IBM Security

IBM Security: Future of Identity Study

Consumer perspectives on authentication: Moving beyond the password

IBM

Click here to start ►

Contents

Introduction

The concept of granting digital access to users based on proper identification has been the very core of how people access online services since the emergence of the public internet in the 1980s. The power of confirming an identity and being granted access to services of value has attracted billions of users to the internet, and as society moved to this parallel universe, so have other parts of it, namely fraudsters, con men and organized crime.

In the past six years, USD 112 billion has been stolen through identity fraud, equating to USD 35,600 lost every minute. The more services are offered to the general public—with additional features for convenience and usability that rely on the internet—the wider the window of opportunity for attackers. Javelin Strategy Research expects fraud related to the creation of new online accounts to rise as much as 44 percent by 2018, increasing losses from USD 5 billion to USD 8 billion in a matter of four years.

While consumer personal information has been compromised on an ongoing basis for years, the massive data breaches of 2017 removed all doubt: Criminals clearly have access to the very information that many banks, companies and other businesses use to grant their users remote access to services. Even social security numbers, which are considered highly private and sensitive personal information, were exposed for hundreds of millions of consumers in 2017.

Recent data breaches have been a resounding wake-up call to the fact that new methods are needed to validate our identities online. In an era where personal information is no longer private, and passwords are commonly reused, stolen or cracked with various tools, the traditional scheme of accessing data and services by username and password has repeatedly shown to be inadequate.

In the past six years, USD 112 billion has been stolen through identity fraud, equating to USD 35,600 lost every minute.

Contents

Evolving authentication methods

Evolution in authentication schemes that move away from passwords has thus been a natural and necessary progression to help secure both individual identities and the organizations providing consumers with services. In an effort to replace traditional passwords, biometric authentication options—such as fingerprint or facial recognition, keystroke dynamics and voice recognition—are becoming more widespread and are seeing increasing popularity amongst the general population. The use of fingerprints to access the latest smart devices is now pervasive, and newer identification models, like facial recognition, quickly rose to the forefront in 2017. The latest iPhone and Samsung smartphone models now offer login via facial recognition, as do banks and ecommerce shops, and the method is likely to see rapid mainstream adoption in 2018 given the smartphone vendors' huge consumer base.

While biometric authentication has gained popularity in recent years, the simple scheme of username and password has been the most common form of accessing services online for decades. This pattern of internet usage—and the visual of the simple sign-in box—are both now deeply embedded in the average internet user's psyche.

Thus, the widespread introduction of multilayered authentication options represents a major change in the way that we relate to the web. Biometric and other forms of multilayered authentication are often presented to users as options that they can choose to adopt (or not) in a variety of ways—such as choosing to log in via fingerprint versus PIN, setting up knowledge-based answer questions to verify logins, or adding an additional step of verification for certain access events or transactions.

Users will ultimately choose whether or not to implement new security features being made available. Therefore, it is critical to better understand their concerns and preferences around emergent types of authentication and to evaluate how these views could impact the future of identity and access.

Contents

Survey at a glance

Survey methodology

IBM Security commissioned a global survey to gain insight into consumer perspectives on current authentication methods—from passwords and biometrics to multifactor authentication schemes—as well as their adoption rates and concerns about functionality and security.

The 15-minute online survey totaled responses from 3,977 adults across the United States (US), European Union (EU) and Asia-Pacific (APAC) regions, including:

- **US: 1,976 respondents**
- **EU: 1,004 respondents (United Kingdom, France, Italy, Germany, Spain)**
- **APAC: 997 respondents (Australia, India, Singapore)**

Key takeaways

Respondents prefer **security over convenience,** particularly for their financial apps and accounts.

Biometrics are indeed seen as part of the future, but change does not come without concern—particularly when it comes to privacy and how that data is collected and stored.

Age is a major influence on attitude toward security and overall security practices; older generations set the bar for better password habits, while younger generations were more likely to take preventative steps like using a password manager and multifactor authentication.

Younger generations expect **stronger inherent security** from their providers and are more likely to switch providers in the aftermath of a breach.

Location influences access, perception and familiarity with more advanced authentication techniques, with APAC being the most knowledgeable and comfortable with tactics like multifactor authentication and using biometrics as part of such schemes.

Contents

Security over convenience

The debate and trade-off between security and privacy versus convenience is an old one. Users naturally prefer smooth interaction with services, and providers have ample incentive to facilitate that experience. But things are not always as simple when risk levels rise, and technology or service providers are forced to add security measures to existing customer journeys in order to prevent abuse and fraud—not to mention protecting enterprise environments, where access controls are even more critical.

Where do users most appreciate the criticality of security, and where do they make trade-offs for convenience? It turns out that users place more value on certain types of data, and as a result will prioritize security and privacy in some cases, while prioritizing speed and convenience in others (see Figure 1).

Seventy-four percent of respondents who would be willing to use **more than one password** or way to authenticate would do so for added security.

For apps related to finances (banking, investing and budgeting), people vastly ranked security as top priority (70 percent on average) over privacy or convenience (16 percent and 14 percent respectively)—yet when it came to social media, convenience took a slight lead (36 percent convenience, 34 percent security, 30 percent privacy).

Unfortunately, even with growing awareness about the value of data shared by users on social media, people still seem to weigh convenience and security equally when it comes to accessing their social media accounts—a trend that reveals a general ambivalence about the dangers of lax personal security for social media accounts.

Contents

This is particularly alarming in light of the fact that nowadays, many consumers opt to use their Facebook, Twitter and Google accounts to authenticate and access other applications and services. Many popular services that house sensitive information, like delivery services, online shopping and dating apps, encourage users to log in using their social accounts. Therefore, if one of these social/email accounts is compromised, there could be a domino effect on how many additional accounts may also fall into the attacker's hands.

Results showing a penchant for speed and convenience shed light on a growing interest in biometrics that can provide an added layer of security without burdening the user. A fingerprint, which is the most popular biometric, is rather unique, dœs not require memorizing, can't be kept on a piece of paper or shared like a password or forgotten, and—most of all—it's both fast and convenient.

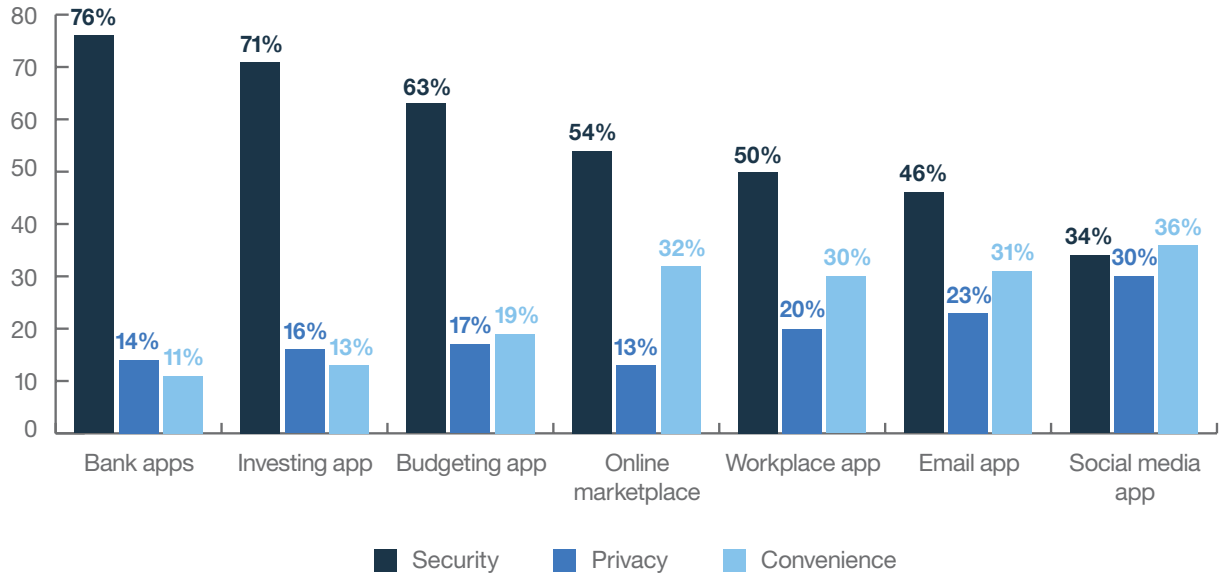


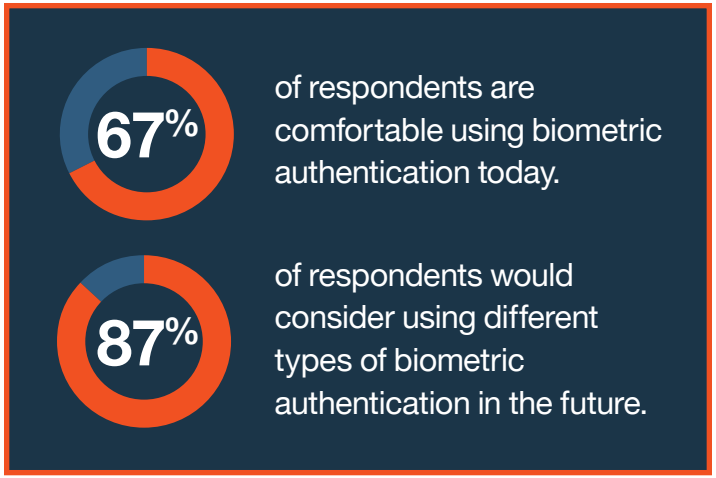
Figure 1. App or account types respondents cared most to protect (global perspective)

Contents

Biometrics are the future, but not without security concerns

Of the top most-secure elements, as perceived by respondents, fingerprint ranked first by 44 percent, retinal scan ranked second (30 percent), and alphanumeric passwords ranked third (27 percent) (see Figure 2). Digital PINs and facial recognition tied for 12 percent.

Interestingly, while fingerprint ranked first, full handprint only reached sixth position with 10 percent of respondents perceiving it to be a secure authentication. The audible methods, such as voice or heartbeat recognition, were last on the list.



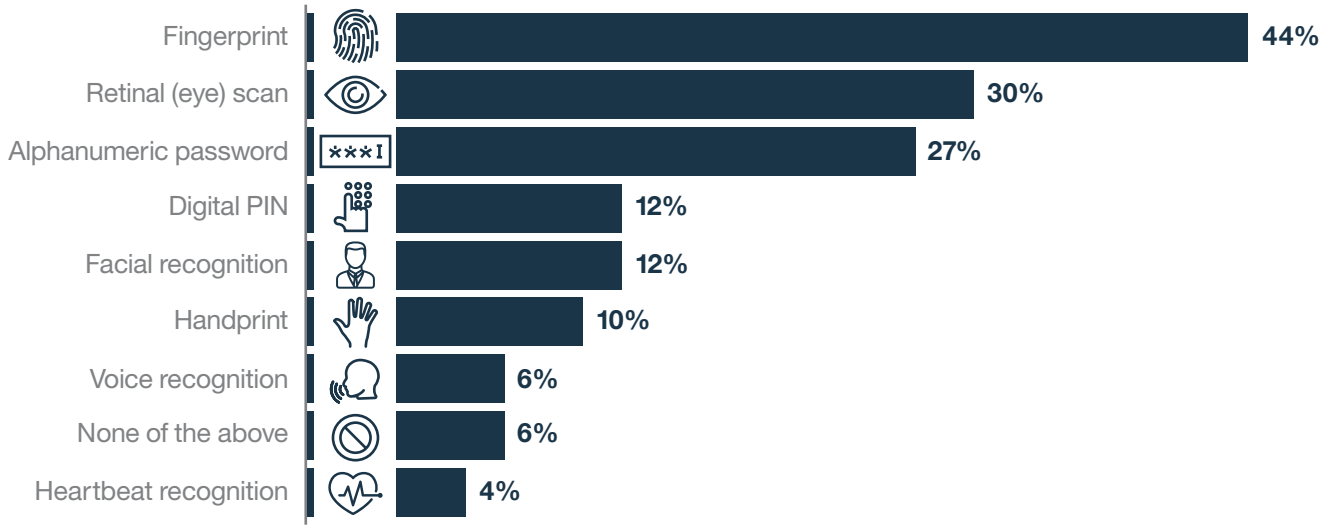


Figure 2. Authentication methods perceived as most secure (global perspective)

Contents

Biometrics are becoming more popular than ever, but privacy concerns over how they are stored and secured persist. Because biometric data can be used to identify an individual beyond doubt, consequences of compromise are grave.

Findings regarding people's biggest concerns with biometric authentication were not very surprising and matched with trending issues reported in the media (see Figure 3). Those concerns are security and privacy, more so than ease of use or functionality.

When it came to their concerns over the use of biometrics as an authentication method, users also worried about how biometrics might be stored and the potential for compromise. While trust levels about securing biometrics were relatively high in some regions, one quarter of survey respondents do not trust any organization to protect their biometric data (see Figure 4).

People's **biggest concerns** with biometric authentication are **privacy and security** (55 percent and 50 percent respectively).

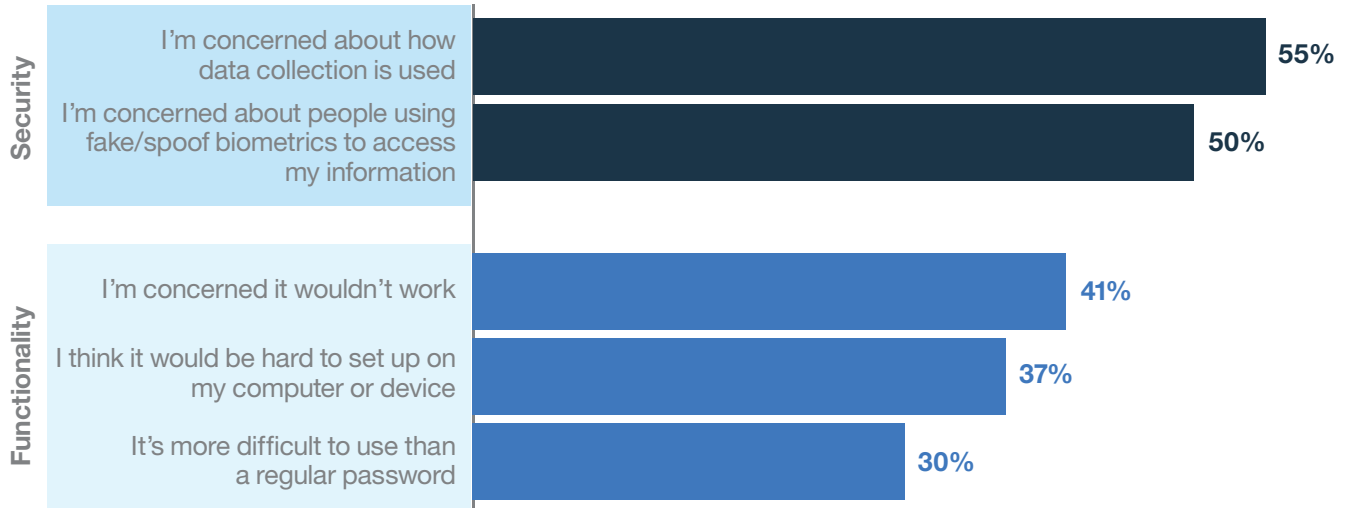


Figure 3. Biggest concerns linked with biometric authentication (global perspective)

Contents

Forty-four percent of respondents view **fingerprint biometrics as the most secure method** of authentication, while alphanumeric passwords and digital PINs were seen as less secure (27 percent and 12 percent respectively).

Trusting organizations to keep biometric data secure varied greatly by industry, with banking leading as the most trusted. Forty-eight percent of people would trust a major financial institution the most with their biometric data, while only 15 percent would trust that data to major social media sites.

On a ranking of different provider types who may use biometrics as part of the user authentication process, major providers were more trusted to secure biometric data than the smaller, regional or niche providers.

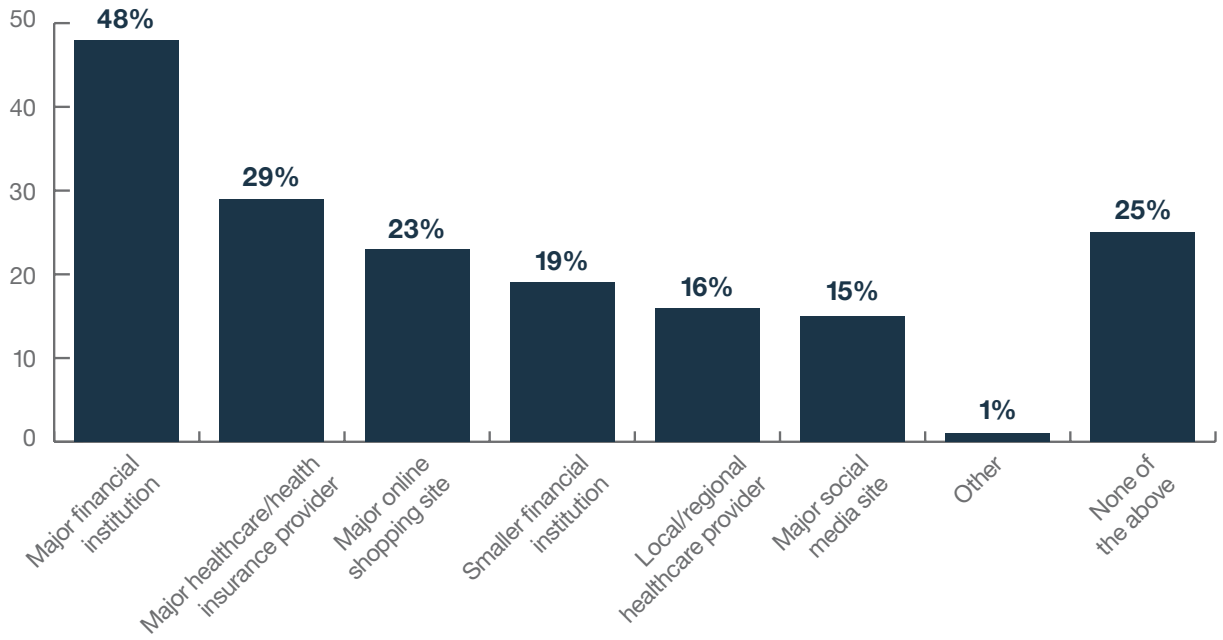


Figure 4. Types of organizations people trust MOST to protect their biometric data (global perspective)

Contents

The age gap around passwords

Password best practices are a very prominent subject in the information security world—but although most people are well aware that strong passwords are more secure, survey responses revealed a generational divide when it comes to acting on that knowledge (see Figure 5). The older generation takes password security more seriously, while younger people put the least amount of effort into password best practices. However, the data revealed that younger generations will take other actions to secure their accounts, such as setting up a password manager or multifactor authentication.

- Millennials (ages 20 – 36) put the least amount of effort into password safety: on average, **only 42 percent use complex passwords** (versus 49 percent of those 55+), and 41 percent reuse the same password multiple times (versus 31 percent of 55+).
- On average, **people aged over 55 use 12 passwords**, while millennials use 8 passwords, and Gen Z (ages 18 – 20) averages only 5 passwords, which could indicate a heavier re-use rate considering most people have more than 5 accounts.

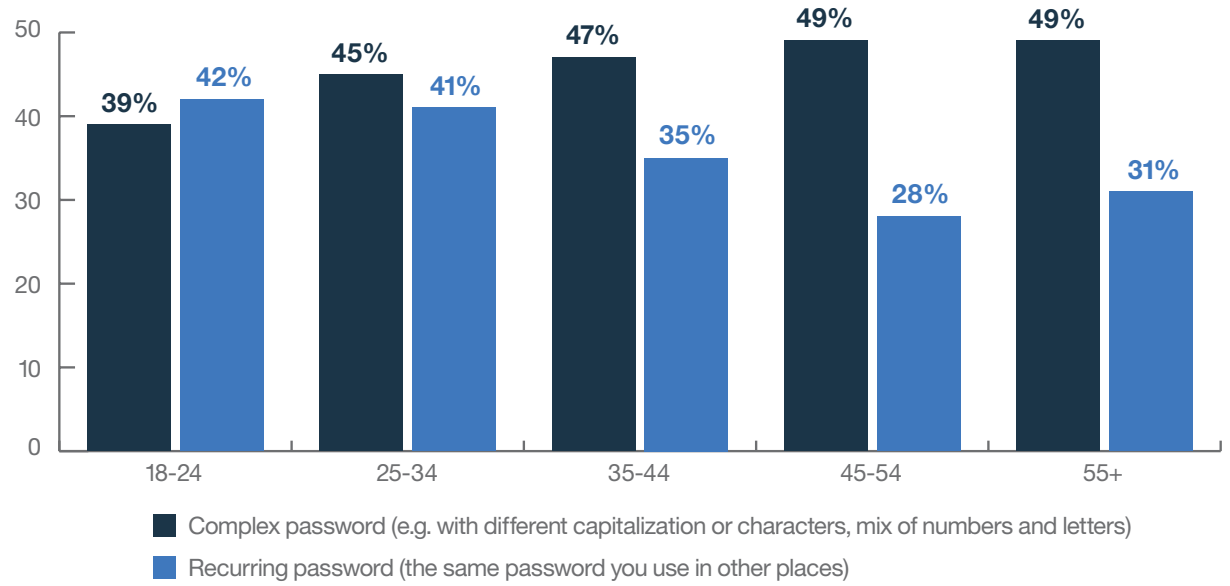


Figure 5. Password habits by age groups (global perspective)

Contents

Password reuse is known as a risky practice that can enable compromise across multiple accounts, even if just one password has been exposed.

> Seventy-five percent of millennials are **comfortable using biometrics** today, versus only 58 percent of those over age 55.

Generational differences also showed striking variances in terms of attitude toward security (see Figure 6). When given the choice between saving time and employing a more secure form of authentication, people under the age of 34 were most likely to prefer a speedy experience to a more secure way to authenticate, if it were shown to save them one to ten seconds. The older generation was not likely to ever make the same tradeoff.

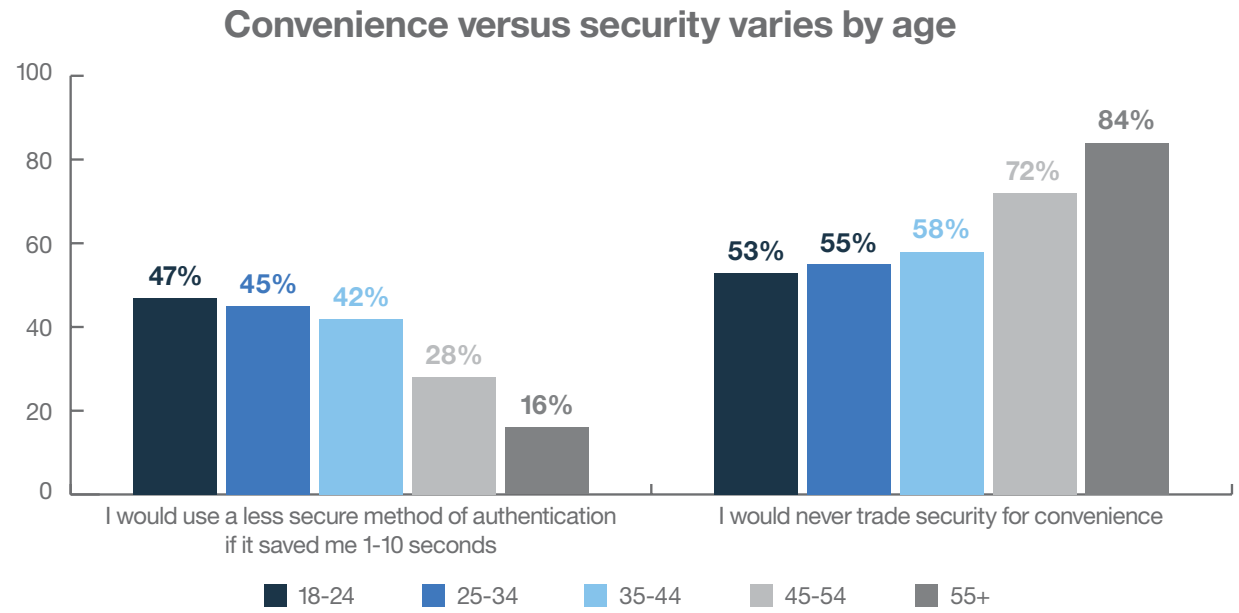


Figure 6. Trading off security for time or convenience (global perspective)

Contents

With those findings in mind, it is not surprising that younger generations would opt to use authentication that saved them time. The survey found that younger generations already have experience with, and have used, biometrics in the past, while older generations were much less likely to say the same.

> According to the survey, **36 percent** of those ages 18 – 20 say they use password managers to keep passwords and avoid having to memorize them, compared to only **26 percent** of users in the general population.

Younger generations take action in the wake of a breach

What influences users of different generations to make changes to their authentication habits? While younger generations were shown to be less concerned about password security in general, our results showed that they were more likely to make changes to their authentication habits in the wake of a data breach—taking mitigating actions like enabling two-factor authentication, or ceasing to use an app or service entirely if their data was compromised by that provider.

The survey found that millennials were more likely to take the following actions in wake of a breach:

- Enable two-factor authentication (32 percent versus 28 percent of the general population)
- Stop using an app or service that was affected (25 percent versus 21 percent of the general population), moving to a competitor's service

As younger generations are more likely to take action to secure their accounts after a breach has taken place, they may expect more inherent security from their providers, and therefore place less emphasis on personal password hygiene in the first place.

Additionally, the survey revealed that younger generations are more likely to use a password manager, a tool which assists in generating and retrieving complex passwords.

Contents

Around the world: Cultural perspectives vary

Technology and biometric adoption

Availability and culture influence the use of digital assets, technology and gadgets—and they affect the attitudes respondents have about securing devices and using different types of authentication.

The slower adoption of new technologies (see Figure 7) may be part of the reason why respondents in the US were the least familiar or comfortable with biometric authentication methods, especially since those have been embedded into popular personal devices in recent years. The survey found that US respondents lagged behind APAC and Europe in comfort and usage of biometrics—and in fact, 23 percent of respondents in the US said they are not interested in using biometrics now, or in the near future (see Figure 10).

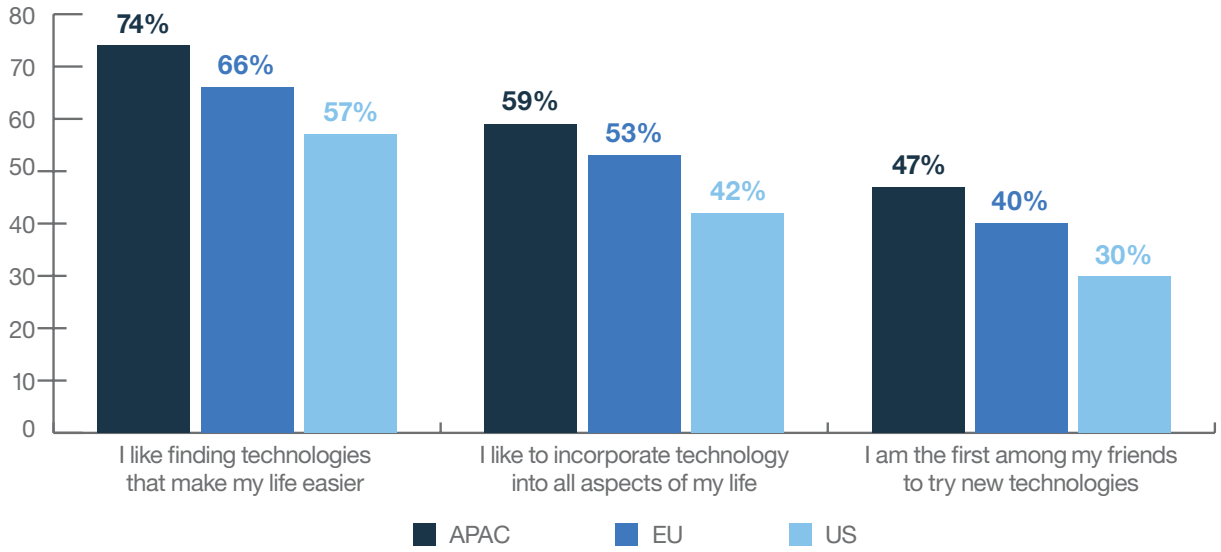


Figure 7. Comfort with current and new technology

But while they did not rush to adopt biometrics per se, US respondents were the most aware of security threats and indicate having heard about data breaches in the recent past (see Figure 8). In spite of awareness that major breaches take place, a large proportion of US users do not believe that breaches are inevitable, which would suggest they believe that security measures can be taken to prevent them.

Seventy-nine percent of US respondents **were aware of data breaches** in the past year (versus 70 percent in APAC and 69 percent in EU).

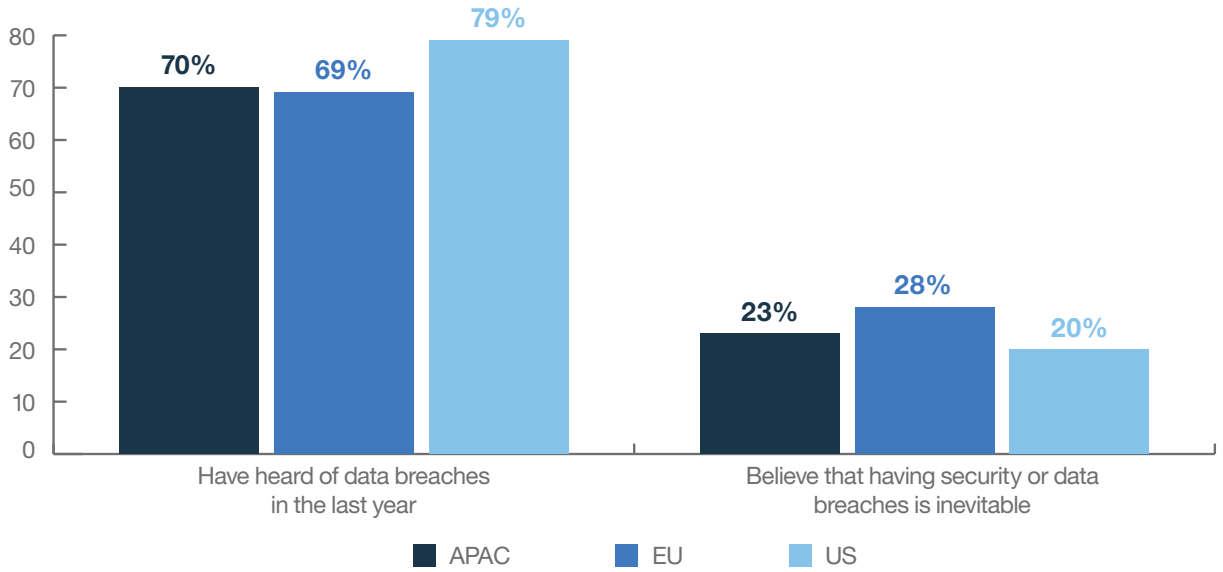


Figure 8. US ranked highest in awareness of technological threats

Contents

Knowing about the occurrence of major breaches but believing they can be avoided seems to translate into US respondents' willingness to use more security. In that sense, they would opt for multifactor authentication, but not as many would opt for biometric authentication as a means to add a layer of security (see Figure 9).

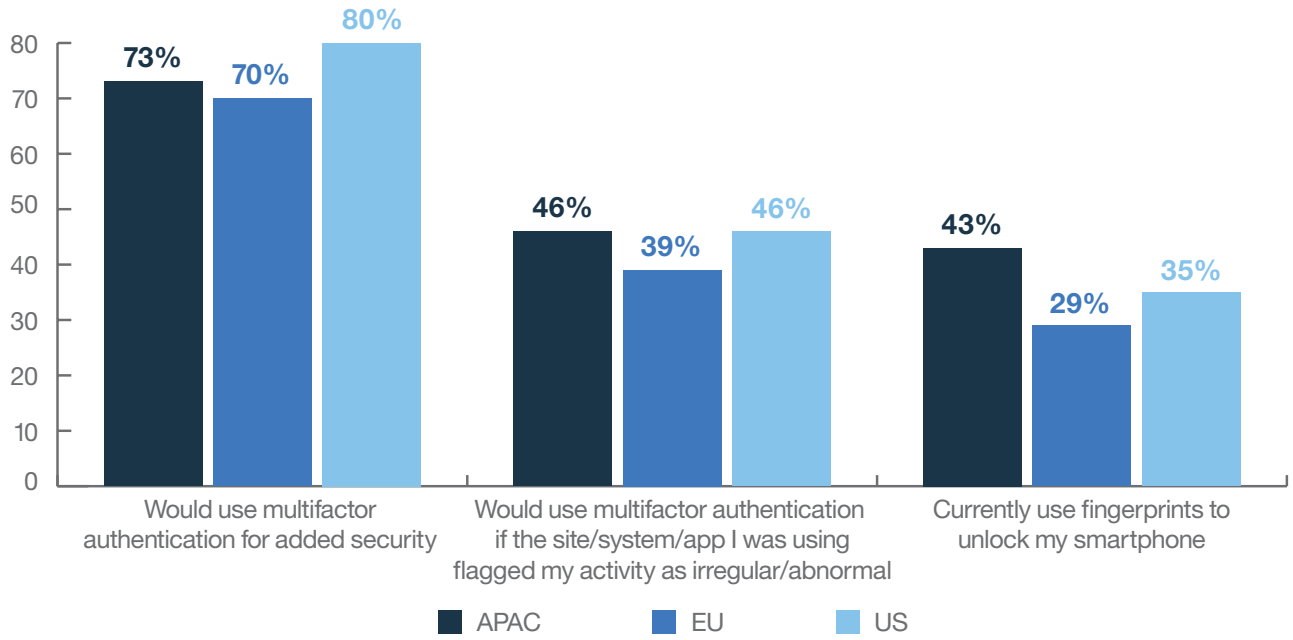


Figure 9. US respondents would use multifactor authentication but won't necessarily opt for biometrics

In APAC countries, respondents are disposed to adopt new technologies. The US lags in comparison with APAC and Europe when replying to questions about device ownership and likelihood of adopting new technology.

Contents

When it came to use of multifactor authentication in other regions, European respondents overall displayed a strong concern for security—and a willingness to use strong passwords—however they were the least likely to use multifactor authentication for added security, even in the wake of a data breach.

Cultural differences and authentication methods

As for the current use of biometric authentication, differences emerged between US, EU and APAC respondents, highlighting the effect of cultural influences on how users perceive and use different means to authenticate their online identities.

- **Europe had the strongest password practices,** with 52 percent of respondents using complex passwords (compared to 46 percent in APAC and 41 percent in the US).
- European respondents were the least likely to say they would use **multifactor authentication for improved security** (70 percent more likely, versus 73 percent in APAC and 80 percent in the US).

European respondents displayed concern for good password practices, but were less likely to enable multifactor authentication on their accounts.

Contents

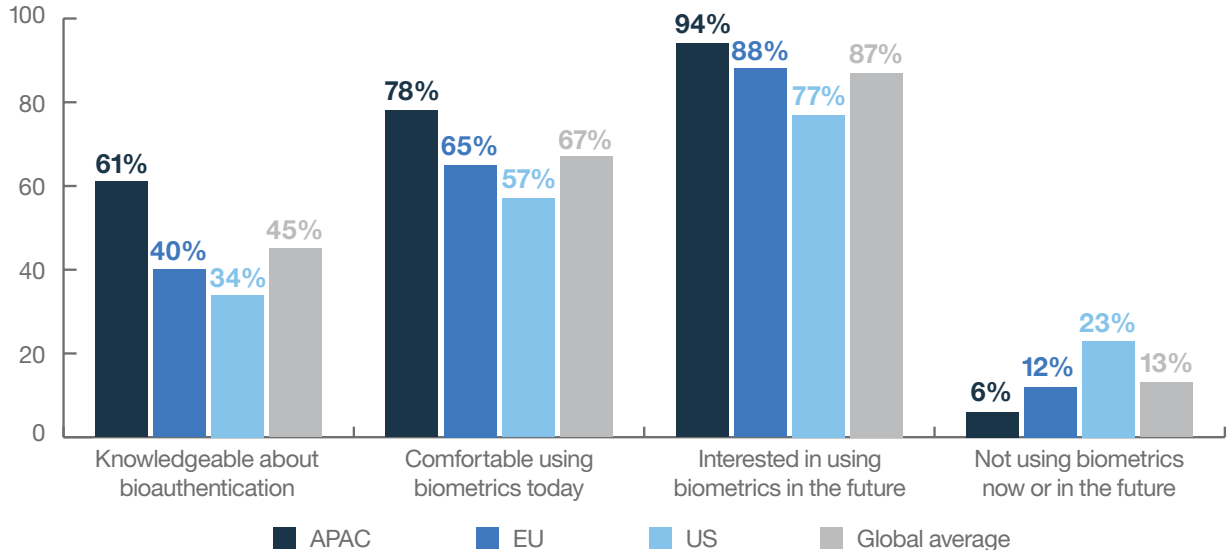


Figure 10. Knowledge and comfort with biometric authentication

When it comes to biometrics, APAC stood out as the region with the highest knowledge, comfort and current usage of biometrics (see Figure 10). This trend is unsurprising, given APAC respondents' stronger inclination to adopt new technologies (see Figure 7), as well as novel use cases for biometrics being piloted with consumers in APAC, such as Alibaba launching "smile to pay" in KFC restaurants in China.

The comfort level with biometric authentication methods is growing in Europe as well, but US respondents remain less knowledgeable and more skeptical, and seem to prefer waiting before turning to biometrics for authentication purposes.

The overall picture of biometrics use in the US shows that it lags furthest behind on biometric adoption—especially with about a quarter of respondents saying they are not interested in using biometrics now, or in the near future.

Easier and more secure

When it comes to seeing biometrics as being both easy to use and more secure, respondents in some regions were more convinced than others.
It was not surprising to see that APAC respondents, once again, are most inclined to perceive biometric authentication as the more convenient and secure option. Respondents in APAC generally felt that biometrics could make life easier by removing the need to remember additional passwords (see Figure 11).

> Over 70 percent of people in APAC said biometrics **increase security** and protection of identity.

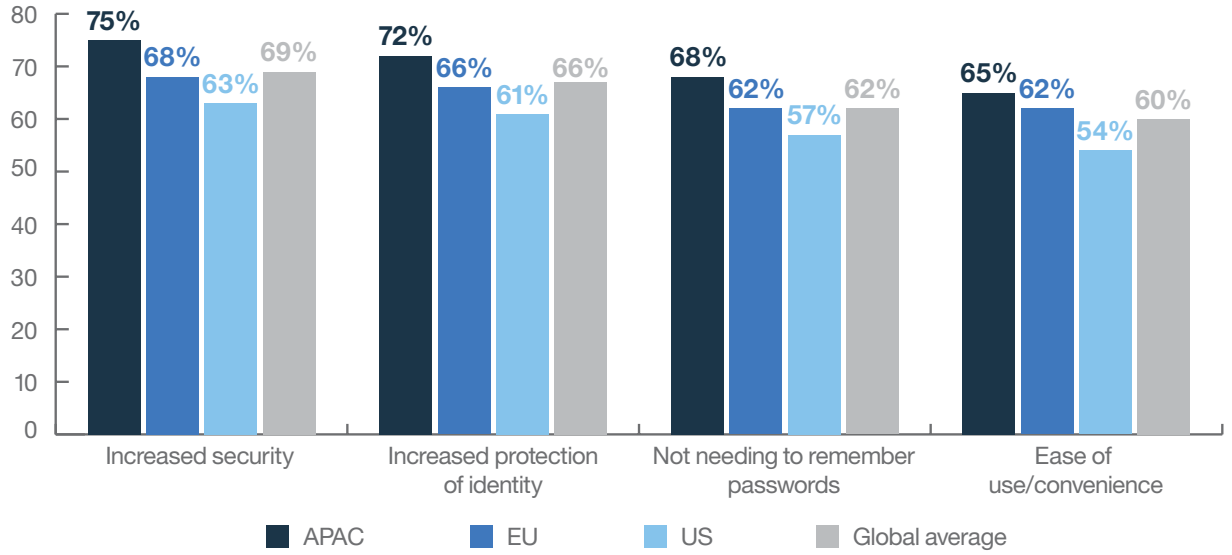


Figure 11. Perceived benefits of biometric authentication

Contents

EU respondents typically ranked the same parameters a few percentage points under the APAC respondents, and US respondents were the least likely to see the benefits of biometric authentication, ranking 11 – 12 percentage points under the APAC segment for each parameter.

No matter the preference, respondents in all geographies agreed that authentication methods need to change to protect against data breaches (see Figure 12). APAC respondents were most anxious to see improvement.

Concern levels also influenced by geography

As this survey reveals, the use of biometrics to authenticate identity is influenced by culture and technology adoption. Also, concerns over biometric authentication affect adoption rates—in particular concerns over how biometric data is collected, stored, shared and may be compromised, highlighting both security and privacy risks.

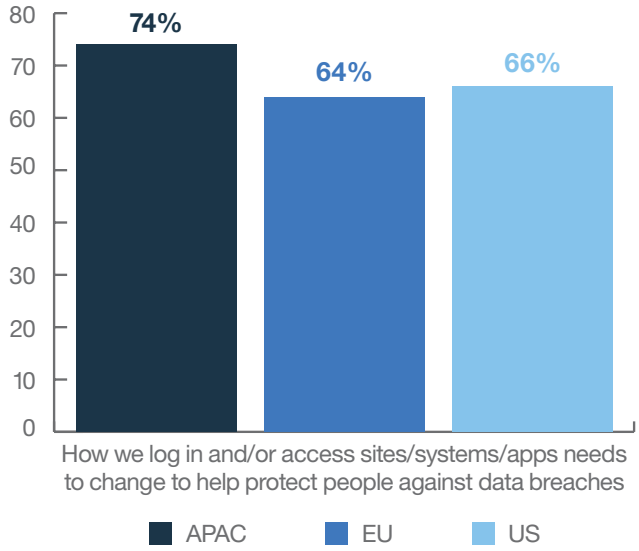


Figure 12. APAC users want to see authentication methods improve to enhance security

Over **65 percent** of people in APAC believe biometrics are easier to use than passwords.

US respondents were least likely to see the benefits of biometric authentication.

Contents

When it came to concerns about using biometrics, respondents worried more about the **risk of compromise** than the technical challenges of getting set up (50 percent versus 37 percent).

When it comes to the influence of location on concerns over some aspects of using biometric authentication, those most knowledgeable about it were also the most concerned about the possibility of biometric data being misused (see Figure 13). APAC respondents ranked highest among the other regions in concern over use of fake or spoofed biometric data to access their information.

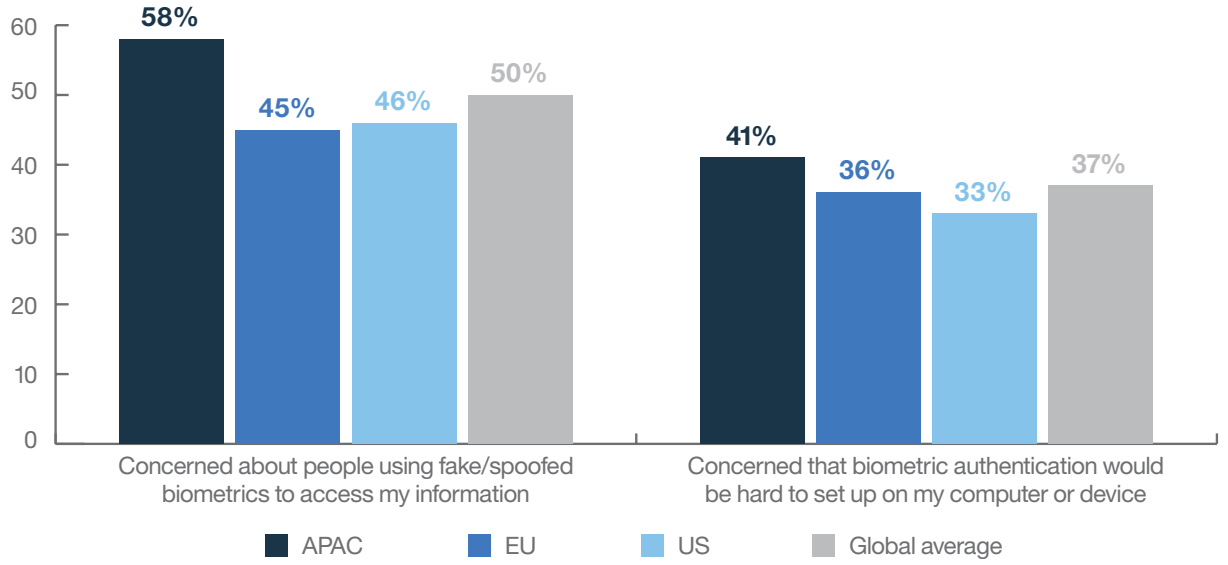


Figure 13. Concerns about biometrics – Geographical comparison versus global average

Contents

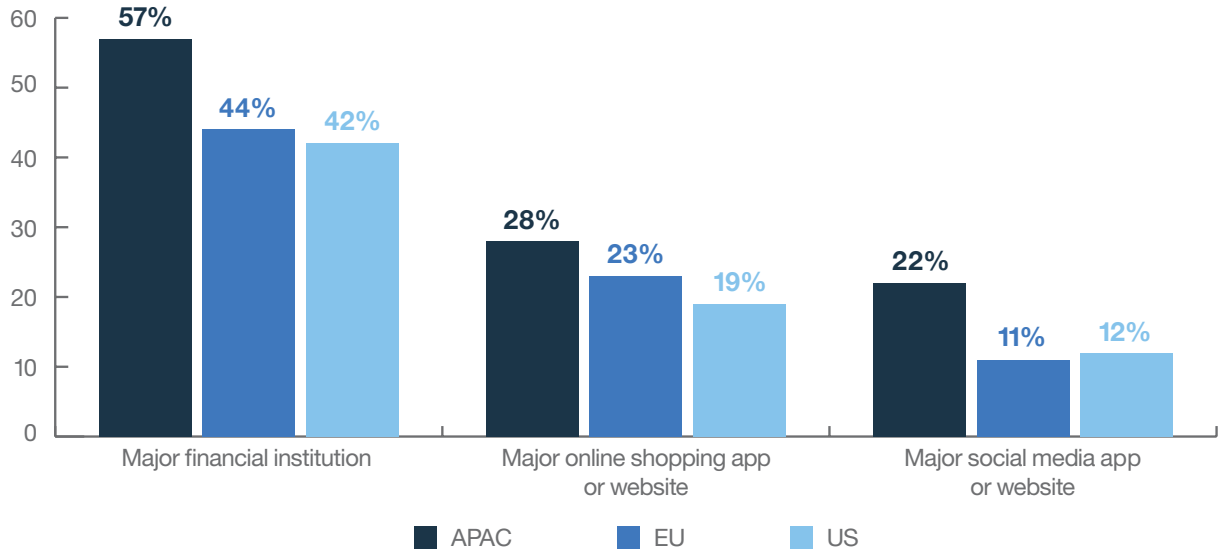


Figure 14. APAC users are most likely to trust their biometric data to major financial institutions

Although they did express concern, APAC respondents still trust their providers to protect biometric data (see Figure 14). US and EU respondents were much less likely to trust their biometric data to their service providers:

- **Fifty-seven percent** of APAC respondents still **trust their financial institution** to protect their biometric data (versus 42 percent in the US and 44 percent in EU).
- **Twenty-eight percent** of APAC respondents **trust major online shopping providers** to do the same (versus 19 percent in the US and 23 percent in EU), and 22 percent believe social media sites can protect their biometric data (versus 12 percent in the US and 11 percent in EU).

Contents

Takeaways: The future of authentication

In view of the ever-escalating risk to our digital identities and constant enhancements in the tools available to authenticate our identities online, developing more secure and strategic approaches to authentication is a major priority across the current business, services and security landscapes.

To minimize illegitimate access while still offering a full range of services to legitimate customers, identity and access management providers have long been looking for new ways to enhance the security and user experience of identity authentication. But managing risk is only one of aspect of the ongoing race to improve authentication—user preferences, habits and attitudes will weigh heavily on the actual adoption and use of new authentication platforms.

Consumers are security-aware

Key takeaways from this IBM Security survey show that respondents are already quite familiar with the different authentication schemes in use today. They are security-aware and understand the types of data they consider most worth protection, even in the cases where they prefer convenience.

Within the overall concept of turning to newer authentication models and biometrics, respondents did prefer particular types of identifiers and had less trust that others were as secure. Most people leaned toward using a fingerprint—a comfort and familiarity level that stems from its prominence in the marketplace and its integration into both Android and iPhone smartphones in recent years.

User preferences, habits and attitudes will largely determine which authentication platforms will succeed in the marketplace.

Contents

Biometrics on the horizon

What will the future of authentication look like in the next few years? It is not hard to see that users are getting more familiar with and warming up to the idea of trying biometrics in the near future.

Information technology decision makers have perhaps the highest level of investment in society's adoption of safer authentication, as their organizations stand to lose most from the poor password practices of their employees and customers. By mandating that employees adopt authentication mechanisms like hardware tokens, one-time passwords or biometrics when signing into workplace services, businesses can reach a higher level of confidence that they're working to keep hackers out—although they often risking frustrating their users in the process.

For organizations that offer digital services to consumers, forcing a user's hand (or fingerprint) when it comes to signing in can result in lost revenue. That's most likely why these security options are being presented to consumers as an added convenience, or under the badge of progress and innovation from their service provider.

Enhancing security while, at the same time, making identity authentication a positive user experience is the challenge facing organizations today. Learn how to balance security and convenience with "silent IAM."

Contents

Offering choice is key to adoption

Results of the survey show that people will adopt the authentication methods that best fit their personal preferences, which are influenced by factors like age and culture. Organizations and service providers can use this knowledge to manage authentication risks as their users get more comfortable with multifactor and even biometric authentication. Providing users with a choice between **multiple different authentication options** when they log on to services or workplace applications is likely to result in better adoption of multifactor authentication across the board, and potentially even better security if different users choose methods that hackers would have a hard time guessing or obtaining in mass quantities.

Investing in access management technology that allows administrators to give their users flexibility can also help organizations remain more secure while giving employees a feeling of empowerment and control over how they choose to authenticate.

Consider a risk-based approach

Another way to enhance security is through the adoption of **risk-based approaches** to authentication. Our research shows that younger generations are less likely to adopt strong passwords and more likely to reuse passwords across multiple sites and services. While these behaviors are proven to expose users to hacking and phishing attempts, organizations can still protect against fraudulent access attempts—even when credentials are stolen—by adopting risk-based authentication.

Adopting a risk-based approach to authentication can help organizations overcome the poor password practices of younger generations. Learn how.

Contents

With **risk-based authentication**, authentication attempts are automatically evaluated based on contextual data and behavioral cues determined by administrators. When risk scores are elevated, the system can prompt the user to prove that they are who they say they are via an additional factor, which could be a biometric or another mechanism of choice.

Offering choice is key to adoption

As users continue to **adapt their authentication habits** to the latest advancements in technology, service providers and IT decision makers will play a critical role in influencing the adoption curve—whether in the workplace or through consumer-facing technologies. Will they mandate stronger authentication methods, provide users with options, or leave users to make their own decisions and treat identity-related threats as acceptable risks? Being offered different access control choices can certainly encourage more users to adhere to better security.

But while IT can influence the movement to a more secure world, the future of authentication ultimately comes down to whether or not individual users choose to employ secure practices.

Future research on global adoption patterns of authentication technology—especially in academic, observed settings—is essential to measuring progress and building secure technology that's pragmatic and user centric.

Service providers and IT decision makers will certainly influence the adoption of new authentication methods—but acceptance in the end will come down to individual users.

Contents

About IBM Security

IBM® Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security intelligence to help organizations holistically protect their infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates one of the world's broadest security research, development and delivery organizations, monitors billions of security events per day in more than 130 countries, and holds more than 3,500 security patents.

For more information

To learn more about the IBM Security portfolio, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security

For more information on IBM Security solutions for identity and access management, visit:
ibm.com/security/identity-access-management

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog

About the author

Limor Kessem, Executive Security Advisor, is one of the top cyber intelligence experts at IBM Security. She is a seasoned security advocate, public speaker and a regular blogger on the cutting-edge IBM Security Intelligence blog.

Limor is considered an authority on emerging cybercrime threats. She participated as a highly-appreciated speaker on live InfraGard New York webcasts (an FBI collaboration), conducts live webinars on all things fraud and cybercrime, and writes a large variety of threat intelligence publications. With her unique position at the intersection of multiple research teams at IBM, and her fingers on the pulse of current day threats, Limor covers the full spectrum of trends affecting consumers, corporations and the industry as a whole.

Contributors

Cassy Lalan, External Relations, IBM Security

Lane Billings, Product Marketing Manager, Access and Authentication, IBM Security

Brian Mulligan, Product Manager, Access and Authentication, IBM Security

Contents

IBM Security

© Copyright IBM Corporation 2018

IBM Security
75 Binney Street
Cambridge MA 02142

Produced in the United States of America
January 2018

IBM, the IBM logo, ibm.com and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at **ibm.com**/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

IBM

22012422-USEN-01