Two-step verification for Apple ID

If you want to improve the security of your account, but don't have devices that can be updated to iOS 9 or OS X El Capitan, you can set up two-step verification for your Apple ID.

What is two-step verification for Apple ID?

Two-step verification is a security feature for Apple ID that's designed to prevent anyone else from accessing or using your account, even if they know your password.

It requires you to verify your identity using one of your devices or another approved method before you can:

- Sign in to your Apple ID account page
- Sign in to iCloud on a new device or at iCloud.com
- Sign in to iMessage or FaceTime*
- Make an iTunes, Apple Books, or App Store purchase from a new device
- Get Apple ID-related support from Apple

Is two-step verification the same as two-factor authentication?

No. Two-factor authentication is a newer security method that's built directly into iOS, macOS, tvOS, watchOS, and Apple's websites. It offers a more streamlined user experience and is required to use certain features that call for enhanced security. Two-factor authentication is available to iCloud users with at least one device using iOS 9 or OS X El Capitan or later.

If you have Apple devices that can be updated to iOS 9 or later or OS X El Capitan or later, you should set up two-factor authentication instead. If you use two-step verification for your Apple ID, and then you upgrade to iOS 11 or later, or macOS High Sierra or later, your security settings may be automatically upgraded to two-factor authentication.

Two-step verification is an older security method that is available to users who don't have Apple devices, can't update their devices, or are otherwise ineligible for two-factor authentication.

How do I set up two-step verification?

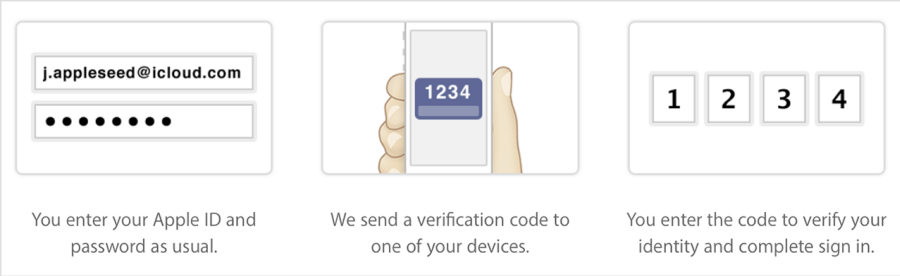
You can set up two-step verification using the link below. Simply click the link, sign in to your Apple ID account page, and follow the instructions provided.

Set up two-step verification now.

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. You're required to provide at least one SMS capable phone number.

Then, any time you sign in to manage your Apple ID, sign in to iCloud, or make an iTunes, Apple Books, or App Store purchase from a new device, you need to verify your identity by entering both your password and a 4-digit verification code.



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

You'll also get a 14-character Recovery Key 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 trusted 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.

Which SMS numbers should I verify for my account?

You're required to verify at least one SMS-capable phone number for your account. You should consider verifying all SMS-capable phone numbers that you normally use with your iPhone or another mobile phone. You should also consider verifying an SMS-capable phone number used by someone close to you, such as a spouse or other family member. You can use this number if you're temporarily without access to your own devices.

You can't use landline or web-based (VOIP) phone services for 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. Consider printing more than one copy, so that you can keep your key in more than one place. Your key is easier to find if you ever need it, and you 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.

If you ever need a new Recovery Key, you can create one from your Apple ID account page. Just sign in with your password and trusted device, go to the Security section and click Edit, then click Replace Lost Key.

After you create a new key, your old Recovery Key won't work.

How do I sign in to my account using an app that doesn't support entering two-step verification codes?

You can generate an app-specific password from your Apple ID account page and enter it into the password field of the app that you want to sign in to. This allows you to sign in securely even if the app you're using doesn't support entering verification codes. For example, you might use an app-specific password to sign in to iCloud using a third-party email, address book, or calendar app.

If you want to generate an app-specific password, sign in to your Apple ID account page. In the Security section, click Edit > Generate Password.

Learn more about app-specific passwords.

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

Two-step verification simplifies and strengthens the security of your Apple ID. After you turn it on, there's no way for anyone to access and manage your account other than by using your password, verification codes sent to your trusted devices, or your Recovery Key. 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. When you use two-step verification, you are 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 permanently.

What if I lose my Recovery Key?

You can sign in to your Apple ID account page and create a new Recovery Key using your Apple ID password and one of your trusted devices.

What if I forget my Apple ID password?

You can reset your password from your Apple ID account page 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 your Apple ID account page 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 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 sends an email to all of 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 can 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 might be triggered.

How do I turn off two-step verification?

1. Sign in to your Apple ID account page.
2. In the Security section, Click Edit.
3. Click Turn Off two-step verification.
4. Create new security questions and verify your date of birth.

You'll get an email confirming that two-step verification for your Apple ID is off.

Which countries or regions is two-step verification available in?

Two-step verification is available in the countries and regions below. When additional countries or regions are added, two-step verification automatically appears in the Security section of your Apple ID account page.

- Albania
- Algeria
- Angola
- Anguilla
- Antigua and Barbuda
- Argentina
- Armenia
- Australia
- Austria
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belgium
- Bolivia
- Botswana
- Brazil
- British Virgin Islands
- Bulgaria
- Cameroon
- Canada
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China mainland
- Guam
- Guadeloupe
- Guatemala
- Guinea
- Guinea-Bissau
- Guyana
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Ireland
- Israel
- Italy
- Jamaica
- Japan
- Jordan
- Kazakhstan
- Kenya
- Kuwait
- Laos
- Latvia
- Lebanon
- Liechtenstein
- Lithuania
- Palau
- Panama
- Paraguay
- Peru
- Philippines
- Poland
- Portugal
- Puerto Rico
- Qatar
- Reunion
- Romania
- Russia
- Saint Kitts and Nevis
- Saint Lucia
- Saint Vincent and Grenadines
- Sao Tome and Principe
- Saudi Arabia
- Senegal
- Seychelles
- Sierra Leone
- Singapore
- Slovakia
- Slovenia
- South Africa
- South Korea

- Colombia
- Congo, Democratic Republic
- Congo, Republic
- Costa Rica
- Cote d'Ivoire
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Dominica
- Dominican Republic
- Ecuador
- Egypt
- El Salvador
- Estonia
- Fiji
- Finland
- France
- Gambia
- Germany
- Ghana
- Greece
- Grenada
- Luxembourg
- Macau
- Macedonia
- Madagascar
- Malaysia
- Mali
- Malta
- Martinique
- Mauritius
- Mexico
- Moldova
- Montserrat
- Morocco
- Namibia
- Netherlands
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Norway
- Oman
- Pakistan
- Spain
- Sri Lanka
- Suriname
- Swaziland
- Sweden
- Switzerland
- Taiwan
- Tanzania
- Thailand
- Trinidad and Tobago
- Tunisia
- Turkey
- Turks and Caicos Islands
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- Uruguay
- Venezuela
- Vietnam
- Yemen
- Zimbabwe

* FaceTime is not available in all countries or regions.

Published Date: May 29, 2019

