Passwords are the weakest link when it comes to protecting digital accounts. Fraudsters take over accounts using well known password attack vectors like phishing, man-in-the-middle, brute force, and credential stuffing attacks, as well as emerging techniques leveraging AI. Unlike passwords, biometrics offer a more secure method of authentication, eliminating passwords and 56% of account takeovers. Contact us for a free consultation and learn how we can help you leverage multi-modal biometric authentication at your organization today.

Visit miteksystems.com/biometric-authentication to learn how we can help you leverage multi-modal biometric authentication at your organization today.

It’s time for a change!

It cracked in under a minute.

In 2022, the average cost of a data breach reached $4.35 million.

Sign up for our biometric updates

73% of people use the same or similar passwords across dozens of sites and applications.

The result is that most people end up reusing the same or similar passwords, which makes biometrics unique to every individual.

The best part about biometrics is that they are 100X more effective at preventing fraud with liveness detection, was demonstrated IDR&D testing.

An AI-powered password-cracking tool called PassGAN was recently tested against 15m+ passwords. —

Biometric authentication

Hate passwords?

Not only do passwords offer a more secure method of authentication, but they also provide a better user experience.

60% of organizations believe that a zero-password future is the future for their organization, and 81% in less than a month.

In fact, 90% of data breaches are caused by compromised credentials.

65% of users would increase their purchase confidence for a company that offers a reliable way to verify their identity.

A study by the Ponemon Institute showed that 73% of people use the same or similar passwords across dozens of sites and applications.

Fraudsters take over accounts using well known password attack vectors like phishing, man-in-the-middle, brute force, and credential stuffing attacks, as well as emerging techniques leveraging AI.

Passwords are the weakest link when it comes to protecting digital accounts. Fraudsters take over accounts using well known password attack vectors like phishing, man-in-the-middle, brute force, and credential stuffing attacks, as well as emerging techniques leveraging AI.