Workplace Password Malpractice Report 2021

Exclusive Research Report

Sponsored by Keeper Security

Pollfish

Introduction

Poor password hygiene in the workplace was a threat to organizational cybersecurity even before the COVID-19 pandemic. When COVID-19 forced organizations worldwide to rapidly deploy and secure remote workforces, teams began connecting to organizational resources remotely, in environments that their employers did not control, many times using their own devices.

Respondents to the Ponemon Institute's **Cybersecurity in the Remote Work Era: A Global Risk Report**, commissioned by Keeper Security in 2020, expressed grave concerns over password security in their organizations:

- 60% of respondents said their organizations experienced a cyberattack in the past 12 months.
- Over 50% of these attacks involved stolen credentials.
- The theft of IT assets caused $5 million or more in damages for 25% of businesses.

The pandemic pushed organizations to rapidly deploy a host of new technologies to keep remote employees connected, collaborating, and working. From Zoom to Google Workspace to Slack, employees had to sign up for yet more online accounts — and keep track of yet more passwords.

Keeper wondered how much password security had changed since companies moved to remote work environments. Were remote employees following simple best practices to secure their passwords, or were they falling prey to "password fatigue" and engaging in bad habits that lead to significant cybersecurity risks? Which is why Keeper, in partnership with Pollfish, conducted the Workplace Password Malpractice Survey.

While Ponemon surveyed organizational leaders, we decided to go straight to employees for this survey, and we queried 1,000 full-time workers in the United States about their password habits. The survey was completed in February 2021, and consisted of only individuals who used passwords to log into work-related online accounts.

Following are the most important findings from the survey. The full data can also be viewed on page 5.

Finding 1: U.S. employees are tracking & storing their login credentials insecurely

Our survey found that U.S. employees are not following best practices when storing and tracking their work-related passwords, presenting major cybersecurity risks for their employers.

- Over half of respondents (57%) admit to writing down work-related online passwords on "sticky notes", and two-thirds (67%) admit to having lost these notes. In addition to leaving sensitive corporate information in full view of anyone else living in or visiting their home, this harms organizational efficiency. Lost sticky notes mean lost passwords, which result in help desk tickets to reset said passwords.
- 62% of respondents store login credentials in a notebook or journal, and the overwhelming majority (82%) say that they keep these notebooks next to or close to their work devices, where they can be accessed by anyone else who lives in or is visiting their home.

Using a pen and paper to keep track of passwords has become even more problematic in the remote work world. Most workers (66%) say that they're more likely to write down work-related passwords when working from home than they are while working in the office.

Even when using digital methods to track and store their passwords, U.S. employees are engaging in poor password security practices.

- Nearly half of respondents (49%) save work-related passwords in a document in the cloud.
- Just over half (51%) say that they currently save these passwords in a document saved on their computer.
- 55% save work-related passwords on their phone.

Storing passwords in unencrypted files is extremely risky. All a cybercriminal needs to do is breach the cloud storage, computer, or mobile device, and they can access all of the employee's passwords.

Finding 2: U.S. employees are creating weak, easily guessed passwords

A strong password consists of a random string of uppercase and lowercase letters, numerals, and special characters. However, many respondents admitted to using passwords that contain personal details, which cybercriminals can easily find on social media channels.

- Over one-third (37%) of respondents have used their employer's name in a work-related password.
- Over one-third (34%) have used their significant other's name or birthday.
- Nearly one-third (31%) have used their child's name or birthday.

Password re-usage between personal and work-related accounts has become a big cybersecurity risk for companies, with 44% of respondents admitting to reusing passwords across personal and work-related accounts and 53% admitting to keeping password-protected personal accounts on their work devices.

Finding 3: U.S. employees are sharing work-related passwords with unauthorized parties

Many U.S. employees are not exercising care regarding whom they share their work-related passwords with. This puts organizations at risk of being breached should these passwords wind up in the hands of someone who is careless or who has malicious intentions.

- Over the past year, 14% of respondents have shared their work-related passwords with their significant other or spouse.
- 11% of respondents have shared work-related passwords with another family member.

Even absent a data breach, an employer could be found out of compliance, and assessed very large penalties, if it is discovered that unauthorized parties have viewed compliance-protected data.

Finding 4: U.S. employers are not doing their part to ensure that passwords are being shared securely and/or only with authorized parties

Our survey found that shared passwords in the workplace are common.

- Nearly half of respondents (46%) report that their company shares passwords for accounts that are used by multiple people.
- Over one-third (34%) have shared work-related passwords with colleagues on the same team.
- Nearly one-third (32%) have shared work-related passwords with their managers.
- 19% have shared their passwords with their executive team.

The best thing to do is to give every user a unique password for every work-related account or application, which can be practically done by utilizing the use of an Enterprise Password Management (EPM) platform. Password-sharing in the workplace is safe if the passwords are shared securely, and if passwords are shared only with unauthorized parties. Our survey results indicate that many U.S. employers are not exercising risk mitigation strategies to help ensure safe password-sharing.

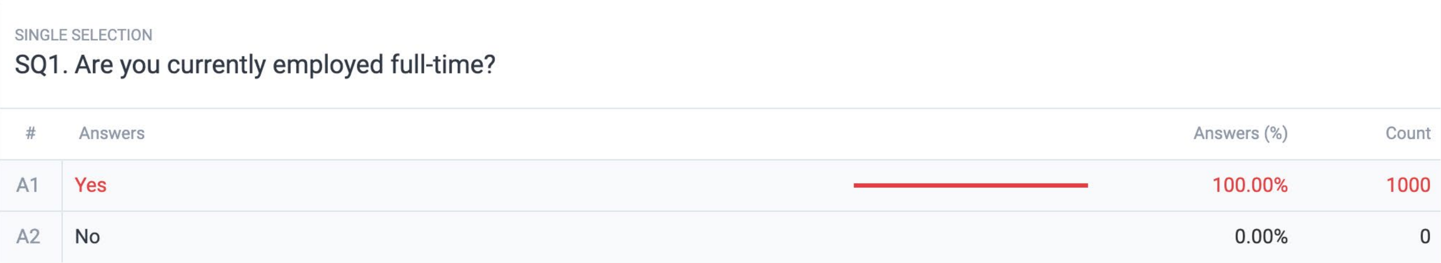
- The majority of respondents (62%) report sharing a work-related password over text message or email, which could be intercepted by cybercriminals in transit.
- Nearly one-third of respondents (32%) admit to accessing an online account belonging to a previous employer, which indicates that many employers are not disabling accounts when employees leave the company.

Conclusion

Adopting and implementing an enterprise password management platform such as Keeper Enterprise would cure the password malpractice uncovered in this survey. Keeper's zero-knowledge password encryption and zero-trust framework provides advanced password management, secure sharing, and other security capabilities. IT administrators and leaders gain complete visibility and control into employee password practices, including:

- Exclusive, proprietary zero-knowledge security model and zero-trust framework system; all data in transit and at rest is encrypted; it cannot be viewed by Keeper Security employees or any outside party.
- Rapid deployment on all devices, with no upfront equipment or installation costs.
- Personalized onboarding and 24/7 support and training from a dedicated support specialist.
- Support for RBAC, 2FA, auditing, event reporting, and multiple compliance standards, including HIPAA, DPA, FINRA, and GDPR.
- Provision secure shared folders, subfolders, and passwords for teams.
- Single Singn-On (SAML 2.0) authentication
- Enable offline vault access when SSO is not available.
- Dynamically provision vaults through SCIM.
- Configure for High Availability (HA).
- Advanced two-factor/multi-factor authentication
- Active Directory and LDP sync
- SCIM and Azure AD provisioning
- Developer APIs for password rotation and backend integration

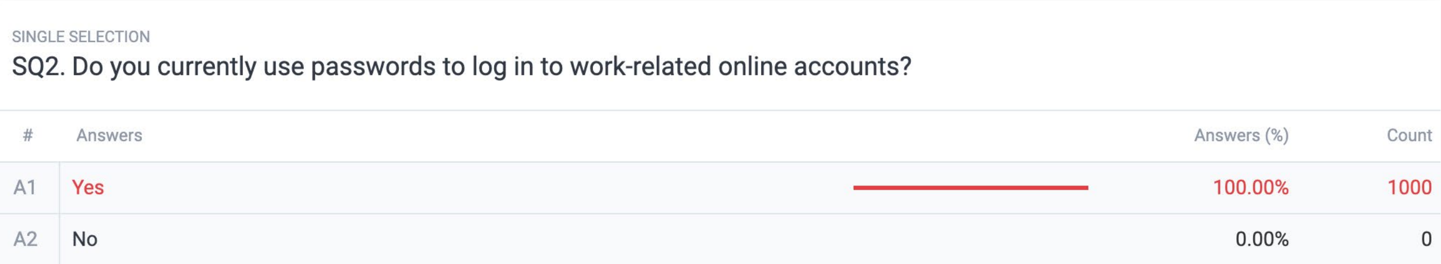
Survey Results



SINGLE SELECTION

SQ1. Are you currently employed full-time?

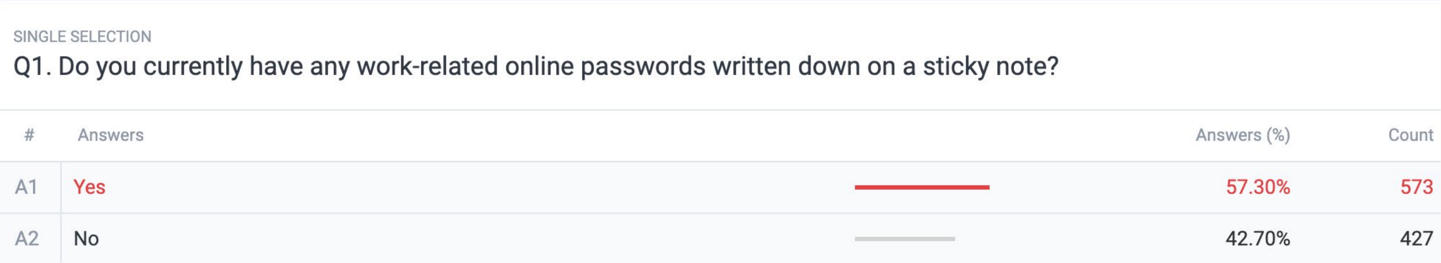
#	Answers	Answers (%)	Count
A1	Yes	100.00%	1000
A2	No	0.00%	0



SINGLE SELECTION

SQ2. Do you currently use passwords to log in to work-related online accounts?

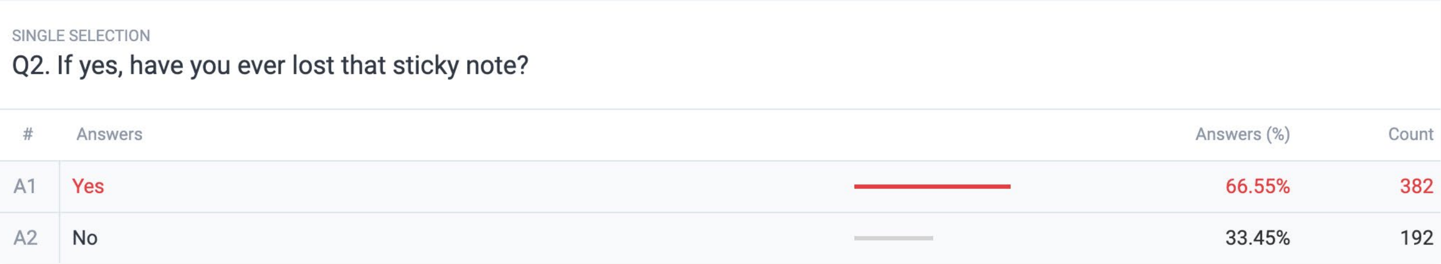
#	Answers	Answers (%)	Count
A1	Yes	100.00%	1000
A2	No	0.00%	0



SINGLE SELECTION

Q1. Do you currently have any work-related online passwords written down on a sticky note?

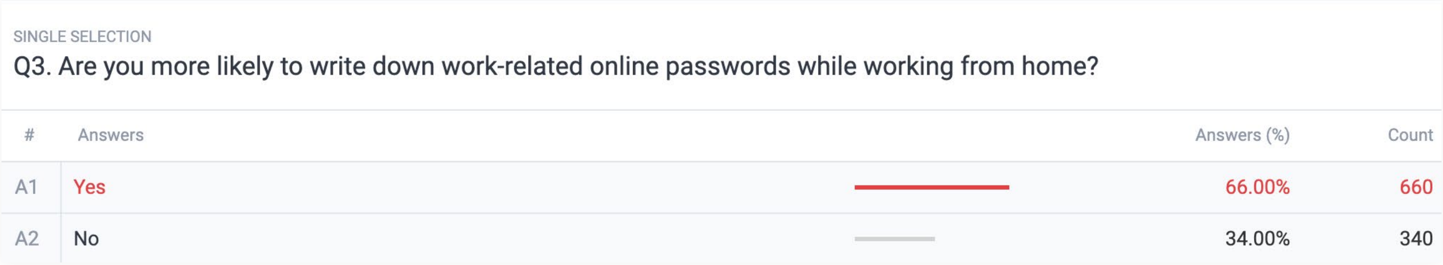
#	Answers	Answers (%)	Count
A1	Yes	57.30%	573
A2	No	42.70%	427



SINGLE SELECTION

Q2. If yes, have you ever lost that sticky note?

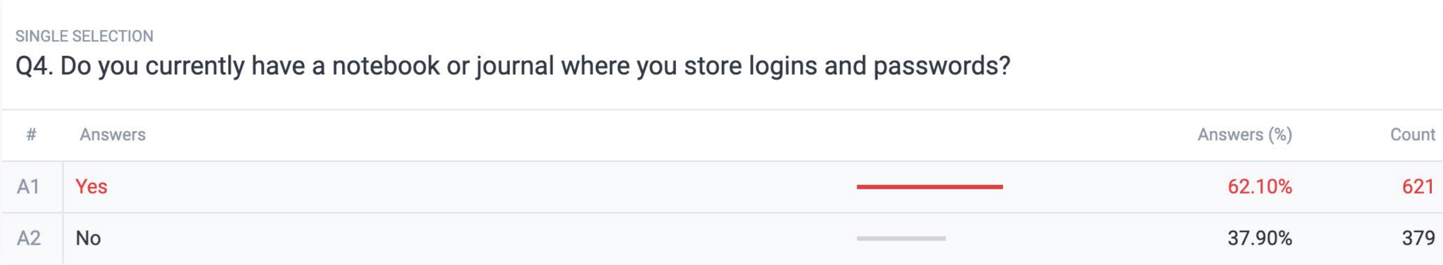
#	Answers	Answers (%)	Count
A1	Yes	66.55%	382
A2	No	33.45%	192



SINGLE SELECTION

Q3. Are you more likely to write down work-related online passwords while working from home?

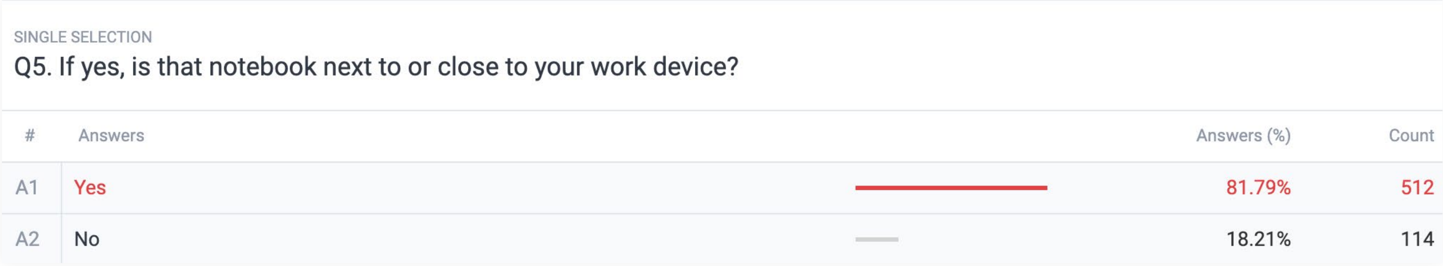
#	Answers	Answers (%)	Count
A1	Yes	66.00%	660
A2	No	34.00%	340



SINGLE SELECTION

Q4. Do you currently have a notebook or journal where you store logins and passwords?

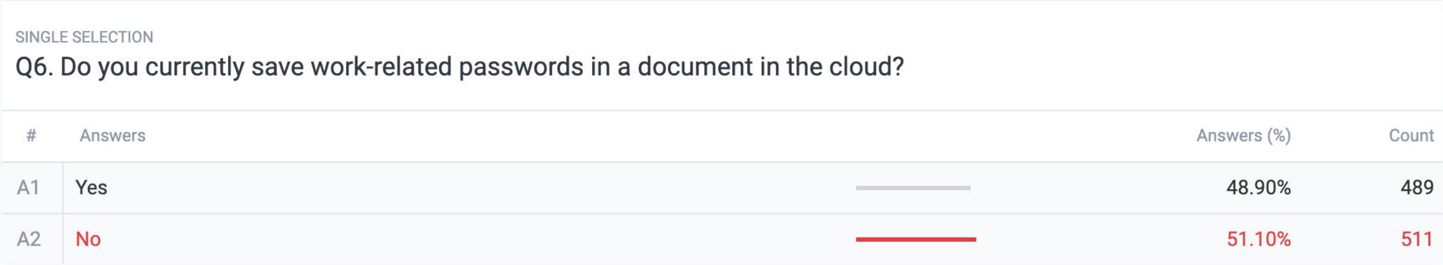
#	Answers	Answers (%)	Count
A1	Yes	62.10%	621
A2	No	37.90%	379



SINGLE SELECTION

Q5. If yes, is that notebook next to or close to your work device?

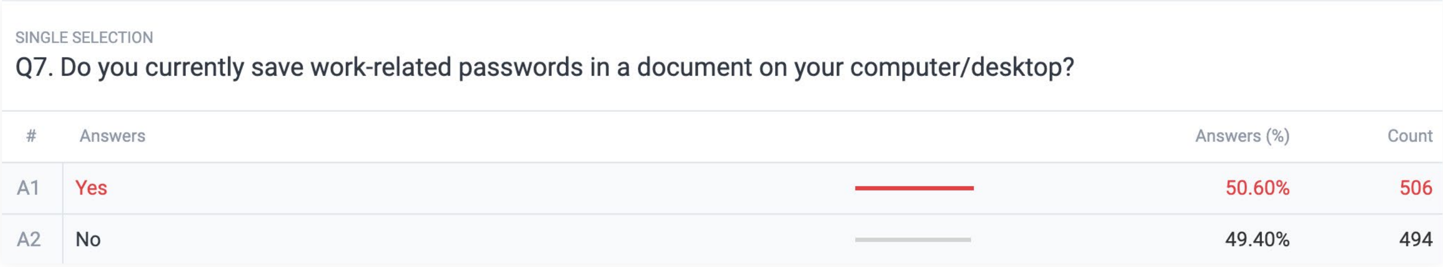
#	Answers	Answers (%)	Count
A1	Yes	81.79%	512
A2	No	18.21%	114



SINGLE SELECTION

Q6. Do you currently save work-related passwords in a document in the cloud?

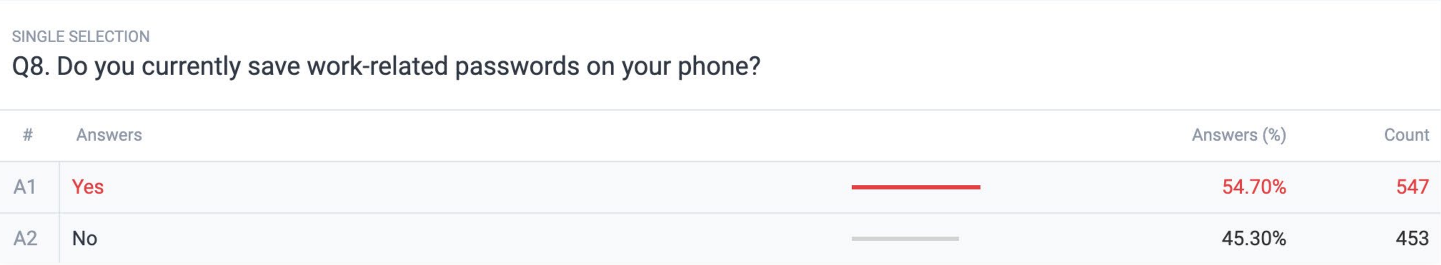
#	Answers	Answers (%)	Count
A1	Yes	48.90%	489
A2	No	51.10%	511



SINGLE SELECTION

Q7. Do you currently save work-related passwords in a document on your computer/desktop?

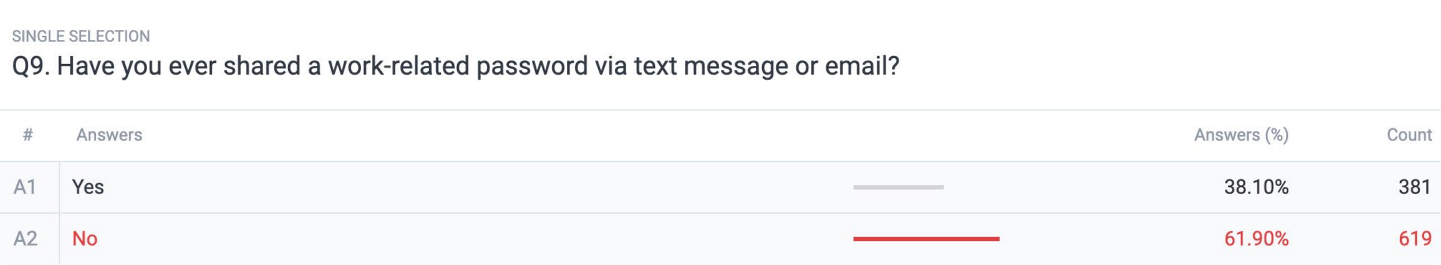
#	Answers	Answers (%)	Count
A1	Yes	50.60%	506
A2	No	49.40%	494



SINGLE SELECTION

Q8. Do you currently save work-related passwords on your phone?

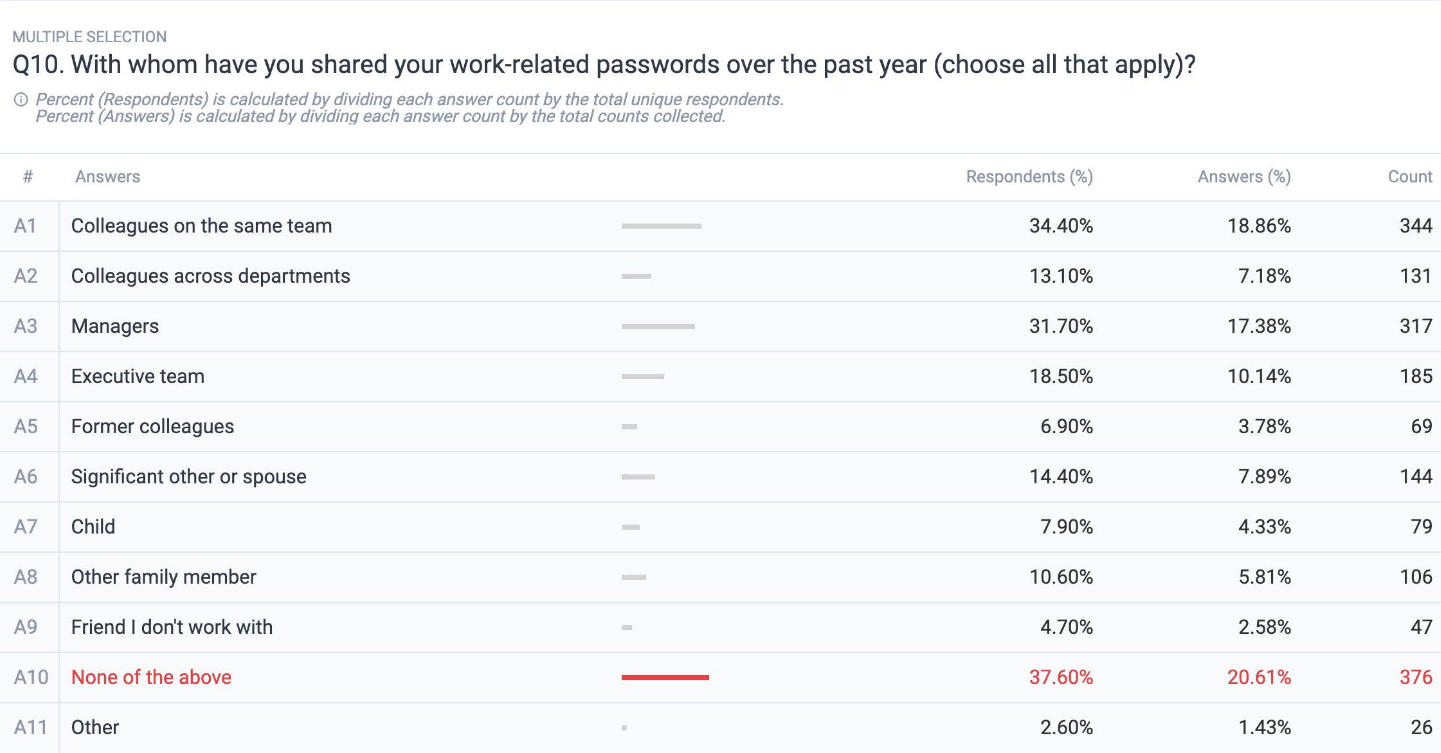
#	Answers	Answers (%)	Count
A1	Yes	54.70%	547
A2	No	45.30%	453



SINGLE SELECTION

Q9. Have you ever shared a work-related password via text message or email?

#	Answers	Answers (%)	Count
A1	Yes	38.10%	381
A2	No	61.90%	619

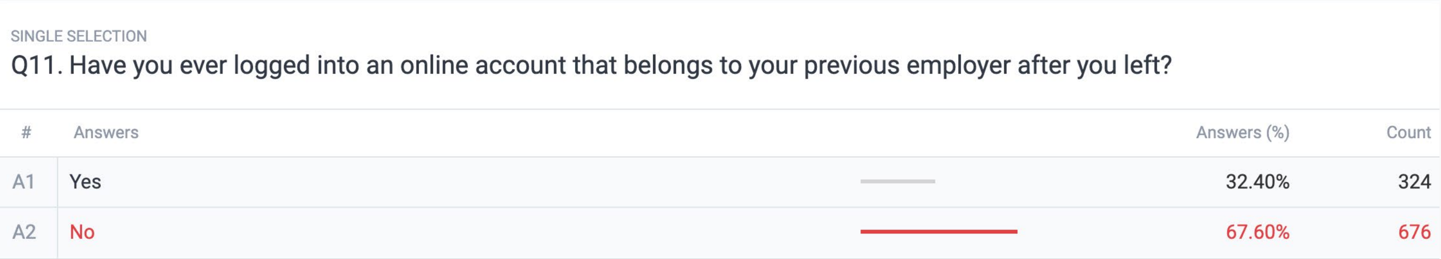


MULTIPLE SELECTION

Q10. With whom have you shared your work-related passwords over the past year (choose all that apply)?

ⓘ *Percent (Respondents) is calculated by dividing each answer count by the total unique respondents.*
Percent (Answers) is calculated by dividing each answer count by the total counts collected.

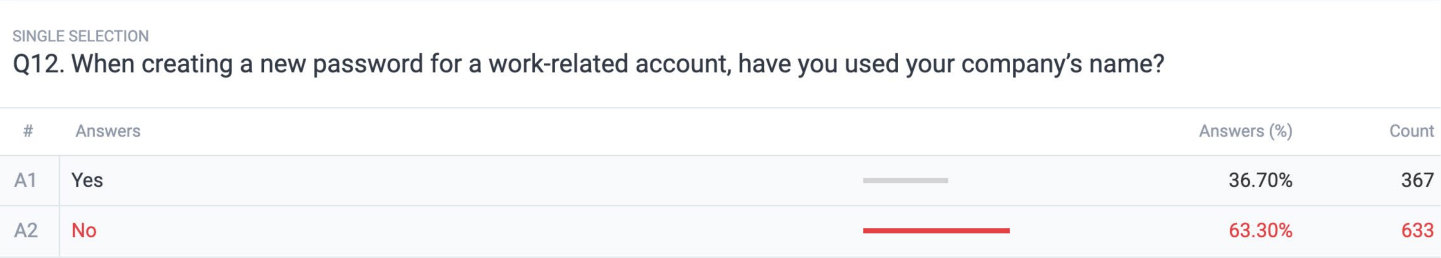
#	Answers	Respondents (%)	Answers (%)	Count
A1	Colleagues on the same team	34.40%	18.86%	344
A2	Colleagues across departments	13.10%	7.18%	131
A3	Managers	31.70%	17.38%	317
A4	Executive team	18.50%	10.14%	185
A5	Former colleagues	6.90%	3.78%	69
A6	Significant other or spouse	14.40%	7.89%	144
A7	Child	7.90%	4.33%	79
A8	Other family member	10.60%	5.81%	106
A9	Friend I don't work with	4.70%	2.58%	47
A10	None of the above	37.60%	20.61%	376
A11	Other	2.60%	1.43%	26



SINGLE SELECTION

Q11. Have you ever logged into an online account that belongs to your previous employer after you left?

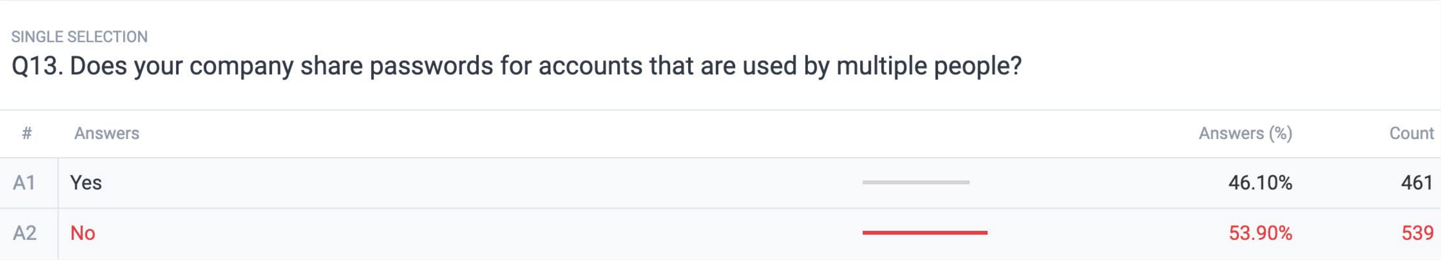
#	Answers	Answers (%)	Count
A1	Yes	32.40%	324
A2	No	67.60%	676



SINGLE SELECTION

Q12. When creating a new password for a work-related account, have you used your company's name?

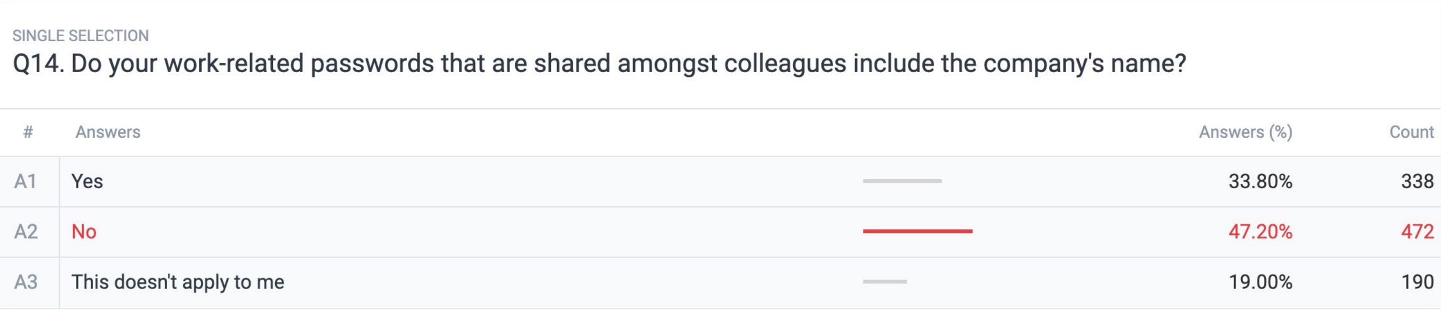
#	Answers	Answers (%)	Count
A1	Yes	36.70%	367
A2	No	63.30%	633



SINGLE SELECTION

Q13. Does your company share passwords for accounts that are used by multiple people?

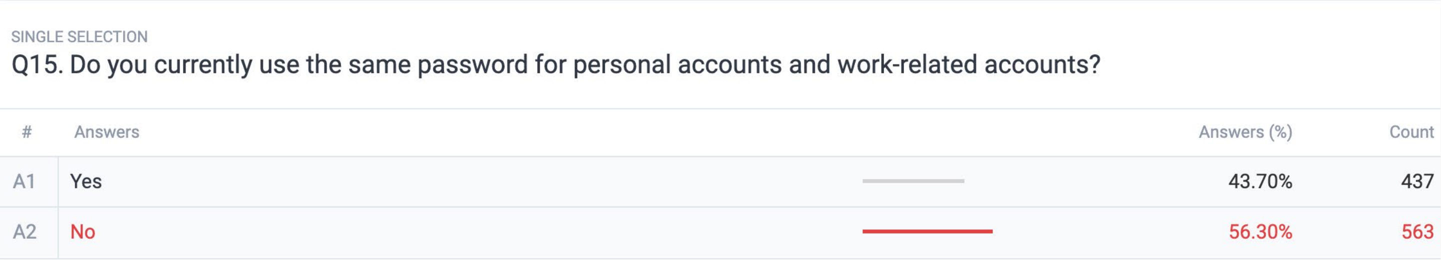
#	Answers	Answers (%)	Count
A1	Yes	46.10%	461
A2	No	53.90%	539



SINGLE SELECTION

Q14. Do your work-related passwords that are shared amongst colleagues include the company's name?

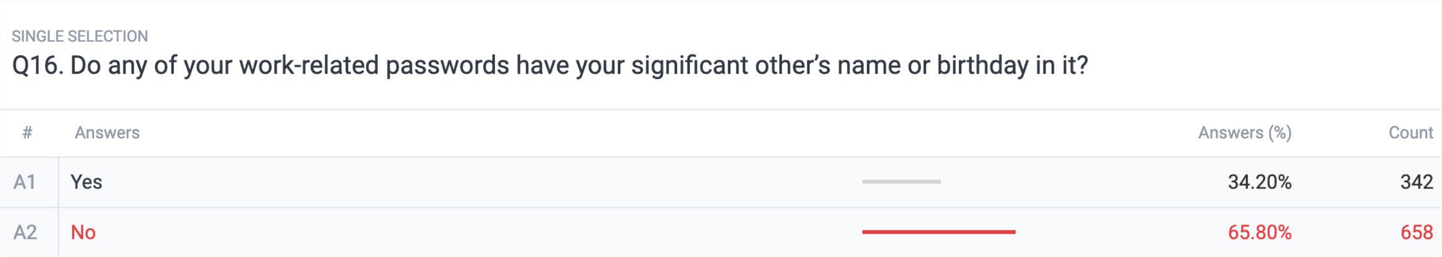
#	Answers	Answers (%)	Count
A1	Yes	33.80%	338
A2	No	47.20%	472
A3	This doesn't apply to me	19.00%	190



SINGLE SELECTION

Q15. Do you currently use the same password for personal accounts and work-related accounts?

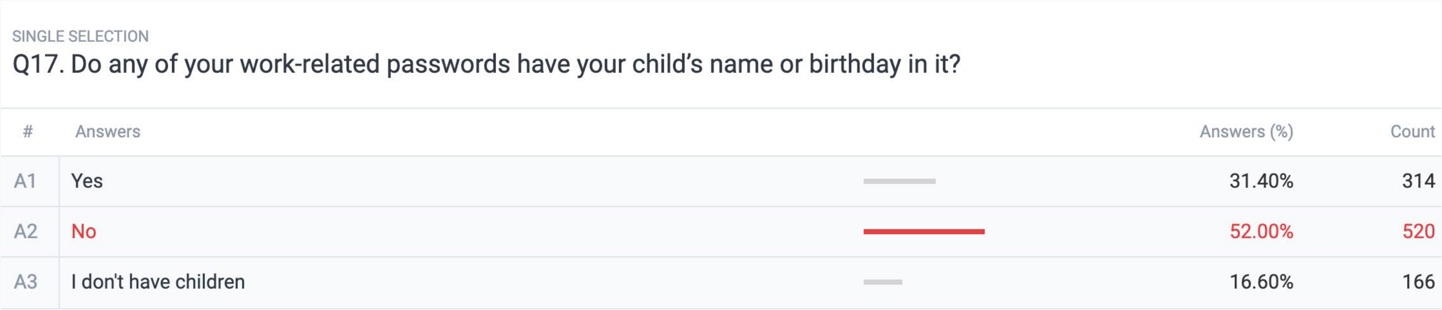
#	Answers	Answers (%)	Count
A1	Yes	43.70%	437
A2	No	56.30%	563



SINGLE SELECTION

Q16. Do any of your work-related passwords have your significant other's name or birthday in it?

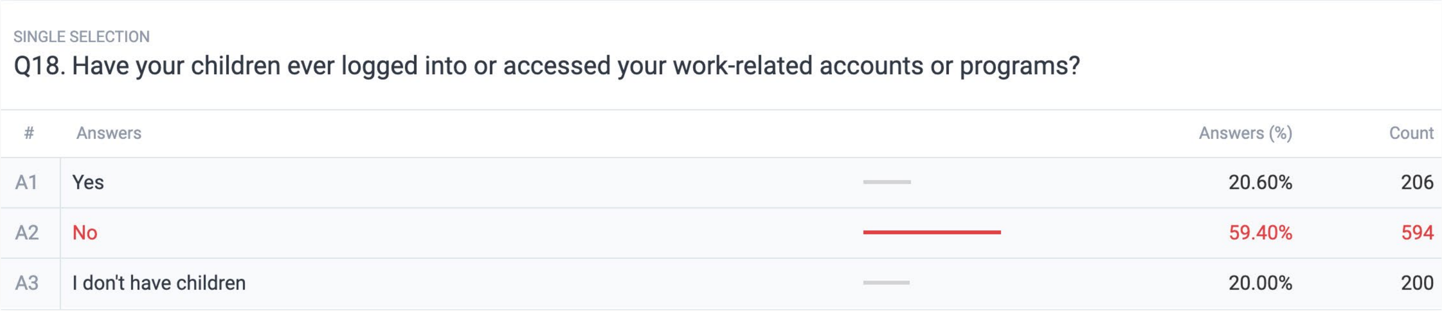
#	Answers	Answers (%)	Count
A1	Yes	34.20%	342
A2	No	65.80%	658



SINGLE SELECTION

Q17. Do any of your work-related passwords have your child's name or birthday in it?

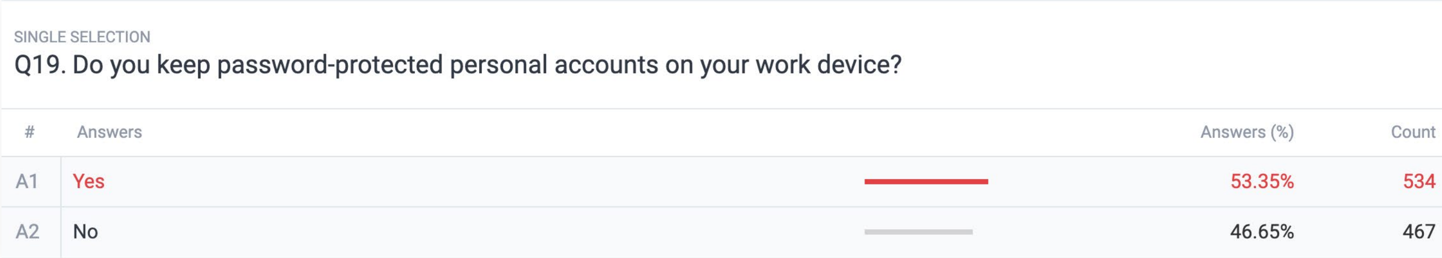
#	Answers	Answers (%)	Count
A1	Yes	31.40%	314
A2	No	52.00%	520
A3	I don't have children	16.60%	166



SINGLE SELECTION

Q18. Have your children ever logged into or accessed your work-related accounts or programs?

#	Answers	Answers (%)	Count
A1	Yes	20.60%	206
A2	No	59.40%	594
A3	I don't have children	20.00%	200



SINGLE SELECTION

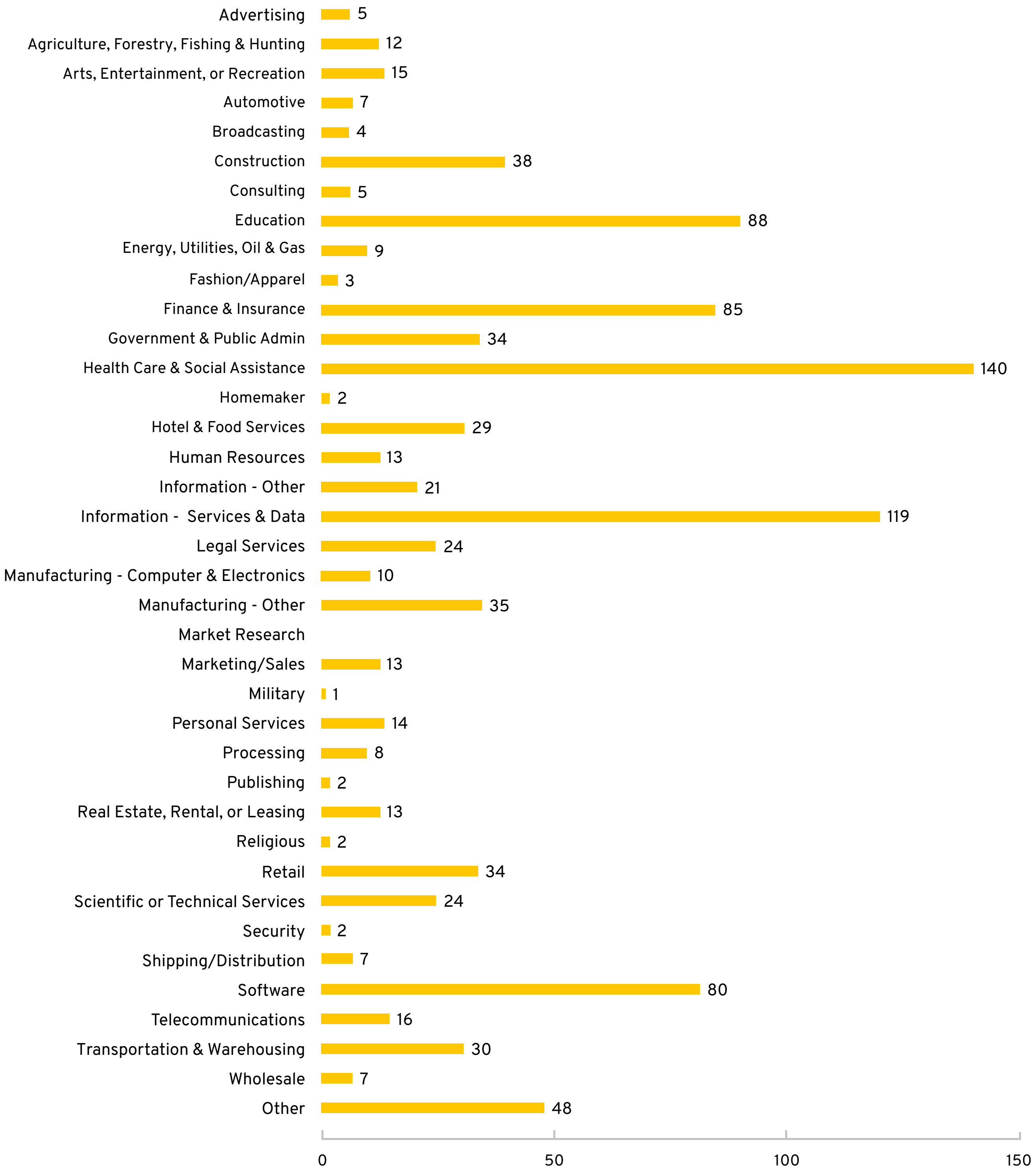
Q19. Do you keep password-protected personal accounts on your work device?

#	Answers	Answers (%)	Count
A1	Yes	53.35%	534
A2	No	46.65%	467

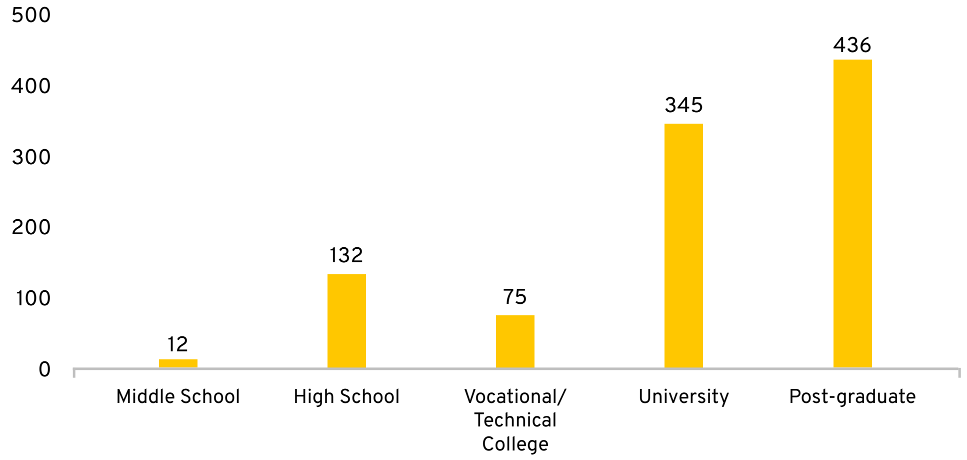
Audience Demographics

Sample Size 1000

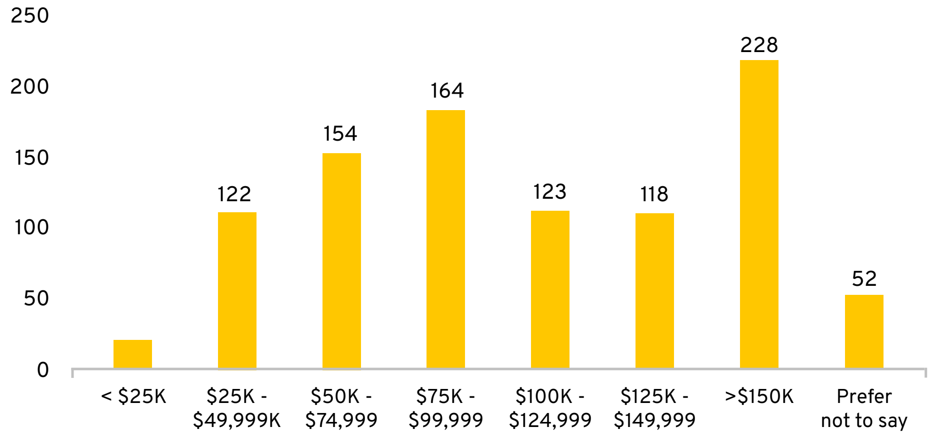
Career



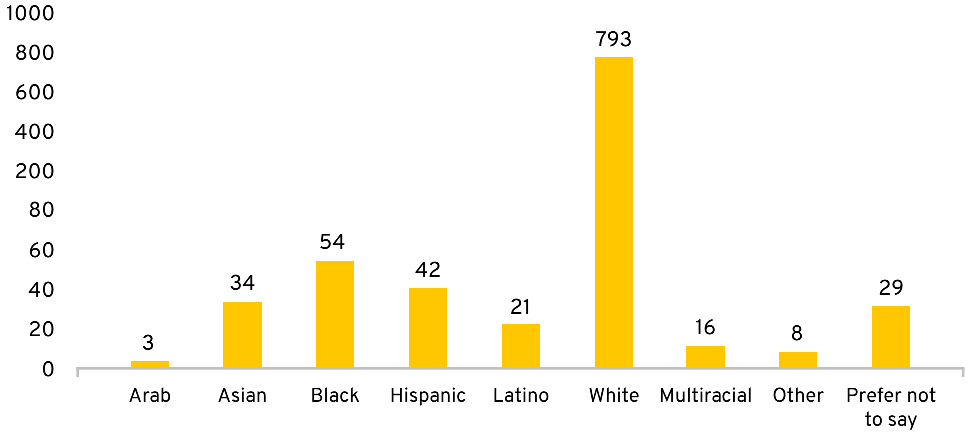
Education



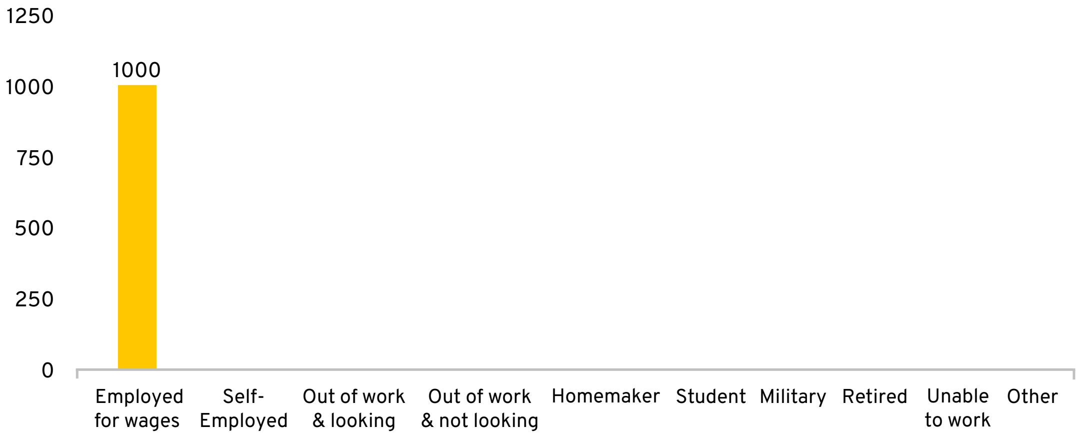
Income



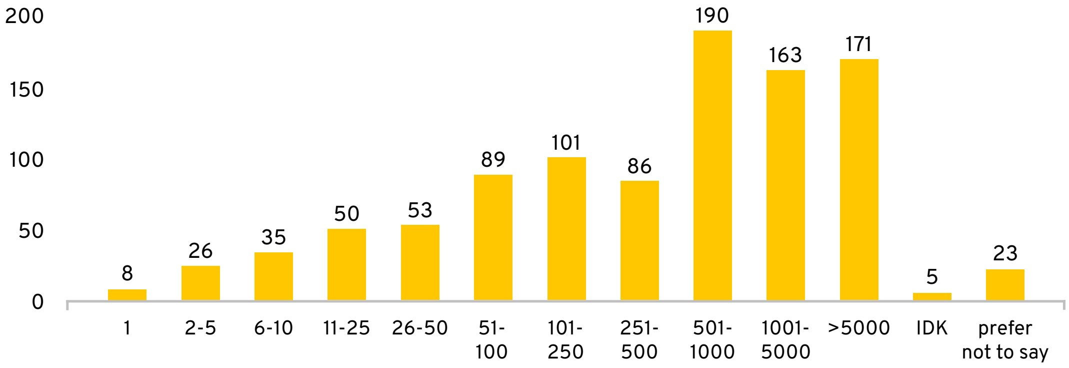
Ethnicity

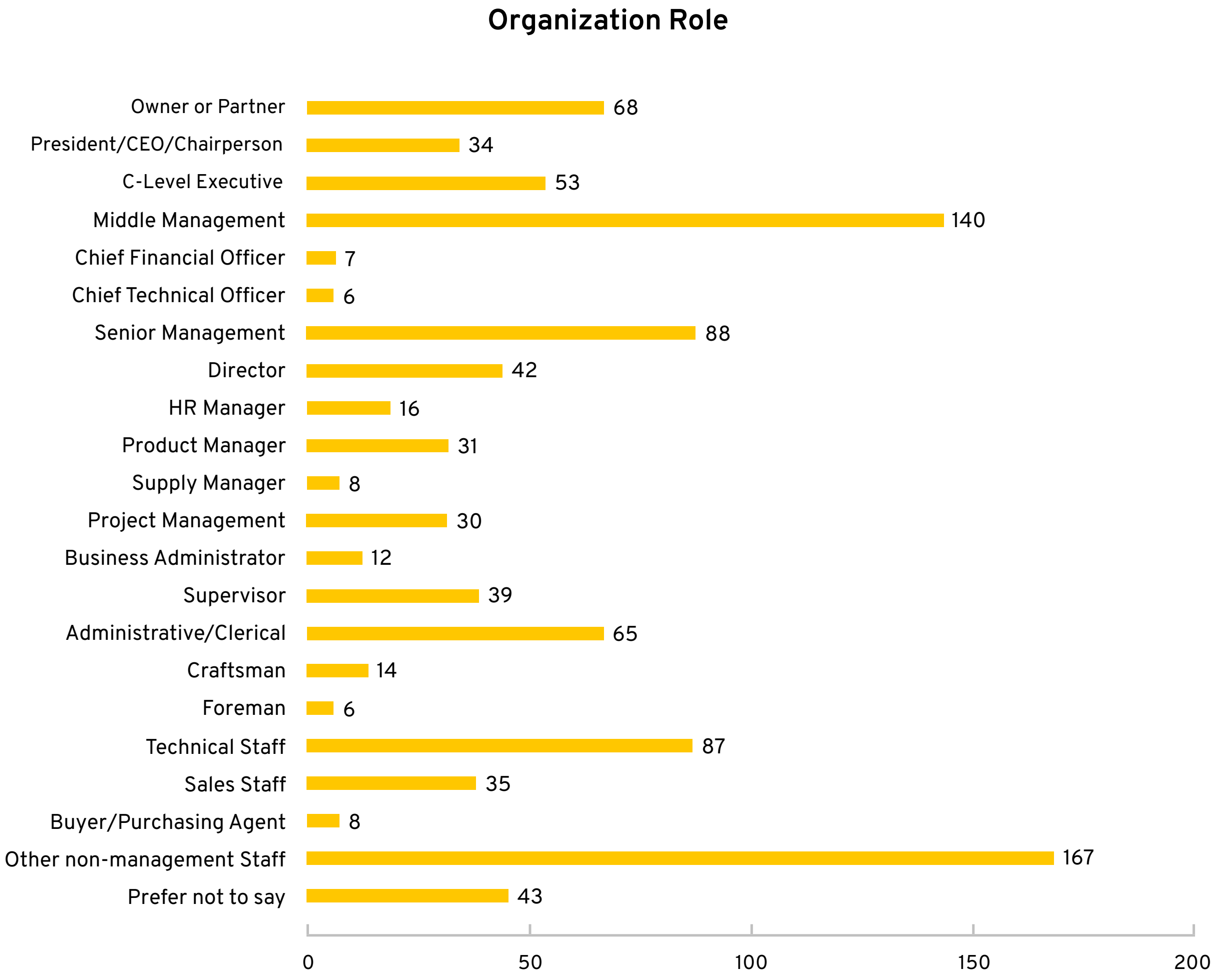


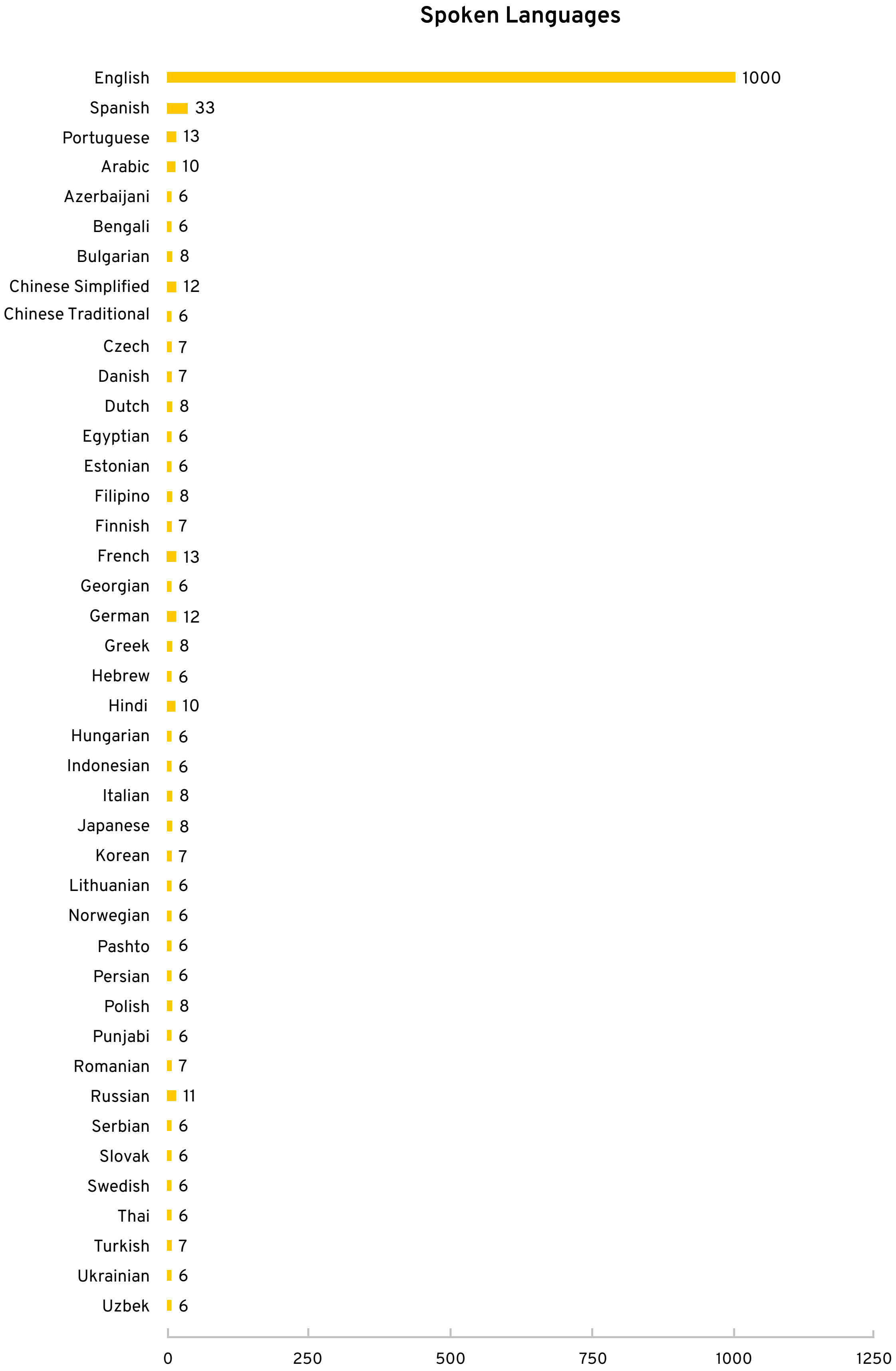
Employment Status



Number of Employees




Organization Role
Owner or Partner 68
President/CEO/Chairperson 34
C-Level Executive 53
Middle Management 140
Chief Financial Officer 7
Chief Technical Officer 6
Senior Management 88
Director 42
HR Manager 16
Product Manager 31
Supply Manager 8
Project Management 30
Business Administrator 12
Supervisor 39
Administrative/Clerical 65
Craftsman 14
Foreman 6
Technical Staff 87
Sales Staff 35
Buyer/Purchasing Agent 8
Other non-management Staff 167
Prefer not to say 43
0
50
100
150
200


Spoken Languages
English 1000
Spanish 33
Portuguese 13
Arabic 10
Azerbaijani 6
Bengali 6
Bulgarian 8
Chinese Simplified 12
Chinese Traditional 6
Czech 7
Danish 7
Dutch 8
Egyptian 6
Estonian 6
Filipino 8
Finnish 7
French 13
Georgian 6
German 12
Greek 8
Hebrew 6
Hindi 10
Hungarian 6
Indonesian 6
Italian 8
Japanese 8
Korean 7
Lithuanian 6
Norwegian 6
Pashto 6
Persian 6
Polish 8
Punjabi 6
Romanian 7
Russian 11
Serbian 6
Slovak 6
Swedish 6
Thai 6
Turkish 7
Ukrainian 6
Uzbek 6
0
250
500
750
1000
1250

Ratings & Awards

Keeper has been named PC Magazine's Best Password Manager of the Year & Editors' Choice, PCWorld's Editors' Choice for two consecutive years and is the winner of four G2 awards for Best Software and four InfoSec Award for Best Product in Password Management for SMB and Best Product for SMB Cybersecurity. Keeper is SOC-2 and ISO 27001 Certified and is listed for use by the U.S. federal government through the System for Award Management (SAM).

Gartner Peer Insights
4.9 out of 5 stars

Spiceworks
5 out of 5 stars

Editors' Choice
4.5 out of 5 stars

2020 Enterprise Leader
4.7 out of 5 stars

INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2019

- **Publisher's Choice Cybersecurity Password Management**
- **Cutting Edge Chief Executive of the Year**

INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2020

- **Best Product in Password Management**
- **Best Product for SMB Cybersecurity**
- **Publisher's Choice for Chief Executive of the Year**
- **Most Innovative CTO of the Year**

Best Password Manager of the Year & Editors' Choice 2019 & 2020

Editors' Choice 2018 & 2019

Leader WINTER 2021

Leader Enterprise WINTER 2021

Leader Mid-Market WINTER 2021

Leader Small Business WINTER 2021

Leader Europe WINTER 2021

Top 100 Software Products BEST SOFTWARE AWARDS 2020

Top 100 Highest Satisfaction Products BEST SOFTWARE AWARDS 2020

Top 50 SMB Products BEST SOFTWARE AWARDS 2020

Top 50 Remote Tools BEST SOFTWARE AWARDS 2020

To download a copy of the Workplace Password Malpractice Report, infographic and more, visit our dedicated **resources hub**. For more information on Keeper Security, or how to defend your organization from password-related data breaches, go to **keepersecurity.com**.

Methodology

Keeper Security contracted with Pollfish to conduct this survey of 1,000 full time employees in the United States. Only individuals who use passwords to log into work-related online accounts were included. The survey was completed in February 2021.

About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the highly-rated and patented cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity and meet compliance standards. In 2020, Keeper was named PCMag's Best Password Manager of the Year & Editors' Choice for the third time. Keeper has also been named PCWorld's Editors' Choice and is the winner of four G2 Best Software Awards and the InfoSec Award for Best Product in Password Management for SMB Cybersecurity. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM).