New Security and Privacy Features in macOS Ventura, iOS 16, and iPadOS 16

Posted on September 12th, 2022 by Kirk McElhearn

In June, Apple announced this year's operating systems, and they are full of new features to boost your productivity and increase your fun. macOS Ventura, iOS 16, and iPadOS 16 also have a number of useful new features to enhance your security and privacy. Most of these features are present in all of the operating systems.

iOS 16 is now available, and iPadOS 16 and macOS Ventura are coming on Monday, October 24. Here's an overview of what's new in iOS, and what to look forward to on the Mac and iPad.

Passkeys

Apple, as part of the FIDO Alliance, is committed to moving toward a future without passwords. At least, without passwords that we have to remember and fill in on websites and in apps. As such, they are introducing on its platforms. As Apple's developer document explains,

> Passkeys use iCloud Keychain public key credentials, eliminating the need for passwords. Instead, they rely on biometric identification such as Touch ID and Face ID in iOS, or a specific confirmation in macOS for generating and authenticating accounts.

What this means is that, instead of having something you know (your password) to log into a website, or also something you have (your second-factor device, for entering one-time codes) if you are using two-factor authentication, in the future, it's your iPhone or other device that will be the authenticating device. The "something you know" will be the passcode that you entered to access the device, and the "something you have" will be the device's confirmation that you are you. Instead of potentially insecure passwords, this system will create robust cryptographic keys that can't be cracked.

We already see this in the chain of trust that links Apple devices; once you have authenticated on one device, you can authenticate on others. It's likely this will take several years to become common, but it's good that Apple is laying the groundwork.

Passkeys protect you from data breaches on websites, because they are not stored on web servers, and from phishing, because they are very specific to each website, and won't work on lookalike sites. They will sync across your devices via iCloud, using end-to-end encryption, so they are available on all your devices.

In addition, you'll be able to sign in to websites and apps on other devices using your iPhone or iPad.

You scan a QR code and use Touch ID or Face ID to authenticate.

The important thing to bear in mind is that you need a very strong passcode to prevent someone from breaking into your device.

Safari passwords

Safari passwords are getting an enhancement, at least until they are replaced by passkeys. You can have Safari suggest a strong password when creating an account on a website. However, sometimes those passwords don't meet the site's requirements, to have, say, a minimum of one upper-case letter, one digit, and one special character. In the coming operating systems, you'll be able to edit these passwords to meet site-specific requirements.

Rapid Security Response

On macOS, you can currently choose to get security updates automatically, even if you don't allow other system updates to install without your intervention. Apple is enhancing this feature to allow much quicker rollout of security updates, rather than waiting for broader OS updates to be issued. They will be pushed out in the background, and will be installed without a restart required, and will be available on the Mac, iPhone, and iPad.

Hide My Email

Apple introduced Hide My Email last year. This feature allows you to create disposable email addresses that are aliases for your iCloud email address. You can sign up to a website using one of these addresses, and, if you start getting spam, you can delete the address. This year, Apple is extending Hide My Email to allow third-party apps to offer Hide My Email sign-in options.

Protected Photo albums

It's possible to hide photos in Apple's Photos app. When you do this, the app creates an album entitled Hidden. In the future, both the Hidden album and the Recently Deleted album will be locked by default, and will only be accessible by entering your password, or by using Touch ID or Face ID to authenticate.

Safety Check

Apple has developed Safety Check for people who are at risk from domestic violence. This feature allows a user to revoke all access they have granted to a spouse or partner, such as location sharing, access to photos, and more. An emergency reset feature allows a user to sign out of iCloud on all

their other devices, reset all privacy settings, and limit messaging to the current device.

Pasteboard permissions

Apps will need to ask your permission on an iPhone or iPad to be able to access information you have copied to the pasteboard.

Face ID

Face ID will (finally) work in landscape, on iPads and supported iPhone models.

There will certainly be other security and privacy features in the new operating systems. We'll find out more in a few months.

How can I learn more?

Each week on the , Intego's Mac security experts discuss the latest Apple news, security and privacy stories, and offer practical advice on getting the most out of your Apple devices. Be sure to to make sure you don't miss any episodes.

You can also subscribe to our and keep an eye here on for the latest Apple security and privacy news. And don't forget to follow Intego on your favorite social media channels:

About Kirk McElhearn

writes about Apple products and more on his blog Kirkville. He is co-host of the Intego Mac Podcast, as well as several other podcasts, and is a regular contributor to The Mac Security Blog, TidBITS, and several other websites and publications. Kirk has written more than two dozen books, including Take Control books about Apple's media apps, Scrivener, and LaunchBar. Follow him on Twitter at @mcelhearn. View all posts by Kirk McElhearn →