How to Create Passkeys

20250825

Contents

Preface

A passkey is a passwordless sign-in method that replaces traditional passwords with cryptographic keys stored securely on your device. In the past, secure logins often relied on a password plus an extra step, such as a one-time code sent to your phone or an authentication app. While these methods added security, they still depended on passwords, which are frequently weak, reused, or stolen.

Instead of entering a password, you sign in using your fingerprint, face, or device PIN. Behind the scenes, advanced encryption verifies your identity with no password required. Each passkey is unique to you and your device, making them difficult for attackers to steal. This results in a stronger protection against phishing, reduced risk of account takeovers, and freedom from the burden of remembering or resetting passwords. Best of all, passkeys work across apps and websites and can be added to your existing accounts, making your online life both more secure and more convenient.

How does a passkey work?
Passkeys are built on the WebAuthentication (or "WebAuthn") standard, which uses public key cryptography. During account registration, the operating system creates a unique cryptographic key pair to associate with an account for the app or website. These keys are generated by the device, securely and uniquely, for every account.

One of these keys is public, and is stored on the server. This public key is not a secret. The other key is private, and is what is needed to actually sign in. The server never learns what the private key is. On Apple devices with Touch ID or Face ID, they can be used to authorize use of the passkey, which then authenticates the user to the app or website. No shared secret is transmitted, and the server does not need to protect the public key. This makes passkeys very strong, easy to use credentials that are highly phishing-resistant. Platform vendors have worked together within the FIDO Alliance to make sure that passkey implementations are compatible cross-platform and can work on as many devices as possible.

Benefits
Even with robust password protection measures in place, passkeys offer several security benefits over traditional passwords. Here are some of the major security benefits of using passkeys.

- *Physical possession requirement*
  Each passkey is unique to you and your device, making it extremely hard to steal. Even if a hacker somehow got your passkey, they still couldn't use it without physical access to your phone, tablet, or computer.
- *Enhanced protection against phishing attacks*
  Passkeys are resistant to phishing attacks because they rely on physical possession of a device rather than passwords, which can be guessed and entered by anyone on any device. Even if you did fall victim to a phishing attempt when using a passkey, the attacker would still need the physical passkey (which is only stored on your device) to access your account. As a result, the use of passkeys can greatly improve security.
- *Reduced risk of account takeover*
  Because passkeys are tied to your device and can't be reused elsewhere, they offer far better protection than traditional passwords or even one-time codes. Bad actors would need both your passkey and your device, a tough combination to beat.
- *Compliance with security standards*
  Passkeys often meet or exceed security standards and compliance requirements in regulated industries such as finance, healthcare, and government. Their robust security features make them well-suited for protecting sensitive data and complying with industry-specific regulations. Passkeys can also be used with OAuth to authorize access between apps and services without compromising sensitive information.
- *Recovery security*
  When you forget traditional sign in credentials, regaining access to an account often requires a password reset and/or the use of some form of two-factor authentication. Passkeys, on the other hand, can be securely synced across your devices. If you lose a device that has your passkey synced to it, you can use another device to recover access to your accounts.

Transitioning to Passkeys: A Five-Phase Approach
As organizations seek better security and user convenience, many are moving away from traditional passwords and adopting passkeys. Here's a step-by-step framework for implementing passkeys effectively:

1. Assessment & Planning
Evaluate your current password management practices, security needs, and compliance requirements. Use this analysis to define your organization's goals and requirements for passkey adoption.

2. Solution Selection
Choose a passkey solution that meets your organization's needs. Consider key factors such as security features, scalability, device compatibility, and integration with existing systems and identity providers.

3. Policy Development
Establish clear policies and guidelines for passkey creation, usage, protection, and storage. This ensures consistent practices across the organization and helps support compliance and governance.

4. Implementation & Integration
Deploy the selected passkey solution across relevant platforms. Configure security settings to match your organizational requirements, and test integration with existing infrastructure (such as SSO and MFA systems) to ensure seamless operation.

5. Training & Awareness
Conduct training to ensure employees understand how to create, manage, and protect their passkeys. Ongoing education helps support secure usage and encourages broad adoption across the organization.

Who Supports Passkeys?
Industry giants like Google, Apple, Samsung, Amazon, and Microsoft are embracing passkeys, marking a significant evolution in online security. Their adoption signals a major move toward a passwordless future.

No matter which platform your users are on (Android, iOS, macOS, Windows, or others), passkeys are rapidly becoming the new standard. Backed by the world's top technology providers, passkeys offer secure, seamless authentication across devices and platforms.

What Devices Are Compatible with Passkeys?
Passkeys are widely supported across a vast range of devices, operating systems, browsers, and applications—covering over 90% of devices in use today.

- Operating Systems:
  - iOS 16 and later
  - macOS 13 and later
  - Android 9 and later
  - Windows 10/11
  - Linux

- Browsers:
  - Safari
  - Chrome
  - Brave
  - Edge
  - Firefox

- Apps: Supported across iOS, macOS, Samsung, and Android applications. I.E. 1Password.

The future of security is here and it doesn't require a password.

Section 1: Passkeys on Apple device

Apple was among the first major companies to embrace passkey technology, demonstrating its commitment to passwordless security as early as 2021. As a member of the FIDO Alliance, Apple collaborated with industry leaders like Google and Microsoft to develop and implement the FIDO2 standards for secure, passwordless authentication. This move toward passkeys underscores Apple's broader focus on enhancing user privacy and security.

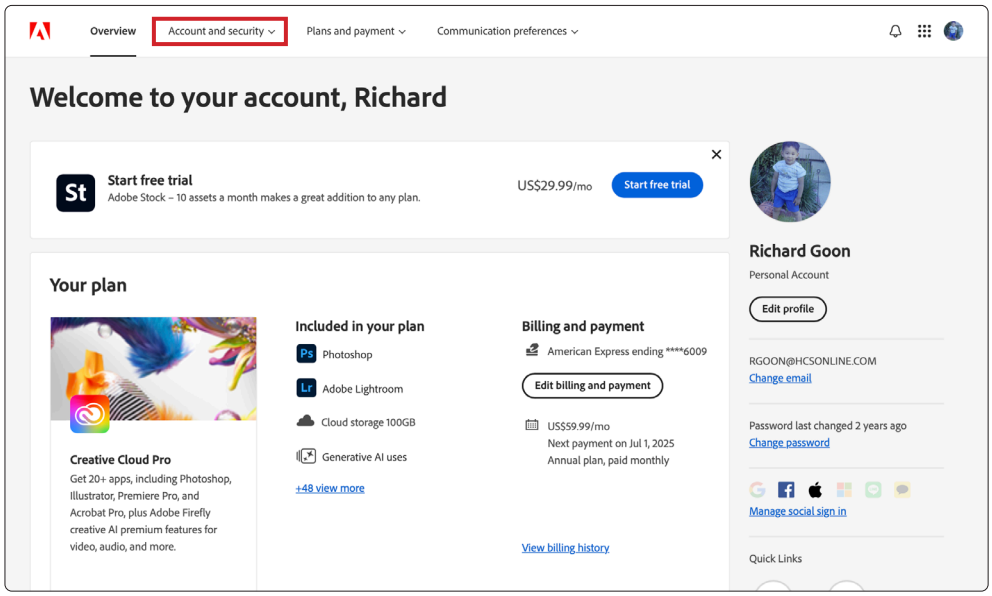
The FIDO Alliance anticipates that passkeys will eventually replace passwords across all platforms, and Apple is positioning itself at the forefront of this shift. Its early adoption and deep integration of passkey technology throughout the Apple ecosystem highlight the company's leadership in shaping the future of digital security.

Apple's passkey system relies on public-key cryptography. When a passkey is created, a unique key pair is generated: the public key is stored on the server, while the private key remains securely stored within the device's secure enclave—a dedicated hardware component designed to prevent the private key from ever leaving the device.

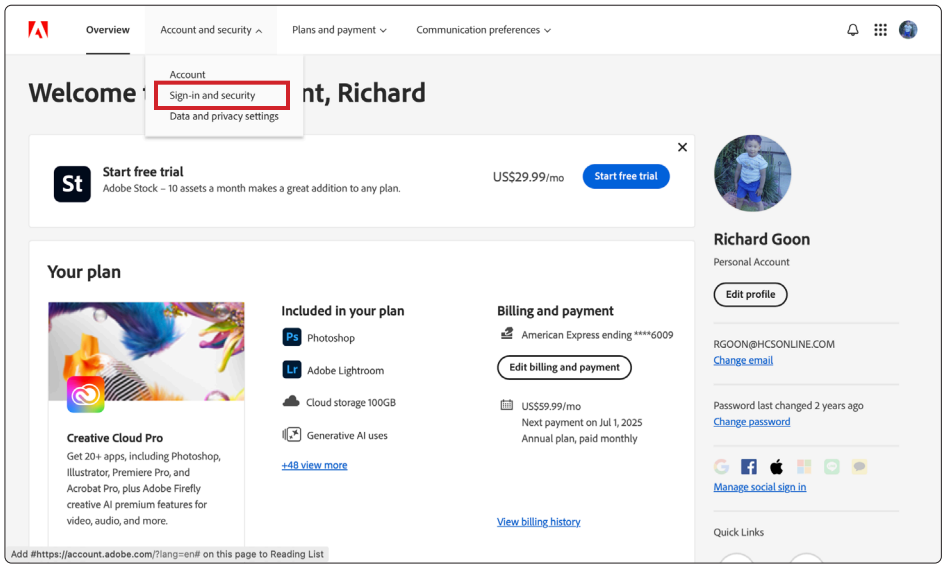
For enhanced convenience, passkeys are synchronized across Apple devices utilizing iCloud Keychain. Authentication leverages the device's native unlock mechanism, employing the private key to securely sign login requests. This integration of secure enclave storage with iCloud synchronization delivers both strong security and seamless usability for Apple users.

Create a passkey for an existing account through Safari and the Password app

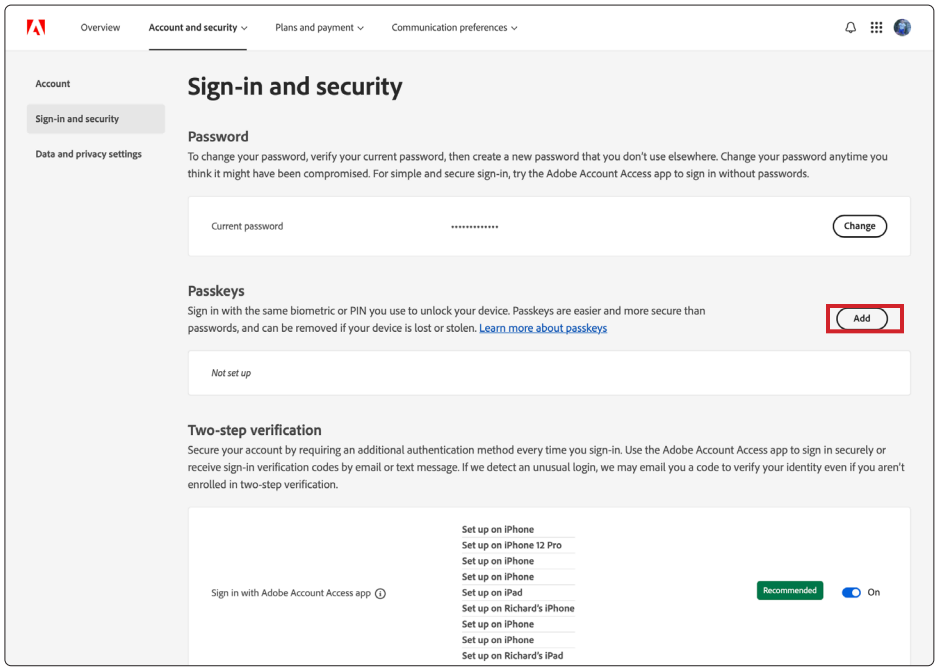
1. For this exercise, we will add a passkey to an Adobe account. Sign into your Adobe Account on Safari.
2. Click on Account and security.



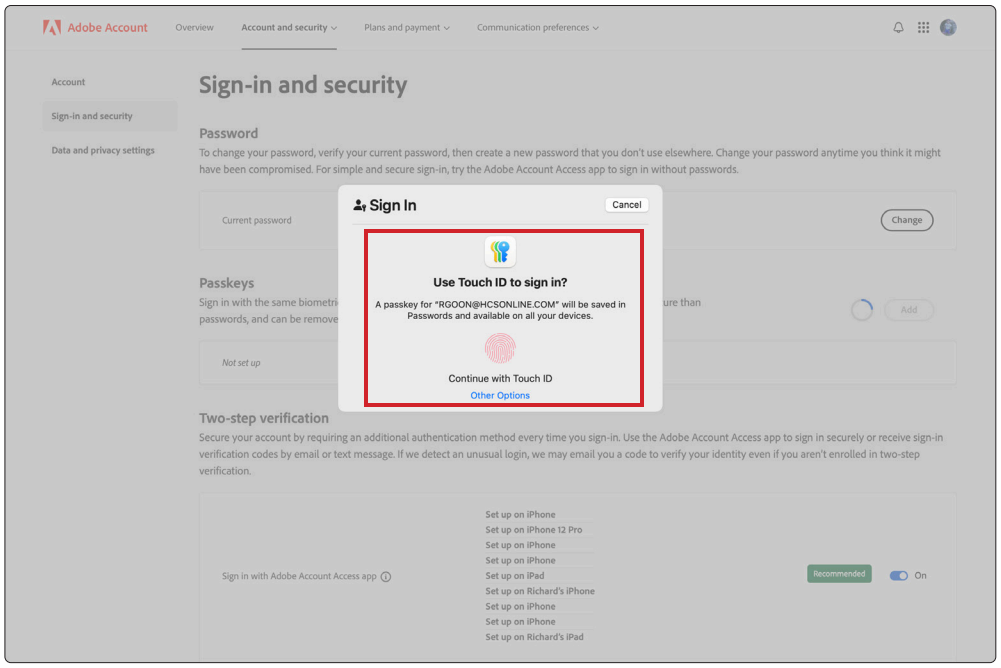
3. Select Sign-in and security.



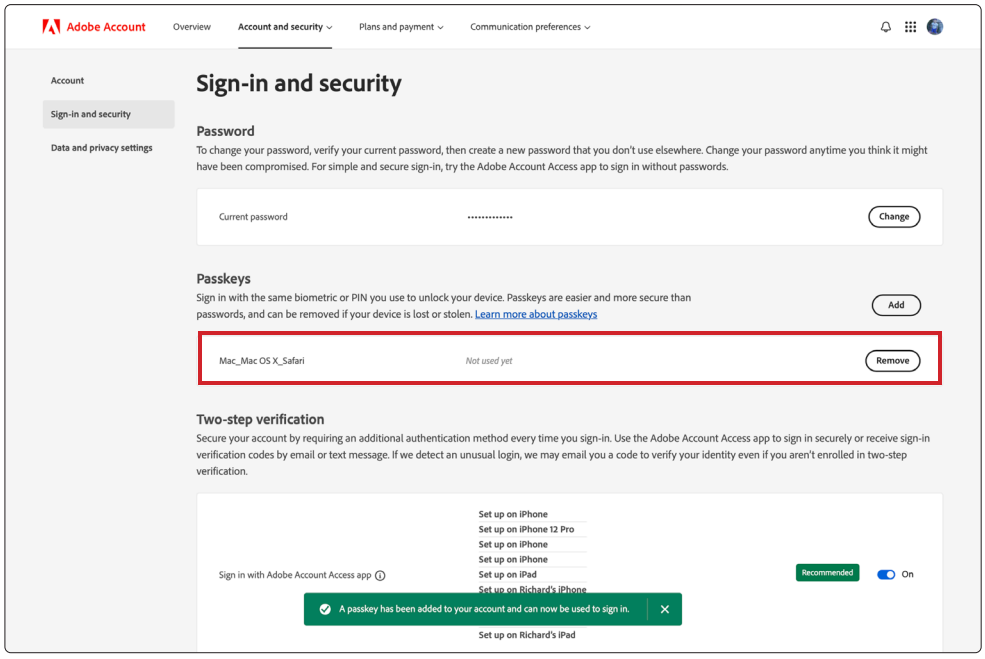
4. In the Passkeys section, click Add.



5. Confirm a window appears asking to create a passkey for the account using Touch ID. Use your Touch ID on your device.

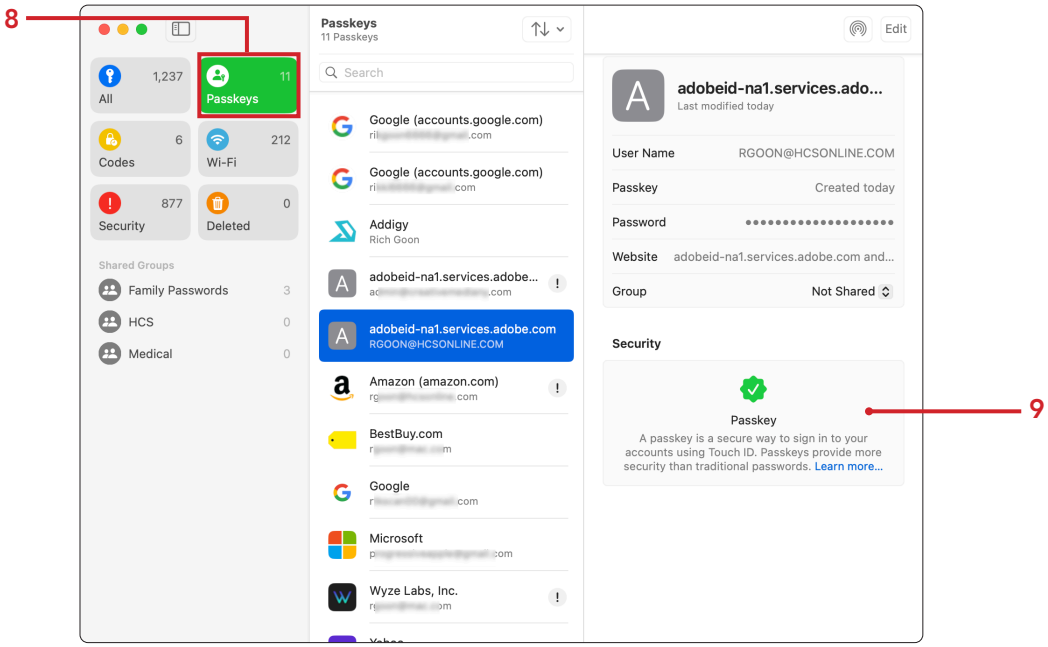


6. Confirm a passkey has been created.

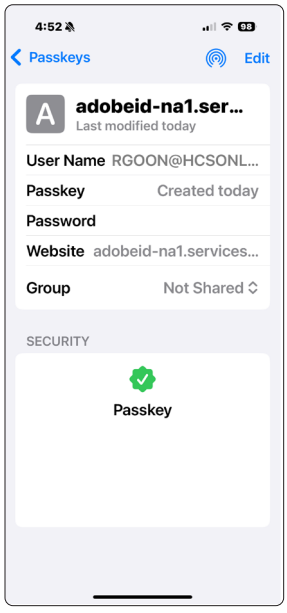


7. Open the Passwords App.

8. Click Passkeys.
9. Confirm the passkey has been created for your Adobe account.

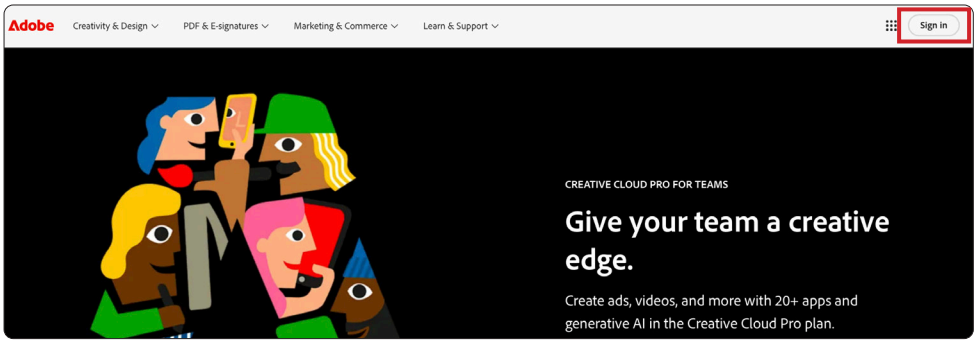


10. On another Apple device, confirm the passkey is in the Passwords app.

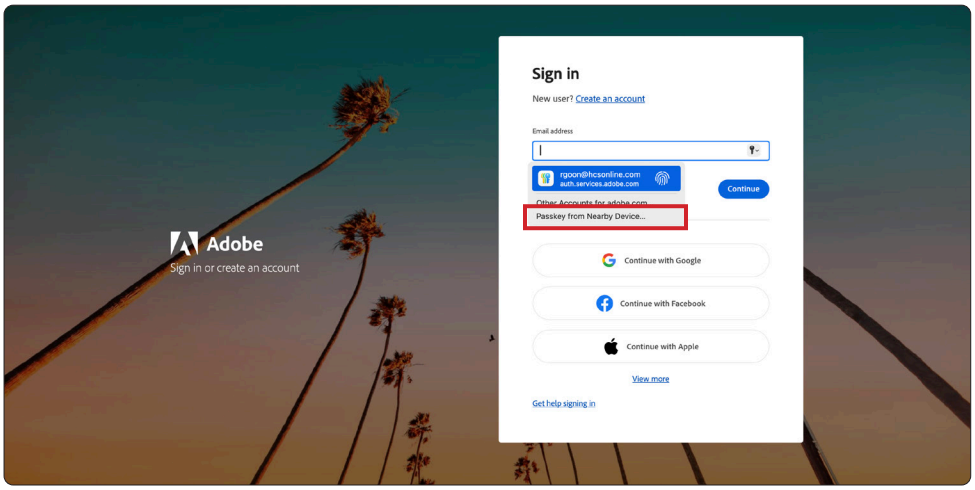


Test the passkey

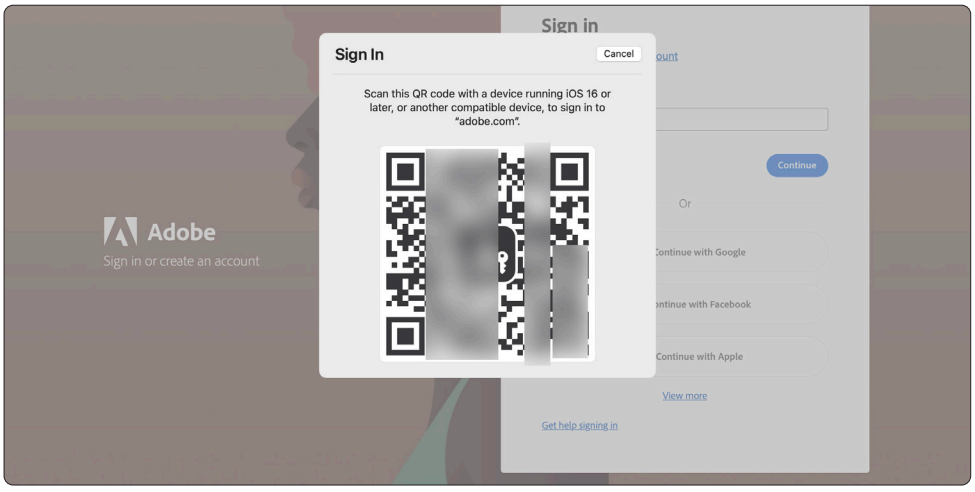
1. Sign out of your Adobe account, quit Safari and relaunch Safari.
2. Go to Adobe.com. Click Sign in.



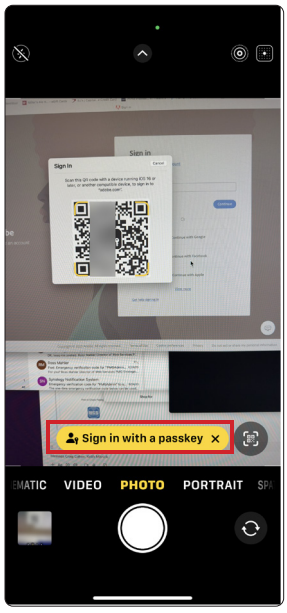
3. Click into the Email address field to launch the Passwords app. Select Passkey from Nearby Device.



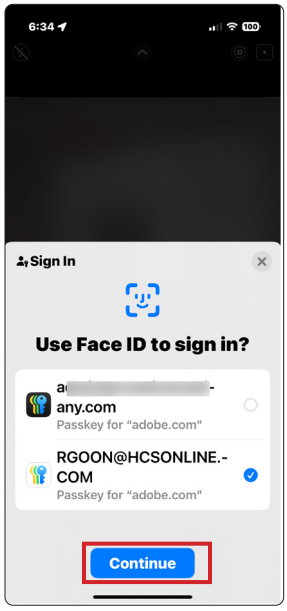
4. Confirm a QR code appears. Scan the QR code with another device, such as an iPhone or iPad



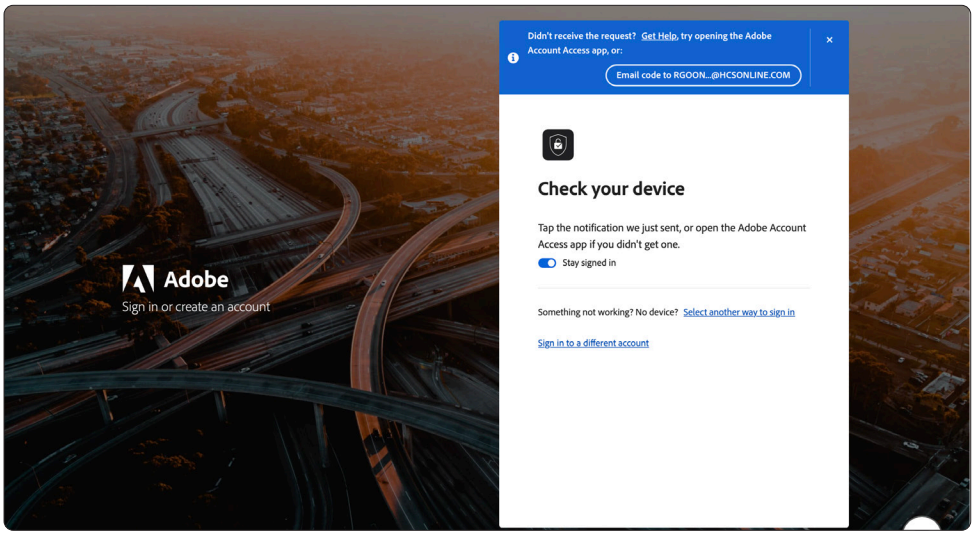
5. Tap Sign in with a passkey.



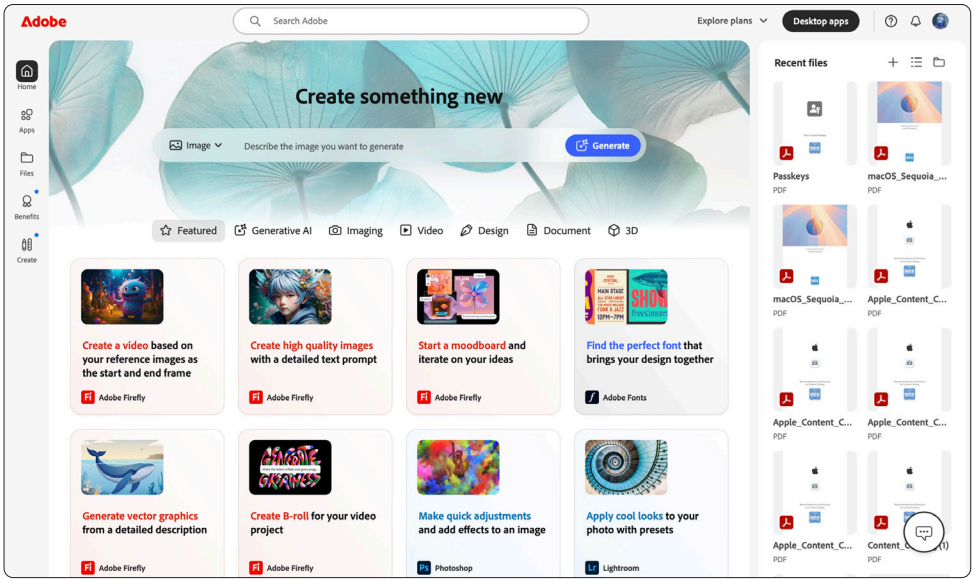
6. Select the appropriate account and tap Continue.



7. If you have two-factor authentication turned, go on to your device and approve sign in.



8. Confirm you have signed in successfully.

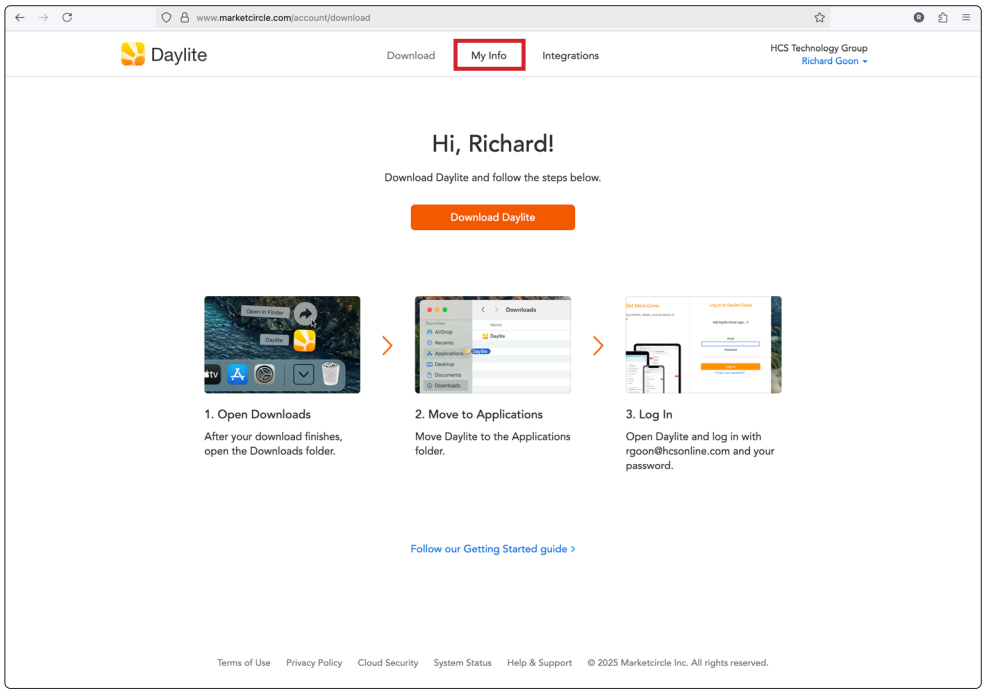


Section 2: Passkeys Stored on Third-Party Apps

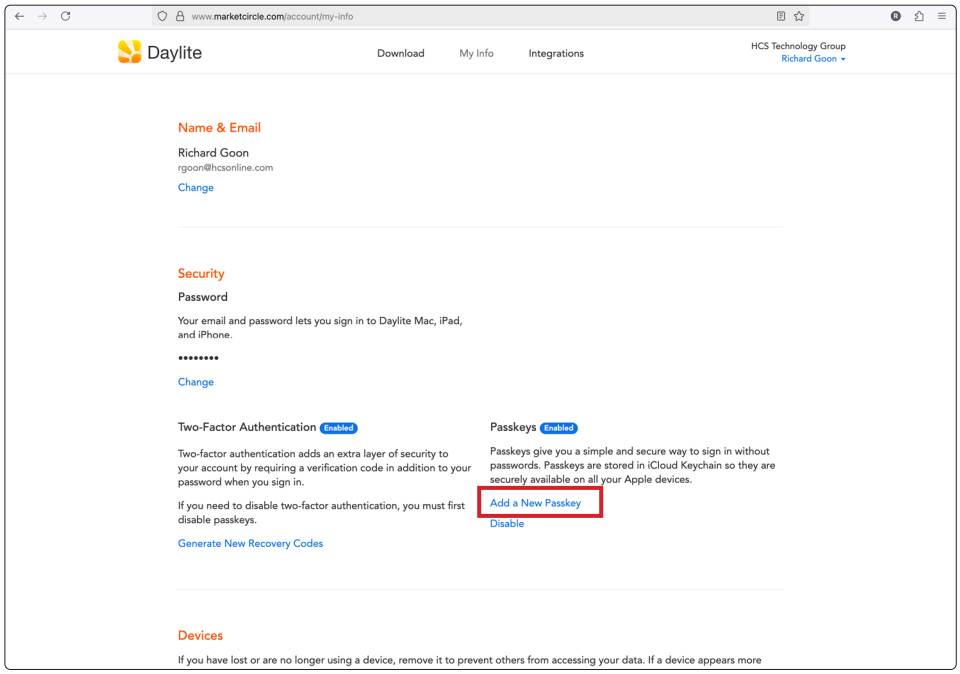
In addition to built-in password managers like Google Password Manager (for Android and Chrome) and iCloud Keychain (now called the Passwords app with iOS 18, iPadOS 18, and macOS Sequoia 15), many third-party password managers also support storing and syncing passkeys. These third-party tools offer similar functionality, including secure storage, synchronization, and cross-device management of passkeys. They are especially useful for users seeking greater control over their data or needing compatibility across multiple platforms. While built-in managers provide seamless integration and a secure, user-friendly experience within their respective ecosystems, third-party options offer a more centralized solution for managing passkeys across diverse devices and operating systems. Notable apps include 1Password, Bitwarden, Dashlane, and Enpass.

Create a passkey for an existing account through 1Password and Firefox
In this Section, we will use 1Password to create a passkey. In order to store a passkey from a browser such as Firefox, you will need to install and enable the 1Password extension in your web browser.

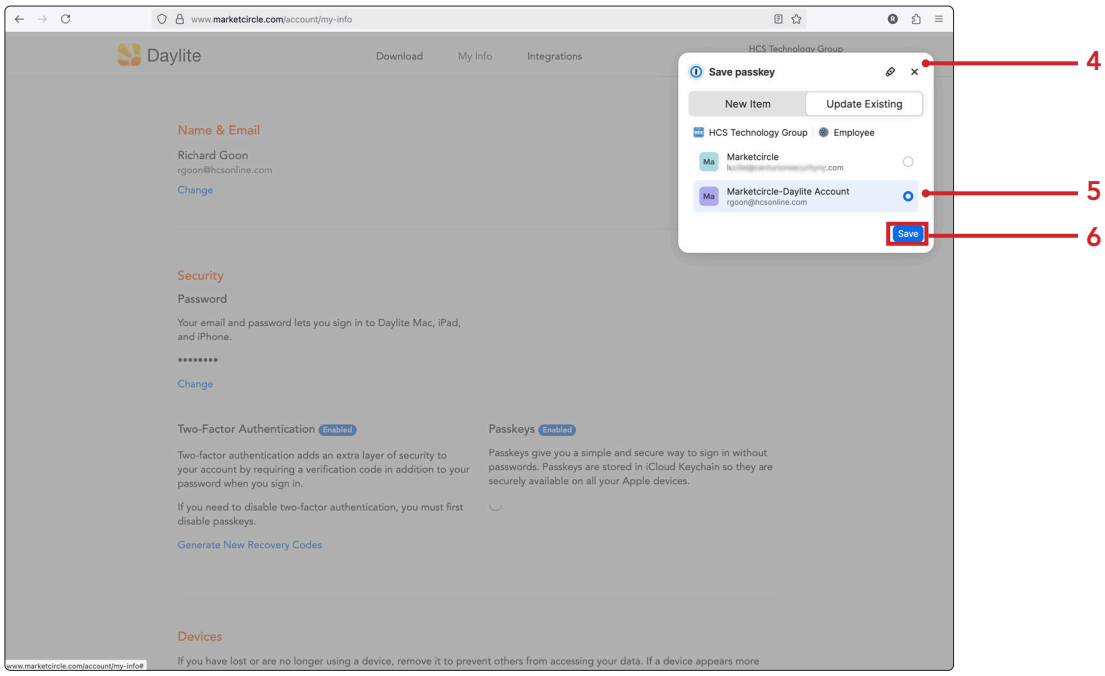
1. For this exercise, we will create a passkey for an account on Marketcircle. Sign into the account using Firefox.
2. Click My Info.



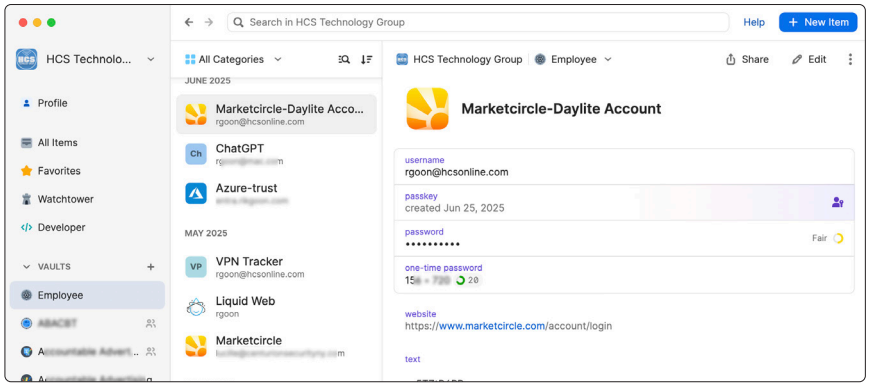
3. Click Add a New Passkey.



4. Confirm the 1Password Extension opens and asks you to save the passkey to an existing account.
5. Select the appropriate account.
6. Click Save.

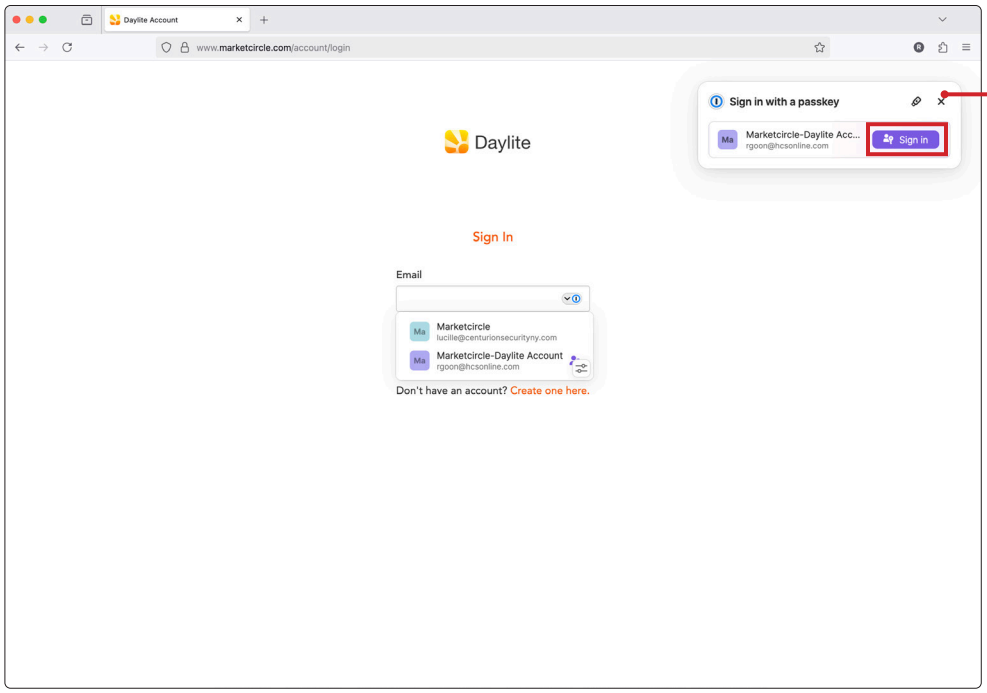


7. Open 1Password and navigate to the account we just created the passkey for.
8. Confirm the passkey is saved for the account.



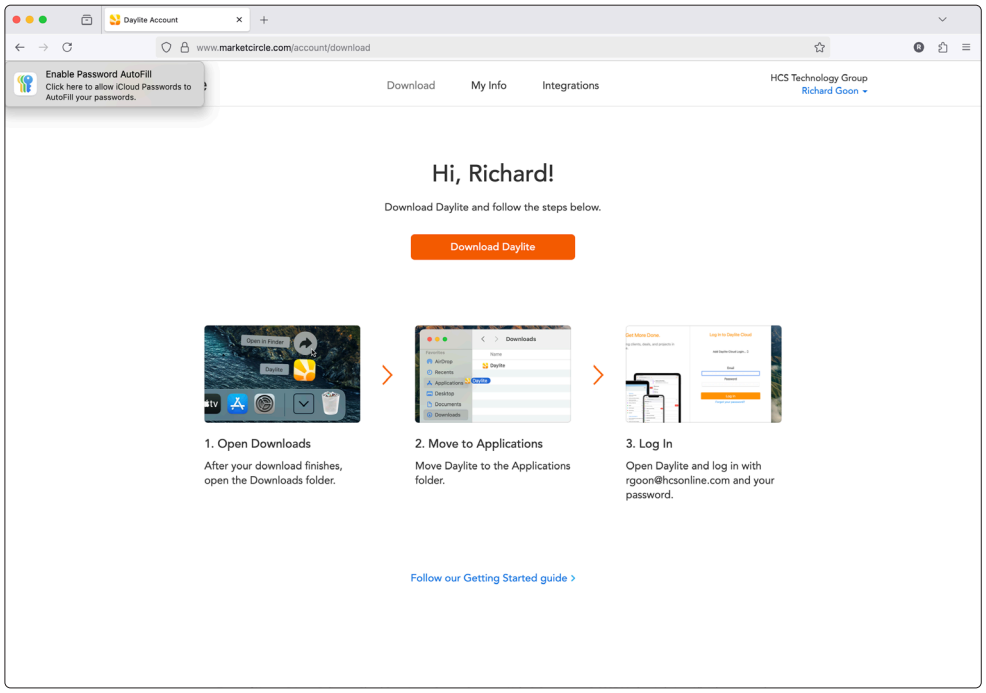
Test the passkey from 1Password extension in Firefox

9. Sign out of the account , quit Firefox and relaunch Firefox.
10. Go to marketcircle.com/account/login.
11. Confirm the 1Password extension appears in the top-right.
12. Click Sign-in



1Password Extension asking to sign in with a passkey

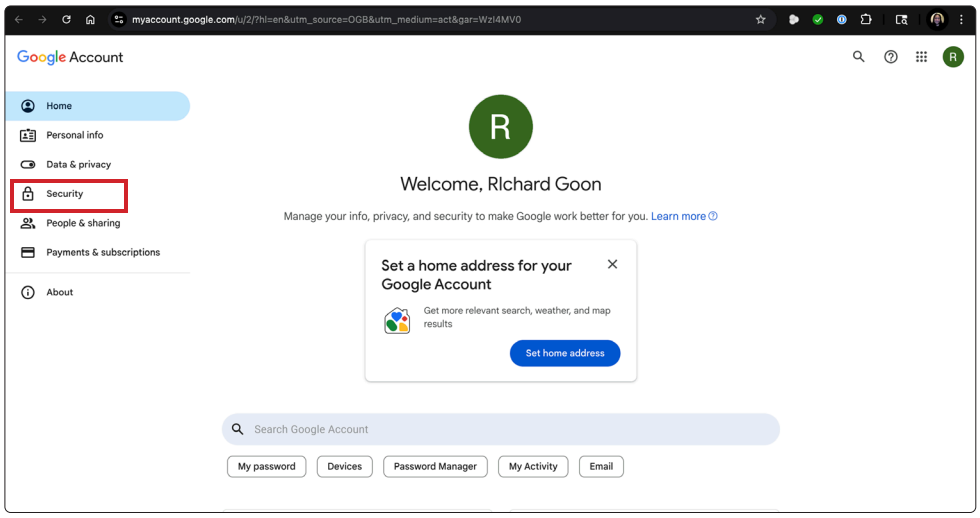
13. Confirm you have been signed into the account.



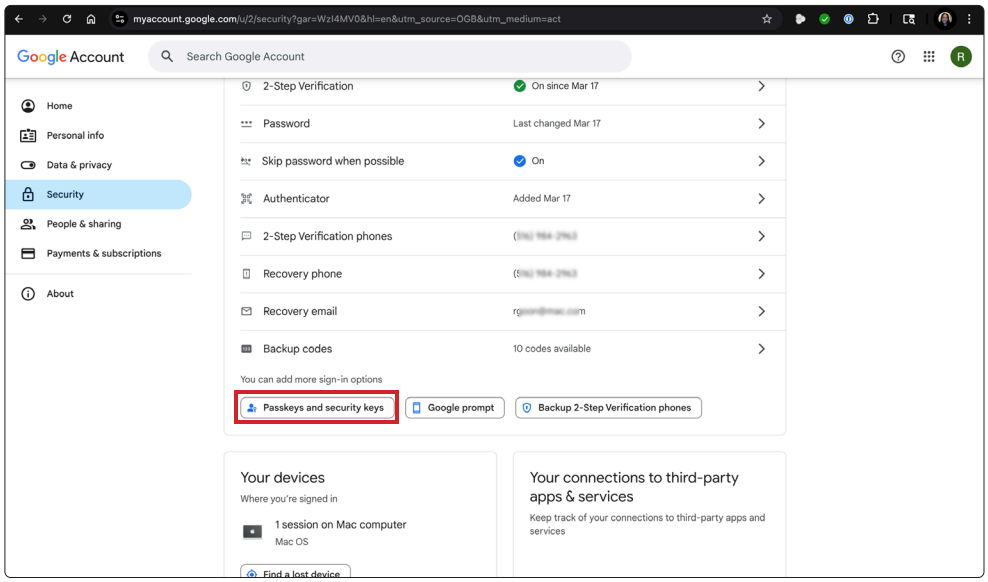
Section 3: Create a Passkey for Your Google Account and store the passkey in iCloud Keychain

You can save passkeys in your Google Chrome profile, where they're protected by a macOS Keychain. If your macOS computer is signed in to an iCloud account, Google Chrome can store passkeys in Apple Passwords. macOS asks you to confirm Google Chrome's access to use passkeys from Apple Passwords. If you don't have an iCloud account, you can also save passkeys in your Google Chrome profile. If your computer is lost or the Google Chrome profile is deleted, you can't recover your passkeys.

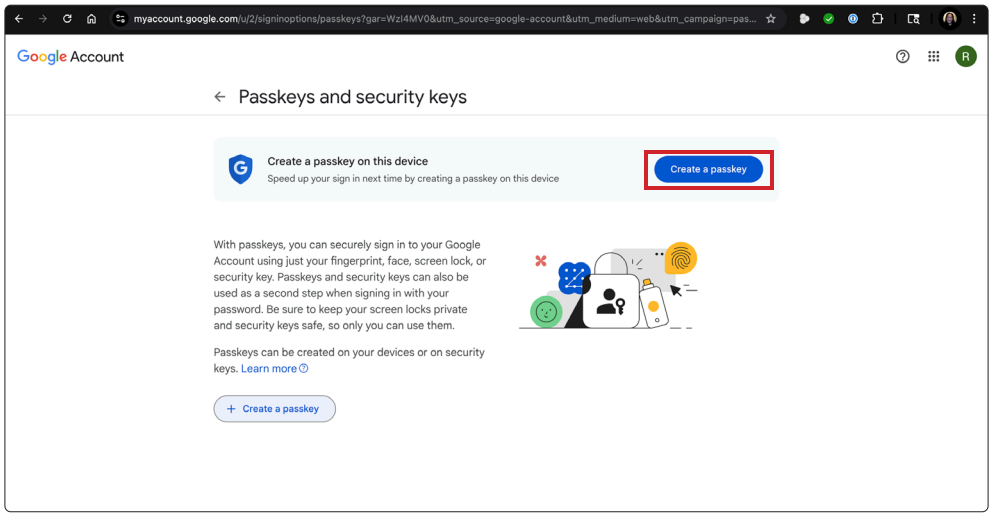
1. In Google Chrome go to your account settings.
2. Click Security.



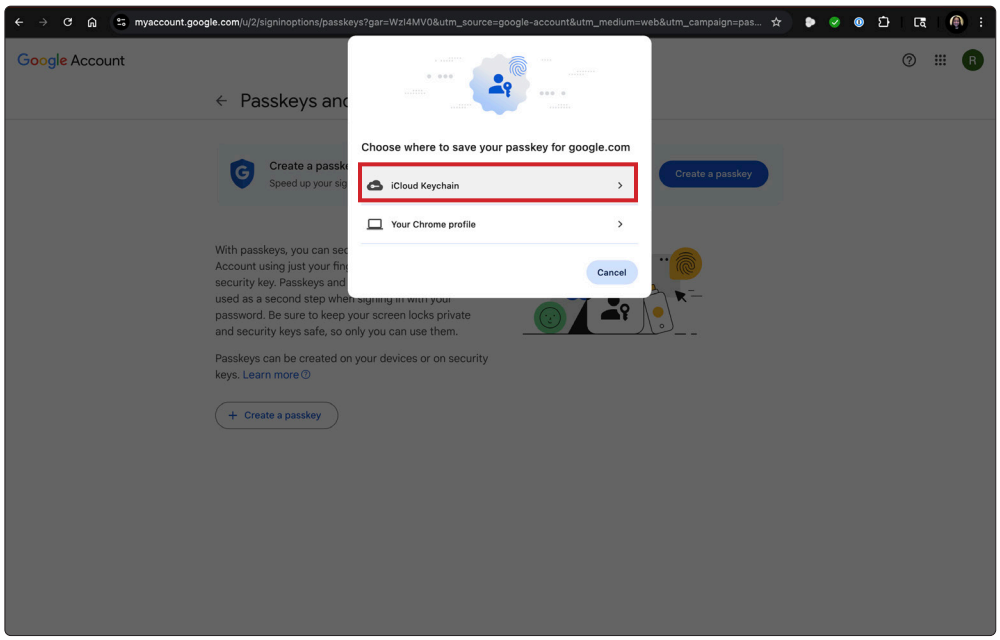
3. Click Passkeys and security keys



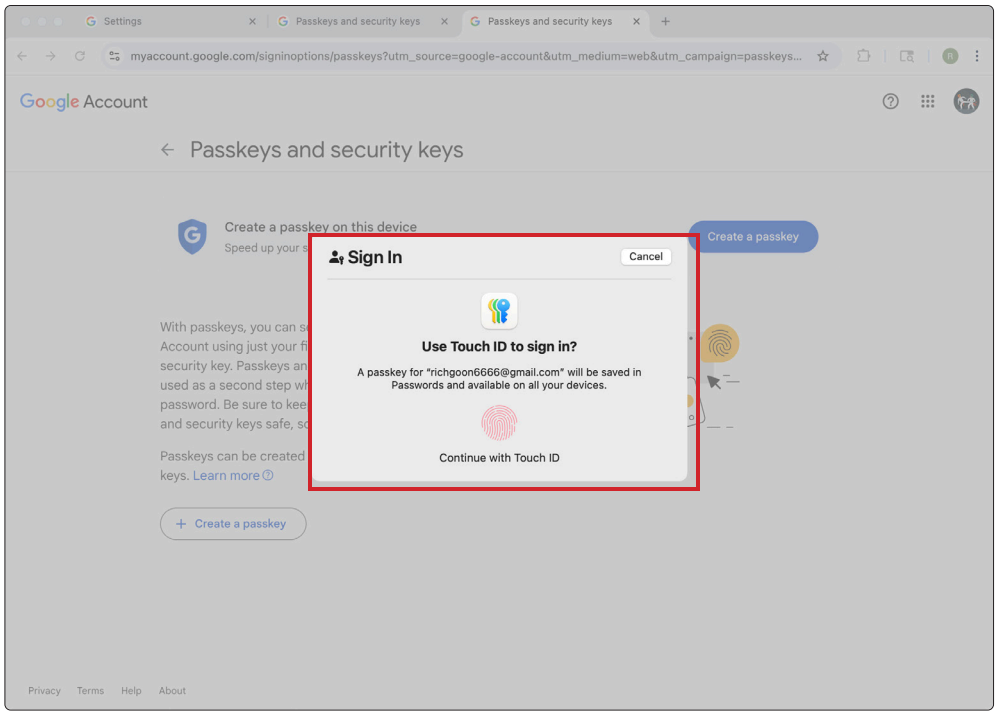
4. Click Create a passkey



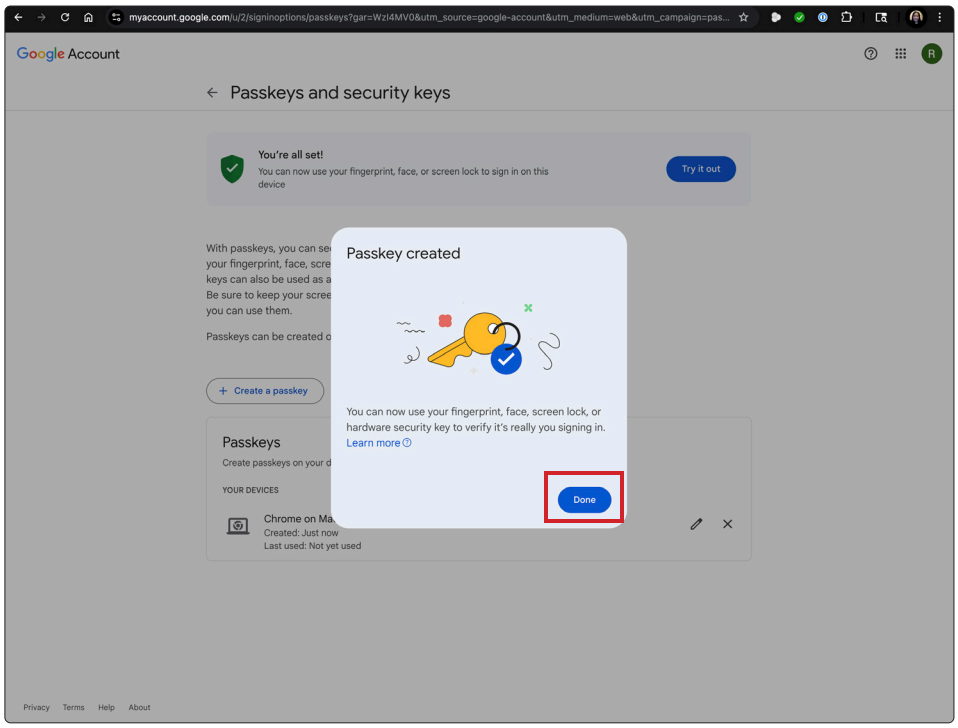
5. Select iCloud Keychain to be able to use the passkey on another device.



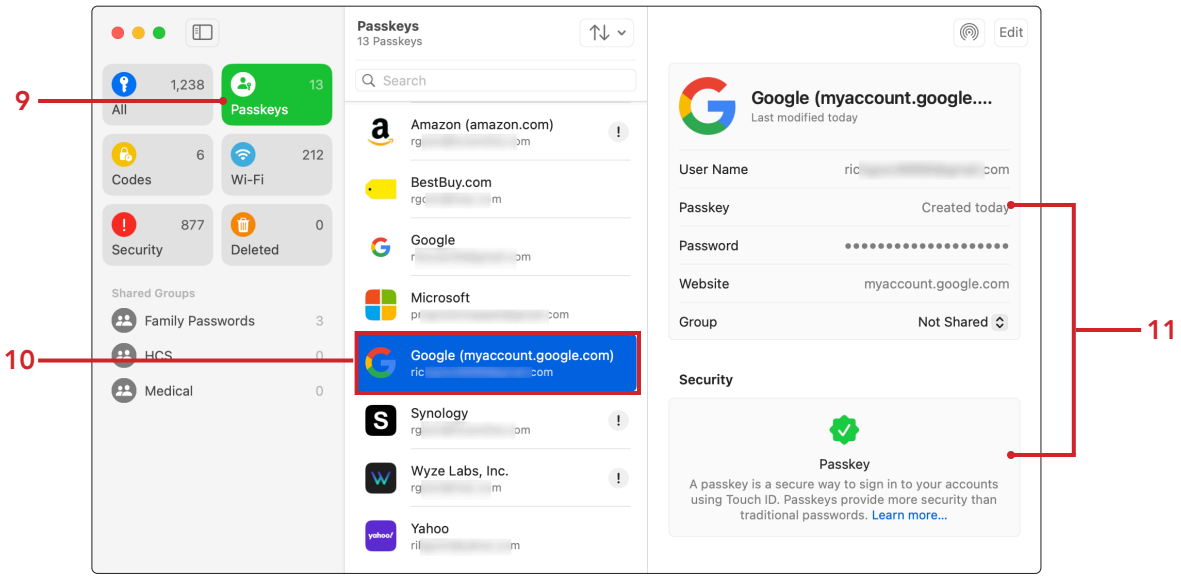
6. When the dialog box that asks for Touch ID to sign in, use your touch ID on your keyboard to save the passkey in iCloud Keychain.



7. Confirm Passkey has been created. Click Done.



8. Go to the Passwords App.
9. Click Passkeys.
10. Select the Google Account.
11. Confirm a Passkey was created.



Section 4: References

About the security of passkeys
https://support.apple.com/en-us/102195

The Complete Passkey Authentication Resource
https://www.passkeys.com

Google Passkey's Passwordless Authentication
https://safety.google/authentication/passkey/

Test how a passkey works
https://www.passkeys.io

List of websites that support passkeys
https://passkeys.directory

https://www.passkeys.com/websites-with-passkey-support-sites-directory

https://www.passkeys.io/who-supports-passkeys

https://www.keepersecurity.com/passkeys-directory/