IBM Future of Identity Study: Millennials Poised to Disrupt Authentication Landscape

Young adults lax on passwords, more comfortable with biometric and multifactor authentication
People now prioritize security over convenience when logging into apps

CAMBRIDGE, Mass., Jan. 29, 2018 /PRNewswire/ -- IBM Security (NYSE:IBM) today released a global[1] study examining consumer perspectives around digital identity and authentication, which found that people now prioritize security over convenience when logging into applications and devices. Generational differences also emerged showing that younger adults are putting less care into traditional password hygiene, yet are more likely to use biometrics, multifactor authentication and password managers to improve their personal security.

With millennials quickly becoming the largest generation in today's workforce,[2] these trends may impact how employers and technology companies provide access to devices and applications in the near future. Overall, respondents recognized the benefits of biometric technologies like fingerprint readers, facial scans and voice recognition, as threats to their digital identity continue to mount.

The IBM Security: Future of Identity Study surveyed nearly 4,000 adults from across the U.S.,Asia Pacific (APAC) and Europe to gain insight into consumer viewpoints around authentication. Some key findings from consumers include:

- **Security outweighs convenience:** People ranked security as the highest priority for logging in to the majority of applications, particularly when it came to money-related apps.[3]
- **Biometrics becoming mainstream:** 67 percent are comfortable using biometric authentication today, while 87 percent say they'll be comfortable with these technologies in the future.
- **Millennials moving beyond passwords:** While 75 percent of millennials[4] are comfortable using biometrics today, less than half are using complex passwords, and 41 percent reuse passwords. Older generations showed more care with password creation, but were less inclined to adopt biometrics and multifactor authentication.
- **APAC leading charge on biometrics:** Respondents in APAC were the most knowledgeable and comfortable with biometric authentication, while the U.S. lagged furthest behind in these categories.

The evolving threat and technology landscape has created widely-known challenges with traditional log-in methods that rely heavily on passwords and personal information to authenticate our identities online. In 2017, data breaches exposed personal information, passwords, and even social security numbers for millions of consumers. Additionally, the average internet user in America is managing over 150 online accounts that require a password, which is expected to rise to over 300 accounts in

coming years. [5]

"In the wake of countless data breaches of highly sensitive personal data, there's no longer any doubt that the very information we've used to prove our identities online in the past is now a shared secret in the hands of hackers," said Limor Kessem, Executive Security Advisor, IBM Security. "As consumers are acknowledging the inadequacy of passwords and placing increased priority on security, the time is ripe to adopt more advanced methods that prove identity on multiple levels and can be adapted based on behavior and risk."

Security Takes Priority; Biometrics Seen as More Secure than Passwords

Survey results around security, convenience and privacy contradict the long-held wisdom that "convenience is king." While consumers have long been thought to prefer a fast sign-in experience with minimal friction, the survey results show that people rank security as a higher preference than privacy or convenience for the majority of applications – particularly for money-related applications.

- Security was vastly ranked as the top priority for banking, investing, and budgeting apps – for these categories on average, 70 percent selected security as the top priority, with 16 percent selecting privacy, and 14 percent selecting convenience.
- Security also ranked as the top priority for online marketplaces, workplace apps, and email.
- For social media apps, priorities became less clear – with convenience taking a slight lead (36 percent), followed by security (34 percent) and privacy (30 percent).

The survey also examined consumers' opinions around the security of various login methods, and found that certain types of biometrics were viewed as more secure than passwords, yet security and privacy remain top concerns when it comes to adopting biometrics.

- 44 percent ranked fingerprint biometrics as one of the most secure methods of authentication; passwords and PINs were seen as less secure (27 percent and 12 percent respectively)
- People's biggest concerns with biometric authentication were privacy (how the data is collected and used – 55 percent), and security (others using fake biometric data to access their accounts – 50 percent).[6]

Age Gap: Older Generations Lead on Password Hygiene, Millennials Using Newer Techniques

The survey revealed several differences in generational viewpoints when it comes to securing their online identities. Older adults displayed better habits when it came to password creation, yet younger generations were more inclined to adopt password managers, biometrics and multifactor authentication as a way to secure their online accounts. This could be an indication that younger generations have less confidence in passwords and are instead looking to alternative methods to secure their accounts.

- Only 42 percent of millennials use complex passwords that combine special characters, numbers and letters (versus 49 percent of those 55 years of age and older), and 41 percent reuse the same password multiple times (versus 31 percent of 55+).
- On average, people 55+ use 12 passwords, while Gen Z (ages 18 – 20) averages only five passwords, which could indicate a heavier re-use rate.
- Millennials are 2x more likely to use a password manager (34 percent) than people over the age of 55 (17 percent).
- Millennials were more likely to enable two-factor authentication in the wake of a breach (32 percent versus 28 percent general population).

Young adults also showed the strongest preference for convenience, with almost half (47 percent) of adults under 24 preferring a faster sign-in experience to a more secure form of authentication. This may be one reason that young people are more likely to adopt biometric authentication, with 75 percent of millennials comfortable using biometrics today compared to 58 percent of those over age 55.

Around the World: Location Impacts Password and Authentication Perspectives

The survey found that geographic location had a strong influence on perception and familiarity with emergent authentication techniques, with the Asia Pacific region being the most knowledgeable and comfortable with tactics like multifactor authentication and biometrics. The U.S. lagged furthest behind in awareness and comfort for most categories. Specifically:

- APAC respondents were the most likely to say they were knowledgeable with biometrics (61 percent said they were knowledgeable vs. 40 percent EU, 34 percent U.S.).
- APAC was also the most comfortable using biometrics today (78 percent comfortable vs. 65 percent EU, 57 percent U.S.).
- Europe had the strongest password practices, with 52 percent of respondents using complex passwords (vs. 46 percent in APAC and 41 percent in the U.S.).
- 23 percent of respondents in the U.S. said they are not interested in using biometrics now or in the near future - nearly double the global average.

Future of Identity

Analysis in the report by IBM Security details that attitudes regarding authentication vary widely, and while acceptance of newer forms of authentication like biometrics is growing, concerns persist – particularly amongst older generations and people in the U.S.

IBM advises organizations to adapt to these preferences by taking advantage of identity platforms that provide users with choices between multiple authentication options – for example, letting users toggle between a mobile push-notification, which invokes fingerprint readers on their phone, or a one-time passcode. Organizations can also balance demands for security and convenience by using risk-based approaches that trigger additional authentication checkpoints in certain scenarios, such as when behavioral cues or connection attributions (device, location, IP address) signal abnormal activity.

The data also reveals that younger generations are placing less emphasis on traditional password hygiene, which poses a challenge for employers and businesses that manage millennial users' access to data via passwords. As the percentage of millennial and Gen Z employees continues to grow in the workforce, organizations and businesses can adapt to younger generations' proclivity for new technology by allowing for increased use of mobile devices as the primary authentication factor and integrating approaches that substitute biometric methods or tokens in place of passwords.

IBM Security provides tips for consumers on how to secure their digital identities in a blog post here.

For additional details on the study and advice for companies to prepare for the future of authentication, download the full report at: ibm.biz/FutureOfIdentity

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, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and has been granted more than 8,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @ibmsecurity on Twitter or visit the IBM Security Intelligence blog.

About the Study

The study was designed with Ketchum Global Research and Analytics. Data collection was conducted by Research Now. The survey was conducted between October 21 and November 5, 2017, with a margin of error of +/- 2.0 for the U.S. sample and +/- 3.07 for the EU and APAC samples, at the 95% confidence level.

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

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

Media Contact:
Cassy Lalan
Media Relations, IBM Security
cllalan@us.ibm.com
319-230-2232

[1] Markets surveyed include Europe, Asia Pacific and United States.

[2] ManPower Group, 2016

[3] IBM Security: Future of Identity Study: 70 percent of respondents ranked security as the top priority over convenience or privacy when logging into financial apps (investing, budgeting, banking apps).

[4] "Millennials" refers to respondents ages 20-36 at time of survey (2017)

[5] Dashlane, 2017

[6] 55% of respondents were concerned with "how data collected is used" ; 50% were concerned about "people using fake/spoof biometrics to access my information"

SOURCE IBM

Additional assets available online: Photos (2)