RED space™

TECH SHARE

Our Password Problem

RED space

TECH SHARE



Luke DeWitt

Director of Web Services

Passwords

What are they good for?

- Unintuitive
- Impossible to Remember
  - Password Manager Woes
- Password Standards
  - Who knows the latest?
- “Prone” to hacking
  - 81% of all hacking-related breaches leverage stolen or weak passwords.
- “Shared” secret problem

Slow down egghead

That's how I log in to my favorite sites and services!



RED space

TECH SHARE

47%

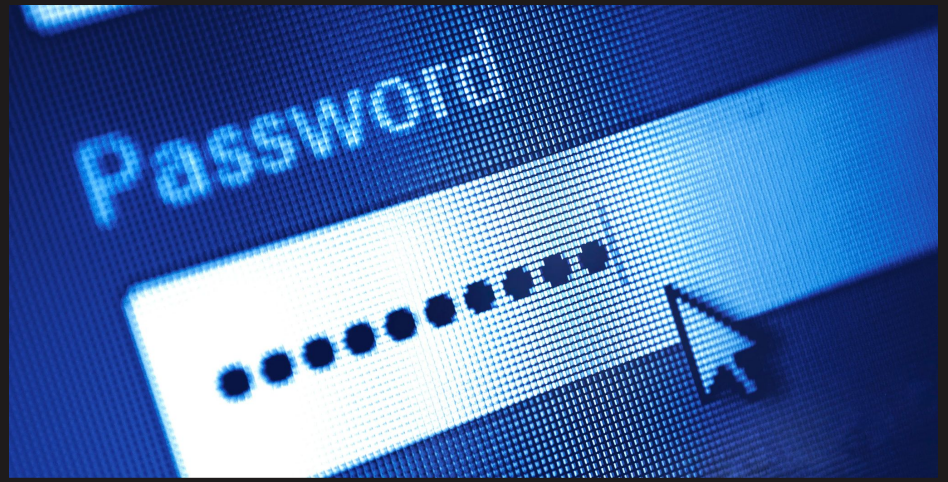
Less than half of users use 2FA

2 Factor Authentication

- Something you know
  - Most often a password for your account.
- Something you have
  - Such as a cell phone with a temporary authentication code.
- Something you are
  - Such as your fingerprint or facial recognition.

👋

Passwords



RED space

TECH SHARE

👋

Passkeys



Goodbye, Passwords
Hello, Passkeys

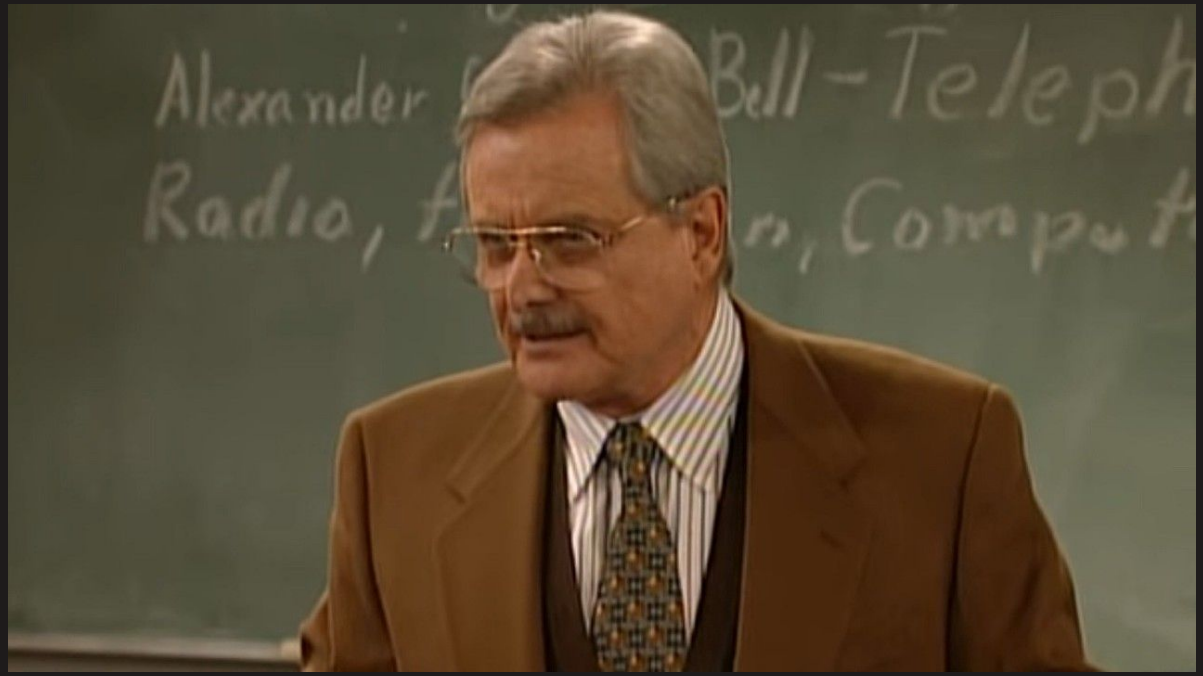
It's about damn time

- Unique
  - Public Key Cryptography (WebAuthN)
  - Private Key remains on device*
- Leverages modern tech (ie/ biometrics, ubikeys)
  - Less Friction
  - Technically multifactor
- Promoted by the major players in the industry
  - Google, Apple



RED space

TECH SHARE



Quick History on WebAuthN

- First proposed in 2013, Finalized in 2019
- Secure authentication on the web without requiring passwords
- Joint effort between the FIDO Alliance the W3C
    - Fast IDentity Online Alliance
        - Universal 2nd Factor (U2F)
        - Universal Authentication Framework (UAF)
    - FIDO2

* About that asterisk...

- Unique per device would indicate unique per device
  - Passkey on your laptop != passkey on your phone != passkey on your tablet
- Secret keys are being synced to the cloud now so you don't have to worry about logging in and setting a new
  - iCloud, Google Password Manager, 1Password
- Still... this isn't ideal.

WebAuthN Support

Platform Authenticators

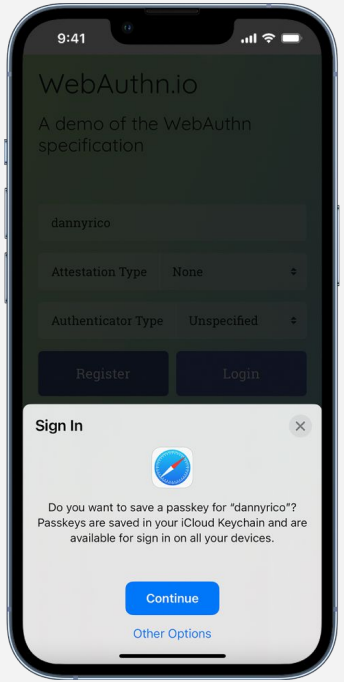
	Android 7+	iOS 14.5+	Windows 10 *(with Windows Hello)*	macOS Catalina	macOS Big Sur	Desktop Linux
Chrome	Yes	Yes	Yes	Yes	Yes	-
Safari	N/A	Yes	N/A	No	Yes	N/A
Firefox	No	Yes	Yes	No	No	-
Brave	No	Yes	Yes	Yes	Yes	-
Edge	No	Yes	Yes	Yes	Yes	-
Internet Explorer	N/A	N/A	No	N/A	N/A	N/A

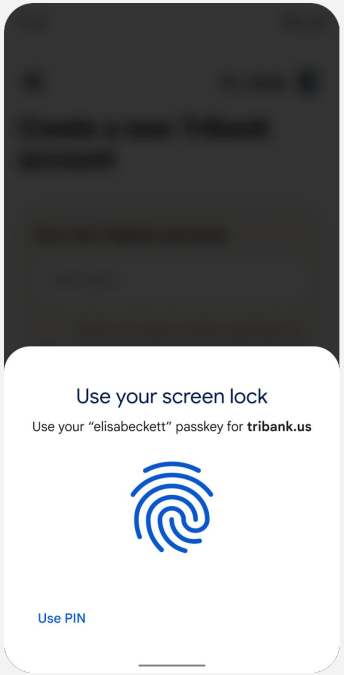
WebAuthN Support

Roaming Authenticators

	Android 7+	iOS 14.5+	Windows 10	macOS Catalina	macOS Big Sur	Desktop Linux
Chrome	Yes	Yes	Yes	Yes	Yes	Yes
Safari	N/A	Yes	N/A	Yes	Yes	N/A
Firefox	No	Yes	Yes	Yes	Yes	Yes
Brave	No	Yes	Yes	Yes	Yes	Yes
Edge	No	No	Yes	Yes	Yes	Yes
Internet Explorer	N/A	N/A	No	N/A	N/A	N/A

Mobile


9:41
WebAuthn.io
A demo of the WebAuthn specification
dannyrico
Attestation Type
None
Authenticator Type
Unspecified
Register
Login
Sign In
Do you want to save a passkey for "dannyrico"? Passkeys are saved in your iCloud Keychain and are available for sign in on all your devices.
Continue
Other Options


Use your screen lock
Use your "elisabeckett" passkey for tribank.us
Use PIN



How does it work?





The steps

1. A user signs in to the website.
2. Once the user is signed in, they request to create a passkey on the frontend, for example, by pressing a "Create a passkey" button.
3. The frontend requests information from the backend to create a passkey, such as user information, a challenge, and the credential IDs to exclude.
4. The frontend calls `navigator.credentials.create()` to create a passkey. This call returns a promise.
5. A passkey is created after the user consents using the device's screen lock. The promise is resolved and a public key credential is returned to the frontend.
6. The frontend sends the public key credential to the backend and stores the credential ID and the public key associated with the user account for future authentications.

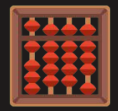
Taken from: https://web.dev/passkey-registration/



So I lied

... you still need a password... kind of...

- But remember that a lot of these passkeys will be stored in the cloud, so that helps...
  - ... but some people won't trust the cloud
- Adoption concerns?



Demo / Code





Another Demo

https://webauthn.me



RED space

TECH SHARE



Thanks for coming!