THE PASSWORDLESS FUTURE REPORT

A Report by Okta
June 2019

Welcome to The Passwordless Future Report

Every company has to become a technology company in order to survive and thrive in today's competitive environment.

But while organizations are innovating and transforming, finding ways to better engage with customers, and protecting their people and data from a variety of threats, trust in technology is eroding due to new challenges. Organizations are under pressure to innovate quickly and issues with security, privacy and consent plague user confidence in much of the technology we rely on.

Traditionally, securing our online identity has relied on one key method: passwords. For decades passwords have been the gateway to our digital identities and what we do online, and for far too long we've been witnessing the failure of passwords. Okta has undertaken research that demonstrates how passwords are impacting our security and quality of our daily lives.

But, imagine a world where our security isn't dependent on letters or numbers which can easily be manipulated. Where access to the things we need to live and work is so inherently unique, no one else could have the same two sets of credentials because they are linked to our personal identity.

2019 will be a turning point in security. Security will begin to be based on our individual identities and completely passwordless, and identity will play an essential role in enabling organizations to build with trust.

How Did Okta Produce the Survey?

Commissioned by Okta, Opinium conducted a survey of 4,013 workers across the UK, France and the Netherlands. Responses were collected in May 2019. We refer to this survey as “Okta’s research” and refer to the people who responded as “respondents.’’

COUNTRY

2007 1003 1003

GENDER

50% female

49% male

1% other

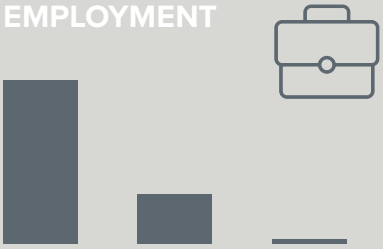
AGE

21% 18-34

52% 35-54

27% 55+

EMPLOYMENT



82% full-time

16% part-time

2% part-time (less than 8 hours)

TYPE OF WORKING

87% work in an office

13% work remotely

COMPANY SIZE

13% micro & small

*6% don’t know

30% medium

52% large

1 PASSWORDLESS SECURITY IS A REALITY

Trust and Identity

Trust is the new frontier, and organizations now more than ever need to prove they are trustworthy to their customers and their employees in order to be successful. The significance of trust has increased in the last decade as a result of increased data breaches, cyber-attacks and privacy issues due to pervasive tracking of our digital identities and monetization of our preferences.

Identity is at the center of trust. People are now paying more attention to their identity and thus businesses must pay more attention to how they treat identities.

For decades our identity and security have been intertwined, and we've used passwords to protect them. But the reality is that passwords have proven to be an ineffective method for enterprises.

Dr Maria Bada, Research Associate, Cambridge University, says passwords have been one of the biggest practical problems facing security engineers for decades.

"Users do not only have to remember passwords, but also the system and user ID with which it is associated. They have to remember if and when they changed a password and of course the actual password[1]. Users cannot remember infrequently-used, frequently-changed passwords.

According to research from Schacter, recalling more than two or three strong passwords is beyond the ability of human memory, and even those would be difficult to recall if used infrequently.[2]

[1] Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link' -- a Human/Computer Interaction Approach to Usable and Effective Security.
[2] Schacter, D. L., Addis, D. R., Hassabis, D., Martin, V. C., Spreng, R. N., and Szpunar, K. K. (2012). The future of memory: remembering, imagining, and the brain.

The Challenge for Business

Passwords cause multiple issues for businesses. According to Verizon's Data Breach Investigations Report in 2018, 81% of hacking-related breaches were as a result of weak, stolen or reused passwords[3]. And the consequences of a breach can be catastrophic. The average cost of a stolen record is $148[4], and the total cost incurred from a data breach averages $3.86m. Once breached, organizations could be struck again with a 32% likelihood of a recurring material data breach over the subsequent two-year period. Not to mention, the reputational damage is often irreparable.

While a cyber incident is the main cause of concern for enterprises when it comes to password use, there are other issues that we've found in Okta's research which have a day-to-day impact on business processes.

Okta's research into password security found that when people forget their password:

37%
are **locked out**
of their account

37%
cannot access
something they need

19%
delay work

Passwords are a hindrance to productivity. And with a sustained decrease in productivity, a business can fail to keep up with its competitors, and let down its customers who are expecting excellent customer services.

[3] Verizon Enterprise. (2018). 2018 Data Breach Investigations Report.
[4] Ibm.com. (2019). Cost of a Data Breach Study.

The Challenge for Workers

Okta's research found that on average, respondents have to remember 10 passwords in everyday life, and forget an average of three passwords in a typical month. It's well-known that the biggest security risk for employers are its employees – nearly half (49%) of organizations in all sectors face serious security incidents due to employee errors[5].

Worryingly, this doesn't seem likely to change any time soon. According to Okta's research, passwords containing sensitive information are changed infrequently, with work passwords changed only three times a year, and others such as bank accounts, phone PINs, personal emails and social media accounts changed just once a year on average.

10

PASSWORDS

(on average) have to be remembered in **everyday life**

 **11**

 **12**

 **9**

3

PASSWORDS

(on average) are **forgotten** in a typical **month**

 **3**

 **2**

 **3**

18

PERCENT

Have felt **stressed/worried** due to the **number of passwords** they have to remember

 **21%**

 **12%**

 **19%**

[5] Kaspersky Industrial CyberSecurity. (2018). The State of Industrial Cybersecurity 2018 | Kaspersky Industrial CyberSecurity.

So why are organizations still relying on a method which has been so far inadequate?

The reliance on passwords has led to organizations and software providers taking a tougher stance on the type of passwords allowed. Everyone has been confronted with a password screen which shows the strength of their chosen password, and the requirement for a mixture of numbers, uppercase and lowercase letters, and special characters. But this alone isn't enough to help security – and in many cases even these measures haven't been put in place.

DR MARIA BADA
Research Associate, Cambridge University

> Even in organizations that explicitly instruct users on how to select strong passwords, many do not comply, and use weak passwords.
>
> User perceptions of security can influence compliance with password mechanisms. Insecure work practices and low security motivation among users can be caused by security mechanisms and policy which take no account of users' work practices, organizational strategies and usability.[6]
>
> Studies have also looked at the connection of culture, language and personality dimensions to their password behaviour. However, no connection has been identified apart from one personality trait (agreeableness).[7]
>
> Passwords are often quite revealing. They are created on the spot, so users might choose something that is readily to mind or something with emotional significance. In this sense, passwords tap into things that are just below the surface of consciousness. Criminals take advantage of this and with a little research they can easily guess a password.

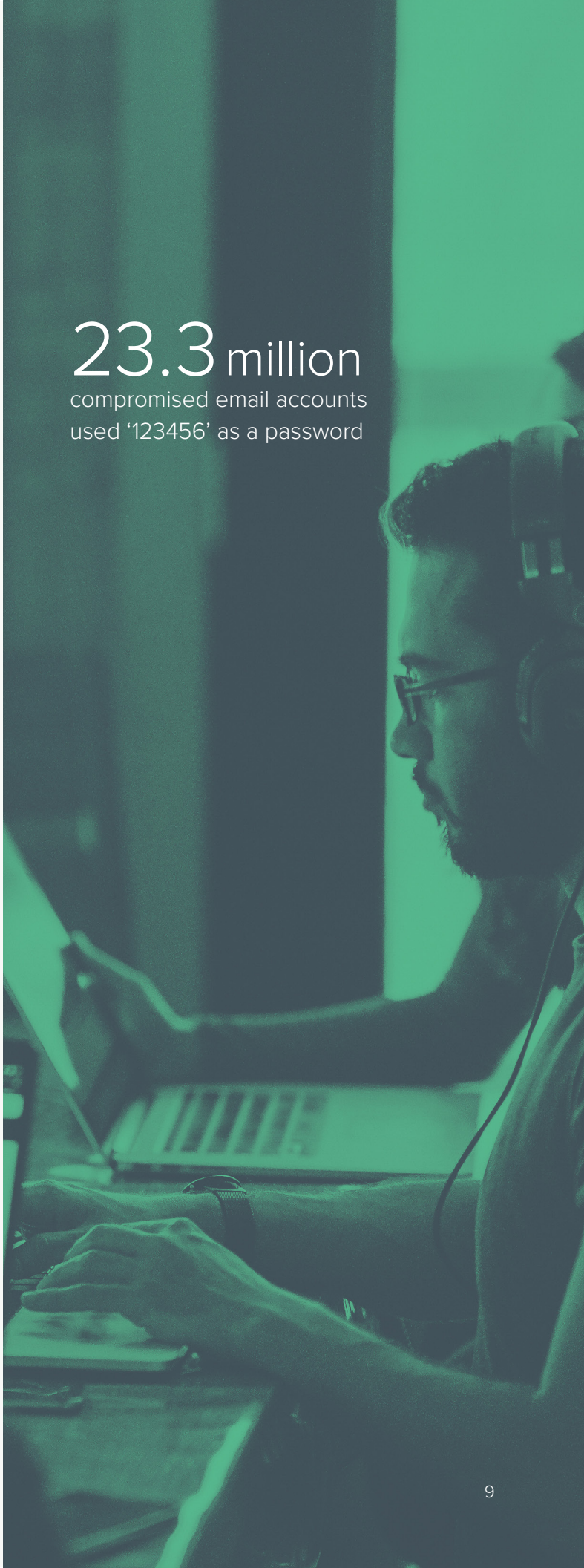
[6] Adams, A., & Sasse, M. A. (1999). Users are not the enemy.
[7] Kawu, A. A, Muhammad, I, Awal A, and Abdullah, M. B (2018). Effect of mental state on password selection among mobile phone users.

Passwords: The Ideal Targets for Cyber Crime

According to the UK's National Cyber Security Centre, 23.3 million compromised email accounts used '123456' as a password[8], while millions of other users were using the term 'password', their favorite soccer team or band as their passwords.

Regardless of a company's best efforts to raise awareness around strong passwords, users will still resort to using a password that they find easy to remember, most likely because of the large number of passwords they need to remember.

For many years, passwords have been seen as an adequate security measure, and the cost compared to alternatives was low. There have been many cases of a false dawn; where those in the technology industry claimed that passwords would be no more. The difference now is that there is both a growing security need to change the status quo, and perhaps more importantly, technology and solutions that can finally mean a dawn of a new passwordless era.



[8] Ncsc.gov.uk. (2019). Most hacked passwords revealed as UK cyber survey exposes gaps in online security.

2

THE HIDDEN PROBLEM WITH PASSWORD SECURITY

Passwords and Mental Health in the Workplace

Over the past several years, we've witnessed society invest in understanding and addressing mental health, but we're just starting to discuss mental health at work. Recent research[9] suggests that as many as 1 in 6 young people will experience an anxiety condition at some point in their lives, and last year, an American Psychiatric Association (APA) poll, found that almost 40% of Americans were more anxious than they were in 2017. Anxiety is on the rise in the workplace due to a number of factors, but security is one that has flown under the radar.

DR MARIA BADA
Research Associate, Cambridge University

> The potential impact from forgetting a password can cause extreme levels of stress, and over time that can lead to breakdown or burnout.
>
> That is due to our brains being sensitive to perceived threats. Being constantly focused on potential threats online, causes us to become hypersensitive to stress. In the long term that can cause mental health problems.

[9] Anxiety UK. (2019). Young People and Anxiety - Anxiety UK.

Okta's research shows that passwords have a direct link to stress with respondents reacting negatively when having to remember so many different passwords:

18%

of respondents stated that they felt **stressed/worried**

47%

(almost half) felt **annoyed** or **hassled**

In large companies this rises to **52%**, while for micro businesses this goes down to **36%**

63%

(two-thirds) said **negative emotions** were evoked

This was highest in France (**73%**) compared with the UK (**67%**) and the Netherlands (**52%**)

Forgetting a password brings to light those negative emotions to even more people with 62% feeling stressed or annoyed as a result of forgetting their password. This was highest in the UK (69%) compared with France (65%) and the Netherlands (53%).

DR MARIA BADA
Research Associate, Cambridge University

"Password fatigue, the stress that users experience due to requirements to create, re-enter, remember and change a large number of passwords can lead to extreme stress.

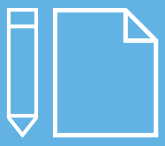
A number of different organizational policies can lead to that sense of password fatigue. Asking a user to change their password while working or disrupting their work flow can lead to rushed, weak and thus forgotten passwords. Similar emotions can be caused due to a session expiry while the user needs to login again.

The Mental Pressure of Passwords

People worry about forgetting passwords, but forgetting a password itself is not a security risk. The majority of hacking-based breaches are a result of reused, stolen or weak passwords, it's riskier for individuals to use insecure passwords and memory aids than to forget and reset:

34%

of users use the **same passwords** for **multiple accounts**



26%

write them down on **paper**

17%

type them on their **phone** or **computer**

6%

even admit to using **well-known** passwords

In total, 78% of respondents use an insecure method to help them remember their password, and this rises to 86% among 18-34 year olds. This is surprising considering how young people are thought to be more tech savvy, and therefore more cybersecurity savvy. However, this may also be because 18-34 year olds generally use more apps, devices and technologies which require passwords, and therefore have to rely on other methods to help them remember their passwords. France (87%) has the highest proportion of people that use an insecure method, followed by the Netherlands (79%) and the UK (74%).

DR MARIA BADA
Research Associate, Cambridge University

> Unfortunately, it does not appear that stress around data security has led the majority of people to improve their personal cybersecurity habits.
>
> Often someone has to fall victim to a crime to change their password. What will lead users into changing their cybersecurity mindset is to think about the trade-off between the risk of not changing passwords and the cost of changing them constantly.

Password Managers and Single Sign-On Solutions

– From Many Passwords to One

There are easy ways to reduce this pressure from passwords. Password managers, where a single strong passphrase is used to unlock a vault holding individual passwords to all the applications, offer a helpful alternative. They can free users to create strong, unique passwords to each of the services they use, without having to worry about remembering any of them. However, we found only 14% of the respondents adopted a password manager. Buying, installing and managing another piece of software can be difficult, and usability is still not quite seamless across applications and devices.

For corporations, an even better solution is deploying a Single Sign-On (SSO) solution, which has all the benefits of password managers, and many more. Users will only have a single password to remember and get access to all the applications. And even better, as SSO solutions leverage modern federation protocols like SAML 2.0 and OpenID Connect behind the scenes, connections to modern applications don't even use passwords making access far more secure. SSO also makes adding strong multi-factor authentication simple and helps protect all application access.

3

WHAT'S THE ALTERNATIVE TO PASSWORDS?

Innovation and Integration

Technology innovation over the last decade has given businesses a myriad of new opportunities to approach security in different ways. Now, organizations can combine methods such as biometrics, with traditional methods that are still secure, and remove inadequate practices altogether. After years of false predictions, there is finally a light at the end of the tunnel for a passwordless future.

Okta's research showed there is an appetite for biometric authentication with many advantages:

EASIER DAY TO DAY LIFE

24% work
28% personal

MAKE DEVICES/ ACCOUNTS SAFER

15% work
20% personal

REDUCE STRESS & ANXIETY LEVELS

13% work
16% personal

LESS WORRIED ABOUT SECURITY

8% work
11% personal

INCREASE PRODUCTIVITY

11% work
8% personal

View of the Future: Biometrics

Biometric authentication leveraging fingerprints, eyes, faces and voices was introduced primarily to offer better protection against unwarranted access to accounts or systems. Unlike usernames, passwords and pin codes, the data is unique to each person.

Biometric authentication is becoming more widespread on personal and work devices, while enterprises are also deploying their own biometric security measures.

Okta's research showed a growing appetite and acceptance of biometrics as a further layer of security at work or even a long-term replacement of passwords:

16% of respondents expect **fingerprint authentication**

6% expect **facial recognition**

4% expect **eye print authorisation** for work devices

A staggering 70% of respondents would consider or currently use biometric data in their personal life, 24% think it could make day-to-day life easier in their work life, and 13% think it could reduce stress and anxiety at work, suggesting that the mental health impact of using passwords would be somewhat mitigated by using biometric authentication.

Respondents also believe that using biometrics could help make accounts safer at work (15%), and would make them worry less about security (8%). Biometrics would also help to increase productivity at work, according to 11% of respondents.

Focusing on Education

While there are many benefits associated with using biometrics, people aren't fully convinced, with 86% of respondents having some reservations of sharing their biometric data with their work. When we asked why these respondents would not be keen on sharing their biometric data with work:

21% 

said that their **biometric data** could be **hijacked**, so they wouldn't be able to use it in the future

15% 

said it would be **too hard to implement**, and the same proportion said they felt the technology would **break** and they wouldn't be able to access things they need

13% 

said they **didn't trust** the **technology**

There is work to be done to address misunderstandings on how modern biometric technology works and build trust.

For example, many employees may incorrectly believe that using Touch ID or Face ID on an iPhone or iPad or Windows Hello For Business would enable an enterprise to access their biometric data at will. In fact, the biometric data is highly secure and not available to external parties, or even to the device's own operating system. Instead it's deeply embedded in the security hardware of the device (such as Secure Enclave or Trusted Platform Module), meaning not even Apple or Microsoft can access it, let alone an employer.

It is up to organizations and those developing biometric technologies to demonstrate how the data will be kept secure, and evangelize the benefits and ease of implementing the technology, to reduce initial reservations.

DR MARIA BADA
Research Associate, Cambridge University

> Biometrics have started coming into wide use for quite some time, with mobile phones or computers using fingerprint readers. Therefore, biometrics on consumer devices such as the iPhone have been embraced.
>
> According to the research conducted by Okta, there are still reservations when it comes to biometric data being shared with an employer though. This can be easily explained due to the lack of previous experience of biometric data use in this part of our everyday life.

> But the sound technical understanding gained over the past decade and the maturity of the systems offered by suppliers can only increase the likelihood that passwords and tokens will be replaced in the working lifetime of most readers.
>
> An assumed usability advantage of biometrics is that, since individuals always carry their characteristics with them, there is no token that users can forget, lose or have stolen and this therefore minimizes the memory load on the user and supports the usability principle of universal access.[10]

New Biometric Standards

Biometrics such as fingerprint scanners and facial recognition have become the norm on leading consumer devices. In addition, a project by the FIDO Alliance and World Wide Web Consortium (W3C), called FIDO2, saw the introduction of the W3C Web Authentication (WebAuthn) browser API standard and the FIDO Client to Authenticator Protocol (CTAP) in March 2019. WebAuthn allows web applications to simplify and secure user authentication by using security keys as well as well as platform authenticators – devices like phones and laptops – as authentication factors. WebAuthn uses public key cryptography to protect users from advanced phishing attacks, and is now supported by all leading browsers (Chrome, Firefox, Microsoft Edge and soon Safari) and operating systems.

For consumers and employees it means trust can be preserved, as WebAuthn is a more secure authentication method that removes the risks associated with passwords. When combined with highly secure device biometrics adding the 'who you are' to 'what you know', usernames and passwords are not necessary. This means that enterprise IT teams can rely on registered devices that belong to the end user as authenticators.

This change is profound, as it changes the threat model completely. Before, anyone on the planet with stolen or guessed credentials could gain access. Today, with WebAuthn, only people with physical access to your security key or your device can gain access, and if the authenticator uses biometrics, only you.

[10] Fairhurst, M.C., Guest, R.M., Deravi, F. and George, J. (2002). Using Biometrics as an Enabling Technology in Balancing Universality and Selectivity for Management of Information Access.

4

MAKING PASSWORDLESS POSSIBLE TODAY

As organizations and people place more importance on identities and trust, there is a requirement to ensure our identities are protected.

And we're already seeing parts of organizations — be it employers, app developers, device manufacturers or IT security providers — increase the trust that the user has in them.

Okta's research has found that the current and dominant method for securing apps, devices, systems and accounts is passwords — and this method is inadequate because passwords are susceptible to hacks, encourage insecure behaviour from users, and cause stress, anxiety and a reduction in productivity. It's time to rethink the use of passwords.

We've seen how modern SSO solutions and strong, phishing-proof authenticators create a more robust and logical way of securing an enterprise. The same approach is necessary to making passwordless a possibility. Okta is helping to deliver a secure, passwordless future for enterprises that is easily implemented into any business, of any size, in any sector.

Okta is combining its leading Single Sign-On and Adaptive Multi-factor Authentication (MFA) capabilities with industry-standard authenticators with biometrics, which will enable us to replace passwords at organizations with a combination of a fully contextual risk assessment and WebAuthn authenticators that are highly resistant to phishing and can't be circumvented or cloned.

Organizations can leverage the devices that people are already carrying in a highly secure way that still respects their privacy and doesn't leak any information about who else they might be communicating with or which apps they may be using.

TODD MCKINNON
CEO and Co-Founder of Okta

At Okta, we believe deeply in the potential for technology, and that for organizations of all sizes and industries attempting to become technology companies, trust is the new frontier. Today, businesses need to adopt technology that enables them to innovate quickly, while prioritizing the security, privacy, and consent controls that help them to be trusted. Passwords have failed us as an authentication factor, and enterprises need to move beyond our reliance on this ineffective method. In 2019, we will see the first wave of organizations going completely passwordless and Okta's customers will be at the forefront.

Visit **www.okta.com** to learn more about our approach