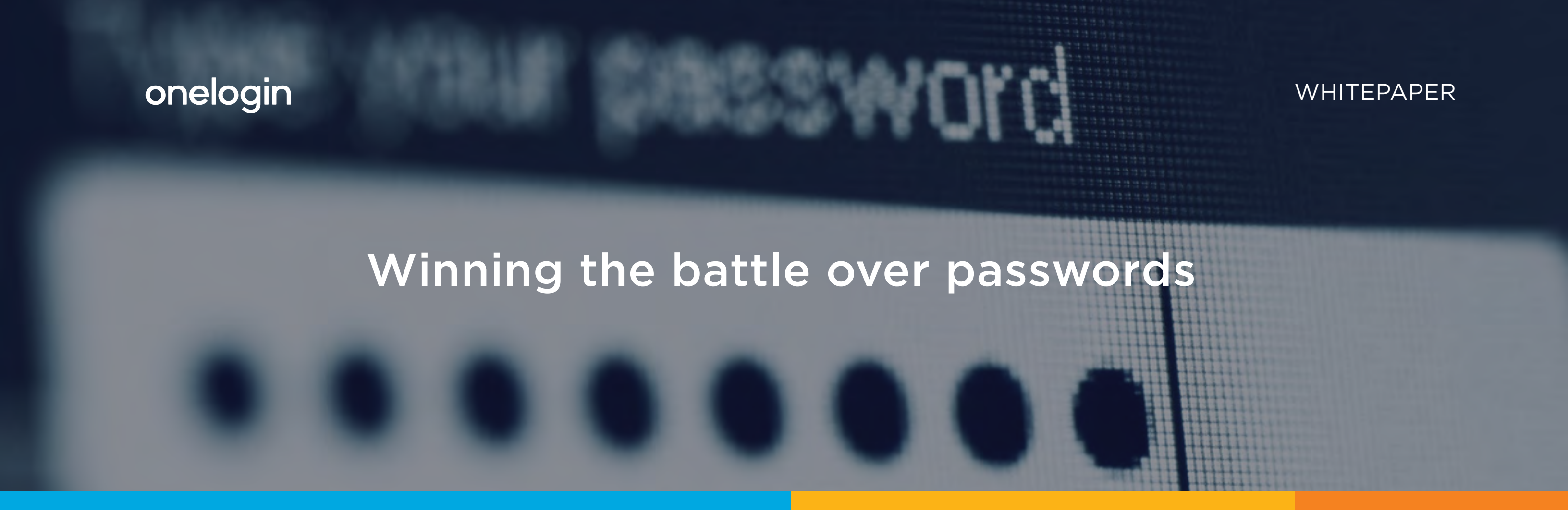


WHITEPAPER

Winning the battle over passwords

Companies worldwide are in a war against cybercriminals. It’s ongoing with no end in sight, and every company is at risk. Access credentials, particularly passwords, are at the heart of the battle because hackers are trying to obtain them.

Companies try to protect passwords, knowing that if the enemy gets an employee’s password, there is a good chance they’ll infiltrate the organization, steal data and IP, and wreak havoc that will cost the business for years and even decades to come. But our recent study of 600 IT professionals in the US and UK suggests that companies have a long way to go.

THE NATURE OF THE WAR

The war against cybercrime is waged every day in the trenches of IT departments. Businesses invest billions, with some projecting an estimated $1 trillion will be spent globally between 2017 and 2021 on cybersecurity.[1] IT professionals implement hardware, software, and spend a considerable budget to protect their companies.

They have to because hackers cost the global economy more than $111 billion annually.[2] And the impact on individual corporations can be huge. In 2018, the average cost of a breach was $3.86 million worldwide and $7.91 million in the United States.[3] And breached companies underperformed the market and were down against the NASDAQ by -15.58 percent even after three years.[4]

[1] https://cybersecurityventures.com/cybersecurity-market-report/
[2] https://www.edts.com/edts-blog/how-much-should-i-spend-on-cyber-security
[3] https://costofadatabreach.mybluemix.net/?cm_mc_uid=51326371932415482902454&cm_mc_sid_50200000=34650641550767365123&cm_mc_sid_52640000=78551551550767365136
[4] https://cybersecurityventures.com/cybersecurity-market-report/

Changing tactics but one constant

The nature of the war is such that tactics are constantly changing. Hackers find new tools and methods for gaining access and companies respond with new defenses. The criminals look for weaknesses in these new defenses—and they usually find them.

It’s a never-ending game of whack-a-mole for IT professionals. The game is made harder because companies just aren’t as nimble as cybercriminals. But it’s a game corporations can’t afford to stop playing.

There is one constant, though. The primary target of cybercriminals continues to be passwords.

Passwords are at the heart of hacking efforts because they are usually the key to unlocking the enterprise and gaining access to corporate data, customer information, and IP. Most organizations still haven’t adopted two-factor or multi-factor authentication, meaning the passwords remain the only true obstacle to entry for hackers. (Usernames are easy to uncover or guess.)

So you would think that organizations would be doing all they can to eliminate the number of passwords needed and protect the ones employees use. But they aren’t. Our recent survey found companies are behind in implementing best practices and adding technology to lock down and protect passwords.

THE PASSWORD CHALLENGE

The enduring challenge for IT is how to secure access to corporate information and resources without burdening those legitimate users trying to access it. That means:

- Making it fast and easy for users to login while making it hard for criminals to do the same.
- Ensuring passwords—still the main lock on data—can be remembered by users but are hard to uncover by hackers.
- And ideally, eliminating passwords wherever possible by deploying single sign-on.

The security/usability juggling act is ongoing. For a long time, the guidance has been to make passwords complex. Specifically, the recommendations required that passwords:

- Be long
- Use a mix of uppercase and lowercase characters
- Include numbers
- Include special characters

Businesses have implemented protection measures and guidelines, with well over 90 percent of companies in both the US and UK reporting they have them. However, long and complex passwords create a problem. Namely, they're hard to remember. So, users resort to tried and true methods like:

- **Reusing the same password.** Over 70 percent of employees reuse the same password at work.[5] And 59 percent reuse their passwords everywhere, for both work and personal accounts.[6]
- **Writing passwords down or otherwise noting them.** 65 percent of business managers record their passwords on a private document such as a post-it note or share it with other individuals.[7]

Or users simply forget their passwords, requiring password resets. And since many companies don't have automatic password reset tools, that means IT eats up its budget resetting them.

Reusing the same password and noting it in insecure locations creates opportunities for criminals. Which defeats the whole purpose of requiring complex passwords. That's probably why the National Institute of Standards and Technology (NIST) recently updated its guidelines to reduce complexity requirements and focus on other best practices.

Unfortunately, the word hasn't gotten out yet to companies in the US and UK, as our survey of 300 IT professionals in each country shows.

To protect your company, you must:

- Stay up-to-date with the latest password best practices.
- Enforce those best practices within your organization.
- And use technology to reduce the number of required passwords and protect access.

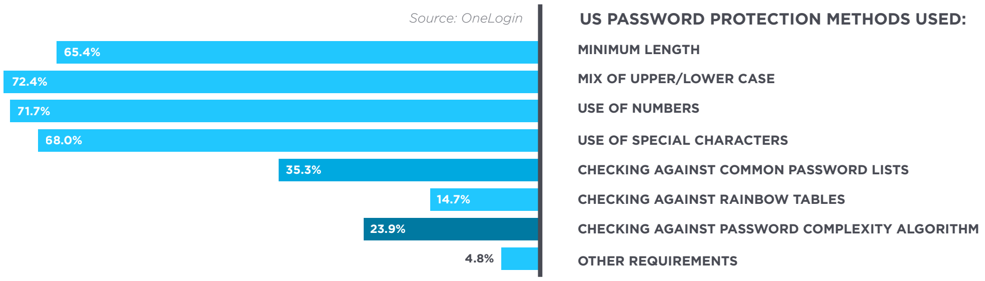
HOW COMPANIES SECURE PASSWORDS NOW

OneLogin's recent survey of 300 IT professionals in the US and 300 in the UK shows that companies believe their password protection measures are adequate. In fact, 91.7 percent of US companies and 95 percent of UK companies believe their password protections are adequate.[8]

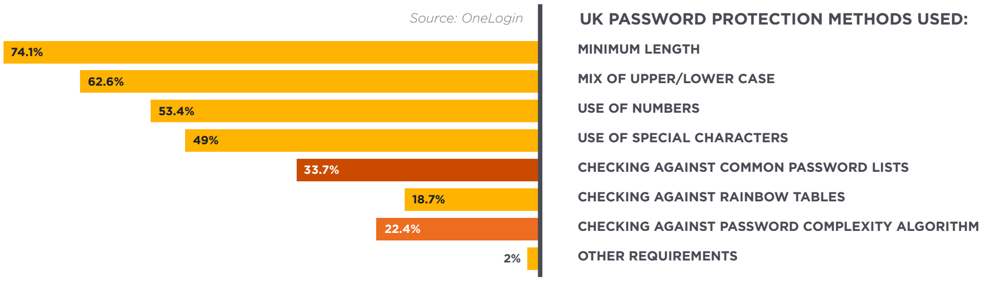
They aren't.

In both the US and the UK, our survey shows that complex passwords are the main method of protection that companies are using. And it isn't enough.

[5] https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report
[6] https://www.tracesecurity.com/blog/articles/81-of-company-data-breaches-due-to-poor-passwords
[7] https://techspective.net/2018/09/10/7-shocking-statistics-that-prove-just-how-important-laptop-security-is/
[8] https://www.onelogin.com/resource-center/whitepapers/password-practices-2019



Source: OneLogin



Source: OneLogin

Sadly, businesses are not embracing the new NIST guidelines or similar ones that call for checking passwords against lists of common passwords, checking them against rainbow tables, or using tools to validate that users have created a complex password.

What is a rainbow table?

A rainbow table is a database of plain text passwords and their corresponding hashed values. Since systems store passwords as hashed values and not plain text, the table can be used by hackers to reverse the hash function and find all or part of a long password.

Another technique that companies employ is to force employees to change their passwords frequently. The idea is to prevent access if a hacker happens to have obtained the password.

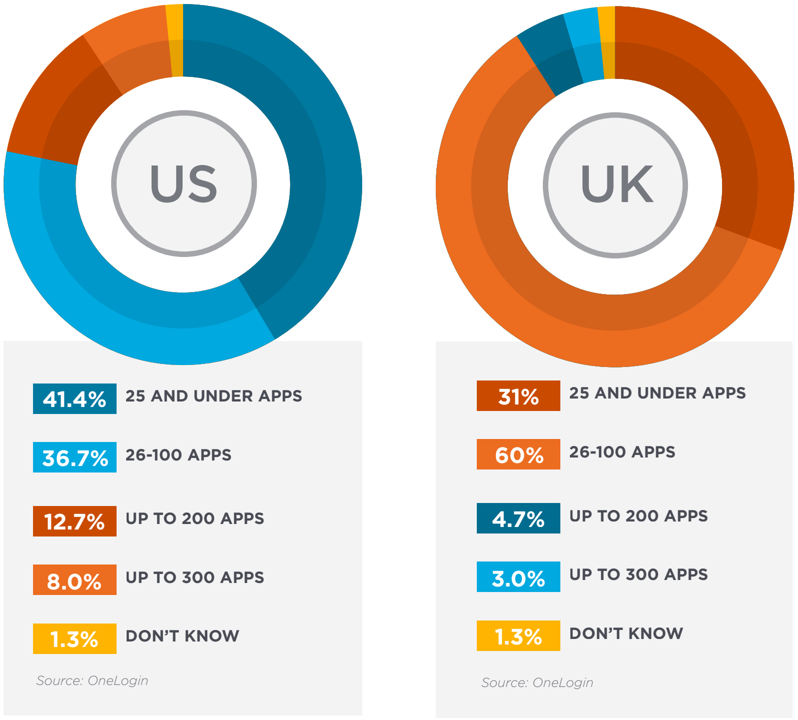
In our survey, a third of US companies rotated passwords monthly and 40.7 percent of UK companies did so. It seems like a good practice. But actually rotating passwords too frequently just adds to the burden on employees trying to remember them and increases the likelihood they'll use the same password or note their password somewhere. The problem is even worse when you consider how much apps are proliferating

APP PROLIFERATION AND SHARED CREDENTIALS PUT COMPANIES AT RISK

A key factor in the password battle is the sheer number of passwords people have to remember. More passwords per user means more opportunities for hackers and more difficulty for users. If people have to remember and enter a password for applications they use, it reduces productivity. And it makes them more likely to resort to insecure practices such as password reuse.

Yet, app proliferation continues and companies are failing to implement tools that could reduce the number of required passwords. Our study found US companies had a mean of 67.65 apps requiring separate credentials. UK companies had a mean of 58.54 apps.

NUMBER OF APPS REQUIRING INDIVIDUAL PASSWORDS



Source: OneLogin

Source: OneLogin

Another practice that many companies employ which creates security risk is shared credentials: multiple people use the same username and password to login to an account. Our survey found that US companies had a mean of 34.39 applications that used shared credentials, and UK companies had a mean of 33.97.

That's a lot of applications whose access is entrusted to multiple employees.

THE RISK AND COST OF POOR PASSWORD HYGIENE

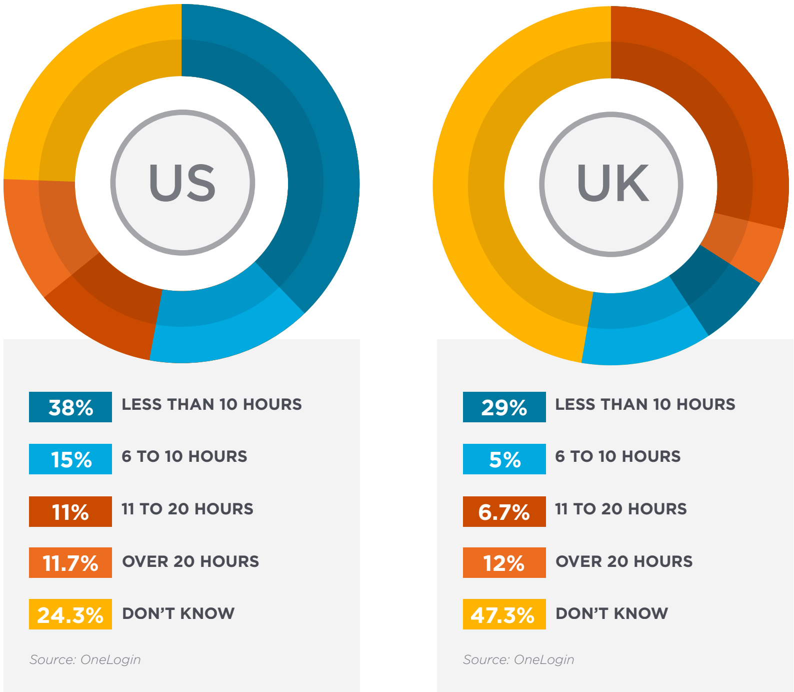
The result of a large number of applications and requiring complex passwords is that companies are spending a significant amount of time resetting passwords. There are tools that enable users to reset their own passwords, but these aren't in high use. Instead, at most companies IT or an outsourced help desk resets user passwords.

Resetting passwords adds up

Forrester found that the average labor cost of a password reset is $70 or £50.

In the US and the UK, IT spent an average of 2.5 months a year on password resets. Even more alarming: 24.3 percent of US respondents and 47.3 percent of UK respondents didn't even know how much time they were spending on password resets.

HOURS/WEEK SPENT ON PASSWORD RESETS



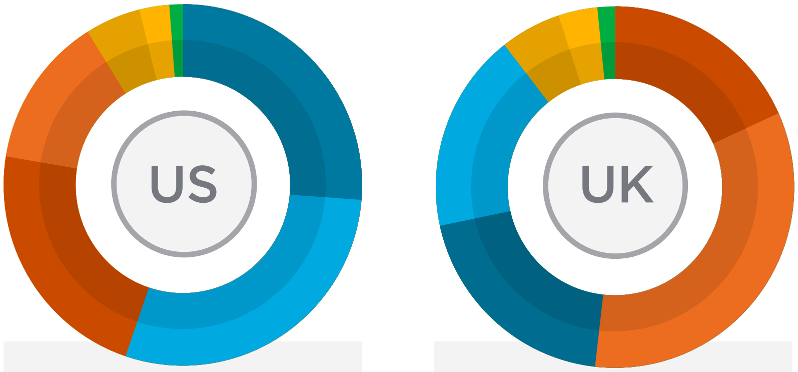
Source: OneLogin

Source: OneLogin

FAILURES TO DEPROVISION USERS RAISES RISKS

Another risk related to password issues is deprovisioning of users. When organizations have dozens of apps for each user and no effective kill-switch for deprovisioning, they must manually deprovision departing employees from each application. It's a time sink. Which is probably why almost half of businesses both in the US and the UK take up to a month to deprovision ex-employees—leaving their organizations vulnerable to a malicious attack.

TIME TO DEPROVISION DEPARTING EMPLOYEES



26.7%	1 DAY
28.3%	1 WORKING WEEK
21.7%	UP TO 1 MONTH
14%	UP TO 6 MONTHS
4.7%	UP TO A YEAR
3%	MORE THAN A YEAR
1%	DON'T KNOW AS WE DO NOT OFTEN DEPROVISION FORMER EMPLOYEES

Source: OneLogin

18%	1 DAY
34.3%	1 WORKING WEEK
19.3%	UP TO 1 MONTH
17.7%	UP TO 6 MONTHS
5.7%	UP TO A YEAR
3.3%	MORE THAN A YEAR
1.7%	DON'T KNOW AS WE DO NOT OFTEN DEPROVISION FORMER EMPLOYEES

Source: OneLogin

COMPANIES FAIL TO IMPLEMENT CRITICAL PROTECTIONS

So, what's the solution to win the war—or at least the password battle—while balancing security with usability? There is no one solution. IT must use a host of weapons in their battle. But two stand out: Single Sign-On (SSO) and Multi-Factor Authentication (MFA).

SSO reduces and eliminates passwords. In the best case scenario, users have only one set of credentials which they use to access all applications and corporate resources. SSO systems let the user login once each day using one password and then, based on trust relationships and tools like SAML, access all their applications without having to login again.

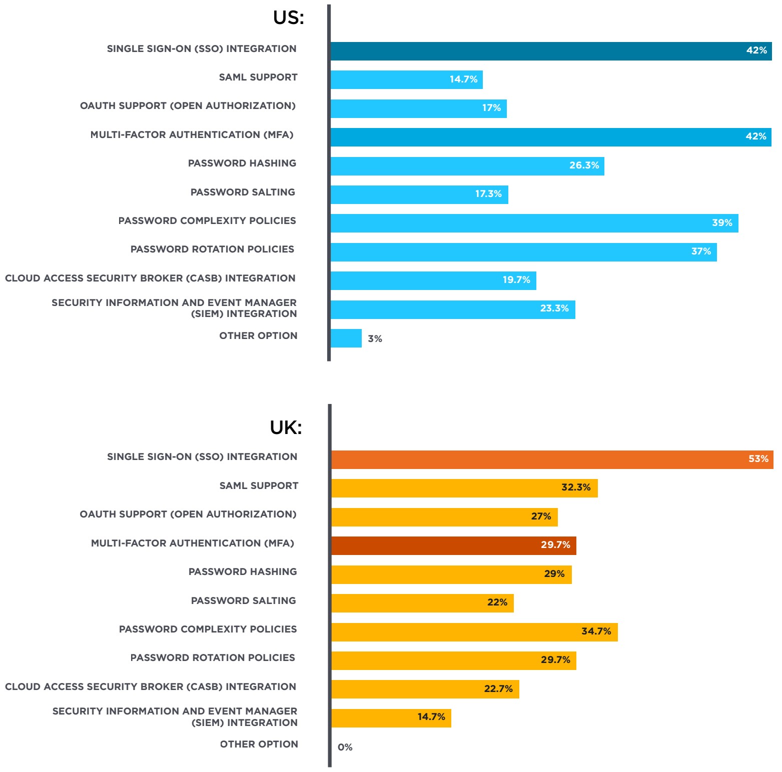
Not familiar with SSO? Find out how it works.

MFA helps secure login by requiring an additional, strong authentication factor that must be provided. Strong authentication factors come in a variety of forms. Some of the more popular include one-time passwords generated by a mobile app, a push notification sent to a mobile phone, or a biometric factor such as a fingerprint or facial recognition.

Not familiar with MFA? Find out how it works.

Unfortunately, our survey found that businesses are not adopting these critical technologies widely enough. While slightly more than half of UK companies have adopted SSO, less than half of US ones have. Less than half of US companies have adopted MFA and a woeful 29.7 percent of UK companies have done so. Tools supporting SO protocols, like SAML and OpenID Connect, are also under-adopted. Even tools like password salting and hashing are under-utilized.

METHODS COMPANIES ARE USING FOR MANDATORY AUTHENTICATION REQUIREMENTS FOR INTERNAL APPS:



Conclusion

As long as companies continue to require users to enter passwords for each application and fail to add MFA to better secure authentication, they will remain at risk. Companies are struggling to juggle security and usability when it comes to passwords. But in reality, security always loses because if password practices are burdensome, users resort to insecure practices.

The path forward requires a move to single sign-on and multi-factor authentication to ease the burden on users while maintaining and even improving login security. As companies wake up to the password challenge and add these critical measures, they will begin to win the battle over passwords and take the lead in the war on cybercrime.

About OneLogin

OneLogin is the leader in Unified Access Management and simple password reset solutions, Enabling Organizations to Access the World™. Businesses of all sizes use OneLogin to secure company data, while increasing IT administrator and end user efficiencies.

Implementation of our identity management solutions can be achieved in hours rather than days, delivering a fully featured administrative and self-service portal. Our ability to handle on-premises and cloud/SaaS applications makes us the identity-as-a-service vendor of choice for the hybrid enterprise. Multi-factor authentication, mobile identity management for one-click access on smartphones and tablets, and real-time directory synchronization all add an extra layer of protection.

Contact us to learn more about OneLogin.

www.onelogin.com/company/contact