Bezpieczeństwo 2.0 w mBanku

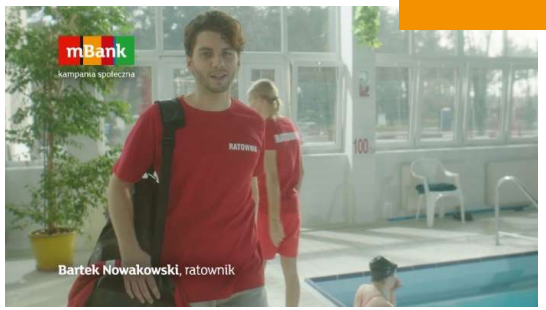
Przełomowa weryfikacja behawioralna

12 grudnia 2018 r.,

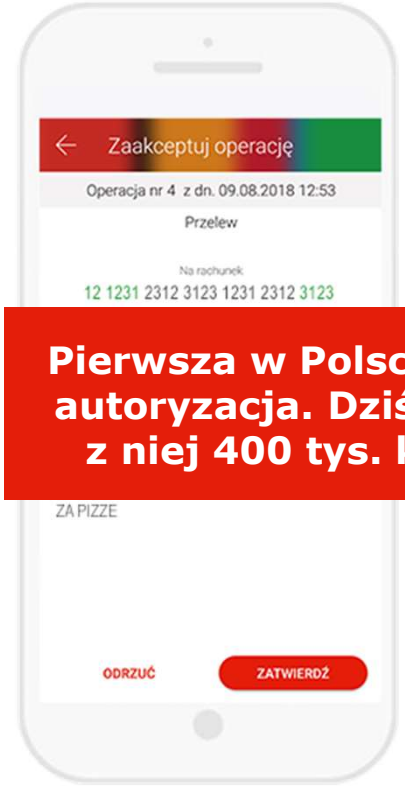
Warszawa

Misja: edukacja

Od trzech lat prowadzimy kampanię społeczną „Uważni w sieci” na temat cyberzagrożeń



Regularnie wprowadzamy nowości z dziedziny bezpieczeństwa



Pierwsza w Polsce mobilna autoryzacja. Dziś korzysta z niej 400 tys. klientów

Wsparcie klientów w cyfrowym świecie poza bankiem

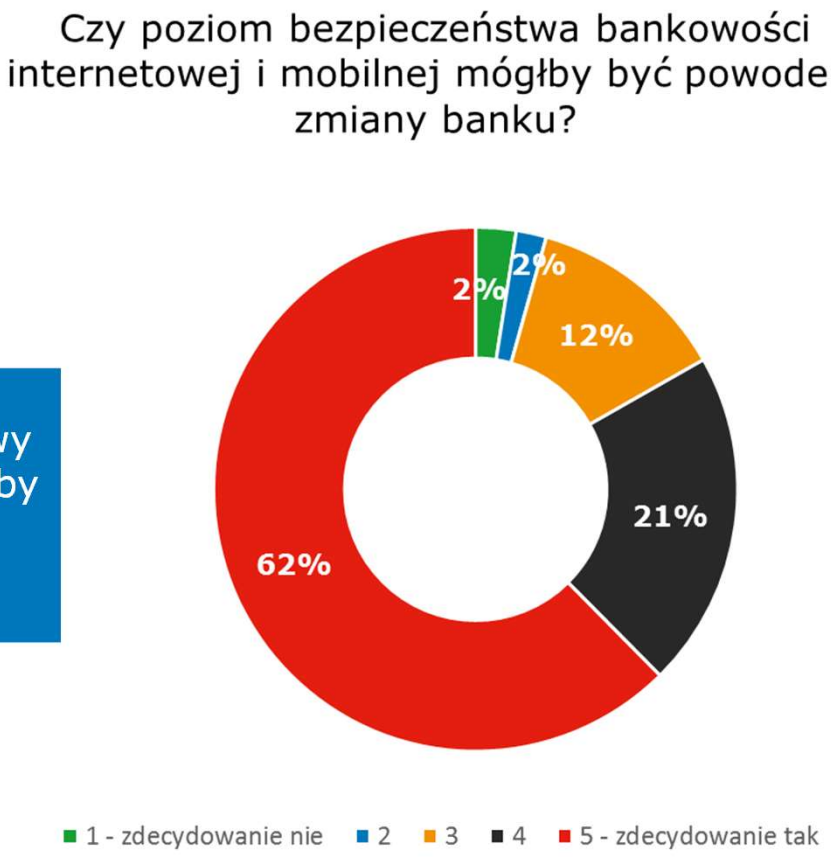
CYBER RESCUE

IQS: ponad 90% klientów banków uważa bezpieczeństwo „digital” za kluczowe

źródło: badanie IQS dla mBanku, grudzień 2018 r.

IQS: klienci wymagają bezpiecznej bankowości on-line

Dla 83% badanych obawy o bezpieczeństwo mogłyby być powodem zmiany banku



źródło: badanie IQS dla mBanku, grudzień 2018 r.

mBank przedstawia nową usługę: weryfikację behawioralną Digital Fingerprints

mBank

mAccelerator

DIGITAL FINGERPRINTS

marka Centrum Bezpieczeństwa Cyfrowego S.A.

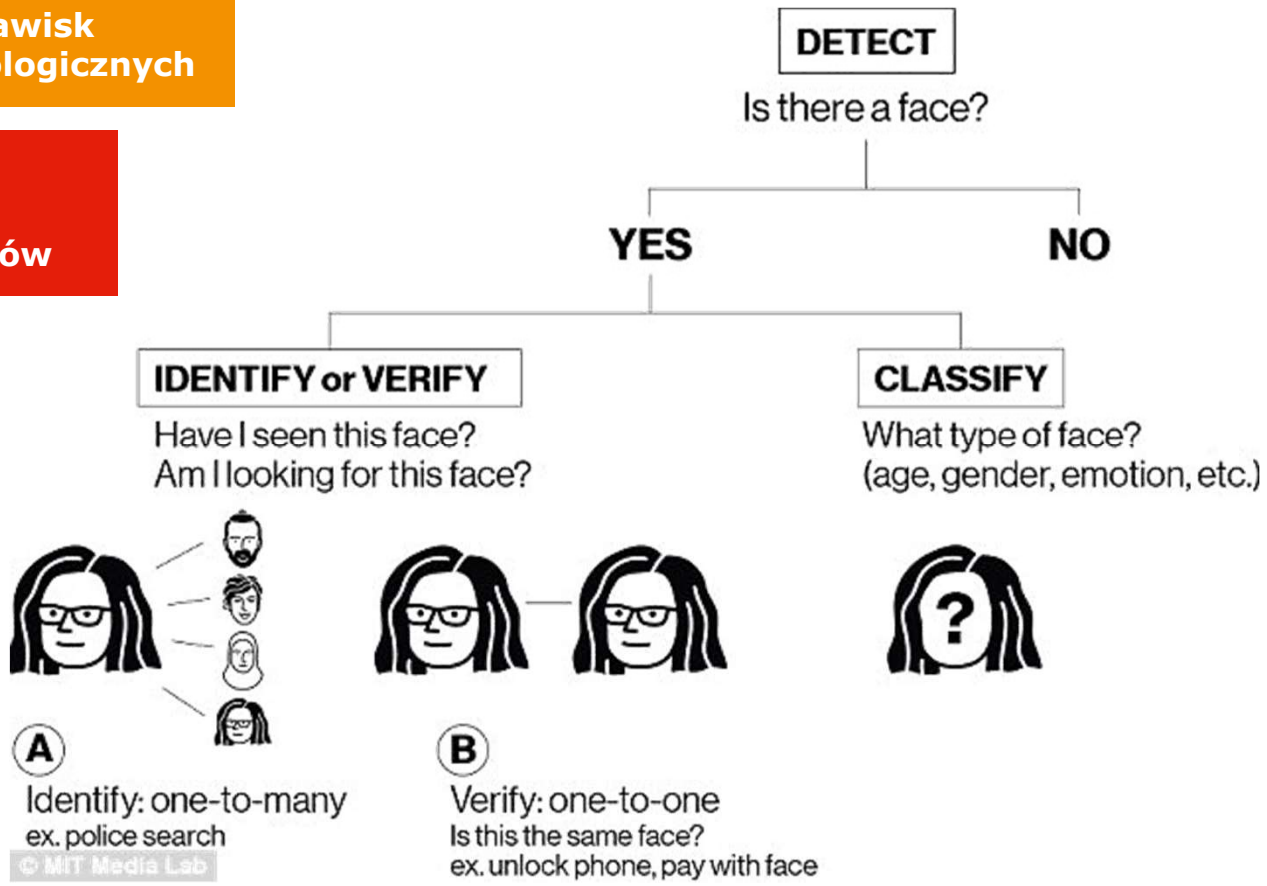
marka Centrum Bezpieczeństwa Cyfrowego S.A.

Mateusz Chrobok,
CEO Centrum Bezpieczeństwa Cyfrowego S.A.

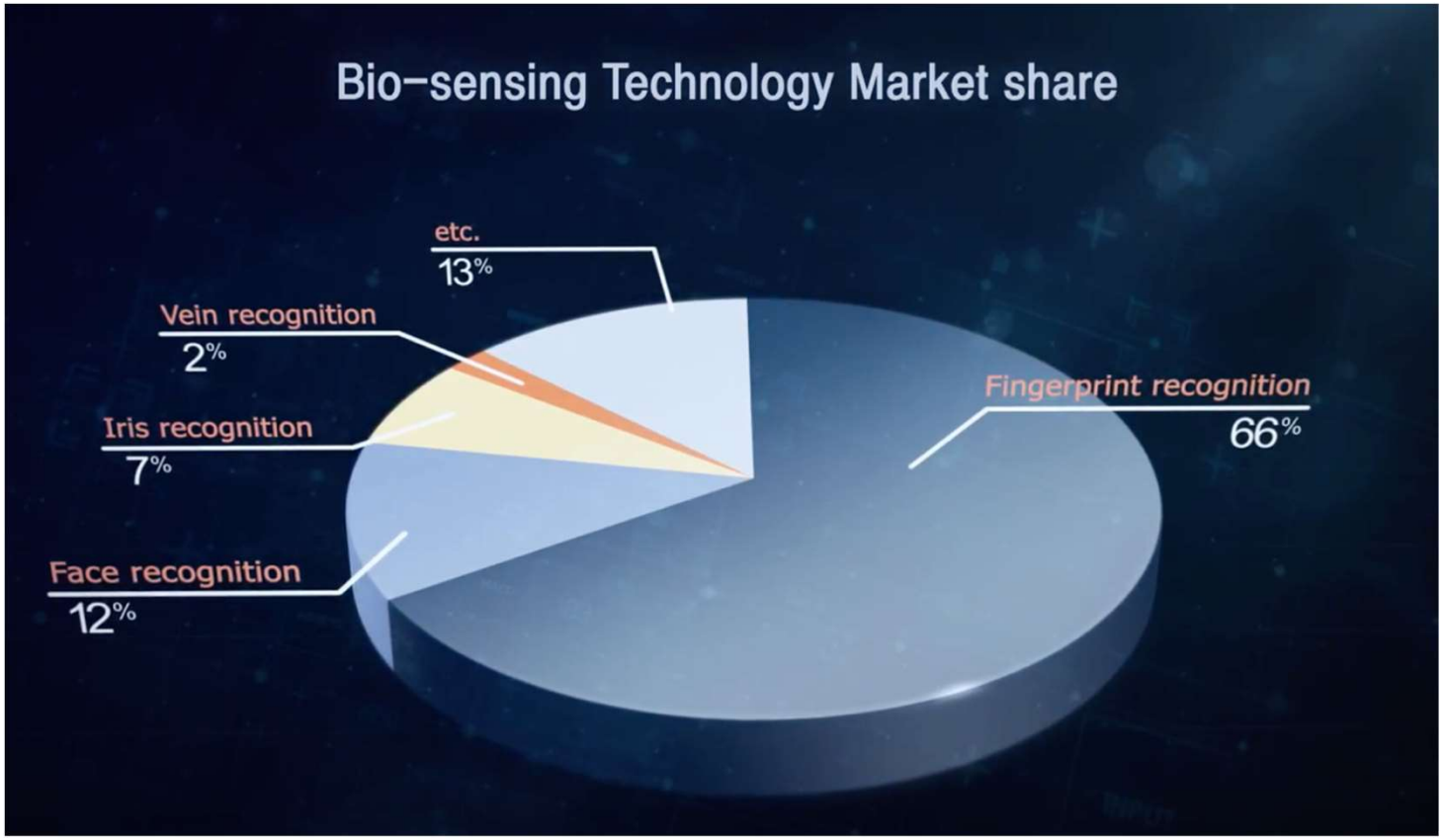
Biometria: czym jest i do czego służy

Jest to analiza statystyczna zjawisk i obserwacji biologicznych

Zależy od cech biologicznych i jakości sensorów



Jak wygląda rynek biometrii „klasycznej”

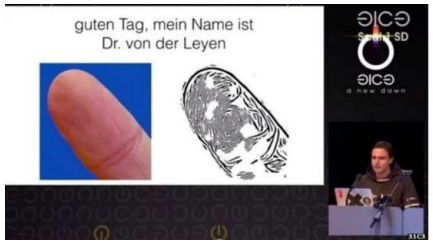


(2017 r.) źródło: https://www.youtube.com/watch?v=_wG2p3PgeYM

Każde rozwiązanie biometryczne ma swoje...

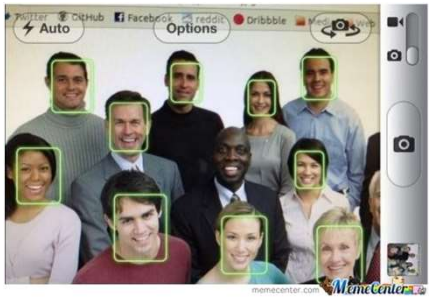
	PLUSY	MINUSY
	- Powszechność i szeroka dostępność urządzeń skanujących - Szybkość działania	- Nie zawsze działa, np. w deszczu - Łatwy do skopiowania (np. zdjęcie, trzymanie szklanki) - Rzadko spotykane są systemy badające czy nie jest to sztuczny odcisk palca - Ktoś może wykorzystać odcisk palca zastraszając nas
	- „Handsfree” - Bada, czy loguje się żywy użytkownik	- Dyskryminujący ze względu na zbiór danych. Efektywnie kolor skóry i płeć. - Słabo działa w ostrym i ciemnym świetle - Często daje się oszukać zdjęciem, maską - Podatne na atak „złego bliźniaka” - Można zbudować „klona” mając zdjęcie
	- „Handsfree” - Trudniejszy do podrobienia niż tylko fotografią	- Słabo działa w ostrym i ciemnym świetle - Jeśli raz wyciekną dane, nie da się tego już zmienić (wzór tęczówki mamy tylko jeden…)

Czasem te metody mogą powodować zamieszanie...



Publicznie dostępne zdjęcie dłoni wystarczyło, aby **haker podszył się pod niemiecką minister** i pokazał problem

Indyjski centralny system danych o obywatelach (w tym biometrycznych, np. ich źrenic) nie chroni danych swoich użytkowników. Można je kupić na czarnym rynku już za 500 rupii (ok. 26 zł) Zastosowane metody w niektórych prowincjach działają tylko w 51%



Algorytmy rozpoznawania twarzy bywają... rasistowskie i seksistowskie.

- Lepiej rozpoznają twarze mężczyzn niż kobiet (8,1 vs. 20,6% błędnych wskazań)
- Lepiej rozpoznają twarze rasy białej niż czarnej (11,8 vs. 19,2% błędnych wskazań)

źródła: https://www.dailymail.co.uk/sciencetech/article-5382979/Study-finds-popular-face-ID-systems-racial-bias.html
https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands
https://link.springer.com/article/10.1007/s12553-017-0202-6

Jest też biometria BEHAWIORALNA...

Mierzy wysoce zróżnicowane i trudne do podrobienia wzory zachowań

KATEGORIE BIOMETRII BEHAWIORALNEJ

1. Stylometria – metoda analizy tekstu pisanego dla ustalenia statystycznej charakterystyki stylu autora
2. **Human-Computer-Interaction (HCI) – analizuje sposób korzystania z klawiatury, „touchpada:, myszy**
3. Analiza sposobu korzystania z klawiatury, „touchpada” czy myszy, ale poprzez obserwowanie akcji podejmowanych przez oprogramowanie użytkownika (np. analiza logów systemu)
4. Analiza wzorca motorycznego użytkownika podczas wykonywania konkretnych zadań
5. Analiza czysto biologicznych danych dotyczących zachowań, np. sposobu, w jaki się poruszamy

źródło: https://www.linkedin.com/feed/update/urn:li:activity:6459513752176988160 by Yampolskiy & Govindaraju

Biometria behawioralna w mBanku

W RAMACH WERYFIKACJI BEHAWIORALNEJ BĘDZIEMY MIERZYĆ:

1. Dynamikę korzystania z klawiatury
2. Sposób poruszania kursorem myszy, „scrollowanie”
3. Sposób posługiwania się „touchpadem”
4. Sposób korzystania ze smartfona (w przyszłości)

Niewidoczne dla klienta, nie wymaga dodatkowych akcji

---

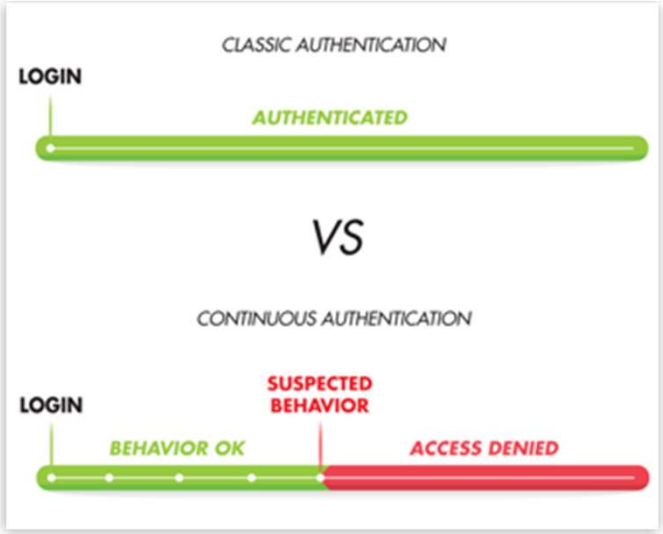
mBank + DIGITAL FINGERPRINTS

marka Centrum Bezpieczeństwa Cyfrowego S.A.

Biometria behawioralna pozwoli na wykrycie zmian w zachowaniu użytkownika i szybszą reakcję

Dane przetwarzane przez Centrum Bezpieczeństwa Cyfrowego nie umożliwiają identyfikacji konkretnej osoby

Broni przed wieloma atakami



1. **Kradzież danych do logowania**
2. **Kradzież sesji**
3. **Problem bramy**
4. **Man in the Middle**
5. **Man in the Browser**

Człowiek
vs.
maszyna

Digital Fingerprints startuje jako pilotaż

test 50k OK

Zaczynamy pilotażem

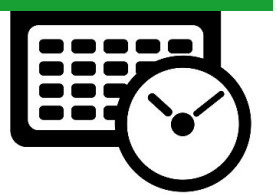
Na grupie 50 tys. klientów

Klient wyraża zgodę

Na podstawie danych zbudujemy profil

Ciągłe porównanie z profilem behawioralnym

Elastyczność czasowa – aż do końca 2019 r.



Weryfikacja behawioralna będzie kolejnym elementem zabezpieczeń

NOWOŚĆ
Identyfikacja urządzeń

Unikalne ID i hasło. Stały monitoring antyfraudowy

Zabezpieczenia i monitoring transakcji kartowych

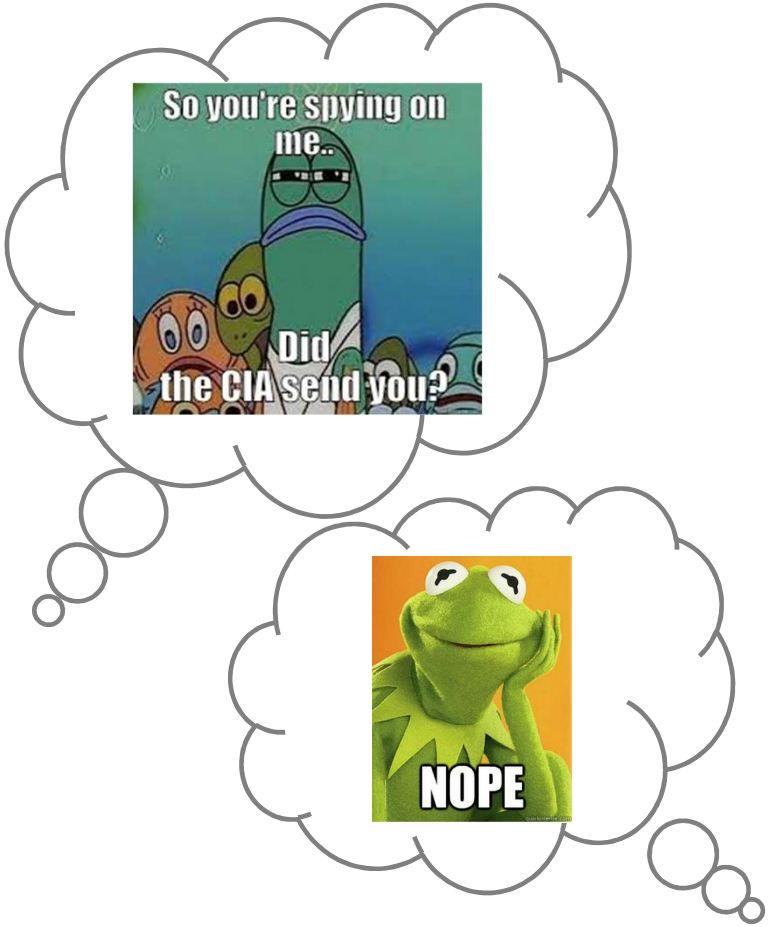
+ Biometria behawioralna

Logowanie biometryczne i potwierdzanie PIN-em w aplikacji

Mobilna autoryzacja i kody SMS

Zarządzanie limitami i dostępami

Czy jest się czego bać? Nie.



Nie będziemy sprawdzać **co** klient robi tylko **w jaki sposób** to robi

Zmierzymy **sposób interakcji z systemem bankowym**, a nie podejmowane w nim akcje

Etyka przede wszystkim

NASZE ZOBOWIĄZANIA:

1. Gwarantujemy, że nie wykorzystamy danych w innych celach niż ochrona klienta
2. Gwarantujemy, że nigdy nie przekażemy tych danych podmiotom trzecim
3. Klient mBanku wie, że dostęp do jego danych ma wyłącznie mBank.

mBank + DIGITAL FINGERPRINTS

marka Centrum Bezpieczeństwa Cyfrowego S.A.

Pierwszy krok do pozbycia się haseł...

Behavioral biometrics will replace passwords by 2022 – Gartner

10 months ago 4 Min Read

Dziękujemy