and Messages up to date across all your iPhone and iPad devices and Mac computers.

Set up iCloud Keychain

If you didn't turn on iCloud Keychain when you first set up your iPhone, go to Settings
 > [*your name*] > iCloud > Passwords and Keychain, turn on iCloud Keychain, then follow the onscreen instructions.

Set up iCloud Keychain on an additional device

When you turn on iCloud Keychain on an additional device, your other devices using iCloud Keychain receive a notification requesting your approval of the additional device.

On one of your other devices, approve the additional device. Your iCloud Keychain automatically begins updating on the additional device.

To approve iCloud Keychain when you don't have access to your other devices, follow the onscreen instructions to use your iCloud Security Code.

Recover your iCloud Keychain if all your devices are lost or stolen

iCloud Keychain synchronization across devices provides convenience and redundancy in case you lose a single device. If all your devices are lost and you've added a recovery contact to your Apple ID account, your contact can help you recover your iCloud Keychain. To learn how, go to Settings > [*your name*] > Password & Security, then tap "Learn more" below Add Recovery Contact.

You can also recover your iCloud Keychain through iCloud Keychain escrow, which is also protected against brute-force attacks. iCloud Keychain escrows a user's keychain data with Apple without allowing Apple to read the passwords and other data it contains. Your keychain is encrypted using a strong passcode, and the escrow service provides a copy of the keychain only if a strict set of conditions is met.

To recover your keychain through iCloud Keychain escrow, authenticate with your Apple ID on a new device, then respond to an SMS sent to a trusted phone number. After you authenticate and respond, you must enter the device passcode. iOS, iPadOS, and macOS allow only 10 attempts to authenticate. After several failed attempts, the record is locked, and you must contact Apple Support on the Apple Support website to be granted more attempts.

To learn more about iCloud Keychain, see the Apple Support article Set up iCloud Keychain.

Draft

Automatically fill in verification codes on iPhone

Some websites and apps offer two-factor authentication (also known as *multifactor authentication*), which helps prevent other people from accessing your accounts even if they know your passwords. Passwords are the first authentication factor, and temporary, one-time verification codes are commonly a second factor. iPhone can automatically generate these verification codes without your reliance on SMS messages or additional apps.

Set up automatic verification codes for a website or app by scanning a QR code

If you have another device with a screen, like a computer or iPad, you can use it to display a QR code from a website or app, then use the iPhone camera to scan the code.

1. On your other device, sign in to the area of the website or app where you manage your account, then select options to enable two-factor authentication and an authenticator app.

   A QR code appears to help you set up an authenticator app.

2. On iPhone, use the camera to scan the QR code.

3. On iPhone, select your account for the website or app.

   A verification code appears below the User Name and Password fields.

4. On your other device, enter the verification code that appears on your iPhone.

Set up automatic verification codes for a website or app by entering a setup key

If you can't scan a QR code from another screen, you can manually enter a setup key.

1. Sign in to the area of the website or app where you manage your account, then select options to enable two-factor authentication and an authenticator app.

2. Choose the option to manually use a setup key (or setup code or similar), then select and copy the setup key.

3. Go to Settings > Passwords, then select your account for the website or app.

4. Tap Set Up Verification Code, then tap Enter Setup Key.

5. Tap the Setup Key field, tap Paste, then tap OK.

6. Tap the Verification Code field, then tap Copy Verification Code.

7. Return to the website or app, then paste the verification code where directed.

Use a verification code on a website or in an app

1. Sign in to the website or app.

2. If prompted, select the option to use an authenticator app.

3. When asked for a verification code, tap the suggestion that appears above the keyboard.

   If no suggestion appears, go to Settings ⚙ > Passwords, select your account for the website or app, tap the verification code, then tap Copy Verification Code. Return to the website or app, then paste the verification code into the field.

Automatically fill in SMS passcodes on iPhone

When you sign in to some websites and apps, a one-time SMS passcode is sent to your iPhone. As a security measure, you're required to enter the code into the website or app. iPhone can detect the passcode in Messages and display it above the keyboard.

To use the passcode, tap it.

Note: With Continuity, all the SMS and MMS messages you send and receive on iPhone can also appear on your other iPhone, iPad, and iPod touch devices and your Mac. See the Apple Support article Use Continuity to connect your Mac, iPhone, iPad, iPod touch, and Apple Watch.

Sign in with fewer CAPTCHA challenges on iPhone

Some app and website sign-ins require you to pass CAPTCHA challenges, such as by recognizing letters in unusual shapes. iCloud allows you to bypass many challenges by automatically and privately verifying your iPhone and account. You can turn this bypass on or off.

Go to Settings ⚙ > [*your name*] > Password & Security, then turn Automatic Verification on or off.

Manage two-factor authentication for your Apple ID from iPhone

Two-factor authentication helps prevent others from accessing your Apple ID account, even if they know your Apple ID password. Certain features in iOS, iPadOS, and macOS require the security of two-factor authentication. With two-factor authentication enabled, only you can access your account on a trusted device or the web. When you sign in to a new device for the first time, you need to provide two pieces of information—your Apple ID password and the six-digit verification code that's automatically sent to your phone number or displayed on your trusted devices. By entering the code, you verify that you trust the new device.Two-factor authentication for Apple ID is available in iOS 9, iPadOS 13, OS X 10.11, or later.

If you create a new Apple ID on a device with iOS 13.4, iPadOS 13.4, macOS 10.15.4, or later, your account automatically uses two-factor authentication. If you previously created an Apple ID account without two-factor authentication, you can turn on its extra layer of security at any time.

Note: Certain account types may be ineligible for two-factor authentication at the discretion of Apple. Two-factor authentication isn't available in all countries or regions. See the Apple Support article Availability of two-factor authentication for Apple ID.

For information about how two-factor authentication works, see the Apple Support article Two-factor authentication for Apple ID.

Draft

Turn on two-factor authentication

1. If your Apple ID account isn't already using two-factor authentication, go to Settings ◉ > [*your name*] > Password & Security.

2. Tap Turn On Two-Factor Authentication, then tap Continue.

3. Enter a *trusted phone number,* a phone number where you want to receive verification codes for two-factor authentication (it can be the number for your iPhone).

   You can choose to receive the codes by text message or automated phone call.

4. Tap Next.

5. Enter the verification code sent to your trusted phone number.

   To send or resend a verification code, tap "Didn't get a verification code?"

   You won't be asked for a verification code again on your iPhone unless you sign out completely, erase your iPhone, sign in to your Apple ID account page in a web browser, or need to change your Apple ID password for security reasons.

After you turn on two-factor authentication, you have a two-week period during which you can turn it off. After that period, you can't turn off two-factor authentication. To turn it off, open your confirmation email and click the link to return to your previous security settings. Keep in mind that turning off two-factor authentication makes your account less secure and means you can't use features that require a higher level of security.

Note: If you use two-step verification and upgrade to iOS 13 or later, your account might be migrated to use two-factor authentication. See the Apple Support article Two-step verification for Apple ID.

Add another device as a trusted device

A trusted device is one that can be used to verify your identity by displaying a verification code from Apple when you sign in on a different device or browser. A trusted device must meet these minimum system requirements: iOS 9, iPadOS 13, or OS X 10.11.

1. After you turn on two-factor authentication on one device, sign in with the same Apple ID on another device.

2. When you're asked to enter a six-digit verification code, do one of the following:

   - *Obtain the verification code on your iPhone or another trusted device that's connected to the internet:* Look for a notification on that device, then tap or click Allow to make the code appear on that device. (A trusted device is an iPhone,

iPad, or Mac on which you've already turned on two-factor authentication and on which you're signed in with your Apple ID.)

- *Obtain the verification code at a trusted phone number:* If a trusted device isn't available, tap "Didn't get a verification code?" then choose a phone number.

- *Obtain the verification code on a trusted device that's offline:* On a trusted iPhone or iPad, go to Settings > [*your name*] > Password & Security, then tap Get Verification Code. On a trusted Mac, do one of the following:

  - *macOS 10.15 to 12.5:* Choose Apple menu > System Preferences > Apple ID > Password & Security, then click Get Verification Code.

  - *macOS 10.14 and earlier:* Choose Apple menu > System Preferences > iCloud > Account Details > Security, then click Get Verification Code.

3. Enter the verification code on the new device.

   You won't be asked for a verification code again unless you sign out completely, erase your device, sign in to your Apple ID account page in a web browser, or need to change your Apple ID password for security reasons.

Add or remove a trusted phone number

When you enrolled in two-factor authentication, you had to verify one trusted phone number. You should also consider adding other phone numbers you can access, such as a home phone, or a number used by a family member or close friend.

1. Go to Settings ⚙ > [*your name*] > Password & Security.

2. Tap Edit (above the list of trusted phone numbers), then do one of the following:

   - *Add a number:* Tap Add a Trusted Phone Number.

   - *Remove a number:* Tap ⊖ next to the phone number.

Trusted phone numbers don't automatically receive verification codes. If you can't access any trusted devices when setting up a new device for two-factor authentication, tap "Didn't get a verification code?" on the new device, then choose one of your trusted phone numbers to receive the verification code.

View or remove trusted devices

1. Go to Settings ⚙ > [*your name*].

   A list of the devices associated with your Apple ID appears near the bottom of the screen.

2. To see if a listed device is trusted, tap it, then look for "This device is trusted and can receive Apple ID verification codes."

3. To remove a device, tap it, then tap Remove from Account.

   Removing a trusted device ensures that it can no longer display verification codes and that access to iCloud (and other Apple services on the device) is blocked until you sign in again with two-factor authentication.

Generate a password for an app that signs in to your Apple ID account

With two-factor authentication, you need an app-specific password to sign in to your Apple ID account from a third-party app or service—such as an email, contacts, or calendar app. After you generate the app-specific password, use it to sign in to your Apple ID account from the app and access the information you store in iCloud.

1. Sign in to your Apple ID account.

2. Tap App-Specific Passwords, then tap "Generate an app-specific password."

3. Follow the onscreen instructions.

After you generate your app-specific password, enter or paste it into the password field of the app as you would normally.

For more information, see the Apple Support article Using app-specific passwords.

Manage what you share with people and apps

Manage information sharing with Safety Check on iPhone

Use Safety Check to periodically review and update information you share with people, apps, and devices. With Safety Check, you can stop sharing your location with others via Find My, remove others' access to shared content like Photos, Notes, and Calendar, reset system privacy permissions for apps, restrict Messages and FaceTime to the device in your hand, and more.
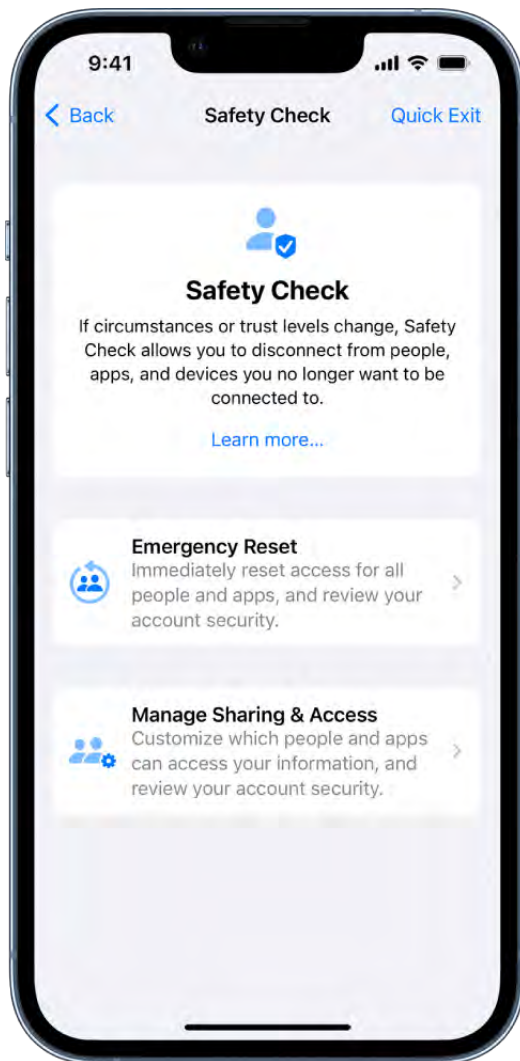
1. Go to Settings ⚙ > Privacy & Security > Safety Check.

2. Tap Manage Sharing & Access, tap Continue, then follow the onscreen instructions.

Important: In an emergency, you can also use Safety Check to quickly reset access. Go to Settings > Privacy & Security > Safety Check, tap Emergency Reset, tap Start Emergency Reset, then follow the onscreen instructions.

To learn what Safety Check does, see How Safety Check on iPhone works to keep you safe in the Personal Safety User Guide.

Control app tracking permissions on iPhone

All apps are required to ask your permission before tracking you or your iPhone across websites or apps owned by other companies for advertising or to share your information with data brokers. After you grant or deny permission to an app, you can change permission later. You can also stop all apps from requesting permission.

Review or change an app's permission to track you

1. Go to Settings 🌐 > Privacy & Security > Tracking.

   The list shows the apps that requested permission to track you. You can turn permission on or off for any app on the list.

2. To stop all apps from asking permission to track you, turn off Allow Apps to Request to Track (at the top of the screen).

For more information about app tracking, tap Learn More near the top of the screen.

Control the location information you share on iPhone

You control whether iPhone and apps have information about your location.

To figure out where you are when getting directions, setting up meetings, and more, Location Services uses information (when available) from GPS networks, your Bluetooth connections, your local Wi-Fi networks, and your cellular network. When an app is using Location Services, ➤ appears in the status bar.

When you set up iPhone, you're asked if you want to turn on Location Services. Afterward, you can turn Location Services on or off at any time.

The first time an app wants location data from your iPhone, you receive a request with an explanation. Some apps may make a one-time only request for your location. Other apps may ask you to share your location now and in the future. Whether you grant or deny ongoing access to your location, you can change an app's access later.
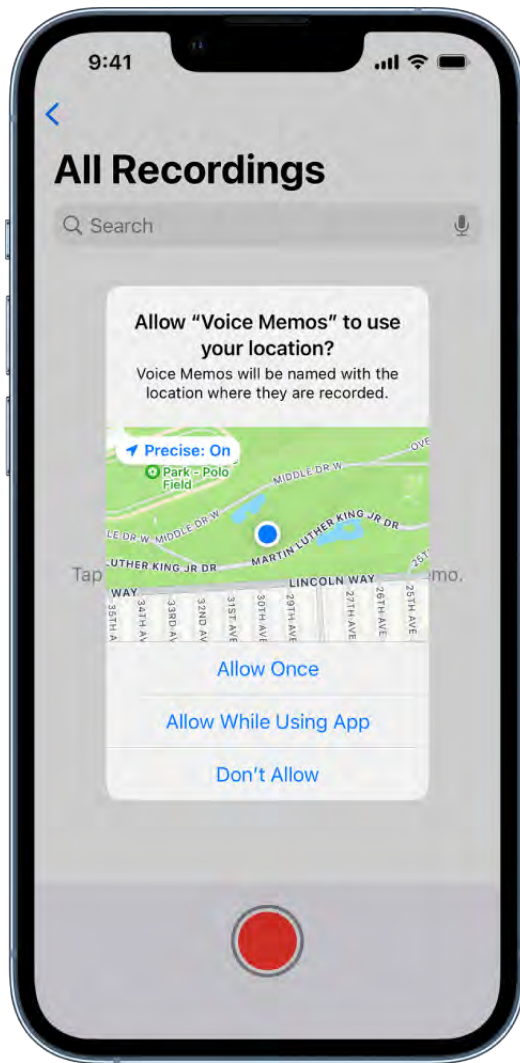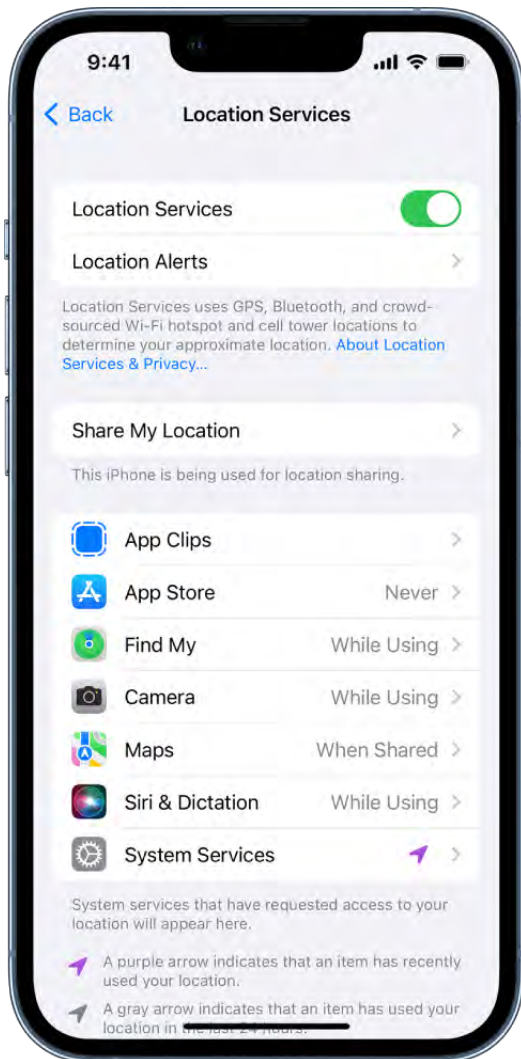
Turn on Location Services

If you didn't turn on Location Services when you first set up iPhone, go to Settings ⚙ > Privacy & Security > Location Services, then turn on Location Services.

Important: If you turn off Location Services, many important iPhone features stop working.

Review or change an app's ongoing access to location information

1. Go to Settings ⚙️ > Privacy & Security > Location Services.

2. To review or change access settings for an app or to see its explanation for requesting Location Services, tap the app.

To allow an app to use your specific location, leave Precise Location turned on. To share only your approximate location—which may be sufficient for an app that doesn't need your exact location—turn Precise Location off.

Note: If you set the access for an app to Ask Next Time, you're asked to turn on Location Services again the next time an app tries to use it.

To understand how a third-party app uses the information it's requesting, review its terms and privacy policy. See the Apple Support article About privacy and Location Services.

Hide the map in Location Services alerts

When you allow an app to always use your location in the background, you may receive alerts about the app's use of that information. (These alerts let you change your permission, if you want to.) In the alerts, a map shows locations recently accessed by the app.

To hide the map, go to Settings 🔘 > Privacy & Security > Location Services > Location Alerts, then turn off Show Map in Location Alerts.

With the setting off, you continue to receive location alerts, but the map isn't shown.

Review or change Location Services settings for system services

Several system services, such as location-based suggestions and location-based ads, use Location Services.

To see the status for each service, to turn Location Services on or off for each service, or to show ➤ in the status bar when enabled system services use your location, go to Settings 🔘 > Privacy & Security > Location Services > System Services.

Control access to information in apps on iPhone

You control whether third-party apps have access to information in Contacts, Photos, Calendar, and other apps.

Review or change access to information in apps

The first time an app wants to use information from another app, you receive a request with an explanation. For example, a messaging app may request access to your contacts to find friends who are using the same app. After you grant or deny access, you can change access later.

1. Go to Settings 🔘 > Privacy & Security.

2. Tap a category of information, such as Calendars, Reminders, or Motion & Fitness.
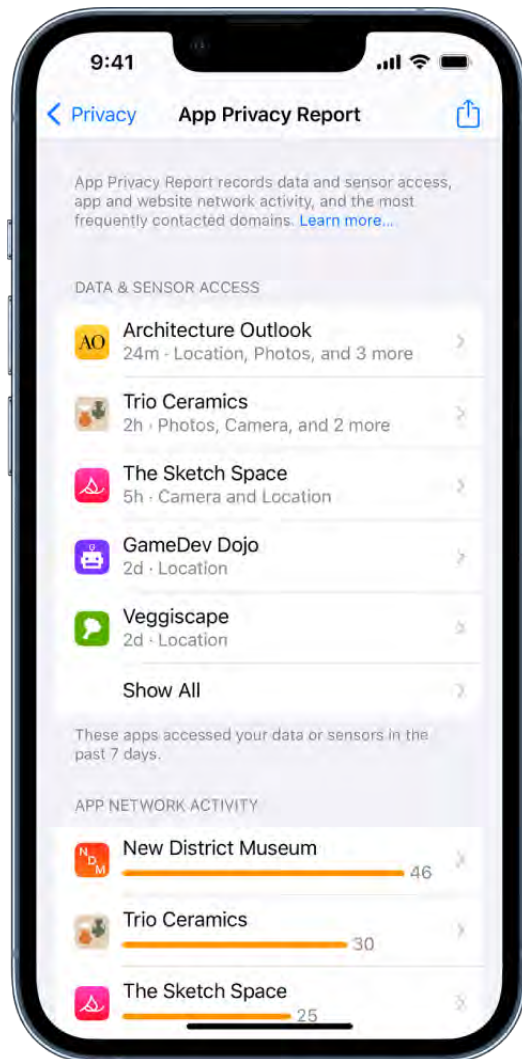
The list shows the apps that requested access. You can turn access on or off for any app on the list.

Review how apps are using the permissions you grant them

Go to Settings 🔘 > Privacy & Security, then tap App Privacy Report.

The App Privacy Report shows you how apps are using the permissions you granted them and shows you their network activity.

To turn off the report and delete its data, go to Settings ⚙ > Privacy & Security > App Privacy Report, then tap Turn Off App Privacy Report. You can return to this Settings screen to turn the report on again.

Control how Apple delivers advertising to you on iPhone

You control how Apple delivers advertising.

Ads delivered by Apple may appear in the App Store, Apple News, and Stocks. These ads don't access data from any other apps. In the App Store and Apple News, your search and download history may be used to serve you relevant search ads. In Apple News and Stocks, ads are served based partly on what you read or follow. This includes publishers you've enabled notifications for and the type of publishing subscription you have. The

articles you read are not used to serve targeted ads to you outside these apps, and information collected about what you read is linked to a random identifier rather than your Apple ID.

Review the information Apple uses to deliver ads

Go to Settings ⚙ > Privacy & Security > Apple Advertising > View Ad Targeting Information.

The information is used by Apple to deliver more relevant ads in the App Store, Apple News, and Stocks. Your personal data isn't provided to other parties.

Turn personalized ads on or off

Go to Settings ⚙ > Privacy & Security > Apple Advertising, then turn Personalized Ads on or off.

Note: Turning off personalized ads limits Apple's ability to deliver relevant ads to you. It may not reduce the number of ads you receive.

Learn more about privacy and Apple's advertising platform

Go to Settings ⚙ > Privacy & Security > Apple Advertising > About Advertising & Privacy.

Control access to hardware features on iPhone

Before apps use the camera or microphone on your iPhone, they're required to request your permission and explain why they're asking. For example, a social networking app may ask to use your camera so that you can take and upload pictures to that app. Apps are similarly required to request your permission to use various other hardware features, including Bluetooth connectivity, motion and fitness sensors, and devices on your local network.

You can review which apps have requested access to these hardware features, and you can change their access at your discretion.

Review or change access to the camera, microphone, and other hardware features

1. Go to Settings ⚙ > Privacy & Security.

2. Tap a hardware feature, such as Camera, Bluetooth, Local Network, or Microphone.

The list shows the apps that requested access. You can turn access on or off for any app on the list.

Note: Whenever an app uses the camera (including when the camera and microphone are used together), a green indicator appears. An orange indicator appears at the top of the screen whenever an app uses the microphone without the camera. Also, a message appears at the top of Control Center to inform you when an app has recently used either.
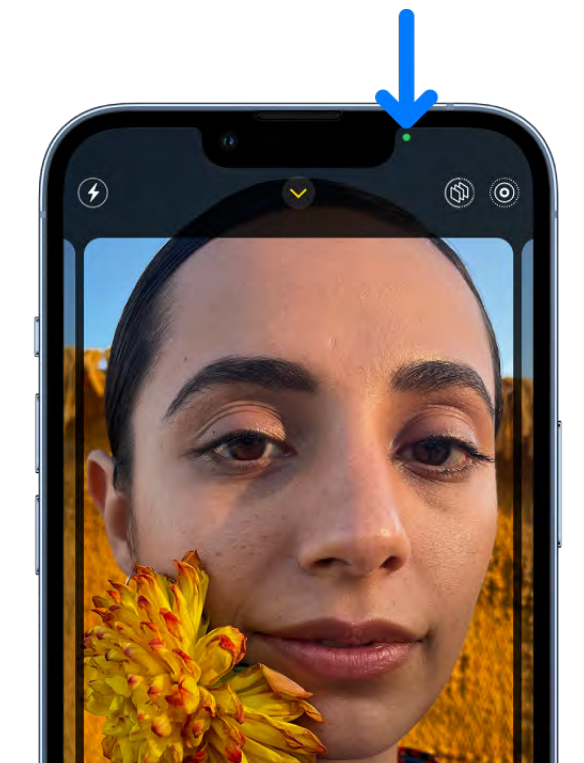
Create and manage Hide My Email addresses in Settings on iPhone

When you subscribe to iCloud+, you can use Hide My Email to keep your personal email address private. With Hide My Email, you can generate unique, random email addresses that forward to your personal email account, so you don't have to share your real email address when filling out forms or signing up for newsletters on the web, or when sending email.

You can create and manage Hide My Email addresses in Settings ⚙️. Go to Settings > [*your name*] > iCloud > Hide My Email, then do any of the following:

- *Create a Hide My Email address:* Tap Create New Address, then follow the onscreen instructions.

- *Deactivate a Hide My Email address:* Tap an address (below Create New Address), then tap Deactivate Email Address. After you deactivate the address, it no longer forwards emails to you.

- *Change which personal email address to forward to:* Tap Forward To, then choose an email address. Options consist of addresses that are available with your Apple ID.

- *Copy a forwarding address to use elsewhere:* Tap an address (below Create New Address), touch and hold the Hide My Email section, then tap Copy. To immediately use that address elsewhere, touch and hold in a text field, then tap Paste.

You can also generate Hide My Email addresses in Safari and Mail wherever email addresses are required. See Use Hide My Email in Safari on iPhone and Use Hide My Email in Mail on iPhone. In supporting apps, you can also generate a Hide My Email address when an email address is required by tapping the email address field, then tapping Hide My Email above the keyboard.

Protect your web browsing with iCloud Private Relay on iPhone

When you subscribe to iCloud+, you can use iCloud Private Relay to help prevent websites and network providers from creating a detailed profile about you. When iCloud Private Relay is turned on, the traffic leaving your iPhone is encrypted and sent through two separate internet relays. This prevents websites from seeing your IP address and exact location while preventing network providers from collecting your browsing activity in Safari.

You can turn off iCloud Private Relay at any time. You can turn off the feature completely for iPhone, or just turn it off for a specific Wi-Fi or cellular network.

Turn iCloud Private Relay completely on or off for iPhone

Go to Settings ⚙ > [*your name*] > iCloud > Private Relay.

Note: You need to turn on iCloud Private Relay on each device where you want to use it.

Turn iCloud Private Relay on or off for a Wi-Fi network

1. Go to Settings ⚙ > Wi-Fi.

2. Tap ⓘ, then turn Limit IP Address Tracking on or off.

If you turn off Limit IP Address Tracking for a Wi-Fi network on your iPhone, iCloud Private Relay is turned off for this network across all your devices where you're signed in with the same Apple ID.

Turn iCloud Private Relay on or off for a cellular network

1. Go to Settings ⚙ > Cellular, then do one of the following:

   - *If your iPhone has a single line:* Tap Cellular Data Options.

   - *If your iPhone has multiple lines:* Select a line (below Cellular Plans).

2. Turn Limit IP Address Tracking on or off.

The network setting is specific to a physical SIM or eSim in your iPhone (eSIM not available in all countries or regions). See View or change cellular data settings on iPhone.

Set the specificity of your IP address location

Go to Settings ⚙ > [*your name*] > iCloud > Private Relay > IP Address Location, then choose one of the following:

- Maintain General Location (for example, to see local content in Safari)

- Use Country and Time Zone (to make your location more obscure)

iCloud Private Relay is not available in all countries or regions.

Harden your iPhone from a cyberattack with Lockdown Mode

Lockdown Mode is an extreme, optional protection for iPhone that should be used only if you believe you may be targeted by a highly sophisticated cyberattack, such as by a private company developing state-sponsored mercenary spyware.

Important: Most people are never targeted by attacks of this nature.

When iPhone is in Lockdown Mode, it won't function as it typically does. Apps, websites, and features will be strictly limited for security, and some experiences won't be available.

Learn about Lockdown Mode

Go to Settings > Privacy & Security > Lockdown Mode, then tap Learn More.

Turn on Lockdown Mode

Go to Settings > Privacy & Security > Lockdown Mode, then turn on Lockdown Mode.

Use a private network address on iPhone

To help protect your privacy, your iPhone uses a unique private network address, called a *media access control (MAC) address*, on each Wi-Fi network it joins.

If a network can't use a private address (for example, to provide parental controls or to identify your iPhone as authorized to join), you can stop using a private address for that network.

Turn a private address off for a network

1. Go to Settings ⚙ > Wi-Fi, then tap ⓘ for a network.

2. Turn Private Address off.

   Important: For better privacy, leave Private Address turned on for all networks that support it. Using a private address helps reduce tracking of your iPhone across different Wi-Fi networks.

Restart, update, reset, and restore

Turn iPhone on or off

Use the side button to turn on iPhone. You can use the side button (along with either volume button on some models) or Settings ⚙ to turn off iPhone.

If your iPhone isn't working as expected, you can try restarting it by turning it off, then turning it back on. If turning it off and on doesn't fix the issue, try forcing it to restart.

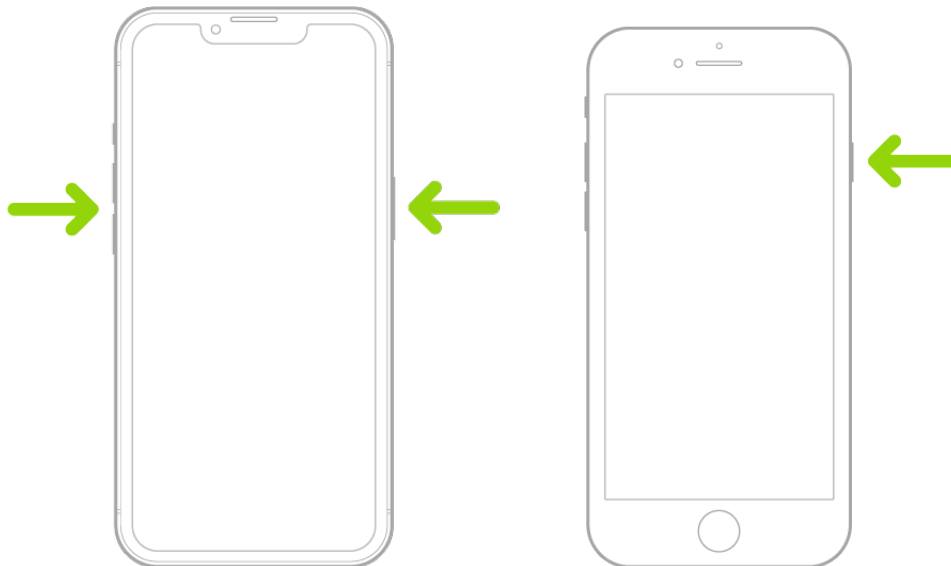**Turn on iPhone**

Press and hold the side button until the Apple logo appears.

Turn off iPhone

- *iPhone with Face ID:* Simultaneously press and hold the side button and either volume button until the sliders appear, then drag the Power Off slider.

- *iPhone with the Home button:* Press and hold the side button, then drag the slider.

- *All models:* Go to Settings ⚙ > General > Shut Down, then drag the slider.

Force restart iPhone

If iPhone isn't responding, and you can't turn it off then on, try forcing it to restart.

---

1. Press and quickly release the volume up button.

2. Press and quickly release the volume down button.

3. Press and hold the side button.

4. When the Apple logo appears, release the side button.
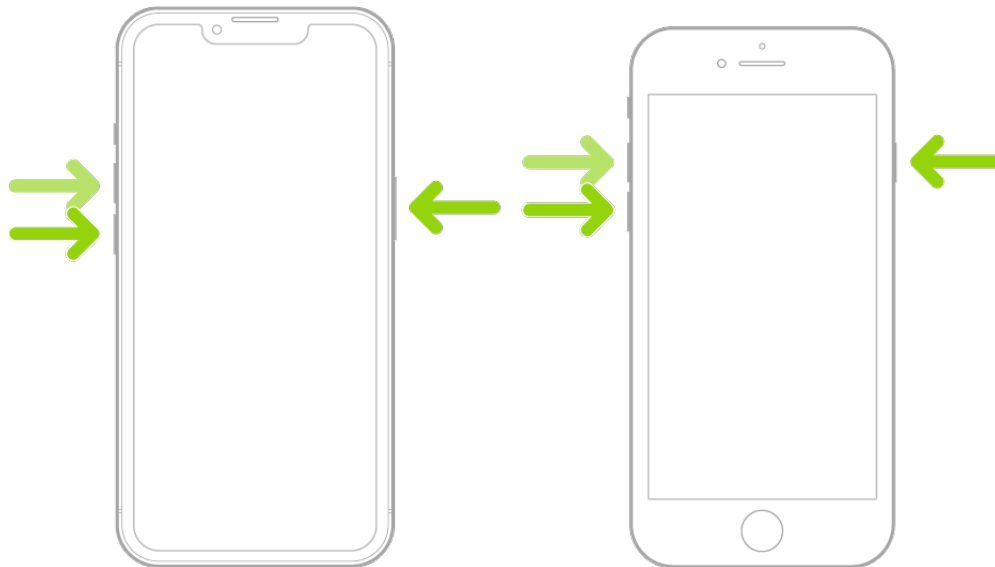
Note: For force restart instructions for iPhone 7, iPhone 6s, or iPhone SE (1st generation) —models that don't support iOS 16—see the iOS 15 version of this page.

If iPhone doesn't restart after you try these steps, see the Apple Support article If your iPhone won't turn on or is frozen. Or if your iPhone isn't working as expected after you restart it, see the iPhone Support website.

Update iOS on iPhone

When you update to the latest version of iOS, your data and settings remain unchanged.

Before you update, set up iPhone to back up automatically, or back up your device manually.

Update iPhone automatically

If you didn't turn on automatic updates when you first set up your iPhone, do the following:

1. Go to Settings 🔘 > General > Software Update > Automatic Updates.

2. Turn on Download iOS Updates and Install iOS Updates.

When an update is available, iPhone downloads and installs the update overnight while charging and connected to Wi-Fi. You're notified before an update is installed.

Update iPhone manually

At any time, you can check for and install software updates.

Go to Settings 🔘 > General > Software Update.

The screen shows the currently installed version of iOS and whether an update is available.

To turn off automatic updates, go to Settings > General > Software Update > Automatic Updates.

Update using your computer

1. Connect iPhone and your computer with a cable.

2. Do one of the following:

   • *On a Mac (macOS 10.15 or later):* In the Finder sidebar, select your iPhone, then click General at the top of the window.

   • *On a Mac (macOS 10.14 or earlier) or a Windows PC:* Open the iTunes app, click the button resembling an iPhone near the top left of the iTunes window, then click Summary.

     Note: Use the latest version of iTunes. See the Apple Support article Update to the latest version of iTunes.

3. Click Check for Update.

4. To install an available update, click Update.

See the Apple Support articles Update to the latest iOS and If you can't update or restore your iPhone, iPad, or iPod touch.

Back up iPhone

You can back up iPhone using iCloud or your computer. To decide which method is best for you, see About backups for iPhone, iPad, and iPod touch.

Tip: If you replace your iPhone, you can use its backup to transfer your information to the new device. See Restore all content to iPhone from a backup.

Back up iPhone using iCloud

1. Go to Settings ⚙ > [*your name*] > iCloud > iCloud Backup.

2. Turn on iCloud Backup.

   iCloud automatically backs up your iPhone daily when iPhone is connected to power, locked, and connected to Wi-Fi.

   Note: On models that support 5G, your carrier may give you the option to back up iPhone using your cellular network. Go to Settings > [*your name*] > iCloud > iCloud Backup, then turn on or off Backup Over Cellular.

3. To perform a manual backup, tap Back Up Now.

To view your iCloud backups, go to Settings > [*your name*] > iCloud > Manage Account Storage > Backups. To delete a backup, choose a backup from the list, then tap Delete & Turn Off Backup.

Note: If you turn on an app or feature to use iCloud syncing (in Settings > [*your name*] > iCloud > Show All), its information is stored in iCloud. Because the information is automatically kept up to date on all your devices, it's not included in your iCloud backup. (See the Apple Support article What does iCloud back up?)

Back up iPhone using your Mac

1. Connect iPhone and your computer with a cable.

2. In the Finder sidebar on your Mac, select your iPhone.

   To use the Finder to back up iPhone, macOS 10.15 or later is required. With earlier versions of macOS, use iTunes to back up iPhone.

3. At the top of the Finder window, click General.

4. Select "Back up all of the data on your iPhone to this Mac."

5. To encrypt your backup data and protect it with a password, select "Encrypt local backup."

6. Click Back Up Now.

Note: You can also connect iPhone to your computer wirelessly if you set up syncing over Wi-Fi.

Back up iPhone using your Windows PC

1. Connect iPhone and your computer with a cable.

2. In the iTunes app on your PC, click the iPhone button near the top left of the iTunes window.

3. Click Summary.

4. Click Back Up Now (below Backups).

5. To encrypt your backups, select "Encrypt local backup," type a password, then click Set Password.

To see the backups stored on your computer, choose Edit > Preferences, then click Devices. Encrypted backups have a lock icon in the list of backups.

Note: You can also connect iPhone to your computer wirelessly if you set up syncing over Wi-Fi.

Return iPhone settings to their defaults

You can return settings to their defaults without erasing your content.

If you want to save your settings, back up iPhone before returning them to their defaults. For example, if you're trying to solve a problem but returning settings to their defaults doesn't help, you might want to restore your previous settings from a backup.

1. Go to Settings ⚙ > General > Transfer or Reset iPhone > Reset.

2. Choose an option:

   WARNING: If you choose the Erase All Content and Settings option, all of your content is removed. See Erase iPhone.

   - *Reset All Settings:* All settings—including network settings, the keyboard dictionary, location settings, privacy settings, and Apple Pay cards—are removed or reset to their defaults. No data or media are deleted.

   - *Reset Network Settings:* All network settings are removed. In addition, the device name assigned in Settings > General > About is reset to "iPhone," and manually trusted certificates (such as for websites) are changed to untrusted.

     Cellular data roaming may also be turned off. (See View or change cellular data settings on iPhone.)

     When you reset network settings, previously used networks and VPN settings that weren't installed by a configuration profile or mobile device management (MDM) are removed. Wi-Fi is turned off and then back on, disconnecting you from any network you're on. The Wi-Fi and Ask to Join Networks settings remain turned on.

     To remove VPN settings installed by a configuration profile, go to Settings > General > VPN & Device Management, select the configuration profile, then tap Remove Profile. This also removes other settings and accounts provided by the profile. See Install or remove configuration profiles on iPhone in this guide.

     To remove network settings installed by MDM, go to Settings > General > VPN & Device Management, select the management, then tap Remove Management. This also removes other settings and certificates provided by MDM. See "Mobile device management (MDM)" in the iOS Deployment Reference.

   - *Reset Keyboard Dictionary:* You add words to the keyboard dictionary by rejecting words iPhone suggests as you type. Resetting the keyboard dictionary erases only the words you've added.

   - *Reset Home Screen Layout:* Returns the built-in apps to their original layout on the Home Screen.

- *Reset Location & Privacy:* Resets the location services and privacy settings to their defaults.

If you want to completely erase your iPhone, see Use Settings to erase iPhone. If you want or need to use a computer to erase your iPhone, see Use a computer to erase iPhone.

Restore all content to iPhone from a backup

You can restore content, settings, and apps from a backup to a new or newly erased iPhone.

Important: You must first create a backup of your iPhone. See Back up iPhone.

Restore iPhone from an iCloud backup

1. Turn on a new or newly erased iPhone.

2. Follow the online instructions to choose a language and region.

3. Tap Set Up Manually.

4. Tap Restore from iCloud Backup, then follow the onscreen instructions.

You're asked for your Apple ID. If you've forgotten your Apple ID, see the Recover your Apple ID website.

Restore iPhone from a computer backup

1. Using USB, connect a new or newly erased iPhone to the computer containing your backup.

2. Do one of the following:

   - *On a Mac (macOS 10.15 or later):* In the Finder sidebar, select your iPhone, click Trust, then click "Restore from this backup."

   - *On a Mac (macOS 10.14 or earlier) or a Windows PC:* Open the iTunes app, click the button resembling an iPhone near the top left of the iTunes window, click Summary, then click Restore Backup.

     Note: Use the latest version of iTunes. See the Apple Support article Update to the latest version of iTunes.

3. Choose your backup from the list, then click Continue.

If your backup is encrypted, you must enter the password before restoring your files and settings.

See the Apple Support articles Restore your iPhone, iPad, or iPod touch from a backup and If you can't update or restore your iPhone, iPad, or iPod touch.

Restore purchased and deleted items to iPhone

You can redownload items purchased from the App Store, Book Store, Apple TV app, and iTunes Store without repurchasing them. If you're part of a Family Sharing group, you can download items purchased by other family members, too. To restore purchases that aren't on your iPhone, see the following Apple Support articles:

- Redownload apps and games from Apple

- Redownload books and audiobooks

- Redownload TV shows and movies that you purchased

- Redownload music

You can also recover recently deleted email, photos, notes, and voice memos.

Sell, give away, or trade in your iPhone

Before you sell, give away, or trade in your iPhone, see the Apple Support article What to do before you sell, give away, or trade in your iPhone, iPad, or iPod touch, and be sure to perform the following tasks:

- If you paired an Apple Watch with your iPhone, unpair your Apple Watch. (See the Apple Support article Unpair and erase your Apple Watch.)

- Back up iPhone. If you replace one iPhone with another, you can use the setup assistant to restore the backup to your new iPhone.

  If you're replacing your iPhone with another one you have on hand, you can use extra free storage in iCloud to move your apps and data from one iPhone to another. Go to Settings ⚙ > General > Transfer or Reset iPhone > Get Started, then follow the onscreen instructions.

- Sign out of iCloud and the iTunes & App Store. Go to Settings > *[your name]*, scroll down, tap Sign Out, enter your Apple ID password, then tap Turn Off.

- Erase all content and settings that contain personal information. If you previously turned on Find My for your iPhone, Activation Lock is removed when you erase iPhone, making it ready for a new owner.

Erase iPhone

When you delete data, it no longer appears in apps on iPhone, but it isn't erased from iPhone storage. To permanently remove all of your content and settings from your iPhone, erase (wipe) your iPhone. For example, erase iPhone before you sell it, trade it in, or give it away.

There are two ways to erase iPhone: using Settings ⚙ on your iPhone, or connecting iPhone to a computer with a USB cable and using the Finder or iTunes. The Settings method is the easiest. If you're unable to open Settings, you need to connect iPhone to a computer and use the Finder or iTunes.

Before you begin

- If you intend to sell your iPhone, trade it in, or give it away, see the Apple Support article What to do before you sell, give away, or trade in your iPhone, iPad, or iPod touch for steps to take before erasing iPhone.

- To save your content and settings, back up your iPhone shortly before erasing it or when you're given the option during the erase process. You can use the backup to later restore your data on a new iPhone or iPad.

- Have your iPhone passcode ready. If you don't remember it, see the Apple Support article If you forgot the passcode on your iPhone, or your iPhone is disabled.

- Have your Apple ID password ready. If you don't remember it, see the Recover your Apple ID website.

- If you received your iPhone from someone else and it's still associated with their Apple ID, return it to them and ask them to follow the instructions in the Apple Support article What to do before you sell, give away, or trade in your iPhone, iPad, or iPod touch. Otherwise, you won't be able to erase it.

Use Settings to erase iPhone

1. Go to Settings ⚙ > General > Transfer or Reset iPhone.

2. Do one of the following:

   - *Prepare your content and settings to transfer to a new iPhone:* Tap Get Started, then follow the onscreen instructions. When you finish, return to Settings > General > Transfer or Reset iPhone, then tap Erase All Content and Settings.

   - *Erase all of your data from iPhone:* Tap Erase All Content and Settings.

Use a computer to erase iPhone

You can use a Mac or Windows PC to erase all data and settings from your iPhone, restore iPhone to factory settings, and install the latest version of iOS.

1. Connect your iPhone to your computer with a USB or USB-C cable. You may also need an adapter. See Connect iPhone and your computer with a cable.

2. Turn on your iPhone.

3. Do one of the following:

- *On a Mac (macOS 10.15 or later):* Click the Finder icon in the Dock to open a Finder window, click the iPhone button in the Finder sidebar (below Locations), click General at the top of the window, then click Restore iPhone.

- *On a Mac (macOS 10.14 or earlier) or a Windows PC:* Make sure you have the latest version of iTunes (see the Apple Support article Update to the latest version of iTunes). Open iTunes, click the iPhone button near the top left of the iTunes window, click Summary, then click Restore iPhone.

For troubleshooting steps, see the Apple Support article If you can't update or restore your iPhone.

Install or remove configuration profiles on iPhone

Configuration profiles define settings for using iPhone with corporate or school networks or accounts. You might be asked to install a configuration profile that was sent to you in an email, or one that is downloaded from a webpage. You're asked for permission to install the profile and, when you open the file, information about what it contains is displayed. You can see the profiles you have installed in Settings 🔘 > General > VPN & Device Management. If you delete a profile, all of the settings, apps, and data associated with the profile are also deleted.

Safety, handling, and support

Important safety information for iPhone

WARNING: Failure to follow these safety instructions could result in fire, electric shock, injury, or damage to iPhone or other property. Read all the safety information below before using iPhone.

Handling. Handle iPhone with care. It is made of metal, glass, and plastic and has sensitive electronic components inside. iPhone or its battery can be damaged if dropped, burned, punctured, or crushed, or if it comes in contact with liquid. If you suspect damage to iPhone or the battery, discontinue use of iPhone, as it may cause overheating or injury. Don't use iPhone with cracked glass, as it may cause injury. If you're concerned about scratching the surface of iPhone, consider using a case or cover.

Repairing. iPhone should only be serviced by a trained technician. Disassembling iPhone may damage it, result in loss of splash and water resistance (supported models), or cause injury to you. If iPhone is damaged or malfunctions, you should contact Apple, or an Apple Authorized Service Provider for service. Repairs performed by untrained individuals or using non-genuine Apple parts may affect the safety and functionality of the device. You can find more information about repairs and service at the iPhone Repair website.

Battery. An iPhone battery should only be repaired by a trained technician to avoid battery damage, which could cause overheating, fire, or injury. Batteries should be recycled or disposed of separately from household waste and according to local environmental laws and guidelines. For information about battery service and recycling, see the Battery Service and Recycling website.

Lasers. The proximity sensor in iPhone 7 and later, the TrueDepth camera system, and the LiDAR Scanner contain one or more lasers. These laser systems may be disabled for safety reasons if the device is damaged or malfunctions. If you receive a notification on your iPhone that the laser system is disabled, you should contact Apple or an Apple Authorized Service Provider for service. Improper repair, modification, or use of non-genuine Apple components in the laser systems may prevent the safety mechanisms from functioning properly, and could cause hazardous exposure and injury to eyes or skin.

Draft

Distraction. Using iPhone in some circumstances may distract you and might cause a dangerous situation (for example, avoid using headphones while riding a bicycle and avoid typing a text message while driving a car). Observe rules that prohibit or restrict the use of mobile devices or headphones. For more about safety while driving, see Stay focused while driving with iPhone.

Navigation. Maps depends on data services. These data services are subject to change and may not be available in all countries or regions, resulting in maps and location-based information that may be unavailable, inaccurate, or incomplete. Compare the information provided in Maps to your surroundings. Use common sense when navigating. Always observe current road conditions and posted signs to resolve any discrepancies. Some Maps features require Location Services.

Charging. To charge iPhone, do any of the following:

- Charge the iPhone battery using the charging cable (included) and an Apple USB power adapter (sold separately).

- Place iPhone face up on MagSafe Charger or MagSafe Duo Charger (connected to Apple 20W USB-C power adapter or other compatible power adapter) or on a Qi-certified charger. (Supported on iPhone 8 and later; MagSafe Charger, MagSafe Duo Charger, power adapters, and Qi-certified chargers are sold separately.)

- Connect iPhone and your computer with a cable.

You can also charge iPhone with "Made for iPhone" or other third-party cables and power adapters that are compliant with USB 2.0 or later and with applicable country regulations and international and regional safety standards. Other adapters may not meet applicable safety standards, and charging with such adapters could pose a risk of death or injury.

Using damaged cables or chargers, or charging when moisture is present, can cause fire, electric shock, injury, or damage to iPhone or other property. When you use the charging cable (included) or a wireless charger (sold separately) to charge iPhone, make sure its USB connector is fully inserted into a compatible power adapter before you plug the adapter into a power outlet. It's important to keep iPhone, the charging cable, the power adapter, and any wireless charger in a well-ventilated area when in use or charging. When using a wireless charger, remove metallic cases and avoid placing metallic foreign objects on the charger (for example, keys, coins, batteries, or jewelry), as they may become warm or interfere with charging.

Charging cable and connector. Avoid prolonged skin contact with the charging cable and connector when the charging cable is connected to a power source because it may cause discomfort or injury. Sleeping or sitting on the charging cable or connector should

be avoided.

Prolonged heat exposure. iPhone and Apple USB power adapters (sold separately) comply with required surface temperature limits defined by applicable country regulations and international and regional safety standards. However, even within these limits, sustained contact with warm surfaces for long periods of time may cause discomfort or injury. Use common sense to avoid situations where your skin is in contact with a device, its power adapter, or a wireless charger when it's operating or connected to a power source for long periods of time. For example, don't sleep on a device, power adapter, or wireless charger, or place them under a blanket, pillow, or your body, when it's connected to a power source. Keep your iPhone, the power adapter, and any wireless charger in a well-ventilated area when in use or charging. Take special care if you have a physical condition that affects your ability to detect heat against the body.

USB power adapter. (sold separately) To operate an Apple USB power adapter safely and reduce the possibility of heat-related injury or damage, plug the power adapter directly into a power outlet. Don't use the power adapter in wet locations, such as near a sink, bathtub, or shower stall, and don't connect or disconnect the power adapter with wet hands. Stop using the power adapter and any cables if any of the following conditions exist:

- The power adapter plug or prongs are damaged.

- The charge cable becomes frayed or otherwise damaged.

- The power adapter is exposed to excessive moisture, or liquid is spilled into the power adapter.

- The power adapter has been dropped, and its enclosure is damaged.

Apple 20W USB-C power adapter specifications:

- *Frequency:* 50 to 60 Hz, single phase

- *Line voltage:* 100 to 240 V

- *Output Voltage/Current:* 9 VDC/2.2A

- *Minimum Power Output:* 20W

- *Output Port:* USB-C

Apple 18W USB-C power adapter specifications:

- *Frequency:* 50 to 60 Hz, single phase

- *Line voltage:* 100 to 240 V

- *Output voltage:* 5V/3A or 9V/2A

- *Output Port:* USB-C

Apple 5W USB power adapter specifications:

- *Frequency:* 50 to 60 Hz, single phase

- *Line voltage:* 100 to 240 V

- *Output voltage:* 5V/1A

- *Output Port:* USB

Hearing loss. Listening to sound at high volumes may damage your hearing. Background noise, as well as continued exposure to high volume levels, can make sounds seem quieter than they actually are. Turn on audio playback and check the volume before inserting anything in your ear. For information about how to set a maximum volume limit, see Use headphone audio level features on iPhone. For more information about hearing loss, see the Sound and Hearing website.

WARNING: To prevent possible hearing damage, do not listen at high volume levels for long periods.

Radio frequency exposure. iPhone uses radio signals to connect to wireless networks. For information about radio frequency (RF) energy resulting from radio signals, and steps you can take to minimize exposure, go to Settings > General > Legal & Regulatory > RF Exposure, or see the RF Exposure website.

Radio frequency interference. Observe signs and notices that prohibit or restrict the use of electronic devices. Although iPhone is designed, tested, and manufactured to comply with regulations governing radio frequency emissions, such emissions from iPhone can negatively affect the operation of other electronic equipment, causing them to malfunction. When use is prohibited, such as while traveling in aircraft, or when asked to do so by authorities, turn off iPhone, or use airplane mode or Settings > Wi-Fi and Settings > Bluetooth to turn off the iPhone wireless transmitters.

Medical device interference. iPhone and MagSafe accessories contain magnets as well as components and/or radios that emit electromagnetic fields. These magnets and electromagnetic fields might interfere with medical devices.

Consult your physician and medical device manufacturer for information specific to your medical device and whether you need to maintain a safe distance of separation between your medical device and iPhone and MagSafe accessories. Manufacturers often provide recommendations on the safe use of their devices around wireless or magnetic products to prevent possible interference. If you suspect iPhone and MagSafe accessories are interfering with your medical device, stop using these products.

Medical devices such as implanted pacemakers and defibrillators may contain sensors that respond to magnets and radios when in close contact. To avoid any potential interactions with these devices, keep your MagSafe compatible iPhone models and MagSafe accessories a safe distance away from your device (more than 6 inches/15 cm, or more than 12 inches/30 cm while wirelessly charging, but consult with your physician and your device manufacturer for specific guidelines).

Not a medical device. iPhone is not a medical device and should not be used as a substitute for professional medical judgment. It is not designed or intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of any condition or disease. Please consult your healthcare provider prior to making any decisions related to your health.

Medical conditions. If you have any medical condition or experience symptoms that you believe could be affected by iPhone or flashing lights (for example, seizures, blackouts, eyestrain, or headaches), consult with your physician prior to using iPhone.

Explosive and other atmospheric conditions. Charging or using iPhone in any area with a potentially explosive atmosphere, such as areas where the air contains high levels of flammable chemicals, vapors, or particles (such as grain, dust, or metal powders), may be hazardous. Exposing iPhone to environments having high concentrations of industrial chemicals, including near evaporating liquified gasses such as helium, may damage or impair iPhone functionality. Obey all signs and instructions.

Repetitive motion. When you perform repetitive activities such as typing, swiping, or playing games on iPhone, you may experience discomfort in your hands, arms, wrists, shoulders, neck, or other parts of your body. If you experience discomfort, stop using iPhone and consult a physician.

High-consequence activities. This device is not intended for use where the failure of the device could lead to death, personal injury, or severe environmental damage.

Choking hazard. Some iPhone accessories may present a choking hazard to small children. Keep these accessories away from small children.

Important handling information for iPhone

Cleaning. Clean iPhone immediately if it comes in contact with anything that may cause stains, or other damage—for example, dirt or sand, ink, makeup, soap, detergent, acids or acidic foods, or lotions. To clean:

- Disconnect all cables, then do one of the following to turn off iPhone:

  - *On an iPhone with Face ID:* Simultaneously press and hold the side button and either volume button until the sliders appear, then drag the top slider.

  - *On an iPhone with a Home button:* Press and hold the side button, then drag the slider.

  - *All models:* Go to Settings ⚙ > General > Shut Down, then drag the slider.

- Use a soft, slightly damp, lint-free cloth—for example, a lens cloth.

- Avoid getting moisture in openings.

- Don't use cleaning products or compressed air.

iPhone has a fingerprint-resistant oleophobic (oil-repellant) coating. This coating wears over time with normal usage. Cleaning products and abrasive materials will further diminish the coating and may scratch iPhone.

Exposure to liquid and dust. If liquid splashes on iPhone or dust gets on it, wipe it off with a soft, lint-free cloth (for example, a lens cloth) and ensure that your iPhone is dry and free of dust before opening the SIM tray. Minimize exposing iPhone to soap, detergent, acids or acidic foods, and any liquids—for example, salt water, soapy water, pool water, perfume, insect repellent, lotion, sunscreen, oil, adhesive remover, hair dye, and solvents. If iPhone comes into contact with any of these substances, follow the instructions above in the Cleaning section.

Supported models are splash, water, and dust resistant and were tested under controlled laboratory conditions with a rating of either IP68 or IP67 under IEC standard 60529. Splash, water, and dust resistance are not permanent conditions and resistance might decrease as a result of normal wear. Liquid damage not covered under warranty. See the Apple Support article About splash, water, and dust resistance of iPhone 7 and later. To prevent liquid damage on iPhone, avoid the following:

- Swimming or bathing with iPhone

- Exposing iPhone to pressurized water or high velocity water, such as when showering, water skiing, wake boarding, surfing, jet skiing, and so on

- Using iPhone in a sauna or steam room

- Intentionally submerging iPhone in water

- Operating iPhone outside the suggested temperature ranges or in extremely humid conditions

- Dropping iPhone or subjecting it to other impacts

- Disassembling iPhone, including removing screws

If your iPhone has been exposed to liquid, unplug all cables and do not charge your device until it's completely dry. Using accessories or charging when wet may damage your iPhone. Allow at least 5 hours before charging or connecting a Lightning accessory.

To dry iPhone, tap it gently against your hand with the Lightning connector facing down to remove excess liquid. Leave the device in a dry area with sufficient airflow. Placing the device in front of a fan blowing cool air directly into the Lightning connector may help the drying process.

Do not dry your iPhone using an external heat source or insert a foreign object into the Lightning connector such as a cotton swab or a paper towel.

Using connectors, ports, and buttons. Never force a connector into a port or apply excessive pressure to a button, because this may cause damage that is not covered under the warranty. If the connector and port don't join with reasonable ease, they probably don't match. Check for obstructions and make sure that the connector matches the port and that you have positioned the connector correctly in relation to the port.

Lightning to USB Cable or USB-C to Lightning Cable. Discoloration of the Lightning connector after regular use is normal. Dirt, debris, and exposure to moisture may cause discoloration. If your Lightning cable or connector becomes warm during use or iPhone won't charge or sync, disconnect it from your computer or power adapter and clean the Lightning connector with a soft, dry, lint-free cloth. Do not use liquids or cleaning products when cleaning the Lightning connector.

Certain usage patterns can contribute to the fraying or breaking of cables. The included cable, like any other metal wire or cable, is subject to becoming weak or brittle if repeatedly bent in the same spot. Aim for gentle curves instead of angles in the cable. Regularly inspect the cable and connector for any kinks, breaks, bends, or other damage. Should you find any such damage, discontinue use of the cable.

Operating temperature. iPhone is designed to work in ambient temperatures between 32° and 95° F (0° and 35° C) and stored in temperatures between -4° and 113° F (-20° and 45° C). iPhone can be damaged and battery life shortened if stored or operated outside of these temperature ranges. Avoid exposing iPhone to dramatic changes in temperature or humidity. When you're using iPhone or charging the battery, it is normal for iPhone to get warm.

If the interior temperature of iPhone exceeds normal operating temperatures (for example, in a hot car or in direct sunlight for extended periods of time), you may experience the following as it attempts to regulate its temperature:

- iPhone stops charging.

- The screen dims.

- A temperature warning screen appears.

- Some apps may close.

Important: You may not be able to use iPhone while the temperature warning screen is displayed. If iPhone can't regulate its internal temperature, it goes into deep sleep mode until it cools. Move iPhone to a cooler location out of direct sunlight and wait a few minutes before trying to use iPhone again.

See the Apple Support article Keeping iPhone, iPad, and iPod touch within acceptable operating temperatures.

Find more resources for iPhone software and service

Refer to the following resources to get more iPhone-related safety, software, and service information.

To learn about	Do this
Using iPhone safely	See Important safety information for iPhone.
iPhone service and support, tips, forums, and Apple software downloads	See the iPhone Support website.
Service and support from your carrier	Contact your carrier or go to your carrier's website.
The latest information about iPhone	See the iPhone website.
Getting personalized support (not available in all countries or regions)	See the Apple Support website.
Managing your Apple ID account	Sign in to your Apple ID account page.
Using iCloud	See the iCloud User Guide.
Using iTunes for Windows	See the iTunes User Guide for Windows.
Using other Apple iPhone apps	See the App Store Support website.
Finding your iPhone serial number, IMEI, ICCID, or MEID	You can find your iPhone serial number, International Mobile Equipment Identity (IMEI), Integrated Circuit Card Identifier (ICCID), or Mobile Equipment Identifier (MEID) on the iPhone packaging. Or, on iPhone, go to Settings ⚙ > General > About. See the Apple Support article Find the serial number or IMEI on your iPhone, iPad, or iPod touch.
Obtaining warranty service	First follow the advice in this guide, then see the iPhone Support website.
Viewing iPhone regulatory information	On iPhone, go to Settings ⚙ > General > Legal & Regulatory.
Battery service	See the Battery Service and Recycling website.
Battery performance and health	See the iPhone Battery and Performance website.
Using iPhone in an enterprise environment	See the Apple at Work website.

FCC compliance statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications to this product not authorized by Apple could void the electromagnetic compatibility (EMC) and wireless compliance and negate your authority to operate the product.

This product has demonstrated EMC compliance under conditions that included the use of compliant peripheral devices and shielded cables between system components. It is important that you use compliant peripheral devices and shielded cables between system components to reduce the possibility of causing interference to radios, televisions, and other electronic devices.

Responsible party (contact for FCC matters only):

Apple Inc.
One Apple Park Way, MS 911-AHW
Cupertino, CA 95014

USA

apple.com/contact

ISED Canada compliance statement

This device complies with ISED Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Le présent appareil est conforme aux CNR d'ISDE Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

La bande 5150–5250 MHz est réservée uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Ultra Wideband information

Ultra Wideband is available on iPhone 11 and later models, and availability varies by region.

Ultra Wideband must be turned off when onboard aircraft, ships, and other prohibited regions by turning on airplane mode. To turn on airplane mode, open Control Center, then tap ✈. You can also turn airplane mode on or off in Settings ⚙. When airplane mode is on, ✈ appears in the status bar.

Australia: Ultra Wideband transmitters must not be operated within a nominated distance from specified Australian radio-astronomy sites. For further information about nominated distance, please refer to the Radiocommunications (Low Interference Potential Devices) Class Licence 2015 published by the Australian Communications and Media Authority.

Class 1 Laser information for iPhone

iPhone 7 and later are classified as Class 1 Laser products per IEC 60825-1 Ed. 3. These devices comply with 21 CFR 1040.10 and 1040.11, except for conformance with IEC 60825-1 Ed. 3., as described in Laser Notice No. 56, dated May 8, 2019. Caution: These devices contain one or more lasers. Use other than as described in the user guide, repair, or disassembly may cause damage, which could result in hazardous exposure to infrared laser emissions that are not visible. This equipment should be serviced by Apple or an authorized service provider.

CLASS 1 LASER PRODUCT
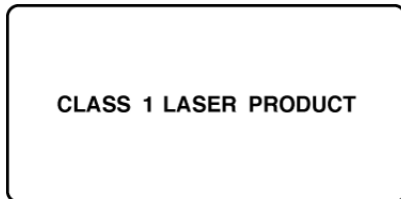
Apple and the environment

At Apple, we recognize our responsibility to minimize the environmental impacts of our operations and products. See our Environment website.

Disposal and recycling information for iPhone

Apple Recycling Program (available in some countries or regions)

For free recycling of your old device, a prepaid shipping label, and instructions, see the Apple Trade In website.

Disposal and Recycling Information

The symbol above means that according to local laws and regulations your product and/or its battery shall be disposed of separately from household waste. When this product reaches its end of life, take it to a collection point designated by local authorities. The separate collection and recycling of your product and/or its battery at the time of disposal will help conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For information about Apple's recycling program, recycling collection points, restricted substances, and other environmental initiatives, visit apple.com/environment.

Brasil – Informações sobre descarte e reciclagem

O símbolo acima indica que este produto e/ou sua bateria não devem ser descartados no lixo doméstico. Quando decidir descartar este produto e/ou sua bateria, faça-o de acordo com as leis e diretrizes ambientais locais. Para informações sobre substâncias de uso restrito, o programa de reciclagem da Apple, pontos de coleta e telefone de informações, visite apple.com/br/environment.

Información sobre eliminación de residuos y reciclaje

El símbolo de arriba indica que este producto y/o su batería no debe desecharse con los residuos domésticos. Cuando decidas desechar este producto y/o su batería, hazlo de conformidad con las leyes y directrices ambientales locales. Para obtener información sobre el programa de reciclaje de Apple, puntos de recolección para reciclaje, sustancias restringidas y otras iniciativas ambientales, visita apple.com/mx/environment o apple.com/la/environment.

Turkey environmental information

Türkiye Cumhuriyeti: AEEE Yönetmeliğine Uygundur.

Battery service

The lithium-ion battery in iPhone should be serviced by Apple or an authorized service provider, and must be recycled or disposed of separately from household waste. See the Battery Service and Recycling website.

Dispose of batteries according to your local environmental laws and guidelines.

China mainland battery statement

警告：不要刺破或焚烧。该电池不含水银。

Taiwan battery statement

廢電池請回收

警告：請勿戳刺或焚燒。此電池不含汞。

Apple, the Apple logo, 3D Touch, AirDrop, AirPlay, AirPods, AirPods Pro, AirPrint, Apple Books, Apple Music, Apple Pay, Apple Podcasts, Apple TV, Apple Wallet, Apple Watch, CarPlay, EarPods, Face ID, FaceTime, Finder, Flyover, Guided Access, Handoff, HomeKit, HomePod, iMessage, iPad, iPad Air, iPad mini, iPadOS,

Draft