WHY DO WE EVEN NEED OAUTH ANYWAY?

AARON PARECKI
@AARONPK

Thank You to Our Sponsors and Hosts!

OWASP
NEW
ZEALAND
owasp.org.nz

QUANTUM
SECURITY

AUT

CyberCX

DATACOM

snyk

Auth0

Checkmarx

HCL AppScan

kordia®

LATERAL
SECURITY

MICRO
FOCUS

Pulse Security
www.pulsesecurity.co.nz

RedShield

Flux

SEQA™
Information Security

Cobalt

LACEWORK

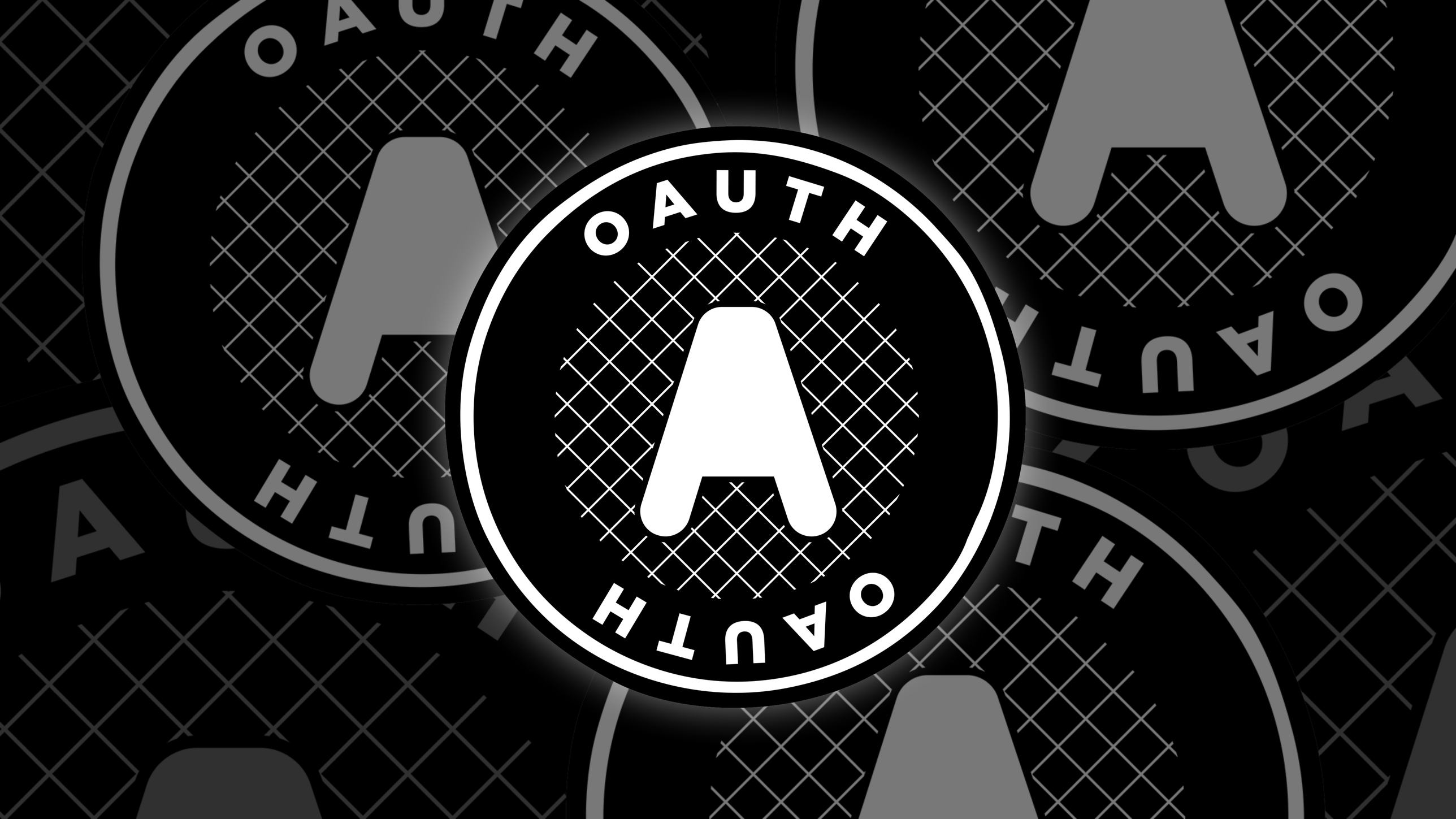
SecureFlag

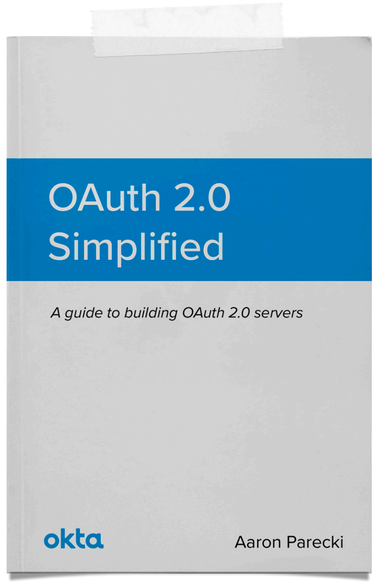
Without them, OWASP New Zealand Day couldn't happen

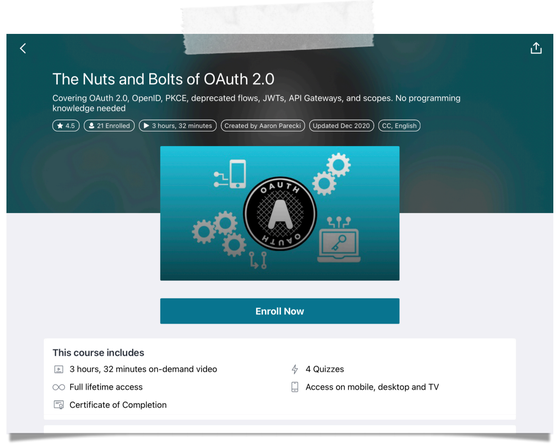
https://unsplash.com/photos/SYTO3xs06fU

https://unsplash.com/photos/dYEuFB8KQJk


Jane Appleseed
appleseed@me.com
125 Main St.
City Name, CA 95014
Work: (408) 123-4567
Home: (408) 765-4321


OAUTH





okta

I E T F®

[Search] [txt|html|pdf] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: (draft-parecki-oauth-v2-1) 00 01 02 03
04

OAuth Working Group
Internet-Draft
Intended status: Standards Track
Expires: 8 April 2022

D. Hardt
Hellō
A. Parecki
Okta
T. Lodderstedt
yes.com
5 October 2021

The OAuth 2.1 Authorization Framework
draft-ietf-oauth-v2-1-04

Abstract

The OAuth 2.1 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and an authorization service, or by allowing the third-party application to obtain access on its own behalf. This specification replaces and obsoletes the OAuth 2.0 Authorization Framework described in RFC 6749.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Updated by: 8252 PROPOSED STANDARD
Errata Exist
Internet Engineering Task Force (IETF) D. Hardt, Ed.
Request for Comments: 6749 Microsoft
Obsoletes: 5849 October 2012
Category: Standards Track
ISSN: 2070-1721

The OAuth 2.0 Authorization Framework

Abstract

The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf. This specification replaces and obsoletes the OAuth 1.0 protocol described in RFC 5849.

Status of This Memo

This is an Internet Standards Track document.

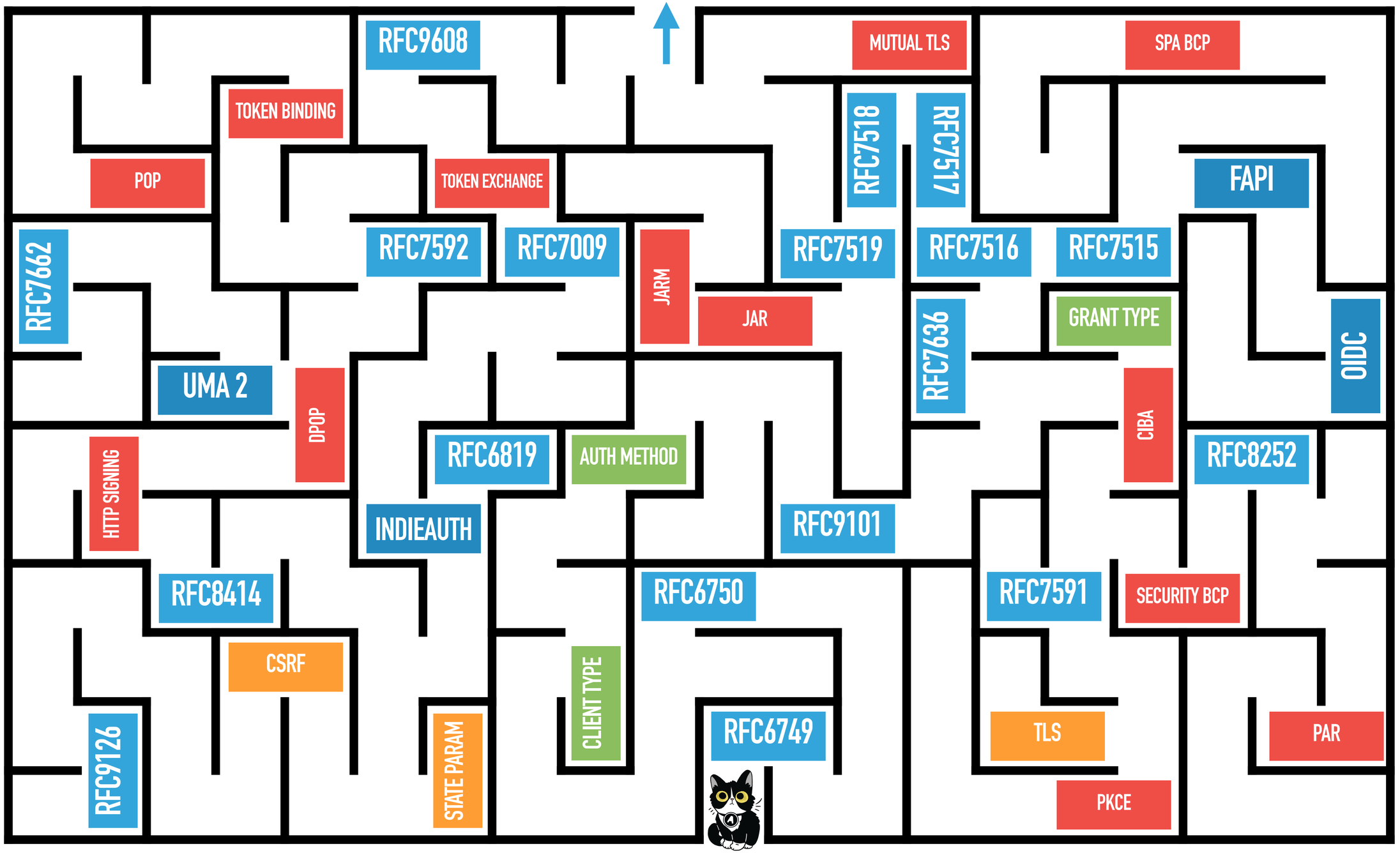
This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

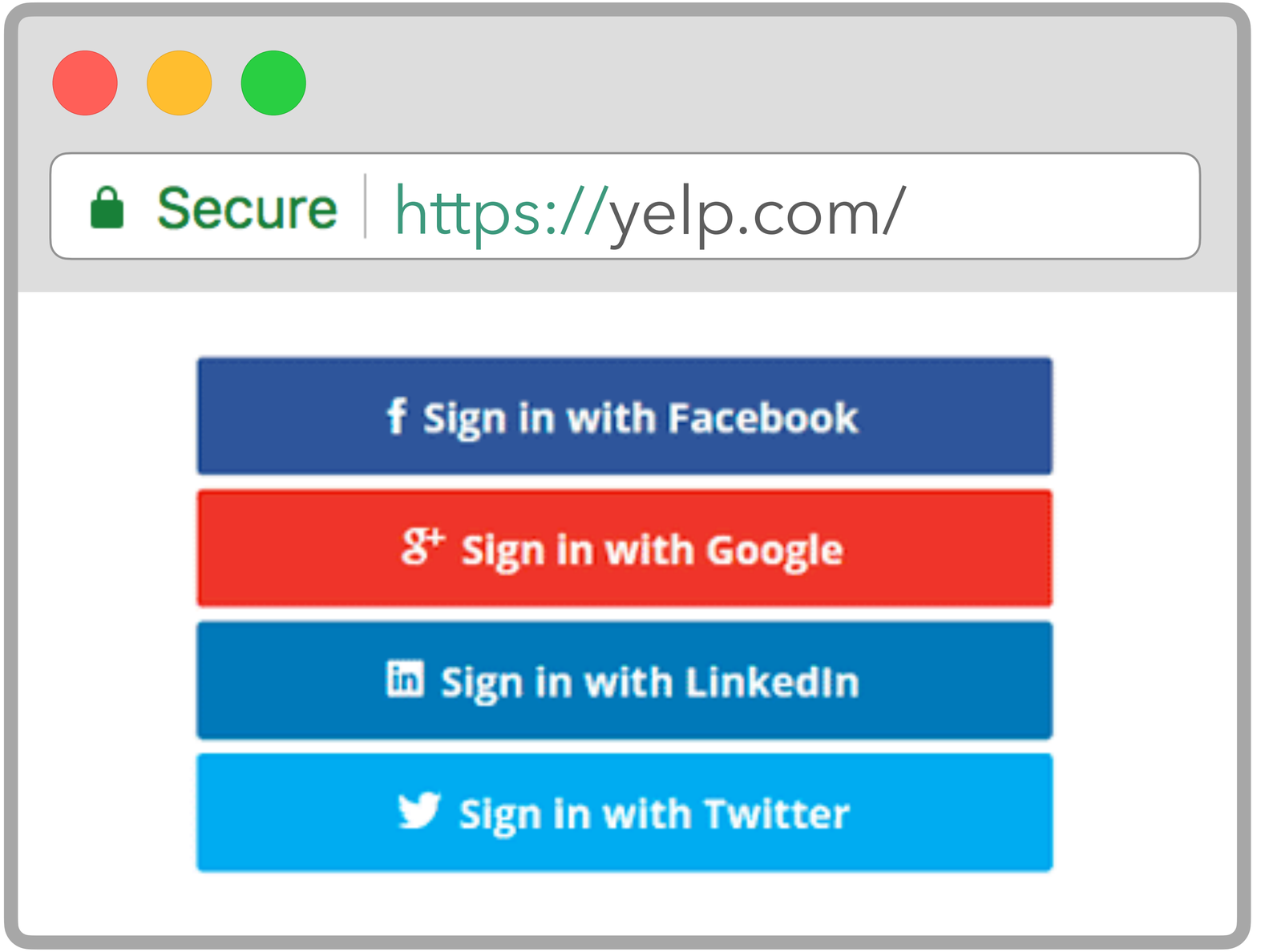
Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6749.

Table of Contents

Specs are not good tutorials!

BUILDING YOUR APPLICATION




Secure
https://yelp.com/
Sign in with Facebook
Sign in with Google
Sign in with LinkedIn
Sign in with Twitter


Sign in with Facebook
Sign in with Google
Sign in with LinkedIn
Sign in with Twitter
IS THIS OAUTH?

LIMIT/DELEGATE ACCESS TO DATA

Are your friends already on Yelp?

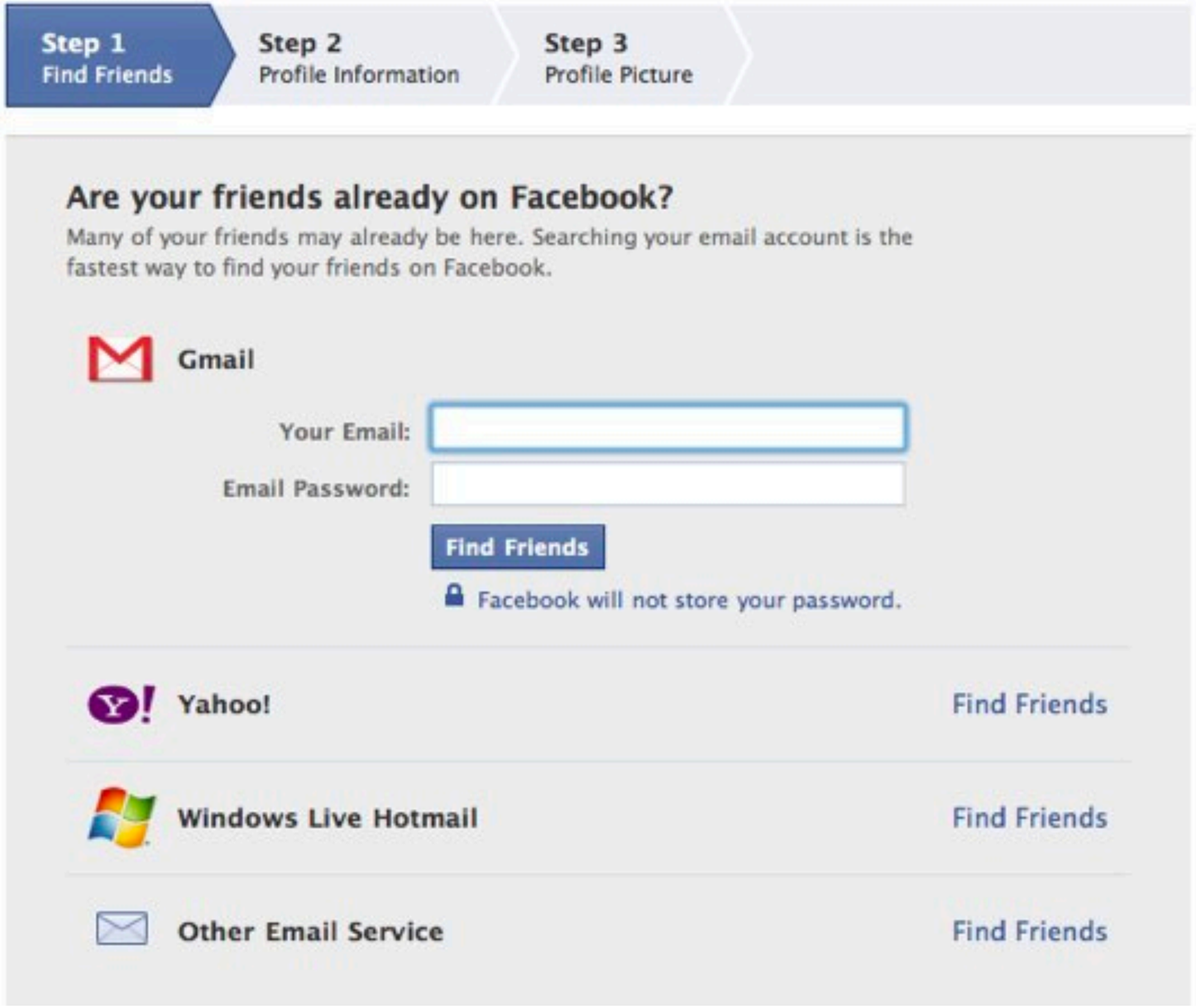
Many of your friends may already be here, now you can find out. Just log in and we'll display all your contacts, and you can select which ones to invite! And don't worry, we don't keep your email password or your friends' addresses. We loathe spam, too.

Your Email Service ○ msn Hotmail ○ YAHOO! MAIL ○ AOL Mail ◉ Gmail

Your Email Address ima.testguy@gmail.com *(e.g. bob@gmail.com)*

Your Gmail Password ●●●●●●●●●● *(The password you use to log into your Gmail email)*

Skip this step **Check Contacts**


Step 1
Find Friends
Step 2
Profile Information
Step 3
Profile Picture
Are your friends already on Facebook?
Many of your friends may already be here. Searching your email account is the fastest way to find your friends on Facebook.
Gmail
Your Email:
Email Password:
Find Friends
Facebook will not store your password.
Yahoo!
Find Friends
Windows Live Hotmail
Find Friends
Other Email Service
Find Friends

WHY IS THIS BAD?

EVEN THOUGH IT ONLY NEEDS ACCESS TO

SOME DATA...

YOU'VE GIVEN
THE APP ACCESS TO
ALL YOUR DATA

NO WAY TO

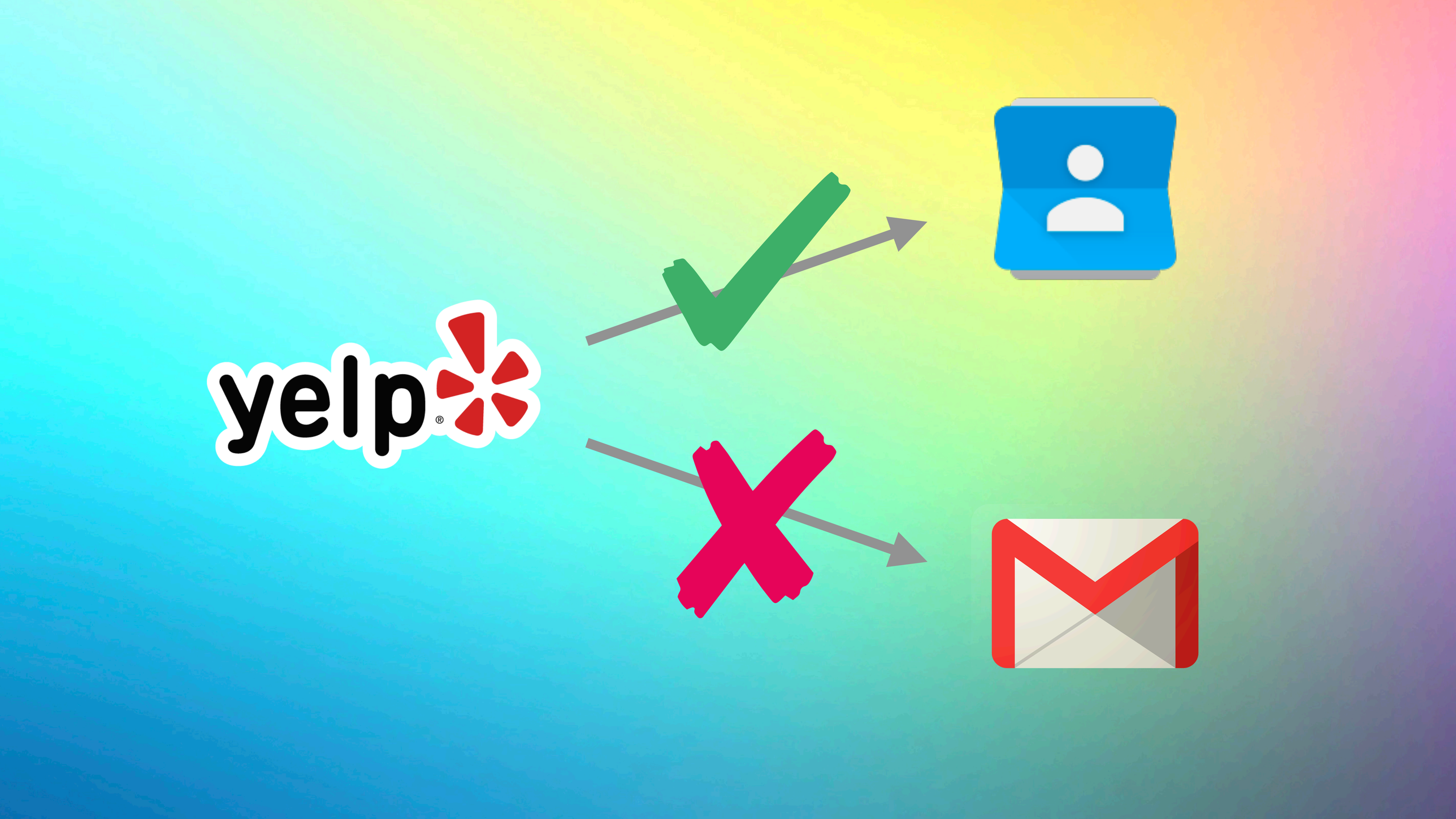
REVOKE

THE APP'S ACCESS

YOU PLACE

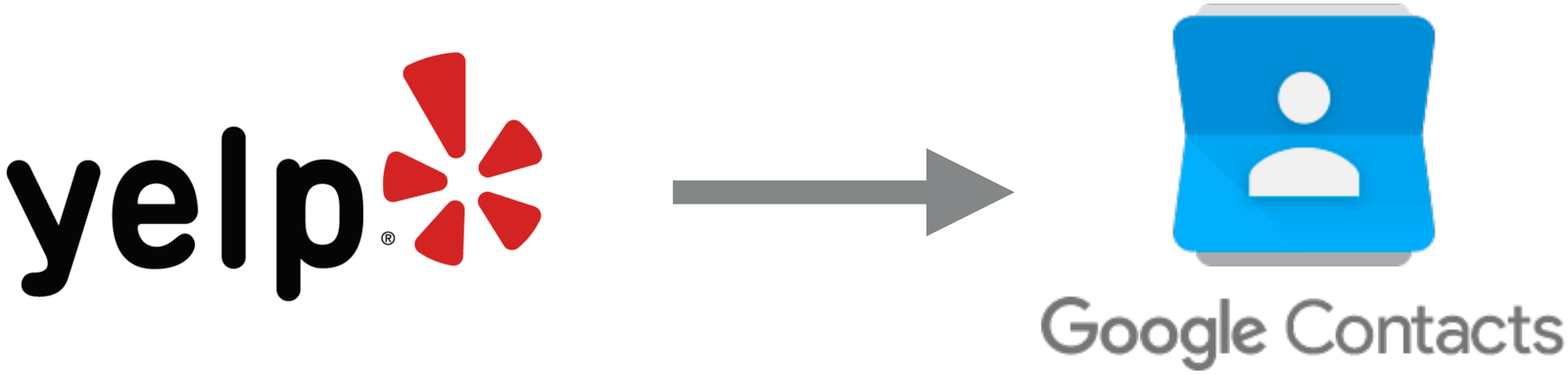
ALL YOUR TRUST

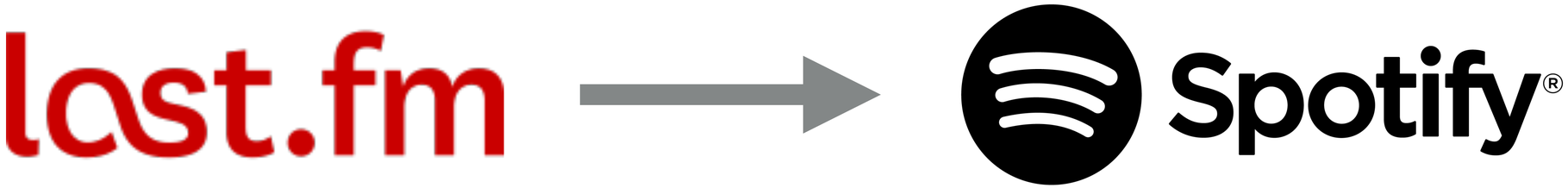
IN THE APP

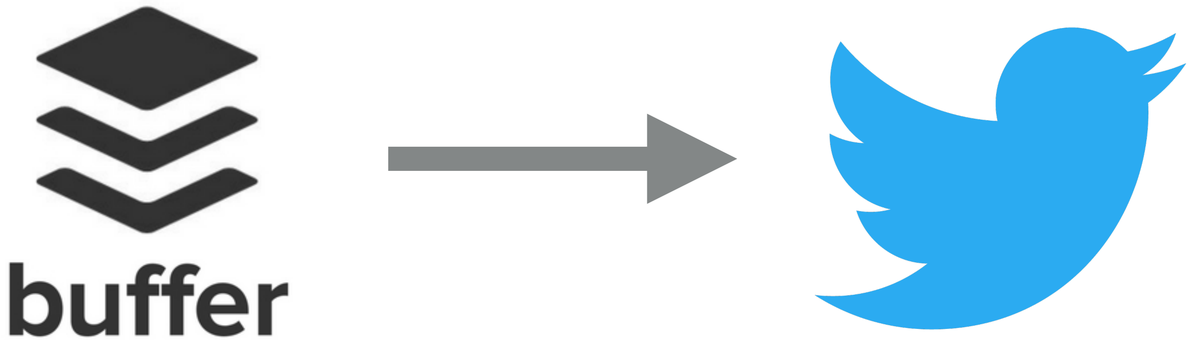

yelp


OAUTH
OAUTH

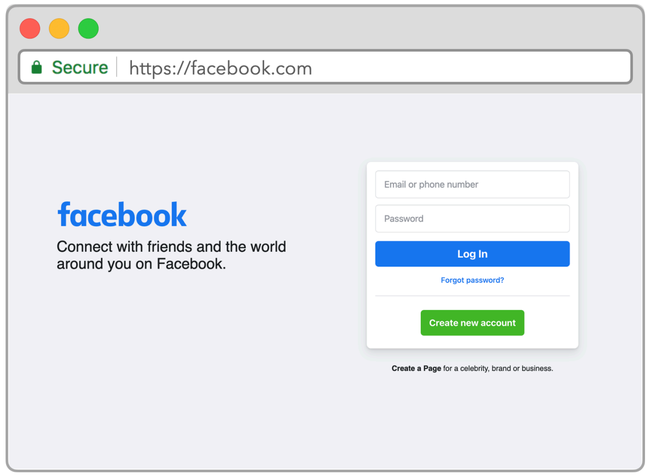
https://unsplash.com/photos/GJY1eAw6tn8

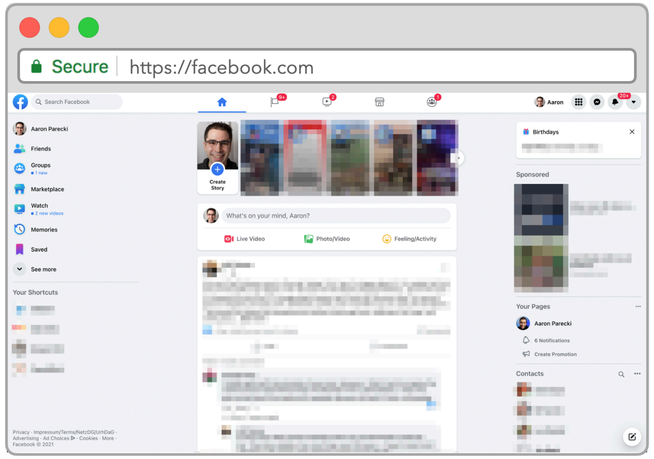

yelp
Google Contacts


last.fm
Spotify

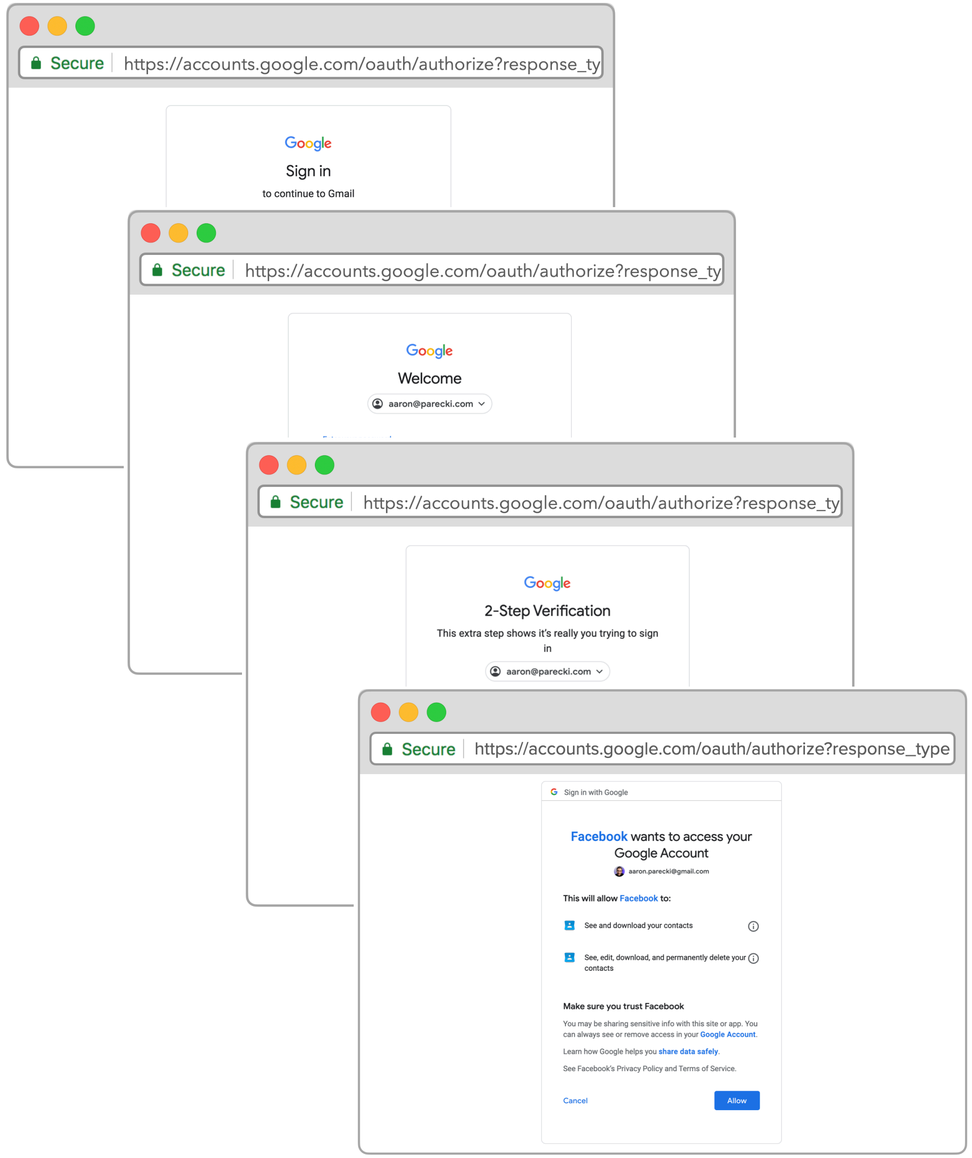

buffer

Application





OAuth Server



Sign in with Google

Facebook wants to access your Google Account

aaron.parecki@gmail.com

This will allow Facebook to:

- See and download your contacts
- See, edit, download, and permanently delete your contacts

Make sure you trust Facebook

You may be sharing sensitive info with this site or app. You can always see or remove access in your **Google Account**.

Learn how Google helps you **share data safely**.

See Facebook's Privacy Policy and Terms of Service.

Cancel

Allow

Authorize Example App to access your account?

Authorize app | Cancel

Example App

By Aaron Parecki

example-app.com

Free Version Control with unlimited private and public repositories.

This application will be able to:

- See Tweets from your timeline (including protected Tweets) as well as your Lists and collections.
- See your Twitter profile information and account settings.
- See accounts you follow, mute, and block.

Learn more about third-party app permissions in the Help Center.

Authorize OAuth 2 Example App

OAuth 2 Example App by **aaronpk**
wants to access your **aaronpk** account

Personal user data
Full access

Repositories
Public only

Organization access

indieweb ✓

microformats ✓

oauth2 ✓

okta ✓

w3c ✓

Authorize aaronpk

Authorizing will redirect to
https://example-app.com.dev

fitbit

Example App by Aaron Parecki would like the ability to access the following data in your Fitbit account

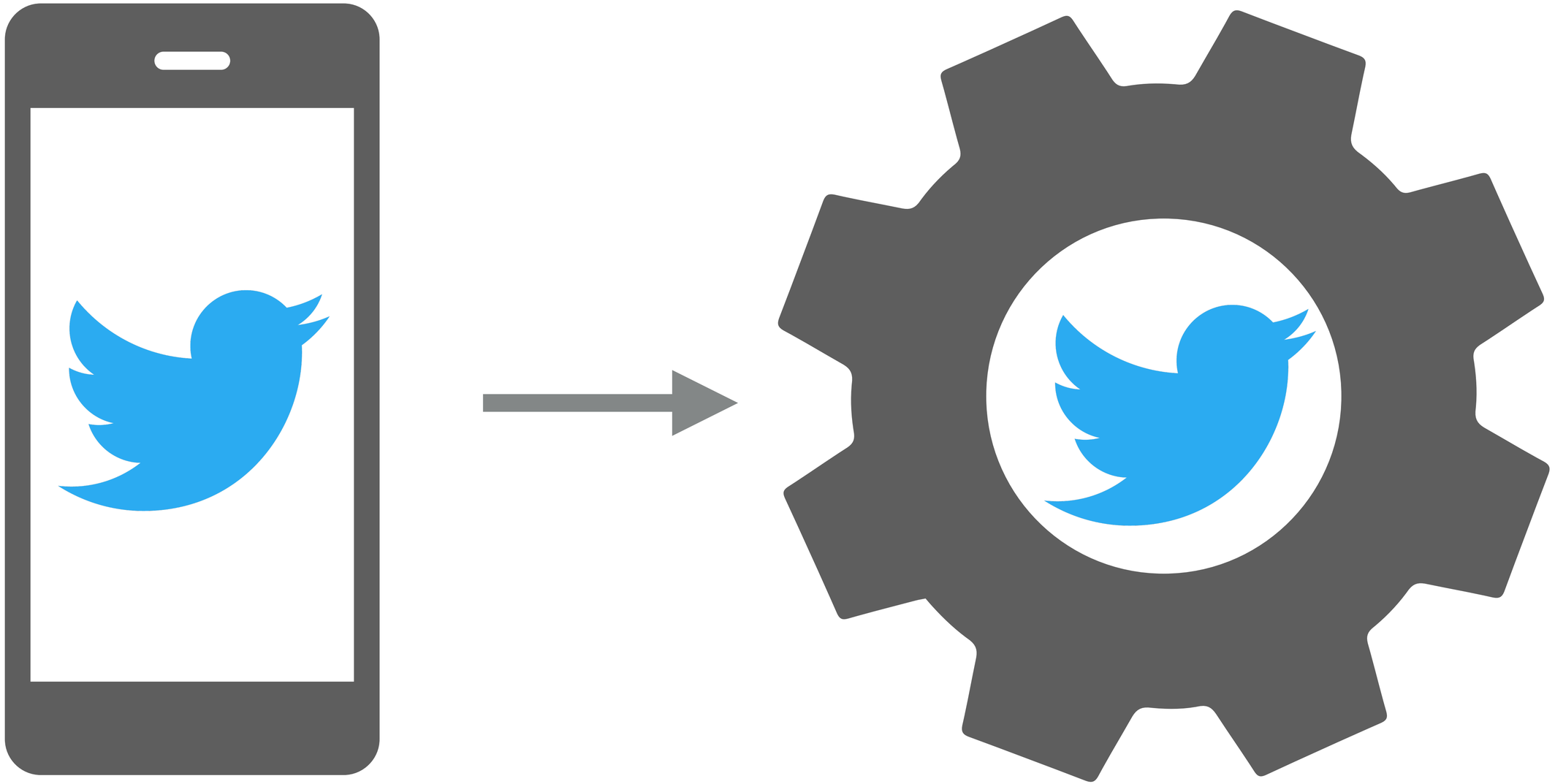
- [x] Select All
- [x] activity and exercise
- [x] weight
- [x] sleep
- [x] food and water logs
- [x] location and GPS
- [x] profile
- [x] heart rate

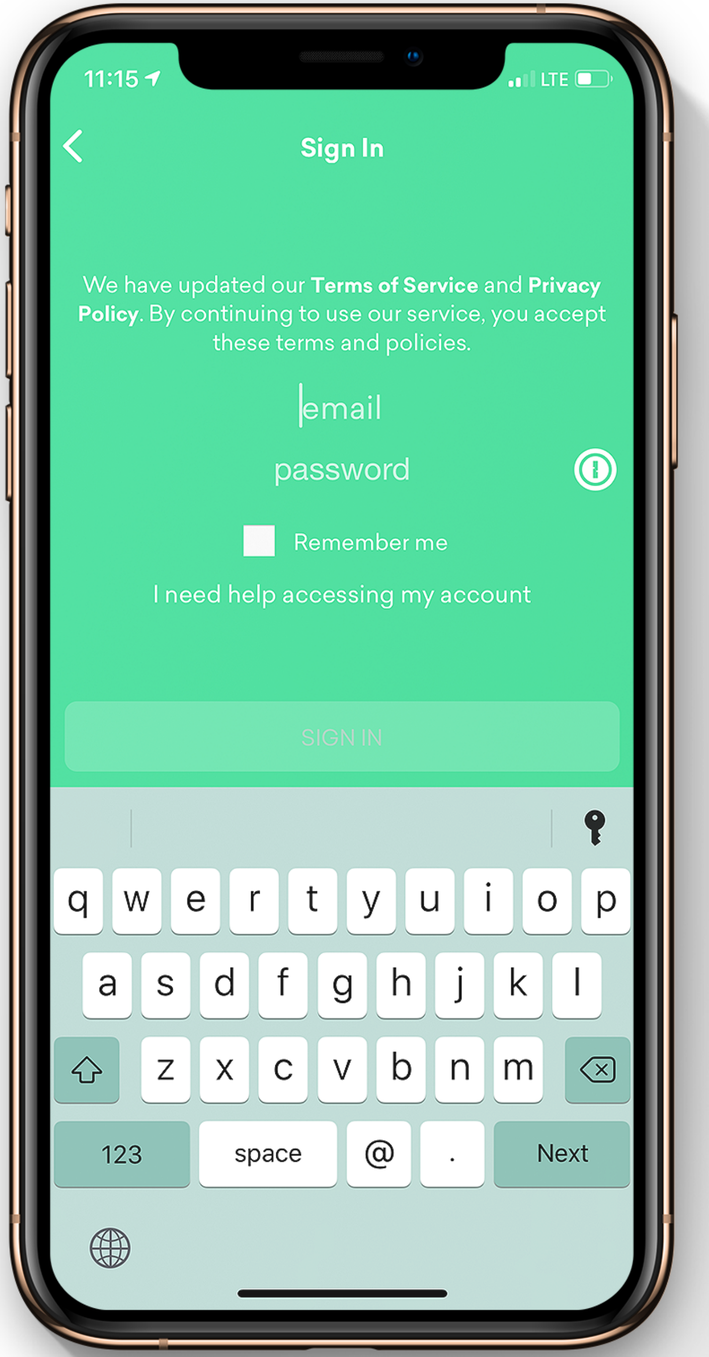
Deny **Allow**

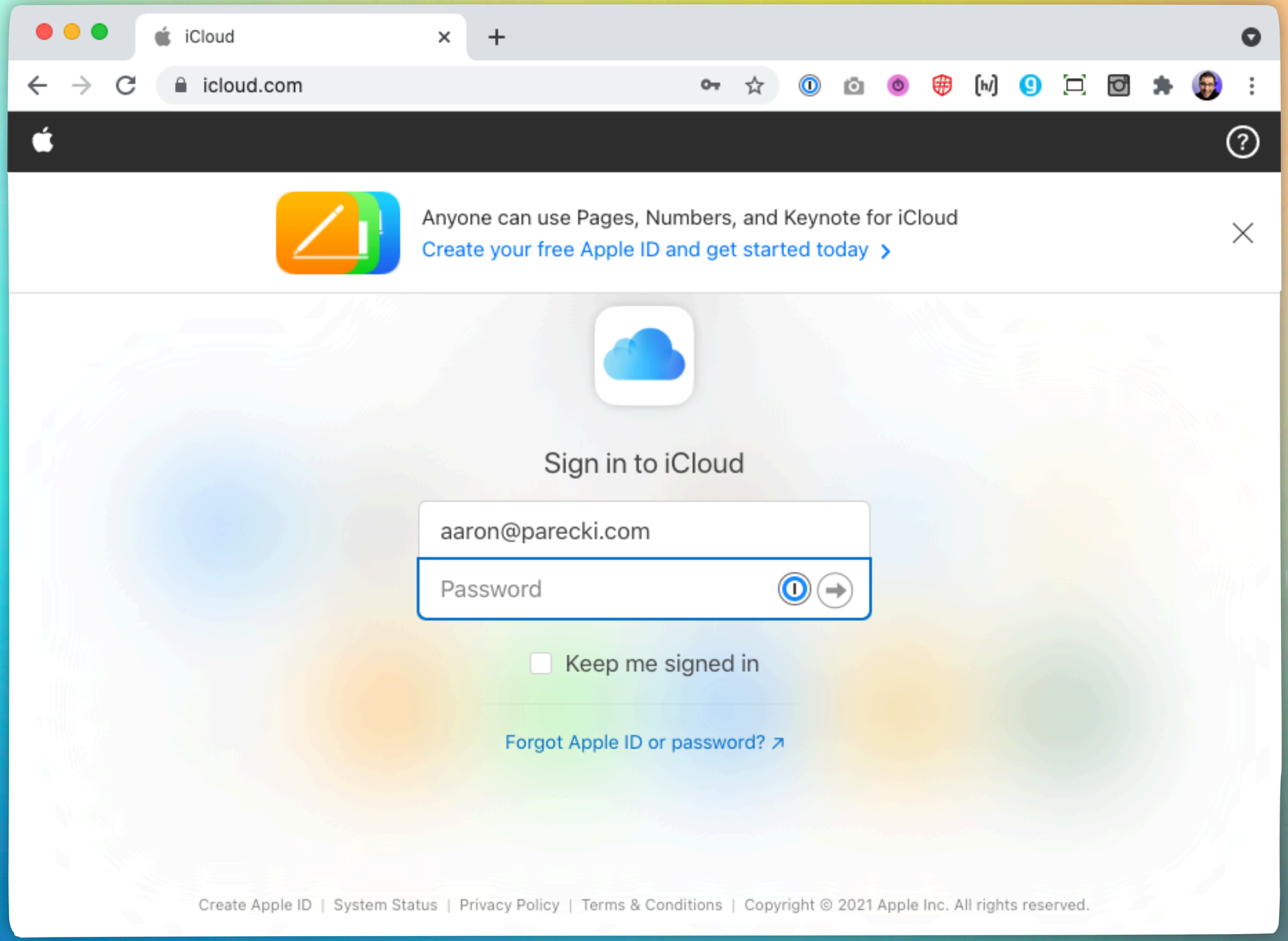
Data shared with aaronpk will be governed by Aaron Parecki's privacy policy and terms of service. You can revoke this consent at any time in your Fitbit account settings. More information about these permissions can be found here.

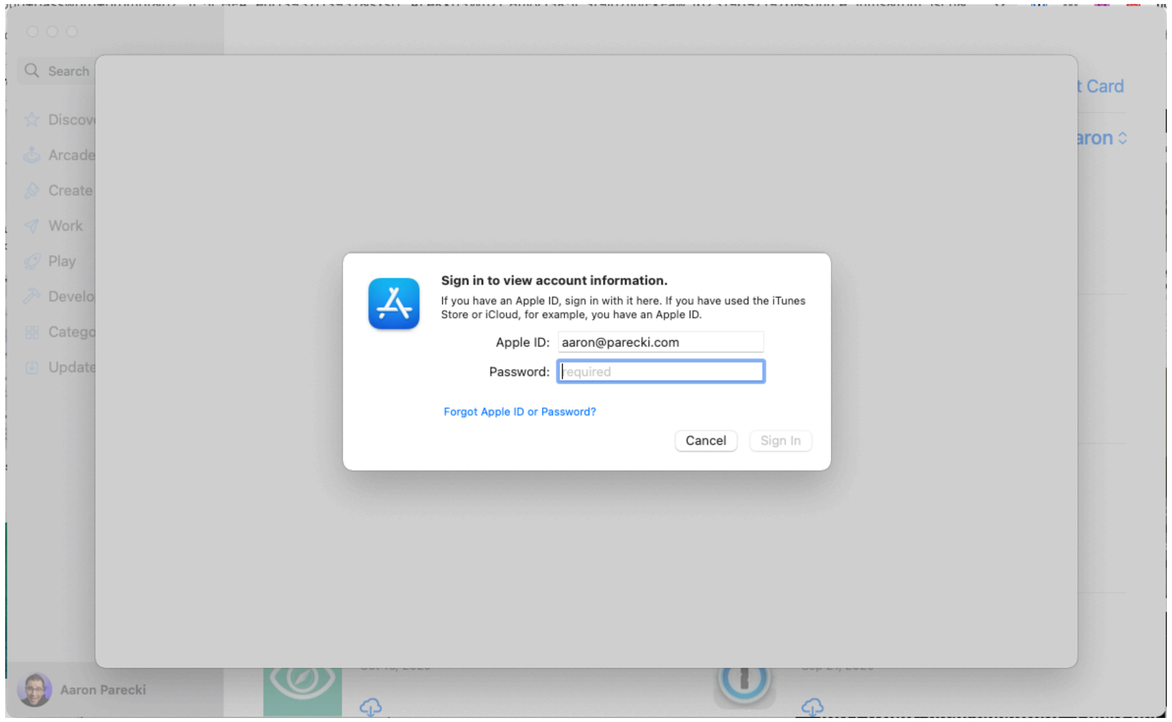
Signed in as aaron@parecki.com
Not you?

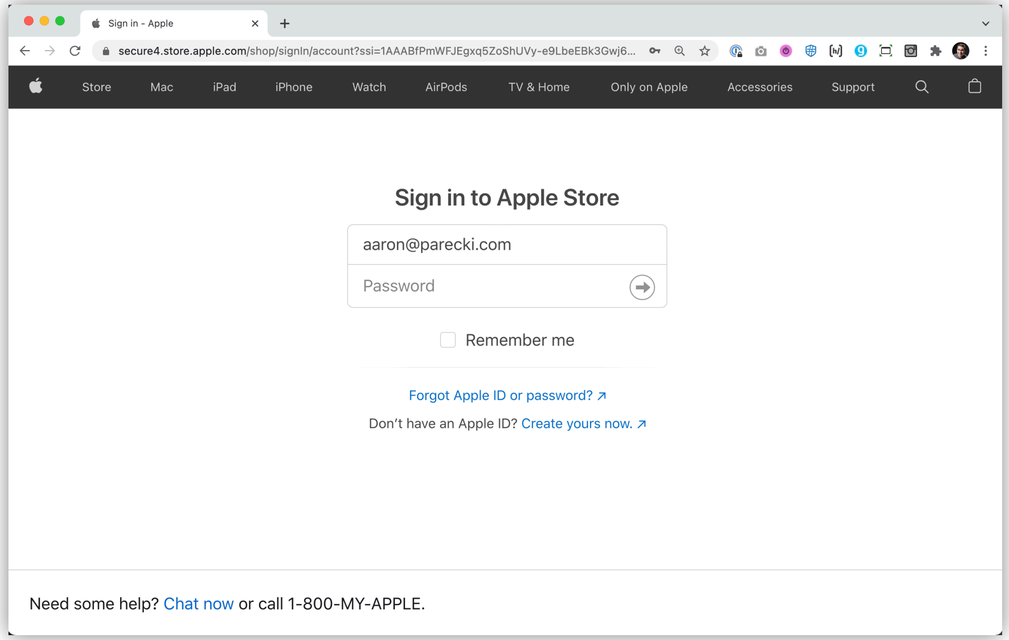
WHAT ABOUT FIRST-PARTY APPS?

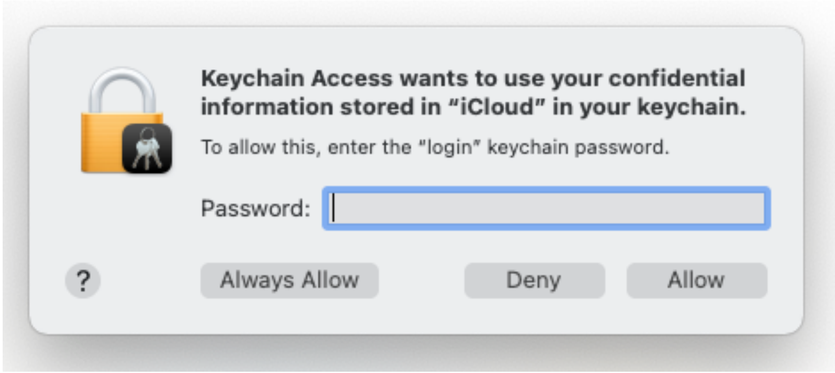


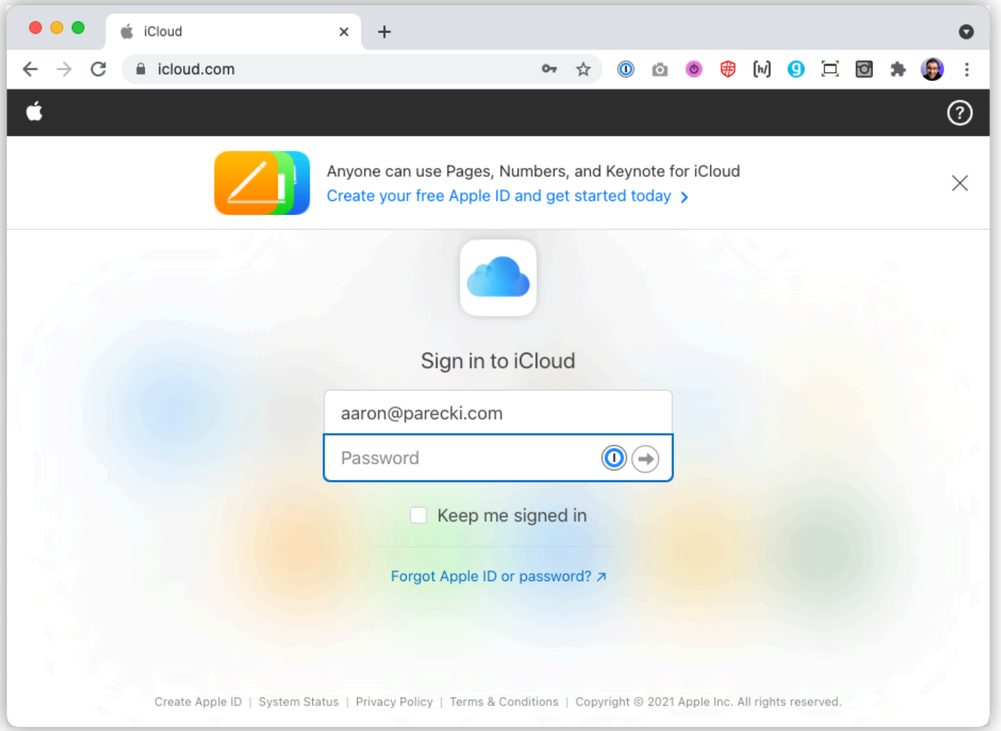

11:15
LTE
Sign In
We have updated our Terms of Service and Privacy Policy. By continuing to use our service, you accept these terms and policies.
email
password
Remember me
I need help accessing my account
SIGN IN
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
@
.
Next

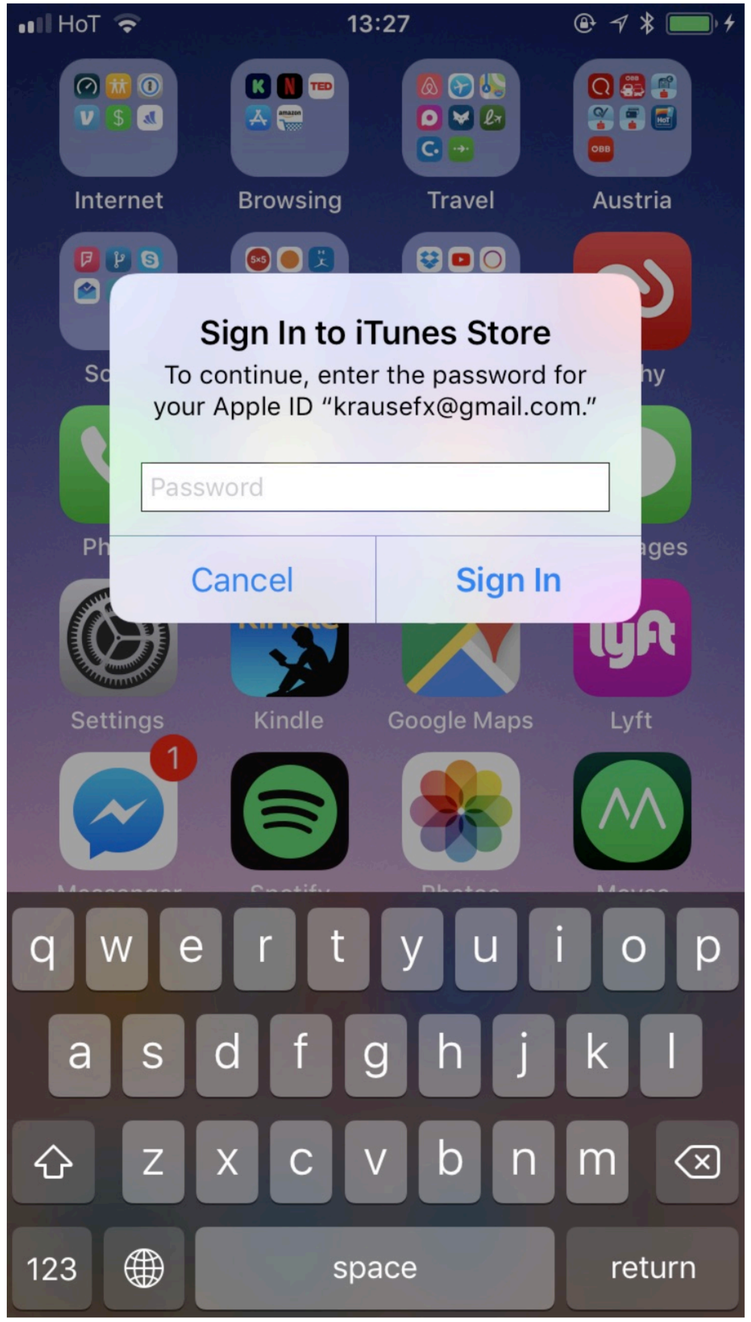

iCloud
icloud.com
Anyone can use Pages, Numbers, and Keynote for iCloud
Create your free Apple ID and get started today ›
Sign in to iCloud
aaron@parecki.com
Password
Keep me signed in
Forgot Apple ID or password? ↗
Create Apple ID | System Status | Privacy Policy | Terms & Conditions | Copyright © 2021 Apple Inc. All rights reserved.

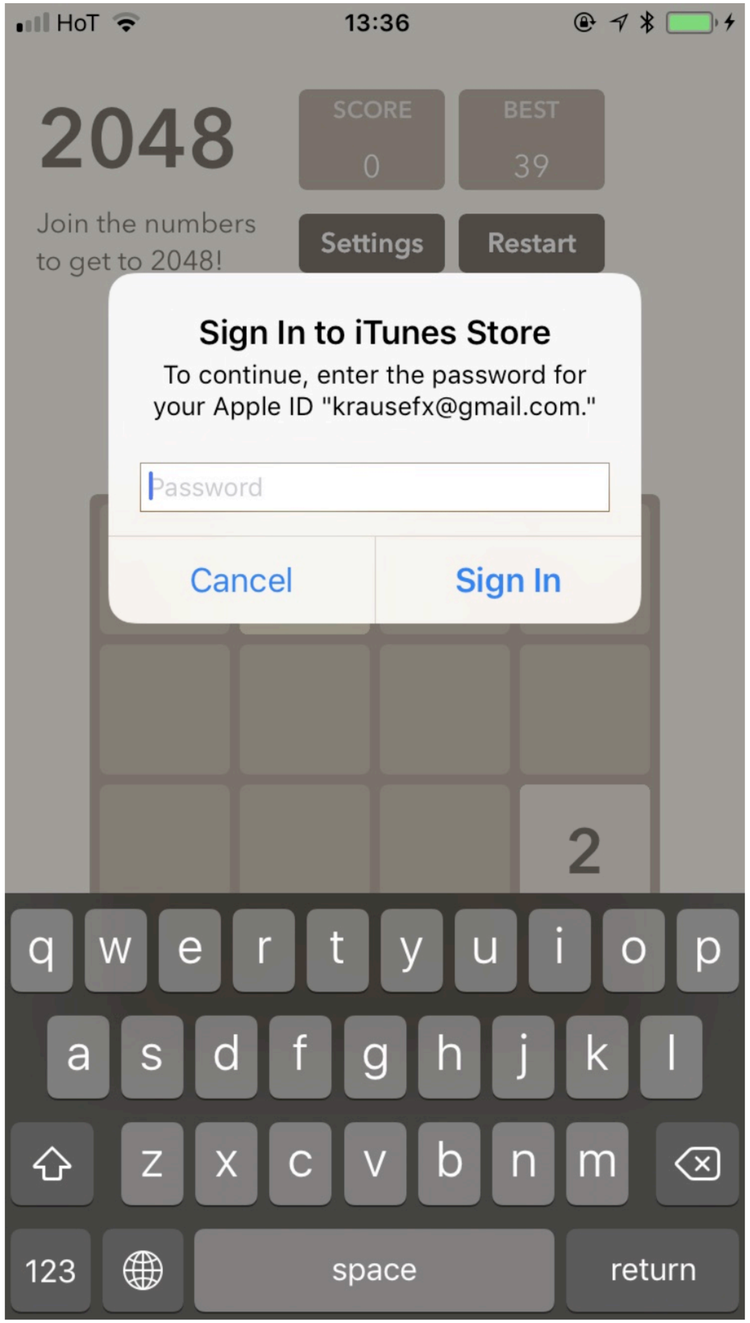

Search
Discov
Arcade
Create
Work
Play
Develo
Catego
Update
t Card
aron
Sign in to view account information.
If you have an Apple ID, sign in with it here. If you have used the iTunes Store or iCloud, for example, you have an Apple ID.
Apple ID: aaron@parecki.com
Password: required
Forgot Apple ID or Password?
Cancel
Sign In
Aaron Parecki


Sign in - Apple
secure4.store.apple.com/shop/signIn/account?ssi=1AAABfPmWFJEgxq5ZoShUVy-e9LbeEBk3Gwj6...
Store
Mac
iPad
iPhone
Watch
AirPods
TV & Home
Only on Apple
Accessories
Support
Sign in to Apple Store
aaron@parecki.com
Password
Remember me
Forgot Apple ID or password?
Don't have an Apple ID? Create yours now.
Need some help? Chat now or call 1-800-MY-APPLE.


Keychain Access wants to use your confidential information stored in "iCloud" in your keychain.
To allow this, enter the "login" keychain password.
Password:
?
Always Allow
Deny
Allow


iCloud
icloud.com
Anyone can use Pages, Numbers, and Keynote for iCloud
Create your free Apple ID and get started today
Sign in to iCloud
aaron@parecki.com
Password
Keep me signed in
Forgot Apple ID or password?
Create Apple ID | System Status | Privacy Policy | Terms & Conditions | Copyright © 2021 Apple Inc. All rights reserved.





https://krausefx.com/blog/ios-privacy-stealpassword-easily-get-the-users-apple-id-password-just-by-asking

mail.google.com/mail/u/0/?ui=2&view=btop&ver=ops2cvpehp6&search=inbox&th=%23thread-f%3A1715764358773187010...

Archive Spam Delete | Mark as unread Snooze | Move to Labels More

“Q1 Bonus” Inbox ×

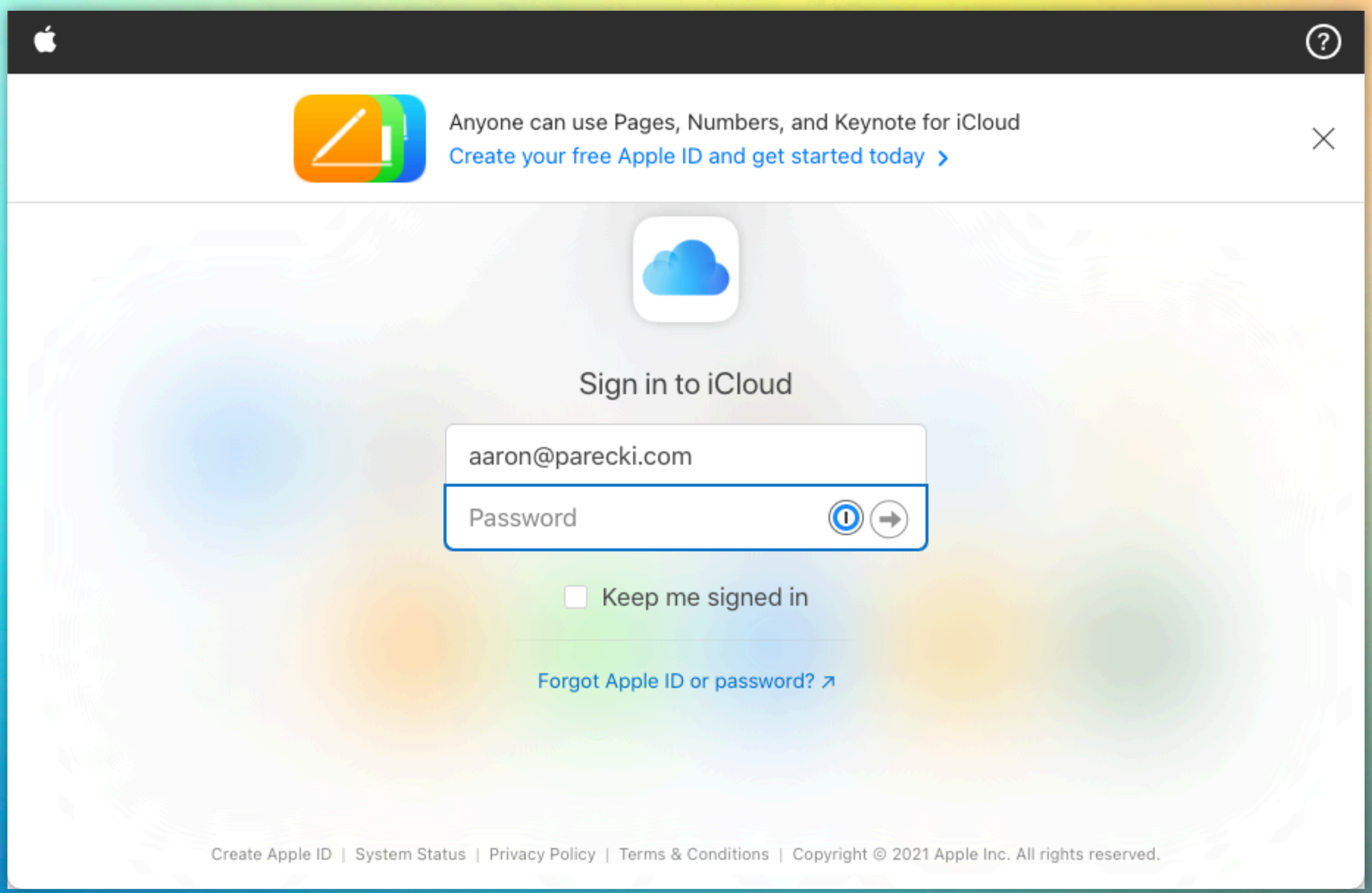
Frank Abagnale <frank.abagnale@noreply-icloud.com> 11:20 AM (0 minutes ago) Reply

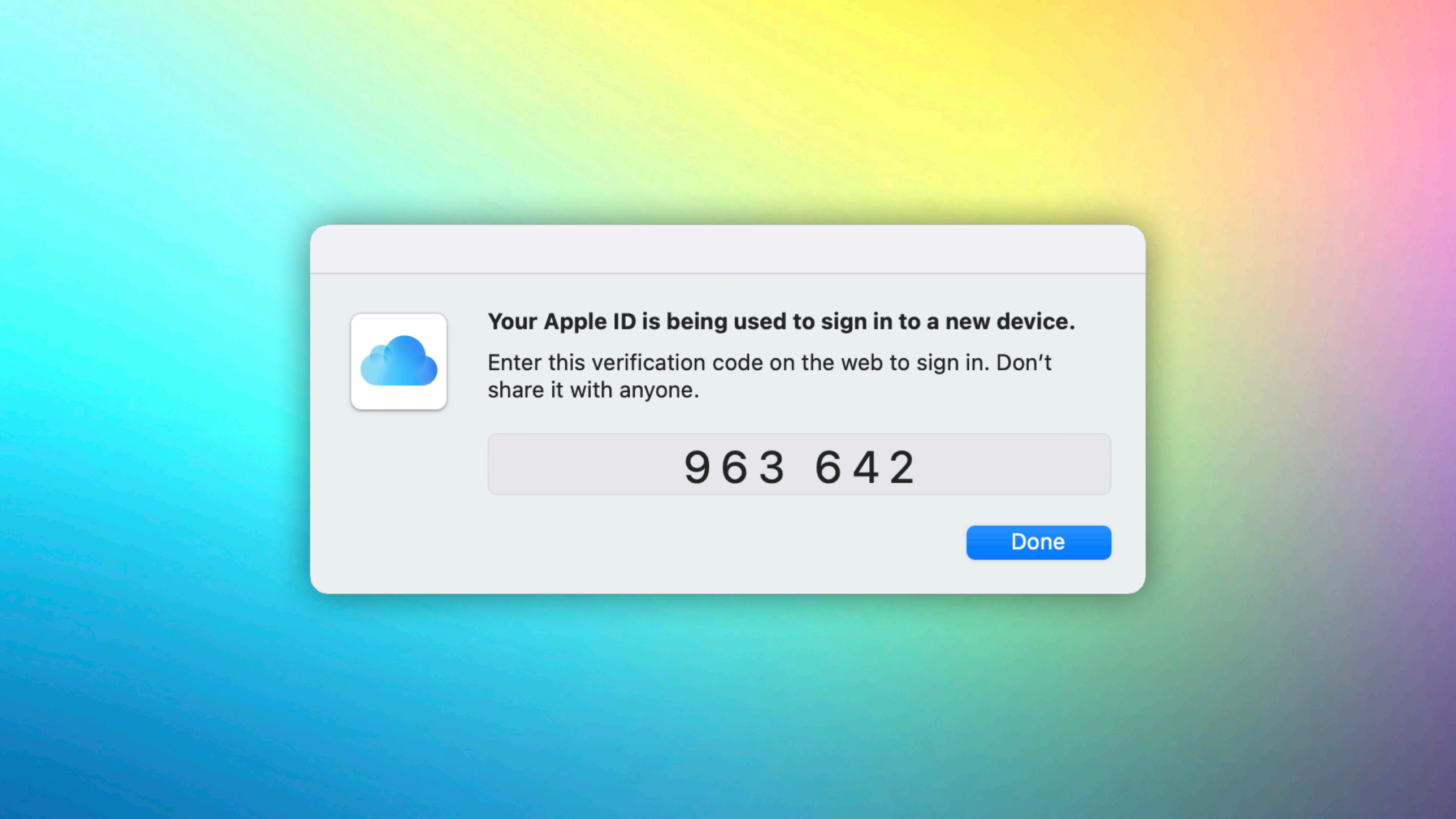
to aaron

Open my shared folder:

Q1 Bonus
iCloud Drive

Reply Reply all Forward


Anyone can use Pages, Numbers, and Keynote for iCloud
Create your free Apple ID and get started today ›
Sign in to iCloud
aaron@parecki.com
Password
Keep me signed in
Forgot Apple ID or password? ↗
Create Apple ID | System Status | Privacy Policy | Terms & Conditions | Copyright © 2021 Apple Inc. All rights reserved.


Your Apple ID is being used to sign in to a new device.
Enter this verification code on the web to sign in. Don’t share it with anyone.
963 642
Done

THEN WHAT GOOD IS

MULTI-FACTOR AUTHENTICATION?

Phishable MFA

678328 is your Microsoft Azure verification code

Your Apple ID is being used to sign in to a new device.

Enter this verification code on the web to sign in. Don't share it with anyone.

963 642

Done

Google

Are you trying to sign in?

aaron@parecki.com

Device
Intel Mac OS X 10_15_7

Near
Düsseldorf, Germany

Time
Just now

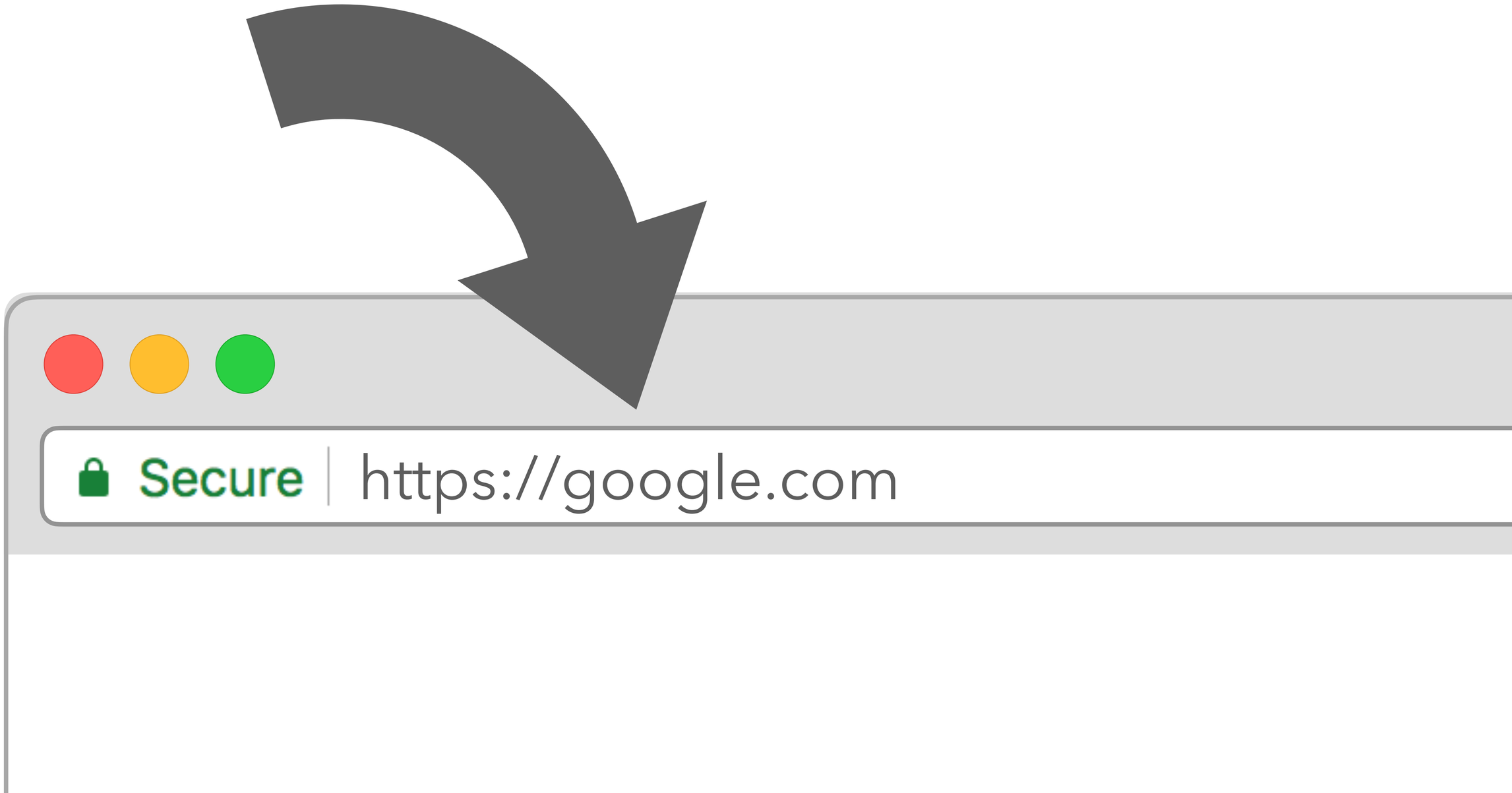
No, don't allow

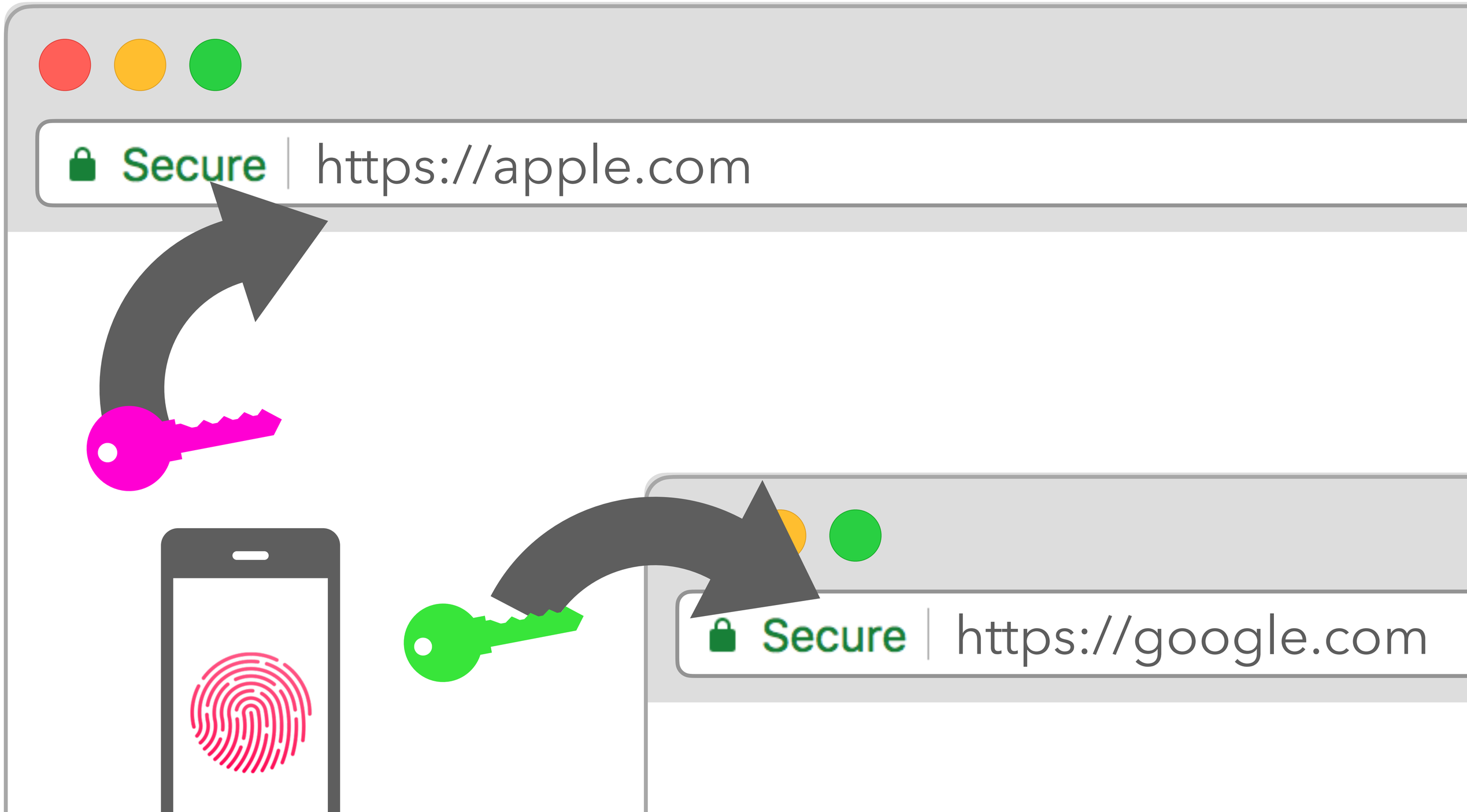
Yes, it's me

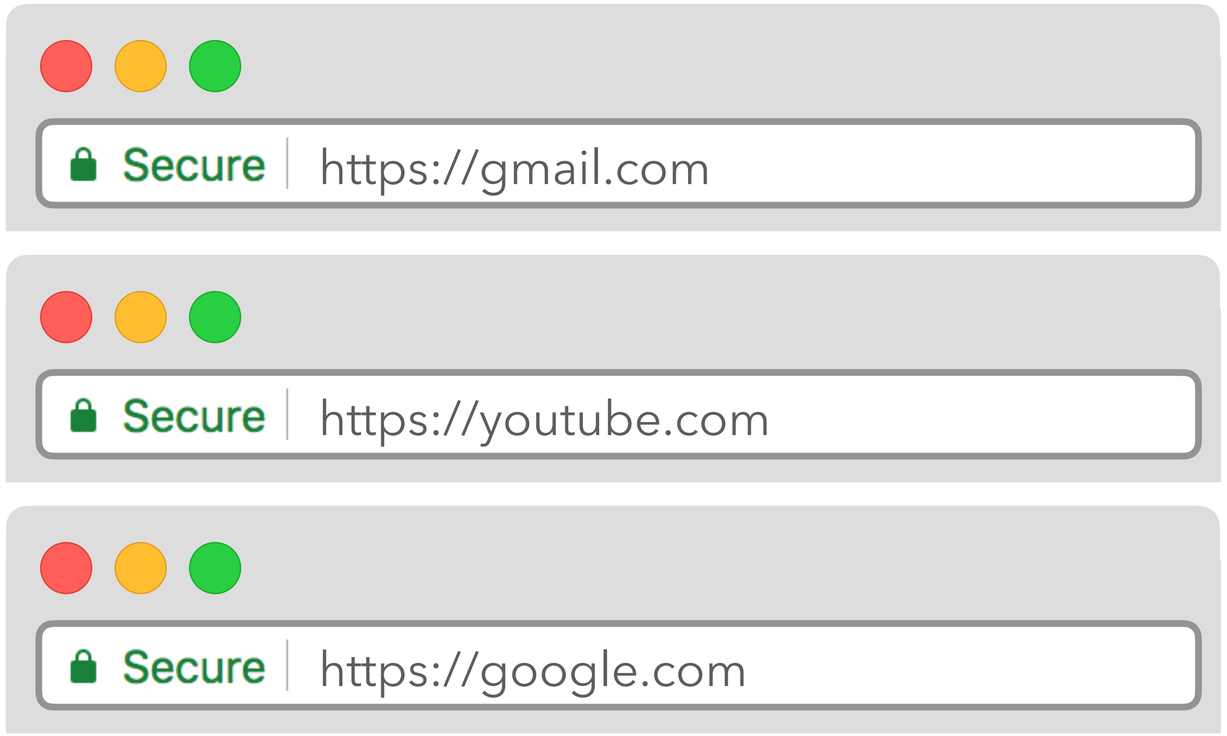
Non-Phishable MFA

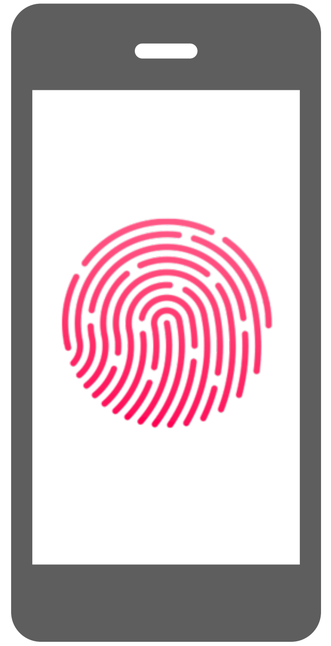
WebAuthn

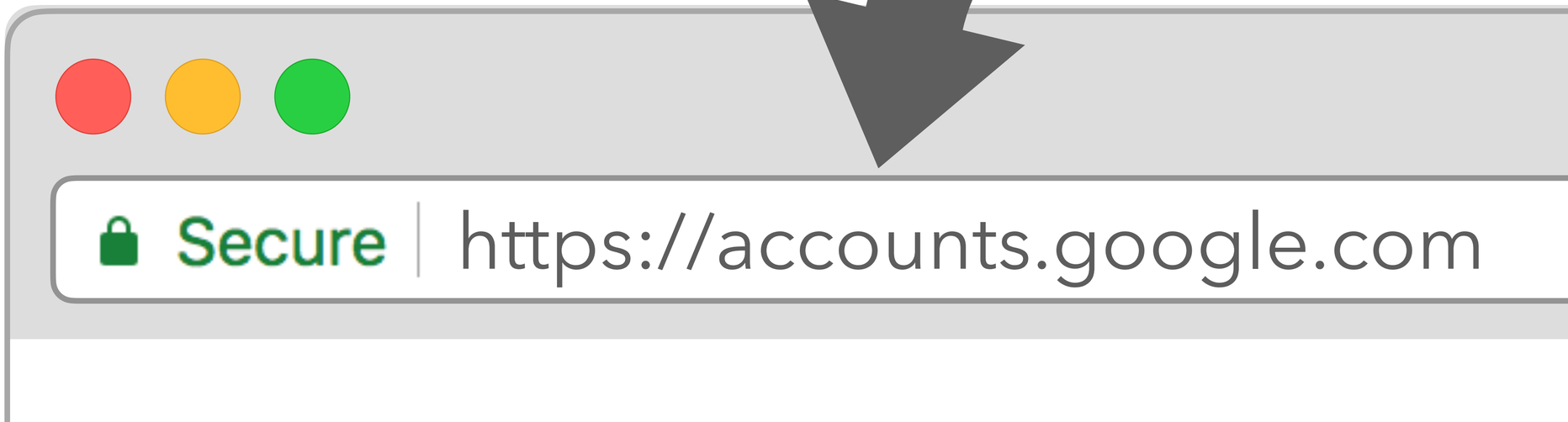
fido™


Secure
https://google.com

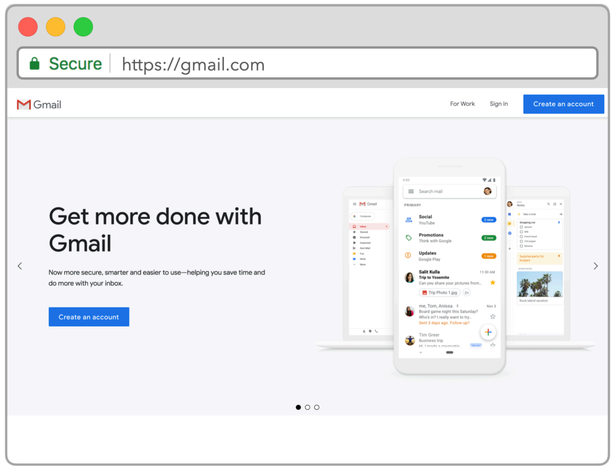

Secure
https://apple.com
Secure
https://google.com

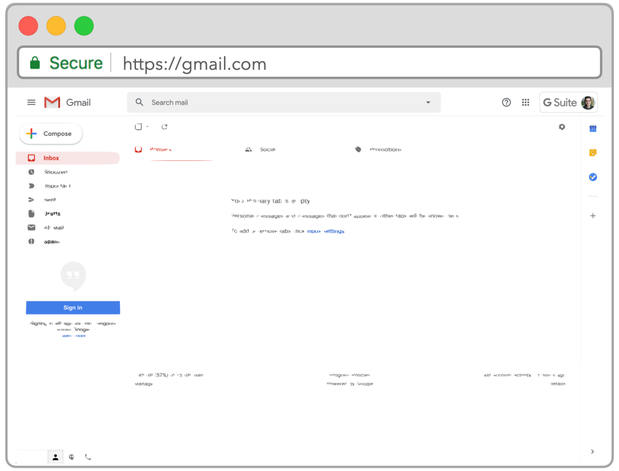

Secure
https://gmail.com
Secure
https://youtube.com
Secure
https://google.com



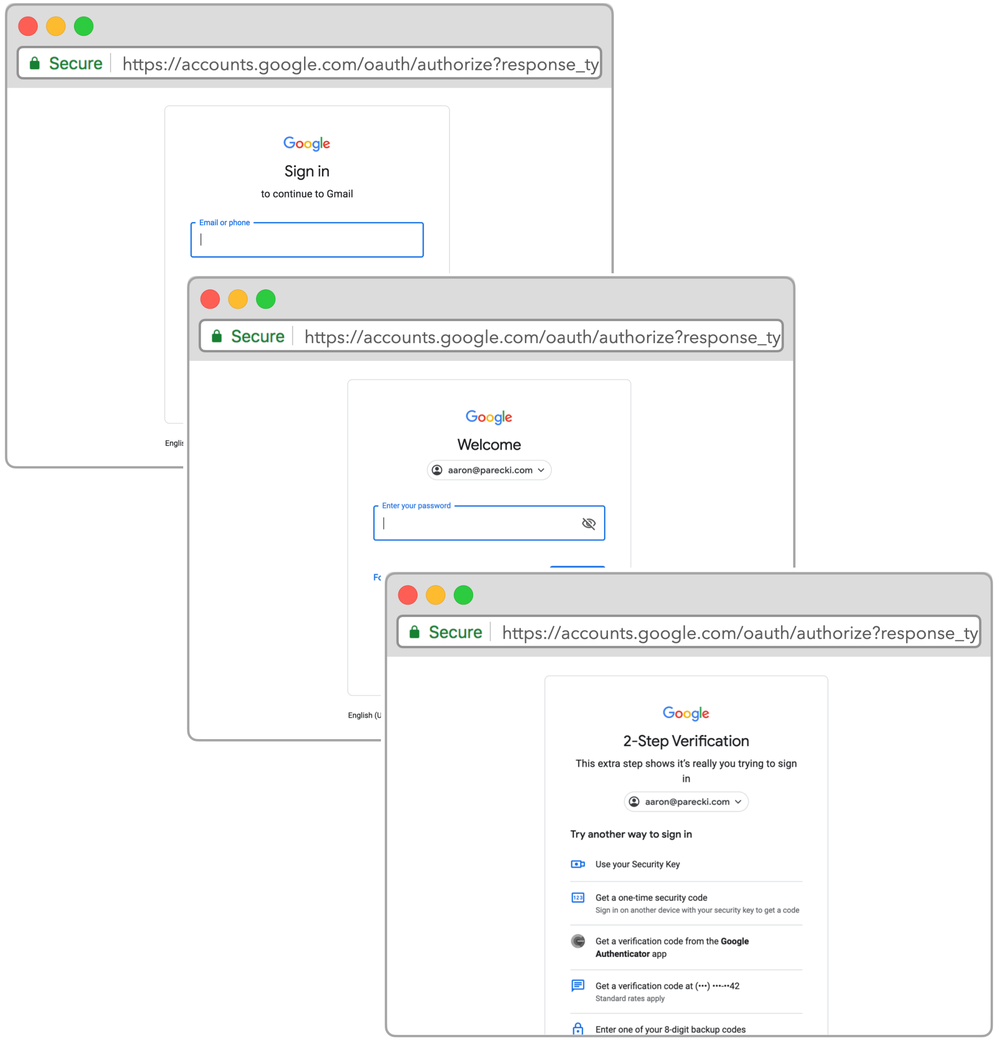

Secure
https://accounts.google.com

Application



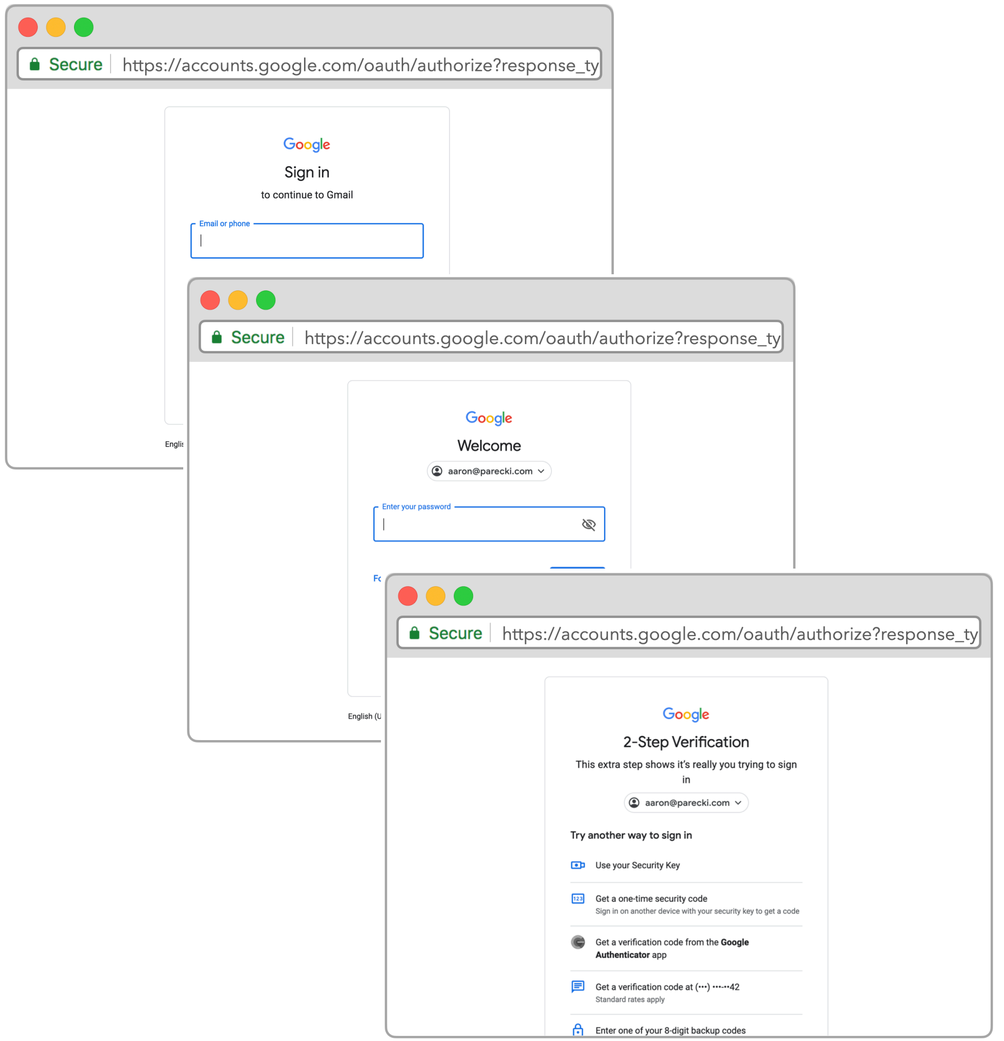


OAuth Server



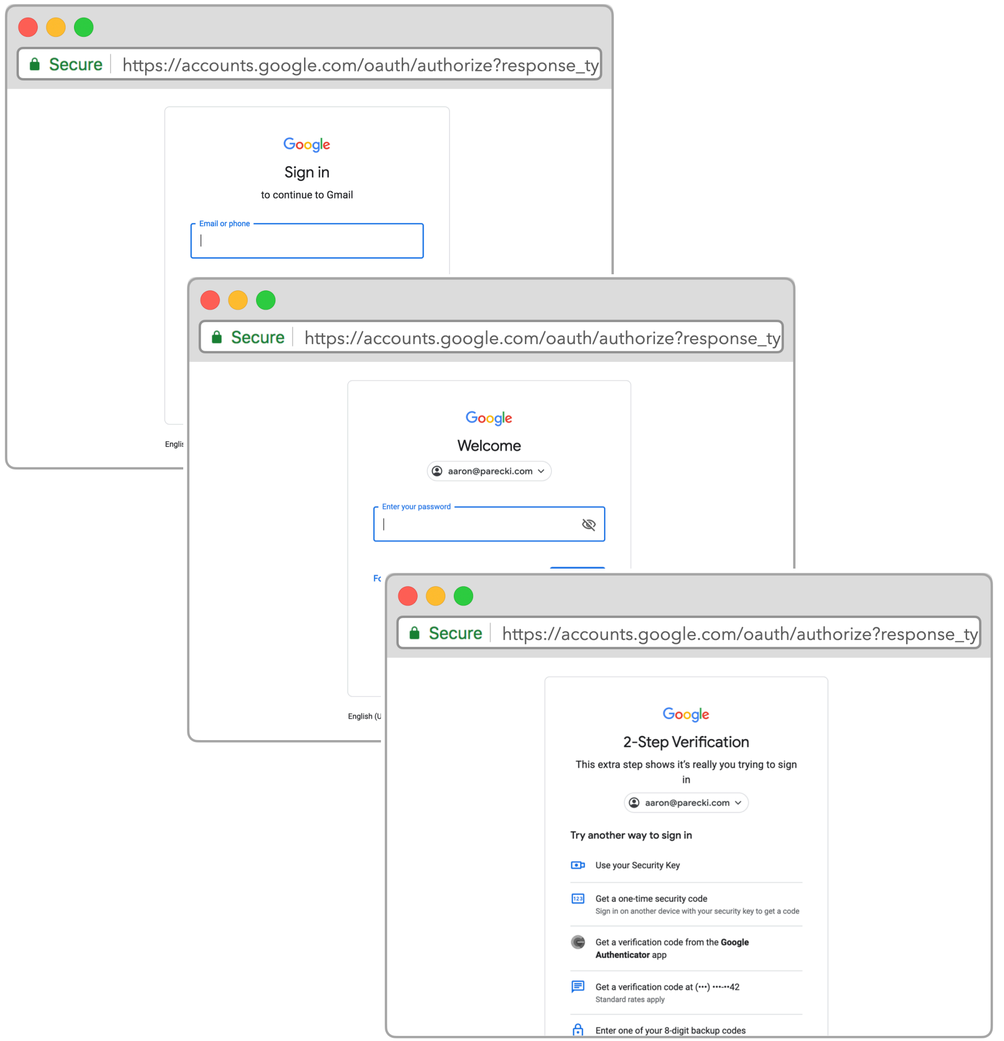
Application

OAuth Server

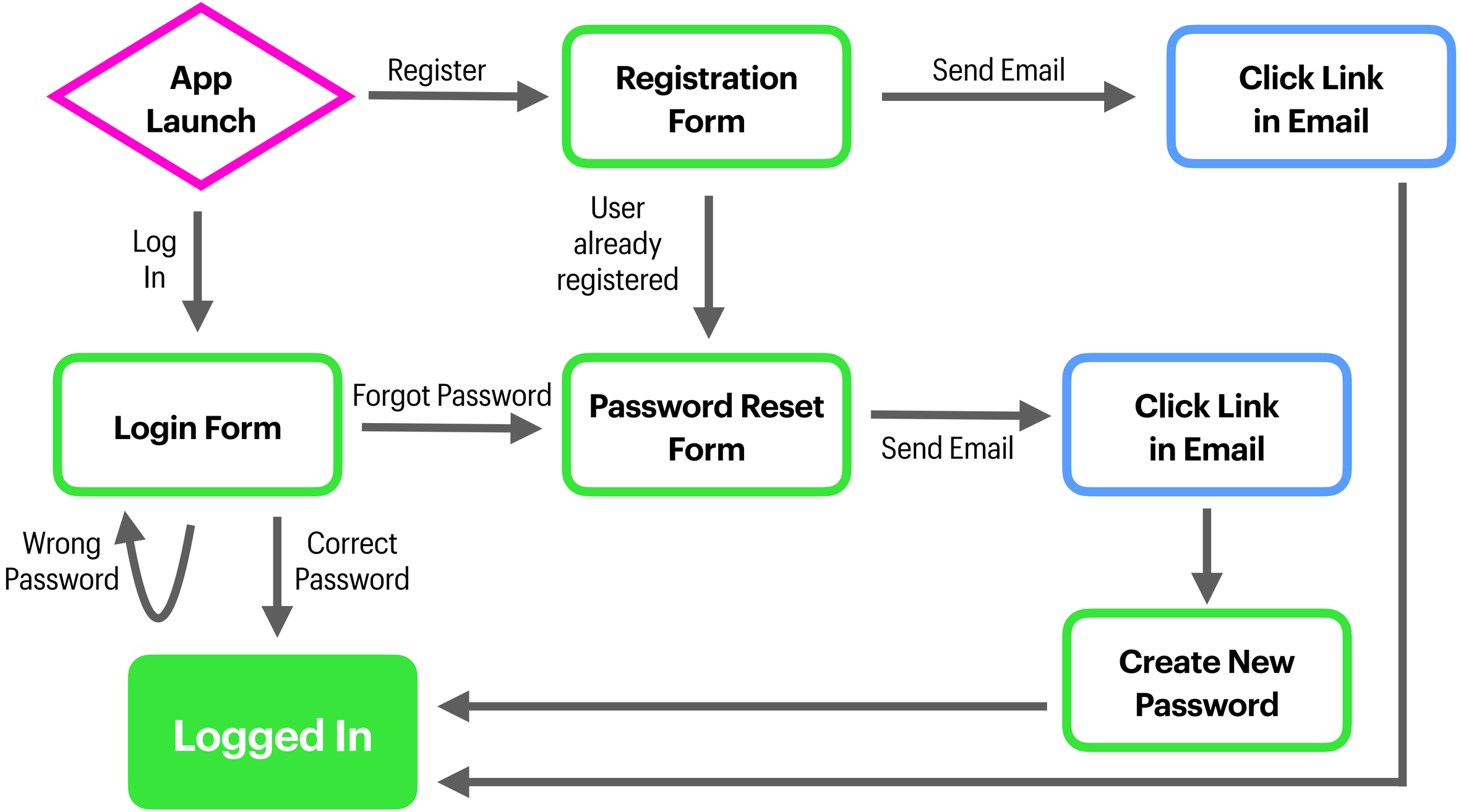


Application

OAuth Server

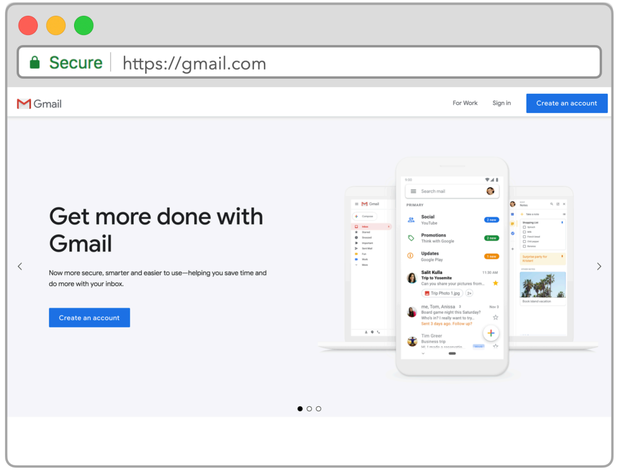


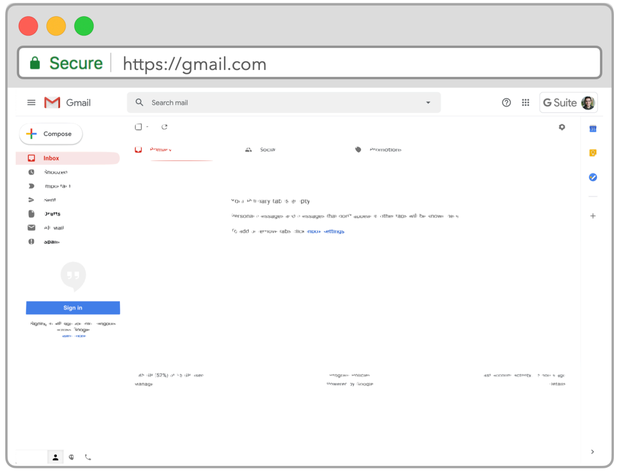
REGISTRATION AND ACCOUNT RECOVERY

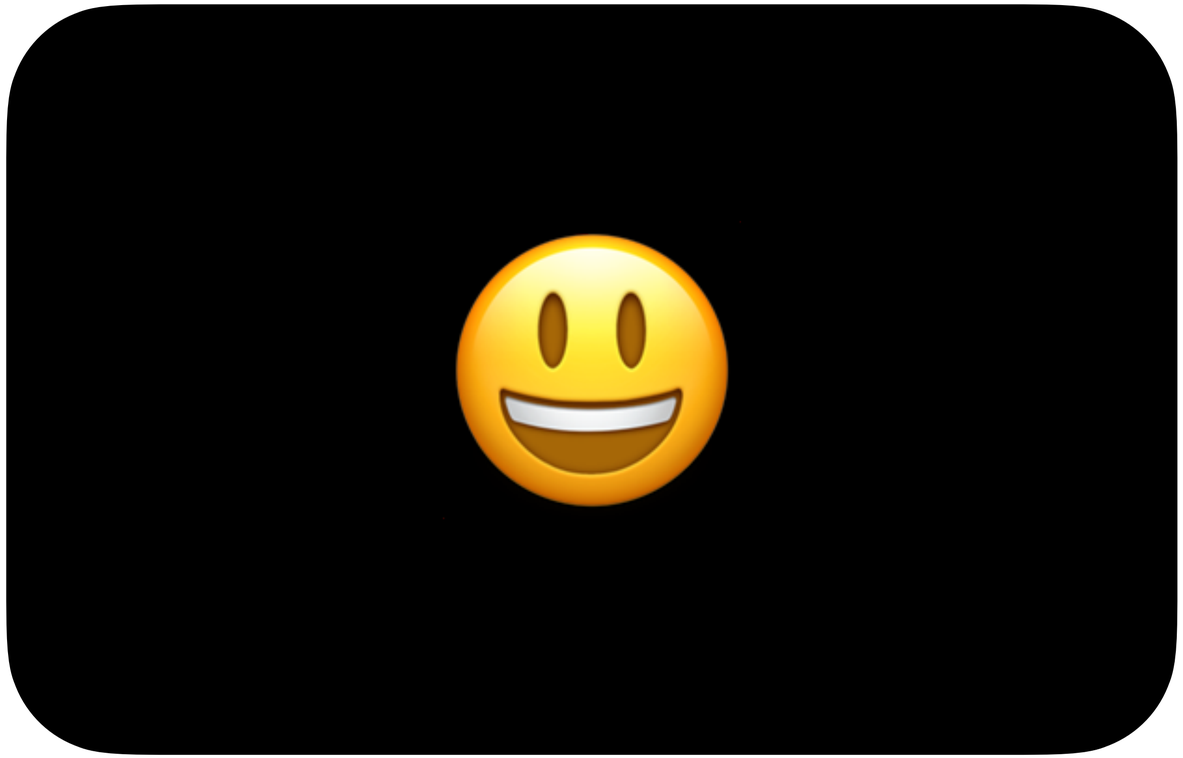

App Launch
Register
Registration Form
Send Email
Click Link in Email
Log In
User already registered
Login Form
Forgot Password
Password Reset Form
Send Email
Click Link in Email
Wrong Password
Correct Password
Create New Password
Logged In

Application

OAuth Server








Sign in with Facebook
Sign in with Google
Sign in with LinkedIn
Sign in with Twitter
IS THIS OAUTH?

OAUTH PROVIDES ACCESS TO DATA


OAUTH
OAUTH

WHAT IS THIS THEN?

+ custom stuff

+

Accessing APIs

Identification

AVOIDS HANDLING PASSWORDS

ENABLES STRONG MULTI-FACTOR AUTH

OFFLOADS COMPLEXITY

GETTING STARTED

oauth.net

specs, extensions and links to resources

oauth.wtf

my video course and book

OAUTH 2.1

OAuth Working Group
Internet-Draft
Intended status: Standards Track
Expires: 8 April 2022

D. Hardt
Hellō
A. Parecki
Okta
T. Lodderstedt
yes.com

5 October 2021

The OAuth 2.1 Authorization Framework
draft-ietf-oauth-v2-1-04

Abstract

The OAuth 2.1 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction

THANK YOU!

@AARONPK
AARONPK.COM
OAUTH.WTF