DIGITAL
FINGERPRINTS

BIOMETRIA, A BIOMETRIA BEHAWIORALNA - TO NIE TO SAMO!



Kliknij i poznaj różnice

DIGITAL FINGERPRINTS

Biometria behawioralna dotyczy naszych zachowań - nawyków, przyzwyczajeń czy preferencji widocznych w trakcie korzystania z komputerów czy smartfonów.

Sama biometria to z kolei wykorzystanie do autoryzacji indywidualnej cechy naszego ciała - najpopularniejszymi przykładami są odciski palców, linie i rysy twarzy czy też siatkówka oka.

DIGITAL
FINGERPRINTS

Co nastąpi, gdy właściciela konta chroni tylko biometria?

BIOMETRIA:

1. Cyberprzestępca wpisuje login i hasło do konta.
2. Zatwierdza dwuetapową weryfikację podrobionym odciskiem palców, wygenerowanym przez specjalny algorytm.
3. Po zalogowaniu na konto dokonuje transakcji, używając podpiętej karty kredytowej ofiary.
4. Płatność zostaje zrealizowana, ponieważ użytkownik został zweryfikowany tylko w momencie logowania oraz finalizowania transakcji, ale nie w trakcie korzystania z konta.

DIGITAL FINGERPRINTS

A co, gdy w tle działa biometria behawioralna?

BIOMETRIA BEHAWIORALNA:

1. Cyberprzestępca wpisuje login i hasło do konta.
2. Nie wykonuje żadnych dodatkowych czynności uwierzytelniających, ponieważ w tle działa już biometria behawioralna.
3. Cyberprzestępca próbuje zalogować się na konto - dane są poprawne, ale system wykrywa niezgodność zachowania z modelem behawioralnym właściciela.
4. Gdy biometria behawioralna wykrywa anomalię, czyli niezgodność za chowania cyberprzestępcy z profilem behawioralnym właściciela, już na etapie logowania blokuje dostęp do konta - tym samym neutralizuje próbę kradzieży środków z karty kredytowej.