SOITRON*
INSPIRE TO ASPIRE

VOICE BIOMETRICS.
Is 2016 the year?

Introduction

Have you ever wondered how you can recognise family, friends or your favourite singer by hearing just a few seconds of their voice? In ancient times, people believed that the voice came from the heart. Fast-forward to today and we know that speech is possible thanks to our vocal chords. But hardly anybody realises just how complicated speech is.

Around a hundred different muscles are involved in speech. It is a sophisticated orchestration of the chest, neck, jaw, tongue and lips. And although two voices might sound similar, no two are identical.

Just like a fingerprint or iris, each human voice is unique.

Recent technological developments mean that computers can now hear, store and recognise our speech. It's a breakthrough that has huge implications in all sorts of areas, and has the potential to make our lives easier. In organisations that speak to customers regularly, what role can voice biometrics have in delivering an efficient, secure and outstanding level of customer service?

A growing discontent

Currently, the onus is on customers to prove their identity when dealing with a business. Normally this involves the customer having to remember a personal identification number (PIN) or a memorable word (such as mother's maiden name), followed by answering a series of account-related questions to prove their identity beyond any doubt.

But research suggests that the uniqueness of a PIN or memorable word is not as safe as people think:

- Half (49%) of internet users use the same password on two or more accounts[1]
- 67% have more than 11 usernames and passwords, and 9% have more than 50 usernames and passwords[2]
- 67% of mobile users reset passwords at least once a month[3]

This, it seems, is leading to a growing discontent among customers for current authentication methods: almost half (49% [4]) of consumers claim that authentication is time-consuming, and the majority (85% [5]) admit frustrations with existing authentication options offered by businesses. But there is hope. More than three-quarters[6] of consumers are interested in using alternatives to protect their security.

With cyber risks now among the top three concerns for UK businesses[7], clearly organisations need a robust way to secure – and authenticate access to – important information. But shouldn't businesses make it easier for customers to conduct business with them?

[1] **Source:** http://www.techweekeurope.co.uk/security/authentification/denial-online-security-password-163011
[2] **Source** *Research by Nuance Communications* (http://www.nuance.com/for-business/customer-service-solutions/voice-biometrics/index.htm)
[3] **Source** *Research by Nuance Communications* (http://www.nuance.com/for-business/customer-service-solutions/voice-biometrics/index.htm)
[4] **Source** *Research by Nuance Communications* (http://www.nuance.com/for-business/customer-service-solutions/voice-biometrics/index.htm)
[5] **Source** *Research by Nuance Communications* (http://www.nuance.com/for-business/customer-service-solutions/voice-biometrics/index.htm)
[6] **Source** *Accenture's 'Digital Trust in the IOT ERA 2015' report*
[7] **Source** *Research from Allianz's 'Risk Barometer.'* (http://www.newstatesman.com/microsites/cyber/2016/02/rise-smart-attack)

Voice Biometrics

Picture the scene. You're abroad on holiday, and need to urgently call your bank to transfer money or pay a bill. Rather than use a Card Reader, divulge your PIN or memorable word and jump through a series of hoops to identify yourself, you're authenticated in seconds. And all you needed to do was talk.

That's the reality of voice biometrics. But how does it actually work?

The Voiceprint

Voice biometrics authenticates customers based on a voice sample (or voiceprint). The voiceprint is then paired with customers' data located in customer relationship management systems used by contact centres. Every time the customer calls the business, they are authenticated by their voice alone, and able to proceed with their request without the need for any other security procedures.

There are typically two types of voice biometrics technology.

1 The first verifies a caller's identity during the course of a natural conversation. It transparently analyses over a hundred unique voice characteristics while the customer speaks and compares these characteristics with the relevant stored voiceprint. It does this in seconds and without interrupting the call. It can do this in any language, with any accent, any device (whether landline, mobile, hands-free or even Skype), and regardless of the content of the call.

2 The second approach verifies a caller's identity during an interaction with a voice application (such as an IVR or a mobile app). The customer recites a passphrase back and the application verifies this against the known voiceprint. It's the unique way the caller says the phrase that enables the authentication.

How robust is it?

No matter how good someone is at impersonations, it's impossible to replicate someone else's voice to the level of matching their individual voiceprint. Voiceprint is improved over time based on the calls with the highest quality of authentication. In fact the system is also able to detect if a voice is 'live' or a pre-recording.

Any company that wants to deploy multi-factor security can quickly combine voice biometrics with a knowledge question or PIN to further enhance security. When industry-standard compliance systems – including PCI-DSS – are integrated with voice biometrics, then businesses have a compelling security system that meets strict industry regulations.

Why should everyone care?

Voice biometrics is a game changer for both consumers and businesses. Consumers can quickly identify themselves with very little effort – safe in the knowledge that access to their personal information is secure. In fact 90 per cent of customers that have used it prefer voice biometrics to the status quo.

From the business' perspective, meanwhile, stripping out the verification step and establishing immediate, solid knowledge that they are the customer would allow more time to help other customers. With an average of 80 per cent faster authentication in five seconds, expected savings total $15 million over a three-year period[8].

And for both parties, voice could be a huge boon in the fight against fraud and identity theft, saving millions all round.

[8] **Source** *Research by Nuance Communications* (http://www.nuance.com/for-business/customer-service-solutions/voice-biometrics/index.htm

What does the future look like for voice biometrics?

- While some businesses remain reluctant to embrace voice biometrics with open arms, a number of high-profile banks have recently announced plans to rollout voice biometrics to customers. **Tatra banka** (member of Raiffeisen Bank International), **Barclays**, **Banco Santander** and more recently **HSBC** have all announced a major shift in the way they authenticate customers.

- The voice biometrics industry is growing faster than ever, according to analyst firm Opus Research. High-profile data breaches, financial losses from fraud, customer experience optimisation, and deployments by the world's largest enterprises, are "pushing voice biometrics adoption into the mainstream."

- **Angela Sasse**, director of the **UK Research Institute in Science of Cyber Security**, has been a long-time proponent of biometrics as a secure replacement for passwords. She argues that consumers show every sign of being ready to switch to biometrics because of the convenience and extra security. *"As essential services such as banking become accessible via less effortful and secure authentication technologies, consumers will expect that other day-to-day services make security easier for them, and biometric solutions will play a leading role in that."*

Tangible benefits that voice biometrics offer to organisations of all sizes include substantial timesavings for employees, and enhanced security. Every business is different and any new technology deployment requires careful evaluation. When **Juan Vucetich**, a Croatian-born police official, started collecting fingerprints back in 1891, little did he know that over a hundred years later his concept would become huge areas of focus for designers and security experts around the globe. The maturity of the technology means that voice biometrics is now a secure and robust option for businesses. It offers genuine efficiencies for both businesses and customers, and allows contact centres to focus on what they do best – customer service.

Case studies:

Tatra banka

TB
TATRA BANKA
Member of Raiffeisen Bank International

An example of voice biometrics in practice is Tatra banka in Slovakia. First introduced in 2013, and now with more than 250,000 registered customer voice samples (one third of the whole customer database of the bank), the average time of client identification process has been reduced by 66 per cent – to an average of just 27 seconds per customer. Now, 85 per cent of all calls to the bank's contact centre that require authentication are verified by voice. This time reduction has resulted in fewer operators required to provide the same level of service, which enabled the bank to focus more on more complex queries, and active sales.

Banco Santander

Another example of voice biometrics benefitting consumers and businesses alike is Banco Santander, which faced a 50-65 per cent failure rate for authenticating customers. Banco Santander needed a better way to authenticate callers to improve satisfaction and agent productivity.

Since using voice biometrics from Nuance, the company has reduced the time agents spend authenticating customers calling into its contact centre from 72 seconds to just 30. As well as eliminating the widespread problem of forgotten PINs, while still meeting stringent government requirements, the bank has lowered contact centre costs by $1 million annually. By slashing agent authentication time by more than 50 per cent, agents are now free to focus on higher value customer interactions.