
ASIGNIO

# Multi-factor Biometric Authentication

## High Security & Deepfake Resistant MFA

# Authentication is Broken

## Passwords can be *phished*

amazon

Refund Notificatic

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

**REF CODE:2550CGE**

You are required to provide us a valid billing address

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
Amazon.com
**Email ID:**

## Passwords can be *stolen*

## Passwords can be *guessed*

- 123456
- 123456789
- Qwerty
- Password
- 12345
- 12345678
- 111111
- 1234567
- 123123
- Qwerty123
- 1q2w3e
- 1234567890
- DEFAULT
- 0
- Abc123
- 654321
- 123321
- Qwertyuiop

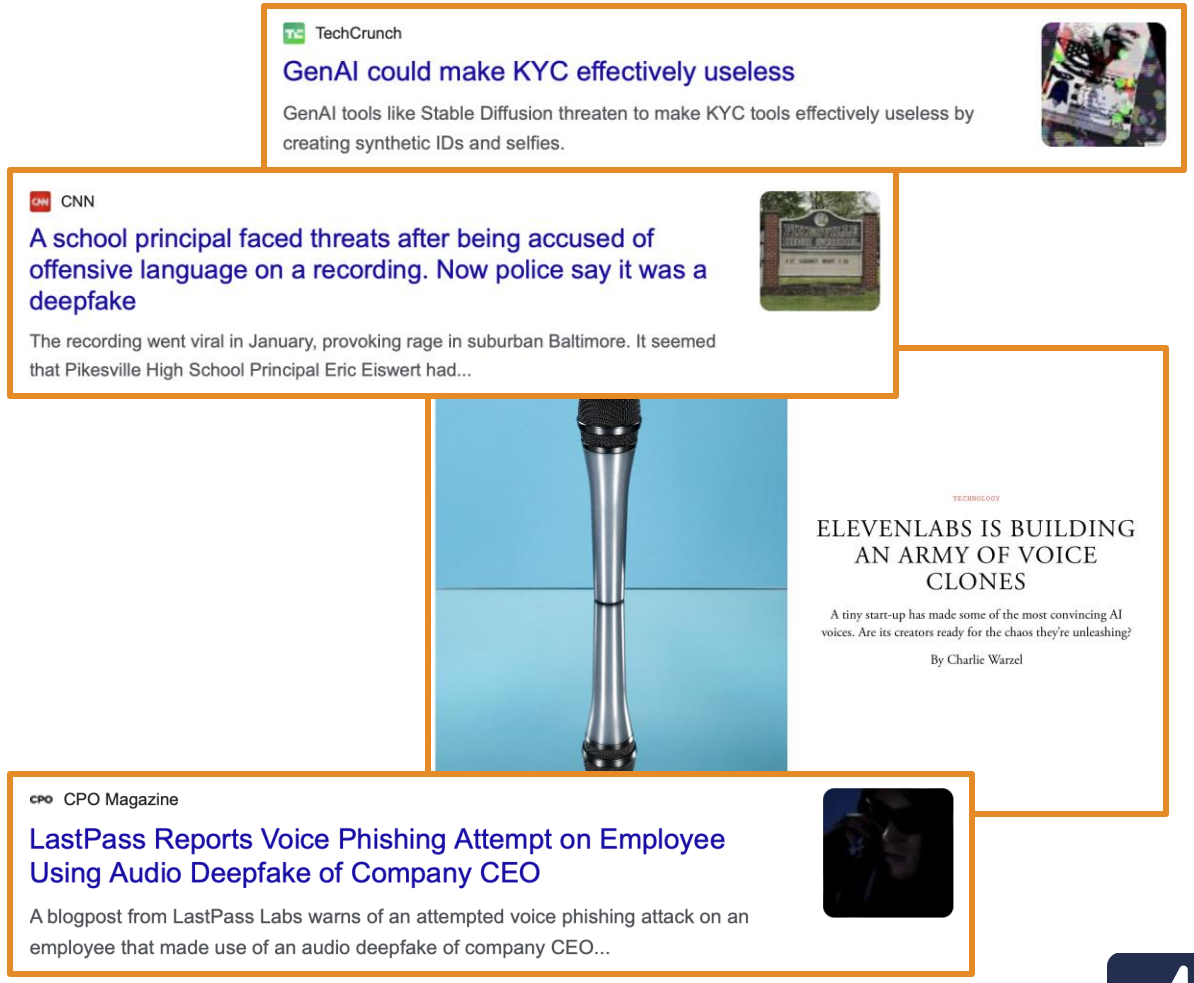
**Passwords are easily defeated.**

# Authentication is Broken

**Facial and voice biometrics are beatable with deepfakes**

**Publicly available tech can animate still images found on the web**

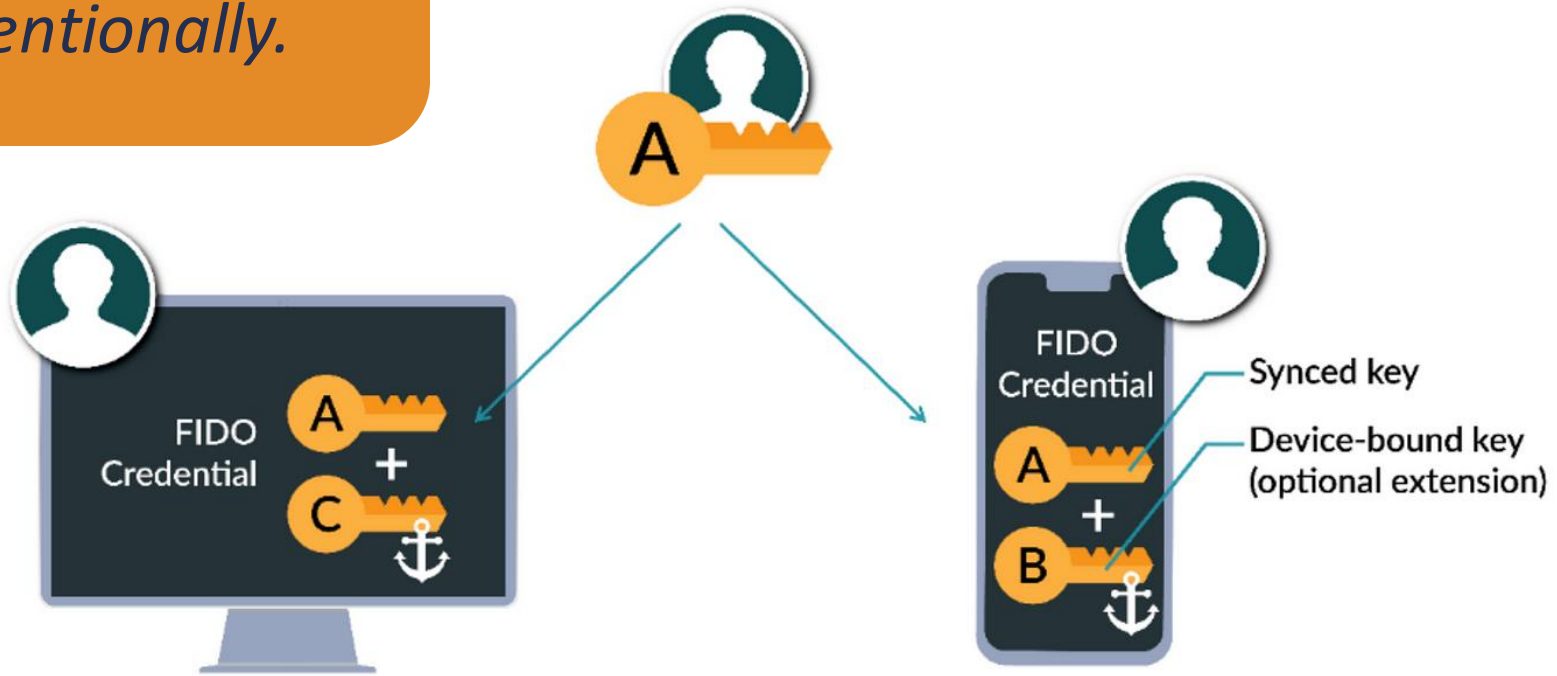
**Fraudsters can deepfake your voice with 10 seconds of audio**



# Authentication is Broken

**And passkeys?**

Turns out they are shareable…
*intentionally or unintentionally.*



# Broken Authentication Fraud is Coming

## MGM Grand Cyberattack Allegedly Caused by 10-Minute Phone Call

Ransomware group ALPHV claims to have used common social engineering tactics to get into the casino's systems.

By **Nikki Main**

Published September

MARKETS • **Published** September 19, 2023 4:36pm EDT

## MGM to lose up to $8.4 million each day as it resolves cyberattack

MGM could lose between 10% and 20% in revenue and cash flow due to the attack, analysts estimated

Home › Tech › News » Password Attacks Rise To 921 Every Second Globally: Microsoft

## Password attacks rise to 921 every second globally: Microsoft

FORBES > INNOVATION > CYBERSECURITY

## Ransomware Attack Takes 100 Hospitals Offline

**Davey Winder** Senior Contributor

*Veteran cybersecurity and tech analyst, journalist, hacker, author*

Follow

0

Feb 13, 2024, 06:44am EST

DATA AND SECURITY

## Deepfake fraud attempts are up 3000% in 2023 — here's why

Fraudsters are capitalising on the rise of GenAI

## CISA orders US government agencies to check email systems for signs of Russian compromise

News

Apr 12, 2024 • 5 mins

World / Asia

## Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

# The Solution: Asignio

## Asignio is a handwriting biometric.

**Private**

You won't find it on the web or overhear it

**Secure**

Multi-biometric, multi-factor and personal

**Dynamic**

Change it when you need to

**Less Friction**

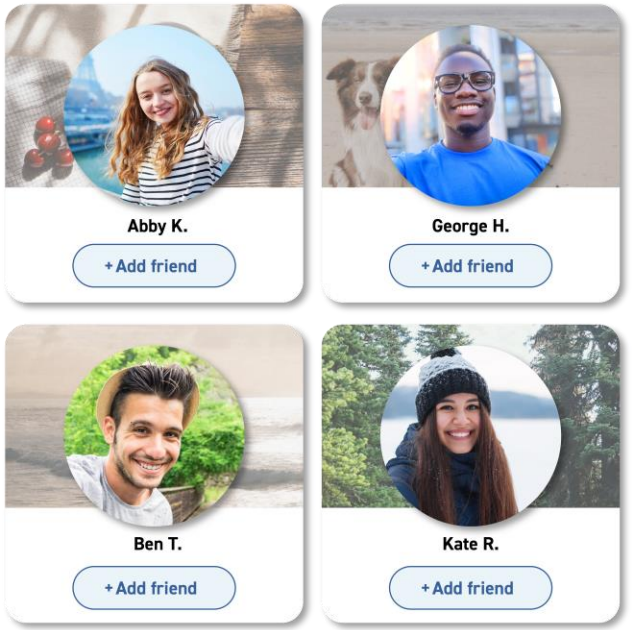
No extra steps, any device, no app required

Use it on a mobile touch device for ***onboarding, sign-in, step-up authentication and account recovery.***

# It's Private

## Face and voice are public

- You are seen, heard by people around you or searching the web.
- Using widely available tech, your voice can be recreated with as little as a 10 second recording, and your face can be animated from a still photo.




**Your Asignio Sign is a private set of symbols that you manually enter with your finger to authenticate.**
*Your handwriting is only seen if you choose.*

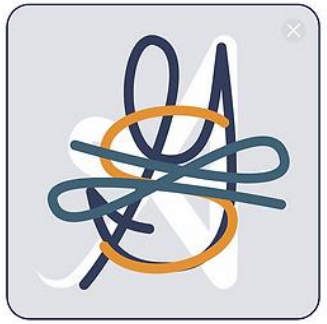
# It's Secure

- Dual biometrics ensure that private Sign is presented by authorized person
- **It is phishing and deepfake resistant**
  - Even if you send a picture of your Sign via email, the fraudster still has to figure out the order of the symbols, the direction they are signed, the speed of the signing and how to send it through a touchpad.

# It’s Dynamic

**Face and voice are static.**

Your face and voice change with age, *but you keep what you were born with.* So, if someone gets a picture of you, or a voice recording, you are at risk.

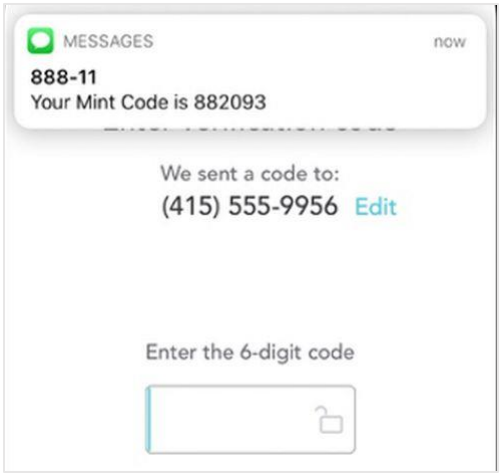


**Your Asignio Sign is whatever you want it to be.**
Unlike face and voice, you can change it if you want to/need to. The biometric aspect is reflected in *how* you sign, not *what* the sign is.

# It's Less Friction

Face and voice are typically used to strengthen a password solution, and typically come with a one time password, a KBA or similar.

***That's a lot of steps and solutions to use.***

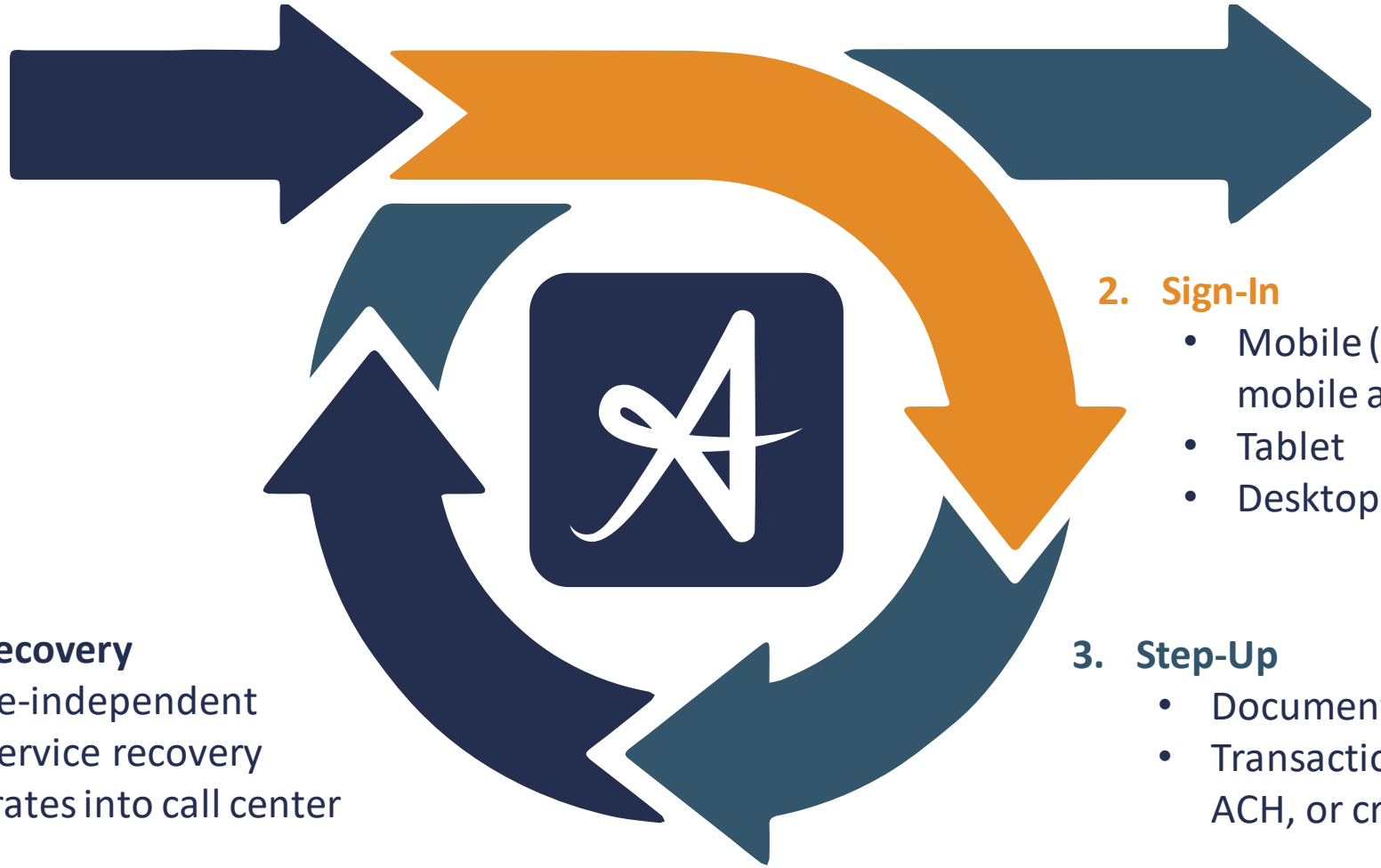




- Asignio's solution is **just the sign**. The selfie happens simultaneously to assure that the person who should be signing is present.
- No extra steps required.
- It works on the smart device that you already have and is not tied to anyone device.

# Convenient Across All Use-Cases

1. **Onboarding**
   - Tie verified ID to user biometrics



5. **Account Closure/Removal**

2. **Sign-In**
   - Mobile (in browser) or mobile app
   - Tablet
   - Desktop

3. **Step-Up**
   - Document Approval
   - Transaction Approval (e.g. wire, ACH, or credit card

4. **Account Recovery**
   - Device-independent
   - Self-Service recovery
   - Integrates into call center


# ASIGNIO

For more information

https://www.web.asignio.com/contact

# Introducing Asignio Sign

**Secure**

- Dual biometrics ensure user match
- Facial verification biometric ensures liveness and person present
- Cannot be stolen through phishing or other fraud


**Convenient**

- Works on any touch-enabled device
- Available in browser or app

**Easy**

- Handwriting is non-static biometric – changeable and secret
- Muscle memory – just like writing
- No passwords – at any step