PCBB BID® Daily Newsletter Oct 23, 2018

Climbing Into The World Of Invisible Biometrics

cyber security technology biometrics

Summary: Unlike traditional biometrics, such as a fingerprint, invisible biometrics use sensors or computer coding that are unknown to an individual. We provide you with the details of this new technology.

The tallest mountains in the world are Mount Everest at 29,029 feet, followed by K2 (28,251), Kangchenjunga (28,169), Lhotse (27,940) and Makalu (27,838). While the readers who are climbers already probably knew that, we ran across it and found it interesting, so we wanted to share.

As you prepare to climb your work mountain today, we delve into the world of biometric security. It wasn't that long ago that biometric security measures such as scanning an individual's iris or fingerprints were considered cutting edge. But, this is definitely not the case anymore.

The capabilities of cybercriminals have improved quickly, so new security measures have been improving as well. It has become increasingly difficult to secure customers' accounts, personal information and even their identities. Now, a handful of banks have begun employing new and updated security tactics known as "invisible biometrics."

Unlike traditional biometric safeguards, such as swiping a fingerprint, invisible biometrics use sensors or computer coding that are unbeknownst to an individual. The way each person holds their phone, swipes their screen, types on their computer keyboard and even uses their mouse is unique.

As such, invisible biometric programs are able to compile databases of thousands of behaviors unique to each individual. In the case of mobile apps, sensors are used to collect information, while computer coding records unique behavioral attributes. These include tracking everything from typing patterns and how fluidly people enter information like passwords or personal details, to how hard they hit the keys on their keyboard, and the way they move their mouse.

Because such data is collected without a user's knowledge, the information compiled is a legitimate depiction of that individual's true behavior and how it differs from the behaviors of others.

Given the extensive information on behaviors and gestures, it is easier to determine if an illegal attempt to use a bank account is made for instance. These programs essentially look for any digital indicator that shows cybercriminals are trying to impersonate an account owner or steal someone's identity.

While several banks have already begun experimenting with and employing invisible biometrics, most do not want their usage of these programs to be known. One exception is Royal Bank of Scotland, which has been testing invisible biometrics for more than 2Ys on bank accounts for some of its high net worth customers. By doing so, the bank has already been able to successfully identify hacking attempts on such accounts. Not surprisingly, invisible biometrics are rapidly gaining popularity, with roughly a dozen technology companies already specializing in the technology and shopping such security programs to banks.

By one security expert's estimates, 500mm passwords and 5B accounts have been compromised. The fight for cybersecurity is far from over. Though invisible biometrics are still far from being mainstream, given everincreasing sophistication of bad actors and the growing amount of fraud, community banks should at least be aware of this new security tool.

OUTSOURCED PROFITABILITY SOLUTION FOR YOU

ProfitIntel is an outsourced relationship profitability solution that combines a powerful pricing model with full-time consulting support. Contact us today for more information.

Copyright 2021 PCBB. *Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.*