Session 4: Accounts

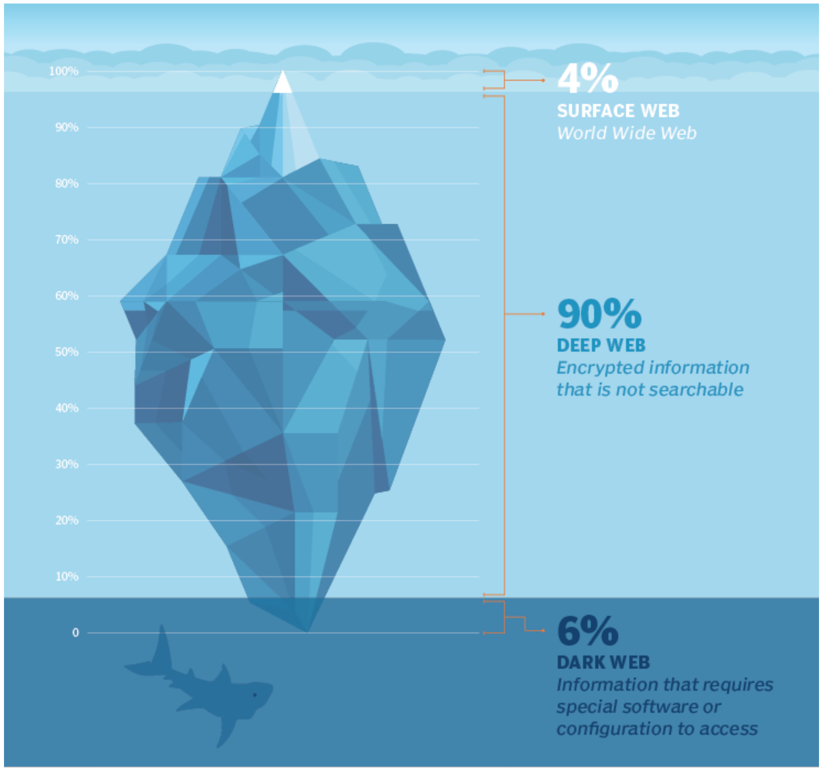
Mastering the Internet
Duke OLLI Spring 2024

David Shamlin

Review of Session 3

- Many Internet sites handle volume of work that are more than one computer can handle
    - Computer **networks** allow large workload volumes to be spread across multiple computers
- A network is a collection of computers connected to each other by **switches**
    - Networks reside in **data centers**
    - Networks are connected to each other by **routers**
- **The Internet is a network of networks!**
- **TCP/IP** is the protocol of the Internet
    - TCP/IP finds the **physical** location of a site on the Internet by translating the site's domain name into it's **IP Address**
    - TCP/IP handles the **packaging** and **routing** of data **packets** across the Internet
- **HTTP(S)** is the protocol of the Web
  HTTP(S) handles the **messages** that pass between a client-side APP and a web server
- An HTTP(S) message is usually comprised of many data packets

What is the Dark Web?



Researchers estimate the average Internet users has between **100 and 200** accounts.

Account: Definition

Internet account means an account created within a bounded system established by an Internet-based service that requires a user to input or store access information in an electronic device in order to view, create, use or edit the user's account information, profile, display, communications of stored data.

— *Law Insider*

A site account is your digital **identify** for that site.

— *David*

Basic Concepts

- “Login” and “logon” are synonyms of “Sign In”

- **Identify**
  The information that represents you when signed in to a site

- **Id / User id**
  A string of characters that is unique to you relative to the scope of the site; some sites use the email address and/or phone number you give when creating your account

- **User Id + Password = Credentials**

- **Authentication**
  The process of verifying your identify with the site; i.e., the act of signing in to a site

- **Authorization**
  The things you are permitted to do on a site after you have successfully signed in

- **Access Token** or Authorization Token
  A cookie that represents your verified identify

- **One-time password (OTP or TOTP)**
  A six to eight digit number used during 2FA/MFA

Sign In Methodologies

1. “Simple” (user id & password)
2. Two-Factor Authentication (2FA)
   aka Multi-Factor Authentication (MFA)
3. Social Sign In
4. Passkeys

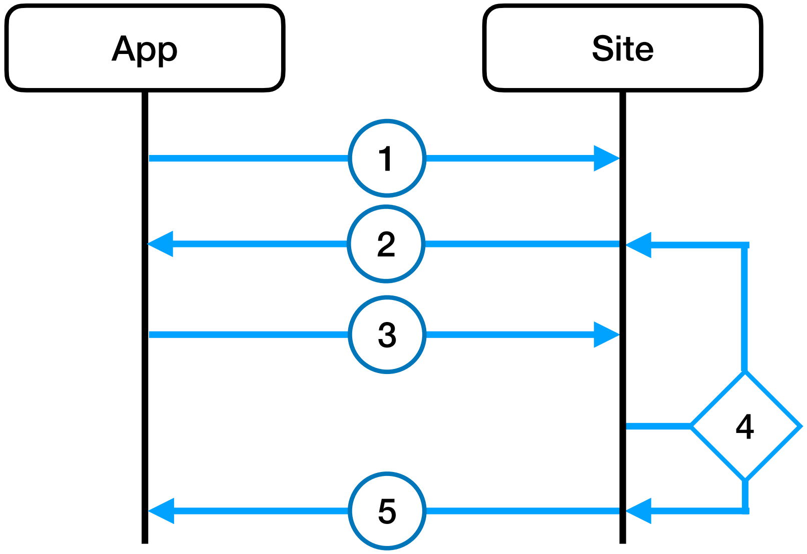
Info typically required when you create an account

- Username
  a.k.a. “user id” or “id” (pronounced *eye-dee*)
- Password
- Email address
  a.k.a. “recovery email” or “backup email”
- Phone number
- First name
- Last name
- Date of birth

- The information you provide when creating an account on a site is your **identity** for the site.
- Together, your user id and password are referred to as your sign-in **credentials.**
- The email address and phone number are used
  - If you forget/loose your password
  - If you choose to also use **two-factor authentication** when signing in
- Site’s use the first & last names given when hey are presenting your content
- A site requires you to give a date of birth when the site has content/features that are restricted to people under a certain age

  Security Tip: Do not give your actual date of birth; instead give some date that is at least 21 years in the past

Basic Sign In

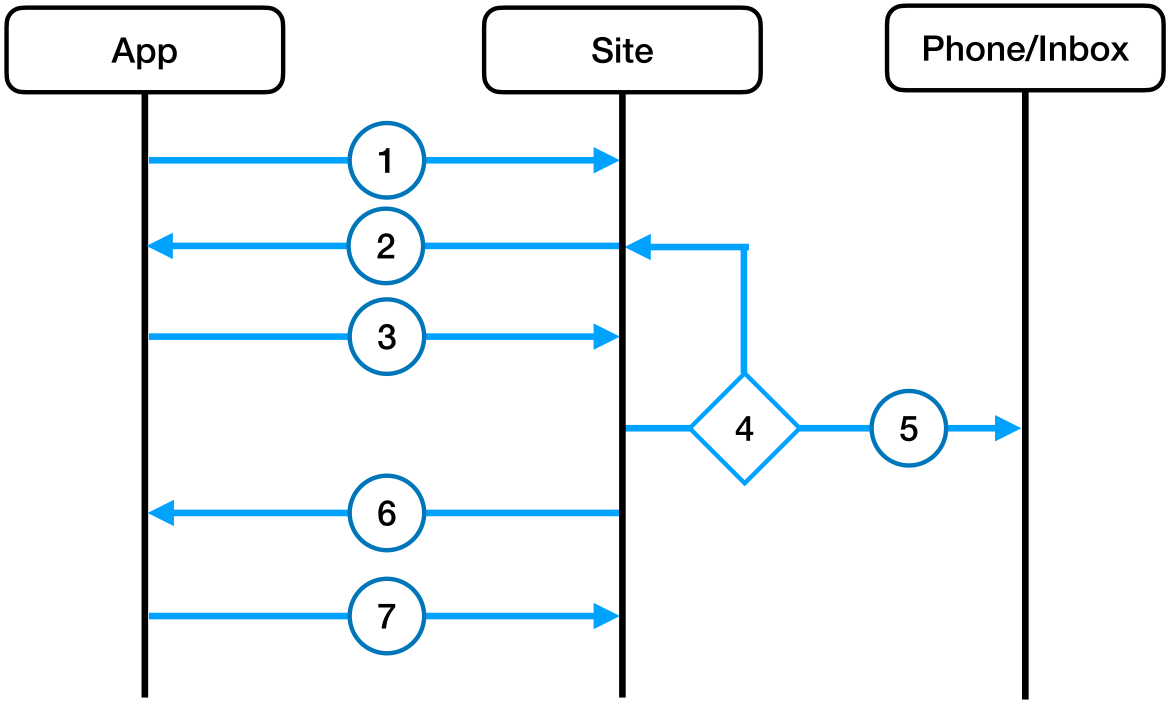


1. You click the sign in button, prompting the site to begin the sign in process
2. The site prompts your user id and password
3. You enter your user id and password (and then click the sign in or submit button)
4. The site compares the id and password values you entered in step 2 against the values it has stored for your user id and password
   - If the id/password values you gave **do not match** the stored values, the site returns to step 2
   - Otherwise the id and password values you gave **do match** what the values the site has stored
5. The site returns an authorization token to your app indicating you have successfully signed in

Two-Factor Authentication (2FA)

- **Definition:** Verifying your identify using a method in addition to providing your user id and password
- Also known as
  - Multi-factor authentication (MFA)
  - Two-step verification
  - Dual-factor authentication
- 2FA provides a higher level of security than user id and password alone
- You often have to explicitly turn on 2FA for an account; you rarely “automatically” (i.e., by default) have 2FA enabled after creating an account
- Not all sites that use accounts support 2FA

2FA sign in using phone number or email

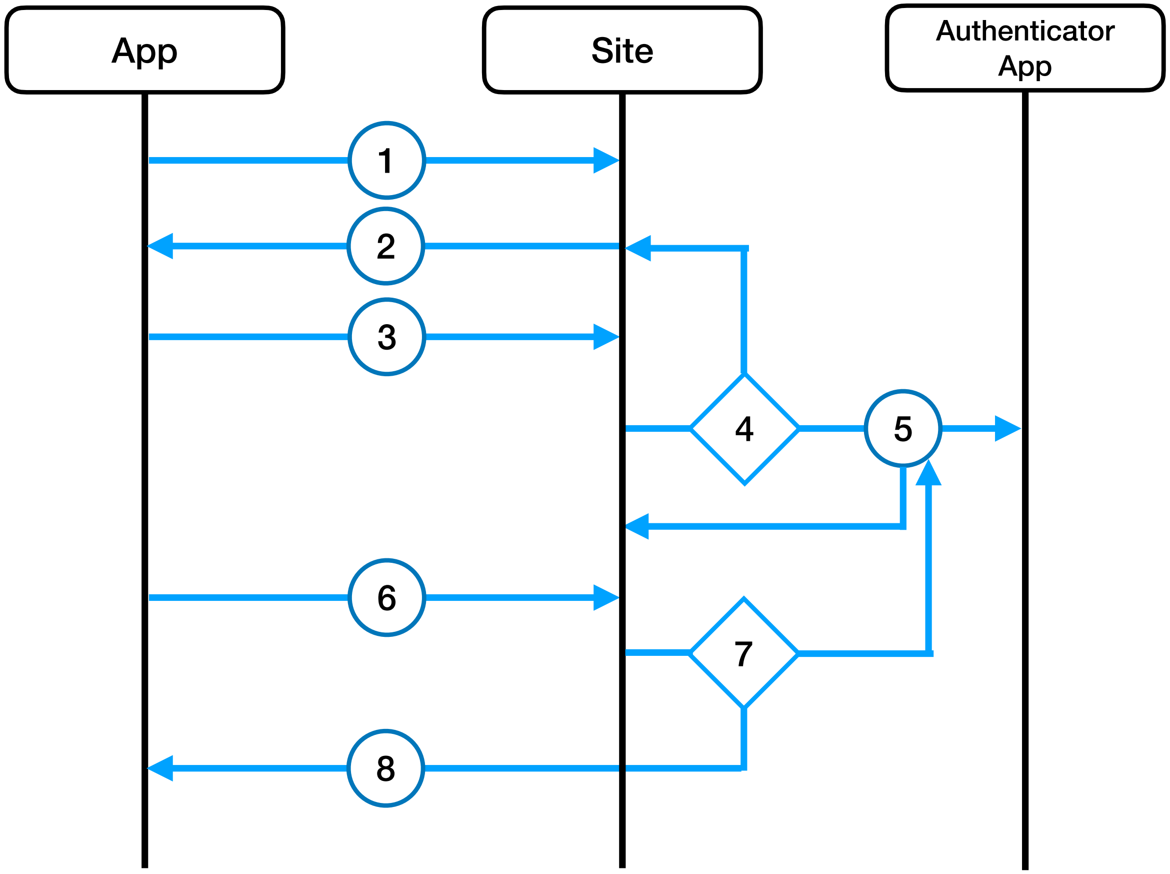


1. You click the sign in button, prompting the site to begin the sign in process
2. The site prompts your user id and password
3. You enter your user id and password (and then click the sign in or submit button)
4. The site compares the id and password values you entered in step 2 against the values it has stored for your user id and password
   - If the id/password values you gave **does not match** the stored values, the site returns to step 2
5. The site sends a TOTP via text or email (your choice)
6. The site prompts you to enter the TOTP
7. You enter the TOTP and click "submit"
   1. If the TOTP you gave **does not match** the code sent to you via text or email, the site returns to step 5
8. The site returns an authorization token to your app indicating you have successfully signed in

Also known as

- Multi-factor authentication (MFA)
- Two-step verification
- Dual-factor authentication

2FA sign in using an authenticator app



1. You click the sign in button, prompting the site to begin the sign in process
2. The site prompts your user id and password
3. You enter your user id and password (and then click the sign in or submit button)
4. The site compares the id and password values you entered in step 2 against the values it has stored for your user id and password
   - If the id/password values you gave does not match the stored values, the site returns to step 2
5. The site and the authenticator app generate the same TOTP
6. The site prompts you to enter the TOTP
7. You enter the TOTP you see in the authenticator app and click “submit”
   1. If the TOTP you gave does not match the TOTP the site generated, the site returns to step 5
8. The site returns an authorization token to your app indicating you have successfully signed in

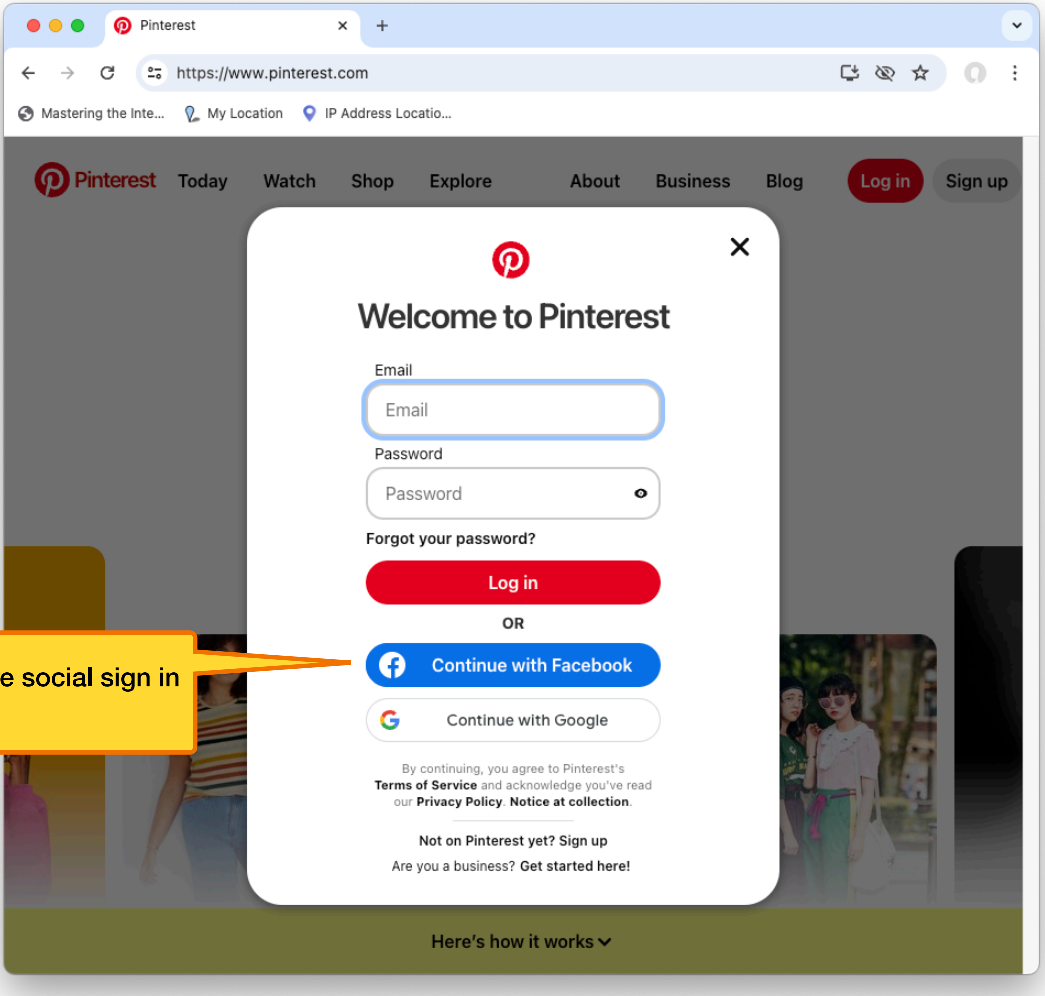
Recommended Authenticator Apps

Product	Help
2FAS	Link
Google Authenticator	Link
Microsoft Authenticator	Link
Authy	Link

- If you want to try any of these, download them from the App Store **on your phone**
- Authenticator apps are only supported on smartphones (to the best of my knowledge)
- Try either Google or Microsoft's first; use one of these authenticator apps to get comfortable using them.
- If don't want to use Google or Microsoft's authenticator app "long term", I recommend Authy over 2FAS
  - 2FAS is an **open source** product; support is likely limited; "help" may also be lacking

Social Sign In

- Method of signing in to a site using sign in information from a “social media site”
- Also known as
  - social login
  - social logon
  - social sign on



By continuing, you agree to Pinterest's **Terms of Service** and acknowledge you've read our **Privacy Policy**. **Notice at collection**.

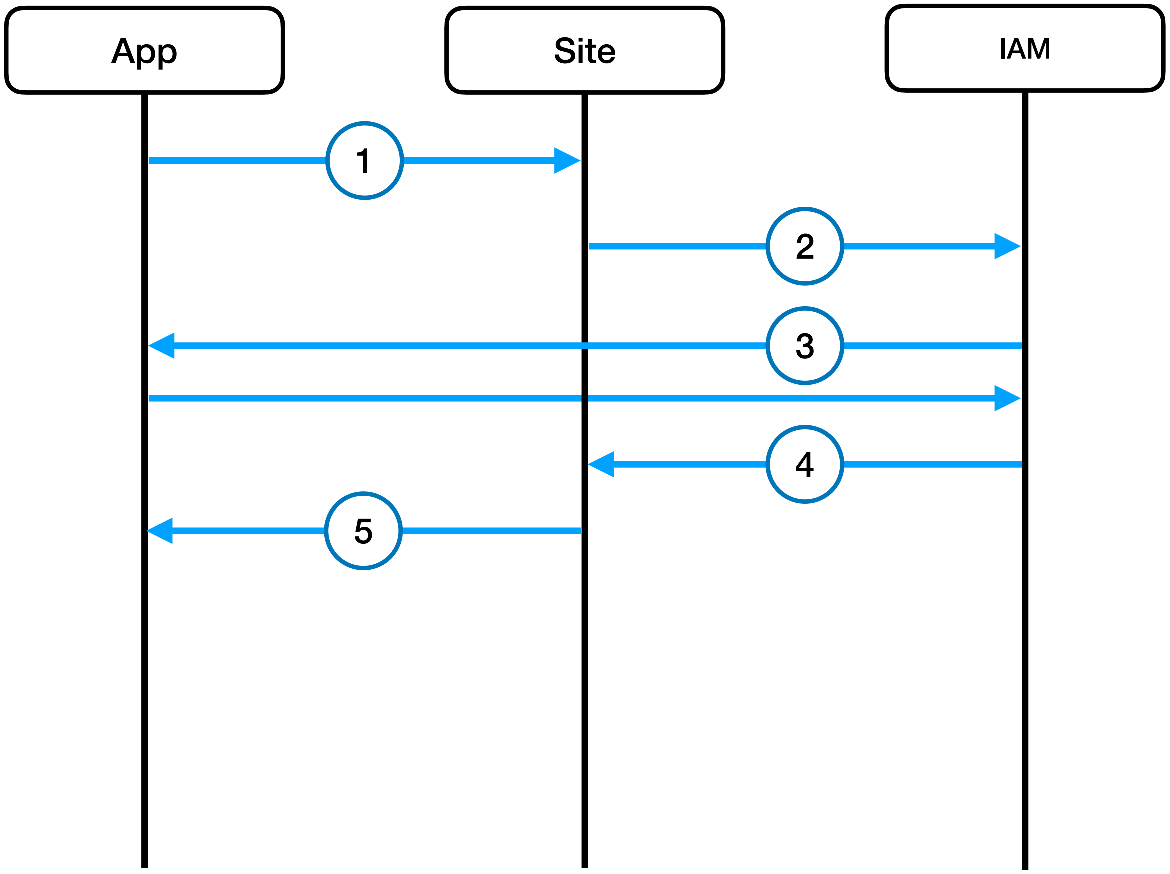
Not on Pinterest yet? Sign up

Are you a business? **Get started here!**

These are social sign in buttons

Social Sign In

IAM = Identify Authorization Manager



1. You click the “Continue with …” button for the Social Sign In provider site of your choice
2. Site sends request to IAM to authenticate your identity (i.e., sign you in to Provider Site)
3. If you are not already signed in to Provider Site, provider Site steps you through it’s sign in process—resulting in the Provider Site having a valid access token
4. IAM returns access token to Site
5. Site returns access token to App

Social Sign In

Pros

- Streamlined sign-up
  I.e., you do not have to create a new account

- Reduced “password fatigue”
  I.e., you do not have to keep track of a new/other password

- Trustworthy authentication process
  The associated technology is “tried and true” having been used for many years by many organizations (referred to as “single sign on” (SSO))

Cons

- Reduced privacy
  The site you sign in to can get your demographic data from the site you sign in with

- Single point of failure
  If the social network account you use for social sign on gets banned/locked, you will also be blocked from the sites you log into using said social network account

- Banned social networks
  Some organizations ban access to social networking sites on their networks

Passkeys

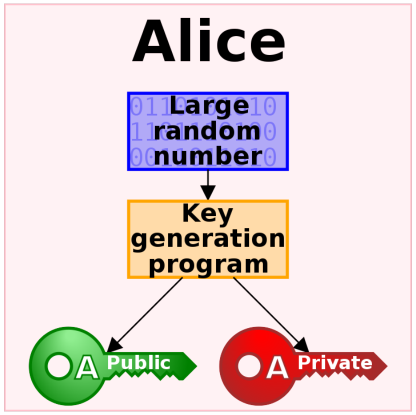
- Allow you to sign in to sites **without** a password

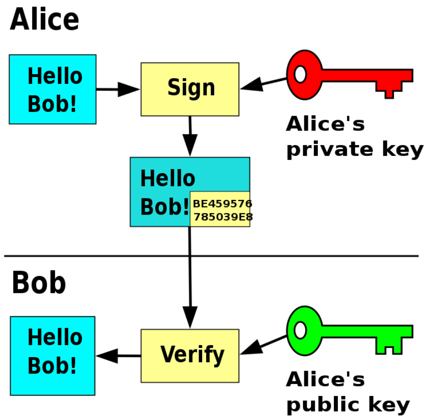
- Passkeys use public key cryptography
  The "secret" part of your credentials is not shared with sites
  I.e., the "secret" part of credentials stays on your device(s)

- Passkeys are safer than other forms of sign in because passkeys can't be stolen of "phished"

- Using Passkeys requires a password manager
  Note: Apple's Keychain service supports passkeys

Recommendation: Become skilled with one of the password managers recommended on next slide before attempting to use passkeys.





Password Managers

- **Definition:** a secure digital tool that you can use to add, store, maintain, and access usernames and passwords for things like apps, software, online services, device sign-ins, and other logins
- Some browsers (e.g. Chrome and Firefox) have “built in” password managers
- **Recommendation: do not use** browser “built in” password managers
  - Not all “built in” password managers are considered sufficiently secure
  - It can be cumbersome to extract an account id/password from a “built in” password manager when signing in from an app other than the browser
  - Instead use one of the **password manager apps** listed in the table to the right

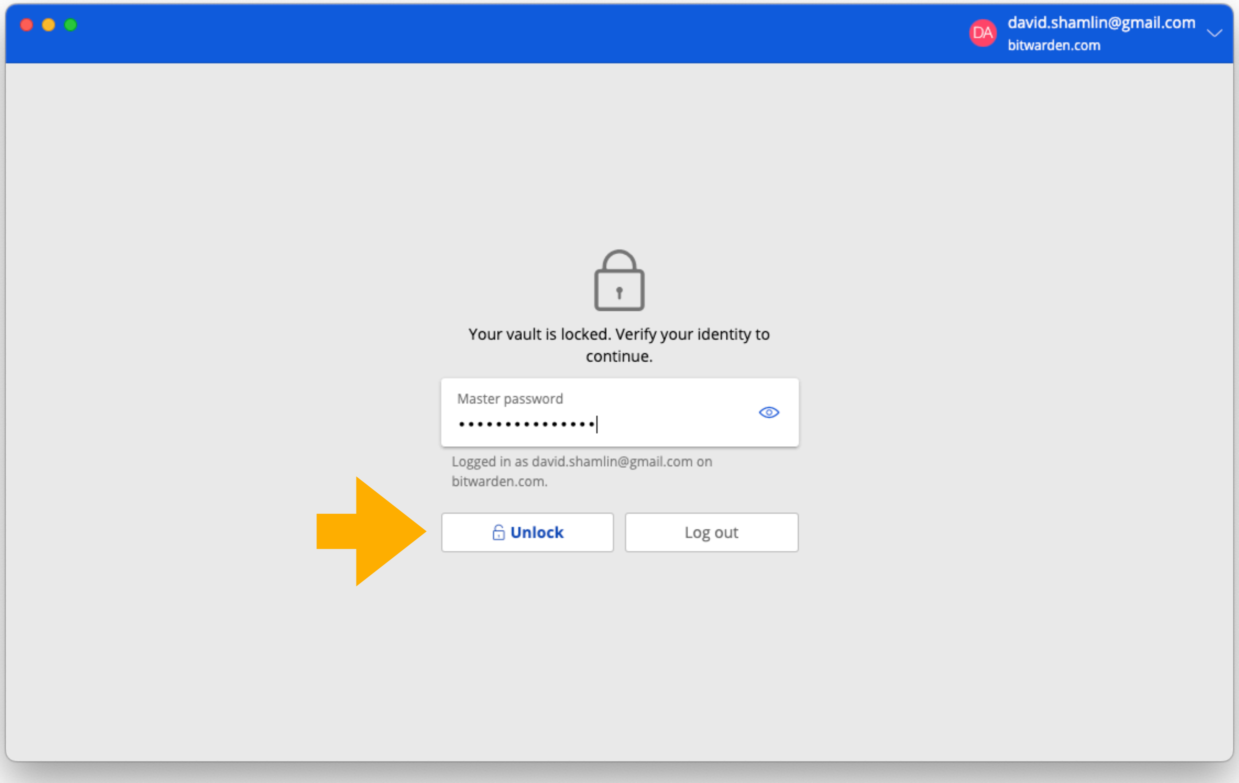
Recommended Password Manager Apps

Product	Help	Pricing
1Password	Link	Link *14 day trial*
Dashlane	Link	Link *30 day trial*
Bitwarden	Link	Link *Free option*
LastPass	Link	Link *Free option*

- Recommended for 1st time users
- Very “user friendly”

Victim of significant data breaches in the last couple of years

Password Managers: Bitwarden Demo

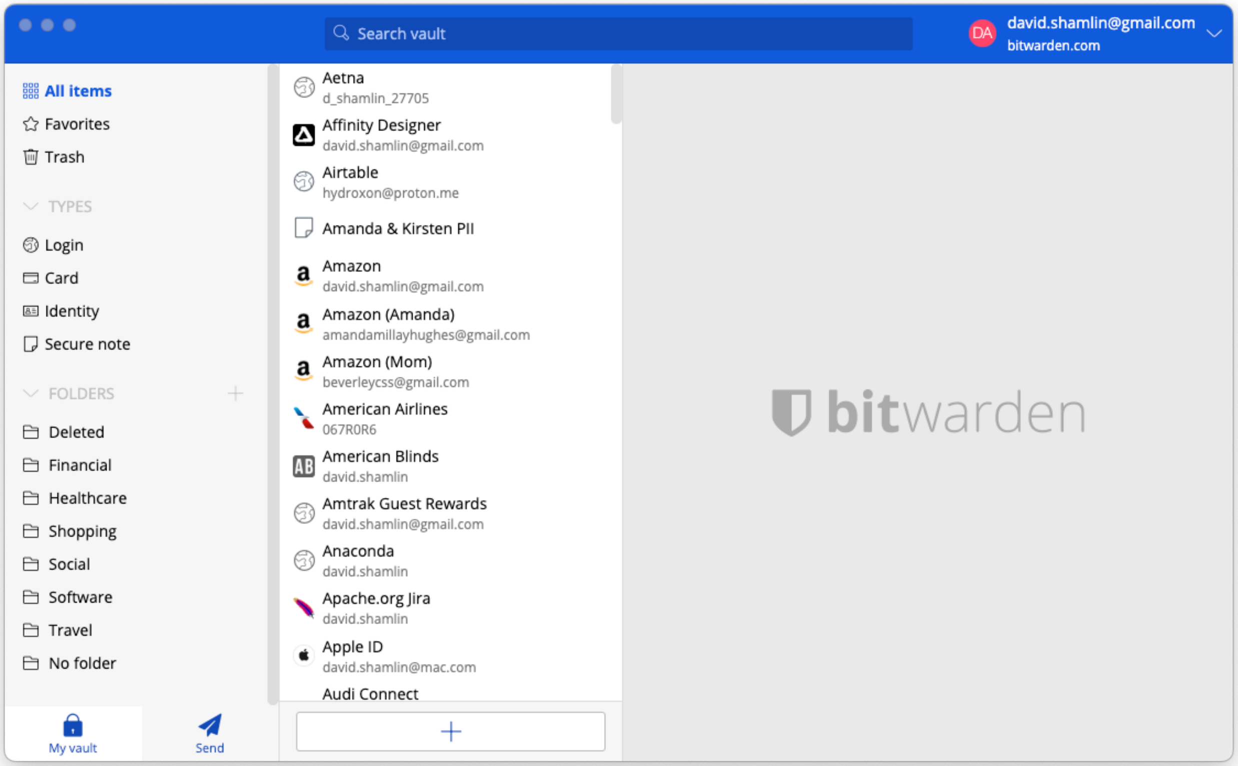


Your vault is locked. Verify your identity to continue.

Master password: ••••••••••••••••

Logged in as david.shamlin@gmail.com on bitwarden.com.

Password Managers: Bitwarden Demo



Aetna
d_shamlin_27705

Affinity Designer
david.shamlin@gmail.com

Airtable
hydroxon@proton.me

Amanda & Kirsten PII

Amazon
david.shamlin@gmail.com

Amazon (Amanda)
amandamillayhughes@gmail.com

Amazon (Mom)
beverleycss@gmail.com

American Airlines
067R0R6

American Blinds
david.shamlin

Amtrak Guest Rewards
david.shamlin@gmail.com

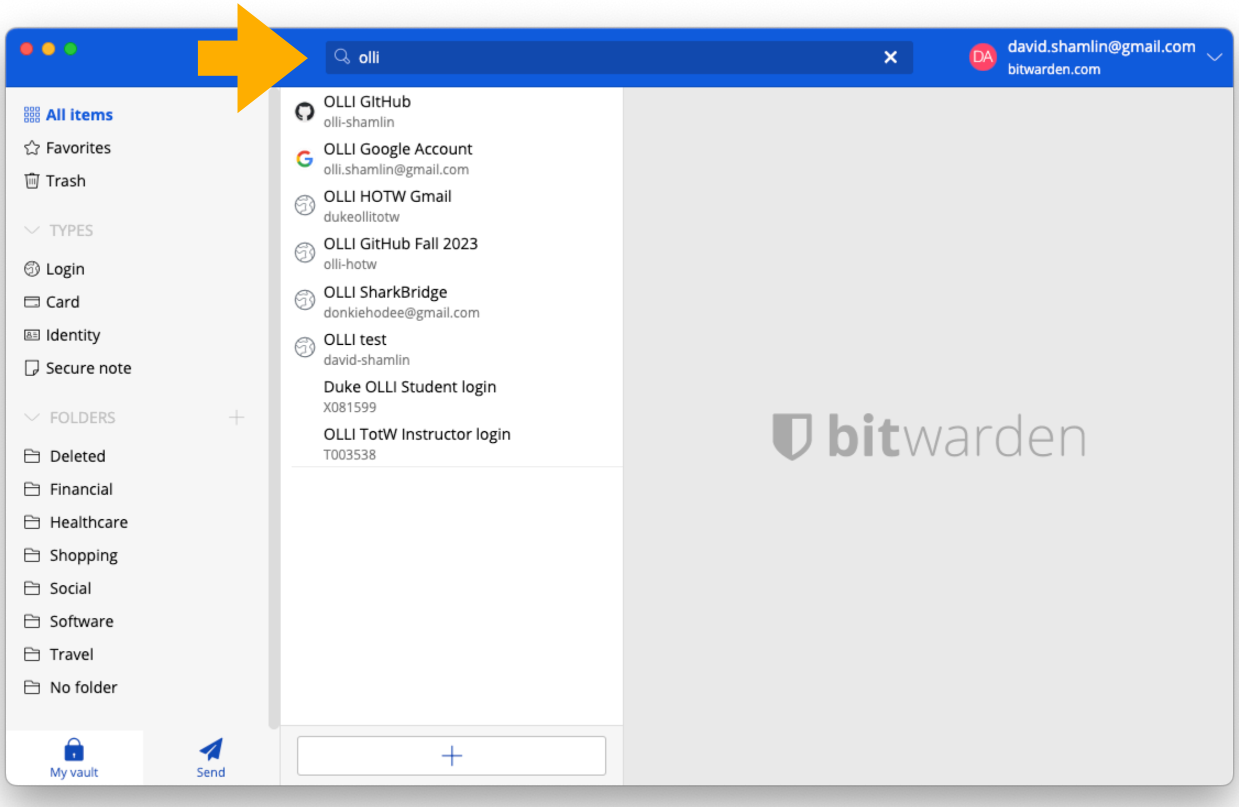
Anaconda
david.shamlin

Apache.org Jira
david.shamlin

Apple ID
david.shamlin@mac.com

Audi Connect

Password Managers: Bitwarden Demo



OLLI GItHub
olli-shamlin

OLLI Google Account
olli.shamlin@gmail.com

OLLI HOTW Gmail
dukeollitotw

OLLI GitHub Fall 2023
olli-hotw

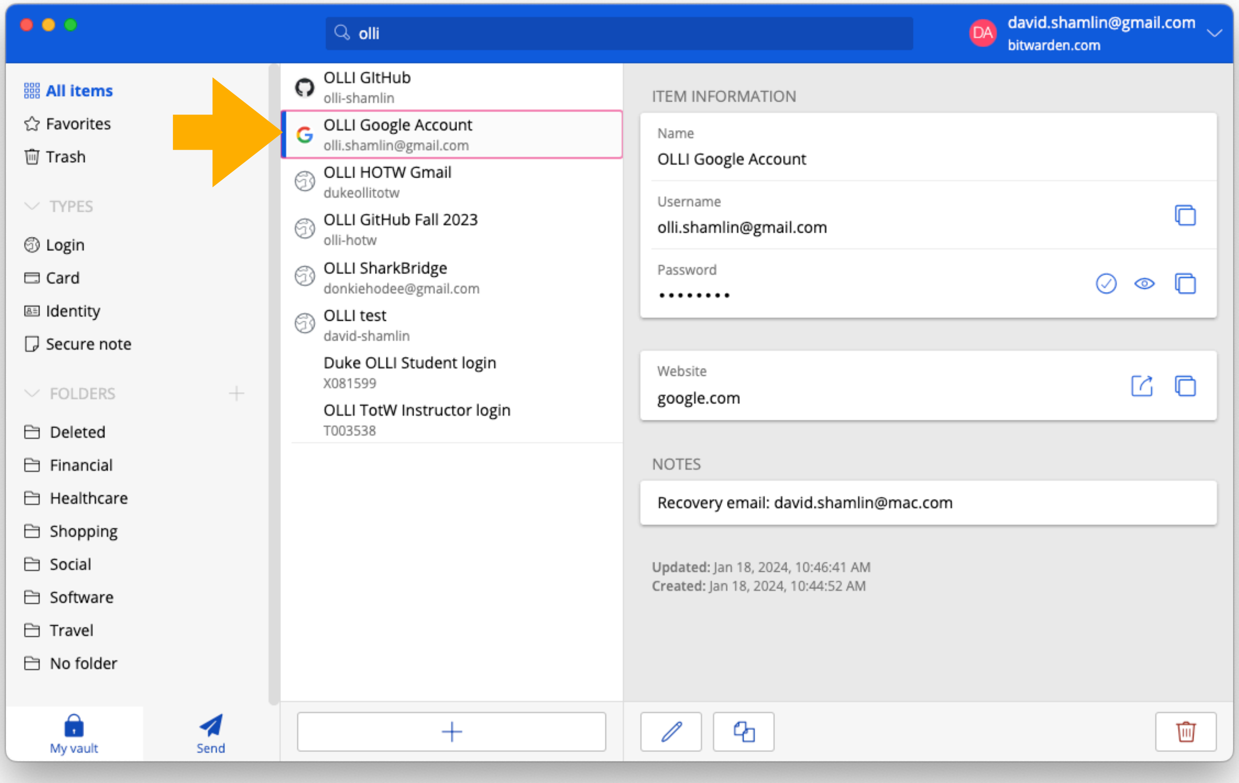
OLLI SharkBridge
donkiehodee@gmail.com

OLLI test
david-shamlin

Duke OLLI Student login
X081599

OLLI TotW Instructor login
T003538

Password Managers: Bitwarden Demo



OLLI GitHub
olli-shamlin

OLLI Google Account
olli.shamlin@gmail.com

OLLI HOTW Gmail
dukeollitotw

OLLI GitHub Fall 2023
olli-hotw

OLLI SharkBridge
donkiehodee@gmail.com

OLLI test
david-shamlin

Duke OLLI Student login
X081599

OLLI TotW Instructor login
T003538

ITEM INFORMATION

Name
OLLI Google Account

Username
olli.shamlin@gmail.com

Password
•••••••••

Website
google.com

NOTES

Recovery email: david.shamlin@mac.com

Updated: Jan 18, 2024, 10:46:41 AM
Created: Jan 18, 2024, 10:44:52 AM

Review

- An account is your digital **identity** for the site associated with the account
- User Id & password—used together—are your **credentials**
  - Some sites use the email address you provide as the user id
    Avoid the common pitfall of mistaking your email account password with your password for the site you are signing into!
- When you sign in to a site using your credentials, the site goes through an **authentication** process that proves you are the account owner
- Learn how to use a password manager app to manage your collection of accounts!

Basic Best Practices

1. Use strong passwords
   1. Truly random
   2. A mix of uppercase, lowercase, digits, and punctuation marks
   3. No shorter than 17 characters
2. Make all your passwords unique
3. Never reuse a password
4. For sites that do support 2FA, turn 2FA on
5. For sites that do not support 2FA, change your password every six months

Homework

- Create an inventory/list of all your accounts
  - For each account in your list include
    - Site name
    - User id and password
    - Recovery email address
    - Did you give a phone number? (Yes or No)
    - Is 2FA used? (Yes or No)
  - Also include any other highly sensitive personal information stored with the account (e.g., home address, credit card info, etc)
- Stretch your comfort zone by using a password manager app to build your account inventory