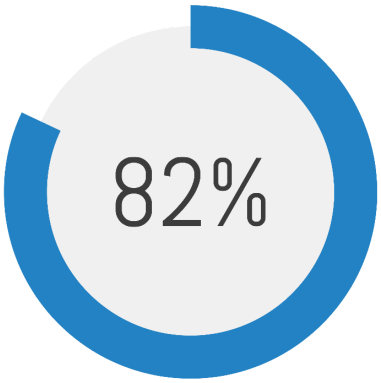
1Password

Protect What Matters: 1Password for Every Corner of the Organization

Business data has never been more valuable or more vulnerable. Faster development, countless apps, smart devices - new security gaps are being created each day, putting critical data at risk. The shift to remote work has accelerated this transformation, with distributed end points and less oversight into security protocols and employee behaviors.



With 82% of breaches involving a human element – adding a password manager to each employee's set of company tools is a necessary part of any security strategy.

All it takes is a slight human error - that is, weak or reused passwords. A single entry point can give a cyber criminal access to the most sensitive data.

Improved security

- 1Password keeps your business secure by making it easy for **everyone** to use strong, unique passwords. It gives departments a secure and convenient way to share those passwords, and helps keep track of accounts and secrets – even if someone leaves the business unexpectedly.

Build a culture of security

- Security should be a team effort - with **every single employee** involved. That's the essence of a "culture of security." By nurturing this mindset, there will be benefits across the organization. Not only will it protect the business and its customers, but also increase overall productivity by letting employees work the way they need to work - while staying secure in the process.

Increase productivity

- Save time by autofilling work logins. Companies that adopt a password manager **save over 1,400 employee hours per year** that would have been spent typing out credentials or waiting for password resets*.

** Information from Forrester's Total Economic Impact™ (TEI) report.*

1Password

Protect What Matters: 1Password for Every Corner of the Organization

Security leaders currently feel their organization lacks sufficient protection against cyberattacks. There's a central theme: Everyone outside of IT thinks security is just an IT problem, and IT thinks it's an "everyone else" problem. The truth is, both are right.

Perception	Reality
Employees are creating strong passwords.	**45% of U.S. adults** use weak passwords (8 characters or fewer.)
Company security guidelines are being followed.	**70% of U.S. workers** think it falls on the company to protect work accounts.
Employees aren't using software not installed by IT.	**63.5% of U.S. workers** have created at least one account that IT doesn't know about (aka shadow IT).
Access management tools (SSO, MFA) cover all the bases.	**33% of those who created shadow IT** accounts reused memorable passwords.

91% of workers understand the risk of password reuse...

but 66% admit to doing it anyway.

This shows the core problem, in a vacuum:
Proper security risk management requires everyone at a company to do their small part, but they likely aren't - because they don't have the tools or guidance.