2021

Password Decisions Survey

IT decision makers shed light on enterprise password management

Brought to you by

bitwarden

About the survey

In December 2020, Bitwarden partnered with Propeller Insights to poll 405 independent U.S.-based IT decision makers across a wide range of industries, who play a key role in enterprise purchasing decisions.

The findings illustrate 3 big themes:

- Employees want their employers to make decisions for them, specifically to mandate the use of an enterprise-wide password manager
- Even IT decision makers struggle with adhering to security best practices at work
- IT decision makers favor two-factor authentication for its effectiveness and versatility

Respondent Demographics

46%
Director within their organization

35%
C-level Executive

49%
Age 35-44

80%
Sole decision maker

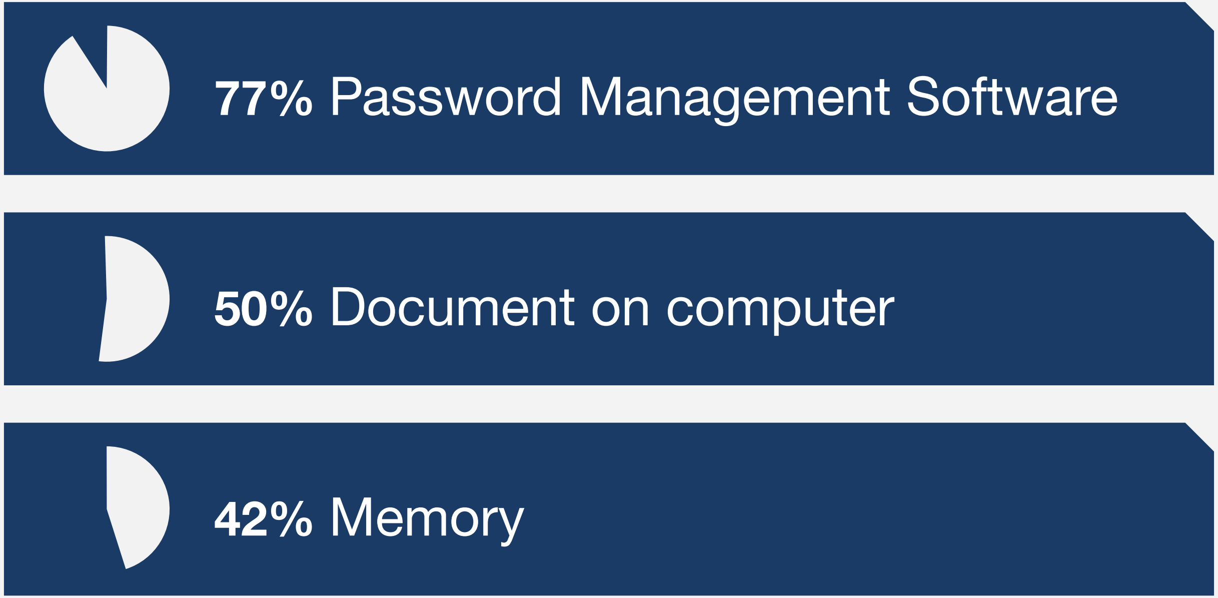
Industries

24%	Information Technology
20%	Science / Tech
11%	Manufacturing
7%	Finance / Insurance

Password practices at work

IT decision makers see value in password managers

How do you manage passwords for websites, apps, and services at work?



77% Password Management Software

50% Document on computer

42% Memory

77% of respondents choose to use a password manager whether their company mandates them or not. However, respondents are still saving passwords using unsecure methods, such as documents and notepads.

Employers are prioritizing password security

77%

of employers

require employees to use an enterprise-wide password manager

80% want mandated password practices

IT decision makers want their employer to mandate use of an enterprise-wide password manager

It leaders identify the usefulness and effectiveness of password managers, but need help from their organizations to implement company-wide rollouts and emphasize the importance of keeping data secure.

Potential reluctance to using a password manager

50%

Lack of motivation or time

44%

Cost

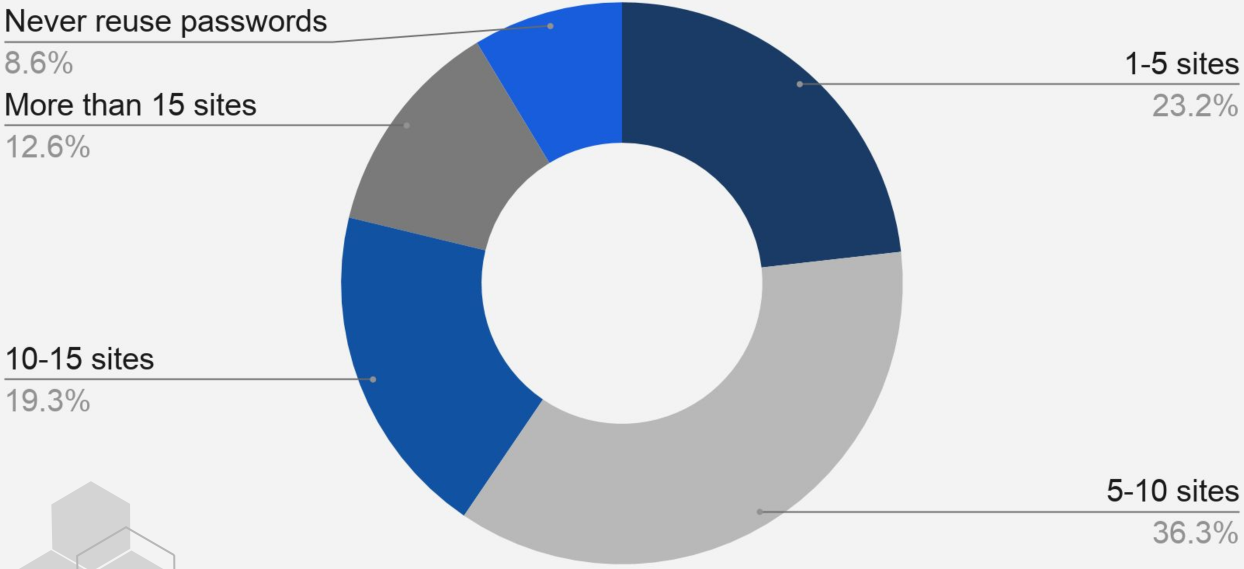
35%

Not always easy to use

IT decision makers cite the top three reasons people may be reluctant to use a password manager.

While time constraints are understable, recovering from a data breach or identity theft is much more time-consuming.

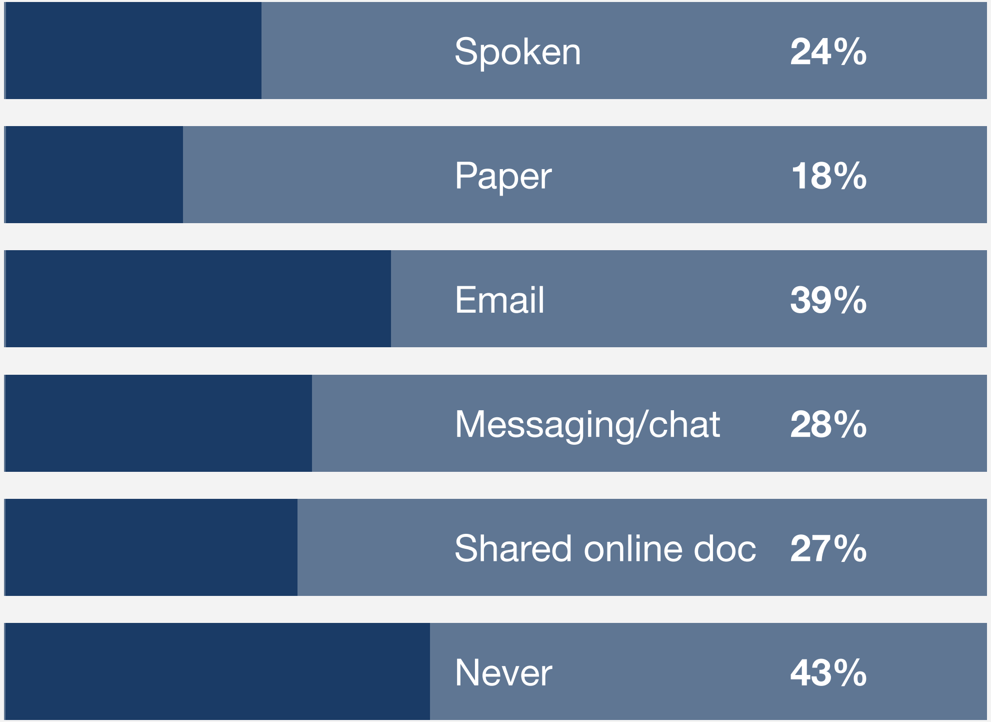
Password reuse unfortunately continues



Many studies have shed light on the risky consumer habit of reusing passwords.

Unfortunately, this also extends to IT pros. Only 8.6% say they never reuse passwords.

Methods of sharing passwords within teams



Despite knowing the risks, many IT decision makers say they share company passwords with colleagues through unsecure methods.

Top 3 attributes of a good **password manager:**

67% Security (strong encryption and subject to 3rd-party audits)

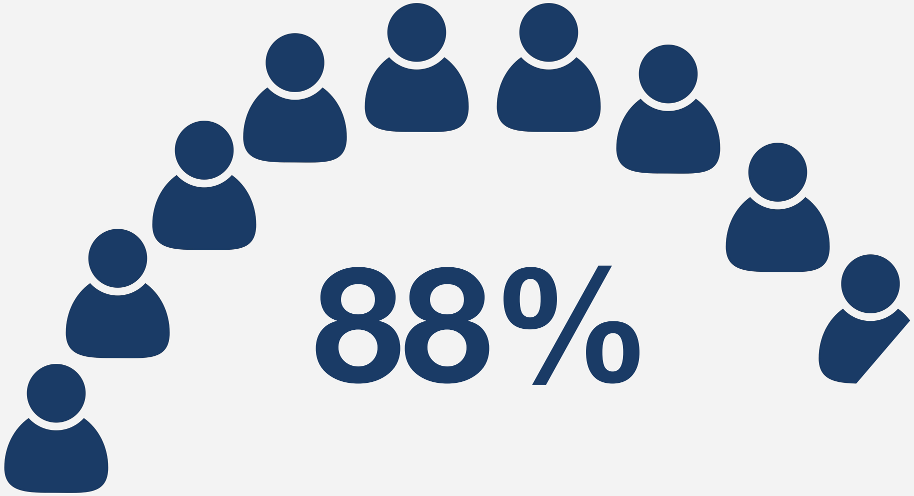
55% Ease of use

53% Operates across many devices and platforms

Technologies in use

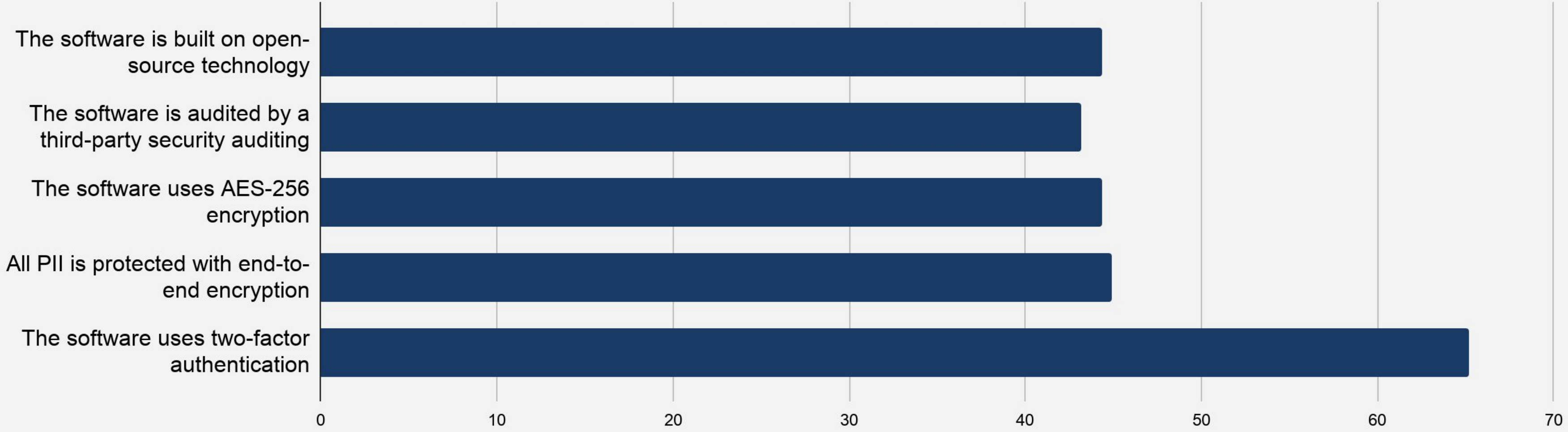
2FA remains pervasive in the workplace

Among IT decision makers, 88% claim two-factor authentication use in the workplace, highlighting adoption of the approach across consumer and business applications.



Two-factor authentication fosters confidence

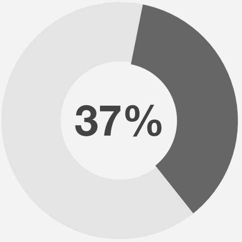
Which of the below measures would make you confident the software you're using is secure? Please select all that apply.



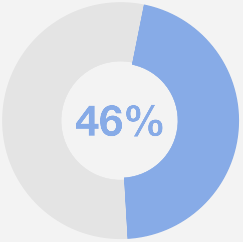
© Bitwarden 2021 Password Decisions Survey

Potential reluctance to using two-factor authentication

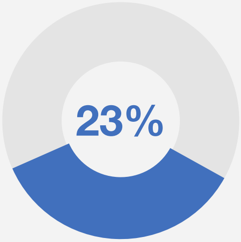
But IT decision makers cite lack of motivation, time, and education as to why general consumers may be reluctant to implement.



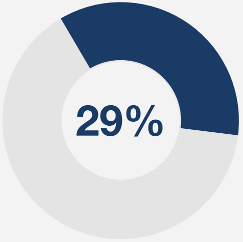
It slows down workflow



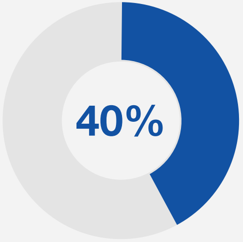
Lack of motivation/time to implement



I don't think 2FA is necessary my password is strong enough

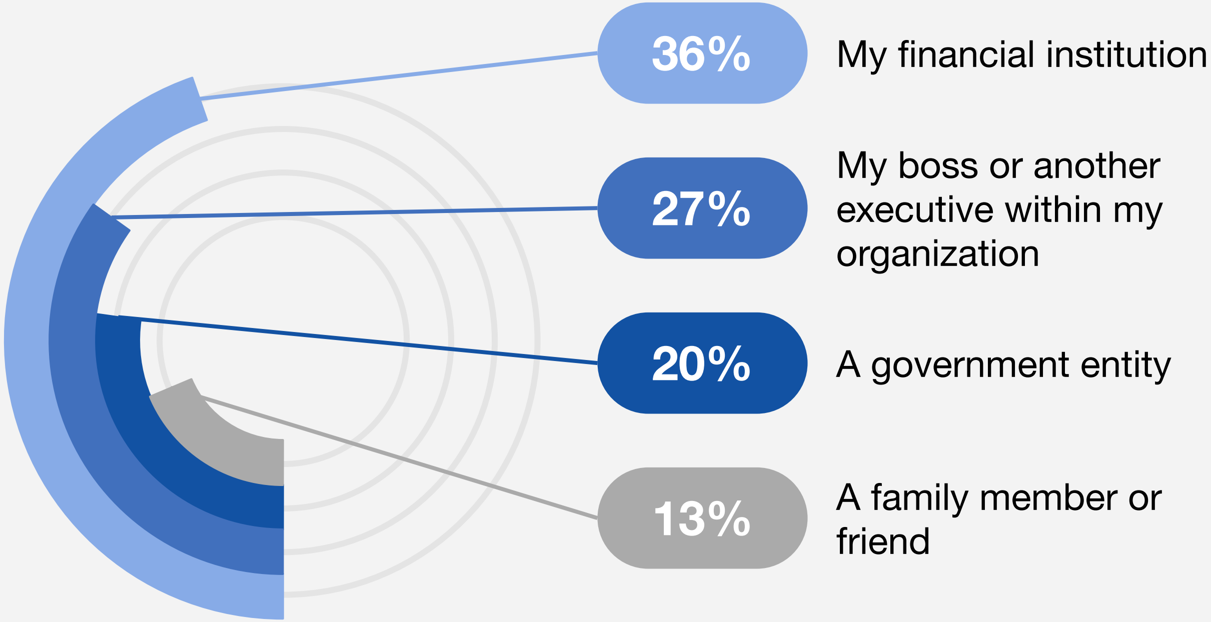


Overall I think it is very unlikely my password will get hacked



I don't think people are aware of the benefits of 2FA

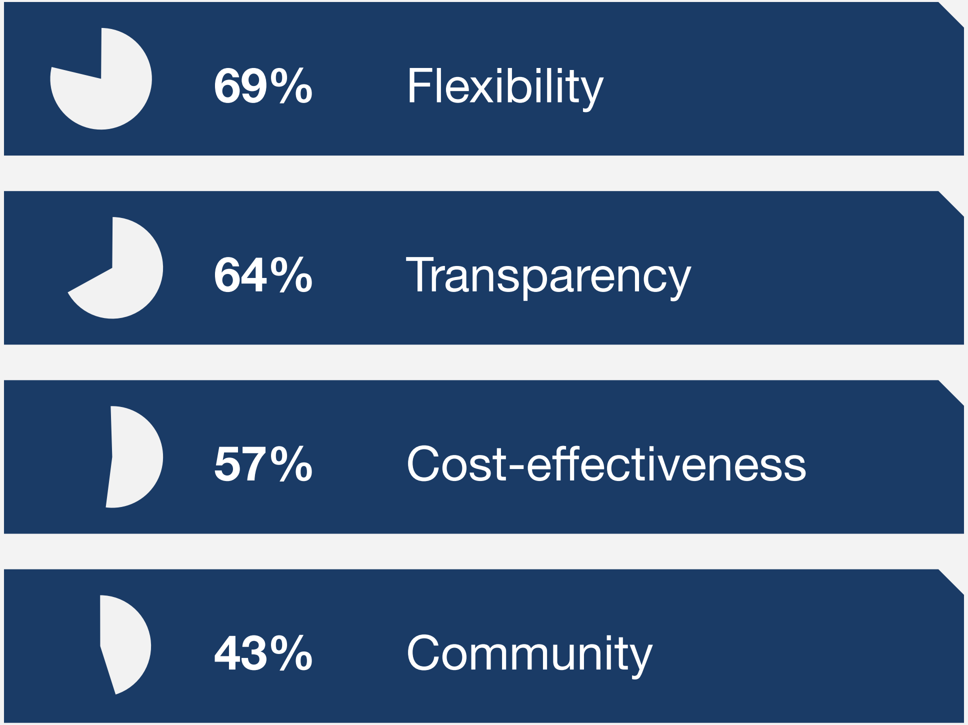
Phishing attempts are on the rise



It leaders report that recent attacks appeared to come from a financial institution or executive within their organization.

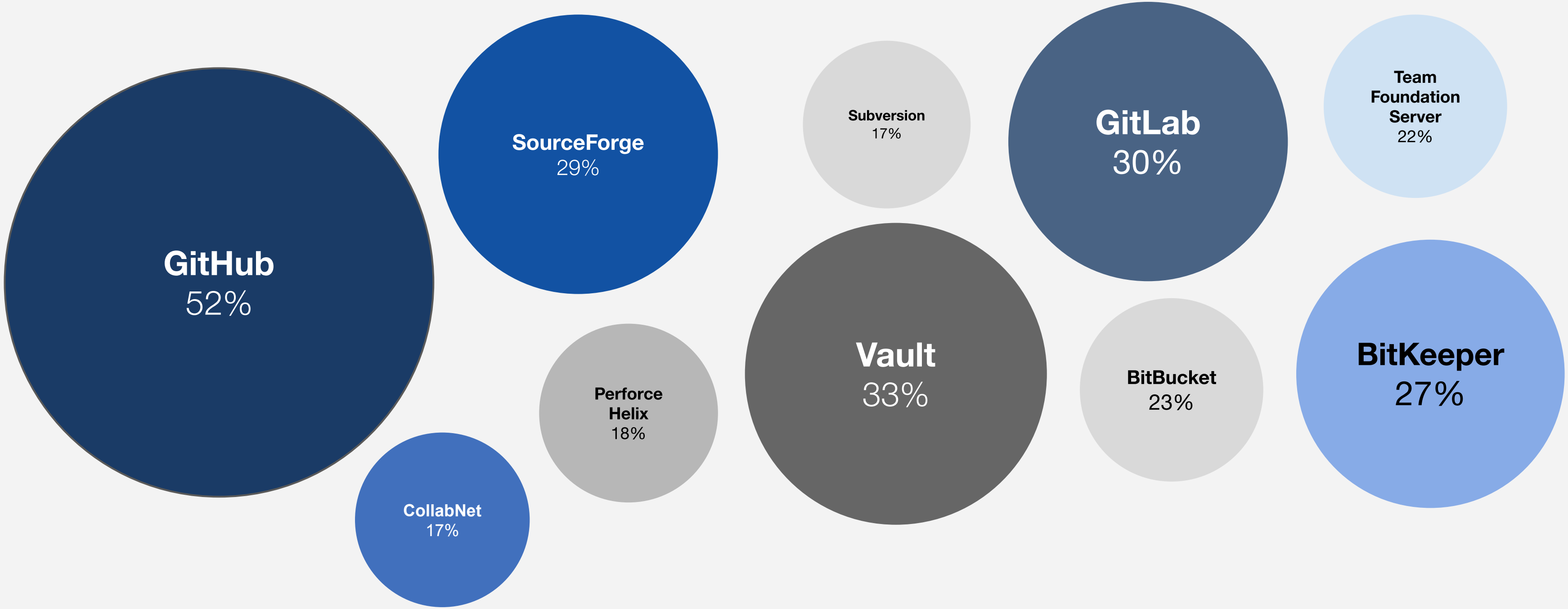
Combating these attacks is possible with the right strategies, which should include 2FA.

Leading benefits of using open-source technology



69%	Flexibility
64%	Transparency
57%	Cost-effectiveness
43%	Community

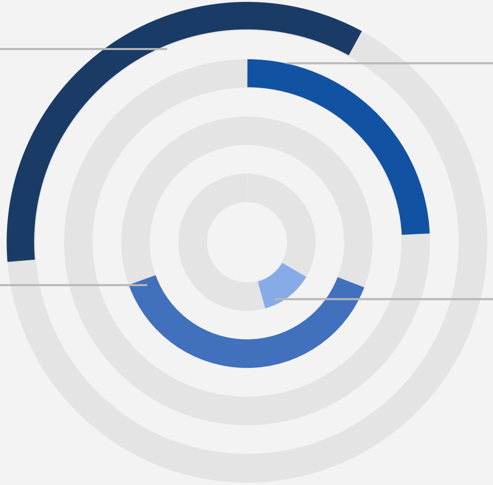
Code repositories used by IT decision makers



Driving confidence in zero-knowledge encryption

Service providers should offer proof of technologies such as IAM, encryption, MFA, and permissions to demonstrate zero-knowledge encryption

What would compel you to believe a service provider is actually utilizing zero-knowledge encryption?



32%

They say they are operating on the zero-knowledge principle and their word is enough for me

26%

They explain how they've implemented zero-knowledge encryption

37%

They can demonstrate they've implemented technologies such as identity and access management, encryption, multi-factor authentication, and permissions to operate

5%

I'm skeptical service providers who claim to take a zero-knowledge approach are telling the truth

Zero-knowledge benefits align to anonymity

Service provider inability to access client data is the leading benefit of using a zero-knowledge encryption service

What do you consider the biggest advantage of zero-knowledge encryption? Please select all that apply.

52% The service provider can't decrypt any of my data

43% The risk of data breach is negligible

43% I don't have to worry about security of data during transmission

39% The service provider has no incentive to resell my data to other companies

Read more about the

2021 Password Decisions Survey

bitwarden.com/blog/post/password-decisions-survey-2021