Sign-In Best Practices

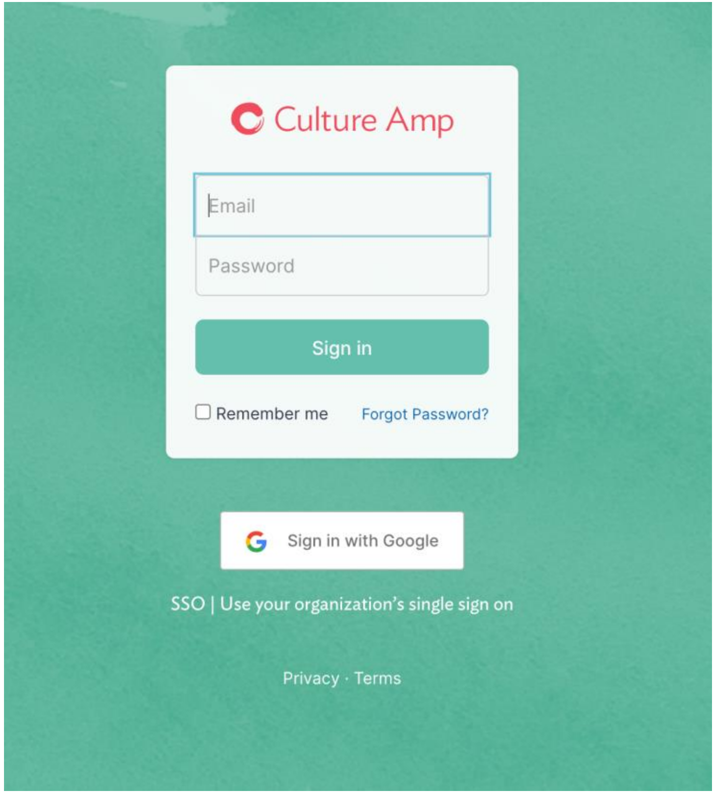
Shannon Clark | Associate UX Designer

April 28, 2021

There are 5 key elements that contribute to creating a great sign-in experience.

1. Clarity in appearance.
2. Clear visual distinction between sign-in and registration.
3. Forgotten password recovery options.
4. Proper error notifications.
5. Remember me options.

1. Clarity in appearance.



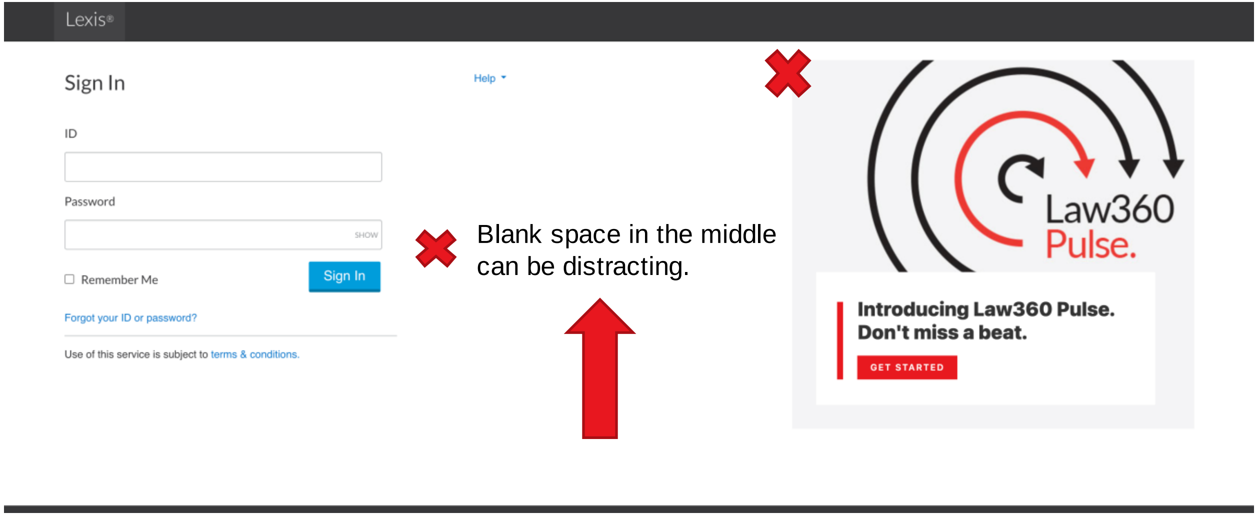
DO

- Keep the login in page simple.
- Insurer users don't become distracted.
- Think of your sign-in screen as a doorway, make the process as quick and steamlined as possible.

★ *Keeps users focused on the task at hand.*

DON'T

Have any kind of distractions on the sign-in page that keeps users from completing their goal



Lexis®

Sign In

Help ▾

ID

Password

SHOW

□ Remember Me

Sign In

Forgot your ID or password?

Use of this service is subject to terms & conditions.

Law360 Pulse.

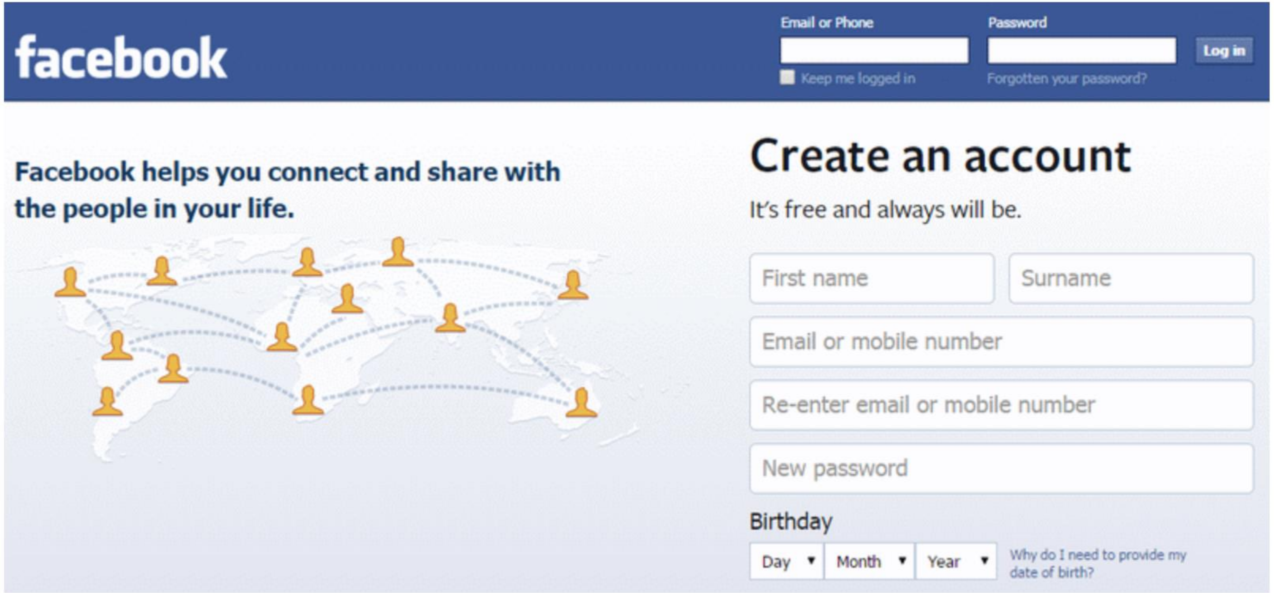
Introducing Law360 Pulse.
Don't miss a beat.

GET STARTED

Blank space in the middle can be distracting.

2. Have visual differences between signing-in and registration.

DO



facebook

Email or Phone

Password

Log in

□ Keep me logged in

Forgotten your password?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name

Surname

Email or mobile number

Re-enter email or mobile number

New password

Birthday

Day ▾ Month ▾ Year ▾

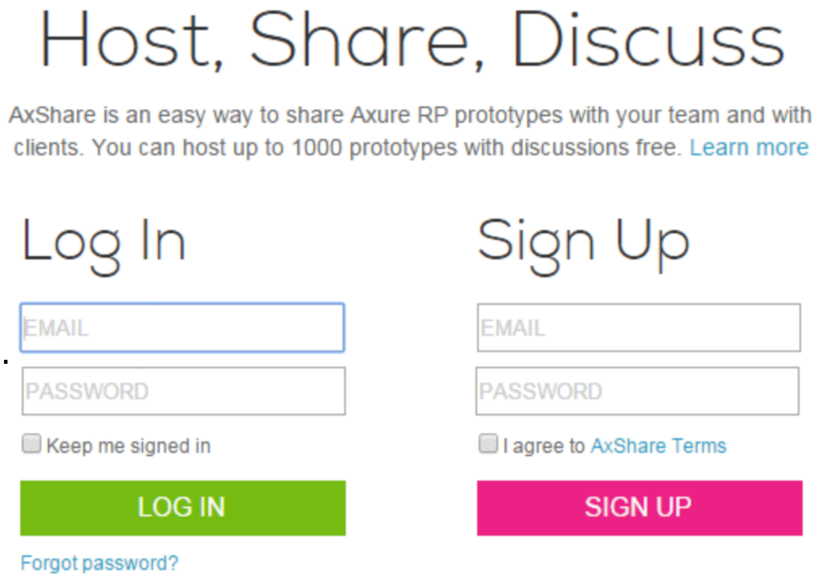
Why do I need to provide my date of birth?

Clear differences between signing in and creating a new account.

★ *Reduces creating unnecessary multiple accounts*

DON'T

Don't confuse users between SIGN UP and SIGN IN!
Minimize the chance users accidently attempt to login in via the registration form.



Host, Share, Discuss

AxShare is an easy way to share Axure RP prototypes with your team and with clients. You can host up to 1000 prototypes with discussions free. Learn more

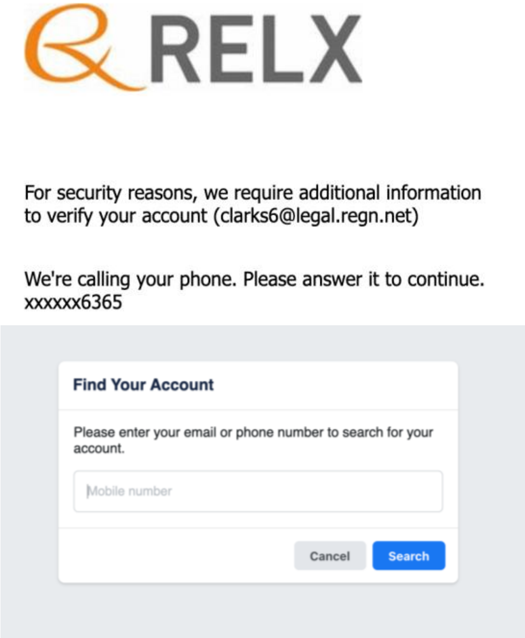
✖ Users can easily become confused and overwhelmed.

✖ Don't put the two besides each-other.

3. Forgotten password recovery options.

DO

Make the password recovery process quick and accessible for the user.



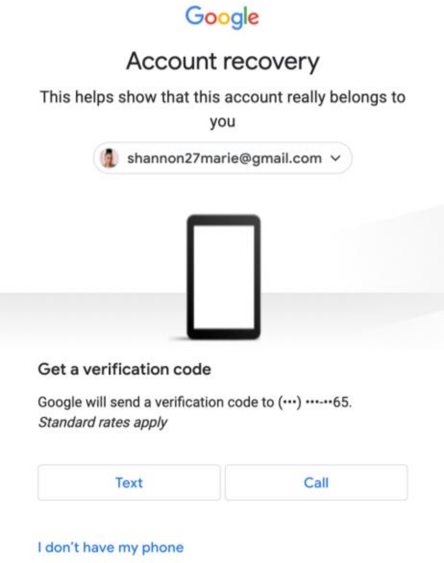
For security reasons, we require additional information to verify your account (clarks6@legal.regn.net)

We're calling your phone. Please answer it to continue.
xxxxxx6365

Find Your Account

Please enter your email or phone number to search for your account.

Mobile number



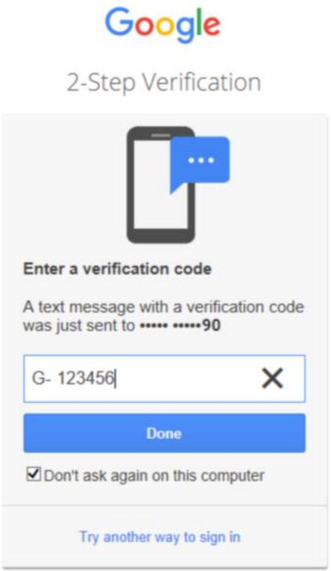
Account recovery

This helps show that this account really belongs to you

shannon27marie@gmail.com

Get a verification code

Google will send a verification code to (•••) •••-••65.
Standard rates apply



2-Step Verification

Enter a verification code

A text message with a verification code was just sent to ••••• •••••90

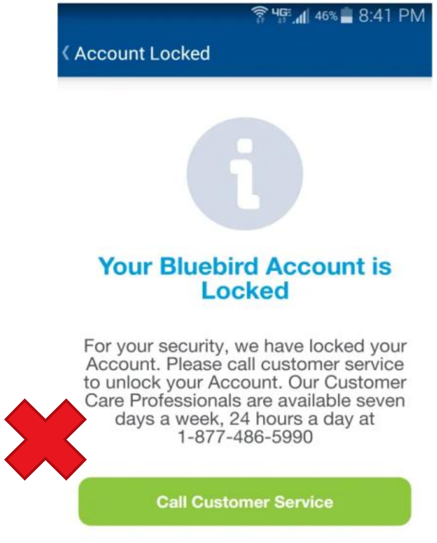
G- 123456

☑ Don't ask again on this computer

★ *Reduce user stress & get them back into using the product.*

DON'T

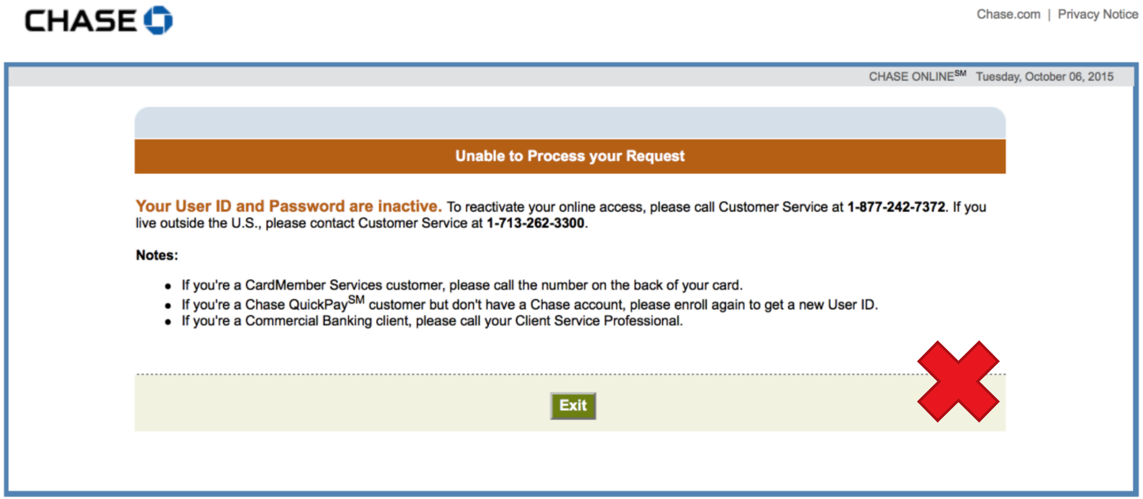
Make the user have-to call customer support to reset their password.



Your Bluebird Account is Locked

For your security, we have locked your Account. Please call customer service to unlock your Account. Our Customer Care Professionals are available seven days a week, 24 hours a day at 1-877-486-5990

A screen you never want to see!



CHASE
Chase.com | Privacy Notice
CHASE ONLINE℠ Tuesday, October 06, 2015

Unable to Process your Request

Your User ID and Password are inactive. To reactivate your online access, please call Customer Service at **1-877-242-7372**. If you live outside the U.S., please contact Customer Service at **1-713-262-3300**.

Notes:

- If you're a CardMember Services customer, please call the number on the back of your card.
- If you're a Chase QuickPay℠ customer but don't have a Chase account, please enroll again to get a new User ID.
- If you're a Commercial Banking client, please call your Client Service Professional.

★ *Consider a 2-step verification process to save users and customer support time, as well as improving security.*

Password recovery options

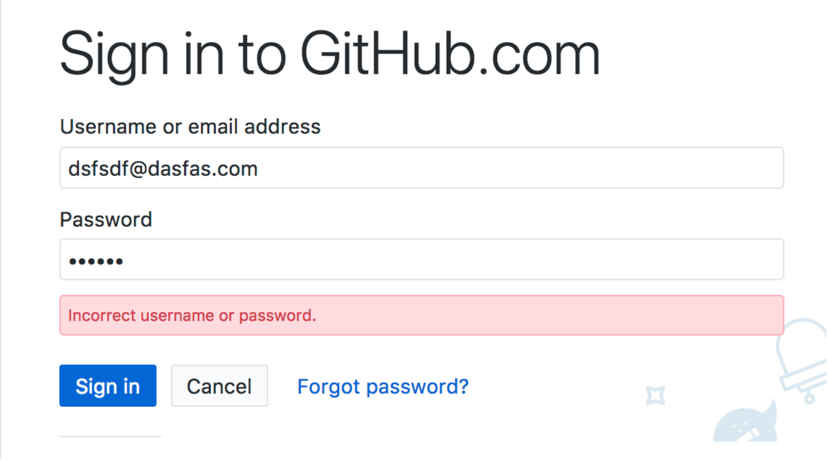
Option	Pros	Cons
Email the original password	Easy for the user to input	Large security risk
Email a new random password	Easy for the user to input	Users still have to create a new password that they could forget
Email a limited time password reset link	More secure than emailing a random password	Still uses the email as the dominant identity
Secret questions	User can rely more on the security question than the password they create	Many of the answers to these questions can be found easily
Reset via phone	Easy because people typically have their phones and it is harder to hack	It means users would have to have the device that it is connected to

Source

4. Proper error notifications

DO

Use Inline Error Messages immediatley alerting users to issues in context avoiding account lockout and uneccessary customer support calls

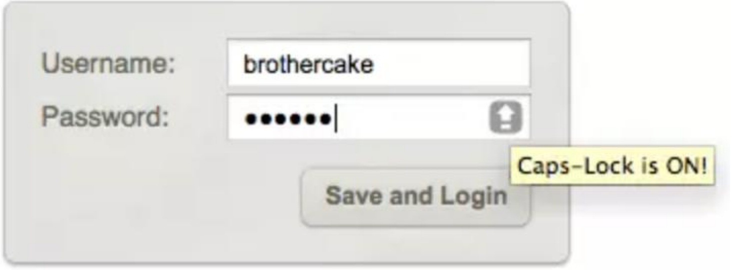


Sign in to GitHub.com

Username or email address: dsfsdf@dasfas.com

Password: ••••••

Incorrect username or password.



Username: brothercake

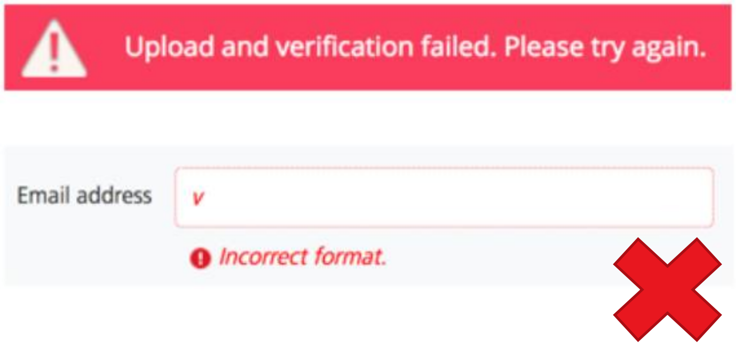
Password: ••••••

Caps-Lock is ON!

Make sure the error notification information is specific.

★ *Reduce user lock outs and frustration*

DON'T



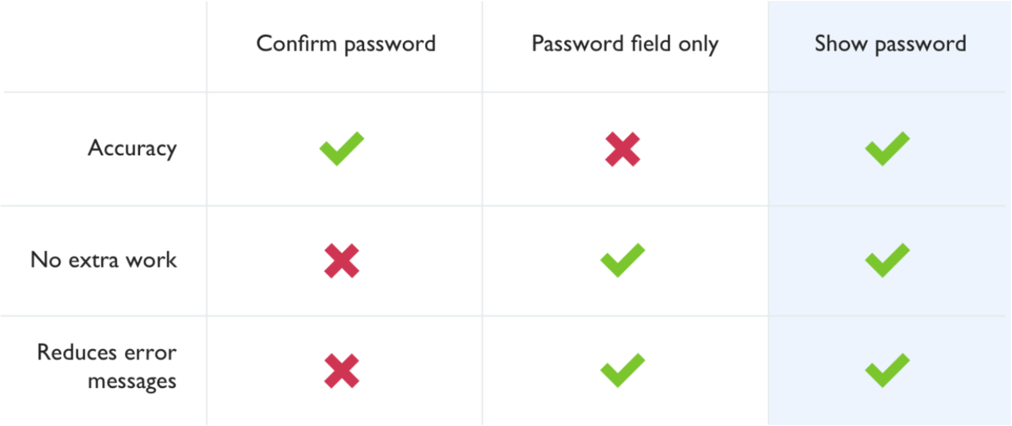
Upload and verification failed. Please try again.

Email address: v

Incorrect format.

Your error message is a conversation with your user — it should sound like they’ve been written for humans. Make sure your error message is polite, understandable, friendly and jargon-free.

Give users the option to view their password.

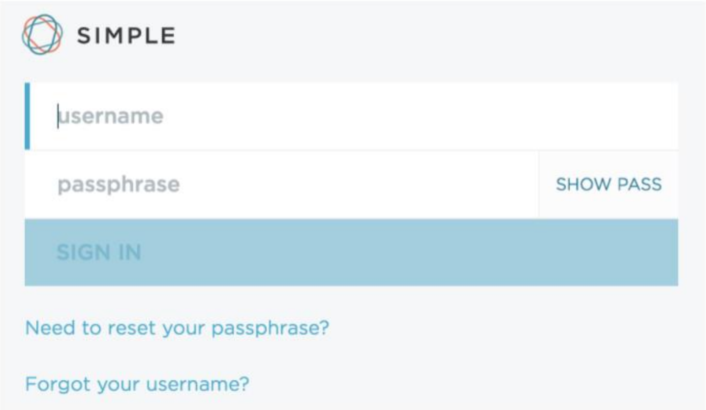


	Confirm password	Password field only	Show password
Accuracy	✓	✗	✓
No extra work	✗	✓	✓
Reduces error messages	✗	✓	✓

- It reduces mistyped passwords
- Doesn’t make users do unnecessary work
- Allows the user to correct mistakes before submitting

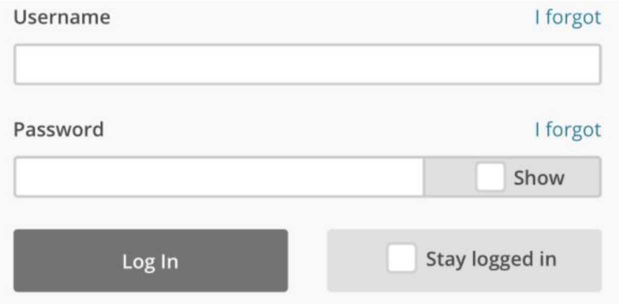
Patterns that work

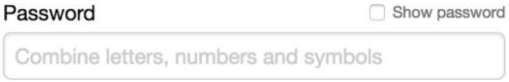
Showing password checkbox: The clearest option is to include a checkbox near the password field that allows the user to view the password field when checked.

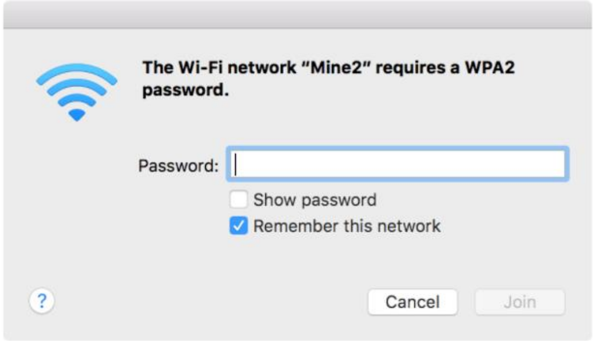


Need to reset your passphrase?

Forgot your username?







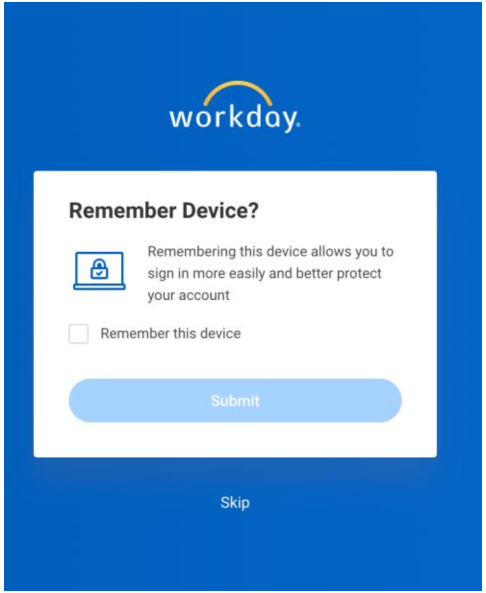
The Wi-Fi network "Mine2" requires a WPA2 password.

Show password link. Another option is to use a label that toggles from "Show" to "Hide" when the user shows and hides the password text.

5. Remember me options

DO

Allow users to let the system 'Remember Me'

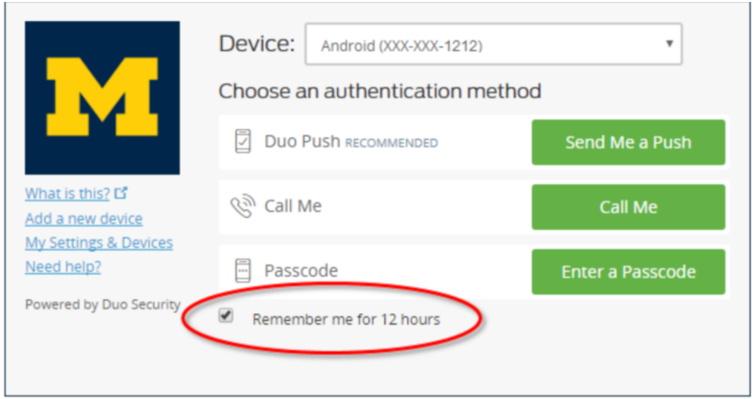


Remember Device?

Remembering this device allows you to sign in more easily and better protect your account

□ Remember this device

By directing users to and implementing a 'Remember Me' option, users won't be prompted for a **two-factor authentication** method over the designated period of time using the same computer and web browser.



Device: Android (XXX-XXX-1212)

Choose an authentication method

☑ Remember me for 12 hours

★ *Reduces logins, login errors, user frustration and delays in accessing product.*

Google 2-Step Verfication

How it Works

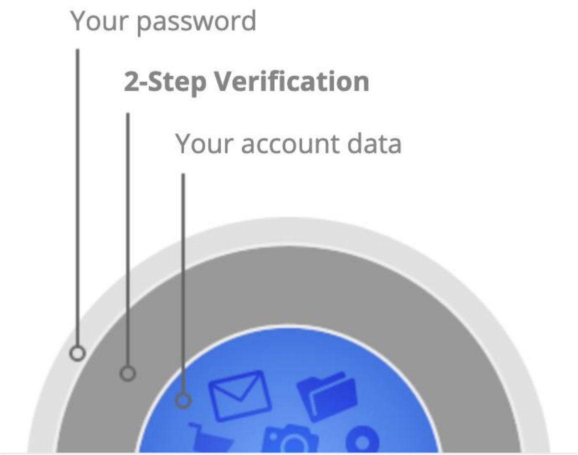
1. **You'll enter your password**

   a. Whenever you sign into Google, you'll enter your password as usual.

2. **You'll be asked for something else**

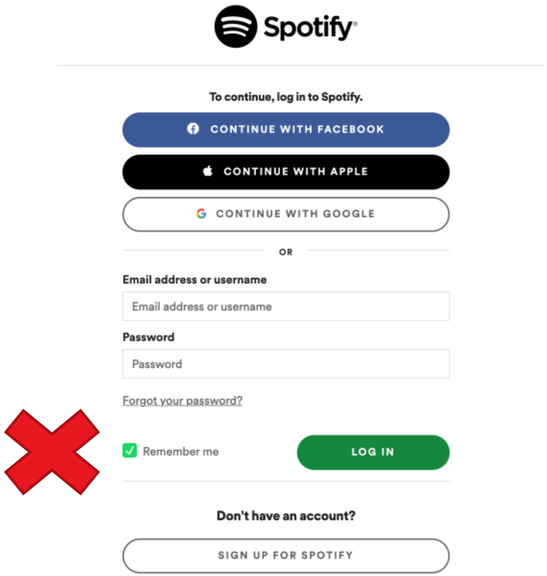
   a. Then, a code will be sent to your phone via text, voice call, or our mobile app. Or, if you have a Security Key, you can insert it into your computer's USB port.

An extra layer of security
Most people only have one layer – their password – to protect their account. With 2-Step Verification, if a bad guy hacks through your password layer, he'll still need your phone or Security Key to get into your account.



DON'T

Force the user to stay signed in. Keep the box unchecked until they decided upon login to check it.



To continue, log in to Spotify.

☑ Remember me

Don't have an account?

When signing into Spotify users have-to uncheck the remember me check box.

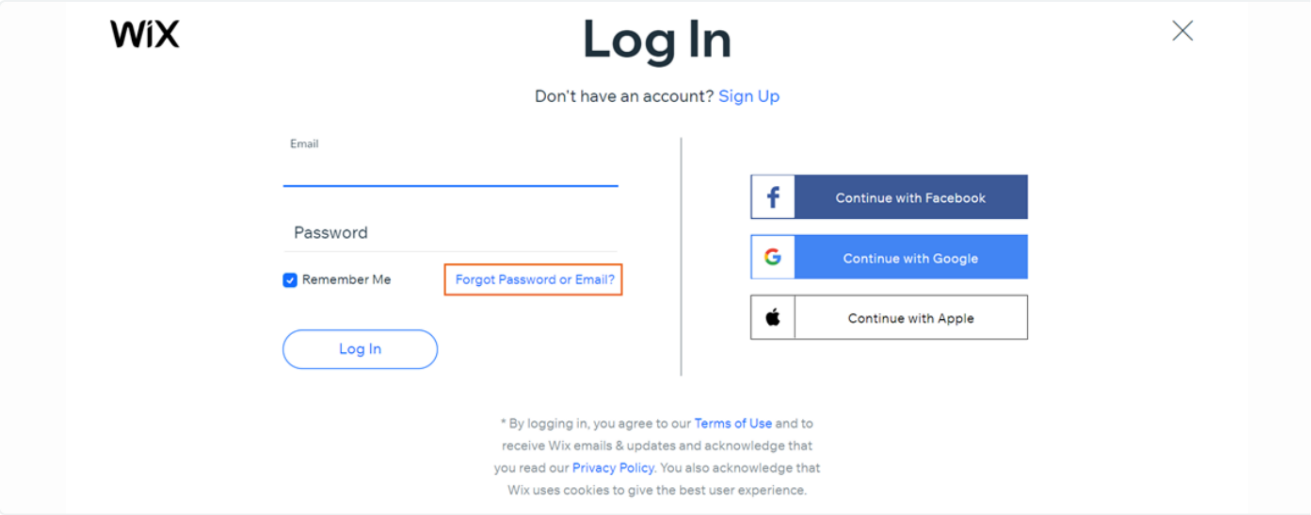
If not, their information will be stored onto the device that they logged in to.

This could be a problem when users are logged in using a public device.

Risk of Passwords that are too strict

When users have-to think of a password that is out of their typical password set in order to fit a set of credentials, they often have trouble remembering what it is.

- When looking at ecommerce sites, there was an 18% dropout rate if a user was not able to remember their password (Source)



* By logging in, you agree to our Terms of Use and to receive Wix emails & updates and acknowledge that you read our Privacy Policy. You also acknowledge that Wix uses cookies to give the best user experience.

☆ External Logins and CRO (Conversion Rate Optimization)

- **86% of users report being bothered by having to create new accounts on websites-** A report from Gigya revealed that the leading reason people use social authentication is to avoid having to fill out online registration forms.

- **77% of users believe social login is a good registration solution…**

  …and should be offered by any website, according to the aggregated research published by WebHostingBuzz.

- **92% of users will leave a site instead of resetting or recovering login info according to** a poll by Blue Research.

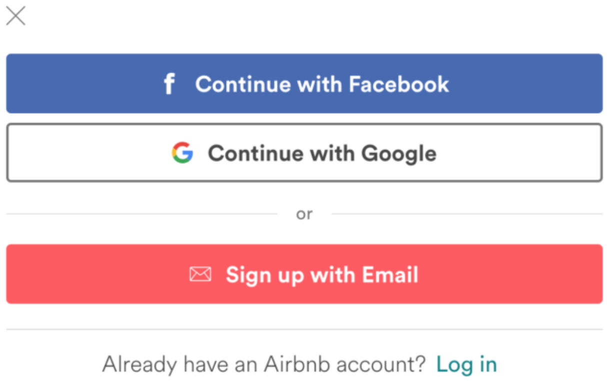
- **8% of users admit to entering incomplete or incorrect data on registration forms**

  in that same survey by Blue, it was found that an alarming majority of users enter the wrong data.

Source

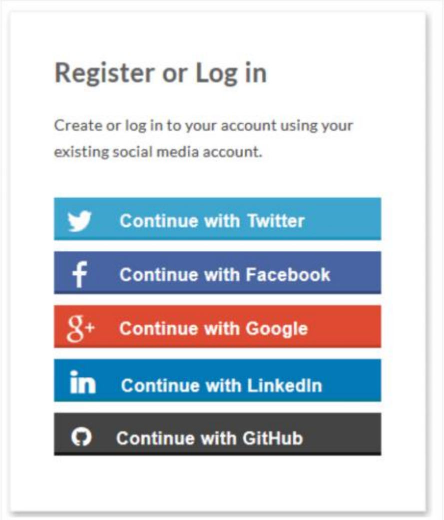
External Sign-In Options

Using external sign in options keeps users from having to remember multiple passwords for different sign-ins.



Already have an Airbnb account? Log in

Source: Airbnb. They allow users to continue with Facebook & Google.



Register or Log in

Create or log in to your account using your existing social media account.

★ *Reduced user login times & improved mobile access*

Advantages

- **Streamlined sign-up**: Third-party web page logins via Facebook or Google accounts typically involve clicking just a few buttons. This creates a much faster path to access sites and apps compared to filling out registration forms.

- **Less password reliance**: Password fatigue is real, and besides the inherent vulnerability of password logins, the idea of remembering yet another password puts users off registering for additional sites. Social login means users don’t have to create and keep track of more credentials, lessening password fatigue and login failures.

- **A trustworthy process**: Regardless of the site users are accessing, social sign-on provides a recognizable, uniform method of logging in. Users may feel more at ease sharing their data with new and unknown sites and apps via social networking platforms they already trust.

Disadvantages

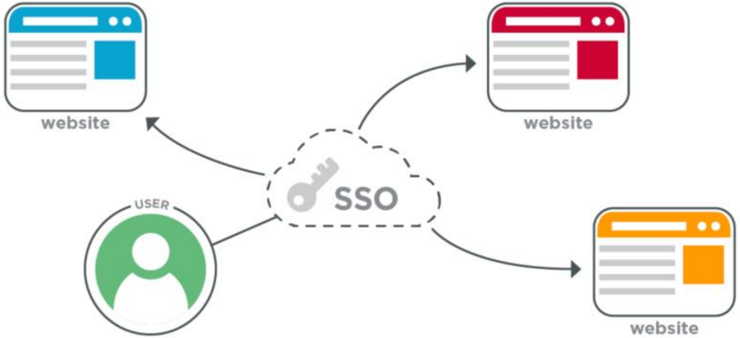
- **Compromised or stolen data**: Social identity providers like Facebook and LinkedIn have faced infamous data breaches over the years, where leaks compromised millions of user accounts at a time.

- **Poor password practices**: Unfortunately, 65% of people report reusing credentials across multiple accounts and sites. If any social login site experiences data theft, users who’ve repeatedly used the same passwords will likely have multiple compromised accounts on their hands. Frequent social login users are those most at risk, as credential leaks jeopardize every app or site login linked to a breached social media account.

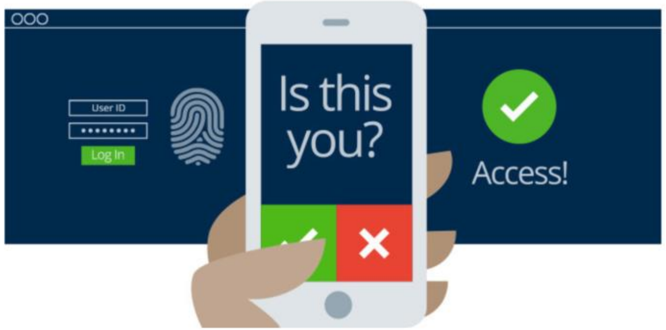
- **Privacy and compliance**: Organizations implementing social login need to be vigilant with regards to privacy, as regulations like the CCPA and GDPR give users legal rights to opt in and out of various data collection and sharing practices. For end users, it’s important to dig into the different permission requests of each platform and determine—before accepting—if each ask is justified.

Single Sign-On vs. MFA (Multiple-Factor Authentication)

- Single-sign on (SSO) is a login method in which users have one set of credentials to access multiple applications. The main benefit of SSO is the streamlined approach. Users can access multiple services without pausing to enter new credentials.



- Multi-factor authentication (MFA) requires users to enter two or more identification factors to access an application. These pieces of information are unique to the user and challenging to guess or replicate. The MFA approach makes it more difficult for hackers or malicious parties to access sensitive data.



Notable Companies

Companies that use SSO Single-Sign-On Practices include…

- Google, LinkedIn, Twitter and Facebook offer popular SSO services that enable an end user to log in to a third-party application with their social media authentication credentials.

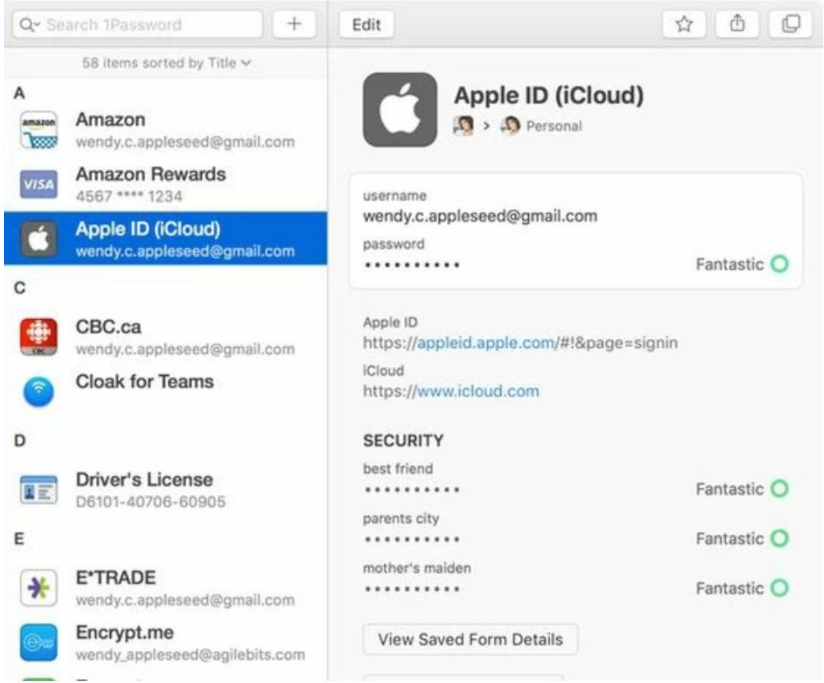
- **Companies that use Multi-factor Authentication (MFA) include…**

BANK OF AMERICA

amazon

Apple

Password Managers



58 items sorted by Title

A

Amazon
wendy.c.appleseed@gmail.com

Amazon Rewards
4567 **** 1234

Apple ID (iCloud)
wendy.c.appleseed@gmail.com

C

CBC.ca
wendy.c.appleseed@gmail.com

Cloak for Teams

D

Driver's License
D6101-40706-60905

E

E*TRADE
wendy.c.appleseed@gmail.com

Encrypt.me
wendy_appleseed@agilebits.com

Apple ID (iCloud)
› Personal

username
wendy.c.appleseed@gmail.com

password
•••••••••• Fantastic

Apple ID
https://appleid.apple.com/#!&page=signin

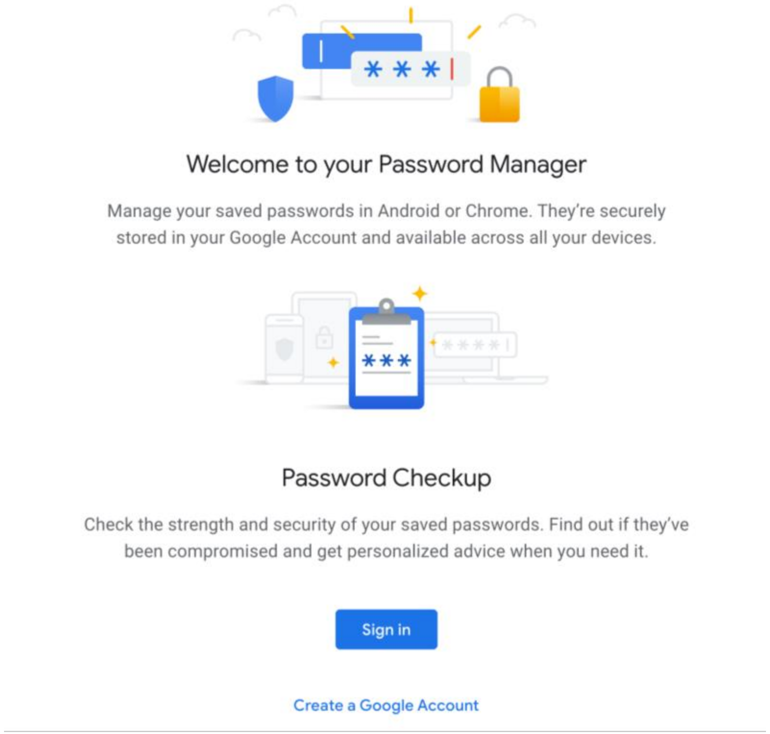
iCloud
https://www.icloud.com

SECURITY

best friend
•••••••••• Fantastic

parents city
•••••••••• Fantastic

mother's maiden
•••••••••• Fantastic



Welcome to your Password Manager

Manage your saved passwords in Android or Chrome. They're securely stored in your Google Account and available across all your devices.

Password Checkup

Check the strength and security of your saved passwords. Find out if they've been compromised and get personalized advice when you need it.

Sources for reference:

- http://www.uxforthemasses.com/login-page/
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3515440/
- https://www.techrepublic.com/blog/software-engineer/five-password-reset-options-for-online-apps/
- https://duo.com/decipher/reality-of-online-account-recovery
- https://support.google.com/chrome/a/answer/6080900?hl=en
- Impact of Single Sign-on Adoption in an Assessment Triage Un... : JONA: The Journal of Nursing Administration (lww.com)
- A_Survey_on_Single_Sign-On_Techniques.pdf
- The password thicket: technical and market failures in human authentication on the web (preibusch.de)
- Account ‘Sign Up’: Ask to Confirm E-mail, Not Password – Articles – Baymard Institute
- For Returning Users, Overly Strict Password Requirements Can Lead to an 18% Abandonment Rate – Articles – Baymard Institute

Continued.....

- https://uxmovement.com/forms/16-innovative-ux-practices-to-simplify-logins/
- https://uxdesign.cc/designing-a-user-friendly-login-25855ae0cc88
- https://www.justinmind.com/blog/20-inspiring-website-login-form-pages/
- https://wpamelia.com/login-page-design/
- https://designsystem.digital.gov/templates/authentication-pages/sign-in/
- https://uxdesign.cc/15-rules-of-user-sign-in-experience-ae9011d04ee3
- https://ux.stackexchange.com/questions/134791/pros-and-cons-of-having-register-login-vs-only-login
- https://www.mockplus.com/blog/post/sign-up-login-design-practices
- https://www.techradar.com/best/password-recovery-solutions
- https://uxmovement.com/forms/why-remember-me-on-logins-should-be-the-default/
- https://pointsmilesandmartinis.boardingarea.com/2015/10/anyone-else-locked-out-of-chase-online-account/

- https://www.travelsummary.com/bluebird-accounts-locked/
- https://designsmarts.co/show-password/
- https://www.sitepoint.com/better-passwords-3-caps-lock-warnings/#:~:text=The%20idea%20is%20simply%20that,protects%20against%20entering%20unintended%20capitals.
- https://www.google.com/search?q=caps+lock+error+messages&sa=X&ved=2ahUKEwjl9svzr5zwAhXtGFkFHY2LDMYQ7xYoAHoECAEQMA&biw=1680&bih=801
- https://designsmarts.co/show-password/
- https://fortifiedhealthsecurity.com/blog/single-sign-on-vs-mfa-do-you-know-the-difference/
- https://www.okta.com/blog/2020/08/social-login/
- https://cxl.com/blog/social-login/#1-86-of-users-report-being-bothered-by-having-to-create-new-acco

Notes from meeting

- Add the benefits to each improvements & recommendation.
- Rearrange the eternal side from number 3 to number 6. (Reason being because we're not sure of the amount of our users will find it useful.)
- Research the behind the necessary inclusion of e-mail addresses vs usernames when signing-in
- Password recovery methods (Password Authentication)

Hi Namit,
Please see my answers below in red.

- What's the percentage split for sign on, FSO, password assistance/ forgot password etc. type calls.
- I have attached the data, but based on the data 1/1/2021-current, there were 12,110 ID/PW related calls. Of those 741, we provided an ID. 991, we reset a password. 3679, we resent a Welcome Email containing both the ID and a temporary password. 103, we helped the customer with their Security Q/A, probably to get through the Forgot Password flow. 18, we renamed/reset the user's ID. We don't have a specific breakdown of FSO.

- Few of the products have their unique sign on pages. Do people usually remember and access the products using those or do they usually start from the Research product URL to authenticate.
- Based on the phone calls that I take, most customers start from the research product page, then choose their product through the product switcher.

LexisNexis®

UX

USER EXPERIENCE

Thank you.