my1login

Connecting People, Apps & Devices

Are you wasting budget on cyber training?

The limited impact of cyber security training and how you can take control

Contents

Introduction

Cybercrime is an ever-present and growing threat.[1] Against this backdrop, reducing the risk of cyber-attacks and the damage they cause is increasingly a priority for organisations across all sectors. In search of ways to prevent such damage, businesses turn to cyber security training time and time again. But training is failing to make a difference.

My1Login surveyed over 2,000 people across the UK, split evenly between office workers and business leaders, to understand attitudes towards passwords and cyber security. The findings revealed that employees often know how to improve their behaviour, but for want of time, motivation, or effort, they don't make the changes required to keep themselves and their organisations safe.

A new approach is needed, one that will shift the burden of responsibility away from the user and put organisations back in control of security. This paper will investigate the results of My1Login's research, outlining the behaviours that put organisations at risk, why existing solutions don't work, and how we can take a different approach to security, moving towards a 'passwordless' future using Access Management solutions. We'll also look at how specific groups are affected, and which sectors are most in need of a fresh approach to reduce their cyber risk.

Section 1:

Risky behaviour in the workplace

Passwords are a perennial problem in cyber security. They are an easy target for criminals, offering a gateway into organisations and enabling criminals to conduct damaging, far-reaching cyber-attacks.

Unfortunately, poor password habits make cyber criminals' lives far easier. From creating weak passwords to reusing them across applications, employees consistently struggle to maintain good password 'hygiene'. This leaves organisations vulnerable to attack: four in ten UK businesses and a quarter of charities experienced a breach or cyber-attack in the last 12 months.[2]

87% of office workers reuse their passwords across applications

The prevalence of poor password behaviour among employees is alarming. My1Login found that a staggering 87% of office workers reuse their passwords across applications. In many ways, this is unsurprising, given how difficult it is for employees to remember multiple passwords. However, the reuse of passwords poses a significant cyber security risk to organisations. It increases the damage potential of an attack, enabling access to multiple accounts when only one application is breached.

Another frequent behaviour among office workers is the use of personal passwords for business applications, and vice versa. This practice was reported by 62% of survey respondents. In these cases, not only are employees reusing passwords, but they are also using them across both personal and business accounts. Personal accounts, beyond the visibility of office IT teams, might be less secure and even more vulnerable to attack. If an employee's personal password is stolen, their professional accounts using the same password would also be compromised, putting their whole organisation at risk.

Case study: *The risk of reuse*

In 2012, Dropbox suffered a breach because one of its employees had reused a corporate password as their LinkedIn password. Criminals initially stole 128 million login details from LinkedIn but, using this employee's reused password, they were also able to access Dropbox and steal 68 million login credentials.

Source: *https://techcrunch.com/2016/08/30/dropbox-employees-password-reuse-led-to-theft-of-60m-user-credentials/.*

To help with remembering passwords, many employees resort to writing them down. Just over half (52%) admit to writing down their work passwords, storing them in a document or on their mobile or computer. Writing passwords down may help employees remember stronger passwords, but it's not a secure solution, and ultimately opens up other avenues for attack. If a Word document or notes application is accessed by a malicious actor, multiple accounts could be at risk. If these documents are backed up to the cloud, they could be stored in an unencrypted form, ready to be harvested if a criminal gains access.

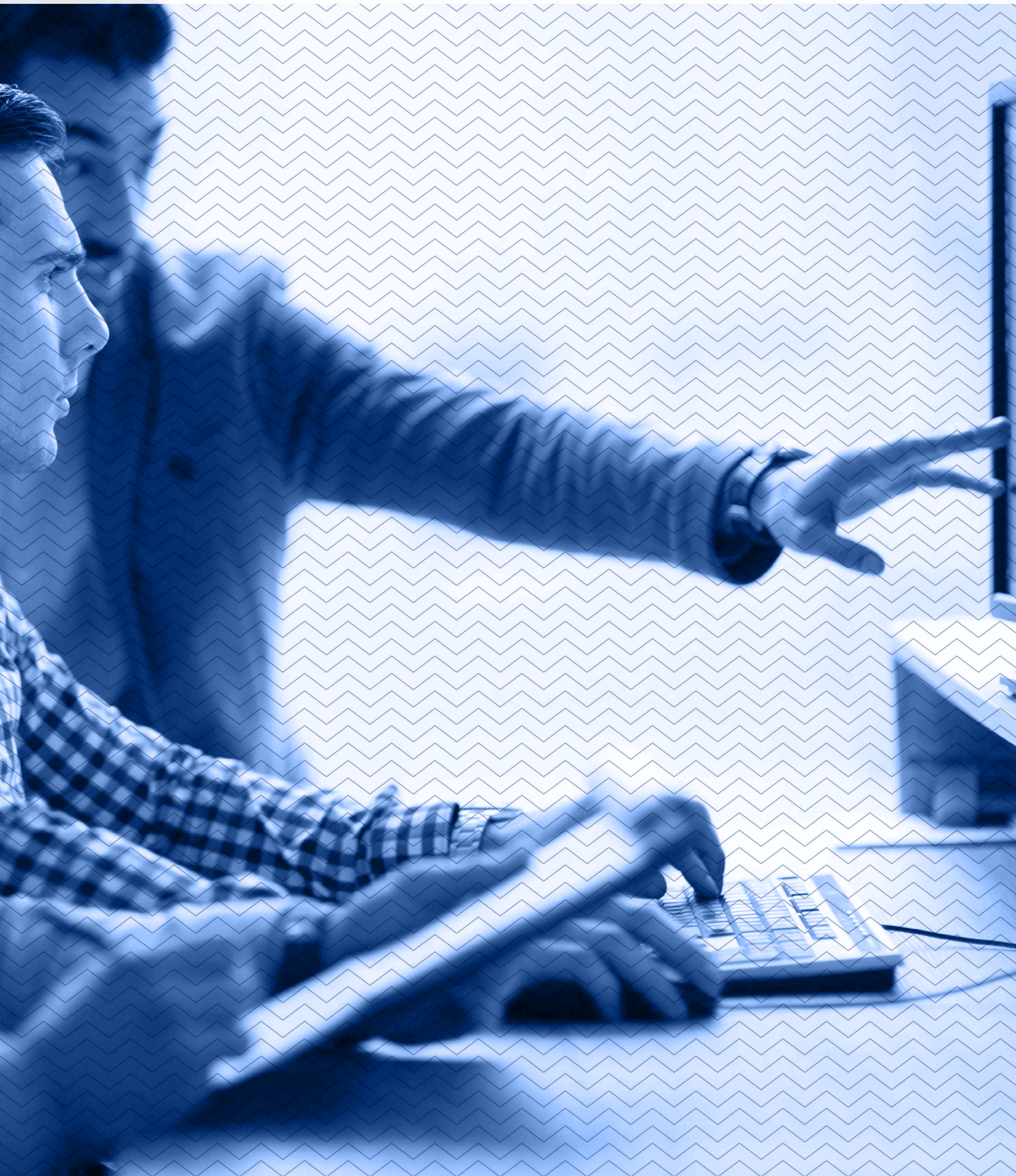
For the most part, business leaders seem to be aware of their employees' poor password habits. The reuse of personal passwords at work is a concern for 70% of business leaders. Similarly, just over 60% are concerned that employees have too many passwords to remember.

46% of employees sign up for web apps not approved by their organisation, but only **25%** of business leaders are concerned about this behaviour

Yet, in other cases, business leaders underestimate risk. This is the case with Shadow IT practices. Nearly half (46%) of employees say they sign up for business web apps not approved by their organisation. However, only a quarter of business leaders say they are concerned about their employees signing up for unapproved apps. Considering the use of unauthorised and unvetted apps compromises the internal security of an organisation, business leaders' lack of concern about this issue is troubling. How many other cyber risks go unnoticed or underestimated? And how much sensitive corporate and personal data is leaking out of enterprises as a result of lack of governance around these practices?

Section 2:

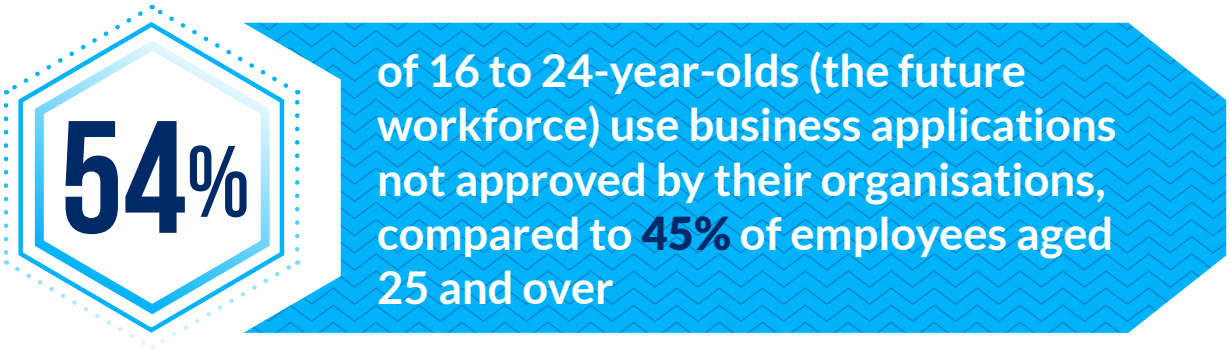
Who is most at risk?



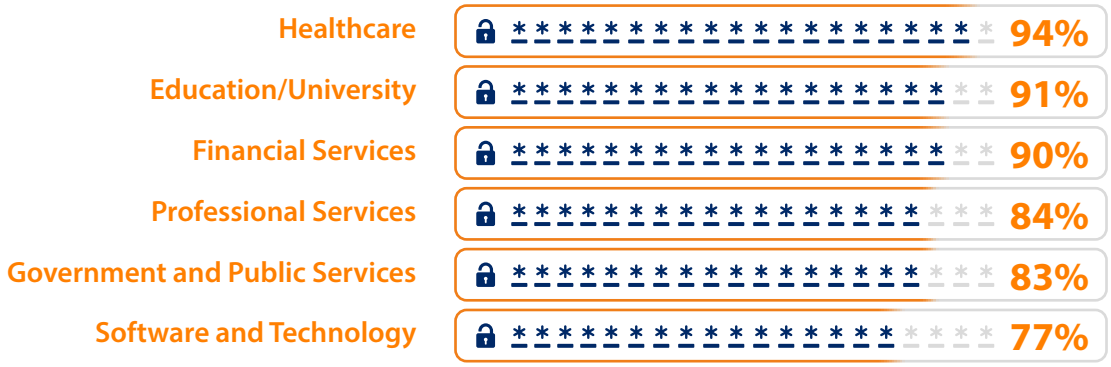
Password habits tend to be poor regardless of age, sector, or organisation size. Yet, some variations in attitudes and behaviours are worth exploring to understand the risks particular groups pose.

While some might assume password habits vary across different age groups – expecting a difference between the habits of tech-savvy Millennials and Gen Z employees, and the habits of older employees – many poor password practices remain consistently high across all age groups. The use of personal passwords for business applications, for example, does not correlate with age and remains relatively high across all groups. Reuse of passwords is high across the board, though older age groups are a little less likely to have this habit than younger age groups; 90% of under 40s reported reusing passwords compared to 81% of employees aged 40 and over.

The habit of writing down passwords is higher among older age groups, with 59% of employees aged 40 and over-reporting this practice compared to 49% of under 40s. On the other hand, the very youngest employees are most likely to use business applications not approved by their organisations. 54% of 16 to 24-year-olds say they do this, compared to 45% of employees aged 25 and over. The latter finding highlights the risk the more tech-savvy generation poses in the workplace. The up-and-coming Generation Z will be more familiar with, and perhaps inherently more trusting of, technology while remaining unaware of the associated risks. Employers will have to bear this in mind as they determine future IT practices and policies.



As well as variations across age groups, some variation exists between industries. While reuse of passwords is common in every industry, employees in healthcare and education report particularly high rates of password reuse, at a staggering 94% and 91% of employees respectively.



This compares with 83% of employees in government and public services and 77% in software or technology reusing their passwords. Similarly, employees' use of personal passwords for business applications, or vice versa, is higher in education (75%) and healthcare (68%) than in professional services (55%) and technology (45%). The public sector ranks somewhere in the middle, with 61% of employees mixing the use of personal and business passwords.

The education and healthcare sectors repeatedly show higher levels of poor password behaviour. In light of the recent spate of cyber-attacks on these sectors, this is somewhat unsurprising. In May 2021, the Irish Health Service Executive (HSE) suffered a ransomware attack, following which patients' personal and medical information was shared online.[3] A month later, all five secondary schools on the Isle of Anglesey were forced to shut down their IT systems after a cyber-attack.[4] These sectors are routinely targeted by cyber criminals. They are viewed as soft targets with minimal resources to invest in protection and the promise of a high reward in the form of sensitive personal information.

[3] Irish Health Service Executive Press Release: https://www.hse.ie/eng/services/news/media/pressrel/hse-cyber-security-incident.html.
[4] Isle of Anglesey County Council Newsroom: https://www.anglesey.gov.uk/en/newsroom/news/secondary-schools-cyber-attack-investigated.

Precisely because they are targets, education and healthcare sectors need better solutions to ensure passwords aren't an easy gateway into their systems for cyber criminals. Leaders are currently addressing this threat by investing in cyber security training, with some variation across industries. Leaders in government and the public sector (85%) and those in finance (88%) report greater provision of cyber security training to their employees than leaders in education (71%) and healthcare (74%) do. But these relatively high levels of investment in cyber security training across the board are not translating into better security behaviour on the part of employees. We need to take a closer look at the existing solutions and why they are not having the desired impact.

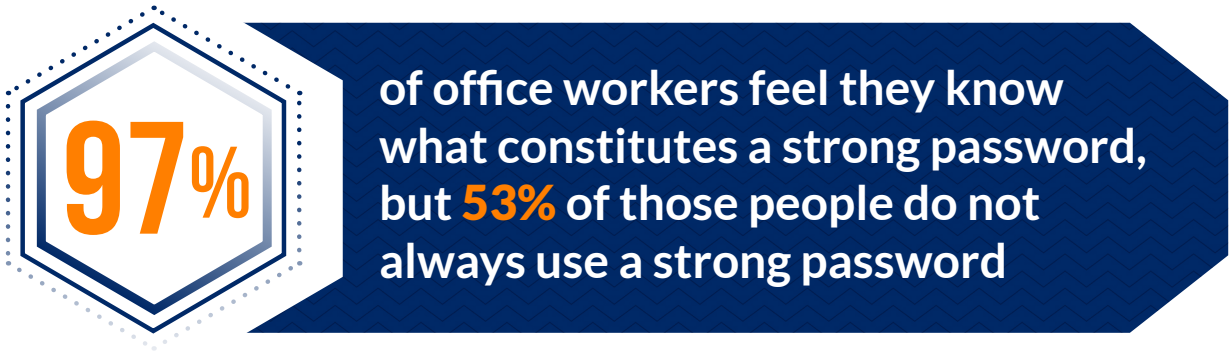
Section 3:

Existing solutions fall short

Existing solutions designed to protect organisations and reduce cyber risk are proving ineffective. In particular, cyber security training – the holy grail of traditional cyber security solutions – is failing.

Cyber security training aims to make users aware of cyber threats and trains them to adopt more secure behaviour online. Along with advice on how to spot phishing attacks, cyber security training typically educates users on password best practice, urging them to choose a strong and unique password for each account.

According to the ICO, human error is the leading cause of data breaches,[5] so it makes sense to target the behaviour of employees to ensure they are not exposing themselves and their organisations to malicious actors. However, time and time again, the lessons of cyber security training are failing to demonstrably impact employees' behaviour. My1Login found that, while 97% of office workers feel they know what constitutes a strong password, 53% of those people do not always use a strong password. The gap between knowledge and behaviour is striking, and it's the primary reason why cyber security training cannot be relied upon to deliver significant risk reduction for organisations.



Indeed, the behaviour of office workers who have received cyber security training and those who have not varies only slightly. This is especially the case for employees who have only received 'a little' training as compared to 'a lot'. Use of personal passwords for business applications and vice versa is reported by 63% of office workers who have received 'a little' training', compared to 61% of those who haven't received any. The proportion of employees who have had 'a lot' of training but still reuse a personal password for business applications is only slightly lower at 57%.

[5] Information Commissioner's Office (ICO): https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.

Reuse of passwords varies slightly more between those who have received training and those who have not, though the difference is still not significant enough to deliver worthwhile ROI for businesses. While 91% of office workers without training reuse passwords at work, 85% of those who have received training reuse their passwords. 78% of those who have had 'a lot' of cyber security training reuse their passwords. With other behaviours, there is no discernible difference.

The proportion of employees who write down passwords, for example, does not vary at all between those who have had cyber security training and those who have not, remaining at 52% for both groups.

The limited impact of cyber security training on user behaviour is striking. But there are further reasons why the training approach falls short. Some aspects of security are not covered by cyber security training at all, in particular the onboarding and offboarding processes for employees. Fast and secure offboarding is key to safeguarding an organisation's data. Employees who have left a company should not be able to log on to work applications once they are no longer employed. Those who leave under duress pose a particularly high risk. It has been known for disgruntled ex-employees to exploit their access to organisations to cause disruption and open up networks to attacks.

Case study: *Incurring the wrath of ex-employees*

In February 2020, Salvatore A. La Rosa wreaked havoc on his ex-employer using his unrevoked admin credentials. La Rosa had worked as an operations and premium services manager for Spectra Food Services and Hospitality for five years. After being let go in January 2020, La Rosa retained access to the company's online administration panel. During the first home game of the San Jose Earthquakes 2020 MLS season, La Rosa deleted Spectra's concessions menu and payment selections, leaving staff unable to take orders or accept payment by credit card. This caused long delays, lost orders, and angry customers. La Rosa was jailed for 20 months after admitting to sabotage of the company's system.

Source: *https://www.courthousenews.com/soccer-stadium-hack/.*

The security risks associated with offboarding have been exacerbated by the Covid-19 pandemic and the shift towards remote working. Where employees leaving a company might previously have handed in their equipment on the last day of work, those working from home now have access to that equipment until arrangements are made to return it. Similarly, IT teams no longer have direct access to an employee who is leaving and must organise the offboarding process remotely.

The risks associated with offboarding are a worry for many employers. 40% of business leaders surveyed by My1Login state they are concerned that when employees leave, they may know passwords or retain access to applications that contain corporate data. To reduce this risk, employers need a solution that caters for remote working and ensures access to corporate applications is immediately retracted once an employee leaves the organisation. Giving organisations greater control over credentials and login processes is the way forward.

Section 4:

Putting organisations back in control

Realistically, we cannot expect a dramatic improvement in employees' password habits any time soon. Even with the best will in the world, people will struggle to create and remember a strong and unique password for every single account they use. Business leaders seem to recognise as much. 63% say they think employees have too many passwords to remember. So, how can the pressure on employees be reduced while still protecting the security of organisations?

Instead of relying on employees, business leaders need to take them out of the equation as much as possible. Shifting responsibility for passwords back to organisations will remove the burden from employees and place organisations back in control of their security. With 84% of employees reporting being frustrated by password requirements, it's clear this approach is beneficial for employee wellbeing, productivity, and satisfaction, as well as for organisational security.

Going 'passwordless' is the most effective way to put organisations in control. If users no longer have to remember passwords to log in, the possibility of credentials being stolen or compromised is removed. Passwordless has been a long time coming. Calls to end the use of passwords date back to at least 2004, when Bill Gates spoke at the RSA Conference and said passwords "just don't meet the challenge for anything you really want to secure".[6] We are now much closer to a passwordless reality, and to removing a weakness that criminals have been able to exploit for far too long.

Access Management is the key to giving employees a passwordless experience. One example of an Access Management solution is single sign-on (SSO), where users log in once to access all accounts. Adopting this kind of solution enables organisations to take control of passwords used within the business and offer a fully passwordless experience for employees. Currently, organisations are adopting such solutions, but too many of these SSO solutions are limited in how many applications they work with, and many do not cover legacy applications. As the use of SaaS grows, SSO solutions also need to integrate easily with new applications as they are created.

While over half (51%) of business leaders surveyed by My1Login say they use an SSO solution at work, only 20% of all business leaders report using an SSO solution that works with all applications. In other words, only 40% of business leaders using SSO say their solution works for all applications. My1Login also found that over a quarter (27%) of business leaders say their employees have to log into legacy Windows desktop applications that fall outside of SSO. Most users are still having to create passwords for multiple applications, meaning the risk an SSO solution is designed to remove is still prevalent.

To give employees a truly passwordless experience, solutions need to work for all applications. An SSO solution should also be seamlessly integrated, allowing users to login without having to interact with a separate interface or portal. Only when users can access all work applications without physically entering a password will corporate accounts be properly secured against password theft. The beauty of a solution that works for all applications is that it not only addresses cyber security risk but also saves employees and organisations time, as 'logging in' becomes a one-time, streamlined, and efficient process.

Passwordless solutions also ease otherwise burdensome processes such as onboarding and offboarding. When logins are controlled centrally by an organisation, access for a particular employee can be granted or revoked with the click of a button. Whether setting up a new employee or offboarding someone who is leaving an organisation, passwordless makes the process faster and more secure. It also removes the need for physical deactivation of accounts, so access can be removed even if an employee is remote.

Conclusion:

Transitioning from current-state to passwordless

For too long, the cyber security community has placed the burden on users to strengthen their passwords against cyber criminals' advances. Instead of improving security, this has left employees frustrated as they struggle to meet complicated password requirements.

It doesn't have to be this way.

Removing the need for passwords liberates employees from unrealistic and burdensome expectations, freeing up their time to spend on work-related tasks. At the same time, it removes a key weapon in the armoury of cyber criminals.

Adopting a solution that transitions the enterprise from password-based to passwordless puts organisations back in control of their security. It enables central control of logins, making processes such as onboarding and offboarding more secure. It also increases efficiency, reducing the need for employees to log in to every single application with a new password.

In an era of rising cyber-attacks, especially those directly linked to credential theft, now is the time to go passwordless.

my1login

Connecting People, Apps & Devices

Founded in 2007, My1Login is a leader in Identity Management, protecting enterprises against cyber security threats through its Identity & Access Management (IAM) solution.

My1Login solves the problem of cyber-security risks created by the increasing sprawl of corporate user identities, usernames, and passwords by providing Single Sign-On for all web and Windows desktop applications that is seamlessly linked to the user's directory login.

My1Login's IAM solution removes the burden of passwords from users and puts the organisation back in control of security by enabling enterprises to transition from password-based to passwordless authentication. It centralises control of passwords, making processes such as onboarding and offboarding more secure and efficient. My1Login's auto-detection of applications being accessed further reduces the attack surface by identifying Shadow IT risks.

My1Login is the UK's most secure, most widely-compatible Identity & Access Management solution that enables organisations to mitigate password-related cyber-security risks, control user identities and help meet critical compliance obligations.

10K+ Apps

In addition to working with today's enterprise cloud apps, My1Login also works with Windows desktop apps and mainframes, including IBM and Unisys, and integrates with virtualised apps such as XenDesktop, XenApp & Storefront.

Securely manage access to EVERY application for ALL users from ANY device

SC 2020 awards EUROPE Winner

2017·2018·2019 Computing Security Awards WINNER

computing Security Excellence Awards 2018 Winner

HAVE A QUESTION? SPEAK TO OUR IDENTITY EXPERTS

Call | 0800 044 3091

Website | www.my1login.com

Email | contact@my1login.com

Reference us | via Gartner