Overcoming Customer Identity Challenges Without Compromising the User Experience

New IDG survey data defines the problems of passwords for customer identity and access management, and highlights what companies can do about it

In the fight against hackers and identity thieves, passwords are losing.

That's because passwords are difficult to remember, end up getting used more than once for different services, and are relatively easy to hack, among other problems. Fortunately, enterprises are well aware of the issue and have prioritized finding solutions, according to new research.

Okta and IDG surveyed 300 IT and business leaders in the U.S., the U.K., and the Asia-Pacific region to learn how companies across major industries are addressing the password problem.

"We need to improve the customer authentication process," summed up one survey respondent.

The survey determined that passwordless authentication is on the radar for the vast majority of companies. At the same time, survey respondents don't believe they need to sacrifice usability for greater security. Survey data point to ways they can do justice to both imperatives, thanks to advanced customer identity and access management (CIAM) methods that not only enhance security but also provide a more seamless experience for users.

Survey respondents cited security risks with passwords for authentication as their top concern.

"Remembering various complicated usernames and passwords not only becomes frustrating to customers, but today's hackers are more skilled than ever before, and they're not going away," one survey respondent said.

A Challenging IT Environment

That's far from an isolated complaint as both users and the organizations they work for or do business with struggle to maintain security in today's challenging IT environment with an authentication method that's more than half a century old.

Most organizations surveyed report having been significantly impacted by weak or common passwords (84%), phishing attacks (80%), and credential sharing (81%). Both phishing attacks, which depend on users giving up login information in response to official-looking but bogus emails, and credential sharing highlight the vulnerabilities inherent in passwords.

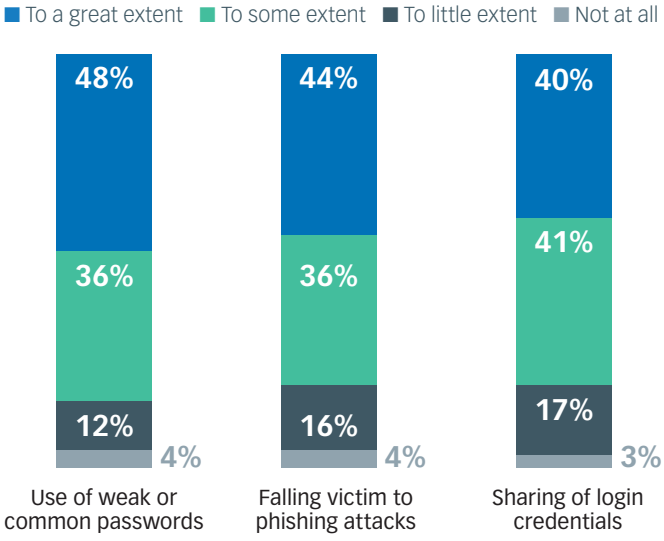
okta

SPONSORED CONTENT

IDG

FIGURE 1.

Impact of Customer Behaviors on Security Posture



Source: IDG

The negative impacts of these vulnerabilities include reputational damage (cited by 59% of respondents), resources getting diverted from other initiatives to deal with the fallout (57%), legal or regulatory fines (52%), and financial losses from outright fraud (50%).

The financial sector is particularly vulnerable to monetary loss, with 68% of respondents in financial services reporting losses to fraud stemming from mismanagement of customer credentials.

More than three-quarters (79%) of respondents with IT, procurement, and/or security responsibilities in the manufacturing sector reported having to reallocate internal resources to address problems with customer credentials. That makes sense, given the sector's relatively low IT expenditures relative to company size. In other words, manufacturing company IT departments are more likely to have to spread themselves thin, especially in times of crisis, when dedicated crisis management teams are not available.

Respondents in the retail industry reported damage to their brands' reputation from credential problems at the highest rate (74%). That should come as no surprise, given increasing concerns among consumers about how the brands they do business with handle their data. Nearly half (49%) of consumers polled in a recent study expressed skepticism of brands saying they had resolved data security issues. Nearly three-quarters (74%) of those surveyed said they believed security issues hadn't gotten better or had worsened over the previous year.

Given the vulnerabilities present in every major industry, it's no wonder, then, that 83% of all those surveyed in the IDG study perceive account takeover (ATO) attacks as a security risk. Of that percentage, nearly half (44%) see ATO attacks as a top security risk, versus 39% who see them as concerning but not necessarily as their top priority.

Looking for Alternatives

All of the problems with passwords add up to the vast majority of IT and business leaders (79%) reporting that they have plans in place to augment or outright replace passwords for user authentication. This finding is consistent across regions.

The U.S. leads in the move to augment or replace passwords, with 83% of respondents reporting plans to do so. More than three-quarters (78%) of respondents in the Asia-Pacific region also have plans to replace or augment passwords. But even in the U.K., the region reporting the lowest numbers planning to replace or augment passwords, 69% of respondents said their organizations would do so in the foreseeable future.

Clearly, passwords are losing importance as other, more secure, and also more user-friendly options take hold. In fact, Gartner predicts that by 2022, most enterprises will deploy passwordless methods for more than half of all use cases requiring authentication. Ninety percent of midsize enterprises will go passwordless for most use cases, including for authenticating customer identity, according to the research firm, and so will 60% of even the biggest, slower-moving organizations.

The User Experience Imperative

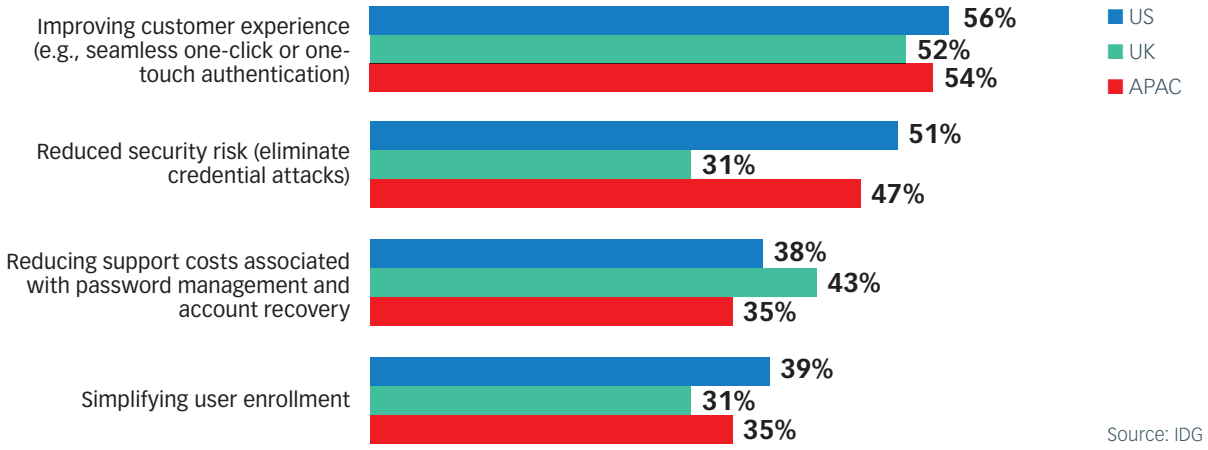
Survey respondents agree that any replacement for passwords must be easy to use. After all, even the most secure solution does no good if people won't to use it. As one respondent put it, "It may be difficult to persuade customers to change over from traditional passwords."

When asked to name the number-one most-appealing benefit for any solution designed to replace passwords, more than half of the respondents in all regions chose improving the customer experience.

> **"Remembering various complicated usernames and passwords not only becomes frustrating to customers, but today's hackers are more skilled than ever before, and they're not going away."**
>
> IDG SURVEY RESPONDENT

FIGURE 2.

Most Appealing Potential Benefits of Passwordless Customer Authentication (by Region)



Source: IDG

Reduced security risk was the second-most cited benefit of passwordless authentication.

And the two imperatives—usability and security—go hand-in-hand.

More than half (58%) of U.S.-based respondents said that the use of weak or common passwords impacted their organization's security posture "to a great extent." In other words, some of their biggest security headaches resulted from bad security hygiene caused by poor user experience.

Finally, reducing support costs associated with password recovery and account management rounded out the top three most-cited benefits of passwordless authentication. That's in alignment with the survey finding that 25% of support center or help desk calls relate to account lockout caused by passwords or multifactor authentication problems.

Along with those benefits, respondents cited speed of authentication and the ability to integrate with their existing technology infrastructure as critical elements of any authentication solutions they might consider.

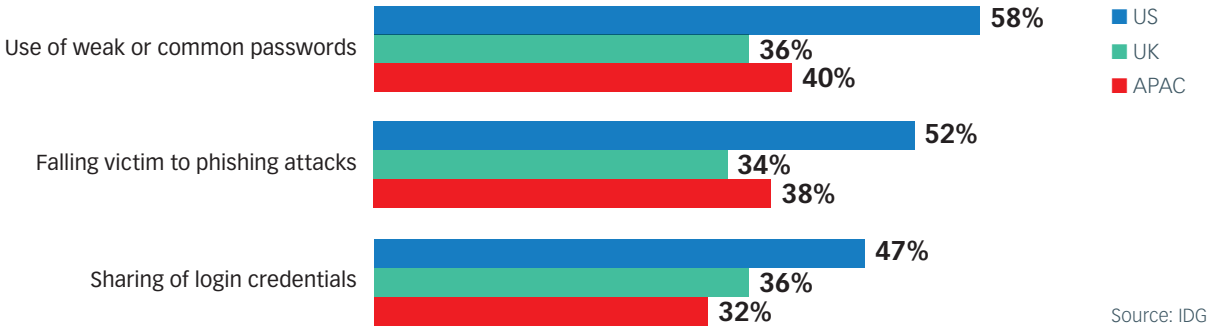
Next-Generation Authentication

Survey respondents showed a preference for three main types of user authentication to augment or replace traditional passwords. These were:

☑ **OTP-based primary authentication**
Considered by 70% of respondents, one-time password-based authentication, or OTP, depends on a password generated for a single login. The password may be delivered as a sequence of numbers via software, text message, or other means.

FIGURE 3.

Impact of Customer Behaviors on Security Posture – % Rating "To a Great Extent" (by Region)



Source: IDG

Market Pulse

☑ **Email "magic links"**
Magic links get high marks for usability since they enable users to log in to a web-based service with a simple click of a unique link sent via email. A cookie placed in the user's browser keeps them logged in, doing away with the need for passwords. Sixty percent of respondents said they were considering emailed magic links for user authentication.

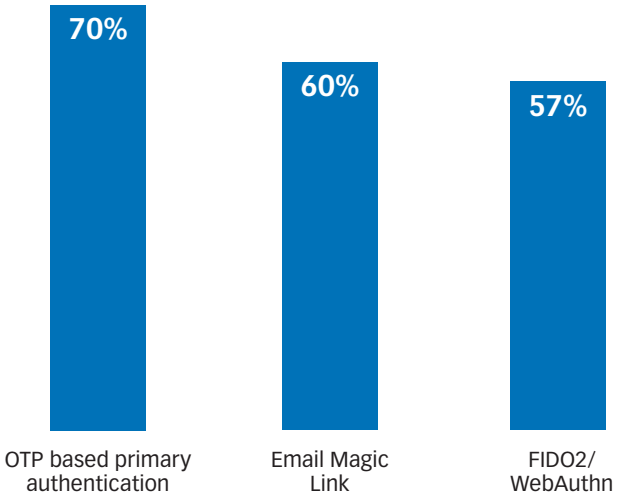
☑ **FIDO2/WebAuthn**
Among the most advanced passwordless authentication methods, FIDO2/WebAuthn pairs web-based applications with an authenticated device such as a mobile phone or hardware-based security key. The physical key plugs into a USB or other port or relies on near field communication (NFC) for authentication to log into the application. While not as widely considered as the other two methods on this list, 57% of respondents view FIDO2/WebAuthn as a strong contender for password replacement. Among the benefits of FIDO2/WebAuthn: widespread browser and mobile device support and faster login times.

Conventional password authentication, a method first deployed in the 1960s at the dawn of the modern computer era, is no longer up to the security and user experience challenges of today's digital economy.

An ever-growing set of threats and an increasing reliance on logins for every aspect of life (including entertainment, shopping, and financial transactions) have put severe strains on applications and services that rely on passwords for authentication. As one survey respondent put it, "In the era in which we now do business, our customers' data security is not only critical, but their vulnerability increases almost daily."

> **"We need to keep pace with the new technology developments in order to provide faster, easier, and safer support to our clients."**
>
> IDG SURVEY RESPONDENT

FIGURE 4.
Approaches to Passwordless Authentication Under Consideration (among those at least somewhat likely to consider passwordless solutions)



Source: IDG

Given all the challenges with passwords, the vast majority of IT and business leaders report having plans to bolster or even replace passwords as their primary means of user authentication.

Modern authentication methods such as one-time passwords, magic links, and WebAuthn point the way forward. Such methods can improve the user experience, enhance security, and lower support costs for organizations. "We need to keep pace with the new technology developments in order to provide faster, easier, and safer support to our clients," summed up a survey respondent.

To learn more about how passwordless authentication can improve your organization's security and the user experience, visit **https://okta.com/passwordless-authentication**.