SPOTLIGHT REPORT

Authentication UX Has Widespread Business Impact

Key Takeaways

64%

of organizations say a poor user experience is a major authentication pain point

Four

different systems for authentication are being used by employees daily

$375/employee

spent on password-related help desk issues annually

39%

of financial services firms plan to adopt/use passwordless (or passkeys) authentication in the next 1-3 years

Introduction

Nearly every aspect of conducting business today begins with an act of authentication. Communicating, using tools, interacting with data, processing transactions – all depend on the ability to verify our identity to gain access. Much attention is paid to the consequences of poor authentication security — just check the headlines for the latest breach — but the user's experience (UX) of authentication also has a profound impact on an organization.

HYPR and Vanson Bourne recently published our 2023 State of Passwordless Security Report, which surveyed 1,000 IT and security experts to better understand current perceptions, challenges and trends when it comes to authentication and IAM. In this State of Passwordless Spotlight report, we dig deeper into the findings, focusing on how the authentication user experience affects organizations and their employees and customers.

This Spotlight Report also specifically looks at the impact of UX on financial services organizations. Finance is the top sector for attacks and is subject to rigorous regulations around security and authentication. As such, it frequently serves as a bellwether in the IAM sphere, providing an early look at important developments and trends.

Authentication UX Challenges

Our research shows that organizations face significant challenges when it comes to authentication and user experience. Nearly two-thirds of surveyed companies (64%) cite challenges with user experience as a major pain point in their authentication processes.

Poor UX not only leads to user frustration and dissatisfaction, it obstructs work, increases costs and actually decreases security because users can bypass certain security features meant to protect the user, systems and data.

Productivity Lost to Time Consuming Logins and Lockouts

There's no getting around it, login methods that rely on passwords create friction, which only gets worse as security stipulations like long, complex strings, frequent rotation and additional authenticating factors are imposed. In 2024 this will be compounded with PCI 2024 requiring longer passwords.

There's also significant time wasted when employees forget their passwords and require resets. Nearly 3 in 10 (29%) of IT and security professionals cite password/credential resets as an ongoing pain point for their organization. Moreover, around eight in ten (81%) report they've been unable to access critical information due to forgetting their password.

81% could not access work-critical information because they forgot a password

Password-Based Authentication Increases Help desk Spend

Poor UX not only harms employee productivity, it places a significant strain on the help desk support system. Over the last 12 months, 76% of organizations had an increase in help desk requests relating to password resets or other authentication issues. In terms of actual costs, organizations spend 32% of their IT help desk budget on password resets and password-based authentication issues. This breaks down to $375 per employee per year, wasted on password issues.

$375 per employee per year is wasted on password issues

Array of Authentication Systems and Requirements

Organizations also face challenges from the sheer variety of authentication systems used on a daily basis — four on average. This means multiple, varying sign-on requirements that employees must remember and use, adding friction and frustration in their day-to-day work.

Four different systems of authentication are being used by employees daily, on average

A Good UX Is Critical to Security

Any security control is bound to fail if people don't use them willingly. Nearly a third (31%) report resistance from employees in using their organization's authentication technology. Resistance frequently expresses itself in workarounds that create security risks for organizations. Employees may share passwords, store password lists on their computers or leave their systems signed in while they are away, some even use tools like a mouse jiggler to avoid having to re-authenticate.

Don't forget IT

We don't usually put the IT experience in the UX category but we should. The IT user experience also impacts adoption, costs and security. The survey found that 56% of organizations face IT-related obstacles in their current authentication approaches, including management complexity (34%) and integration difficulties (31%).

Outsized Impact on the Finance Sector

We already know that the finance sector experiences the most attacks on its authentication processes — 81% for those in financial services vs. a global average of 74%.[1] They also face tremendous pressure from regulations and security frameworks to implement stronger authentication processes to combat these greater risks.

[1] 2023 State of Passwordless Security Report, HYPR, March 2023

Most of the regulations currently on the books require multi-factor authentication, which traditionally incorporates a password as one of the factors. This is creating demonstrable friction in financial services organizations. For nearly every UX issue discussed above, the finance sector has been hit even harder.

- 85% of respondents in the finance industry report they've been unable to access work-critical information due to forgetting a password; 5% higher than the global average
- The help desk spend on password-related authentication issues is $389/employee vs. a $375 average across industries
- Nearly half (48%) face challenges in implementing traditional 2FA/MFA due to time consuming login

Passwordless Authentication Improves UX

Authentication plays a central role in enterprise digital transformation and almost every other strategic initiative or service. A poor authentication experience can slow or even derail projects so it's critical to get it right.

Nearly half of the IT and security (45%) experts name improved user experience as the reason to move to passwordless authentication. A full 86% believe passwordless authentication helps ensure user satisfaction. Benefits of passwordless authentication, specifically FIDO-based (passkeys) authentication include:

- No password resets
- Faster login speeds: FIDO-based passwordless MFA uses a single, secure gesture for login that is up to 3 times faster than traditional MFA
- Reducing account lockout
- Consolidating multiple authentication systems into one
- Increased employee and customer satisfaction

86% believe that passwordless authentication is needed to ensure user satisfaction

Conclusion

These findings reveal the toll that the authentication user experience can take on all aspects of a business. Many organizations are contending with significant hits to productivity and their bottomline due as a result of their current authentication practices.

Passwordless MFA That Is Built for Users

HYPR's passkey-based solutions are designed from the ground-up for the way people work and live. We apply UX best practices and principles in tandem with strong security for phishing-resistant authentication that people want to use. Designed to deploy rapidly into existing infrastructure, it turns an ordinary smartphone into a FIDO Certified passkey for frictionless authentication everywhere. In a single, secure authentication gesture, users gain seamless access to their desktop device and all downstream local and cloud-based applications. HYPR secures organizations globally with large-scale deployments in some of the most complex and security-focused environments, including two of the top four banks.

THE PASSWORDLESS COMPANY

info@hypr.com | www.hypr.com

HYPR fixes the way the world logs in. HYPR's True Passwordless™ MFA combines phishing-resistant multi-factor authentication with an intuitive and simple user experience so that organizations decrease their risk of attack, improve user experience, lower operational costs and ensure regulatory compliance.