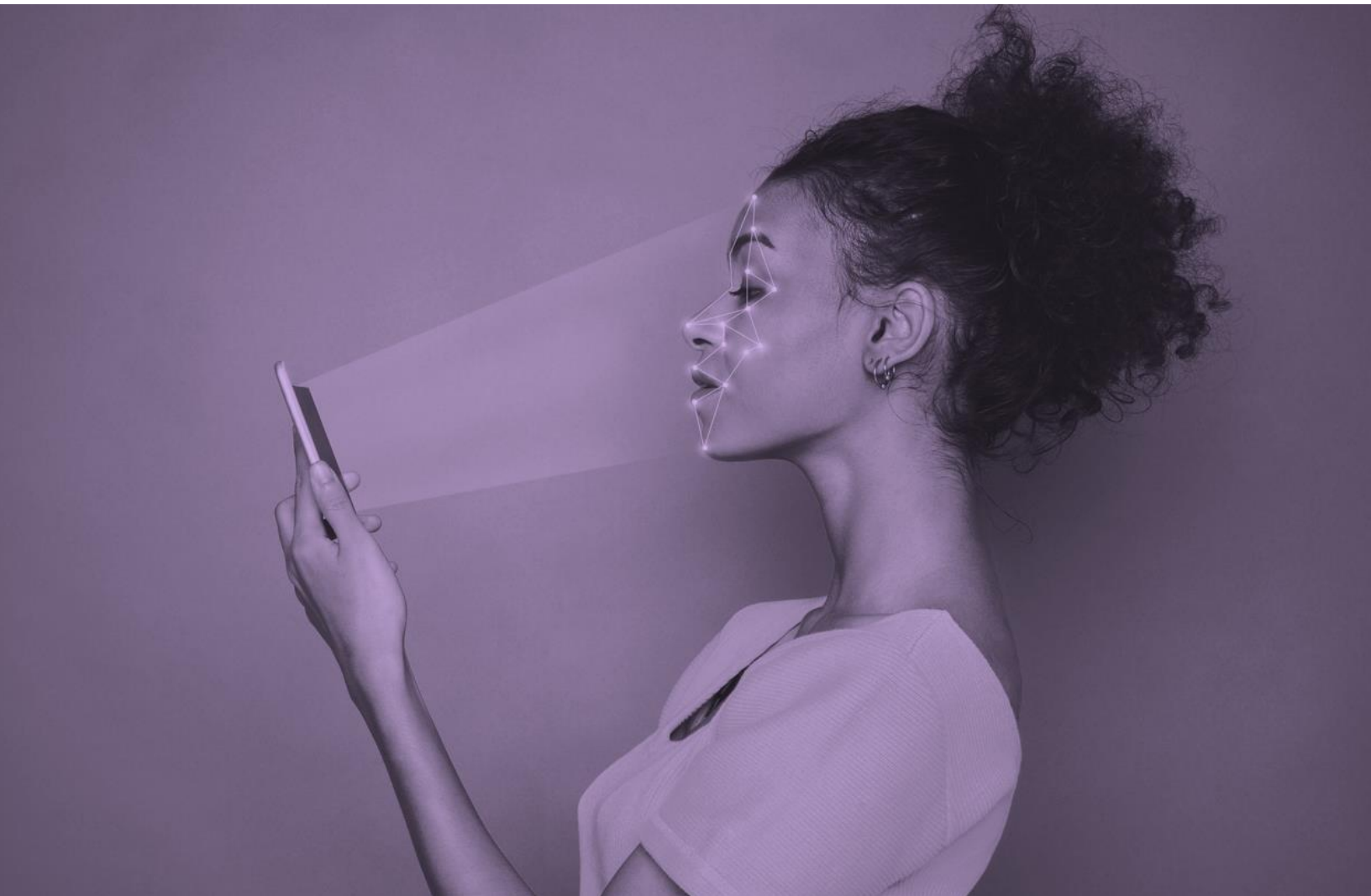
BlokSec

Tokenless Multi-Factor Authentication

Reduce your risk exposure with tokenless multi-factor authentication



Contents

Summary

Multi-factor authentication provides organizations with a stronger security control that overcomes the weaknesses of knowledge-based, i.e. password, authentication and protects applications and mobile apps. By combining passwords with physical devices and/or biometric options, organizations add a layer of authentication security and protect against credential harvesting theft.

Recent advances in multi-factor authentication along with large scale adoption of mobile devices, enables organizations to support widespread deployment of this technology for their users i.e. internally within the organization or for their customers. Using multi-factor authentication is now as simple as unlocking a mobile device that a user is already carrying. This simple and intuitive approach improves authentication security while increasing user satisfaction.

Over 80% of hacking-related breaches involve the use of stolen credentials

Source: Verizon DBIR 2020

According to Verizon's recently released 2020 Data Breach Investigations Report (DBIR), over 80% of hacking-related breaches involved the use of lost or stolen credentials. Data breaches can cause devastating financial losses and affect an organization's reputation and brand for years. From lost business to regulatory fines and remediation costs, data breaches have far-reaching consequences.

Over 15 billion credentials for sale on dark web

Source: Forbes

More than 15 billion username and password credentials to online digital services, including bank and social media accounts, are openly for sale on the dark web – over three times the amount available to cyber criminals just two years ago. The impact of compromised credentials can include the breach of sensitive information and the compromise of IT systems and data, a serious loss of brand reputation, and financial losses that include the cost of responding to and remediating a breach, as well as lost sales.

What's wrong with passwords?

Password-based authentication has always been challenging for organizations throughout the evolving security landscape. The key problem with password authentication lies in the fact that passwords are simply static information that can be easily stolen and used by a malicious actor without the knowledge and consent of the rightful owner.

The authentication that is based on a user's knowledge of the secret, i.e. a password, to access an account containing sensitive information is no longer a feasible option to protect the account from attackers. To distinguish between the account owner and the attacker, organizations need to move beyond using just passwords for protection.

What is Multi-factor Authentication?

Multi-factor authentication is the process of identifying users by validating two or more “factors,” or characteristics that are unique to that user. These characteristics are often used as factors in the authentication process:

- something you know
- something you have
- something you are

Common implementations of two-factor authentication include the “something you know” factor (i.e. password) and “something you have” (i.e. one-time passcode sent to your smartphone or provided via a token).

While authentication is the process by which a user’s identity is verified (i.e. username and password), multi-factor authentication adds an additional layer of protection and security against one of the most common types of breach - compromised credentials. Without the added layer of security through multi-factor authentication, it is more difficult to truly verify that the user who accessed the system is who they say they are because passwords are very easy to steal and guess**.**

Tokenless MFA + Passwords. More secure.

As passwords have become less secure due to sophisticated and advanced attack vectors, the use of multi-factor authentication solutions has become widespread within the enterprise and customers / partners of the enterprise. In addition, with the proliferation of SaaS-based web services and the number of reused passwords, multi-factor authentication methods have become more important.

To enable the next generation of modern authentication, BlokSec has built an authentication platform to support strong authentication. BlokSec's platform provides security and privacy by design, leveraging a patent-pending consent-based approach for authentication. Advanced technologies like biometrics and cryptography, built upon passwords, ensure user identity.

The mobile device used as part of the multi-factor authentication process creates a unique private key that is stored locally on the device and can only be unlocked using a local gesture such as a biometric recognition (fingerprint scan, facial recognition) associated to the user of the mobile device. This modern approach to multi-factor authentication ensures that the person is who they say they are – i.e. the account owner – rather than an attacker.

BlokSec's modern multi-factor authentication, built on top of its decentralized-identity-as-a-service platform, provides stronger security than the traditional method of multi-factor authentication available today i.e. SMS or token-based (software or hardware). With the biometry multi-factor authentication, the user is not required to enter a one-time SMS or token, increasing user satisfaction by reducing the friction.

To provide user authenticity, the BlokSec platform leverages decentralized identity, personal smart contracts and distributed ledger

technology to provide a consensus-based digital signature verification process. This approach makes it impossible for attackers to bypass traditional multi-factor authentication via various methods including tools such as Evilginx**.**

BlokSec's multi-factor authentication solution can be used to authenticate across any service a user interacts with – consumer websites, mobile apps, and web-based business applications.

BlokSec's unique approach to transaction logging by leveraging a distributed ledger technology that provides tampered-proof auditing to help organizations to support audit and compliance requirements for important transactions**.**

Multi-factor authentication use cases

Retail

Online retail fraud is estimated to surpass more than $12 billion in losses by 2021 based on a recent study published by Signal Sciences. Account takeover, is the main offender constituting 29.8 percent of all eCommerce fraud.

Here's how it works: When a malicious actor finds or steals user credentials, they enter the account, change their settings i.e. email and phone number, and lock out the user. Next, the malicious actor essentially takes over the account and purchases from the site. They can also run automated tests of the same credentials against other sites.

Multi-factor authentication provides an added layer of security to stop the malicious actors to gain access to an account and act as the user without their knowledge and consent.

With BlokSec's biometry multi-factor authentication retail organizations can reduce fraud and increase their revenue by offering a frictionless and secure login experience.

Finance

According to Terbium Labs, credentials for financial accounts ranks in the top five most popular resources for sale on dark web marketplaces. Credentials can be purchased starting from $100+ based on the funds available in the bank account.

Phishing is by far the most common type of attack carried by malicious actors because they prey on a person's fear and sense of panic.

With multi-factor authentication, a second layer of security is added – stopping the malicious actors to act on behalf of the user without their knowledge and consent.

With BlokSec's biometry multi-factor authentication finance / banking organizations can reduce fraud and increase their revenue by offering a frictionless and secure login experience.

Loyalty Rewards Programs

Loyalty and rewards programs are growing and becoming increasingly popular with businesses and consumers. According to LoyaltyOne, a loyalty advisory company, there are more than 3.8 billion rewards memberships in North America. The loyalty rewards accounts in North America are worth more than $60 billion with an estimate of $250 billion globally according to Loyalty Fraud Prevention Association group. According to PYMNTS, attacks on loyalty accounts rose nearly three times from 2016 to 2017, at a global cost of $2.3 Billion (USD) and are expected to keep rising in the next 5 years.

In 2019, account takeover attacks increased by 79% year-over-year. With the rise of account takeovers, organizations offering loyalty rewards programs will require increased attention and investment in cybersecurity. Peter R. Maeder, co-founder of the Loyalty Fraud Prevention Association, in an interview with PYMNTS pointed out that "biometric technology, such as fingerprint and face scanning, are tools that could be used to prevent fraudsters from gaining access to accounts".

With BlokSec's biometry multi-factor authentication, organizations can help themselves and their customers from being victims of digital fraud.

Health Sector

According to Health IT Security, the health sector was the most targeted by hackers in 2019 with breach costs rising to $17.76B. As healthcare institutions go through digital transformation and allow access online via websites or mobile apps, the threat vector also increases.

Unauthorized access and phishing were the most common type of breach accounting for 54% of incidents in 2019.

With BlokSec's modern multi-factor authentication, health care institutions can curb unauthorized access to stop exposure and leak of sensitive healthcare data.

Multi-factor authentication can help healthcare institutions reduce risk exposure and reduce the cost of data breaches.

BlokSec provides decentralized-identity-as-a-service (DIaaS)™ to support the next generation security features to stop account takeovers, phishing attacks, online fraud and identify theft.

Let's keep in touch.

inquiries@bloksec.com | bloksec.com | @bloksec