Safe Computing

User Authentication

- *Authentication* is based on one or more of the following factors:
    - Knowledge – something you know, like a password.
    - Possession – something you have.
    - Inherence – something that you are (biometric data).

Safe Computing

User Authentication

- Passwords
  - Strong passwords are long.
  - Switching case is helpful.
  - That's it – more characters means more possibilities for bad actors to deal with.
  - You will see contradictory advice on this...

Safe Computing

User Authentication

Safe Computing

User Authentication

- How are passwords found by bad actors?
  - Educated guesses
  - Knowledge you have shared on social media
  - Brute force (trying all possible combinations)
  - Stuffing (get credentials for one site, use on another)
  - Phishing

Safe Computing

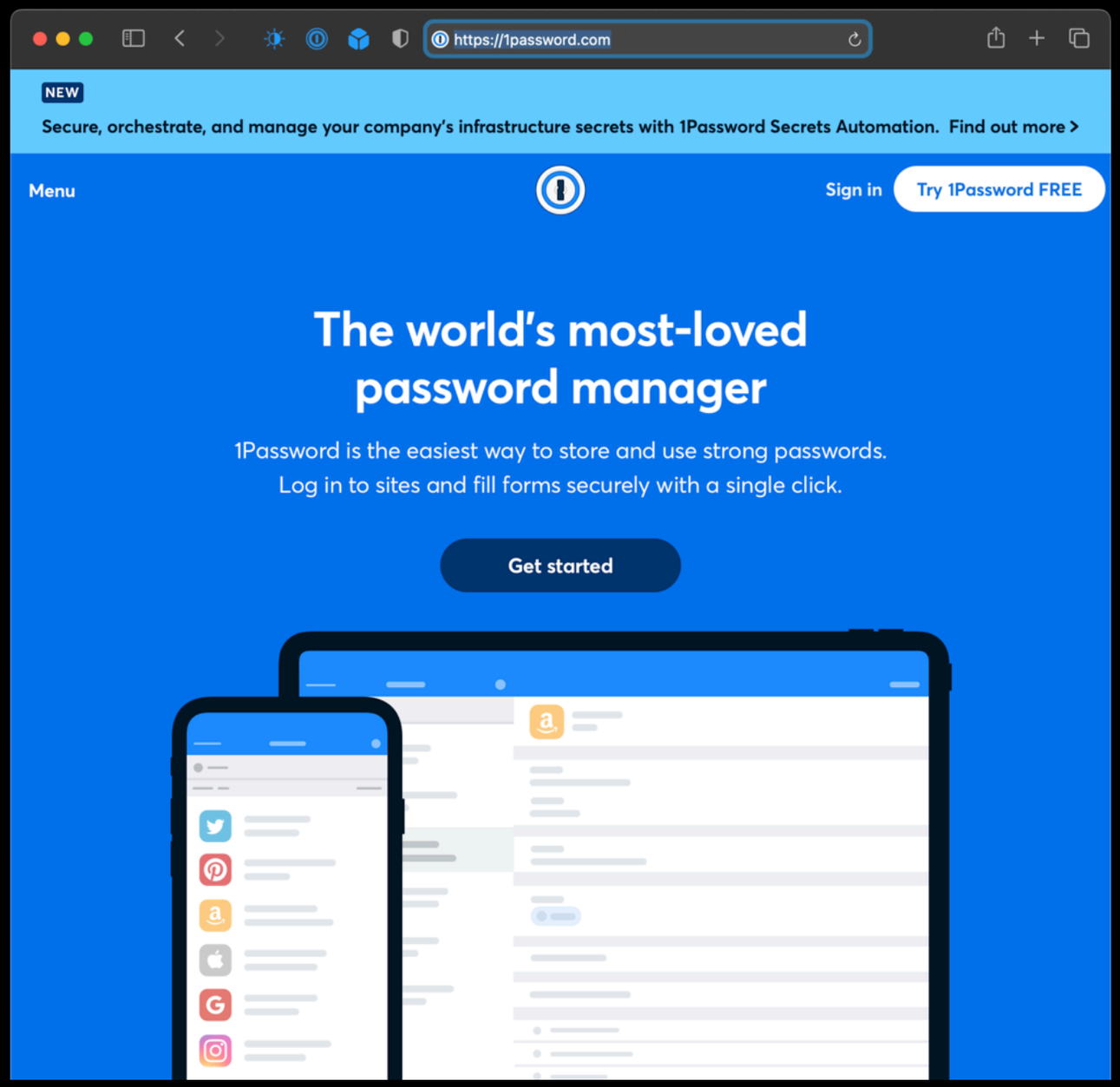
User Authentication

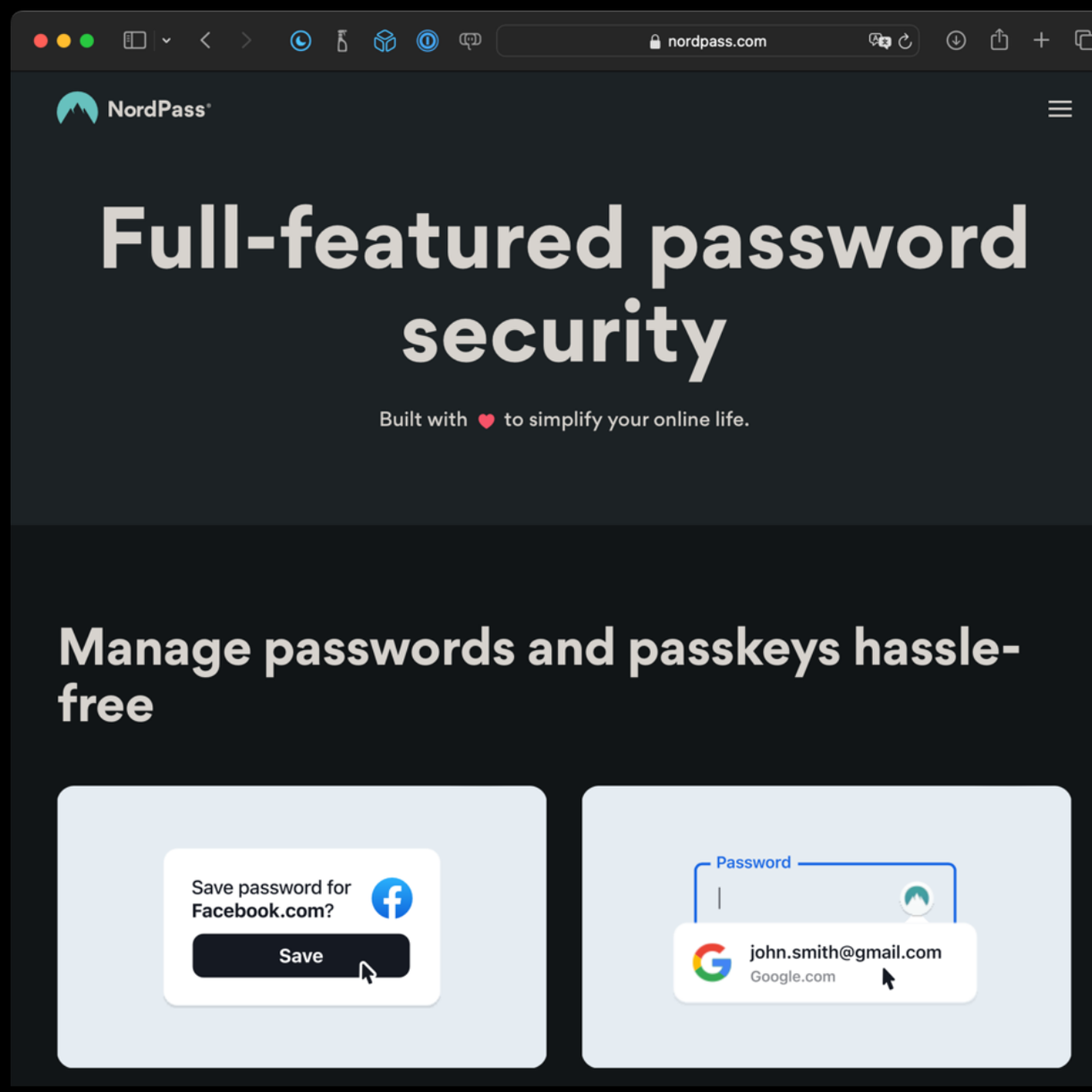
- How to avoid problems with your passwords?
  - Use a password manager!
    - No, really.

- Use a password manager.
  - iCloud Keychain across Apple platforms
  - 1Password is an amazing password manager.
    - And a Canadian company! 🇨🇦
  - Nordpass

Safe Computing

User Authentication





Safe Computing

User Authentication

- Passkeys
  - Pass*words* are problematic, despite the existence of password managers
  - Pass*keys* are a new, cross-platform, cross-vendor standard
    - Passkeys are an implementation of the WebAuthentication or WebAuthn standard, which uses public-key cryptography to secure accounts
    - No need to remember passwords; uses information inherent to who you are for authentication (biometrics via another device)
  - Here is a good overview of what passkeys are and how to use them

Safe Computing

User Authentication

Safe Computing

User Authentication

- Passkeys demo
  - GitHub login