DIGITAL FINGERPRINTS

Digital Fingerprints to firma z branży cyberbezpieczeństwa specjalizująca się w procesie logowania i weryfikacji tożsamości użytkownika.

Rozwiązania z portfolio Digital Fingerprints pozwalają podnieść bezpieczeństwo procesu autoryzacji dostępu/ logowania.

Narzędzia służą też do wykrywania anomalii takich jak:

- współdzielenie kont, logowania,
- kradzież konta,
- przejęcie konta/ sesji
- kradzież tożsamości użytkownika,
- Kradzież danych do
- Friendly frauds,
- przejęcie cookies,
- zdalne pulpity i wiele innych

Kluczowi Klienci:

ING

mBank

Jak podnieść bezpieczeństwo procesu logowania?

DIGITAL FINGERPRINTS

1. Device Fingerprinting – jak odcisk palca.

Device Fingerprinting zbiera informacje zebrane o danym urządzeniu w celu jego identyfikacji.
Na podstawie tych informacji może stwierdzić, czy podczas kolejnych logowań do systemu, nadal łączy się to samo urządzenie.

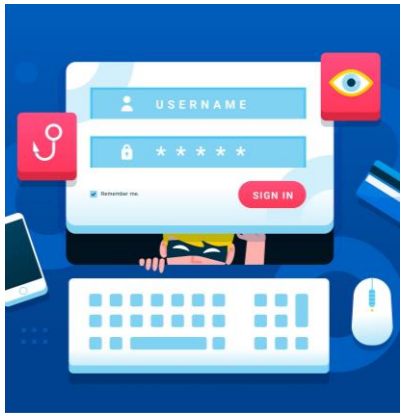
- Nie korzysta z ciasteczek i storage'u na urządzeniu
- Nie jest wrażliwy na zmiany w środowisku użytkownika
- System działa w tle, dostarczając uwierzytelniania wieloskładnikowego bez negatywnego wpływu na UX

Rozwiązanie Device Fingerprinting jest potężnym narzędziem do rozpoznawania powracającego oszusta (nawet jeśli ten zmieni swoją tożsamość, czy skorzysta z pomocy wspólników).

Sytuacja wygląda podobnie przy problemach z botami.

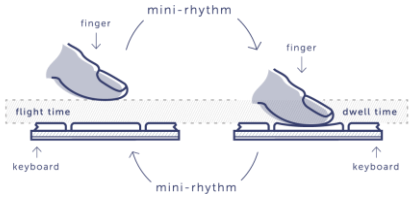
Jak podnieść bezpieczeństwo procesu logowania?

2. PureSecure – Najnowocześniejsze MFA.



PureSecure – jest rozwiązaniem, które podnosi bezpieczeństwo podczas logowania. Podczas weryfikacji tożsamości, następuje badanie trzech składników logowania:

- Wiedza – PIN, hasło
- Posiadanie – Device Fingerprinting
- Biometria behawioralna – sygnatura naszego zachowania (sposób wpisania na klawiaturze swojego PINu)

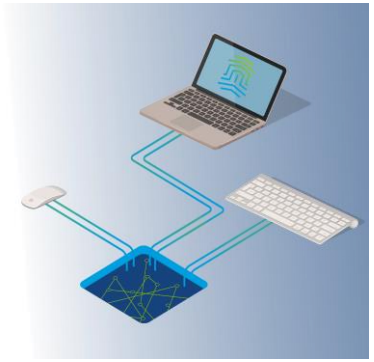


- Bycie sobą wystarczy, aby być chronionym
- Nie jest wymagany żaden dodatkowy sprzęt
- System działa w tle, dostarczając uwierzytelniania wieloskładnikowego bez negatywnego wpływu na UX

Jak podnieść bezpieczeństwo procesu logowania?

DIGITAL FINGERPRINTS

3. Biometria behawioralna.



Biometria behawioralna to wykorzystanie technologii to weryfikacji tożsamości użytkownika na podstawie jego zachowania on-line. Dzięki informacjom, takim jak sposób pisania na klawiaturze, prędkość kursora czy krzywej podczas ruchu myszą, możemy zweryfikować użytkownika. Weryfikacja ta jest nie tylko w momencie logowania użytkownika, ale w tracie trwania **całej sesji**.

- Bezkontekstowe działanie
- Ciągłe potwierdzanie tożsamości
- Stała adaptacja modeli behawioralnych
- Możliwość implementacji własnej logiki alertowej
- Bezinwazyjny dla użytkownika
- Zgodność z wymogami RODO i PSD2
- Niemożliwe do podrobienia, zhakowania

Digital Fingerprints **anonimizuje** dane z interakcji z komputerem.
Istotne jest tylko **jak** użytkownik pisze, a nie **co**.
Dane biometryczne są zbierane na podstawie zgody użytkownika końcowego.

contact@fingerprints.digital