okta

6 ways strong customer authentication makes your user experience flow

To satisfy customers' demands for simple and secure digital experiences, organisations are turning to strong customer authentication as part of a modern customer identity & access management (CIAM) solution. Here are 6 ways stronger identity security helps turn friction into flow.

1

Simple login that customers love

Passwords are a hassle to remember and easily hacked. A modern CIAM solution allows you to offer a choice of convenient login options, such as single sign-on and social login, which eliminate the need to create vulnerable usernames and passwords.

83%
of customers have abandoned an interaction due to a slow login process
Source: Auth0, Expectation vs Reality at the Log Inn

53%
log in with social media credentials all or some of the time
Source: Auth0, Expectation vs Reality at the Log Inn

2

Extra assurance with MFA

Passwords breached elsewhere could be used to attack your systems. MFA adds an extra layer of security by requiring users to validate with another factor, such as a one-time code, ensuring your organisation is protected even if a password has been compromised.

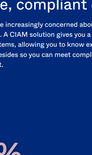
86%
of customers reuse passwords across multiple sites
Source: Auth0, Expectation vs Reality at the Log Inn

70%
of breached passwords are still in use
Source: SpyCloud, 2022 Annual Identity Exposure Report

3

Security you can dial up or down

One-size-fits-all security adds needless friction for low-risk customers. With adaptive MFA you can require extra verification only when it's needed – for example, when your customer is entering sensitive information, or appears to be logging in from an unusual location or device.



49%
of customers are more likely to sign up to an app if it offers MFA
Source: Auth0, Expectation vs Reality at the Log Inn

75%
reduced risk of a security breach with adaptive MFA
Source: Okta

4

Automatic threat detection

Identity attacks involving stolen credentials are rising fast and can be costly in reputational damage and loss of trust. A CIAM solution has security features that can spot suspicious activity, detect breached passwords and block malicious IP addresses before they have a chance to attack your systems.

61%
of cyber attacks in 2021 involved stolen credentials
Source: Verizon Data Breach Investigations Report 2021

3 attacks that threaten identity security

- Phishing
- Credential stuffing
- Password spraying

Source: Okta, 5 identity attacks that exploit your broken authentication

5

Private, compliant experiences

Customers are increasingly concerned about the privacy of their personal data. A CIAM solution gives you a streamlined user view across all systems, allowing you to know exactly where consent information resides so you can meet compliance requirements with minimal effort.

65%
of the world's population will have its personal data covered under modern privacy regulations by 2023
Source: Gartner

71%
of customers would stop doing business with a company if it gave away sensitive information without permission
Source: McKinsey

6

Free up developers to innovate

Developers are in short supply – you want them to use their time building great products. A modern identity solution provides a standardised approach to adding identity, freeing up your developers to focus on what they do best.

4 million
shortage of full-time developers by 2025
Source: IDC

Build trusted digital experiences with Okta

Use Okta's customer identity solutions to build frictionless login and registration experiences that your customers and developers will love. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta is trusted by over 14,000 brands worldwide to secure digital interactions and accelerate innovation.

To learn more about protecting your business with strong customer authentication, **watch the video podcast** with Brian Glick, Computer Weekly Editor in Chief, and Okta's Ian Lowe.