recordia identia

WHITEPAPER

Voice biometrics as a Two-Factor Authentication

Authentication based on passwords and OTPs has weak security and offers poor user experience

Passwords have significant weaknesses.

Weak passwords

Passwords and PINs can be stolen, intercepted, hacked or phished.

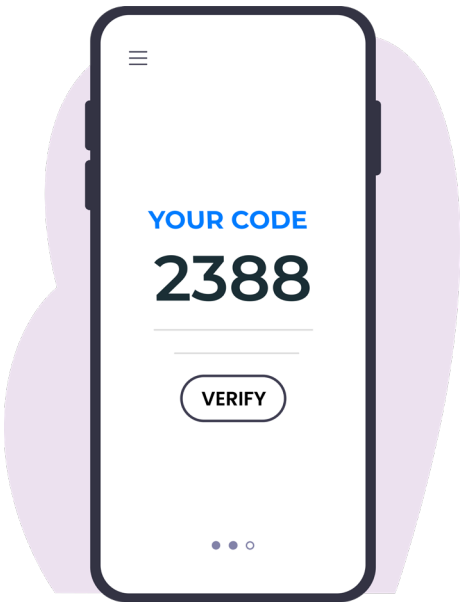
Re-used passwords

Passwords can be reused or shared.

Phishing Attacks

Social engineering attacks confirm the inherent weakness of Possession Factors (passwords) as they cannot 100% guarantee a person's identity.

Why shouldn't OTPs be used as Two-Factor Authentication?



1.

SIM cards can be stolen and used by intruders in their own phones to receive SMS or calls and commit fraud.

2.

Cybercriminals can illicitly obtain SIM card data through the application of social engineering.

3.

OTP codes can be intercepted by criminals, taking advantage of flaws in message transmission protocols.

A complex authentication process leads to frustration and bad user experiences.

Identia Two-Factor Authentication

A different and smarter way to authenticate by voice to ensure identity.

We offer a frictionless voice biometric authentication solution that provides organizations the ability to secure the identity of the workforc. This applies to every channel that an employee can use to connect to corporate assets in person or remotely.

Features

- **Flexible and easy to implement:** Identia offers a simplified, flexible and easy to implement solution for any type of company to include two-factor authentication with voice biometrics.
- **Identity verified:** Identia combines voice biometrics with transcription to provide an additional layer of security to the voice authentication process and prevent access through prerecorded or artificially generated voices.
- **Reduced dependency on external devices:** By using voice biometrics as a second authentication factor, there is no need to rely on additional mobile devices to receive OTP codes.
- **Improved user experience:** By not relying on external devices or needing to remember any passwords, Identia enables faster, more secure and frictionless authentications in a matter of seconds.

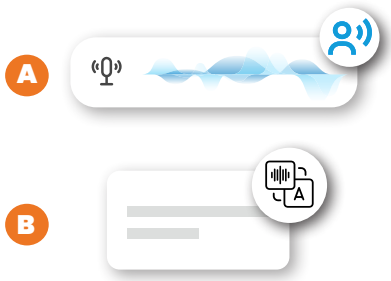
How does it work?

Once the Identia API is installed in your services, the user registers with their usual credentials and then a second authentication is performed in the Identia® service through their voiceprint.

PHASE 1: Enrollment
A first registration of biometric fingerprints in the database is made through an audio recording in which the user must read a random text, or through the ingestion of pre-recorded audios.

PHASE 2: Authentication
The user must read a short phrase that is randomly generated to authenticate his identity in order to ensure that he is a real person and not a bot or a recording and thus avoid impersonation.

Connection to Identia for authentication



A **Voice biometrics:** Who is speaking.

B **Transcription**: What did he say.

Guaranteed access