Passkey is spelled with a lowercase “p”

Joel and Charles

What’s Relevant?

Biometrics

- Facial Recognition research began in 1964 with Woody Bledsoe, Helen Chan Wolf and Charles Bisson

- The FBI in the US researched automated fingerprint identification in 1969 and funded prototypes for scanners in 1975

- Sirovich and Kirby researched using linear algebra for facial recognition in 1988, which evolved into Eigenface

- Bill Gates predicted the death of the password in 2004

- JWT introduced in 2010

Elsewhere…

- Fernando Corbató conceived of passwords on computers in 1960
- German Helmut Gröttrup patented putting an integrated circuit on a card in 1968
- French Roland Moreno patented secure memory on a “smart card” in 1974
- SecurID was released in 1993 by Secure Dynamics (merged with RSA Data Security)
- AT&T filed a U.S. patent for 2FA in 1996
- RSA introduced SecurID software tokens in 2002
- Yubikey was introduced in 2008
- Duo Security was founded in 2010
- Webauthn proposed and the FIDO Alliance was formed in 2013

https://commons.wikimedia.org/wiki/File:RSA-SecurID-Token.jpg

10 Years Of Biometrics at Apple

- Keychain was released in 1999, for Mac OS 8.6
- The iPhone 5s introduced the first onboard biometric sensor for Apple products in 2013
- The Mac got the Touch Bar in 2016
- Face ID was introduced in 2017 on the iPhone X
- Magic Keyboard with Touch ID released in 2021
- Passkey support added in 2022

Passwords, tokens, and passkeys

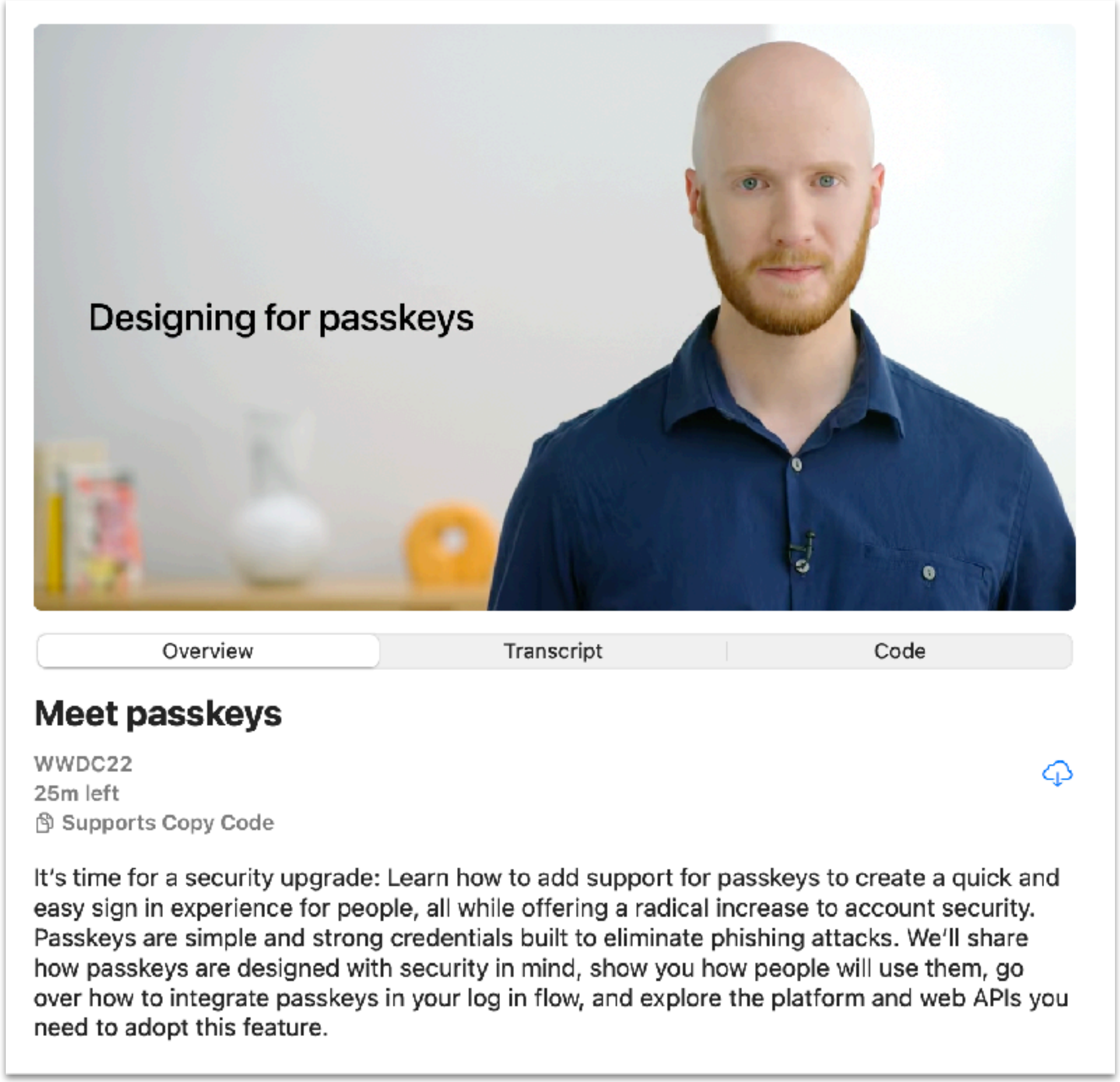
FIDO2 was introduced in 2018

Passkeys are an implementation of the FIDO2 standard

Instead of being on hardware, FIDO credentials can be on multiple devices

They are also cross-platform

WWDC 2022



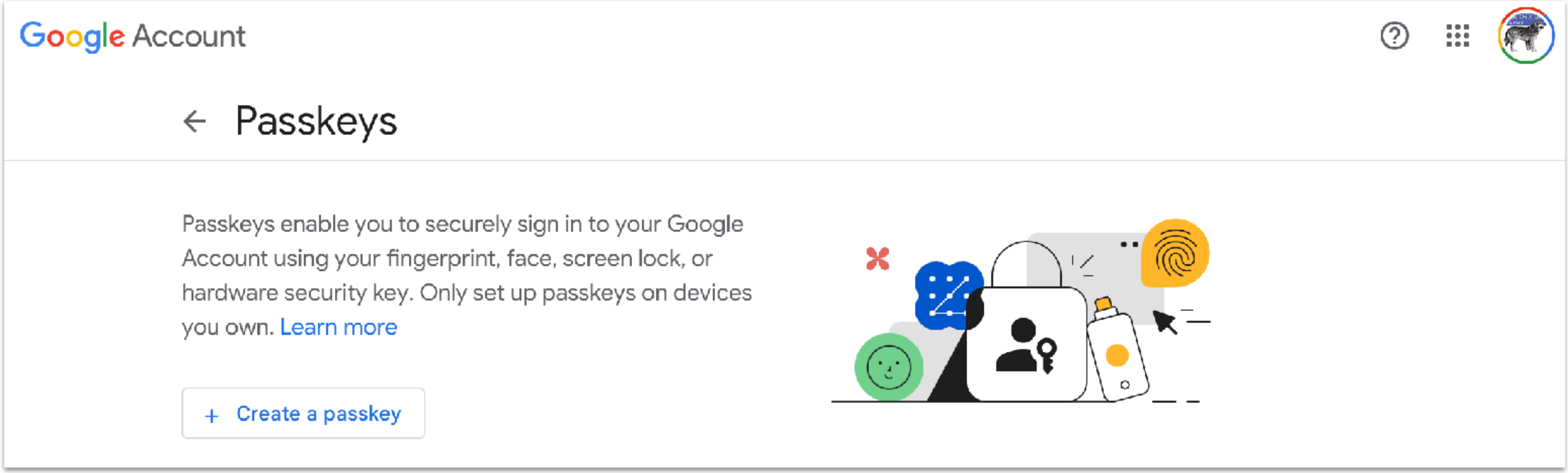
Meet passkeys

WWDC22
25m left
Supports Copy Code

It's time for a security upgrade: Learn how to add support for passkeys to create a quick and easy sign in experience for people, all while offering a radical increase to account security. Passkeys are simple and strong credentials built to eliminate phishing attacks. We'll share how passkeys are designed with security in mind, show you how people will use them, go over how to integrate passkeys in your log in flow, and explore the platform and web APIs you need to adopt this feature.

Google introduced passkey support in 2022

Click “Create a Passkey” From Accounts -> Security

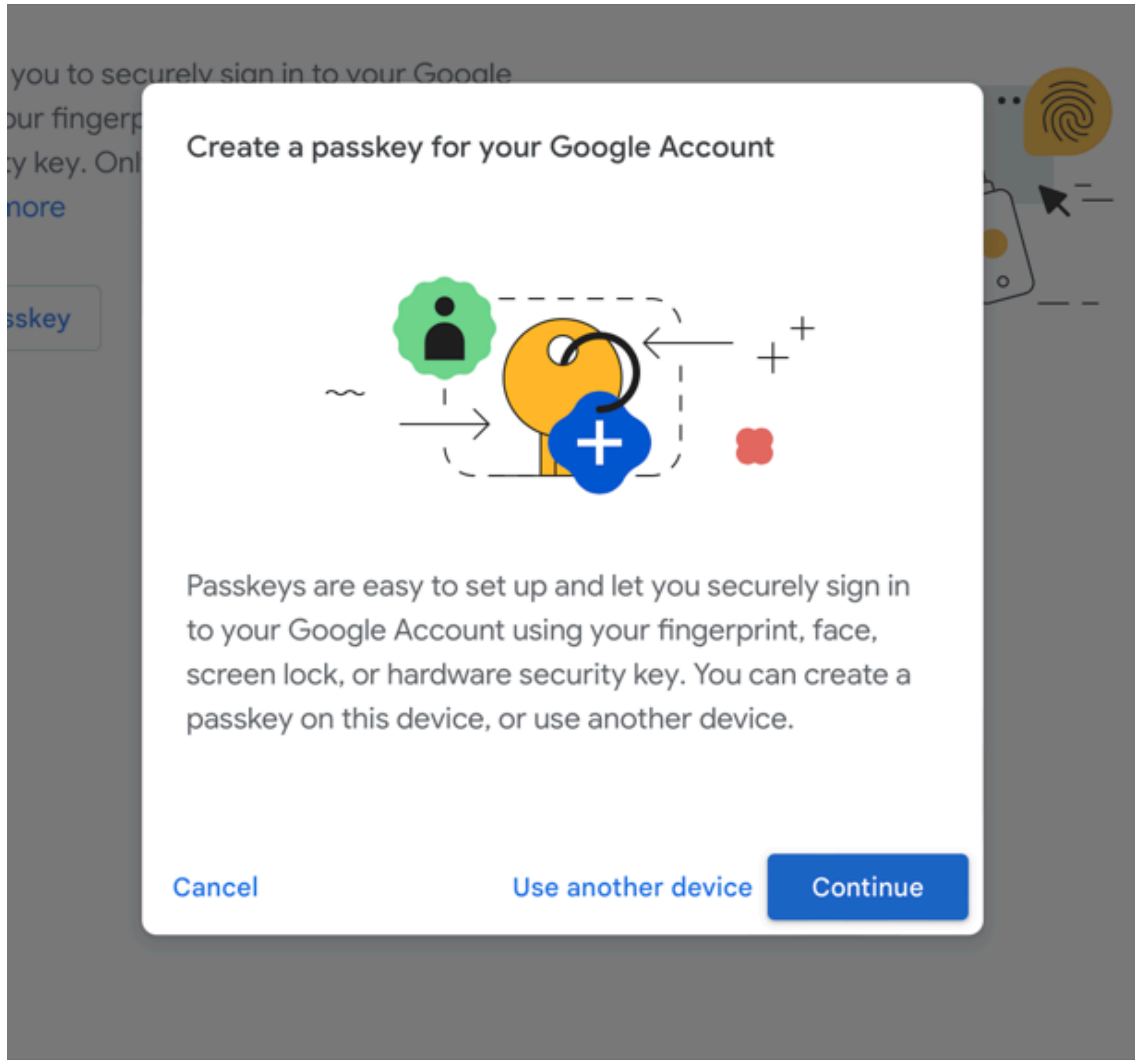


Google Account

← Passkeys

Passkeys enable you to securely sign in to your Google Account using your fingerprint, face, screen lock, or hardware security key. Only set up passkeys on devices you own. Learn more

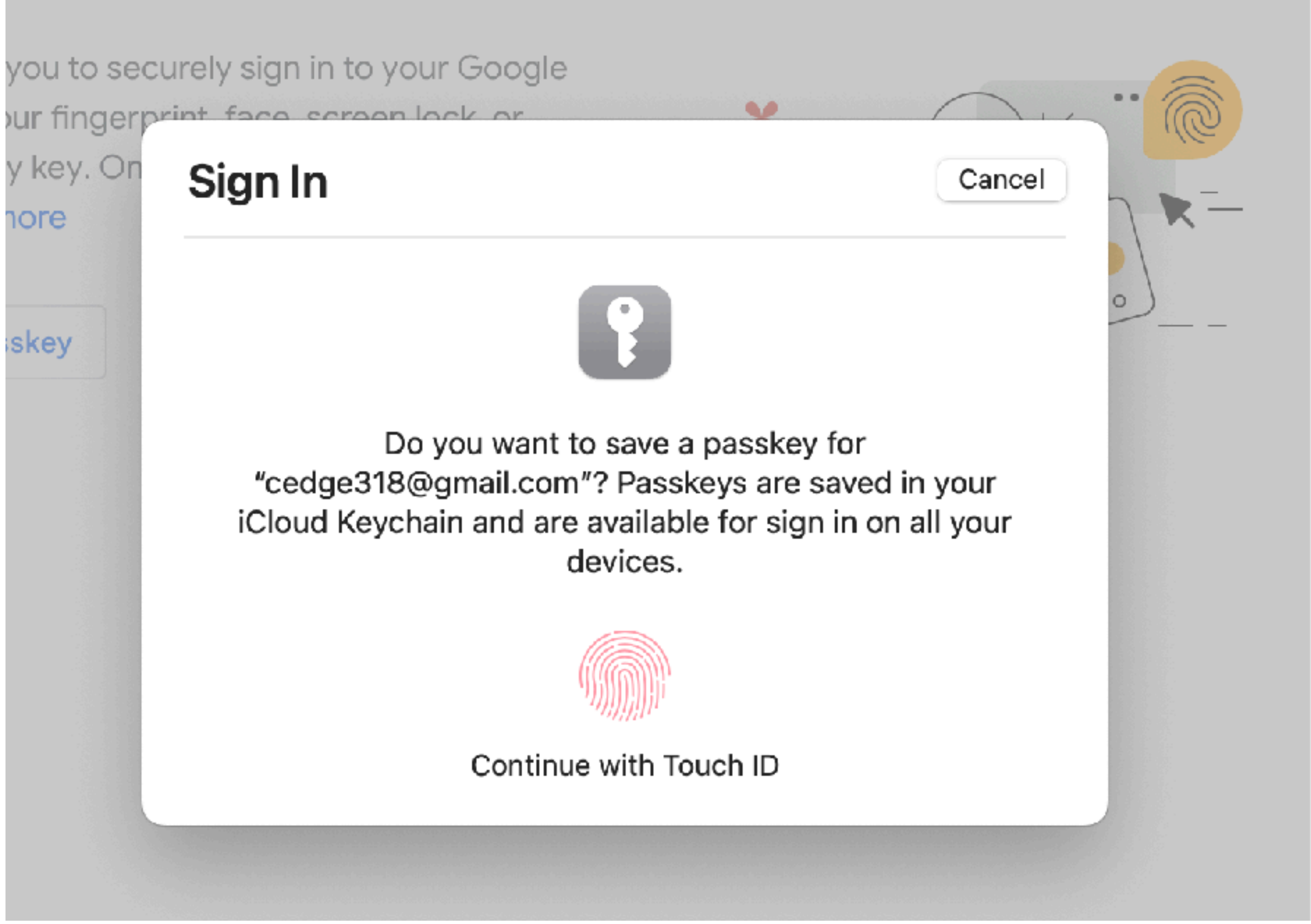
Click Continue



Create a passkey for your Google Account

Passkeys are easy to set up and let you securely sign in to your Google Account using your fingerprint, face, screen lock, or hardware security key. You can create a passkey on this device, or use another device.

Give Fingerprint



you to securely sign in to your Google
ur fingerprint, face, screen lock, or
y key. On
nore

skey

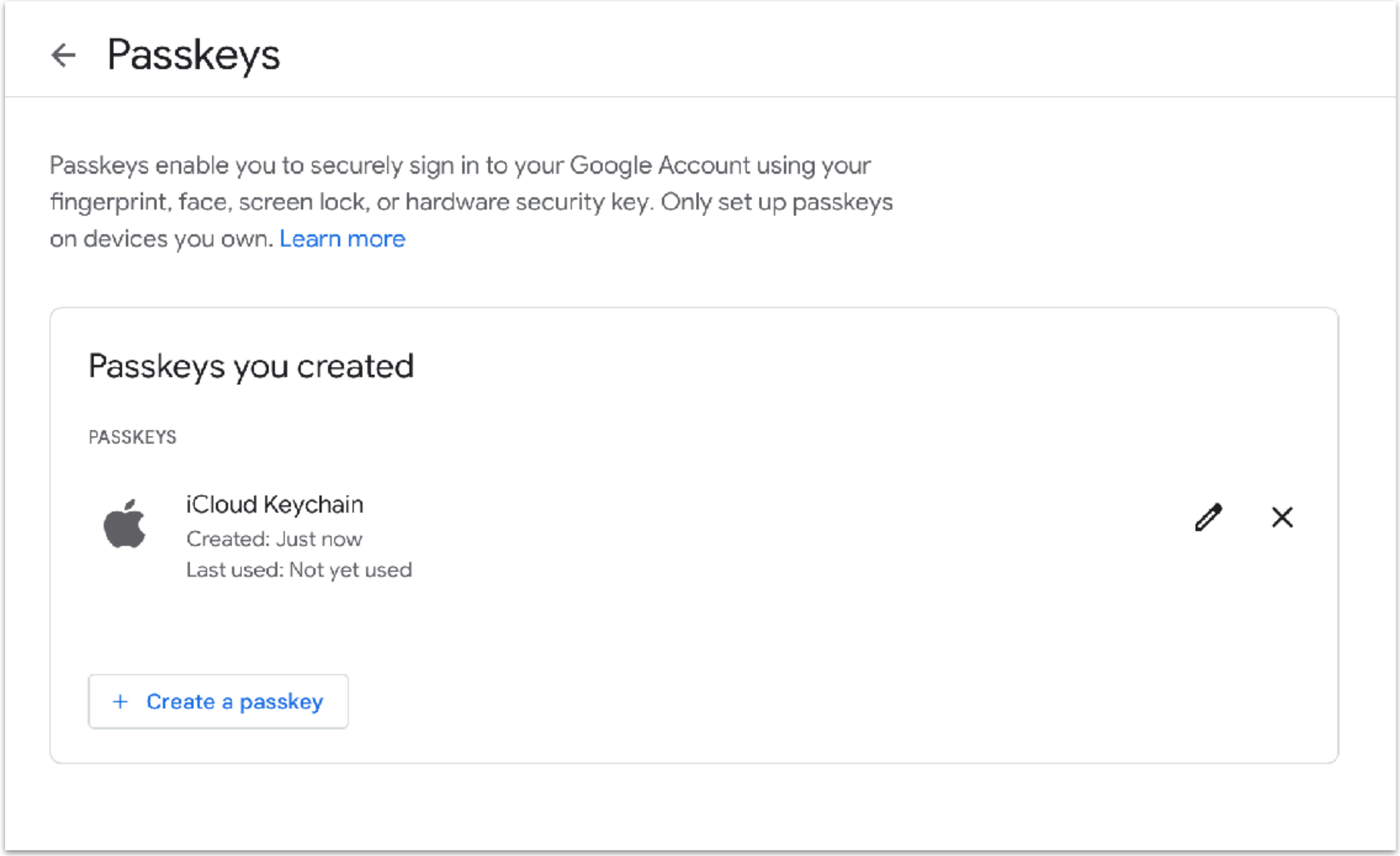
Sign In

Cancel

Do you want to save a passkey for "cedge318@gmail.com"? Passkeys are saved in your iCloud Keychain and are available for sign in on all your devices.

Continue with Touch ID

Get Passkey



← Passkeys

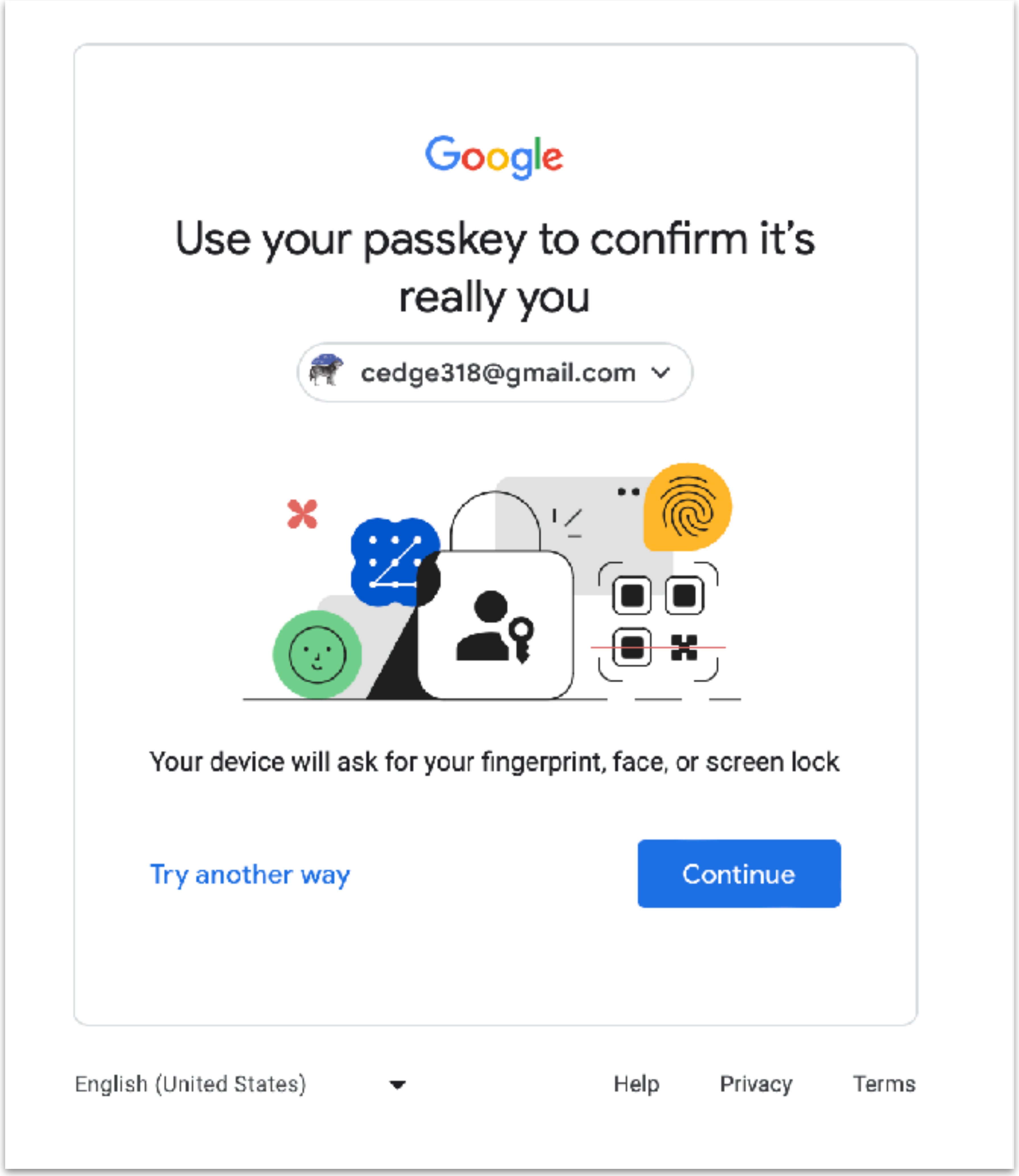
Passkeys enable you to securely sign in to your Google Account using your fingerprint, face, screen lock, or hardware security key. Only set up passkeys on devices you own. Learn more

Passkeys you created

PASSKEYS

iCloud Keychain
Created: Just now
Last used: Not yet used

Verify From The Accounts Page



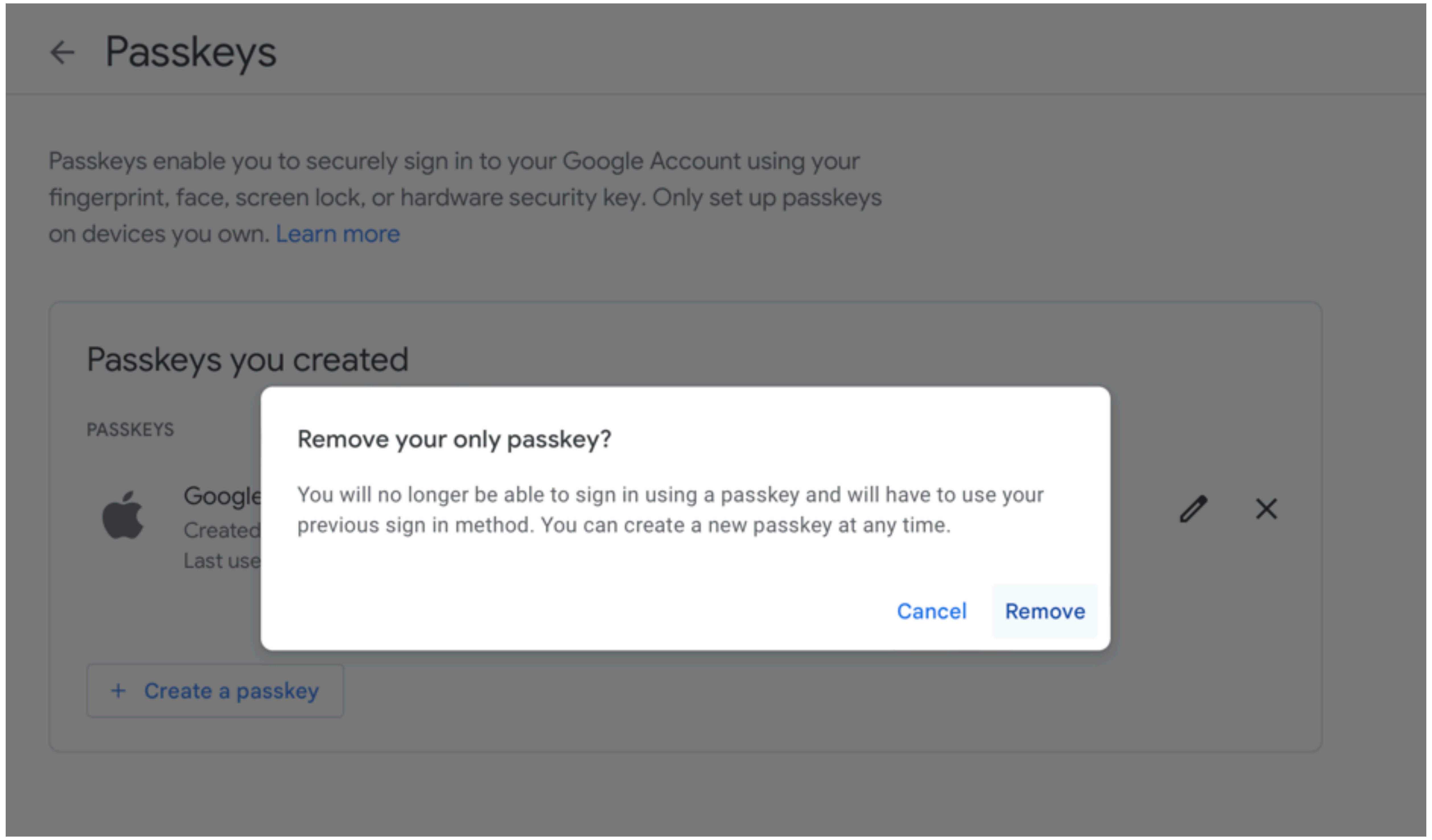
Google

Use your passkey to confirm it's really you

cedge318@gmail.com

Your device will ask for your fingerprint, face, or screen lock

Click the X to Disable



Passkeys

Passkeys enable you to securely sign in to your Google Account using your fingerprint, face, screen lock, or hardware security key. Only set up passkeys on devices you own. Learn more

Passkeys you created

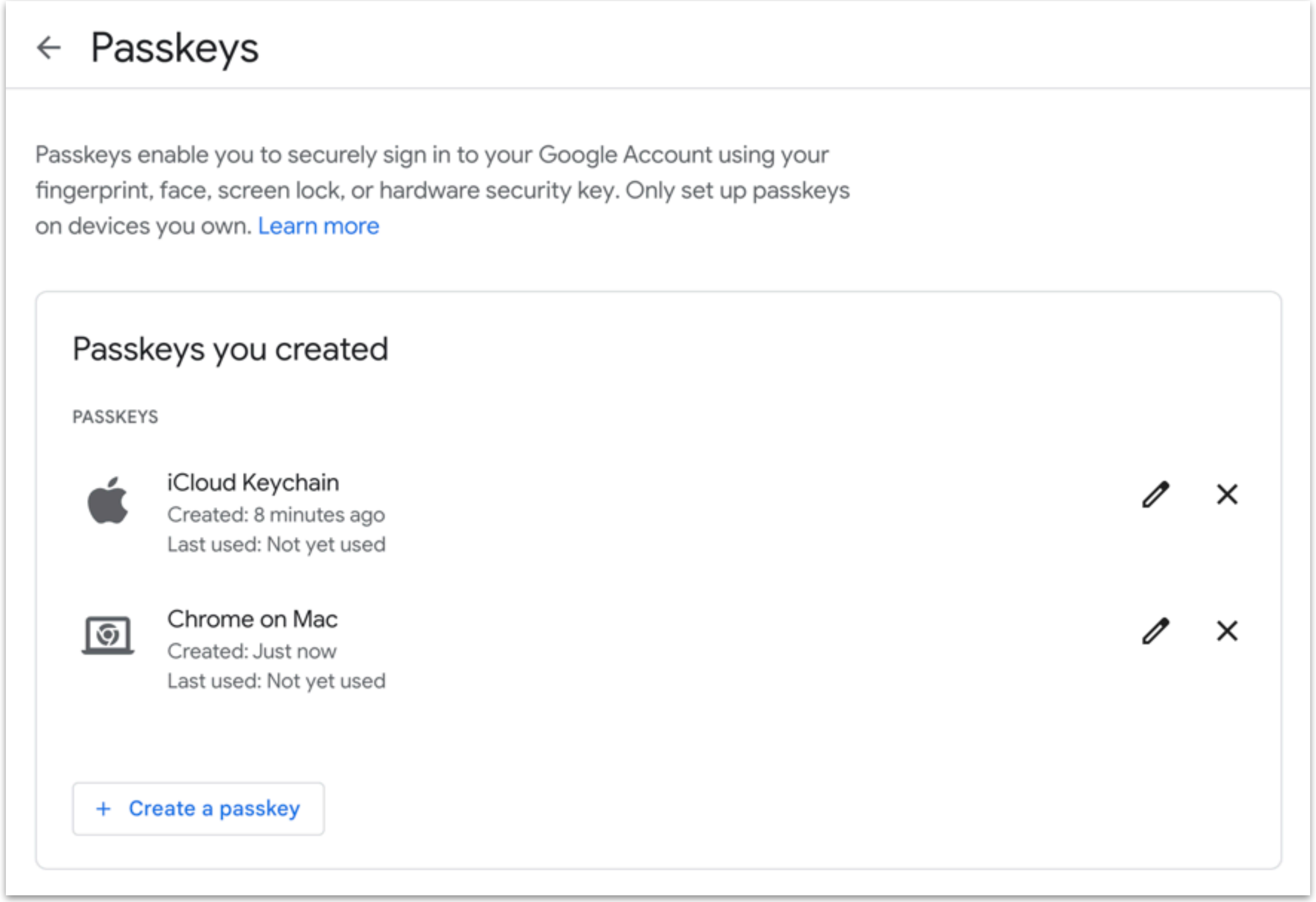
PASSKEYS

Google
Created
Last use

Remove your only passkey?

You will no longer be able to sign in using a passkey and will have to use your previous sign in method. You can create a new passkey at any time.

Repeat Process In Chrome



← Passkeys

Passkeys enable you to securely sign in to your Google Account using your fingerprint, face, screen lock, or hardware security key. Only set up passkeys on devices you own. Learn more

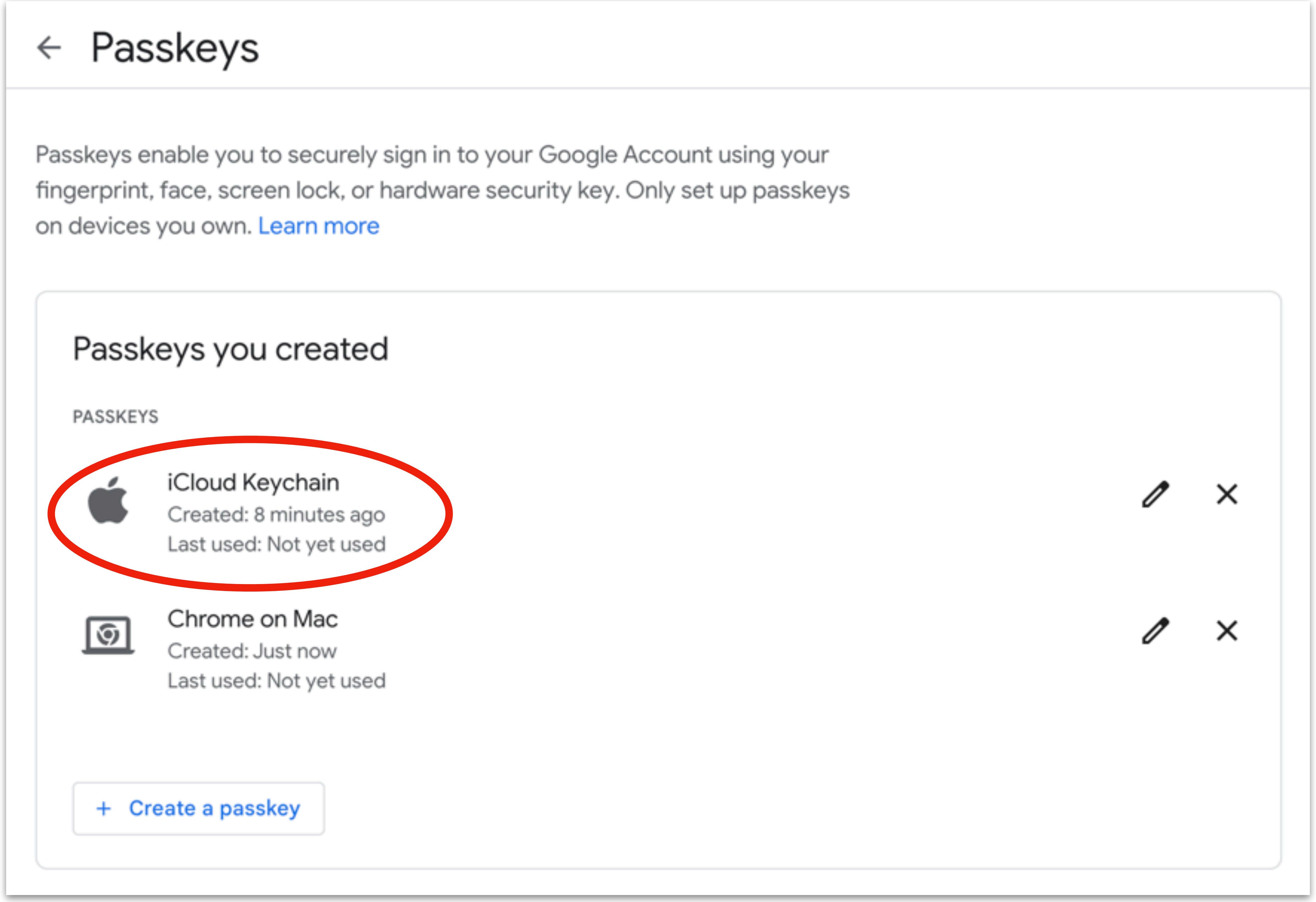
Passkeys you created

PASSKEYS

iCloud Keychain
Created: 8 minutes ago
Last used: Not yet used

Chrome on Mac
Created: Just now
Last used: Not yet used

Repeat Process In Chrome



← Passkeys

Passkeys enable you to securely sign in to your Google Account using your fingerprint, face, screen lock, or hardware security key. Only set up passkeys on devices you own. Learn more

Passkeys you created

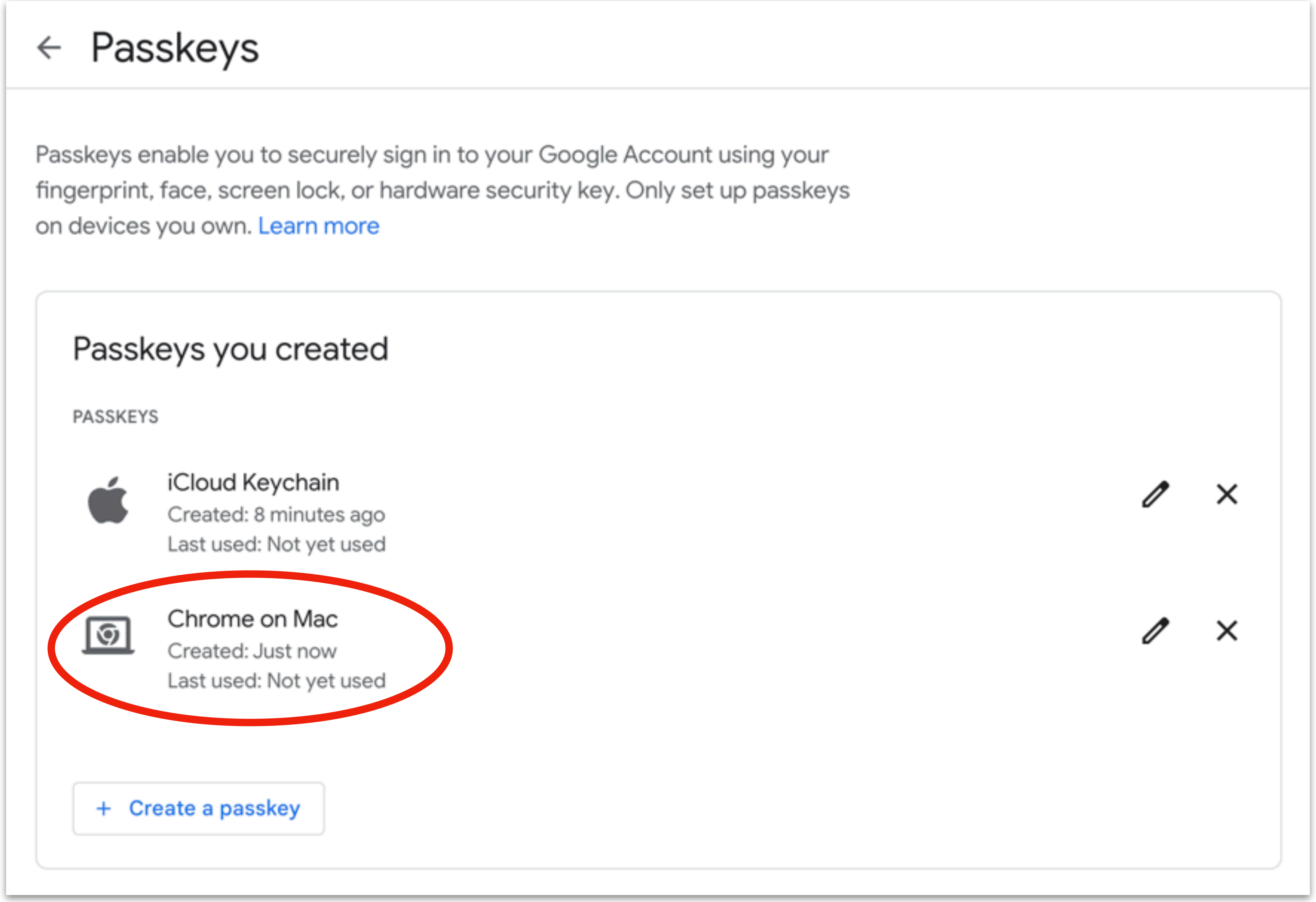
PASSKEYS

iCloud Keychain
Created: 8 minutes ago
Last used: Not yet used

Chrome on Mac
Created: Just now
Last used: Not yet used

Passkeys Require iCloud Keychain, Which Only Came To MAIDs In The Past Few Weeks

Repeat Process In Chrome



← Passkeys

Passkeys enable you to securely sign in to your Google Account using your fingerprint, face, screen lock, or hardware security key. Only set up passkeys on devices you own. Learn more

Passkeys you created

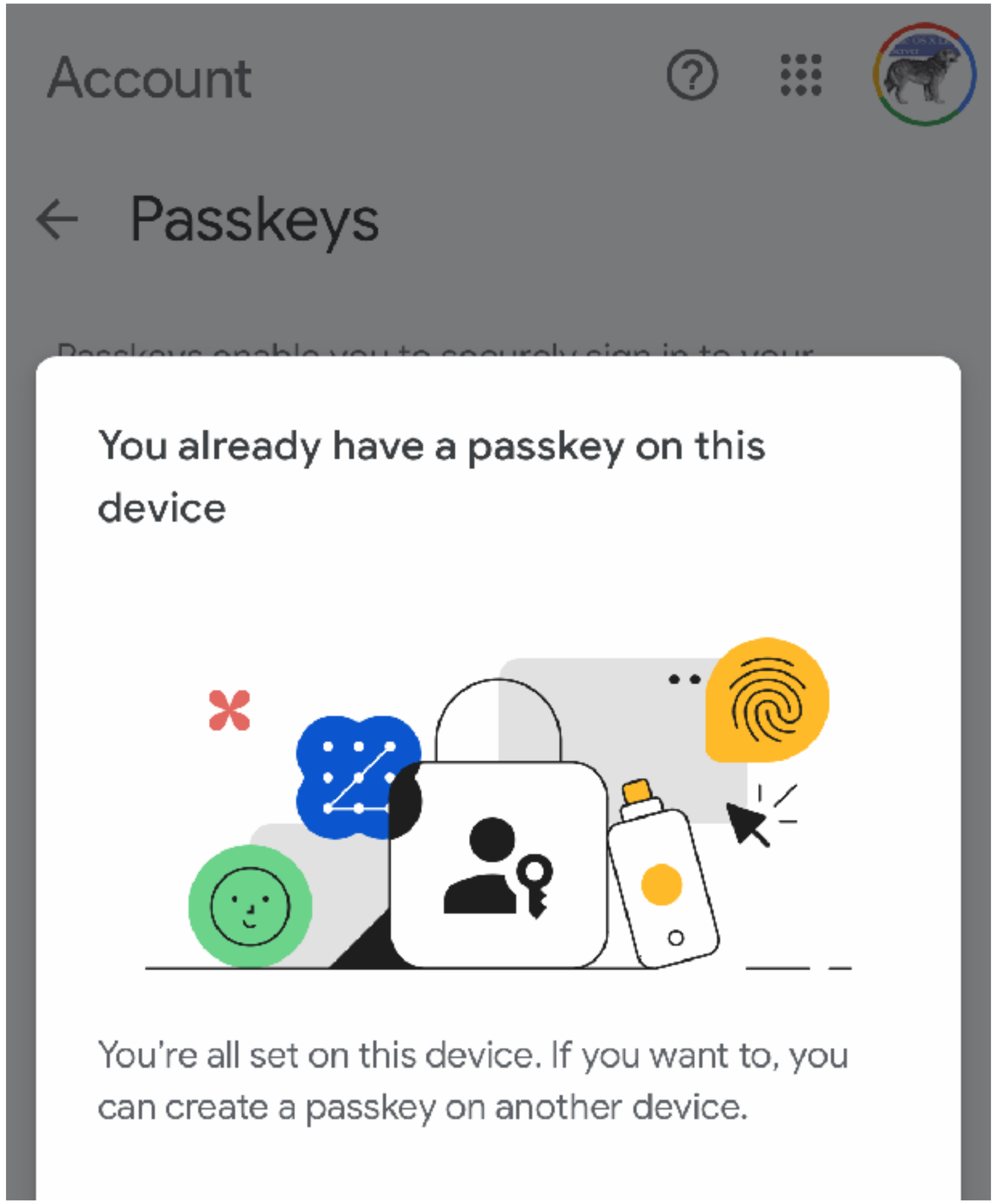
PASSKEYS

iCloud Keychain
Created: 8 minutes ago
Last used: Not yet used

Chrome on Mac
Created: Just now
Last used: Not yet used

Each Password Manager Needs Its Own passkey

But Then - No Need On iPhone



Account

Passkeys

Passkeys enable you to securely sign in to your

You already have a passkey on this device

You're all set on this device. If you want to, you can create a passkey on another device.

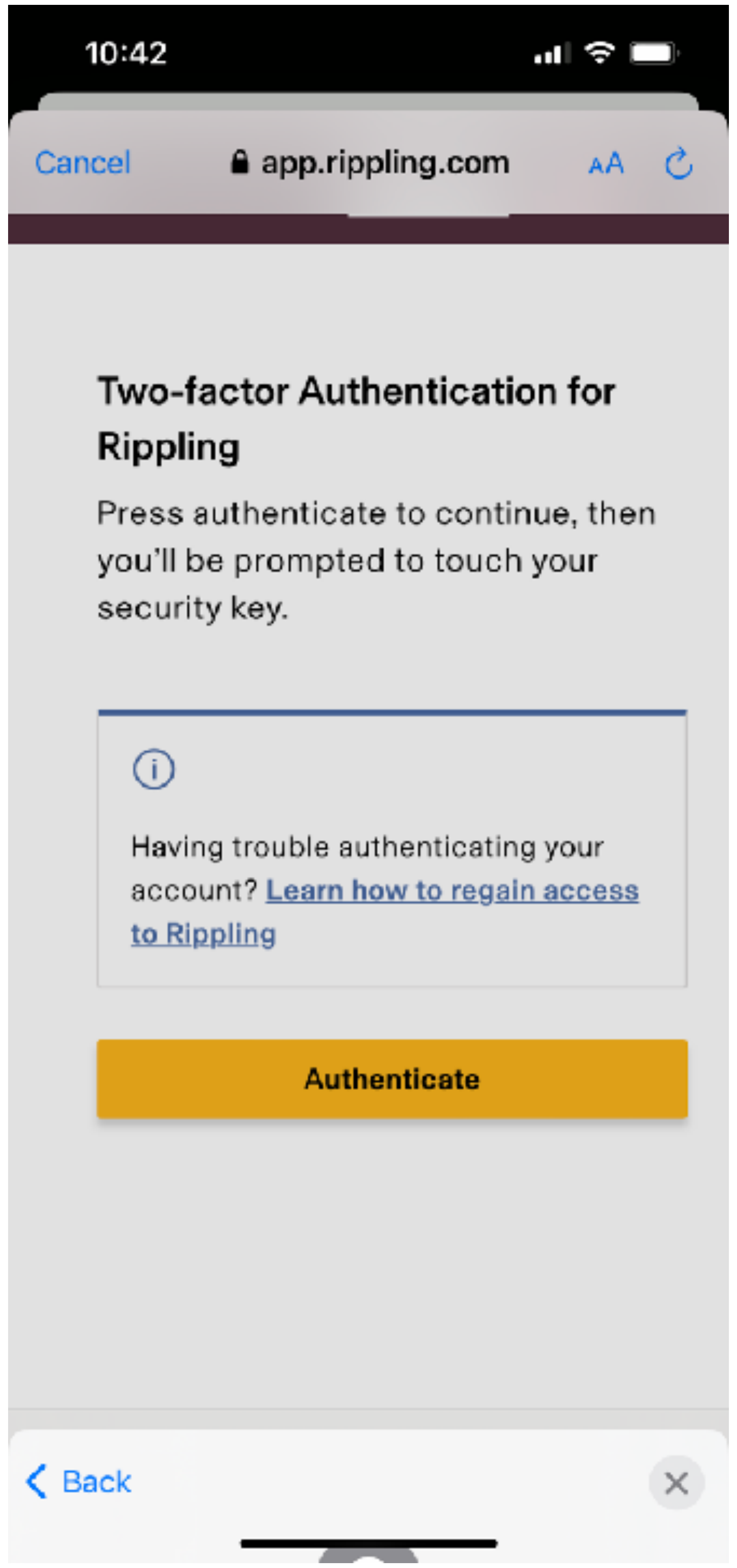
Do you still have a password for Google, though?

PINs for biometrics
&& passwords to get passkeys

Other vendors

Rippling introduced support in 2023

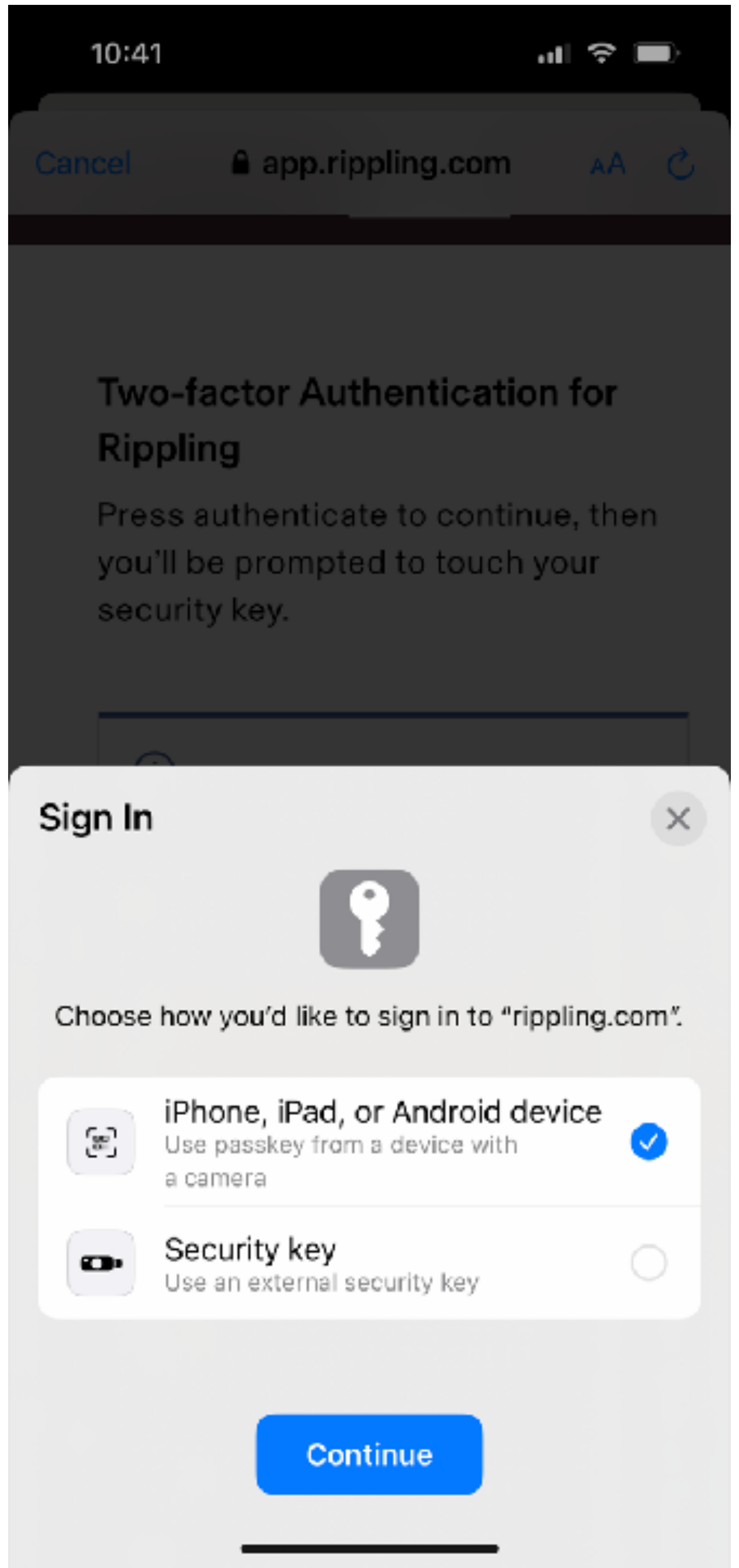
Log Into Web App



Two-factor Authentication for Rippling

Press authenticate to continue, then you'll be prompted to touch your security key.

Having trouble authenticating your account? Learn how to regain access to Rippling



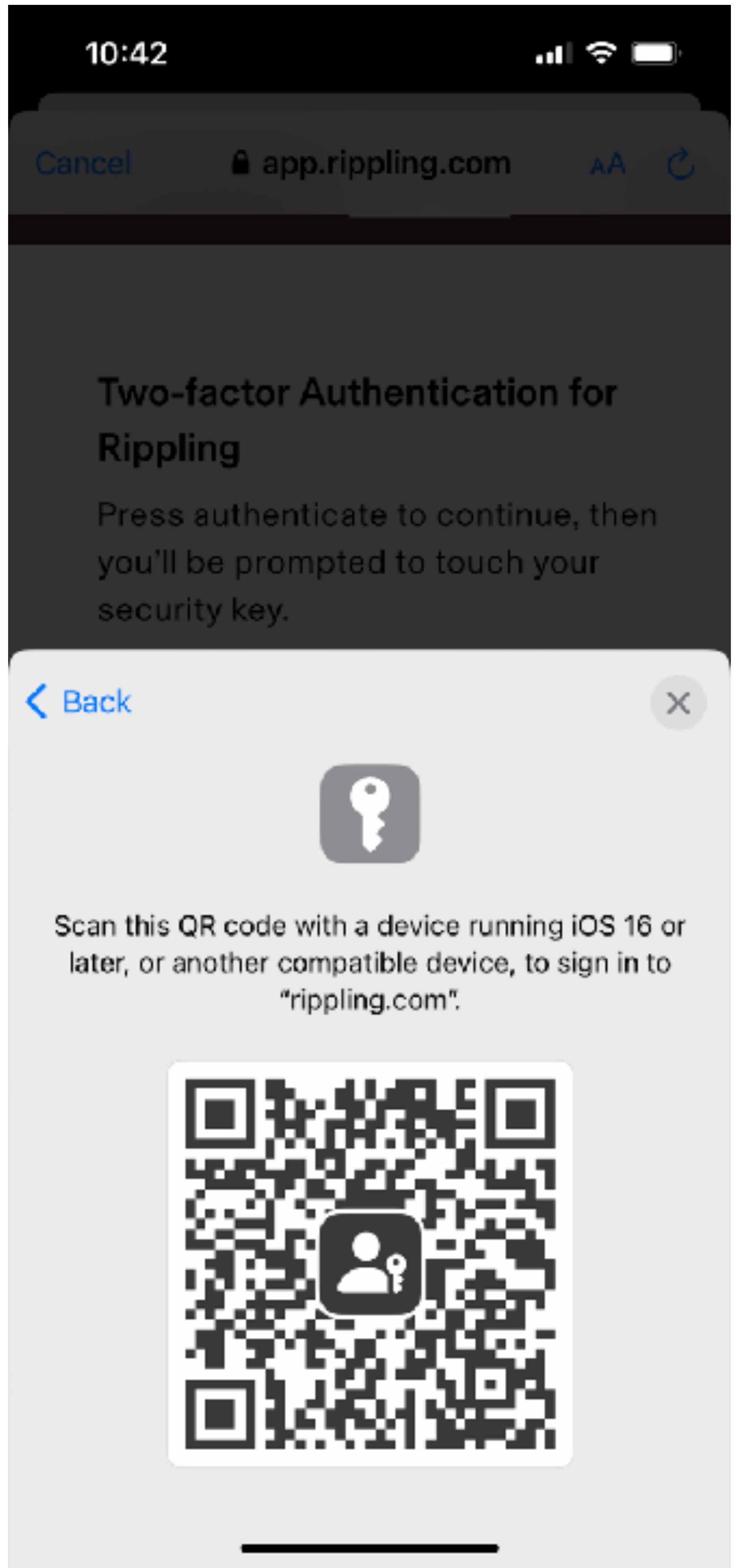
Two-factor Authentication for Rippling

Press authenticate to continue, then you'll be prompted to touch your security key.

Sign In

Choose how you'd like to sign in to "rippling.com".

- iPhone, iPad, or Android device ☑
  Use passkey from a device with a camera
- Security key ○
  Use an external security key



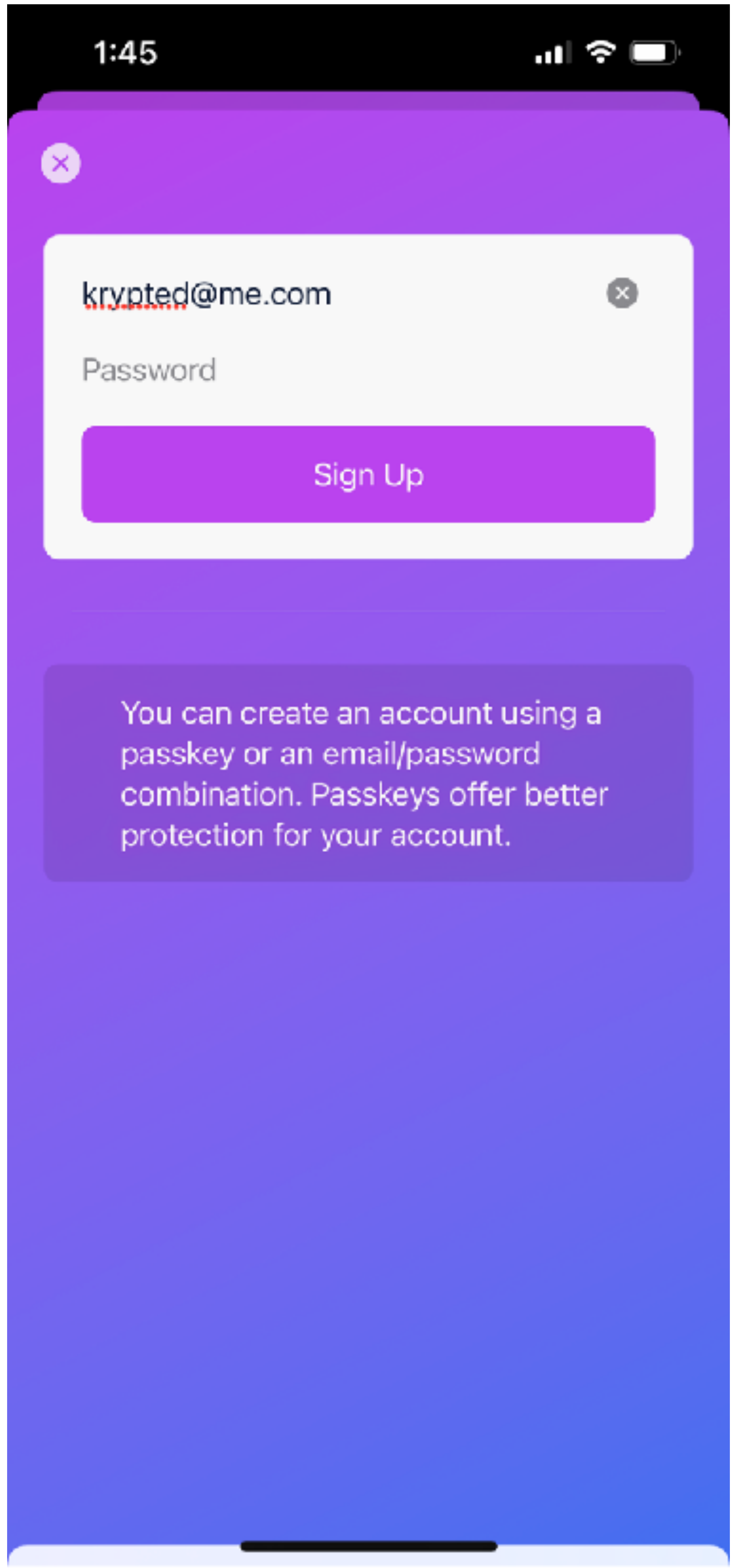
Two-factor Authentication for Rippling

Press authenticate to continue, then you'll be prompted to touch your security key.

Scan this QR code with a device running iOS 16 or later, or another compatible device, to sign in to "rippling.com".

Random App We Don’t Endorse

A Typical Flow

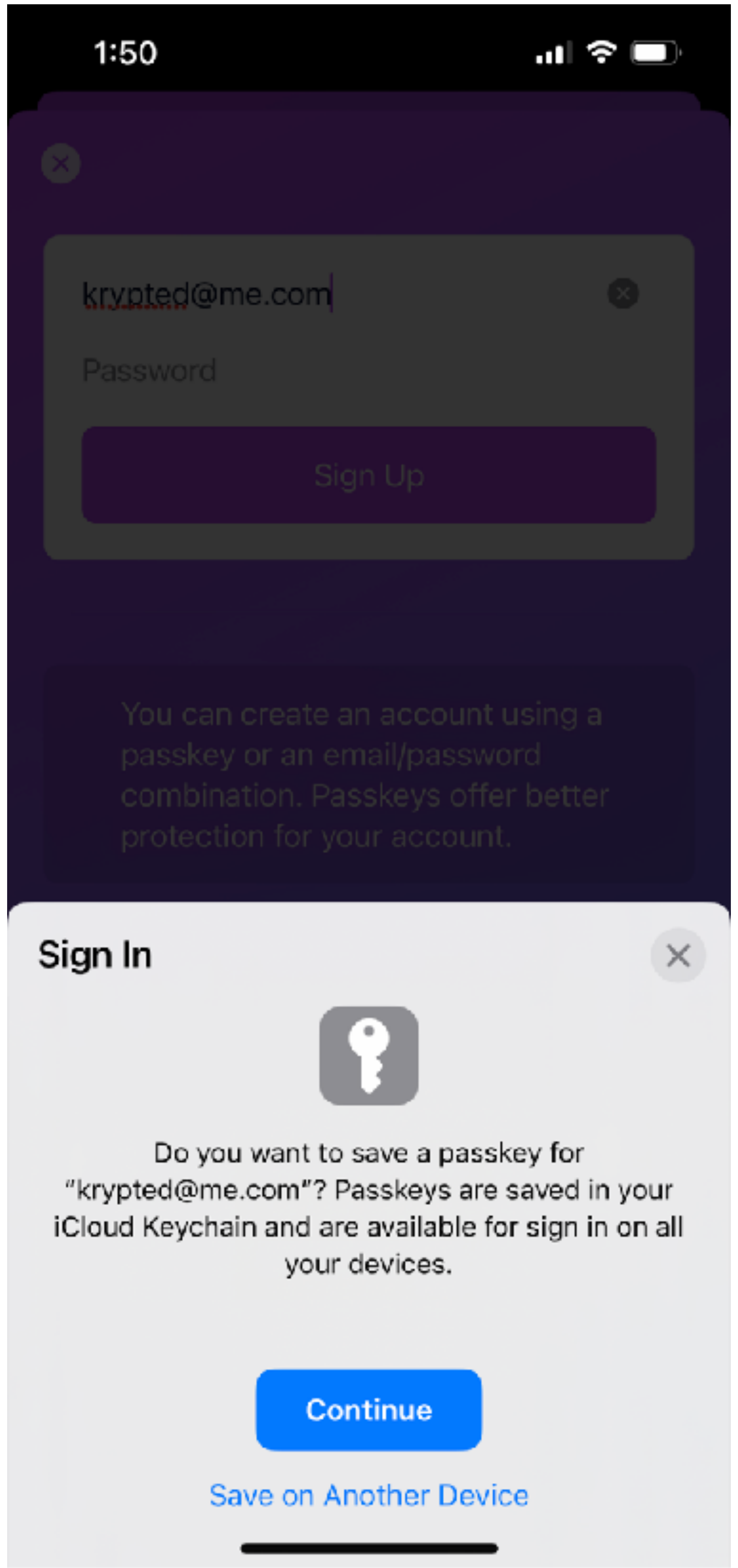


1:45

krypted@me.com

Password

You can create an account using a passkey or an email/password combination. Passkeys offer better protection for your account.



1:50

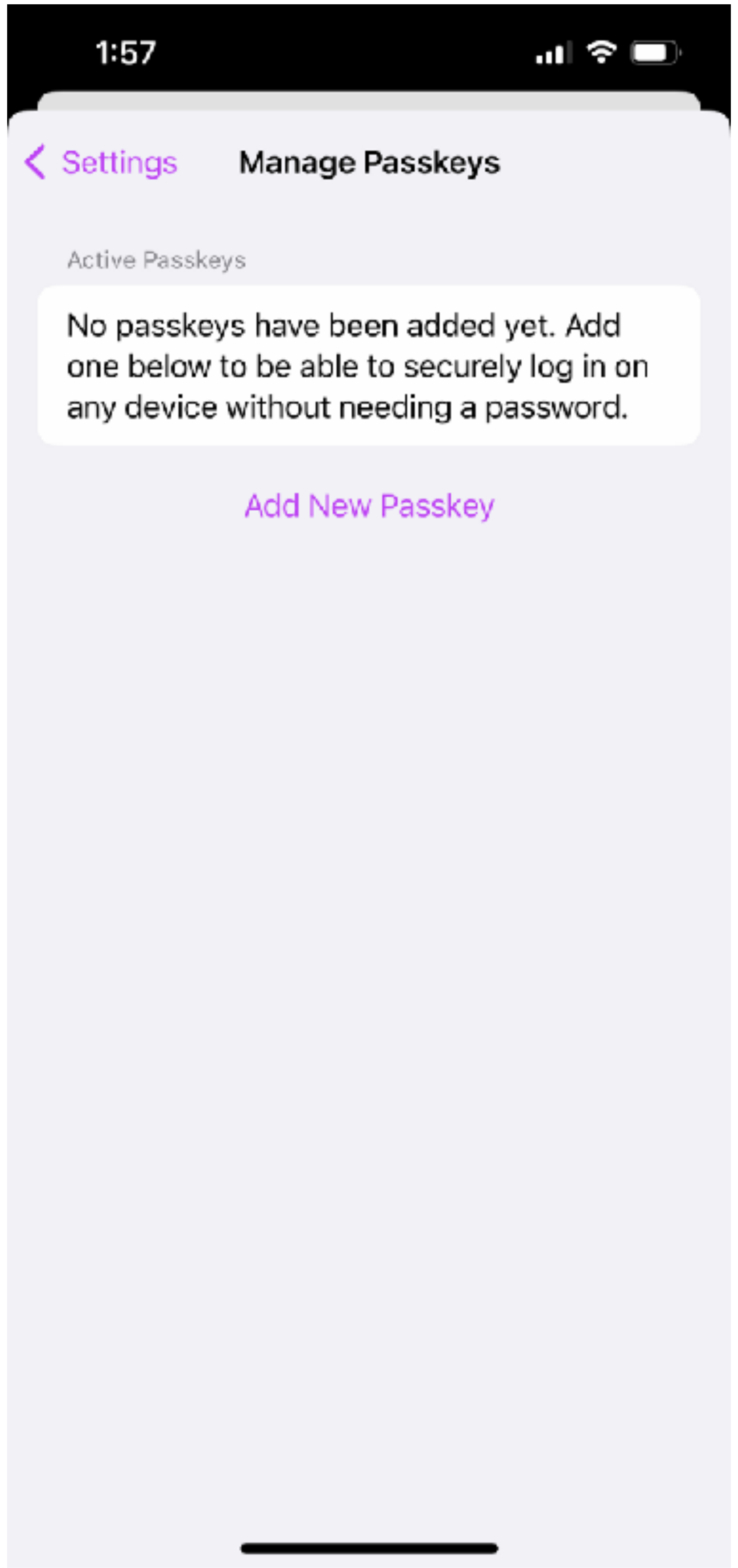
krypted@me.com

Password

You can create an account using a passkey or an email/password combination. Passkeys offer better protection for your account.

Sign In

Do you want to save a passkey for "krypted@me.com"? Passkeys are saved in your iCloud Keychain and are available for sign in on all your devices.



1:57

Manage Passkeys

Active Passkeys

No passkeys have been added yet. Add one below to be able to securely log in on any device without needing a password.

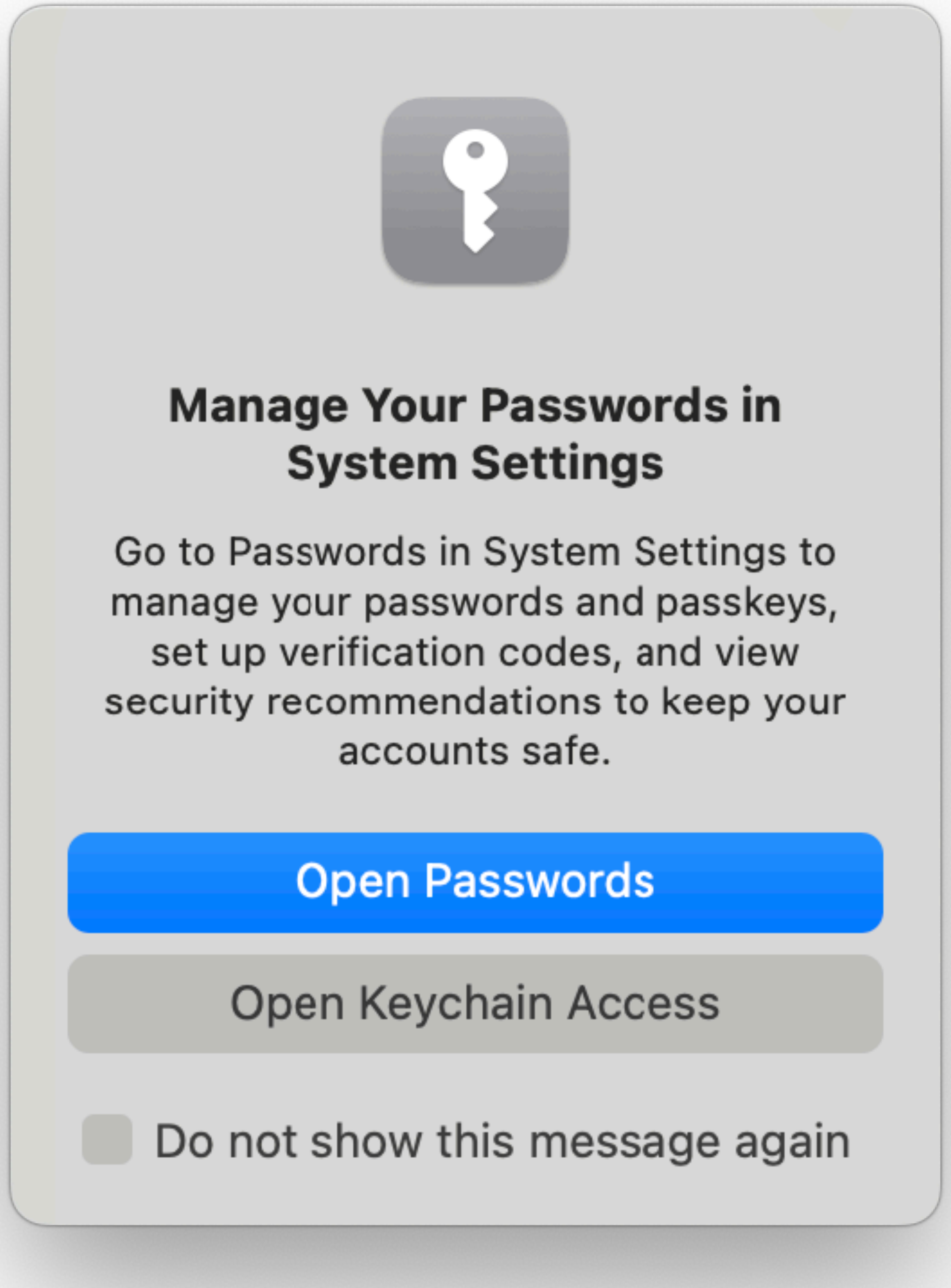
Illustrates again, a password AND a passkey

Joel’s PassStash

Simple Enough So Far

But We Can’t See Much In Keychain Access

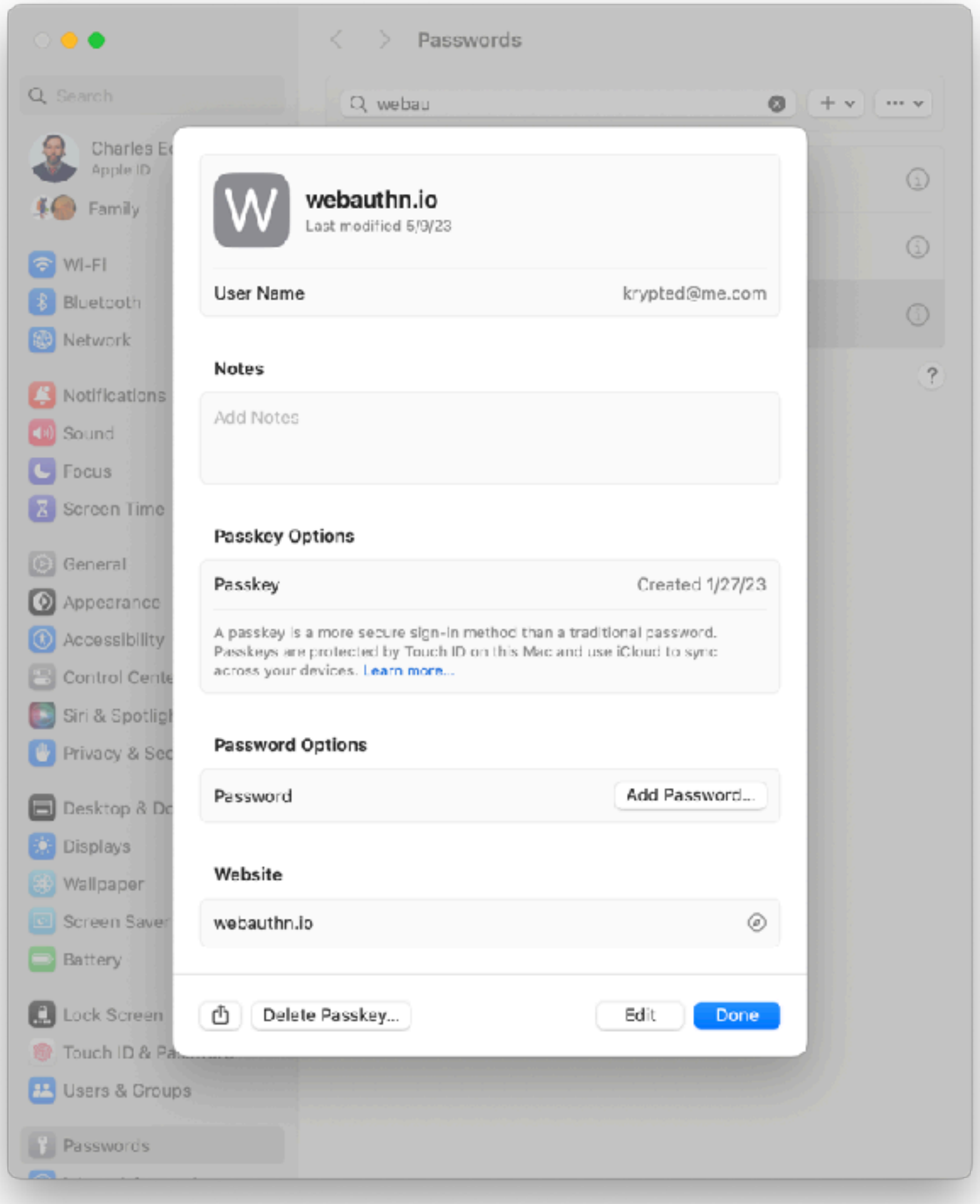
The Future of Keychain Access?



Manage Your Passwords in System Settings

Go to Passwords in System Settings to manage your passwords and passkeys, set up verification codes, and view security recommendations to keep your accounts safe.

In System Preferences



webauthn.io
Last modified 5/9/23

User Name: krypted@me.com

Notes

Add Notes

Passkey Options

Passkey: Created 1/27/23

A passkey is a more secure sign-in method than a traditional password. Passkeys are protected by Touch ID on this Mac and use iCloud to sync across your devices. Learn more...

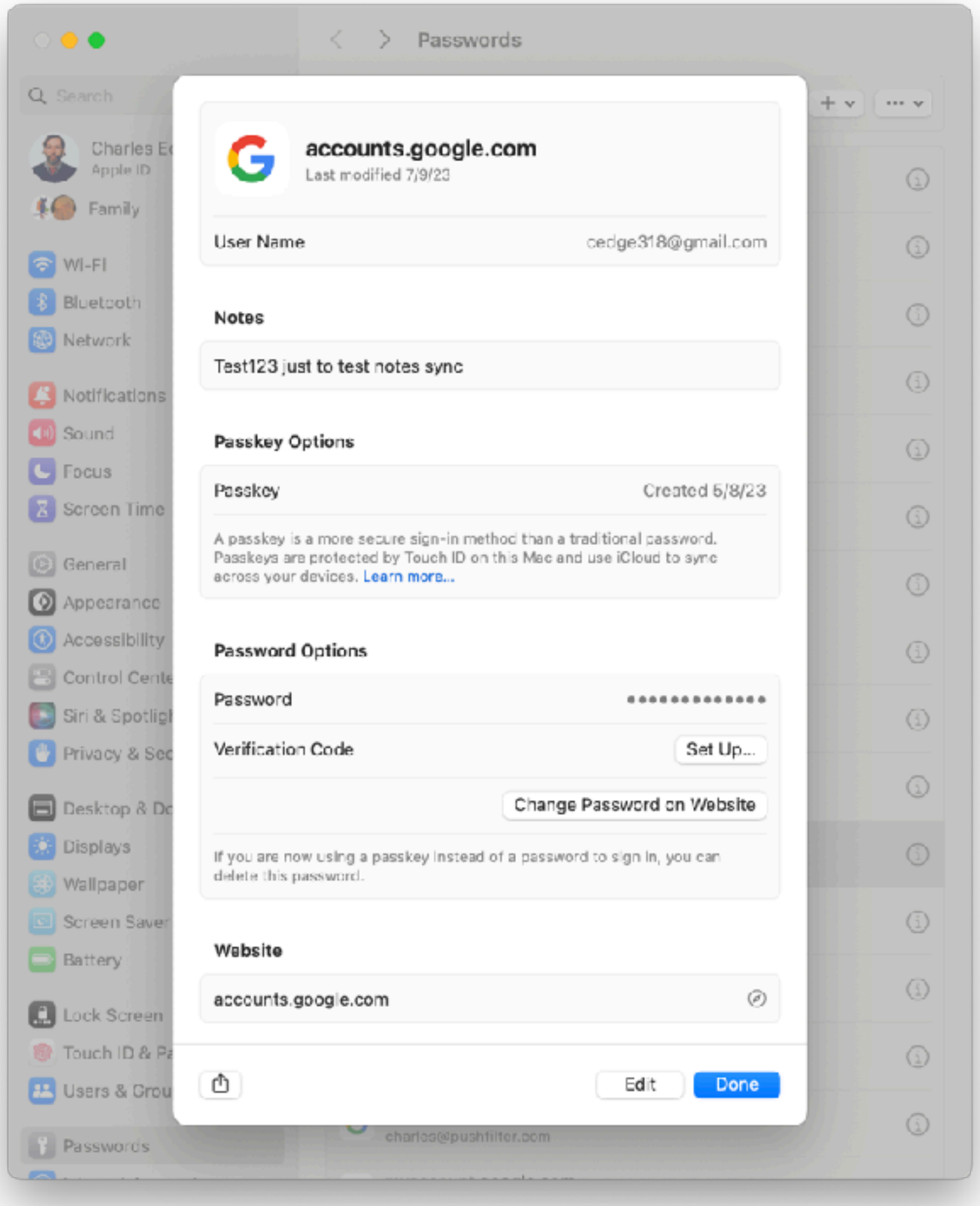
Password Options

Password: Add Password...

Website

webauthn.io

Delete Passkey... Edit Done



accounts.google.com
Last modified 7/9/23

User Name: cedge318@gmail.com

Notes

Test123 just to test notes sync

Passkey Options

Passkey: Created 6/8/23

A passkey is a more secure sign-in method than a traditional password. Passkeys are protected by Touch ID on this Mac and use iCloud to sync across your devices. Learn more...

Password Options

Password: •••••••••••••

Verification Code: Set Up...

Change Password on Website

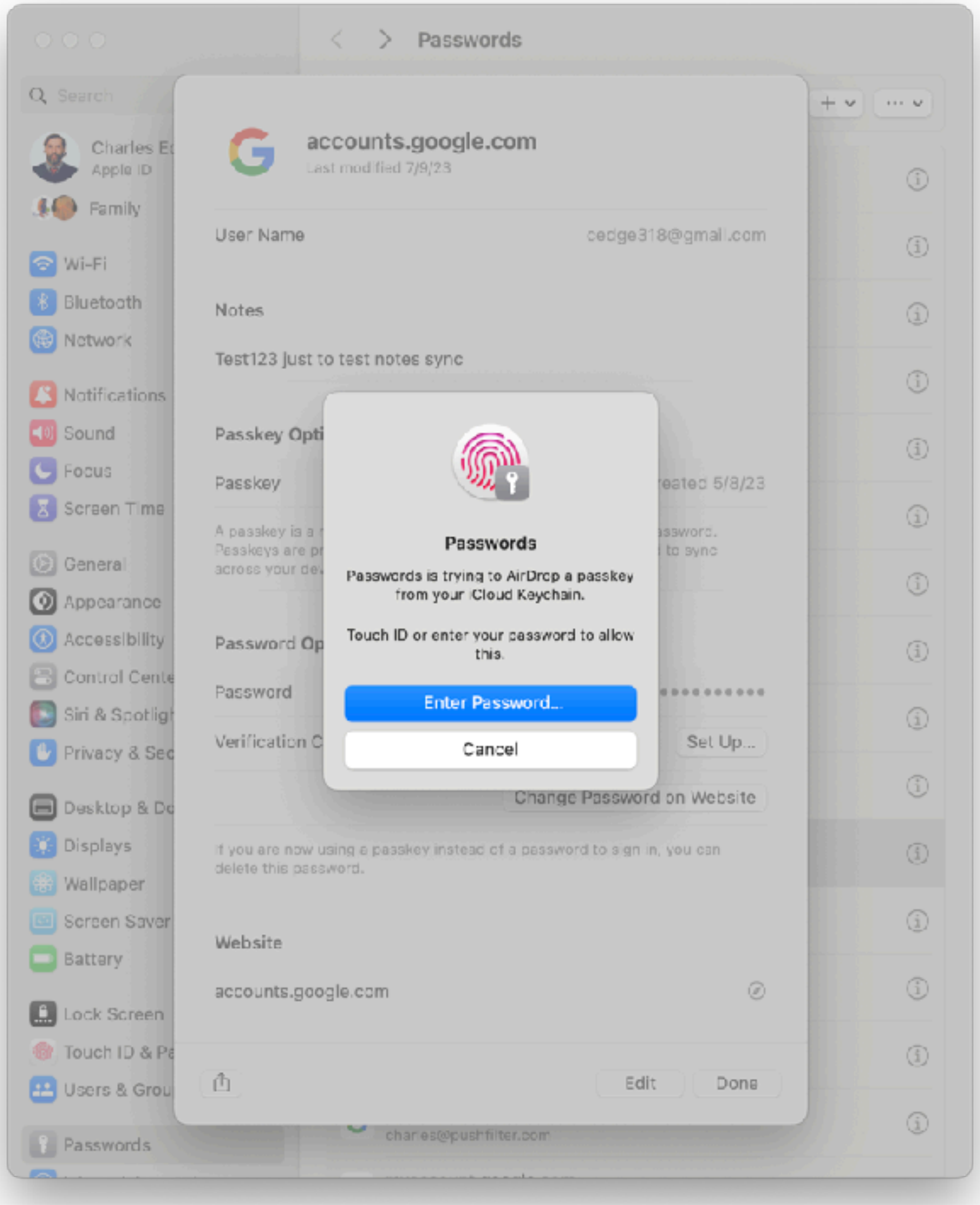
If you are now using a passkey instead of a password to sign in, you can delete this password.

Website

accounts.google.com

Edit Done

And You Can Share



Passwords

accounts.google.com

Last modified 7/9/23

User Name cedge318@gmail.com

Notes

Test123 Just to test notes sync

Passkey Opti

Passkey reated 5/8/23

A passkey is a … ssword. Passkeys are pr… to sync across your dev…

Password Op

Password ●●●●●●●●●●

Verification C

If you are now using a passkey instead of a password to sign in, you can delete this password.

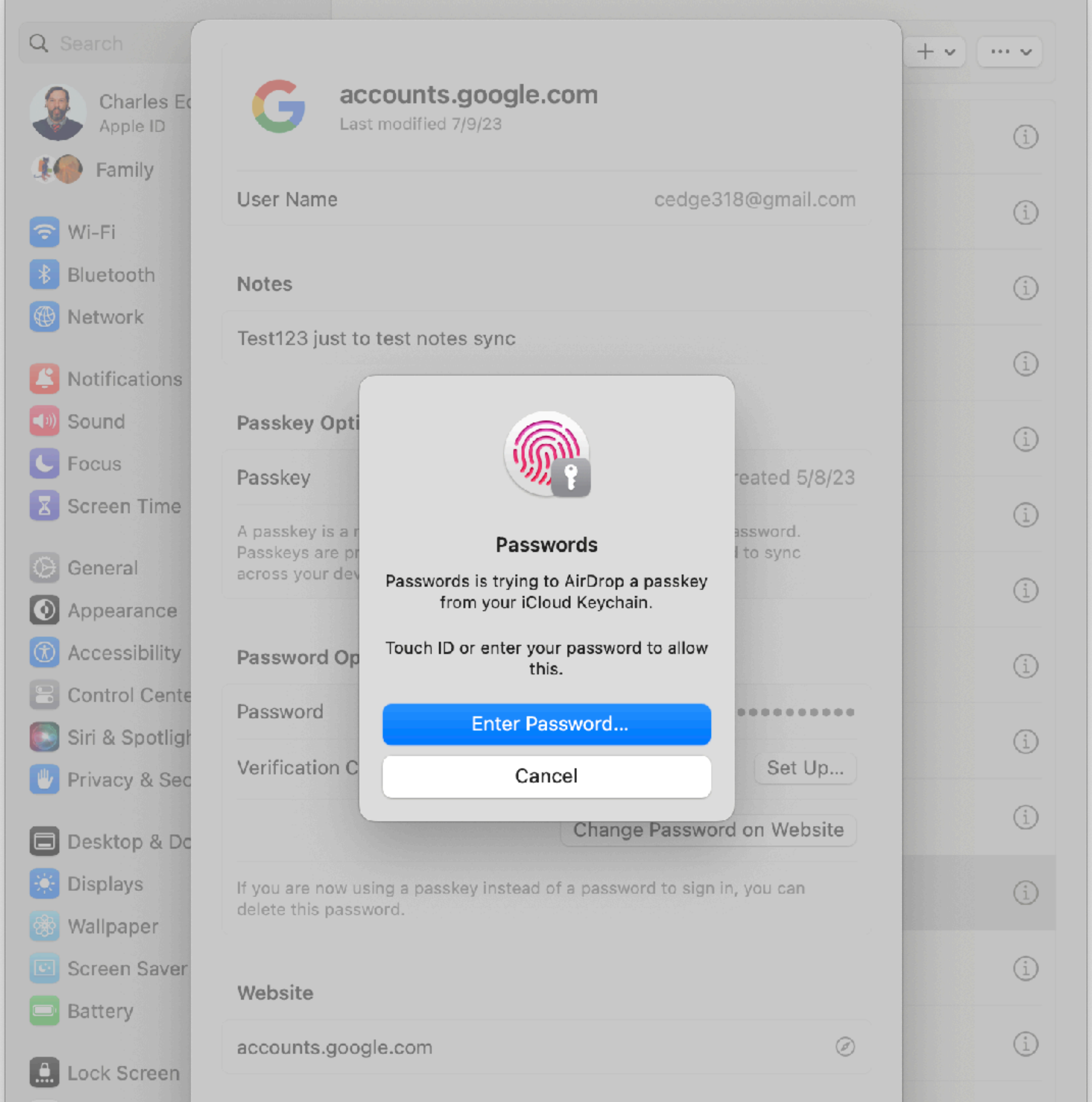
Website

accounts.google.com

Passwords

Passwords is trying to AirDrop a passkey from your iCloud Keychain.

Touch ID or enter your password to allow this.



accounts.google.com
Last modified 7/9/23

User Name cedge318@gmail.com

Notes

Test123 just to test notes sync

Passkey Opti

Passkey reated 5/8/23

A passkey is a r ssword.
Passkeys are pr l to sync
across your dev

Password Op

Password ●●●●●●●●●●●

Verification C Set Up...

Change Password on Website

If you are now using a passkey instead of a password to sign in, you can delete this password.

Website

accounts.google.com

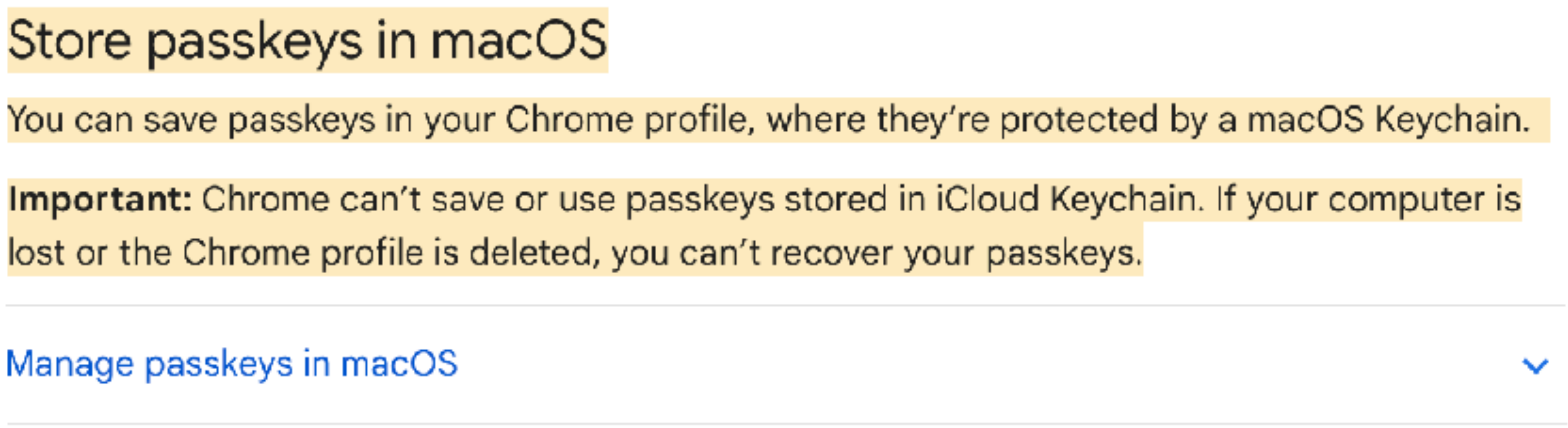
Passwords

Passwords is trying to AirDrop a passkey from your iCloud Keychain.

Touch ID or enter your password to allow this.

Passkeys in Chrome

- Passkeys are managed from Settings -> Autofill -> Manage Passkeys

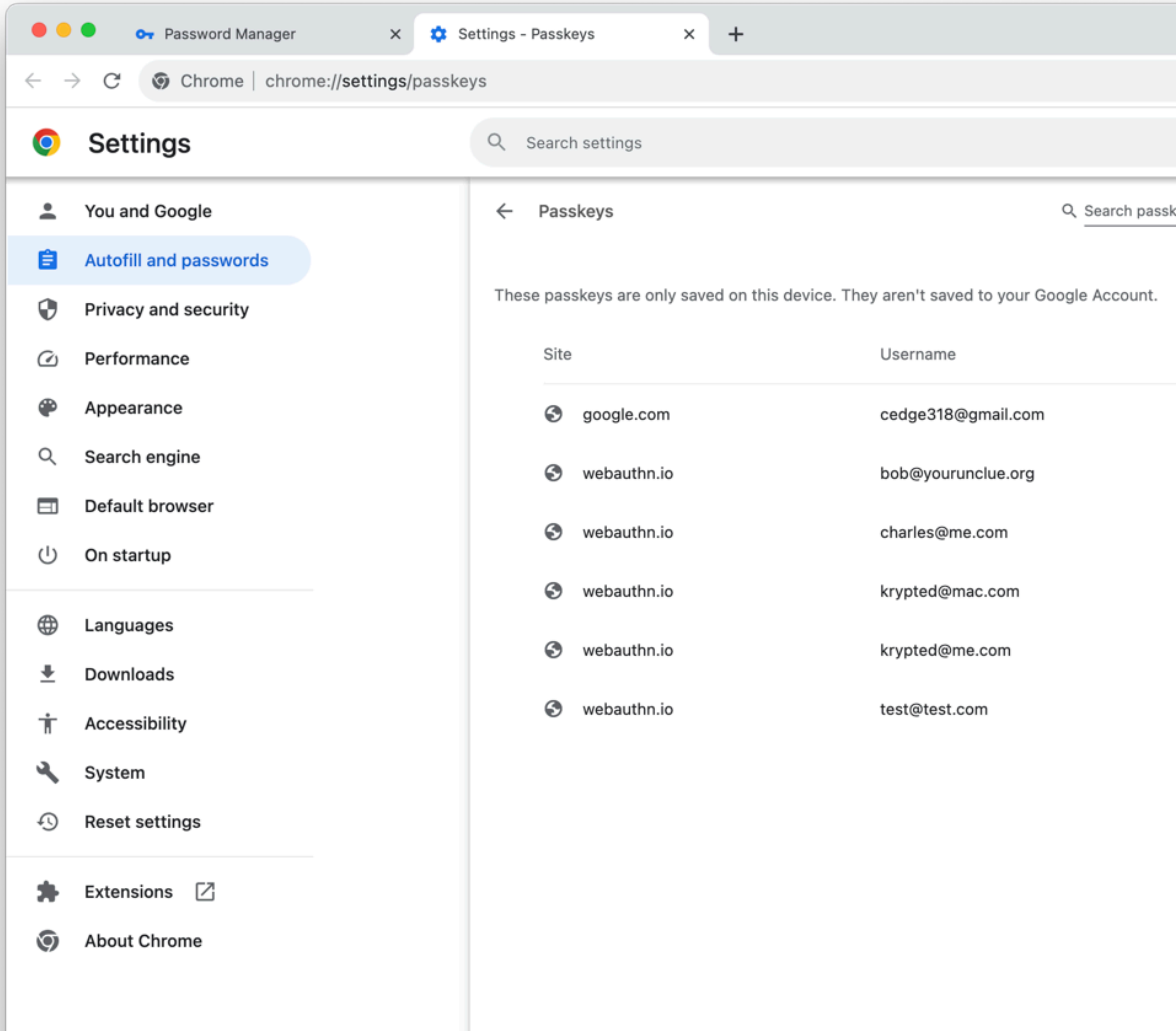


Store passkeys in macOS

You can save passkeys in your Chrome profile, where they're protected by a macOS Keychain.

Important: Chrome can't save or use passkeys stored in iCloud Keychain. If your computer is lost or the Chrome profile is deleted, you can't recover your passkeys.

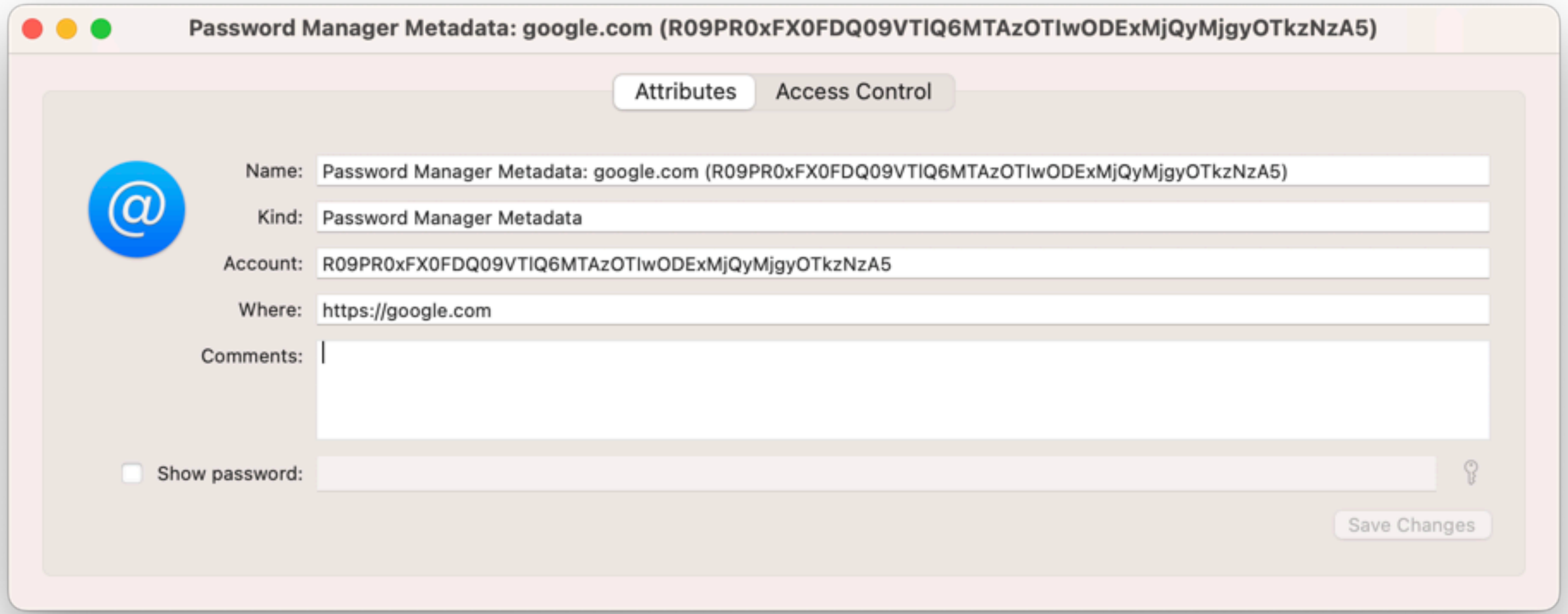
Manage passkeys in macOS



These passkeys are only saved on this device. They aren't saved to your Google Account.

Site	Username
google.com	cedge318@gmail.com
webauthn.io	bob@yourunclue.org
webauthn.io	charles@me.com
webauthn.io	krypted@mac.com
webauthn.io	krypted@me.com
webauthn.io	test@test.com

Now that it’s in Chrome



Password Manager Metadata: google.com (R09PR0xFX0FDQ09VTlQ6MTAzOTIwODExMjQyMjgyOTkzNzA5)

Name: Password Manager Metadata: google.com (R09PR0xFX0FDQ09VTlQ6MTAzOTIwODExMjQyMjgyOTkzNzA5)

Kind: Password Manager Metadata

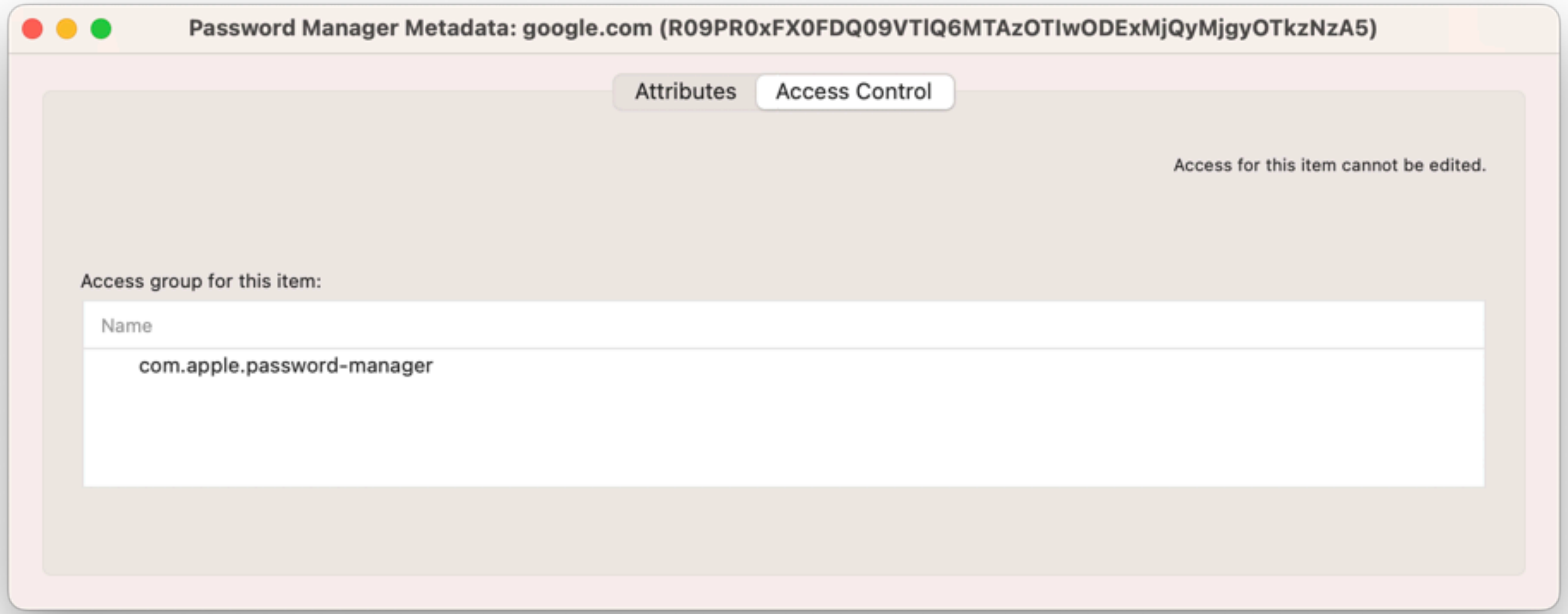
Account: R09PR0xFX0FDQ09VTlQ6MTAzOTIwODExMjQyMjgyOTkzNzA5

Where: https://google.com

Comments:

□ Show password:

But…



Password Manager Metadata: google.com (R09PR0xFX0FDQ09VTlQ6MTAzOTIwODExMjQyMjgyOTkzNzA5)

Access for this item cannot be edited.

Access group for this item:

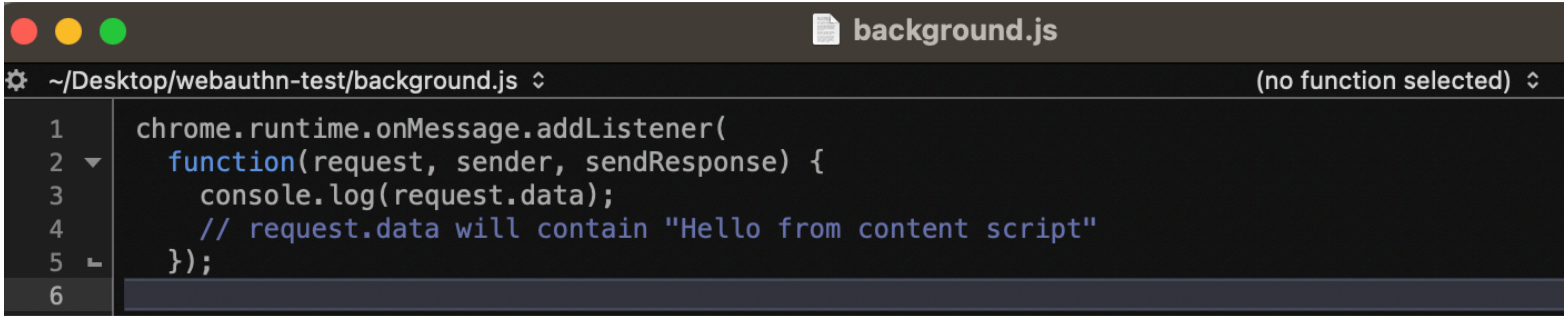
Name
com.apple.password-manager

Under The Hood

Navigator Endpoints

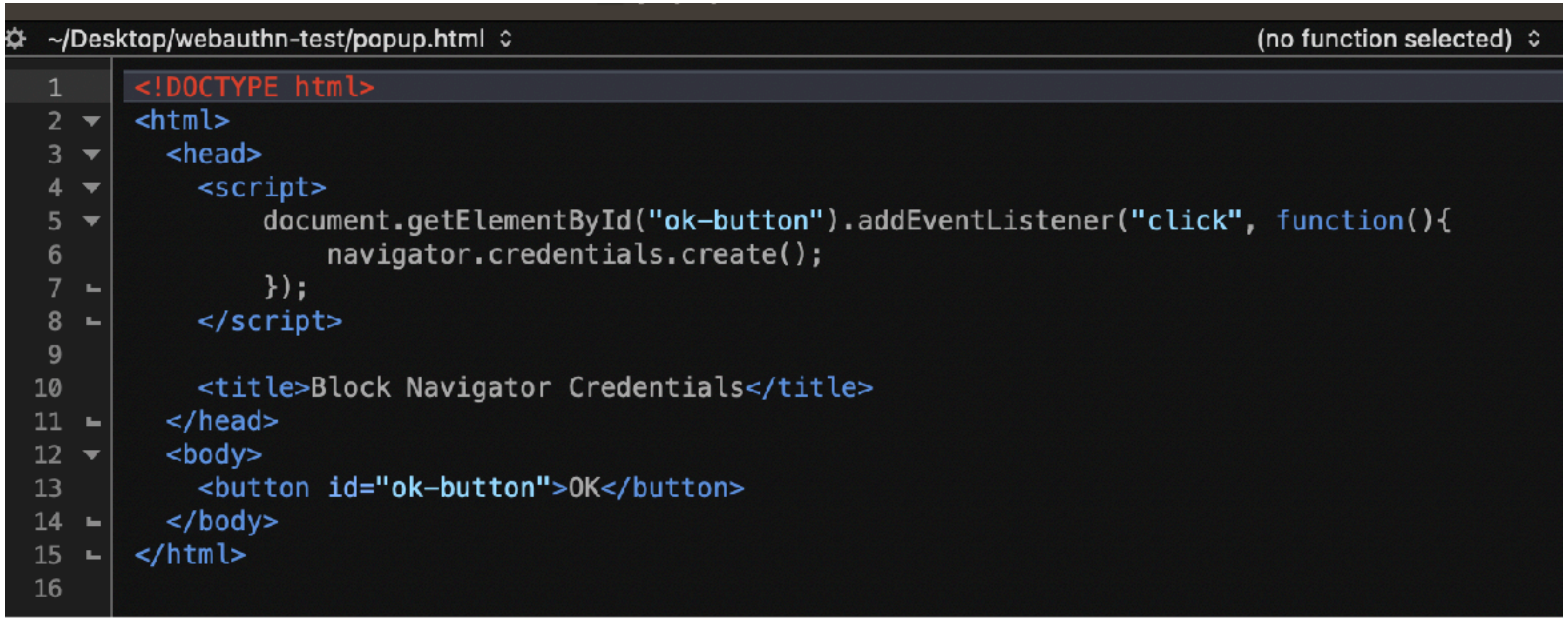
- Webauthn-ish, with some other options
- navigator.credentials.create: Creates the passkey https://w3c.github.io/webappsec-credential-management/#dom-credentialscontainer-create
- navigator.credentials.get: Gets the passkey https://w3c.github.io/webappsec-credential-management/#dom-credentialscontainer-get
- These are well documented, so…
- Let’s make a Chrome Extension

The Listener



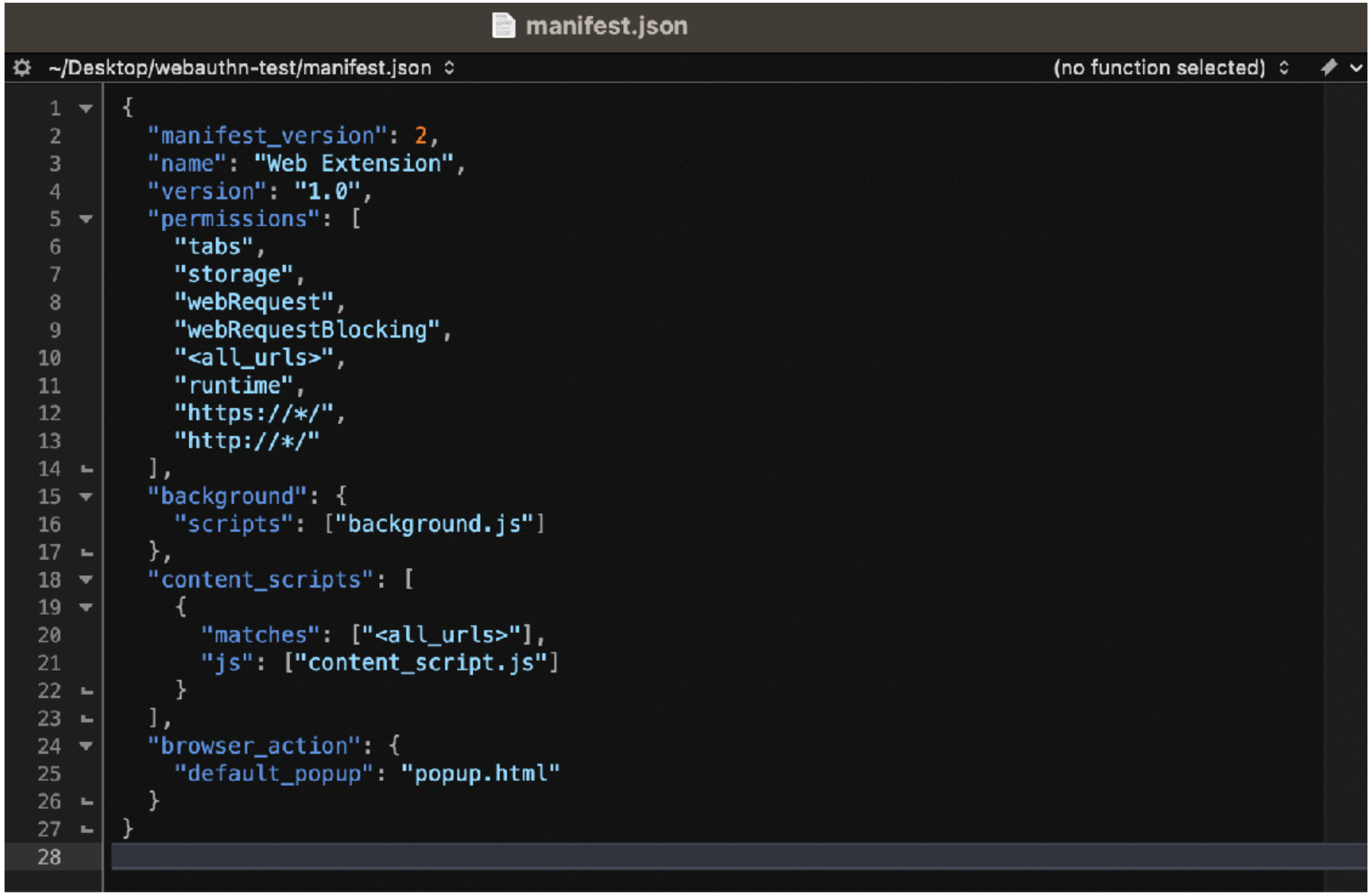
```
chrome.runtime.onMessage.addListener(
  function(request, sender, sendResponse) {
    console.log(request.data);
    // request.data will contain "Hello from content script"
  });
```

A Pop-up On navigator.credentials.create



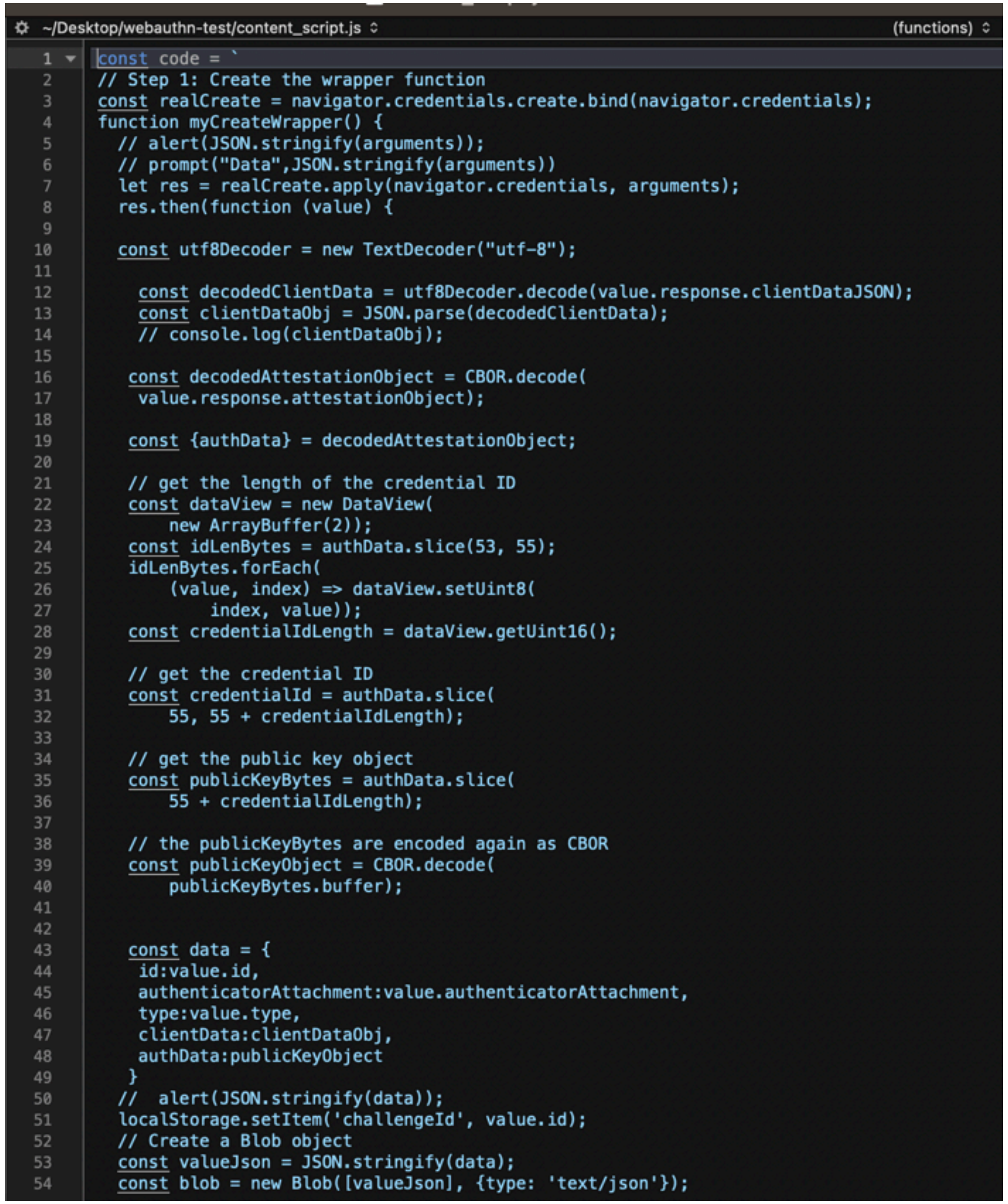
```
<!DOCTYPE html>
<html>
  <head>
    <script>
        document.getElementById("ok-button").addEventListener("click", function(){
            navigator.credentials.create();
        });
    </script>

    <title>Block Navigator Credentials</title>
  </head>
  <body>
    <button id="ok-button">OK</button>
  </body>
</html>

```

A Manifest That Includes “webRequest”



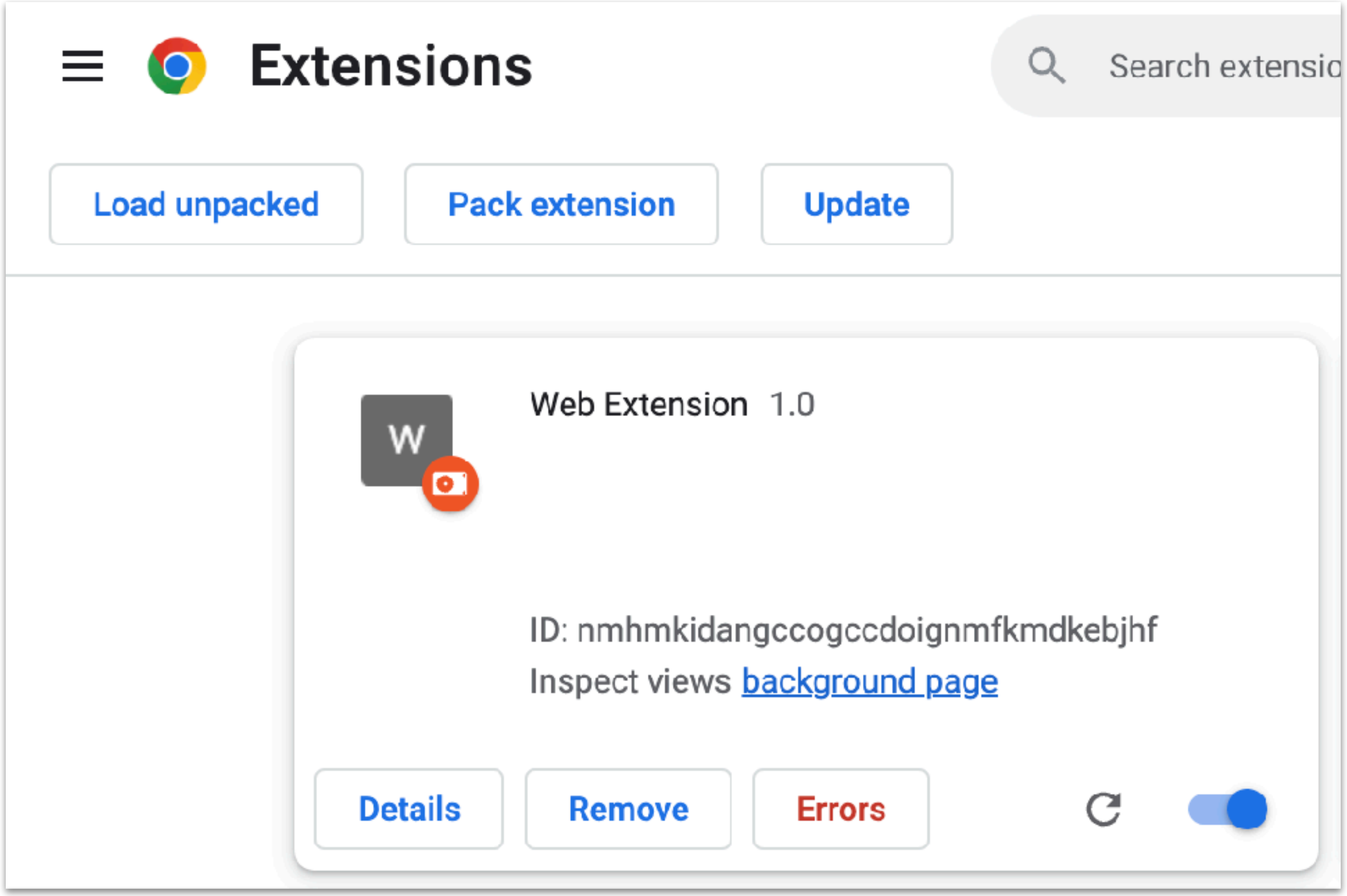
```
{
  "manifest_version": 2,
  "name": "Web Extension",
  "version": "1.0",
  "permissions": [
    "tabs",
    "storage",
    "webRequest",
    "webRequestBlocking",
    "<all_urls>",
    "runtime",
    "https://*/",
    "http://*/"
  ],
  "background": {
    "scripts": ["background.js"]
  },
  "content_scripts": [
    {
      "matches": ["<all_urls>"],
      "js": ["content_script.js"]
    }
  ],
  "browser_action": {
    "default_popup": "popup.html"
  }
}
```

And A Script



```javascript
const code = `
// Step 1: Create the wrapper function
const realCreate = navigator.credentials.create.bind(navigator.credentials);
function myCreateWrapper() {
  // alert(JSON.stringify(arguments));
  // prompt("Data",JSON.stringify(arguments))
  let res = realCreate.apply(navigator.credentials, arguments);
  res.then(function (value) {

  const utf8Decoder = new TextDecoder("utf-8");

    const decodedClientData = utf8Decoder.decode(value.response.clientDataJSON);
    const clientDataObj = JSON.parse(decodedClientData);
    // console.log(clientDataObj);

   const decodedAttestationObject = CBOR.decode(
    value.response.attestationObject);

   const {authData} = decodedAttestationObject;

   // get the length of the credential ID
   const dataView = new DataView(
       new ArrayBuffer(2));
   const idLenBytes = authData.slice(53, 55);
   idLenBytes.forEach(
       (value, index) => dataView.setUint8(
           index, value));
   const credentialIdLength = dataView.getUint16();

   // get the credential ID
   const credentialId = authData.slice(
       55, 55 + credentialIdLength);

   // get the public key object
   const publicKeyBytes = authData.slice(
       55 + credentialIdLength);

   // the publicKeyBytes are encoded again as CBOR
   const publicKeyObject = CBOR.decode(
       publicKeyBytes.buffer);


   const data = {
    id:value.id,
    authenticatorAttachment:value.authenticatorAttachment,
    type:value.type,
    clientData:clientDataObj,
    authData:publicKeyObject
   }
  //  alert(JSON.stringify(data));
  localStorage.setItem('challengeId', value.id);
  // Create a Blob object
  const valueJson = JSON.stringify(data);
  const blob = new Blob([valueJson], {type: 'text/json'});
```

Load The Extension

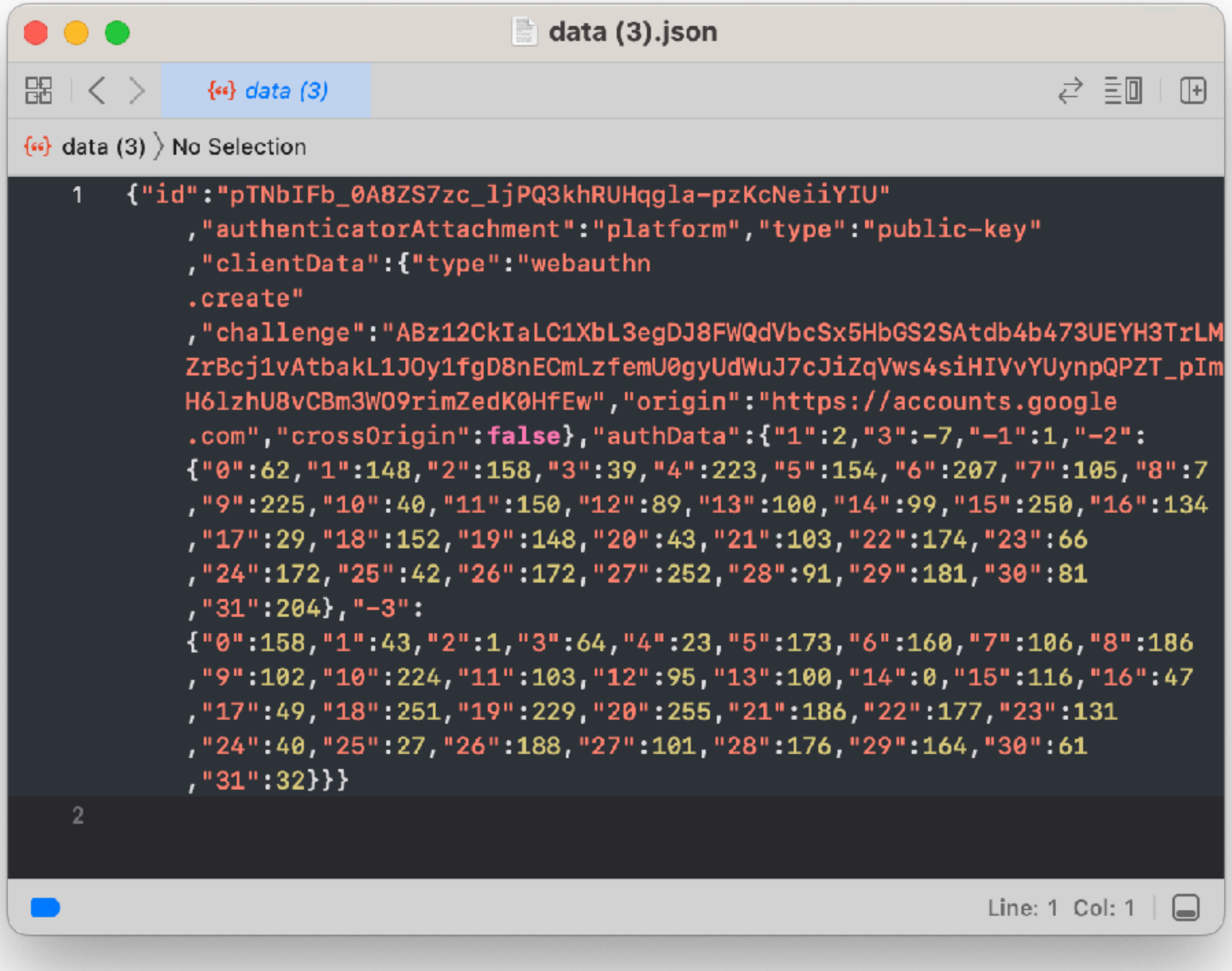


Web Extension 1.0

ID: nmhmkidangccogccdoignmfkmdkebjhf

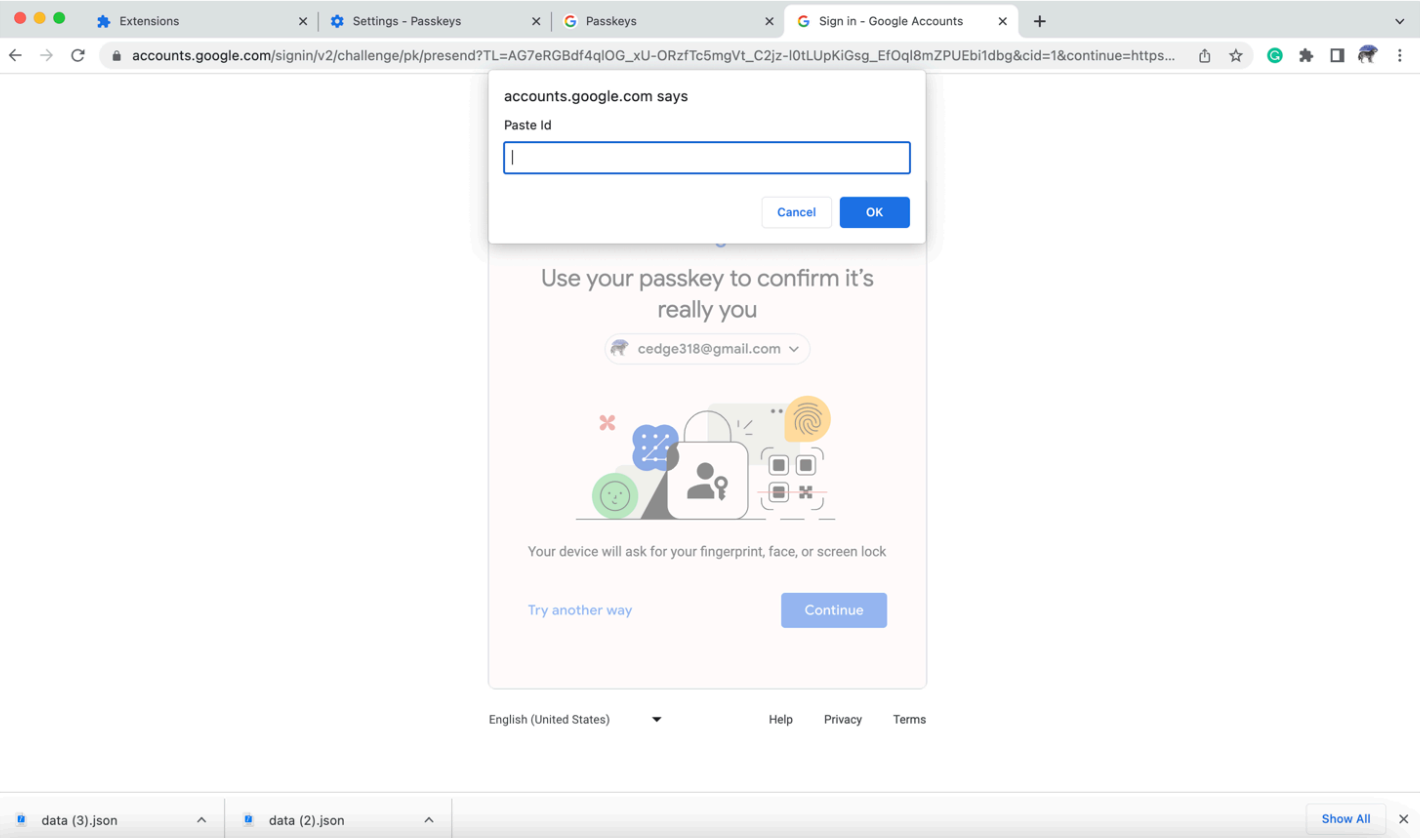
Inspect views background page

Make The Passkey Again



```
{"id":"pTNbIFb_0A8ZS7zc_ljPQ3khRUHqgla-pzKcNeiiYIU"
    ,"authenticatorAttachment":"platform","type":"public-key"
    ,"clientData":{"type":"webauthn
    .create"
    ,"challenge":"ABz12CkIaLC1XbL3egDJ8FWQdVbcSx5HbGS2SAtdb4b473UEYH3TrLM
    ZrBcj1vAtbakL1JOy1fgD8nECmLzfemU0gyUdWuJ7cJiZqVws4siHIVvYUynpQPZT_pIm
    H6lzhU8vCBm3WO9rimZedK0HfEw","origin":"https://accounts.google
    .com","crossOrigin":false},"authData":{"1":2,"3":-7,"-1":1,"-2":
    {"0":62,"1":148,"2":158,"3":39,"4":223,"5":154,"6":207,"7":105,"8":7
    ,"9":225,"10":40,"11":150,"12":89,"13":100,"14":99,"15":250,"16":134
    ,"17":29,"18":152,"19":148,"20":43,"21":103,"22":174,"23":66
    ,"24":172,"25":42,"26":172,"27":252,"28":91,"29":181,"30":81
    ,"31":204},"-3":
    {"0":158,"1":43,"2":1,"3":64,"4":23,"5":173,"6":160,"7":106,"8":186
    ,"9":102,"10":224,"11":103,"12":95,"13":100,"14":0,"15":116,"16":47
    ,"17":49,"18":251,"19":229,"20":255,"21":186,"22":177,"23":131
    ,"24":40,"25":27,"26":188,"27":101,"28":176,"29":164,"30":61
    ,"31":32}}}
```

Now Let’s Allow For Arbitrary Passkey Entry



accounts.google.com/signin/v2/challenge/pk/present?TL=AG7eRGBdf4qlOG_xU-ORzfTc5mgVt_C2jz-l0tLUpKiGsg_EfOql8mZPUEbi1dbg&cid=1&continue=https...

accounts.google.com says

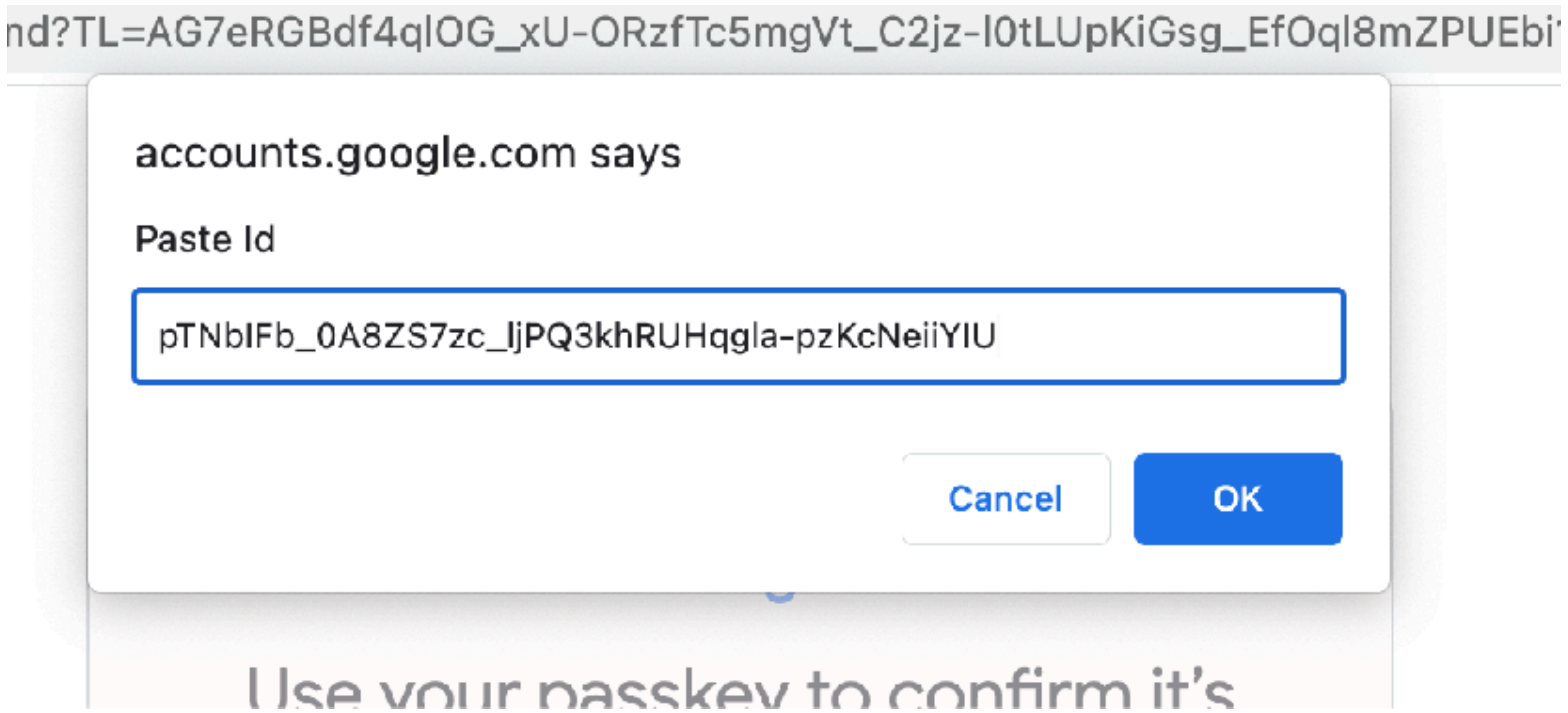
Paste Id

Use your passkey to confirm it’s really you

cedge318@gmail.com

Your device will ask for your fingerprint, face, or screen lock

Paste In The Passkey From The .json



nd?TL=AG7eRGBdf4qlOG_xU-ORzfTc5mgVt_C2jz-l0tLUpKiGsg_EfOql8mZPUEbi

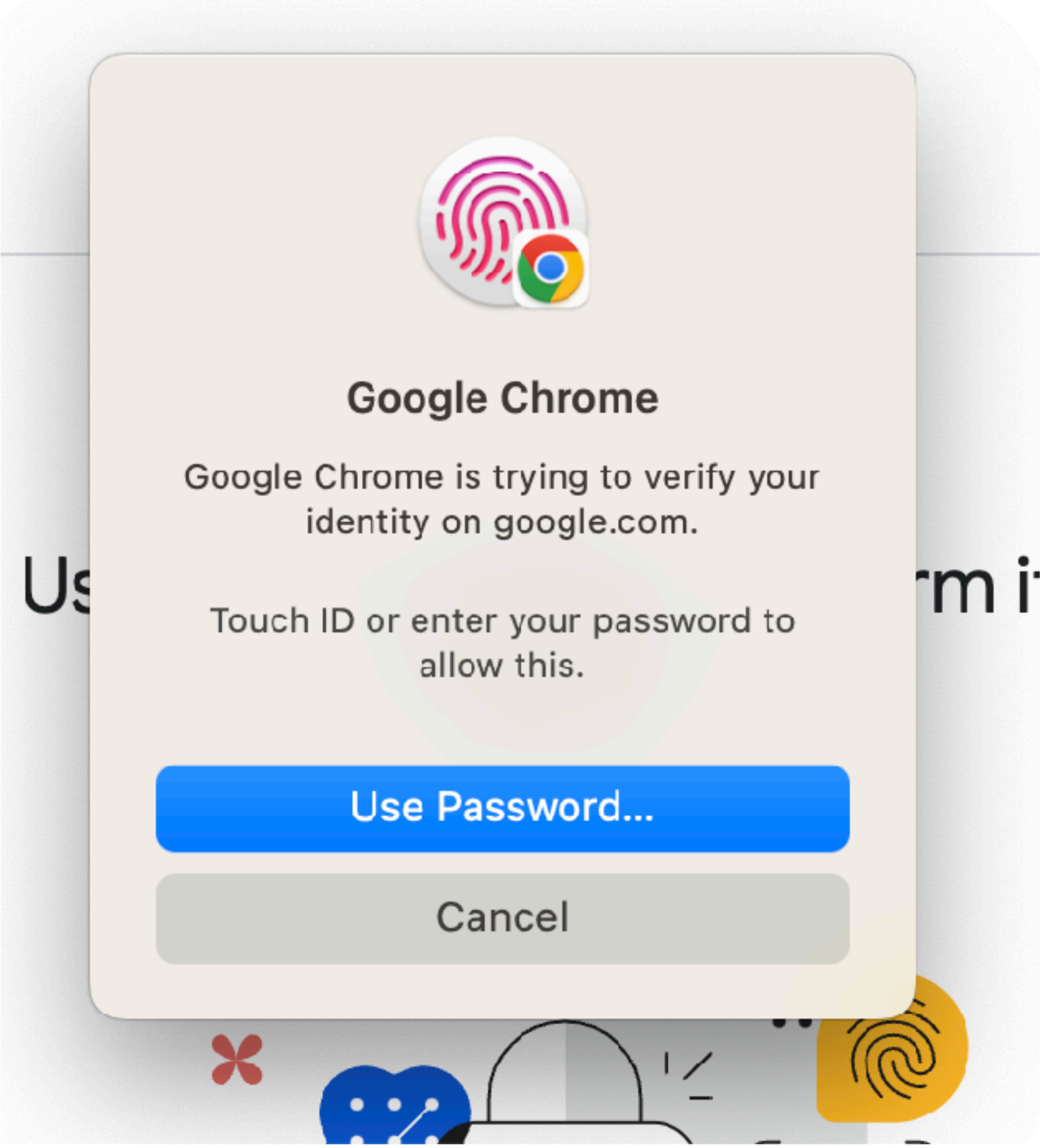
accounts.google.com says

Paste Id

pTNbIFb_0A8ZS7zc_ljPQ3khRUHqgla-pzKcNeiiYIU

Use your passkey to confirm it's

Give Fingerprint



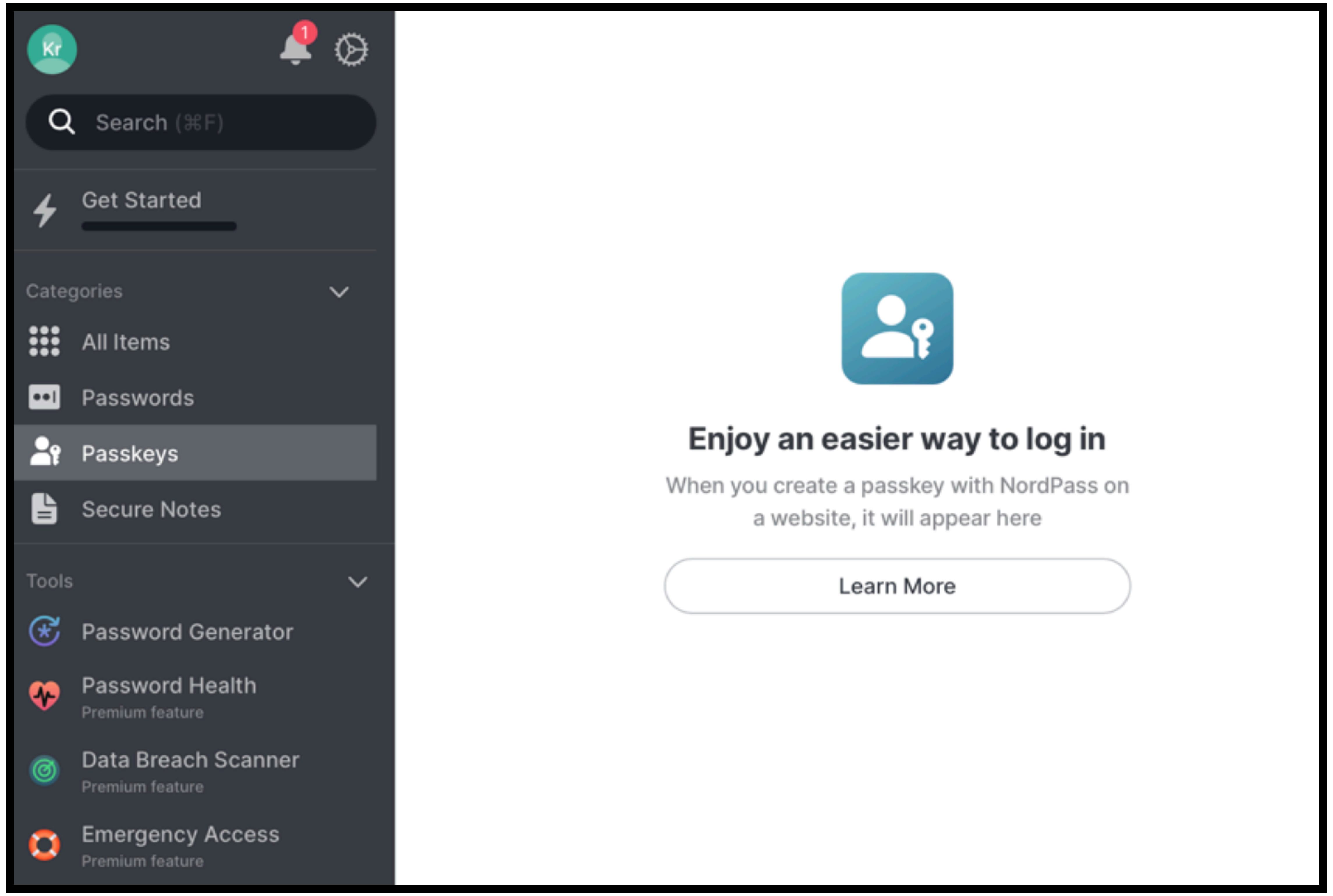
Google Chrome

Google Chrome is trying to verify your identity on google.com.

Touch ID or enter your password to allow this.

What’s Cool About Browser Extensions…

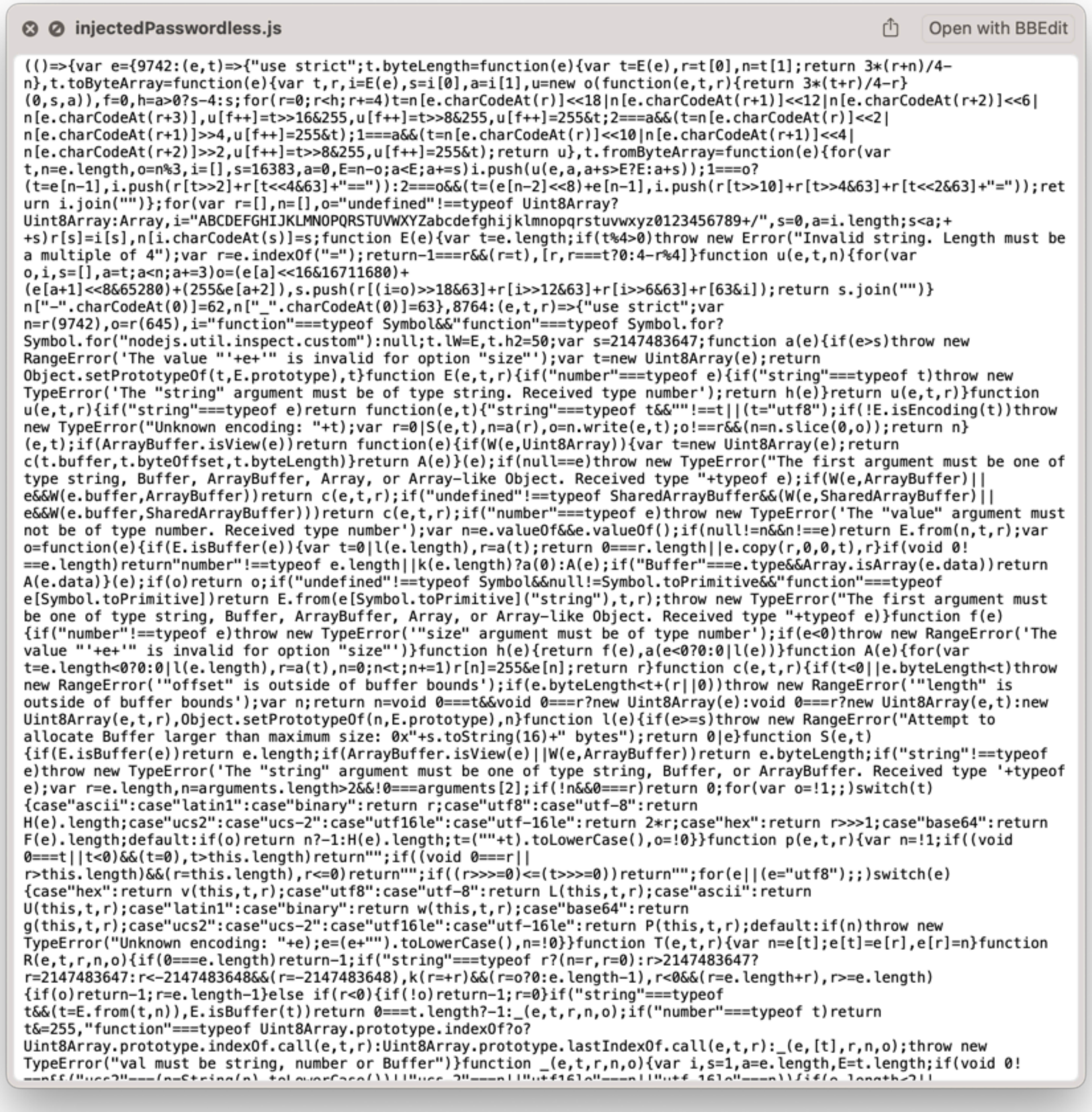
Some Password Managers Use Them



Enjoy an easier way to log in

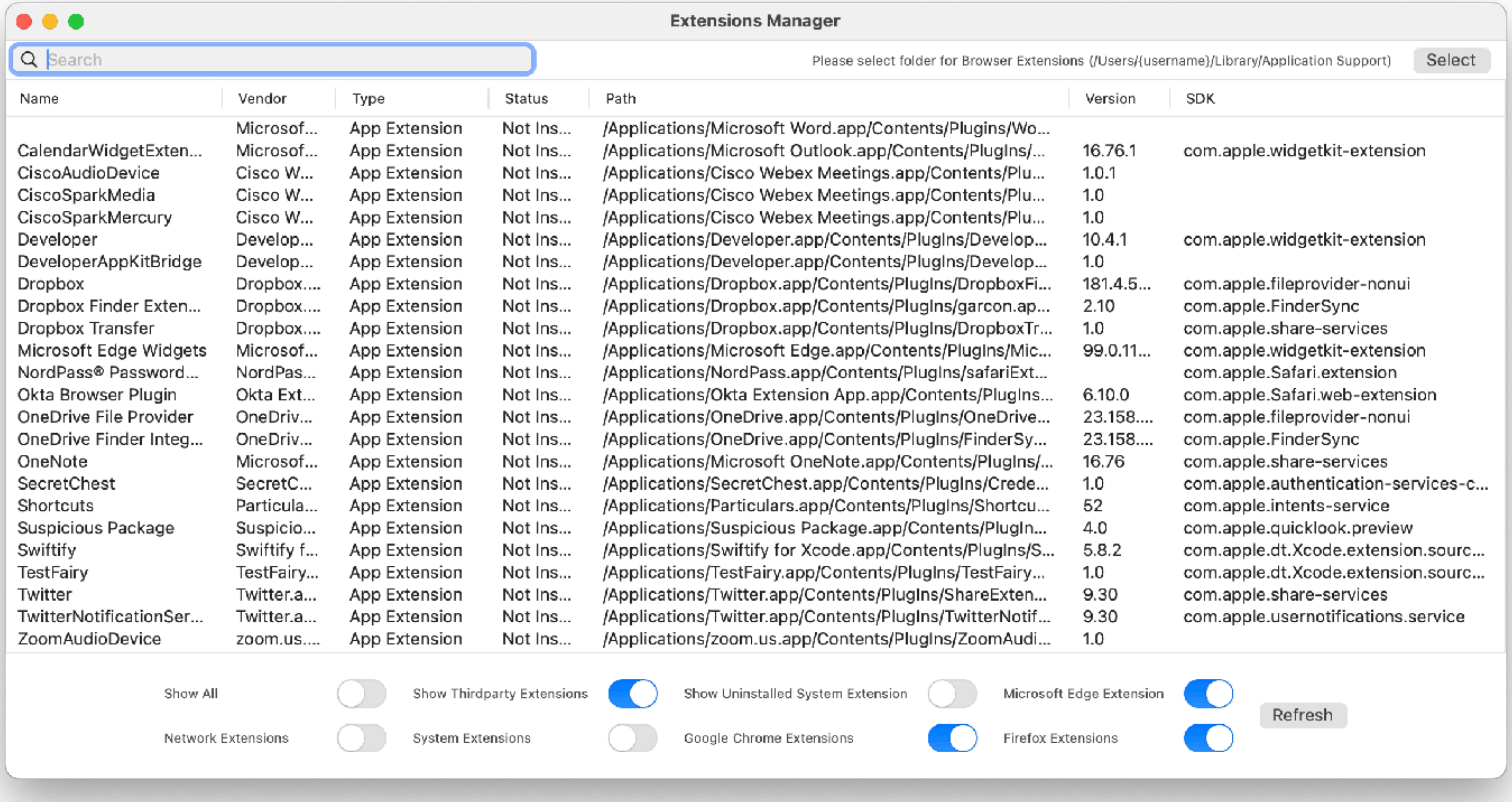
When you create a passkey with NordPass on a website, it will appear here

See How Others Handle Them



```
(()=>{var e={9742:(e,t)=>{"use strict";t.byteLength=function(e){var t=E(e),r=t[0],n=t[1];return 3*(r+n)/4-
n},t.toByteArray=function(e){var t,r,i=E(e),s=i[0],a=i[1],u=new o(function(e,t,r){return 3*(t+r)/4-r}
(0,s,a)),f=0,h=a>0?s-4:s;for(r=0;r<h;r+=4)t=n[e.charCodeAt(r)]<<18|n[e.charCodeAt(r+1)]<<12|n[e.charCodeAt(r+2)]<<6|
n[e.charCodeAt(r+3)],u[f++]=t>>16&255,u[f++]=t>>8&255,u[f++]=255&t;2===a&&(t=n[e.charCodeAt(r)]<<2|
n[e.charCodeAt(r+1)]>>4,u[f++]=255&t);1===a&&(t=n[e.charCodeAt(r)]<<10|n[e.charCodeAt(r+1)]<<4|
n[e.charCodeAt(r+2)]>>2,u[f++]=t>>8&255,u[f++]=255&t);return u},t.fromByteArray=function(e){for(var
t,n=e.length,o=n%3,i=[],s=16383,a=0,E=n-o;a<E;a+=s)i.push(u(e,a,a+s>E?E:a+s));1===o?
(t=e[n-1],i.push(r[t>>2]+r[t<<4&63]+"==")):2===o&&(t=(e[n-2]<<8)+e[n-1],i.push(r[t>>10]+r[t>>4&63]+r[t<<2&63]+"="));ret
urn i.join("")};for(var r=[],n=[],o="undefined"!==typeof Uint8Array?
Uint8Array:Array,i="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/",s=0,a=i.length;s<a;+
+s)r[s]=i[s],n[i.charCodeAt(s)]=s;function E(e){var t=e.length;if(t%4>0)throw new Error("Invalid string. Length must be
a multiple of 4");var r=e.indexOf("=");return-1===r&&(r=t),[r,r===t?0:4-r%4]}function u(e,t,n){for(var
o,i,s=[],a=t;a<n;a+=3)o=(e[a]<<16&16711680)+
(e[a+1]<<8&65280)+(255&e[a+2]),s.push(r[(i=o)>>18&63]+r[i>>12&63]+r[i>>6&63]+r[63&i]);return s.join("")}
n["-".charCodeAt(0)]=62,n["_".charCodeAt(0)]=63},8764:(e,t,r)=>{"use strict";var
n=r(9742),o=r(645),i="function"===typeof Symbol&&"function"===typeof Symbol.for?
Symbol.for("nodejs.util.inspect.custom"):null;t.lW=E,t.h2=50;var s=2147483647;function a(e){if(e>s)throw new
RangeError('The value "'+e+'" is invalid for option "size"');var t=new Uint8Array(e);return
Object.setPrototypeOf(t,E.prototype),t}function E(e,t,r){if("number"===typeof e){if("string"===typeof t)throw new
TypeError('The "string" argument must be of type string. Received type number');return h(e)}return u(e,t,r)}function
u(e,t,r){if("string"===typeof e)return function(e,t){"string"===typeof t&&""!==t||(t="utf8");if(!E.isEncoding(t))throw
new TypeError("Unknown encoding: "+t);var r=0|S(e,t),n=a(r),o=n.write(e,t);o!==r&&(n=n.slice(0,o));return n}
(e,t);if(ArrayBuffer.isView(e))return function(e){if(W(e,Uint8Array)){var t=new Uint8Array(e);return
c(t.buffer,t.byteOffset,t.byteLength)}return A(e)}(e);if(null==e)throw new TypeError("The first argument must be one of
type string, Buffer, ArrayBuffer, Array, or Array-like Object. Received type "+typeof e);if(W(e,ArrayBuffer)||
e&&W(e.buffer,ArrayBuffer))return c(e,t,r);if("undefined"!==typeof SharedArrayBuffer&&(W(e,SharedArrayBuffer)||
e&&W(e.buffer,SharedArrayBuffer)))return c(e,t,r);if("number"===typeof e)throw new TypeError('The "value" argument must
not be of type number. Received type number');var n=e.valueOf&&e.valueOf();if(null!=n&&n!==e)return E.from(n,t,r);var
o=function(e){if(E.isBuffer(e)){var t=0|l(e.length),r=a(t);return 0===r.length||e.copy(r,0,0,t),r}if(void 0!
==e.length)return"number"!==typeof e.length||k(e.length)?a(0):A(e);if("Buffer"===e.type&&Array.isArray(e.data))return
A(e.data)}(e);if(o)return o;if("undefined"!==typeof Symbol&&null!=Symbol.toPrimitive&&"function"===typeof
e[Symbol.toPrimitive])return E.from(e[Symbol.toPrimitive]("string"),t,r);throw new TypeError("The first argument must
be one of type string, Buffer, ArrayBuffer, Array, or Array-like Object. Received type "+typeof e)}function f(e)
{if("number"!==typeof e)throw new TypeError('"size" argument must be of type number');if(e<0)throw new RangeError('The
value "'+e+'" is invalid for option "size"')}function h(e){return f(e),a(e<0?0:0|l(e))}function A(e){for(var
t=e.length<0?0:0|l(e.length),r=a(t),n=0;n<t;n+=1)r[n]=255&e[n];return r}function c(e,t,r){if(t<0||e.byteLength<t)throw
new RangeError('"offset" is outside of buffer bounds');if(e.byteLength<t+(r||0))throw new RangeError('"length" is
outside of buffer bounds');var n;return n=void 0===t&&void 0===r?new Uint8Array(e):void 0===r?new Uint8Array(e,t):new
Uint8Array(e,t,r),Object.setPrototypeOf(n,E.prototype),n}function l(e){if(e>=s)throw new RangeError("Attempt to
allocate Buffer larger than maximum size: 0x"+s.toString(16)+" bytes");return 0|e}function S(e,t)
{if(E.isBuffer(e))return e.length;if(ArrayBuffer.isView(e)||W(e,ArrayBuffer))return e.byteLength;if("string"!==typeof
e)throw new TypeError('The "string" argument must be one of type string, Buffer, or ArrayBuffer. Received type '+typeof
e);var r=e.length,n=arguments.length>2&&!0===arguments[2];if(!n&&0===r)return 0;for(var o=!1;;)switch(t)
{case"ascii":case"latin1":case"binary":return r;case"utf8":case"utf-8":return
H(e).length;case"ucs2":case"ucs-2":case"utf16le":case"utf-16le":return 2*r;case"hex":return r>>>1;case"base64":return
F(e).length;default:if(o)return n?-1:H(e).length;t=(""+t).toLowerCase(),o=!0}}function p(e,t,r){var n=!1;if((void
0===t||t<0)&&(t=0),t>this.length)return"";if((void 0===r||
r>this.length)&&(r=this.length),r<=0)return"";if((r>>>=0)<=(t>>>=0))return"";for(e||(e="utf8");;)switch(e)
{case"hex":return v(this,t,r);case"utf8":case"utf-8":return L(this,t,r);case"ascii":return
U(this,t,r);case"latin1":case"binary":return w(this,t,r);case"base64":return
g(this,t,r);case"ucs2":case"ucs-2":case"utf16le":case"utf-16le":return P(this,t,r);default:if(n)throw new
TypeError("Unknown encoding: "+e);e=(e+"").toLowerCase(),n=!0}}function T(e,t,r){var n=e[t];e[t]=e[r],e[r]=n}function
R(e,t,r,n,o){if(0===e.length)return-1;if("string"===typeof r?(n=r,r=0):r>2147483647?
r=2147483647:r<-2147483648&&(r=-2147483648),k(r=+r)&&(r=o?0:e.length-1),r<0&&(r=e.length+r),r>=e.length)
{if(o)return-1;r=e.length-1}else if(r<0){if(!o)return-1;r=0}if("string"===typeof
t&&(t=E.from(t,n)),E.isBuffer(t))return 0===t.length?-1:_(e,t,r,n,o);if("number"===typeof t)return
t&=255,"function"===typeof Uint8Array.prototype.indexOf?o?
Uint8Array.prototype.indexOf.call(e,t,r):Uint8Array.prototype.lastIndexOf.call(e,t,r):_(e,[t],r,n,o);throw new
TypeError("val must be string, number or Buffer")}function _(e,t,r,n,o){var i,s=1,a=e.length,E=t.length;if(void 0!
==n&&("ucs2"===(n=String(n).toLowerCase())||"ucs-2"===n||"utf16le"===n||"utf-16le"===n)){if(e.length<2||
```

See them all



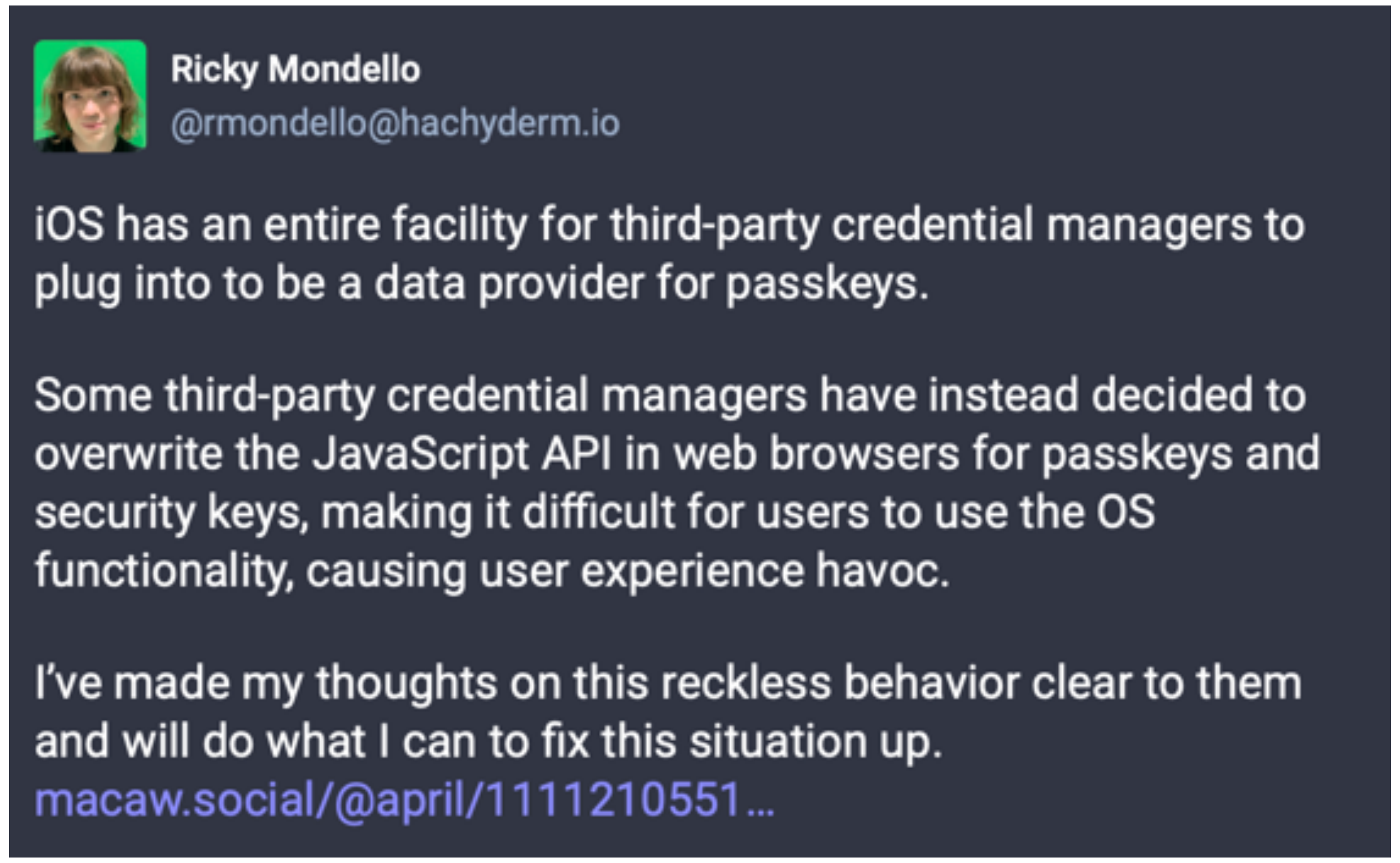
Please select folder for Browser Extensions (/Users/{username}/Library/Application Support)

Name	Vendor	Type	Status	Path	Version	SDK
	Microsof...	App Extension	Not Ins...	/Applications/Microsoft Word.app/Contents/Plugins/Wo...		
CalendarWidgetExten...	Microsof...	App Extension	Not Ins...	/Applications/Microsoft Outlook.app/Contents/PlugIns/...	16.76.1	com.apple.widgetkit-extension
CiscoAudioDevice	Cisco W...	App Extension	Not Ins...	/Applications/Cisco Webex Meetings.app/Contents/Plu...	1.0.1	
CiscoSparkMedia	Cisco W...	App Extension	Not Ins...	/Applications/Cisco Webex Meetings.app/Contents/Plu...	1.0	
CiscoSparkMercury	Cisco W...	App Extension	Not Ins...	/Applications/Cisco Webex Meetings.app/Contents/Plu...	1.0	
Developer	Develop...	App Extension	Not Ins...	/Applications/Developer.app/Contents/PlugIns/Develop...	10.4.1	com.apple.widgetkit-extension
DeveloperAppKitBridge	Develop...	App Extension	Not Ins...	/Applications/Developer.app/Contents/PlugIns/Develop...	1.0	
Dropbox	Dropbox....	App Extension	Not Ins...	/Applications/Dropbox.app/Contents/PlugIns/DropboxFi...	181.4.5...	com.apple.fileprovider-nonui
Dropbox Finder Exten...	Dropbox....	App Extension	Not Ins...	/Applications/Dropbox.app/Contents/PlugIns/garcon.ap...	2.10	com.apple.FinderSync
Dropbox Transfer	Dropbox....	App Extension	Not Ins...	/Applications/Dropbox.app/Contents/PlugIns/DropboxTr...	1.0	com.apple.share-services
Microsoft Edge Widgets	Microsof...	App Extension	Not Ins...	/Applications/Microsoft Edge.app/Contents/PlugIns/Mic...	99.0.11...	com.apple.widgetkit-extension
NordPass® Password...	NordPas...	App Extension	Not Ins...	/Applications/NordPass.app/Contents/PlugIns/safariExt...		com.apple.Safari.extension
Okta Browser Plugin	Okta Ext...	App Extension	Not Ins...	/Applications/Okta Extension App.app/Contents/PlugIns...	6.10.0	com.apple.Safari.web-extension
OneDrive File Provider	OneDriv...	App Extension	Not Ins...	/Applications/OneDrive.app/Contents/PlugIns/OneDrive...	23.158....	com.apple.fileprovider-nonui
OneDrive Finder Integ...	OneDriv...	App Extension	Not Ins...	/Applications/OneDrive.app/Contents/PlugIns/FinderSy...	23.158....	com.apple.FinderSync
OneNote	Microsof...	App Extension	Not Ins...	/Applications/Microsoft OneNote.app/Contents/PlugIns/...	16.76	com.apple.share-services
SecretChest	SecretC...	App Extension	Not Ins...	/Applications/SecretChest.app/Contents/PlugIns/Crede...	1.0	com.apple.authentication-services-c...
Shortcuts	Particula...	App Extension	Not Ins...	/Applications/Particulars.app/Contents/PlugIns/Shortcu...	52	com.apple.intents-service
Suspicious Package	Suspicio...	App Extension	Not Ins...	/Applications/Suspicious Package.app/Contents/PlugIn...	4.0	com.apple.quicklook.preview
Swiftify	Swiftify f...	App Extension	Not Ins...	/Applications/Swiftify for Xcode.app/Contents/PlugIns/S...	5.8.2	com.apple.dt.Xcode.extension.sourc...
TestFairy	TestFairy...	App Extension	Not Ins...	/Applications/TestFairy.app/Contents/PlugIns/TestFairy...	1.0	com.apple.dt.Xcode.extension.sourc...
Twitter	Twitter.a...	App Extension	Not Ins...	/Applications/Twitter.app/Contents/PlugIns/ShareExten...	9.30	com.apple.share-services
TwitterNotificationSer...	Twitter.a...	App Extension	Not Ins...	/Applications/Twitter.app/Contents/PlugIns/TwitterNotif...	9.30	com.apple.usernotifications.service
ZoomAudioDevice	zoom.us....	App Extension	Not Ins...	/Applications/zoom.us.app/Contents/PlugIns/ZoomAudi...	1.0	

Show All ○
Show Thirdparty Extensions ●
Show Uninstalled System Extension ○
Microsoft Edge Extension ●
Network Extensions ○
System Extensions ○
Google Chrome Extensions ●
Firefox Extensions ●

https://github.com/krypted/extensionsmanager/tree/main

Buuuut...

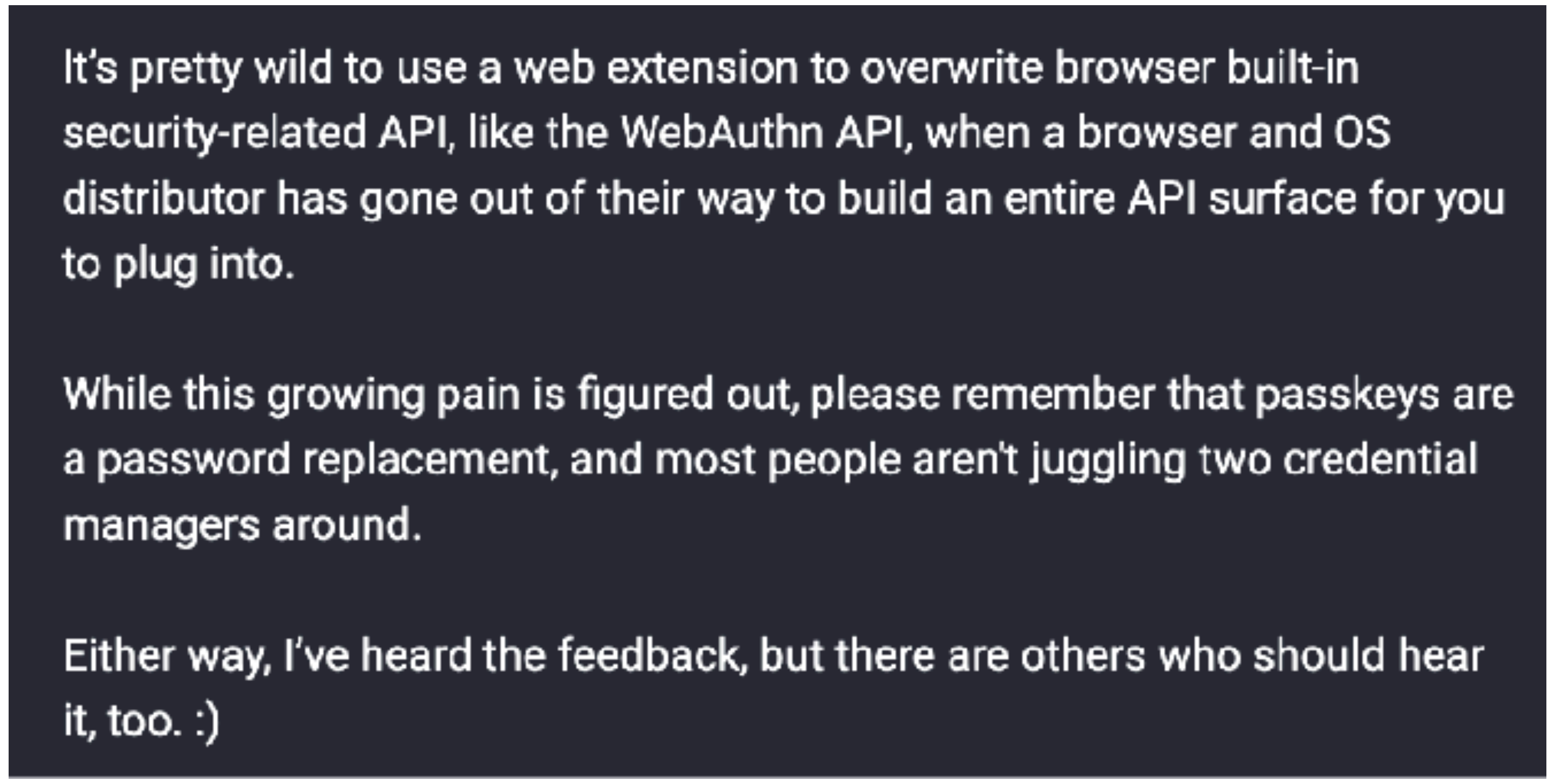


Ricky Mondello
@rmondello@hachyderm.io

iOS has an entire facility for third-party credential managers to plug into to be a data provider for passkeys.

Some third-party credential managers have instead decided to overwrite the JavaScript API in web browsers for passkeys and security keys, making it difficult for users to use the OS functionality, causing user experience havoc.

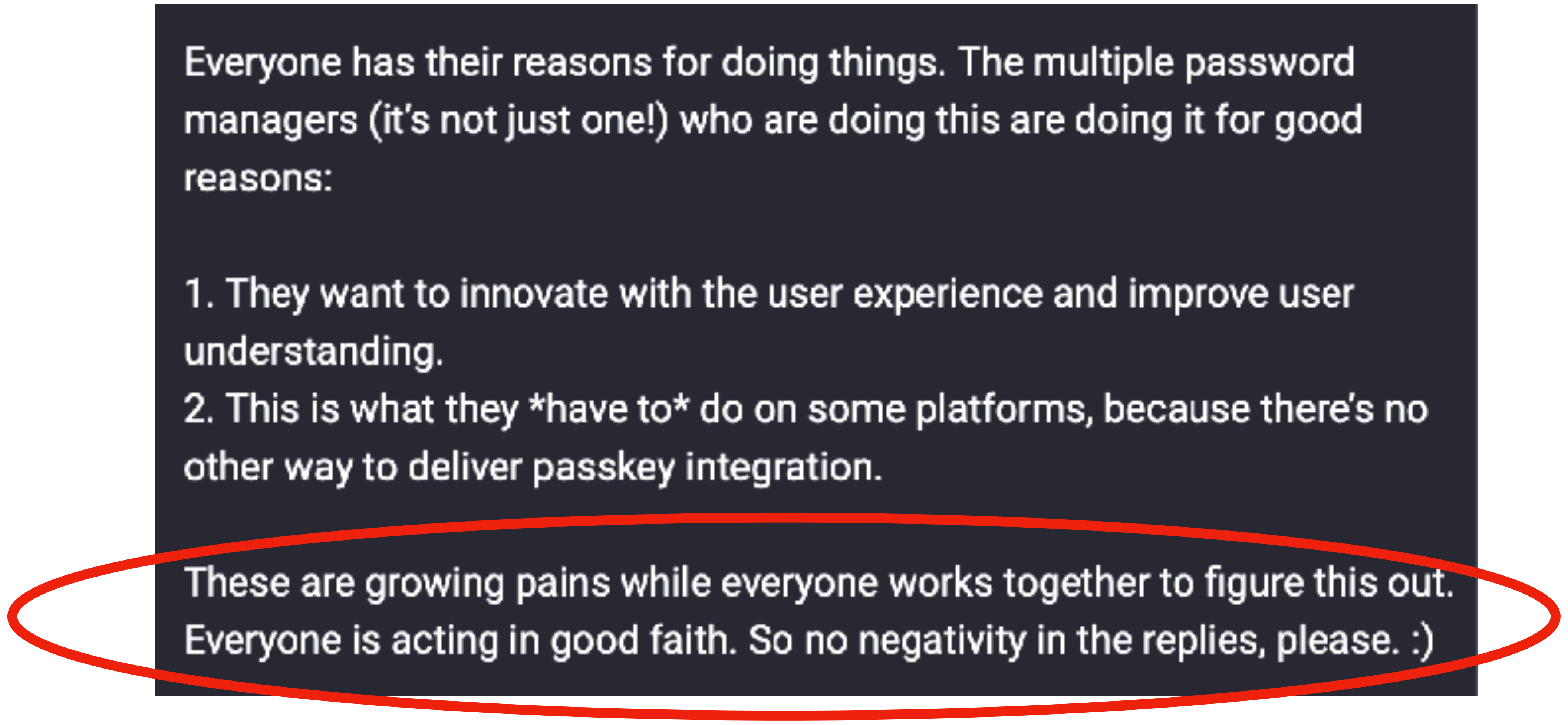
I've made my thoughts on this reckless behavior clear to them and will do what I can to fix this situation up.
macaw.social/@april/1111210551...



It's pretty wild to use a web extension to overwrite browser built-in security-related API, like the WebAuthn API, when a browser and OS distributor has gone out of their way to build an entire API surface for you to plug into.

While this growing pain is figured out, please remember that passkeys are a password replacement, and most people aren't juggling two credential managers around.

Either way, I've heard the feedback, but there are others who should hear it, too. :)



Everyone has their reasons for doing things. The multiple password managers (it's not just one!) who are doing this are doing it for good reasons:

1. They want to innovate with the user experience and improve user understanding.
2. This is what they *have to* do on some platforms, because there's no other way to deliver passkey integration.

These are growing pains while everyone works together to figure this out. Everyone is acting in good faith. So no negativity in the replies, please. :)

We have thoughts…

The Genesis Problem

Legacy flows vs New flows

Are passkeys *actually* more phishing resistant

Only one autofill provider at a time

Developers don’t have to do some things…

Can a user with a personal Apple ID later sign in with MAID and get passkeys?

The MAID must be the primary account holder

The identity ecosystem: Passwords, Platform SSO, keys, certificates, and passkeys (oh my)

That One Takeaway

Further Reading

Some Apple passkey docs

- https://developer.apple.com/passkeys/
- https://developer.apple.com/documentation/authenticationservices/aspasskeycredentialidentity?changes=_2__9&language=objc
- https://developer.apple.com/documentation/authenticationservices/ascredentialproviderextensioncontext/4172624-completeassertionrequest
- https://developer.apple.com/forums/thread/731615

Useful Links

- Webauthn.guide: Webauthn documentation
- Webauthn.io: Reference implementation for testing
- Matt Miller from Cisco && webauthn.io: https://podcast.macadmins.org/2023/02/27/episode-304-webauthn-and-webauthn-io/
- Directory of sites that support Passkeys: https://passkeys.directory/
- See Extensions: https://github.com/krypted/extensionsmanager
- See passkey stuffs: https://github.com/krypted/webauthn-inspector