GENERAL ASSEMBLY

OAUTH

Zeke Abuhoff

Lead iOS Instructor, General Assembly

OAUTH

LEARNING OBJECTIVES

- Describe the security considerations of authentication
- Explain the purpose of an access token
- Accommodate an authentication flow in an app

OAUTH

SECURITY

Does this sound familiar?

> **We may send you emails in the future about changes to your account.**
> **We will never ask for your account name or password.**

SECURITY

Does this sound familiar?

> **We may send you emails in the future about changes to your account.**
> **We will never ask for your account name or password.**

Standard security stuff when you’re making an account, right?

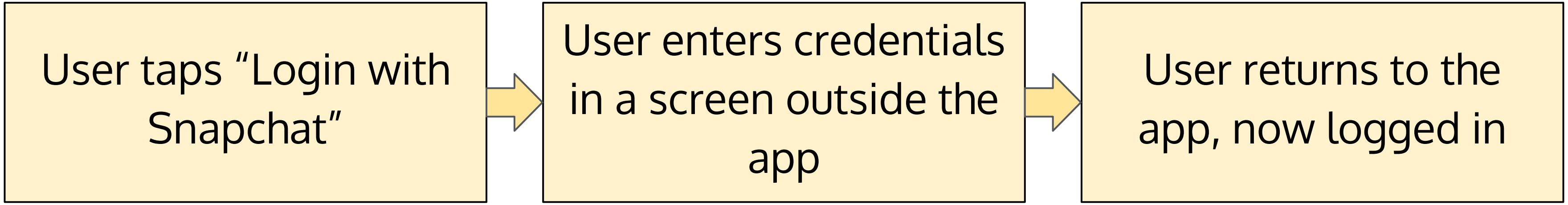
Why do companies say this?

OAUTH 2.0

Your app may have its own account name and password, but users shouldn’t have to trust you with their other credentials.

That’s where **OAuth 2.0** comes in. It’s a standard for authenticating users with a third party service.

Here’s the flow for user authentication:



User taps “Login with Snapchat”

User enters credentials in a screen outside the app

User returns to the app, now logged in

OAUTH 2.0

Like REST APIs, Oauth procedures are detailed in service-specific documenation.

They also are often facilitated by a service-specific **SDK**. An SDK is a software development kit. You can add one to your app to gain prebuilt functionality.

Despite each service being unique, the elements of OAuth tend to be the same.

App ID

A unique string that identifies your app

Application Access Token

A unique string that proves an app is really yours

User Access Token

A unique string that proves you have permission to represent a user

OAUTH PITFALLS

When implementing OAuth, make sure you’re doing the following right:

- Pick the right process for your app (app authorization vs user authorization)
- Check the lifespan of tokens you receive so you’re not trying to use an expired one
- When using an OAuth SDK, make sure it’s properly integrated into your project and that you’re using its methods as intended
- Use the correct documentation (not an outdated version, not the wrong OAuth process)