# 2022
# Password Decisions Survey

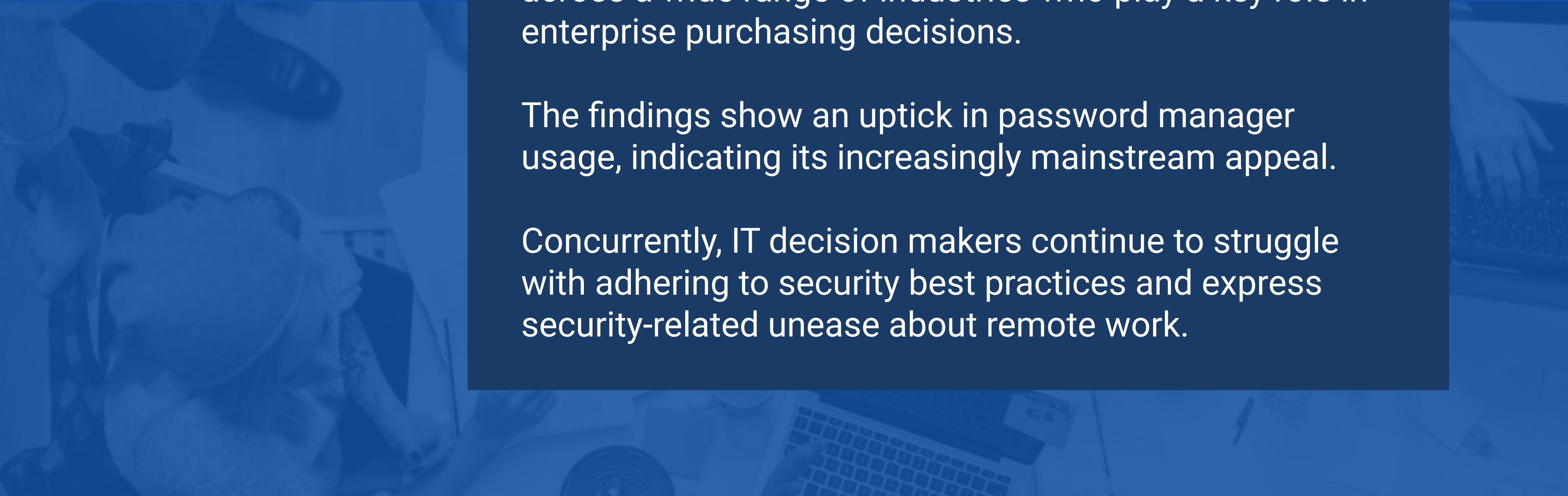
Brought to you by bitwarden

# About the survey

In November 2021, Bitwarden partnered with Propeller Insights to poll over 400 independent IT decision makers across a wide range of industries who play a key role in enterprise purchasing decisions.

The findings show an uptick in password manager usage, indicating its increasingly mainstream appeal.

Concurrently, IT decision makers continue to struggle with adhering to security best practices and express security-related unease about remote work.



# Demographics

**26%**
C-level Executive

**54%**
Director

**83%**
Sole Decision Maker

**48%**
Age 35-44

**26%** Information Technology

**14%** Manufacturing and Production

**12%** Science/Programming/Software

**8%** Health Care

**7%** Finance/Accounting

# Password Practices at Work

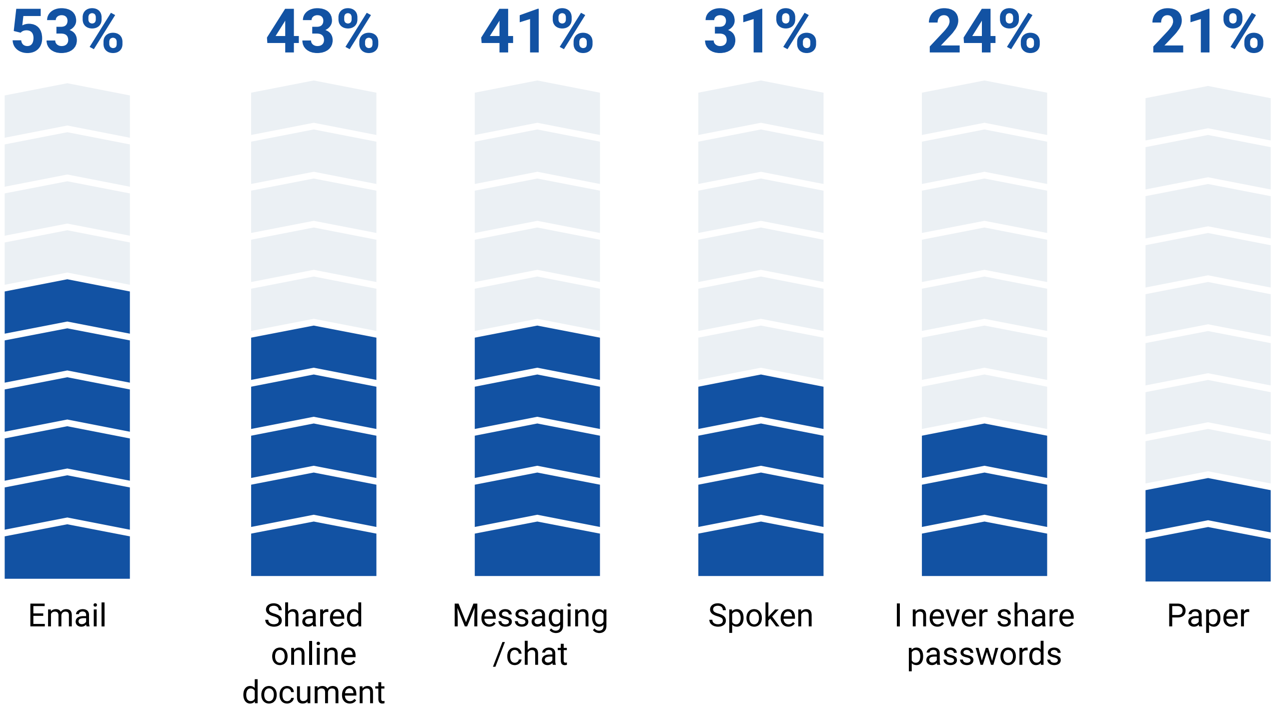
# Strategies for managing passwords

Password managers are on the rise, but risky security practices remain pervasive - such as relying on computer documents and paper.

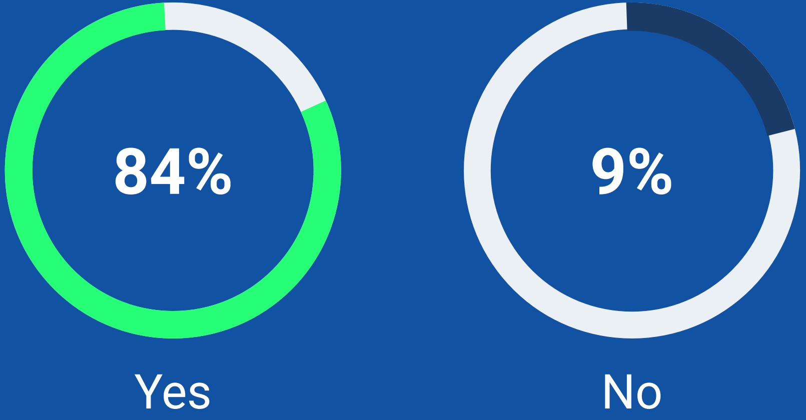
| | |
|---|---|
| Password management software | 86% |
| Document on my computer | 53% |
| My memory | 42% |
| Pen and paper | 29% |

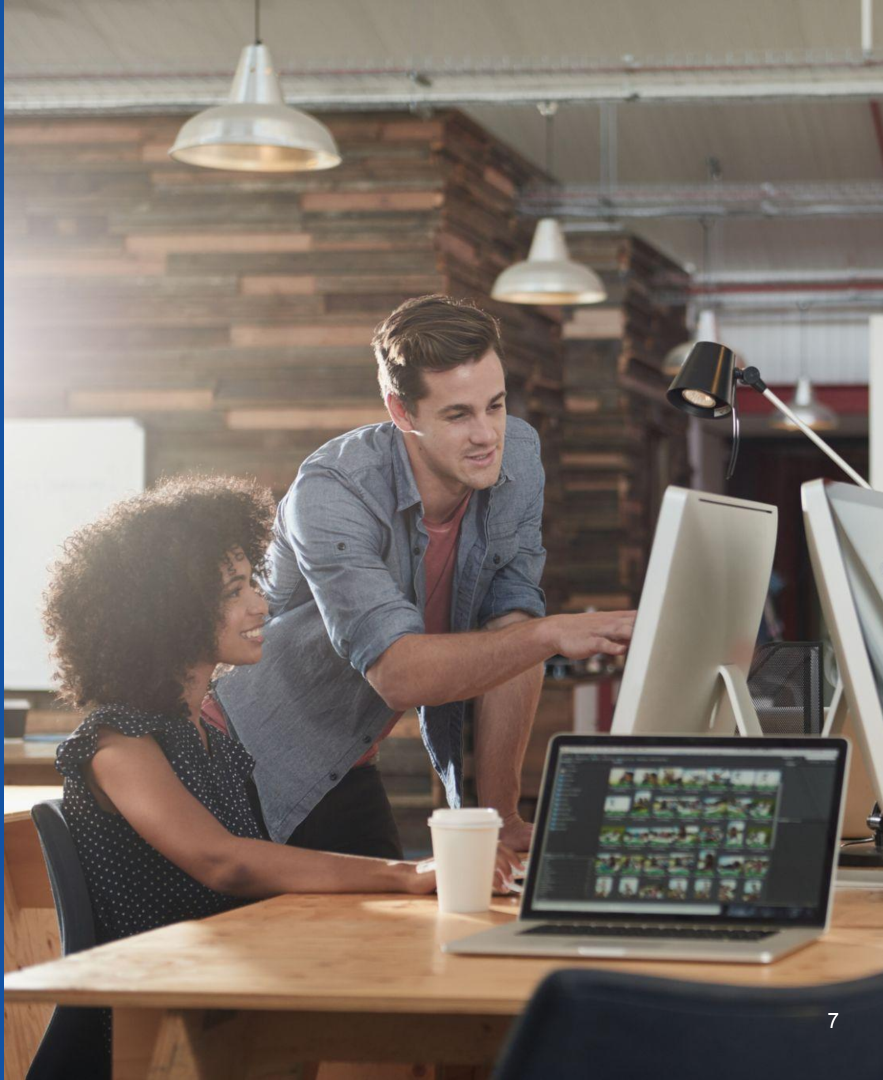
# Password sharing methods

Compared to last year, the number of IT decision makers sharing passwords via email skyrocketed from 39% to 53% due in part to the sudden adjustment to remote work and increased rate of employee turnover.

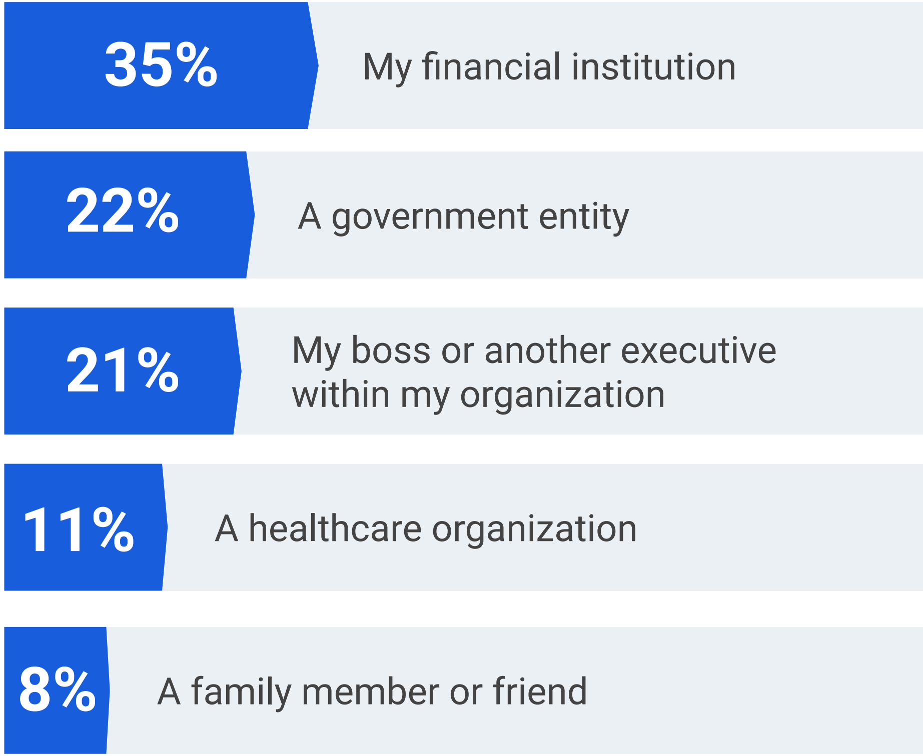


# Most respondents want their employers to require employees to use the same enterprise-wide password manager





# Security Risks and Cyberattacks



## Most represented industries in phishing attacks

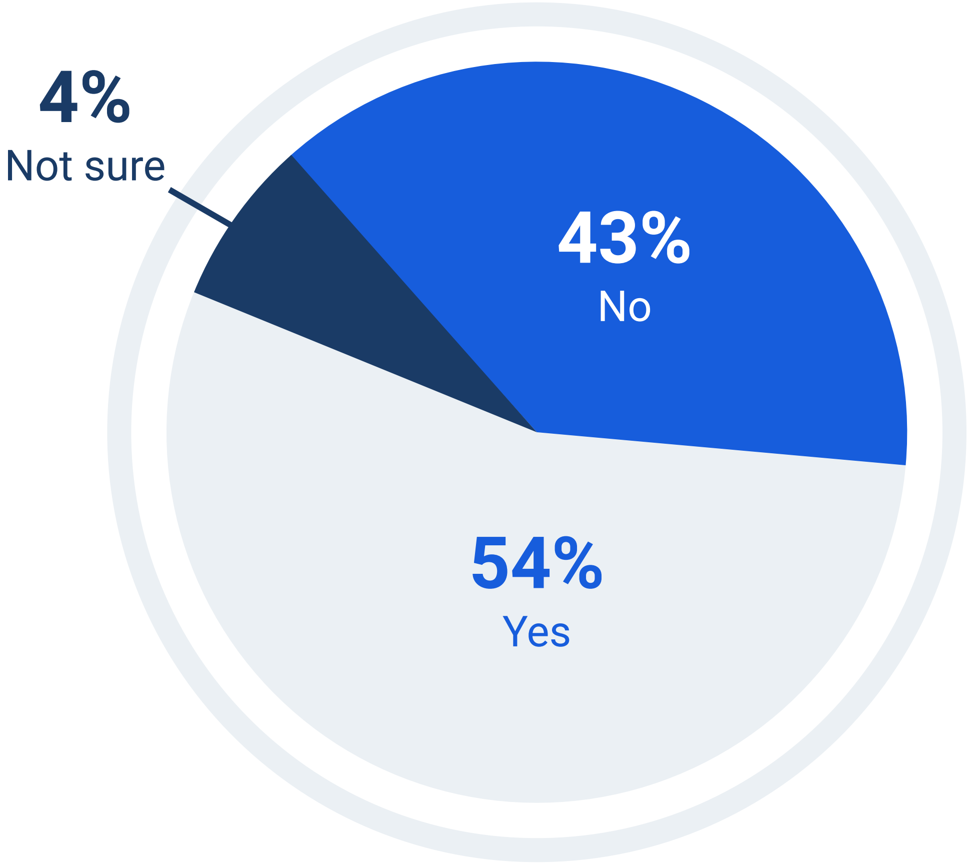
Phishing attacks remain a scourge as criminals hone more sophisticated social engineering tactics.

# Password reuse

Despite a year of high-profile cyberattacks and increasing vulnerabilities posed by remote work, almost all respondents reuse passwords across multiple sites.

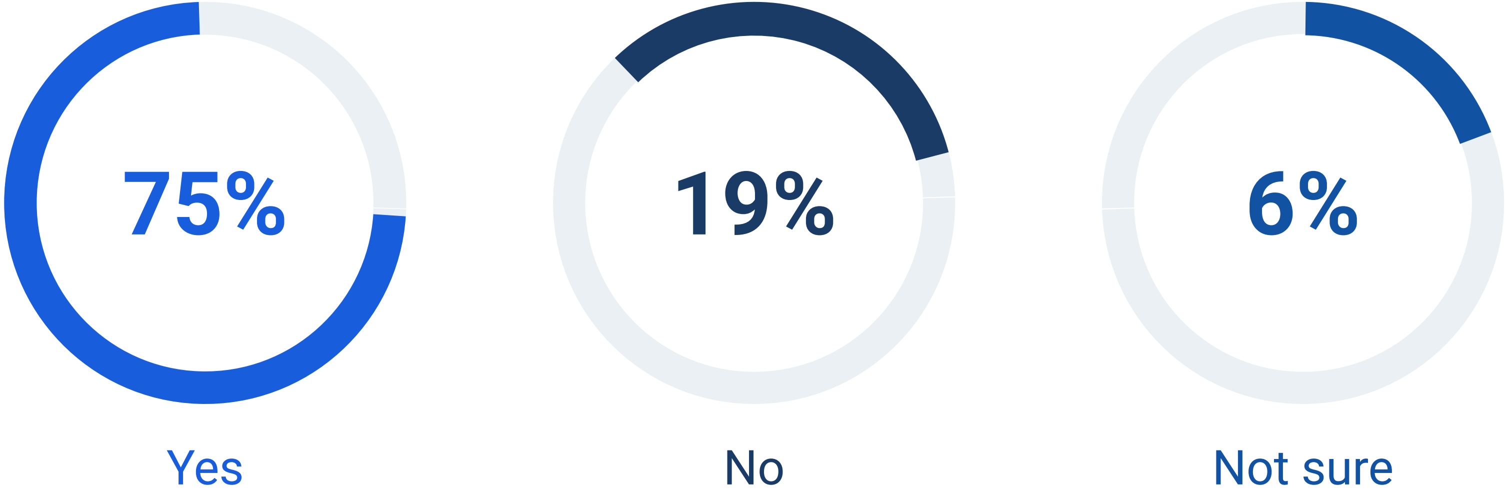
| | |
|---|---|
| More than 15 sites | 15% |
| 10-15 sites | 27% |
| 5-10 sites | 33% |
| 1-5 sites | 16% |
| I never reuse my passwords | 8% |

## More than half of respondents confirmed their organization has experienced a cyber attack



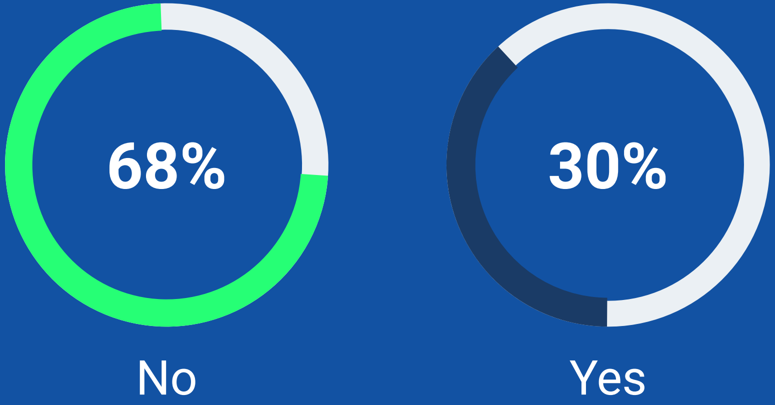
# Do you have a ransomware mitigation strategy?

In spite of recent high-profile breaches, 25% of organizations either don’t have or aren’t sure if they have a ransomware mitigation strategy in place.



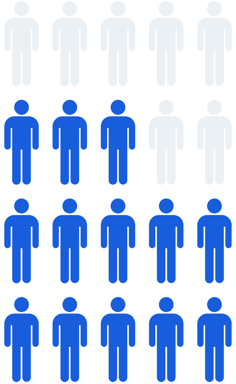
# Both employees AND IT decision makers still resort to using Shadow IT

30% of decision makers find themselves resorting to shadow IT as a workaround



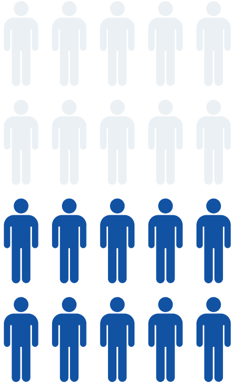
# Why employees resort to shadow IT practices

While some may believe shadow IT helps make their work faster and more efficient, the long-term security impact is potentially ruinous.



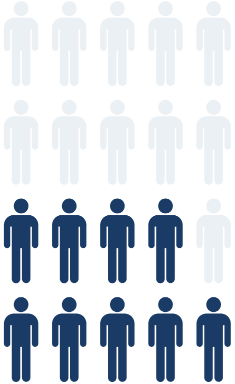
63%

Belief it makes daily activities faster and more efficient



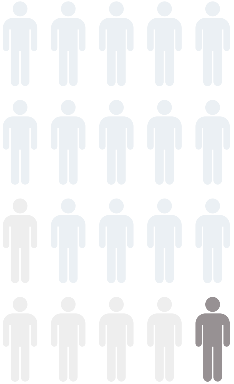
48%

Lack of authorization for certain applications or software



38%

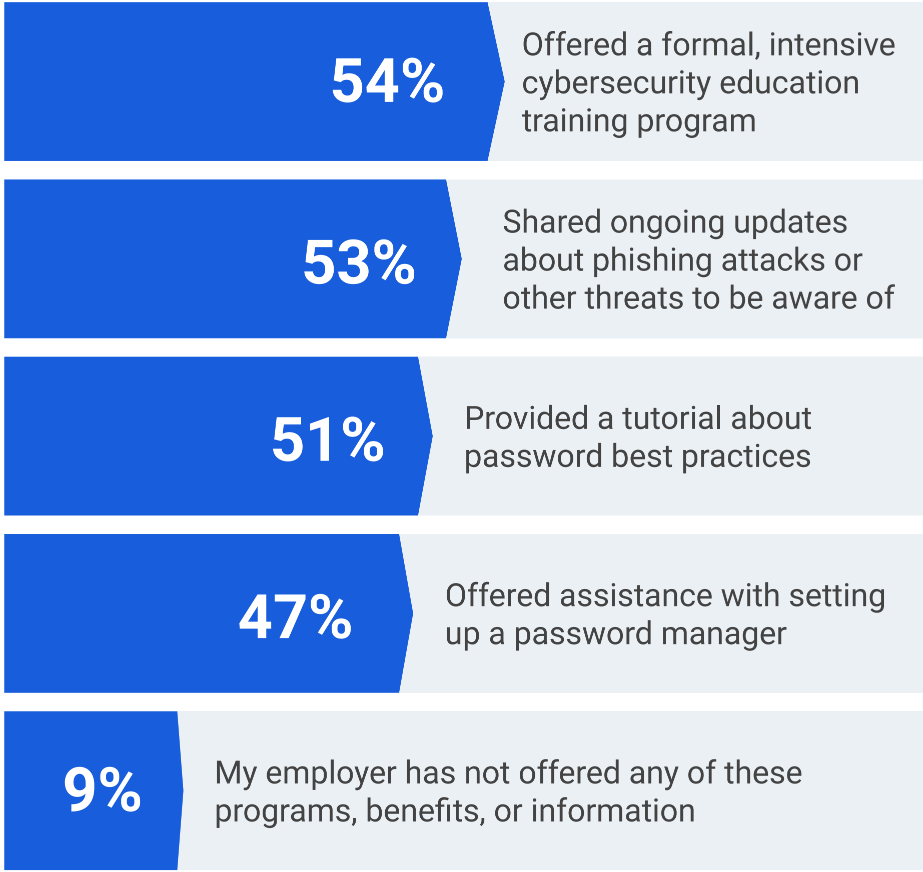
Slow response times from IT



8%

Unsure/don’t know

# Employer-led cybersecurity continuing education

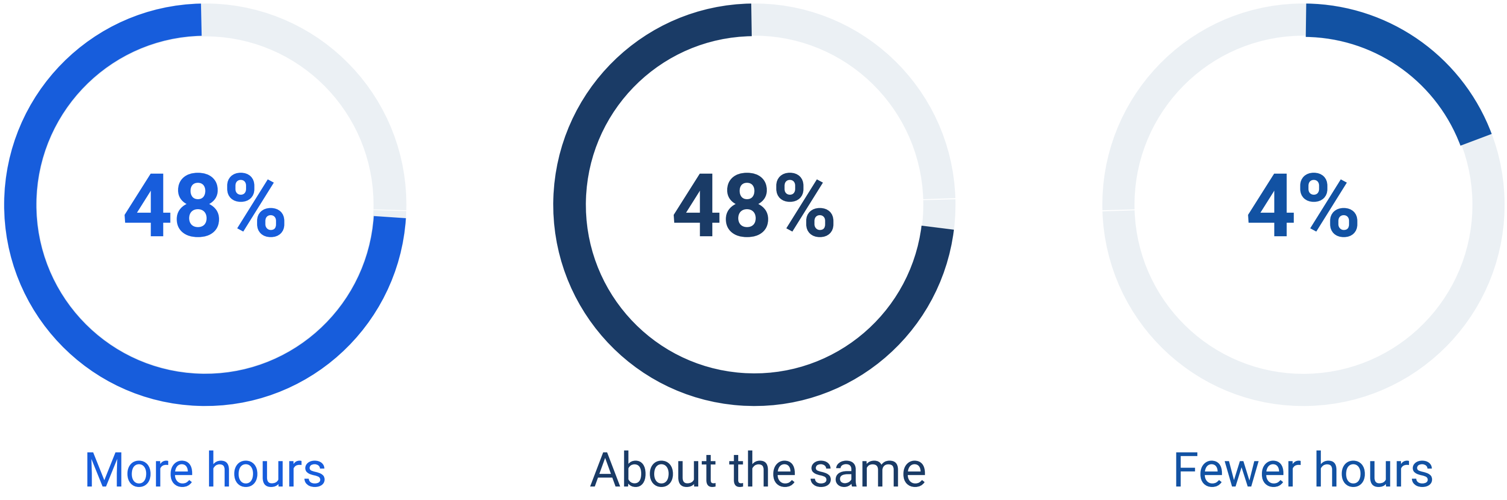


# Remote work and the Great Resignation

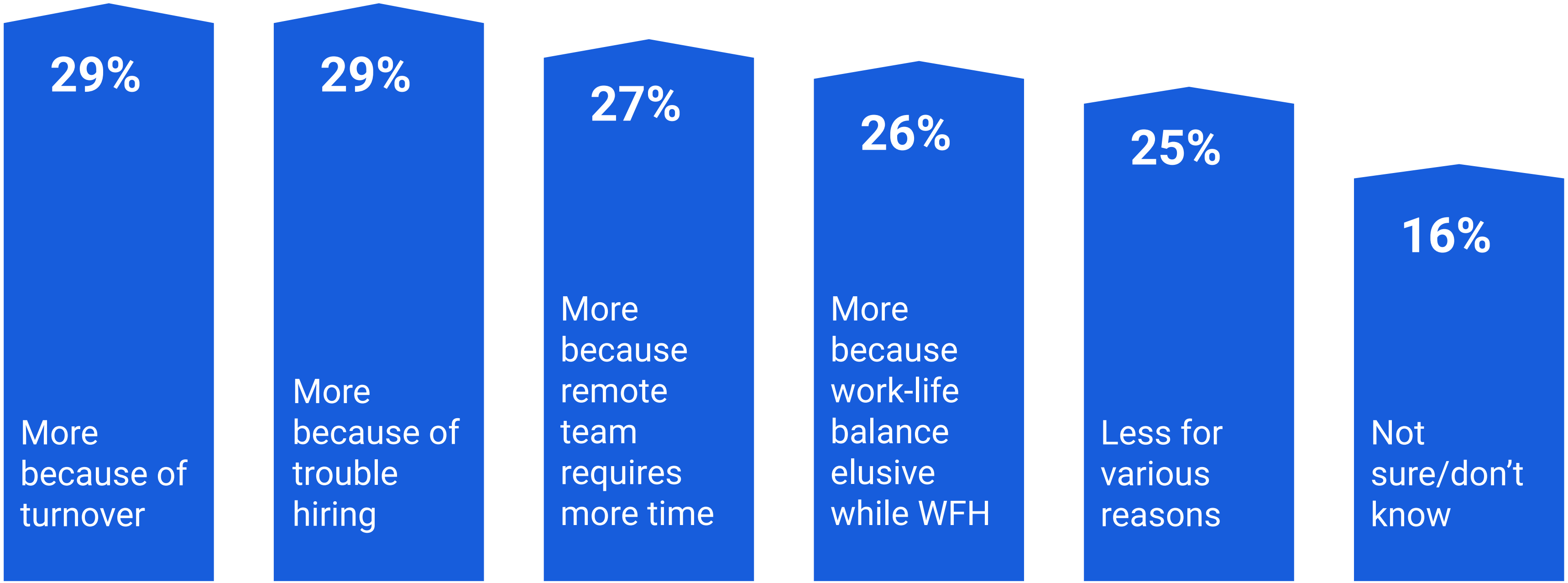
# Rise of remote work has heightened cybersecurity concerns

| | |
|---|---|
| Because remote work may lead to weaker security posture | 61% |
| Because password breaches have led to high-profile cyberattacks | 55% |
| Because turnover is making password management more difficult | 23% |
| No, not more concerned | 9% |

# The Great Resignation hasn't spared the world of IT decision makers with 48% working more hours than last year

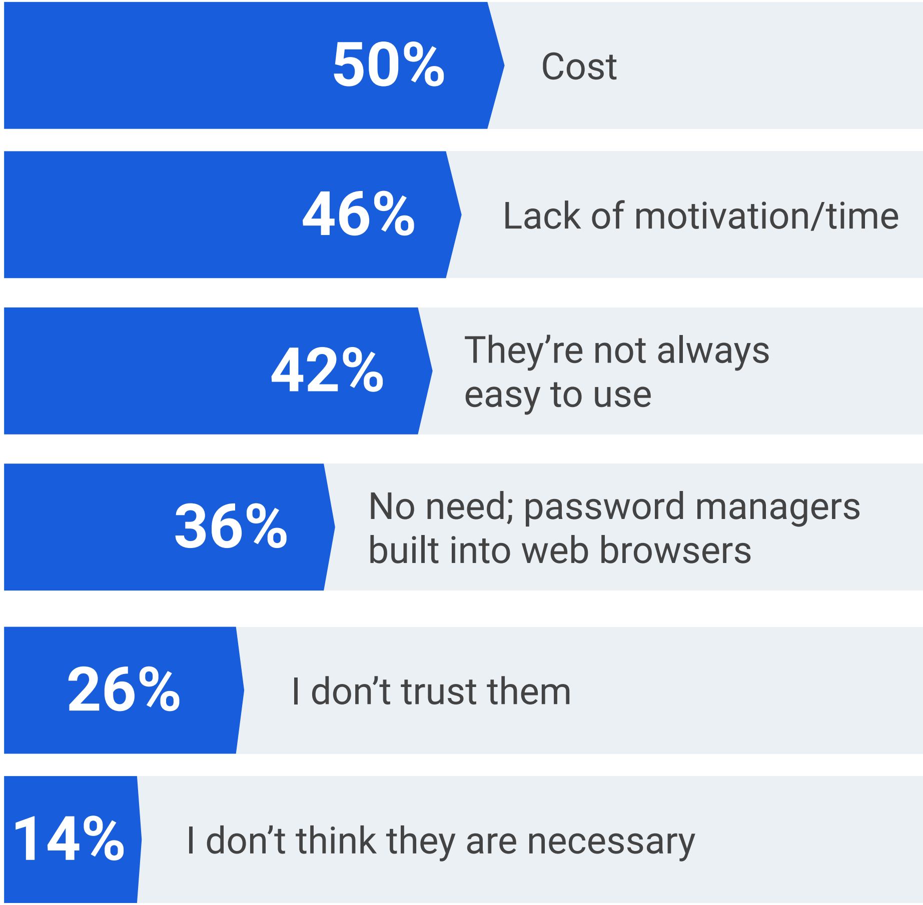


# 58% of IT decision makers are working more hours due to turnover and difficulty hiring

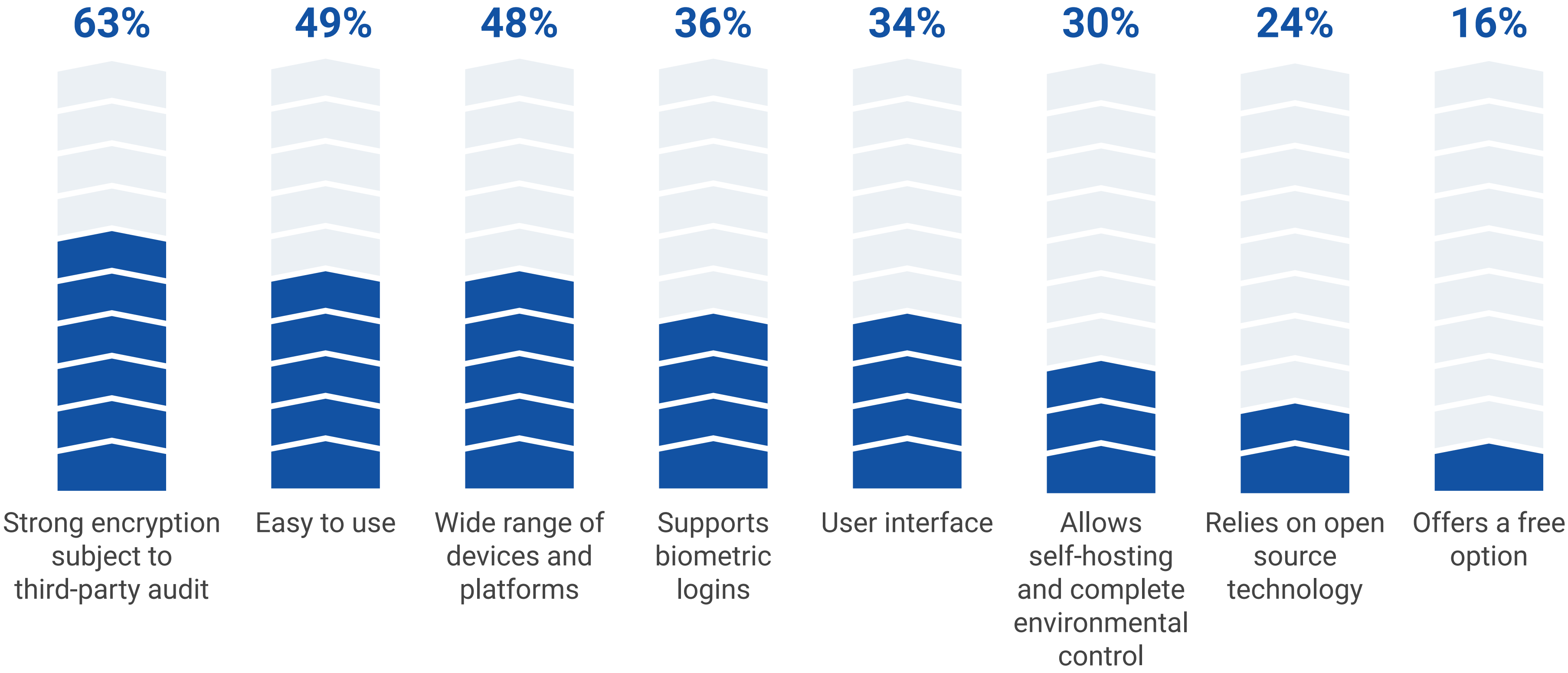


# Technologies in Use

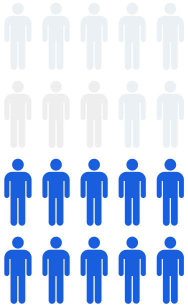
# Perceived barriers to implementing password managers



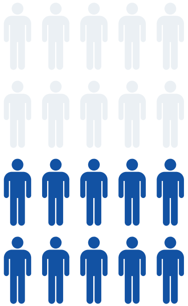
# Top attributes of a good password manager



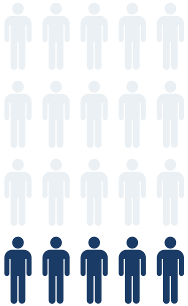
# While 2FA popularity is encouraging, perceptions that it “slows down workflow” and “takes time to implement” drive employees away from embracing it



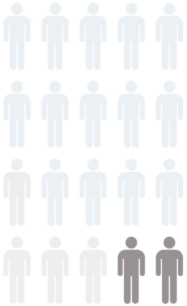
**45%**
It slows down workflow



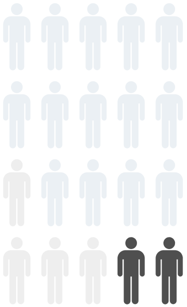
**44%**
Lack of motivation/time to implement



**28%**
Think being hacked is unlikely



**23%**
People aren’t aware of the benefits of 2FA



**21%**
Perception that a password is strong enough

# 2FA has become mainstream

**88%**

of respondents use two-factor authentication in the workplace