Mitek

Hate passwords?

Embrace the future with biometrics.

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.

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

It cracked 51% in under a minute

and 81% in less than a month.[1]

Unfortunately, today's digital economy has only made the problem bigger.

The **average person** now has approximately

100 passwords

to remember and manage.[2]

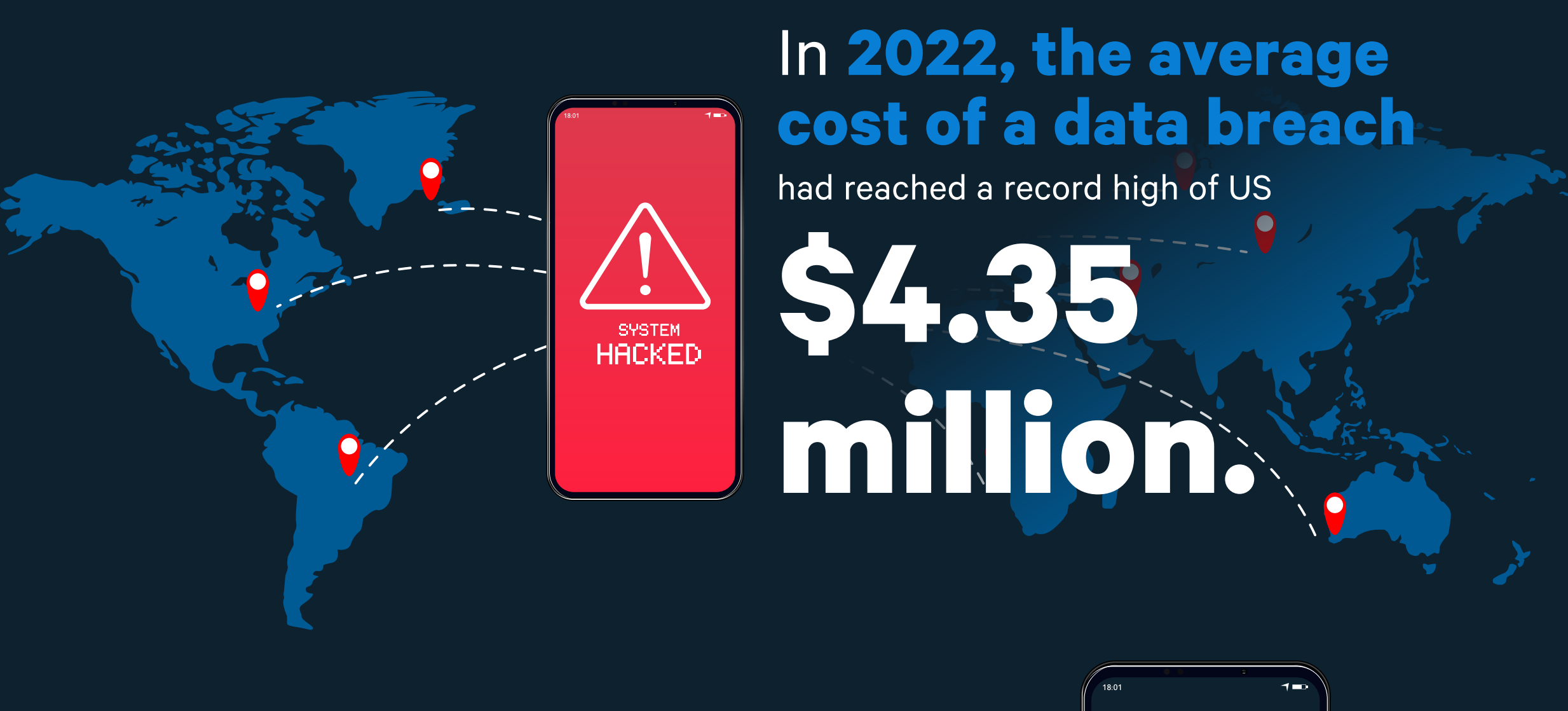
The result is that most people end up reusing the same or similar passwords across dozens of sites and applications.

73% of people **duplicate their passwords** in both their personal and work accounts.[3]

And **43% have shared** at least one password with a colleague, friend, or family member.[4]

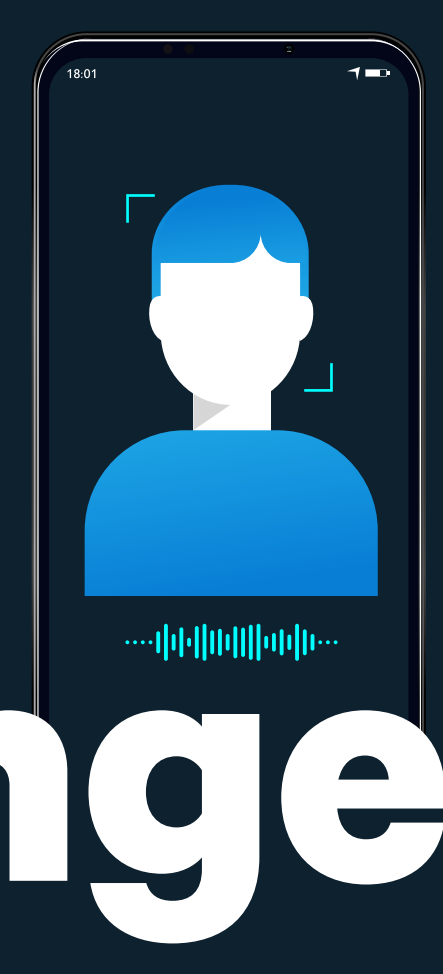
90%

This means BIG losses for companies, because **90% of data breaches are caused by compromised credentials.[5]**



In **2022, the average cost of a data breach** had reached a record high of US

$4.35 million.



It's time for a change!

Biometric authentication offers a reliable way to confidently authenticate customers without relying on passwords.

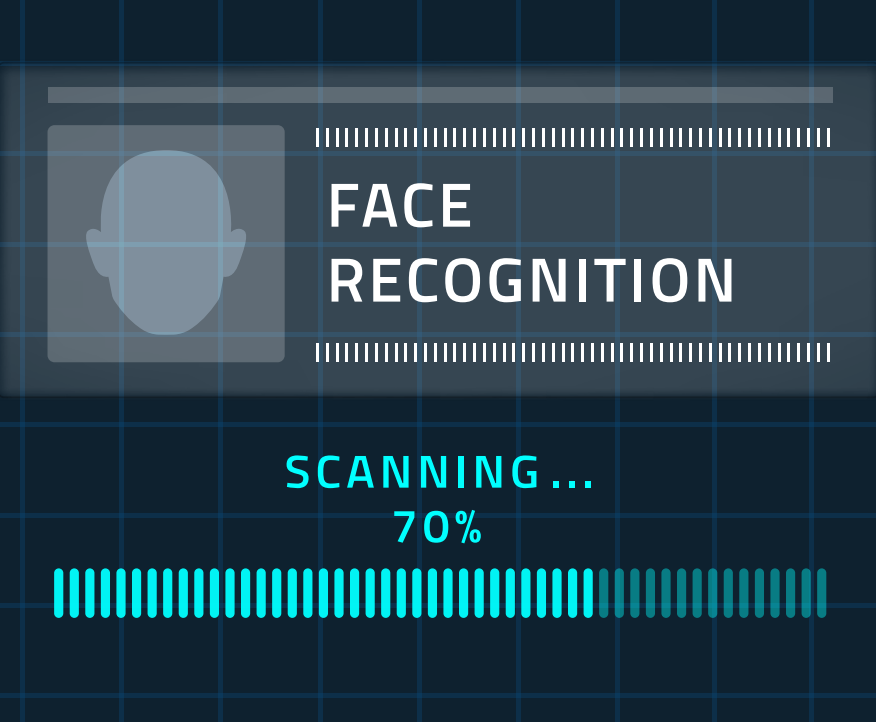
A study by the Ponemon Institute showed that **56%** of **IT professionals believe that eliminating passwords** would improve the security of their organization, and

65% believe biometrics would increase security.[7]

In fact,

92%

of organizations believe that **delivering a passwordless** experience for end-users is the future for their organization.[8]



The **best part about biometrics** is that they are unique to every individual. That means they cannot be shared, stolen, or forgotten, which makes biometrics an incredibly strong defense against fraud.

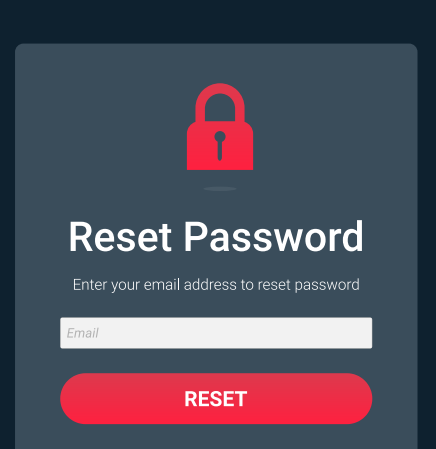
IDR&D testing demonstrated

that the **combination of face & voice biometrics,** coupled with liveness detection, was

100X

more effective at preventing fraud than traditional authentication methods.[9]

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

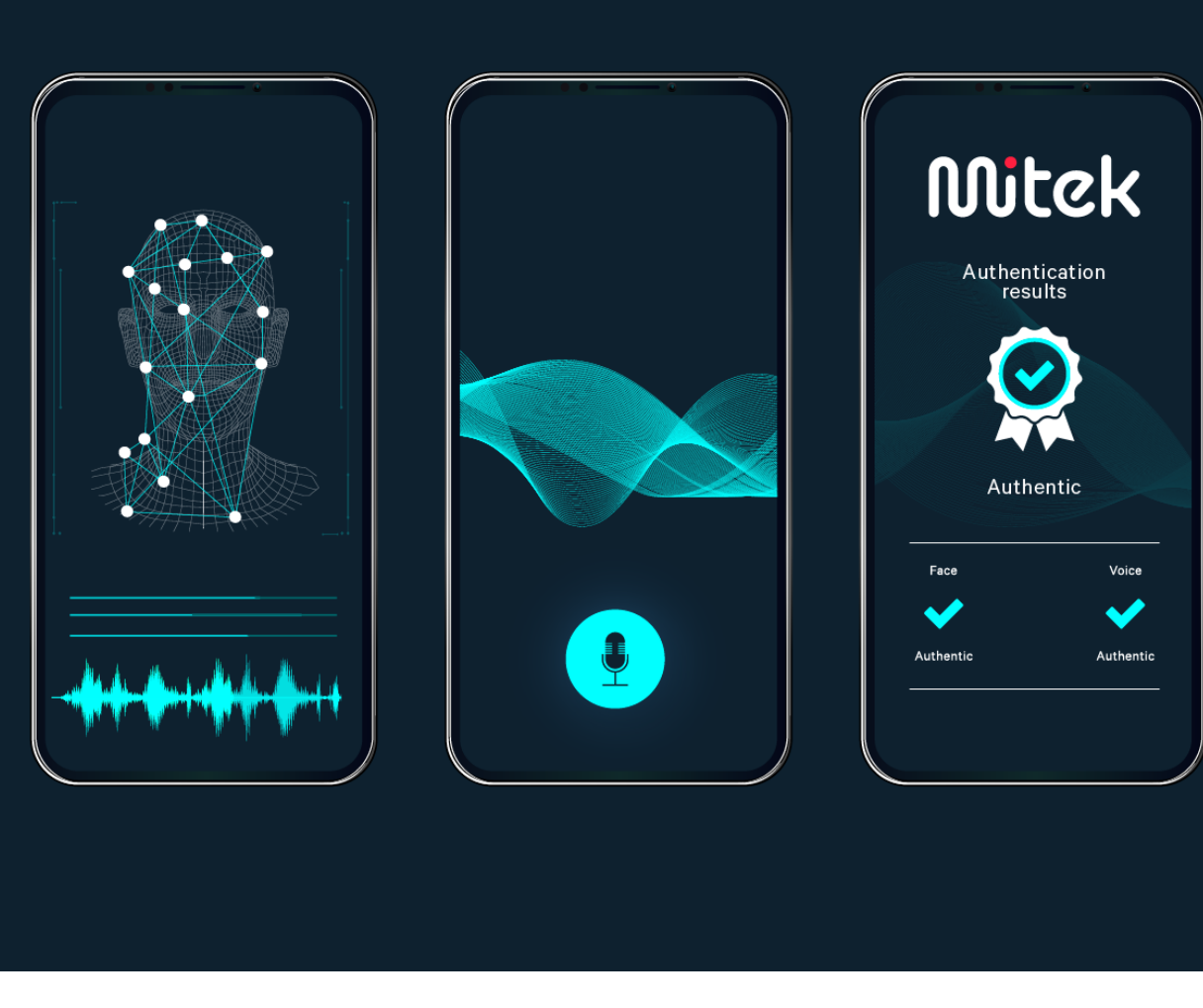


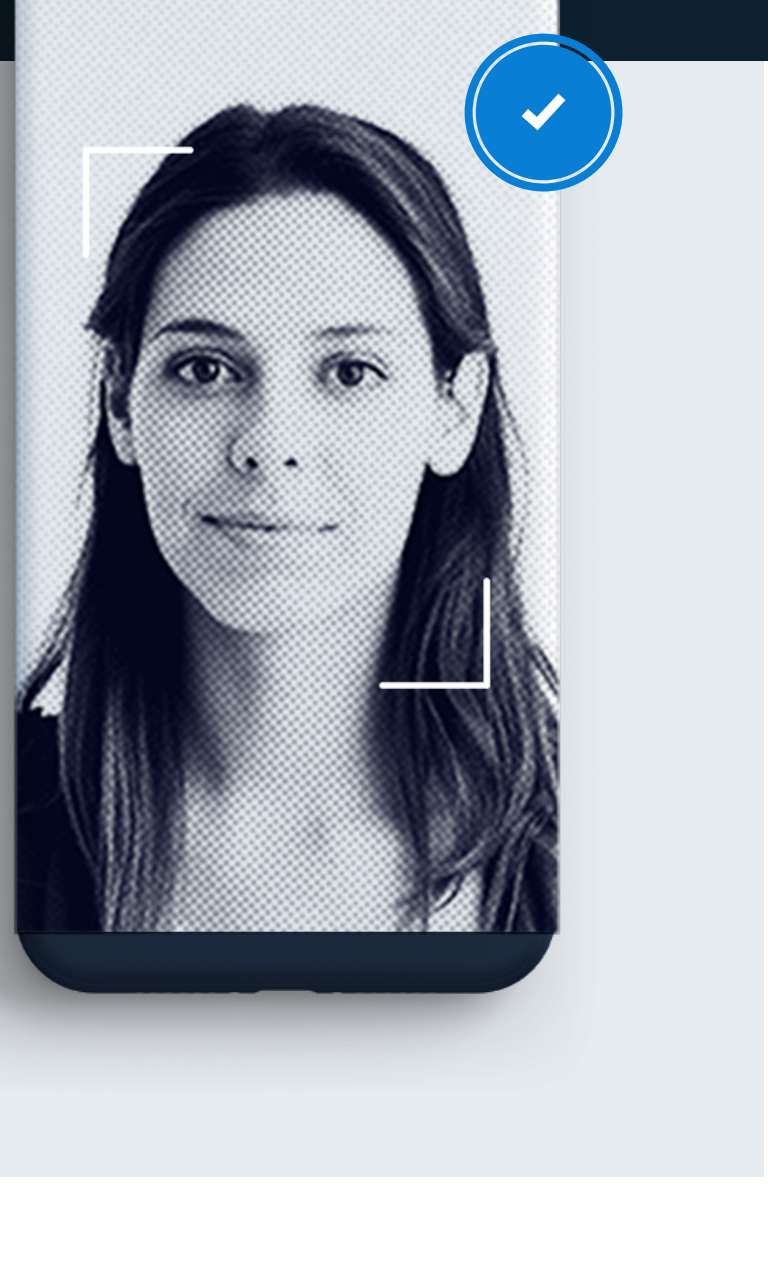
60%

of consumers say they have **abandoned a business transaction due to frustration with the authentication** process, and

81%

prefer to interact with companies that verify their identity **"simply, quickly, and safely."** [10]





MiPass from Mitek can affirm your customers' identities in seconds using multi-modal biometrics to provide secure, effortless access. You'll reduce customer friction, reduce helpdesk and IT costs, and secure your business by eliminating the most common attack vector for fraudsters.

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

Contact us

Sources:
1 https://thehustle.co/ai-roundup--guessing-passwords--conjuring-images-out-of-peoples--minds--and--writing-fortune-cookies/
2 https://www.zippia.com/advice/password-statistics/
3 https://www.enzoic.com/blog/8-stats-on-password-reuse/
4 https://cybersecurity.asee.co/blog/password-statistics-that-will-change-your-attitude/
5 https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
6 https://www.ibm.com/reports/data-breach
7 https://mms.businesswire.com/media/20200219005336/en/773763/5/191522-Ponemon-Infographic-2020-final-1.jpg?download=1
8 https://www.securitymagazine.com/articles/93522-of-businesses-believe-going-passwordless-is-the-future
9 https://www.idrnd.ai/5-reasons-to-make-biometrics-part-of-multi-factor-authentication/
10 https://www.biometricupdate.com/202110/consumers-prefer-biometrics-to-passwords-think-less-of-brands-with-bad-authentication