Are weak passwords putting your company at risk of a breach?

Your employees are sacrificing password security for convenience, but you cannot. People naturally default to simple passwords because they have too many to remember, but it only takes one weak password to put your company at risk.

LastPass ••• | by LogMeIn

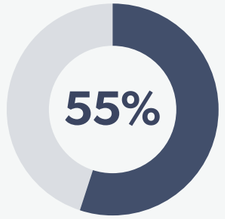
When employees manage their own password security:

Passwords are the weak link.

81% of confirmed breaches are due to weak, reused or stolen passwords.[1]

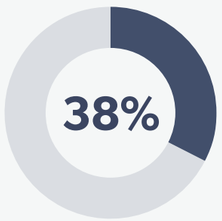
If employees have too many passwords to remember or have to change them frequently, they are going to take shortcuts like writing credentials in notebooks and sticky notes.

Passwords are used over and over again.



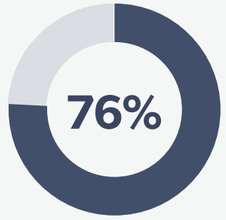
55% of people reuse passwords despite understanding the risks.[2]

Passwords are stored insecurely.

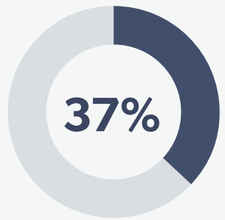


38% of people keep passwords in a file on their computer, mobile device or handwritten notes.[3]

Onboarding is disjointed, messy and time-consuming.



76% of employees experience regular (at least once per month) password usage problems.[4]

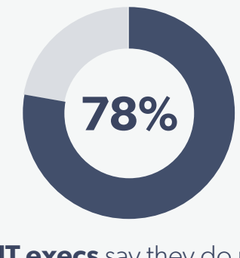


37% of people forget a password at least once a week.[5] This is a lot of work for IT and leads to employees taking shortcuts that sacrifice security.

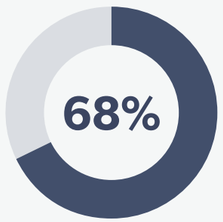
Management lacks control over cloud apps.

Employee training is not enough.

61% of IT executives rely exclusively on employee education to enforce strong passwords.[6]



78% of IT execs say they do not have complete control over cloud apps used by employees.[7]



68% of IT execs acknowledged that this lack of control opens them to significant risk.[7]

Even with the best training and policies enforcing strong passwords, employees can’t possibly remember all 191 passwords the average person uses.[8]

Don’t believe us? Here’s what happens when passwords aren’t managed.

Target

Target experienced a landmark breach in 2013, in which hackers gained access to some 40 million credit cards and jeopardized the personal information of as many as 70 million consumers. The security consultants who investigated the weaknesses within Target’s IT systems found that 86% of the 547,470 passwords used by Target employees could be cracked within one week. Target had a password policy, but it was not being followed or enforced. The researchers reported that weak, default and reused passwords allowed them to quickly gain domain administrator access – and compromise the entire system. All it took was one weak password to bring the whole system down.

Yahoo

Yahoo experienced a breach in 2014 that became public in 2016, and we’re still reading about the effects today. The hack started with a spear phishing email sent to Yahoo employees, which allowed hackers to steal employee credentials. Once inside the system, they stole a copy of Yahoo’s user database containing names, phone numbers, password recovery emails and more. The hack impacted 3 billion accounts[9], and in March 2017, the FBI indicted four people for the attack, including two Russian spies.[10]

What happens when you deploy a password manager to your entire organization?

Strong passwords are the norm.

Every employee has an automated password generator and a vault to store those complex passwords.

The dangers of phishing are greatly reduced.

Employees only have the level of access appropriate to their role, and no passwords are reused, making it substantially harder for an attacker to gain access.

Departed employees are removed immediately.

Offboarding is automated and password changes can be performed instantly behind the scenes without disrupting the work of other employees.

Management can immediately detect employees who are at risk and take action.

Centralized reporting and management features give insight into password behavior at the employee level.

Onboarding is automated and easy.

A new employee can simply be added to the central access management solution and all the logins he or she needs are automatically deployed to start the job on day one.

Employee cyber security training becomes actionable.

Now employees have a set of tools that help them practice good security every day, with no extra effort or impact on their productivity.

Passwords are never reused.

It's easy to use a different password for every account when every password is remembered and entered for them.

Compliance is a reality and not just a checkbox.

With a password system in place, you have data that shows that you've mitigated risk at every level of the organization and truly protected your company.

Passwords are never left out in the open or shared unencrypted.

It's quick and easy for employees to share logins with other team members via their password vault.

Better security starts with passwords.

Don’t let weak passwords make you a breach target. With LastPass Enterprise you can arm your employees with an easy-to-use solution to eliminate weak and reused passwords.

For more than 33,000 businesses of all sizes, LastPass simplifies password security through centralized control for IT, while removing password obstacles for employees. With the same experience loved and trusted by more than 13 million people worldwide, LastPass Enterprise reduces the risk of breach, while delivering the convenient log-in experience employees want.

Features to keep your company safe

Centralized User Management: The admin dashboard offers automated user management, policies and more that busy IT admins need.

100+ Security Policies: Enforce best practices and control password behavior across the business.

Secure Password Sharing: Give teams a flexible, safe way to share access to apps without sacrificing accountability or security.

User Directory Integrations: Automate onboarding and offboarding, group management and more with AD, Azure AD, OneLogin, Okta or a custom API.

Detailed Security Reports: Tie actions to individuals with automated, detailed reporting that helps your business maintain compliance.

Multi-Factor Authentication: Augment security for LastPass accounts with LastPass Authenticator, a leading multi-factor authentication solution with one-tap verification.

1. Verizon 2017 Data Breach Investigations Report (DBIR): http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
2. LastPass Psychology of the Password Report 2016: http://prod.cdata.app.sprinklr.com/DAM/434/LastPass_ExecutiveSummary_fina-88e8a5a2-00cb-4a09-b363-e01a45f829d6-1389898992.pdf
3. ibid.
4. Ovum Report: Closing the Password Security Gap: https://blog.lastpass.com/2017/10/research-closing-password-security-gap.html/
5. Intel Security Poll 2016: buzzfeed.com/josephbernstein/survey-says-people-have-way-too-many-passwords-to-remember?utm_term=.dud82LVQa#.ee4Bv0pXE
6. Ovum Report: Closing the Password Security Gap: https://blog.lastpass.com/2017/10/research-closing-password-security-gap.html/
7. ibid.
8. LastPass Password Expose: https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose.html/
9. http://www.chicagotribune.com/business/ct-biz-yahoo-breach-3b-accounts-20171003-story.html
10. https://www.csoonline.com/article/3180762/data-breach/inside-the-russian-hack-of-yahoo-how-they-did-it.html

3.13.18/BX00683/PDF