How to enable end-to-end encryption for your iCloud backups

With iOS 16.2, Apple is bringing advanced security features to more of your data. Among other things, it is adding highly secure end-to-end encryption for iCloud backups under the name Advanced Data Protection. This means that essentially only you can access the data stored in your iCloud device backup — Apple doesn't have the key to access it. This is a strong layer of security, and although it takes a little bit of work to set up and requires you to take more responsibility for recovering your data, it's well worth the effort if you'd like to make sure that you're the only one who can access your backed up information.

Here's how to set up end-to-end encryption for your iCloud backups on your iPhone. You'll need to be running iOS 16.2, which is available only in beta at this time. Apple says it will be available to the public in the US by the end of 2022 and will come to the rest of the world in early 2023.

There are two main things you'll need to do in order to enable Advanced Data Protection: update all of your Apple devices to their latest OS version (or remove them from your account) and set up account recovery. As of the time of writing, that means iOS 16.2, iPadOS 16.2, watchOS 9.1, and macOS 13.1. Any HomePods or Apple TVs using your iCloud account also need to be updated to at least version 16.2.

So first, go through all your devices and do a little housekeeping. Once you've done that, you need to set up account recovery.

As a first step, you'll need to set up **Account Recovery** since Apple will no longer be able to help recover your data.

You can also set up a recovery contact and / or a recovery key in the process.

With Account Recovery enabled, you can start setting up Advanced Data Protection.

With that done, you're on your way to a future of much more secure iCloud backups.

https://www.theverge.com/23498690/apple-advanced-data-protection-icloud-encryption-iphone-mac-how-to