The Password Exposé

8 truths about the threats – and opportunities – of employee passwords.

LastPass •••|

Table of Contents

Let's get real about passwords.

The standard approach to password security in the workplace has failed. Even worse, businesses aren't responding to that failure quickly enough.

For most people, the fear of forgetting a password far outweighs the seemingly-remote risk of getting hacked.[2]

91% of people understand the risk of reusing passwords[1]

61% still reuse passwords[2]

1 LastPass Psychology of the Password 2016 Report.

2. 47% of people choose easy passwords due to a fear of forgetting them. LastPass Psychology of the Password 2016 Report.

LastPass •••|

11.1.2017/BX00299/PDF

Passwords are a leading security threat.

81%

of confirmed breaches are due to weak, reused, or stolen passwords.[3]

Whether passwords are old, weak, reused, or compromised, password mismanagement is the leading cause of breaches. With over 4.2 billion credentials leaked in 2016 alone,[4] attackers can easily use stolen passwords to access a corporate network and steal data.

Just one reused password can compromise an entire organization.[5] The problem is not new, and worsens every year as breaches impact companies of all sizes, across every industry. Alarmingly, despite the data, businesses are not prioritizing this password security crisis.

4.2B

credentials stolen in 2016 alone.[4]

3. Verizon 2017 Data Breach Investigations Report (DBIR): http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

4. Risk Based Security's 2016 "Data Breach QuickView Report".

5. A Dropbox employee's password reuse led to the theft of 60M+ user credentials in 2012: https://techcrunch.com/2016/08/30/dropbox-employees-password-reuse-led-to-theft-of-60m-user-credentials/

The true threat: Lack of IT visibility.

Businesses must face today's reality: Passwords are a core part of every employee's daily workflow, and failing to secure them can have dire consequences. We'll reveal the true gap between what IT thinks, and what's really happening. The challenge is gaining visibility into this hidden world, fixing poor passwords, and helping employees manage the sheer volume of credentials in the workplace.

The problem is compounded by employee-introduced, non-sanctioned cloud apps. 78% of IT executives say they do not control all the cloud apps their employees use for business.[6] With no oversight of these apps, there is little protection against the exposure of sensitive corporate data, with an unknown quantity of touchpoints and security behaviors outside the control of the IT team.

By analyzing aggregated data from real businesses using LastPass, we move past the assumptions, to show the true state of password security. In this report, we're sharing the facts businesses don't have – but desperately need. Companies must put the right policies and technology in place to address password problems, without becoming the enemy of the employees.

Methodology:

We anonymized and aggregated customer data from over 30,000 companies using LastPass as their business password manager.

The anonymized data set represents organizations of all types and sizes, from small businesses to large enterprises, across nearly every industry. Though the data set is reflective of companies using LastPass, we've broadened our conclusions about what these findings mean for the business IT community at large.

6. Ovum's 2017 report "Close the password security gap: convenience for employees and control for IT" published in collaboration with LastPass.

The human element is the largest and most effective attack surface. Every business needs to re-evaluate their security policies and adapt accordingly.

— Matt Kaplan, GM, LastPass

Truth #1:
Passwords are everyone's problem.

The numbers don't lie: Passwords are out of control. We estimate that the average 250-employee company would now have some 47,750 passwords in use across their entire organization.

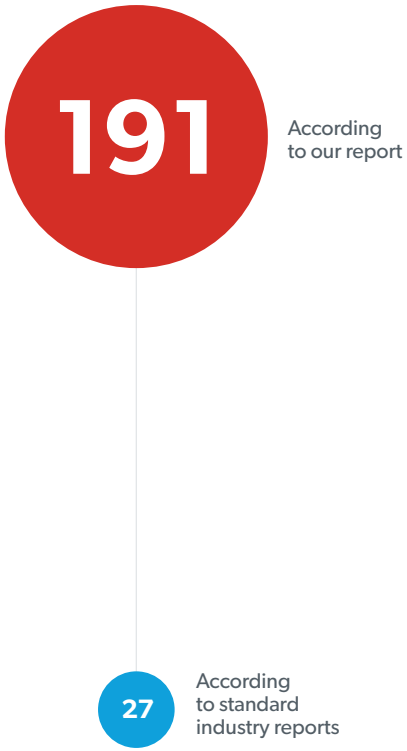
Can companies confidently say they know the strength of every one of those entry points? Are they truly measuring for reused, weak, or old passwords at every single one of those entry points?

The lack of visibility makes it difficult to enforce best practices, to say nothing of the increased frustration due to password proliferation that businesses are experiencing.

Every single password in the company is an entry point that must be secured.

Truth #2:
Employees are overwhelmed by passwords.

How many passwords does the average employee using LastPass have to keep track of?



191. That's how many passwords the average LastPass business user keeps track of. Despite standard industry reports that say employees only have 27 passwords to remember[7], we're seeing a number that's nearly 7 times higher.

Why? People often underestimate how many accounts they truly have.

- If you're a marketer, how many advertising and analytics platforms are you using?
- If you're a systems administrator, how many servers are you managing?
- If you're a sales representative, how many demo accounts are you setting up?

Beyond the enterprise-level apps that are standardized across a business, individual employees have dozens more, whether they use them once a year or every day. When credentials are systematically collected and organized in one place, a more accurate picture emerges.

7. Intel World Password Day Survey 2016:
https://www.buzzfeed.com/josephbernstein/survey-says-people-have-way-too-many-passwords-to-remember

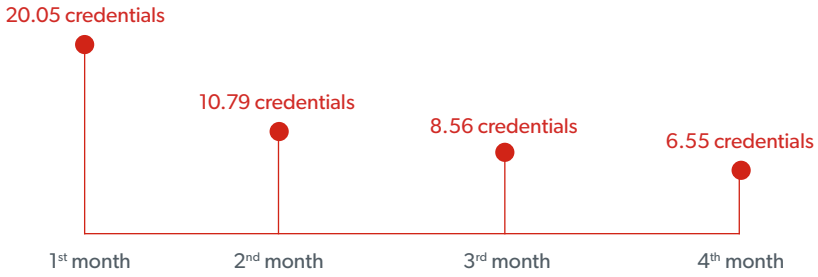
Truth #3:
Passwords are a compounding problem.

Interestingly, in one analysis we performed, the average employee starts with 20 credentials in their password vault and doubles that total after only 3 months. It's no wonder that 61% of people use the same or similar password everywhere,[8] despite knowing it's insecure.

Many businesses can't accurately report on how often employees are creating new accounts, especially outside the apps that are officially sanctioned and provisioned by IT. Once a business adopts a password manager, it serves as a "net" to capture these credentials, giving a much more accurate picture of password proliferation across the organization.

The verdict: Employees are drowning in passwords right now. And it's a problem that continues to worsen in the course of their day-to-day work.

How many passwords do employees add to the vault per month?



61%

use the same or similar password everywhere.[2]

8. LastPass Psychology of the Password Report 2016: https://blog.lastpass.com/2016/09/infographic-introducing-the-psychology-of-passwords.html/

Truth #4:
Employees are constantly logging in.

On average, an employee must type out credentials to authenticate to their websites and apps 154 times a month.

One thing is clear: Typing passwords is (still) a part of the daily grind. If the average employee is storing 191 logins in their vault, it seems that not all passwords are used all the time. It also explains why estimates are too low for the number of passwords employees have. If many passwords are only used a handful of times a year, they're much harder to remember – and secure properly.

Our data also shows that it takes an average of 14 seconds to type a password. That's an average of about 36 minutes a month wasted on an activity with no value-add to the business. When 76% of employees report experiencing regular password usage problems,[9] it's clear there is also a significant productivity impact – and ultimately cost – associated with passwords. Employees are suffering from password-related inefficiencies, which translate directly to a company's bottom line.

9. Ovum's 2017 report "Close the password security gap: convenience for employees and control for IT" published in collaboration with LastPass.

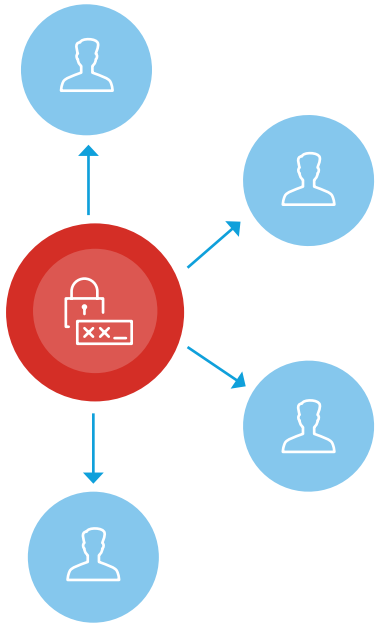
Truth #5:
Approved or not, password sharing is common.

On average, an employee shares about 4 items with others, according to our data.

Common security advice is to keep your passwords private – and for good reason. The fewer people who know a password, the less likely it will fall into the wrong hands. In the workplace, though, sharing of credentials and other sensitive data is also an essential part of getting the job done.

From branded social media accounts managed by marketing to server configurations managed by IT, employees from all departments need to share passwords. Passwords also need to frequently be shared with vendors, partners, clients, and others.

Since sharing is an expected behavior, the key becomes ensuring each of those passwords is unique, and rotating after shared access is no longer needed – especially when an employee leaves the organization.



Truth #6:

It's a blurry line between personal and business passwords.

Of the top 36 domains employees are using in the workplace, at least half are popular consumer solutions. Plus, a recent study showed that 23% of employees are using social media credentials to sign in to business systems and applications.[10] Google, Dropbox, Evernote – for all of these popular apps, employees likely maintain ownership of these accounts, even though they are actively using them in the workplace and may store or share sensitive company data on them.

In today's "bring-your-own-everything", tech-savvy workforce, employees have become a source of new, innovative services for the workplace. When poorly managed, these hidden apps and password behaviors are a threat. But with the proper oversight, these new technologies fuel productivity, efficiency, and even security gains across the organization.

10. Ovum's 2017 report "Close the password security gap: convenience for employees and control for IT" published in collaboration with LastPass.

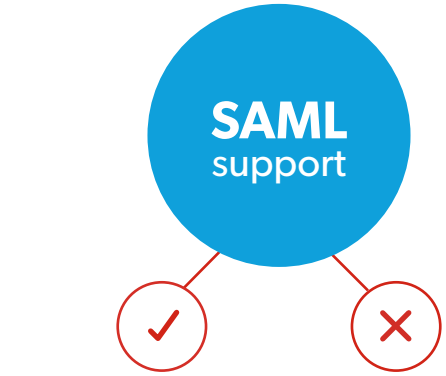
Truth #7:

Single Sign-On is not a one-stop solution for passwords.

While many enterprise-grade apps are SSO-ready, our data shows that over 50% of the most popular websites and services in use do not have out-of-the-box support for SSO.

Single Sign-On (SS0) allows a user to unlock access to all other logins or applications they use at work with a single password or authentication device. For companies who can invest the time and resources into implementing an SSO solution, they focus on integrating with the high-value apps that are pervasive in their organization. Most apps that fall outside that group – including those hidden from IT's view – are left outside the system to be managed by the employees.

Either IT teams need to pick up the burden of configuring and deploying these services, or, more likely, employees are left to manage those credentials on their own. And by sacrificing that control and visibility, IT is again leaving those entry points vulnerable to poor password hygiene and employee misuse.

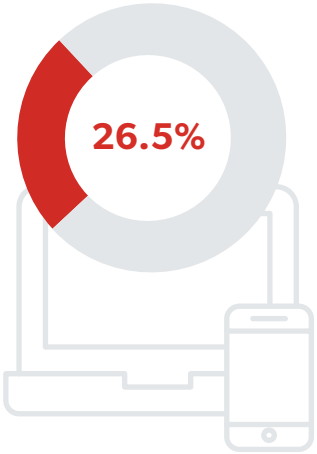


google.com	live.com
amazon.com	facebook.com
microsoftonline.com	linkedin.com
salesforce.com	paypal.com
slack.com	twitter.com
dropbox.com	apple.com
adobe.com	godaddy.com
adp.com	mailchimp.com
intuit.com	netflix.com
atlassian.com	chase.com
atlassian.net	yahoo.com
github.com	americanexpress.com
zendesk.com	instagram.com
trello.com	box.com
	verizonwireless.com
	ebay.com

Truth #8:

Not enough businesses are using multi-factor authentication, yet.

Companies that are taking advantage of the extra protection offered by MFA



26.5% of businesses have enabled multi-factor authentication to protect their password vaults. While we're seeing that a significant portion of businesses are investing in multi-factor authentication, it is not yet adopted widely enough to compensate for the shortcomings of passwords.

We expect to see growing adoption of multi-factor authentication solutions, with a particular emphasis on those that leverage technology already in use, like employee smartphones. In doing so, IT does not have to invest in additional devices or expensive, lengthy deployments of new services. As multi-factor authentication goes mainstream for consumers, we also expect employees to drive the adoption of their preferred authentication solutions in the workplace.

However, multi-factor authentication doesn't solve all of your password security challenges. Unless multi-factor authentication is enabled for every single login in use across the organization (including all 191 in use by the average employee), passwords are often still a low-barrier, high-value target for attackers looking to find a way in. Though multi-factor authentication will compensate for a weaker password, every password should be unique and as strong as possible to slow down or even deter attacks.

Conclusion:
Build a better framework for password visibility and control.

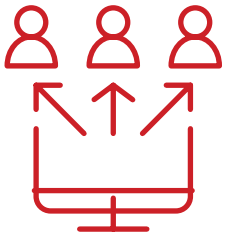
It's time for IT leadership to think about passwords differently. Password management solutions provide that essential "net" that IT can leverage to measure and address password hygiene across the organization, even as they build out a comprehensive Identity and Access Management (IAM) strategy.

Solving the password problem impacts security, productivity, and even employee satisfaction in the workplace. The organizations that can rapidly and effectively address that challenge are well-positioned to keep their business safe while building an innovative workforce.

Solving the password problem with a password manager.

A password manager provides businesses with the insights they need to truly protect their company's information, while removing password obstacles for their employees. We recommend the following:

Deploy a business password manager.
The right solution helps achieve best practices, including:



- Randomizing every password for every account.
- Rotating passwords when appropriate.
- Applying role-based permissions to passwords.
- Achieving proper oversight and accountability for shared credentials.
- Adding protection with multi-factor authentication wherever possible.
- Decommissioning employee credentials after they leave or change roles.

Create a security policy that aligns with the password manager. Communicate policies and best practices to all employees, including how and why to use the password manager. Once integrated into their workflow, they won't know how to live without it!

Solving the password problem with a password manager.

Leverage password management to augment an SSO solution. A password manager captures new and updated account credentials in real time, and facilitates secure sharing of those credentials. An SSO solution, in comparison, allows IT to reduce the number of passwords in use across the organization, but requires more investment of IT time and resources to execute. A password manager helps IT identify and prioritize the services that should be managed and deployed through an SSO solution, without preventing employees from using their apps of choice in the meantime.

Embracing a new approach to password security benefits employees, IT departments, and the company as a whole. With a solution to ensure passwords are randomized and properly stored, the growth of apps in the workplace is no longer a threat, but an opportunity. By embracing emerging technology, businesses can go beyond the constraints of their internal expertise and resources to build faster, create better, and achieve more.

Learn more: www.lastpass.com/business

LastPass •••|

11.1.2017/BX00299/PDF