

Use the built-in security and privacy protections of iPhone

iPhone is designed to protect your data and your privacy. Built-in security features help prevent anyone but you from accessing the data on your iPhone and in iCloud. Built-in privacy features minimize how much of your information is available to anyone but you, and you can adjust what information is shared and where you share it.

To take maximum advantage of the security and privacy features built into iPhone, follow these practices.

Protect access to your iPhone

- *Set a strong passcode:* [Setting a passcode](#) to unlock iPhone is the most important thing you can do to safeguard your device.
- *Use Face ID or Touch ID:* Face ID ([supported models](#)) or Touch ID ([supported models](#)) provides a secure and convenient way to unlock your iPhone, authorize purchases and payments, and sign in to many third-party apps. See [Set up Face ID on iPhone](#) or [Set up Touch ID on iPhone](#).
- *Turn on Find My iPhone:* Find My helps you [find your iPhone](#) if it's lost or stolen and prevents anyone else from activating or using your iPhone if it's missing.
- *Control what features are available without unlocking your iPhone:* [Disallow or allow access](#) to some commonly used features, such as Control Center and USB connections, when your device is locked.

Keep your Apple ID secure

Your [Apple ID](#) provides access to your data in iCloud and your account information for services like the App Store and Apple Music. To learn how to protect the security of your Apple ID, see [Keep your Apple ID secure on iPhone](#).

This guide copied from [Apple Official website](#) and edited by [iphone14manual.com](#) for iPhone user's.

Make account sign-ins safer and easier

For participating websites and apps, there are multiple ways to make sign-in more convenient and secure.

- *Sign in with passkeys:* Passkeys let you [sign in](#) to website and app accounts with Face ID or Touch ID instead of a password. Because a passkey doesn't leave the devices where you're signed in with your Apple ID, and because it's specific to the website or app you create it for, it's protected from leaks and phishing attempts. And unlike a password, you don't have to create, guard, or remember it.
- *Use Sign in with Apple:* You can use your Apple ID instead of creating and remembering user names and passwords for signing in to accounts. [Sign in with Apple](#) also provides the security of [two-factor authentication](#), and it limits the information shared about you.
- *Let iPhone create strong passwords:* If passkey support or Sign in with Apple isn't available when you sign up for a service, let iPhone automatically [create a strong password](#) that you don't have to remember.

For all your website and app passwords, there are many other ways to make sign-in safer and easier.

- *Replace weak passwords:* If you create any weak or compromised passwords, iPhone automatically [identifies them](#) for you to fix.
- *Share passkeys and passwords securely:* Use AirDrop to securely [share a passkey or password](#) with someone using their iPhone, iPad, or Mac.
- *Use the built-in authenticator for two-factor authentication:* For websites and apps that offer two-factor authentication, [fill in automatically generated verification codes](#) without relying on SMS messages or additional apps.
- *Easily fill in SMS passcodes:* You can automatically [fill in one-time passcodes](#) sent from websites and apps to your iPhone.
- *Keep passkeys and passwords up to date on all your devices:* iCloud Keychain automatically [keeps your credentials](#) up to date across your other devices.

Manage the information you share with people and apps

- *Use Safety Check:* You can quickly and conveniently [review and update](#) information you share with people and apps. If your personal safety is at risk, you can also use Safety Check to immediately [stop sharing information](#).
- *Control app tracking:* All apps are required to ask your permission before tracking you or your iPhone across websites and apps owned by other companies for advertising or to share your

information with a data broker. You can [change permission](#) later, and you can stop all apps from requesting permission.

- *Control what you share with apps:* You can review and adjust [the data you share with apps](#), [the location information you share](#), [the hardware you share](#), and [how Apple delivers advertising to you in the App Store, Apple News, and Stocks](#).
- *Review the privacy practices of apps:* [Go to the app's product page](#) in the App Store for a developer-reported summary of the app's privacy practices, including what data is collected. For the apps that you download, [review the App Privacy Report](#), which shows you how apps are using the permissions you granted them.

Protect your email privacy

- *Protect your Mail activity:* [Turn on Mail Privacy Protection](#) to make it harder for senders to learn about your Mail activity. Mail Privacy Protection hides your IP address so senders can't link it to your other online activity or use it to determine your exact location. Mail Privacy Protection also prevents senders from seeing whether you've opened the email they sent you.
- *Hide your personal email address:* When you subscribe to iCloud+, Hide My Email allows you to generate unique, random email addresses that forward to your personal email account. You don't have to share your personal email address when [filling out forms or signing up for newsletters](#) on the web, or when [sending email](#).

Protect your web browsing

- *Use the internet more privately with iCloud Private Relay (beta):* 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.
- *Manage your privacy, and help protect yourself against malicious websites:* Safari helps prevent trackers from following you across websites. You can review the Privacy Report to see a summary of trackers that have been encountered and prevented by Intelligent Tracking Prevention on the current webpage you're visiting. You can also review and adjust Safari settings to keep your browsing activities private from others who use the same device, and help protect yourself from malicious websites. See [Browse privately in Safari on iPhone](#).

This guide copied from [Apple Official website](#) and edited by [iphone14manual.com](#) for iPhone user's.

Lock down your iPhone if it's facing a sophisticated cyberattack

If you find your iPhone and personal accounts are targeted by sophisticated remote attacks, you can also help protect yourself with Lockdown Mode. Lockdown Mode offers an extreme level of security for the very few users who, because of who they are or what they do, may be personally targeted by some of the most sophisticated digital threats, such as those from private companies developing state-sponsored mercenary spyware. Lockdown Mode automatically protects Safari, Messages, Home, and many other Apple services and apps. Webpages and internet communications continue working, but with reduction in performance and usability. See [Harden your iPhone from a cyberattack with Lockdown Mode](#).


To get personalized support for these practices, go to the [Apple Support website](#) (not available in all countries or regions).

To learn how Apple designs security into the core of its platforms, see the [Apple Platform Security User Guide](#). To learn more about how Apple protects your information, go to the [Privacy website](#).

Set a passcode on iPhone

For better security, set a passcode that needs to be entered to unlock iPhone when you turn it on or wake it. Setting a passcode also turns on data protection, which encrypts your iPhone data with 256-bit AES encryption. (Some apps may opt out of using data protection.)

Set or change the passcode


1. Go to Settings , then do one of the following:
 - *On an iPhone with Face ID:* Tap Face ID & Passcode.
 - *On an iPhone with a Home button:* Tap Touch ID & Passcode.
2. Tap Turn Passcode On or Change Passcode.

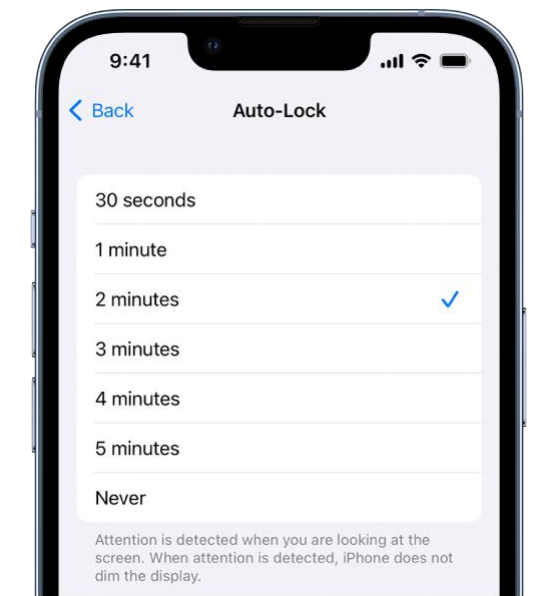
To view options for creating a password, tap Passcode Options. The most secure options are Custom Alphanumeric Code and Custom Numeric Code.

After you set a passcode, you can [use Face ID](#) or [Touch ID](#) to unlock iPhone (depending on your model). For additional security, however, you must always enter your passcode to unlock your iPhone under the following conditions:

- You turn on or restart your iPhone.
- You haven't unlocked your iPhone for more than 48 hours.
- You haven't unlocked your iPhone with the passcode in the last 6.5 days, and you haven't unlocked it with Face ID or Touch ID in the last 4 hours.
- Your iPhone receives a remote lock command.
- There are five unsuccessful attempts to unlock your iPhone with Face ID or Touch ID.
- An attempt to use Emergency SOS is initiated (see [Use Emergency SOS](#)).
- An attempt to view your Medical ID is initiated (see [Set up and view your Medical ID](#)).


Change when iPhone automatically locks

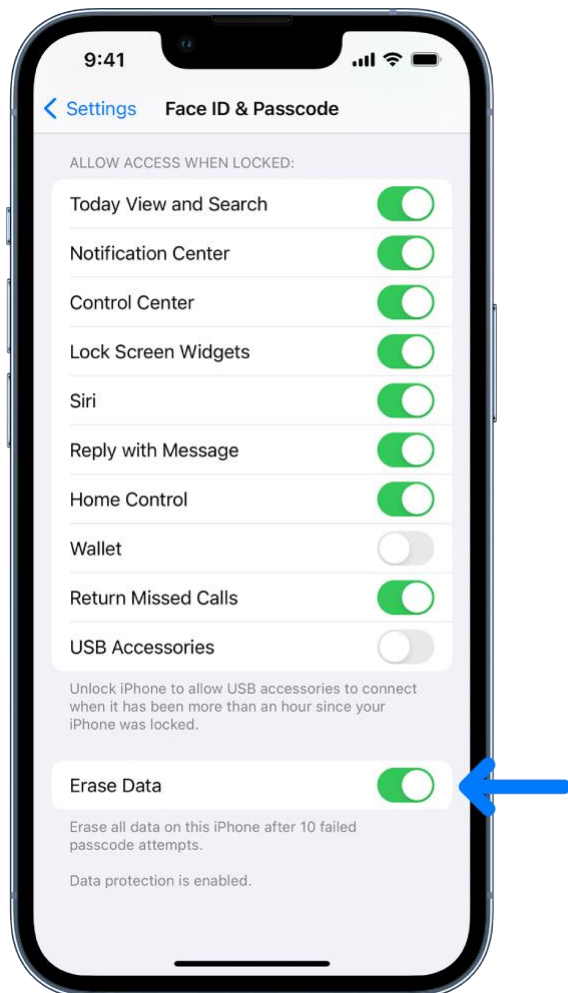
Go to Settings  > Display & Brightness > Auto-Lock, then set a length of time.



Erase data after 10 failed passcodes


Set iPhone to erase all information, media, and personal settings after 10 consecutive failed passcode attempts.

1. Go to Settings , then do one of the following:
 - *On an iPhone with Face ID:* Tap Face ID & Passcode.
 - *On an iPhone with a Home button:* Tap Touch ID & Passcode.
2. Scroll to the bottom and turn on Erase Data.



After all data is erased, you must [restore your device from a backup](#) or [set it up again as new](#).

Turn off the passcode

1. Go to Settings , then do one of the following:
 - On an iPhone with Face ID: Tap Face ID & Passcode.
 - On an iPhone with a Home button: Tap Touch ID & Passcode.
2. Tap Turn Passcode Off.

Reset the passcode

If you enter the wrong passcode six times in a row, you'll be locked out of your device, and you'll receive a message that says iPhone is disabled. If you can't remember your passcode, you can erase your iPhone with a computer or with recovery mode, then set a new passcode. See the Apple Support article [If you forgot the passcode on your iPhone, or your iPhone is disabled](#).


Note: If you made an iCloud or computer backup before you forgot your passcode, you can restore your data and settings from the backup.

Set up Face ID on iPhone

Use Face ID ([supported models](#)) to securely and conveniently unlock iPhone, authorize purchases and payments, and sign in to many third-party apps by simply glancing at your iPhone.

To use Face ID, you must also [set up a passcode](#) on your iPhone.

Set up Face ID or add an alternate appearance

- If you didn't set up Face ID when you first set up your iPhone, go to Settings  > Face ID & Passcode > Set up Face ID, then follow the onscreen instructions.
- To set up an additional appearance for Face ID to recognize, go to Settings > Face ID & Passcode > Set Up an Alternate Appearance, then follow the onscreen instructions.




If you have physical limitations, you can tap Accessibility Options during Face ID set up. When you do this, setting up facial recognition doesn't require the full range of head motion. Using Face ID is still secure, but it requires more consistency in how you look at iPhone.

Face ID also has an accessibility feature you can use if you're blind or have low vision. If you don't want Face ID to require that you look at iPhone with your eyes open, go to Settings > Accessibility, then turn off Require Attention for Face ID. This feature is automatically turned off if you turn on VoiceOver when you first set up iPhone. See [Change Face ID and attention settings on iPhone](#).

Use Face ID while wearing a face mask

On iPhone 12 models, iPhone 13 models, and iPhone 14 models, you can use Face ID to unlock your phone while you wear a face mask (or other covering that blocks your mouth and nose).

When you turn on Face ID with a Mask, Face ID analyzes the unique characteristics around your eyes, and it works with all of the Face ID options you turn on in Settings  > Face ID & Passcode.

Note: Face ID is most accurate when it's set up for full-face recognition only.

Go to Settings > Face ID & Passcode, then do any of the following:

- *Allow Face ID to work while you wear a face mask:* Turn on Face ID with a Mask, then follow the onscreen instructions.

Important: If you usually wear glasses, you can improve the accuracy of Face ID by wearing a pair of transparent glasses (not sunglasses) when you turn on Face ID with a Mask.

- *Add a pair of transparent glasses (not sunglasses) to your appearance:* Tap Add Glasses, then follow the onscreen instructions.
- *Don't allow Face ID to work while you wear a face mask:* Turn off Face ID with a Mask.

Alternatively, you can use Apple Watch with all models of iPhone that support Face ID to unlock iPhone while you wear a face mask. See [Unlock iPhone with Apple Watch](#).

This guide copied from [Apple Official website](#) and edited by [iphone14manual.com](#) for iPhone user's.

Temporarily disable Face ID


You can temporarily prevent Face ID from unlocking your iPhone.

1. Press and hold the side button and either volume button for 2 seconds.
2. After the sliders appear, press the side button to immediately lock iPhone.

iPhone locks automatically if you don't touch the screen for a minute or so.

The next time you unlock iPhone with your passcode, Face ID is enabled again.

Turn off Face ID

1. Go to Settings  > Face ID & Passcode.
2. Do one of the following:
 - *Turn off Face ID for specific items only:* Turn off one or more of the options.
 - *Turn off Face ID for face masks:* Turn off Face ID with a Mask.
 - *Turn off Face ID:* Tap Reset Face ID.

If your device is lost or stolen, you can prevent Face ID from being used to unlock your device with Find My iPhone Lost Mode. (See [Locate a device in Find My on iPhone.](#))

For more information about Face ID, see [About Face ID advanced technology.](#)

Set up Touch ID on iPhone

Use Touch ID ([supported models](#)) to securely and conveniently unlock iPhone, authorize purchases and payments, and sign in to many third-party apps by pressing the Home button with your finger or thumb.

To use Touch ID, you must also [set up a passcode](#) on your iPhone.

This guide copied from [Apple Official website](#) and edited by [iphone14manual.com](#) for iPhone user's.

Turn on fingerprint recognition

1. If you didn't turn on fingerprint recognition when you first set up your iPhone, go to Settings



> Touch ID & Passcode.


2. Turn on any of the options, then follow the onscreen instructions.

If you turn on iTunes & App Store, you're asked for your [Apple ID](#) password when you make your first purchase from the App Store, Apple Books, or the iTunes Store. When you make your next purchases, you're asked to use Touch ID.

Note: If you can't add a fingerprint or unlock your iPhone using Touch ID, see the Apple Support article [If Touch ID isn't working](#).

Add a fingerprint

You can add multiple fingerprints (both of your thumbs and forefingers, for example).

1. Go to Settings  > Touch ID & Passcode.
2. Tap Add a Fingerprint.
3. Follow the onscreen instructions.

Name or delete a fingerprint


1. Go to Settings  > Touch ID & Passcode.

If you added more than one fingerprint, place a finger on the Home button to identify its print.

2. Tap the fingerprint, then enter a name (such as "Thumb") or tap Delete Fingerprint.

This guide copied from [Apple Official website](#) and edited by [iphone14manual.com](#) for iPhone user's.


Turn off Touch ID

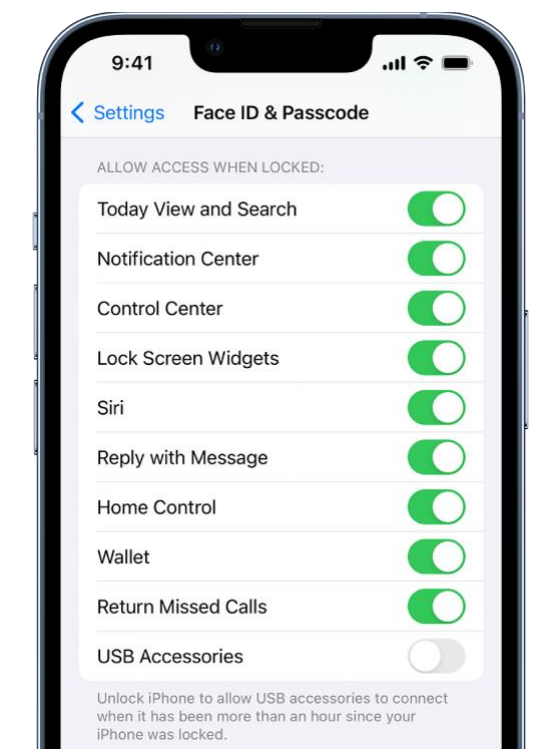
Go to Settings  > Touch ID & Passcode, then turn off one or more of the options.

Control access to information on the iPhone Lock Screen

You can easily access a few commonly used features (such as widgets, media playback controls, and Control Center) from the Lock Screen. You can control access to these items when iPhone is locked. (For security, USB connections aren't allowed when iPhone is locked.)

If you turn off Lock Screen access to a feature, you prevent someone who has your iPhone from viewing any personal information that it might contain (such as an upcoming event in the Calendar widget). However, you also lose quick access to the information yourself.

Go to Settings  > Face ID & Passcode (on an iPhone with Face ID) or Touch ID & Passcode (on an iPhone with a Home button), then select your options below Allow Access When Locked.



You can turn access on or off to the following features while iPhone is locked:

- Widgets (see [Add widgets on iPhone](#))
- Notification Center (see [Change notification settings on iPhone](#))
- Control Center (see [Use and customize Control Center on iPhone](#))
- Siri (see [Use Siri on iPhone](#))
- Replying to messages (see [Send and receive messages on iPhone](#))
- Home Control (see [Intro to Home on iPhone](#))
- Wallet (see [Add and use passes in Wallet on iPhone](#))
- Returning missed calls (see [Answer or decline incoming calls on iPhone](#))
- Connecting to a Mac, a Windows PC, or an accessory with USB (such as when you connect iPhone to your computer using USB)

Important: If you change the default setting and allow USB connections when iPhone is locked, you disable an important security feature of your iPhone.

You can also supply medical information and emergency contacts in a Medical ID that first responders and others can view on your iPhone when it's locked. See [Set up and view your Medical ID](#).

Keep your Apple ID secure on iPhone

Your [Apple ID](#) is the account you use to access Apple services like the App Store, Apple Music, iCloud, iMessage, FaceTime, and more. Your account includes the email address and password you use to sign in as well as the contact, payment, and security details you use across Apple services. Apple employs industry-standard practices to safeguard your Apple ID.


Best practices for maximizing the security of your Apple ID

- Don't let others use your ID, even family members.

To share purchases, subscriptions, a family calendar, and more without sharing Apple IDs, [set up Family Sharing](#).

- Use two-factor authentication. If you created your 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, [turn on two-factor authentication](#).

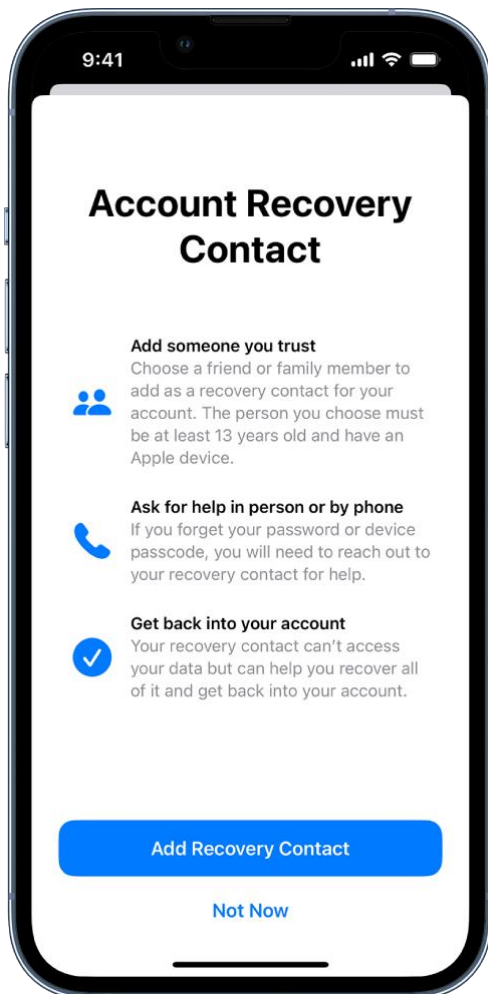
- Never provide your password, security questions, verification codes, recovery key, or any other account security details to anyone else. Apple will never ask you for this information.
- When accessing your Apple ID account page in Safari or another web browser, look for the lock icon  in the address field to verify that your session is encrypted and secure.
- When using a public computer, always sign out when your session is complete to prevent other people from accessing your account.
- Avoid phishing scams. Don't click links in suspicious email or text messages and never provide personal information on any website you aren't certain is legitimate. See the Apple Support article [Recognize and avoid phishing messages, phony support calls, and other scams](#).
- Don't use your password with other online accounts.


This guide copied from [Apple Official website](#) and edited by [iphone14manual.com](#) for iPhone user's.

Add Account Recovery Contacts

Choose one or more people you trust as Account Recovery Contacts to help you reset your Apple ID password and regain access to your account if you ever forget your password or get locked out.


Go to Settings  > [your name] > Password & Security > Account Recovery, tap Add Recovery Contact, then follow the onscreen instructions.

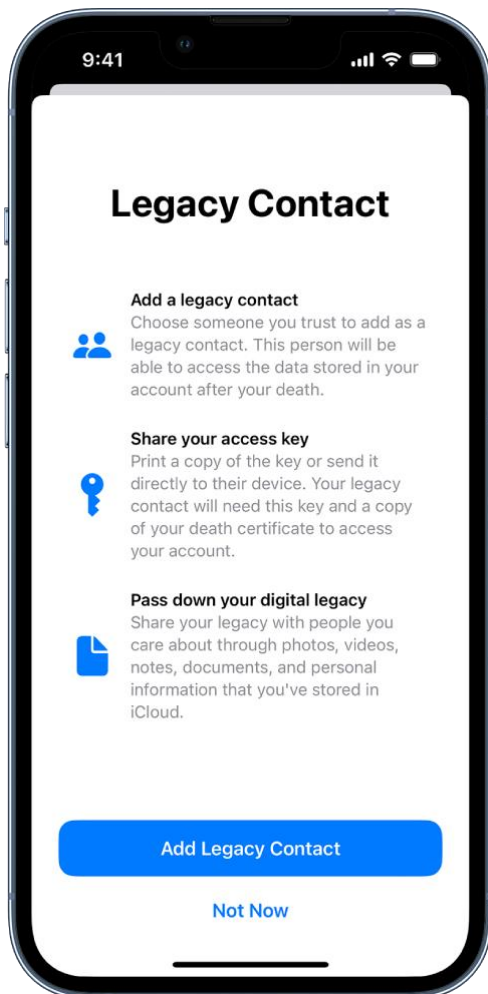


For more information, go to Settings  > [your name] > Password & Security, then tap “Learn more” below Add Recovery Contact.

Add Legacy Contacts

The Digital Legacy program allows you to designate people as Legacy Contacts so they can access your Apple ID account in the event of your death.

Go to Settings  > [your name] > Password & Security > Legacy Contact, tap Add Legacy Contact, then follow the onscreen instructions.



For more information about how to share the access key with a legacy contact, how to remove a legacy contact, and how your legacy contact can request access to your account, see the Apple Support article [How to add a Legacy Contact for your Apple ID](#). Also see the Apple Support article [Data that a Legacy Contact can access](#).

This guide copied from [Apple Official website](#) and edited by [iphone14manual.com](#) for iPhone user's.

Generate a recovery key for your account

For additional control over your account security, you have the option to generate a recovery key that helps you reset your account password or regain access to your Apple ID. A recovery key is a randomly generated 28-character code that you should keep in a safe place. You can reset your account password by either entering your recovery key or using another device already signed in with your Apple ID. To ensure you have access to your account, you are personally responsible for maintaining access to the recovery key and your trusted devices.

See the Apple Support article [How to generate a recovery key](#).

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](#).

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.

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](#).

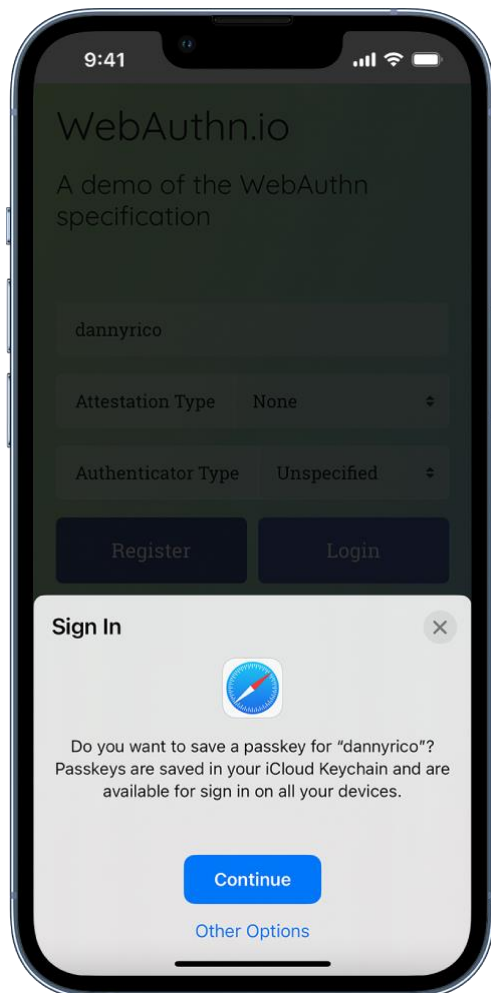
Note: Passkeys are an industry-wide security standard, and many websites and apps are quickly adding passkey support.

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 credentials 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 follow the 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 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](#).

This guide copied from [Apple Official website](#) and edited by [iphone14manual.com](#) for iPhone user’s.

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.

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

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.

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 a Confirm Password field if asked, 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.

This guide copied from [Apple Official website](https://appleofficialwebsite.com) and edited by iphone14manual.com for iPhone user's.

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.

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 a website or app 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.

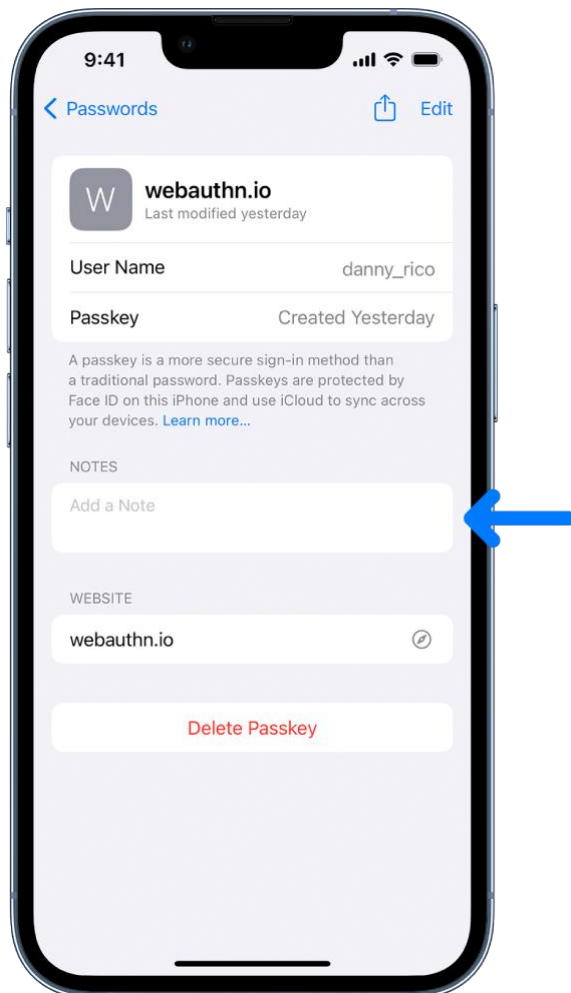
If you're connected to a Wi-Fi network, its name appears at the top of the screen. To see a list of all saved Wi-Fi networks, tap Edit at the top right.

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 website and app 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](#).

This guide copied from [Apple Official website](#) and edited by [iphone14manual.com](#) for iPhone user's.


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, except for passkeys, which require iOS 16 or tvOS 16 or later). iCloud Keychain is secured with 256-bit AES encryption during storage and transmission, and its data can't 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.

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 website and app sign-in screens require you to pass CAPTCHA challenges, such as 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. When two-factor authentication is on, only you can access your account by using a trusted device. 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](#).

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.

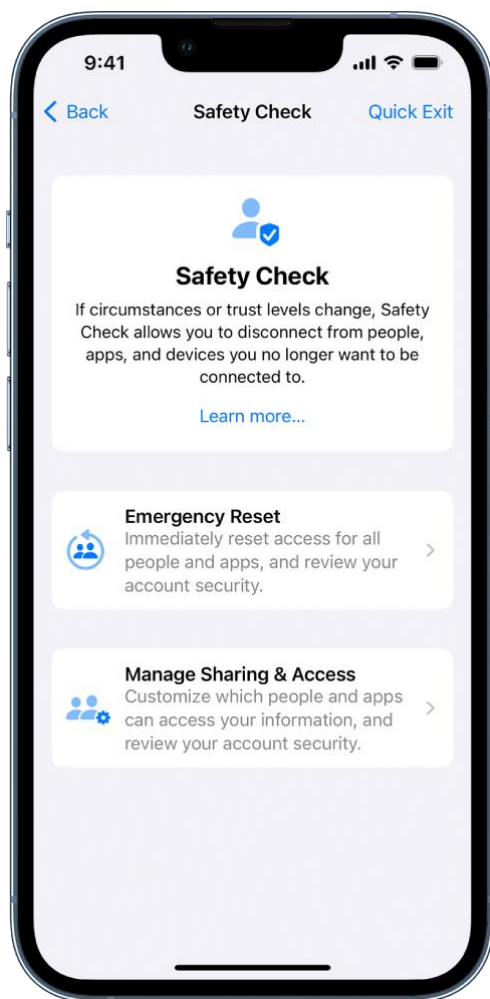
1. Sign in to your [Apple ID account](#).
2. Tap App-Specific Passwords, then tap "Generate an app-specific password."
3. Follow the onscreen instructions.


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 information sharing with Safety Check on iPhone

Use Safety Check to periodically review and update information you share with people, apps, and devices. From Safety Check, you can stop sharing your location with others in 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 to your device and personal information. Go to Settings > Privacy & Security > Safety Check, tap Emergency Reset, tap Start Emergency Reset, then follow the onscreen instructions.

To learn more about Safety Check, 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.

This guide copied from [Apple Official website](#) and edited by [iphone14manual.com](#) for iPhone user's.

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.

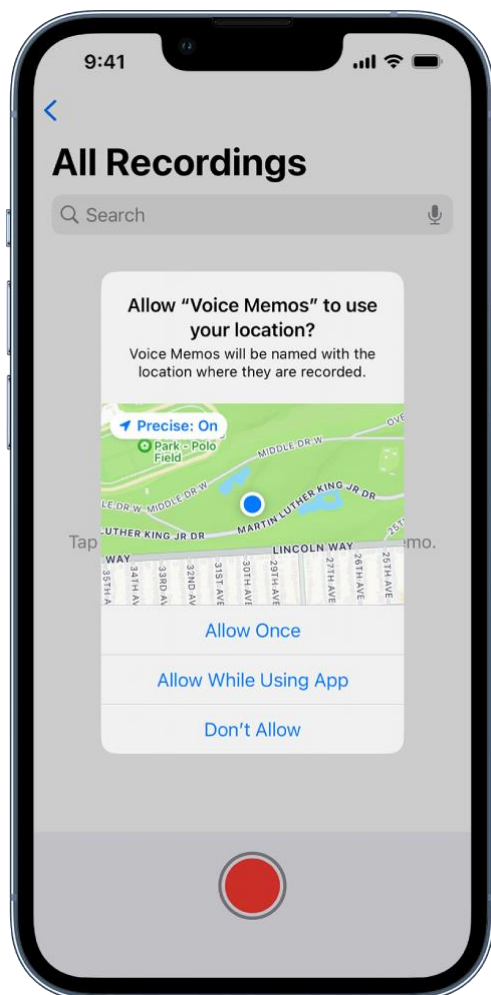
Control the location information you share on iPhone

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

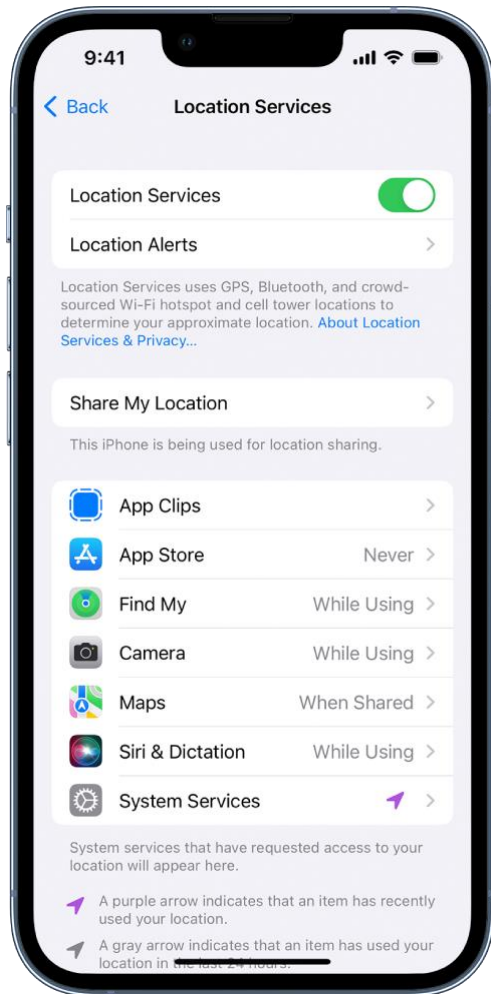
If you didn't turn on Location Services when you first set up iPhone, go to Settings  > Privacy & Security > Location Services, then turn on Location Services.

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

This guide copied from [Apple Official website](https://apple.com) and edited by iphone14manual.com for iPhone user's.

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.

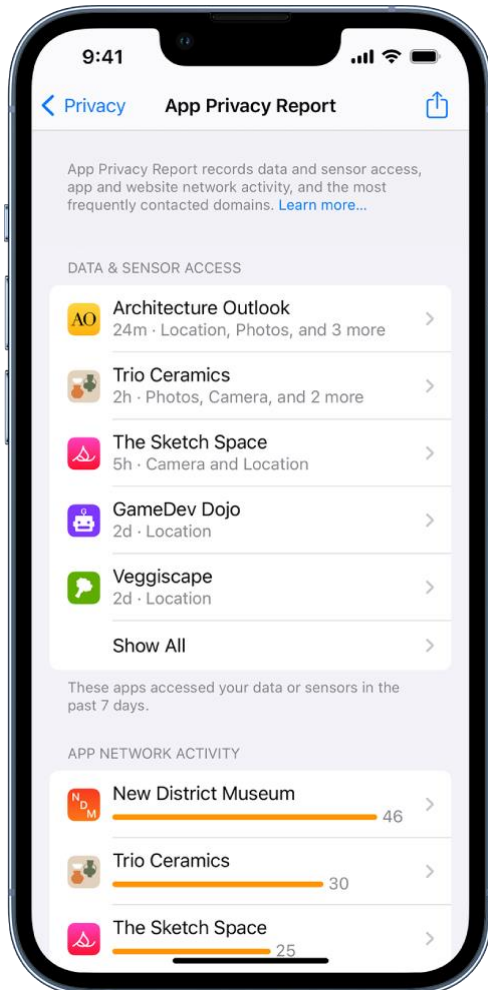
1. Go to Settings  > Privacy & Security.
2. Tap a category of information, such as Calendars, Reminders, or Motion & Fitness.


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.

This guide copied from [Apple Official website](https://apple.com/privacy) and edited by iphone14manual.com for iPhone user's.

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.


This guide copied from [Apple Official website](https://apple.com/privacy) and edited by iphone14manual.com for iPhone user's.

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.

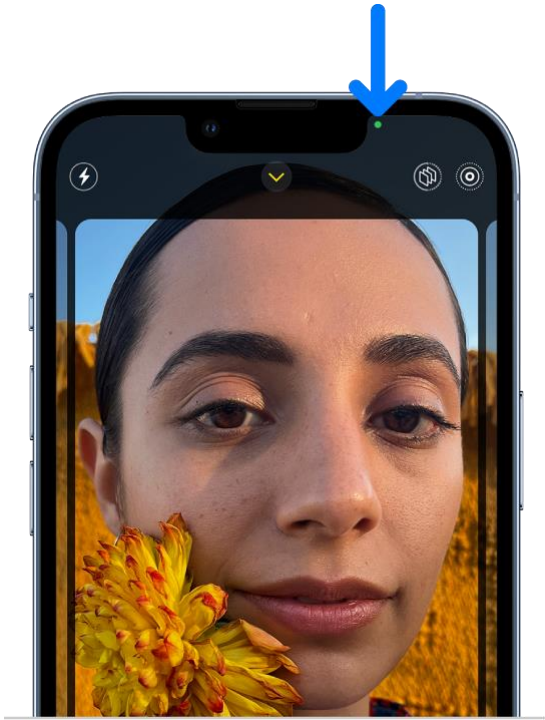
You can review which apps have requested access to these hardware features, and you can change their access at your discretion.

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 (beta) to help prevent websites and network providers from creating a detailed profile about you. When iCloud Private Relay is 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 SIMs).
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 tap 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.

This guide copied from [Apple Official website](https://apple.com/privacy) and edited by iphone14manual.com for iPhone user's.