Apple Two-Step Verification

What is two-step verification for Apple ID?

Two-step verification is an optional security feature for your Apple ID. Two-step verification requires you to verify your identity using one of your devices before you can take any of these actions:

- Sign in to My Apple ID to manage your account
- Make an iTunes, App Store, or iBooks Store purchase from a new device
- Get Apple ID related support from Apple

Turning on two-step verification reduces the possibility of someone accessing or making unauthorized changes to your account information at My Apple ID or making purchases using your account.

Why should I use two-step verification with my Apple ID?

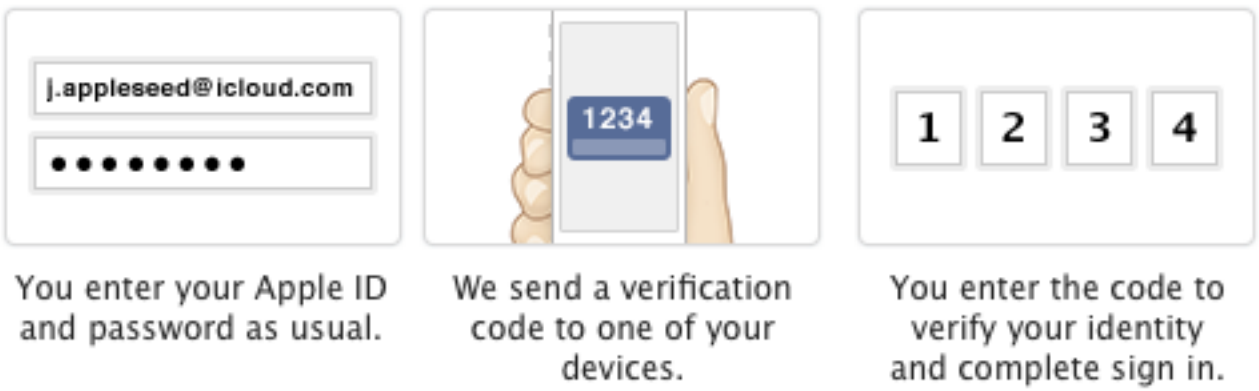
Your Apple ID is the key to a lot of things you do with Apple, so it's important that only you have the ability to access your account details, update your password, or make other changes to your account. Two-step verification is a feature you can use to keep your Apple ID account as secure as possible.

How do I set up two-step verification?

1. Go to My Apple ID, select “Manage your Apple ID,” and sign in.
2. Select “Password and Security.”
3. Under Two-Step Verification, select Get Started and follow the onscreen instructions.

How does it work?

When you set up two-step verification, you register one or more trusted devices. A trusted device is a device you control that can receive 4-digit verification codes using either SMS or Find My iPhone. Then, any time you sign in to manage your Apple ID at My Apple ID or make an iTunes, App Store, or iBooks Store purchase from a new device, you'll need to verify your identity by entering both your password and a 4-digit verification code, as shown below.



After you sign in, you can manage your account or make purchases as usual. Without both your password and the verification code, access to your account will be denied.

You will also get a 14-digit Recovery Key for you to print and keep in a safe place. Use your Recovery Key to regain access to your account if you ever lose access to your devices or forget your password.

Do I still need to remember any security questions?

With two-step verification, you don't need to create or remember any security questions. Your identity is verified exclusively using your password, verification codes sent to your trusted devices, and your Recovery Key.

Is an SMS-capable phone number required to use two-step verification?

Yes. When you set up two-step verification, you're required to add and verify at least one SMS number for your account. Add the SMS number that you use most frequently. For example, the number you use with your iPhone or other primary phone. You can also add an SMS number used by someone close to you, such as a spouse or other family member, in case you're temporarily without access to your own devices. Landline or web-based (VOIP) phone services can't be used with two-step verification.

How do I use Find My iPhone notifications to receive verification codes?

Find My iPhone notifications can be used to receive verification codes on any iOS device with Find My iPhone turned on. Learn how to set up Find My iPhone.

Where should I keep my Recovery Key?

Keep your Recovery Key in a secure place in your home, office, or other location. You should consider printing more than one copy so that you can keep your key in more than one place. Your key will be easier to find if you ever need it, and you'll have a spare copy if one is ever lost or destroyed.

You shouldn't store your Recovery Key on your device or computer, because that could give an unauthorized user instant access to your key.

Can I turn off two-step verification after I turn it on?

Yes. Learn how to turn off two-step verification.

What do I need to remember when I use two-step verification?

Two-step verification simplifies and strengthens the security of your account. After you turn it on, there is no way for anyone to access and manage your account at My Apple ID other than by using your password, verification codes sent your trusted devices, or your Recovery Key. You must be responsible for:

- Remembering your password
- Keeping your trusted devices physically secure
- Keeping your Recovery Key in a safe place

If you lose access to two of these three items at the same time, you could be locked out of your Apple ID account permanently. With two-step verification turned on, only you can reset your password, manage your trusted devices, or create a new Recovery Key. Apple Support can help you with other aspects of your service, but they aren't able to update or recover these three things for you.

What if I lose my Recovery Key?

If you lose your Recovery Key, you can replace it any time:

1. Go to My Apple ID, select "Manage your Apple ID," and sign in with your password and trusted device.
2. Select "Password and Security."
3. Under Recovery Key, select Replace Lost Key.

When you create a new key, your old Recovery Key is no longer usable.

What if I forget my Apple ID password?

If you forget your password, you can reset it at My Apple ID using your Recovery Key and one of your trusted devices.

Apple Support can't reset your password for you. To reset your password, you must have your Recovery Key and access to at least one of your trusted devices.

What if I lose or give away one of my trusted devices?

If you no longer have access to one of your devices, go to My Apple ID as soon as possible to remove that device from your list of trusted devices. That device can then no longer be used to help verify your identity.

What if I no longer have access to *any* of my trusted devices?

If you can't access any of your trusted devices, you can still access your account at My Apple ID using your password and Recovery Key. You should then verify a new trusted device as soon as possible.

Why was I asked to wait before setting up two-step verification?

As a basic security measure, Apple doesn't allow setup of two-step verification to proceed if significant changes were recently made to your Apple ID account information. Significant changes can include a password reset or new security questions. This waiting period helps Apple make sure that you are the only person accessing or modifying your account. While you are in this waiting period, you can continue using your account as usual with all Apple services and stores.

Apple will send an email to all the addresses you have on file notifying you of the waiting period and encouraging you to contact Apple Support if you think that someone else has unauthorized access to your account. You'll be able set up two-step verification after the date listed on your Apple ID account page and in the email that you receive.

When your waiting period is over, you have 30 days to complete setup of two-step verification. If you attempt to complete setup after 30 days have passed, or you made significant changes to your account during that time, another waiting period may be triggered.