The 2019 State of Password and Authentication Security Behaviors Report

Research sponsored by Yubico

Independently Conducted by Ponemon Institute LLC

January 2019

Ponemon Institute© Research Report

The 2019 State of Password and Authentication Security Behaviors Report

Ponemon Institute, January 2019

Table of Contents	From Page	To Page
Part 1. Introduction	**2**	**3**
Part 2. Key findings	**4**	**24**
How privacy and security concerns affect personal password practices	**4**	**8**
Risky password practices in the workplace	**8**	**9**
Authentication and account security in organizations	**10**	**13**
Differences in password practices and authentication by age	**14**	**17**
Country differences in password practices and authentication security behaviors	**18**	**24**
Part 3. Methods	**25**	**28**
Part 4. Caveats	**29**	**29**
Appendix: Detailed survey results	**30**	**39**

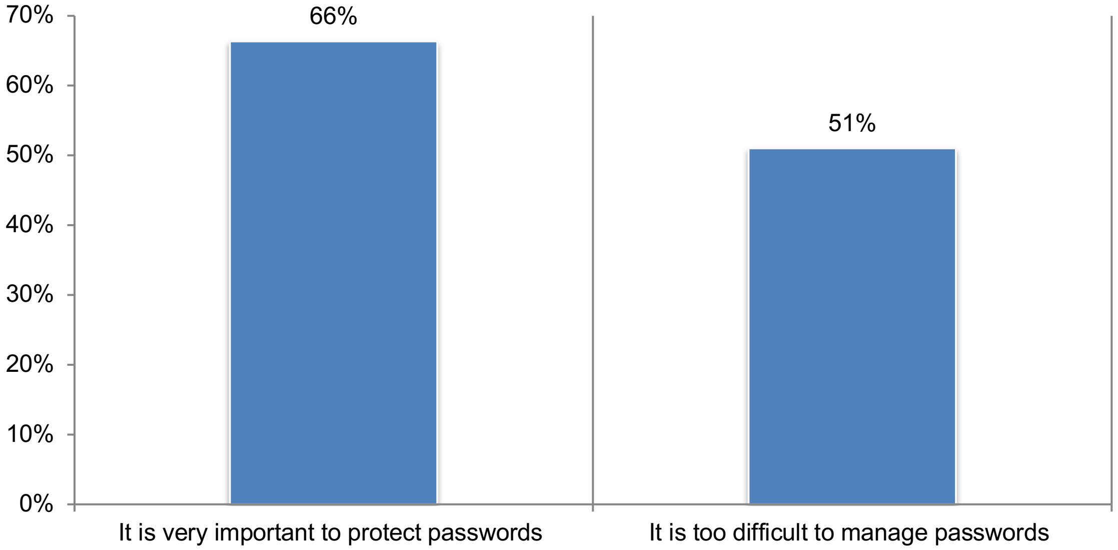
Part 1. Introduction

There are a growing number of security breaches happening daily to both individuals and businesses. As a result, organizations and online services have shifted efforts in recent years to help educate employees and end users on proper password hygiene, two-factor authentication, signs of a phishing scam, and so on. Despite our worsening state of online security, are we becoming more security-minded individuals, and better yet, are we putting it into practice?

Ponemon Institute is pleased to present the results of *The 2019 State of Password and Authentication Security Behaviors Report,* sponsored by Yubico*.* The purpose of this study is to understand the beliefs and behaviors surrounding password management and authentication practices for individuals both in the workplace and at home. The goal was to understand if these beliefs and behaviors align, and why or why not. The conclusion is that despite the increasing concern regarding privacy and protection online and a greater understanding of the best security practices, individuals and businesses are still falling short. Both parties are in dire need of solutions that will offer both added security and convenience.

Ponemon Institute surveyed 1,761 IT and IT security practitioners in the United States, United Kingdom, Germany and France. These respondents should be more knowledgeable and aware of the risks of poor password practices than individuals who do not work in IT or IT security. As shown in Figure 1, 66 percent of respondents believe it is important to protect the passwords used in the workplace and 63 percent of respondents say it is important to protect passwords on their personal devices. However, 51 percent of respondents acknowledge that it is difficult to manage their passwords.

Figure 1. Perceptions about managing passwords in the workplace
Strongly agree and Agree responses combined



Following are the most salient findings of this research.

- Sixty-three percent of respondents say they have become more concerned about the privacy and security of their personal data over the past two years. Respondents report being most concerned with Social Security number or Citizen ID, payment account details and health information. The reason respondents reported being more concerned about their privacy was due to government surveillance (59 percent), the growing use of mobile devices (51 percent) and connected devices (40 percent).

- Almost half of respondents (47 percent) say their companies are most concerned about protecting customer information and 45 percent of respondents say they are most concerned about protecting employee information.

- As cyberattacks become more prevalent, vulnerabilities created by poor password and authentication practices lead to attacks such as phishing. More than half of respondents (51 percent) say they have experienced a phishing attack in their personal life, while 44 percent of respondents have experienced a phishing attack at work. However, while phishing attacks are occurring on a frequent basis, 57 percent of respondents who have experienced a phishing attack have not changed their password behaviors.

- Approximately two out of three respondents (69 percent) admit to sharing passwords with their colleagues in the workplace to access accounts, and more than half of respondents (51 percent) reuse an average of five passwords across their business and/or personal accounts. Furthermore, added protection beyond a username and password, in the form of two-factor authentication, is not widely used. Sixty-seven percent of respondents do not use any form of two-factor authentication in their personal life and 55 percent of respondents do not use it at work.

- It is increasingly clear that new security approaches are needed to help individuals manage and protect their passwords both personally and professionally. On average, respondents report having to spend an average of 12.6 minutes each week or 10.9 hours per year entering and/or resetting passwords. Based on the average headcount in this research of almost 15,000, we estimate the annual cost of productivity and labor loss per company averages $5.2 million annually.

- Because managing passwords is inconvenient and cumbersome, 57 percent of respondents expressed a preference for passwordless logins that protect their identity. Fifty-six percent of respondents believe that a physical hardware token offers better security.

Part 2. Key findings

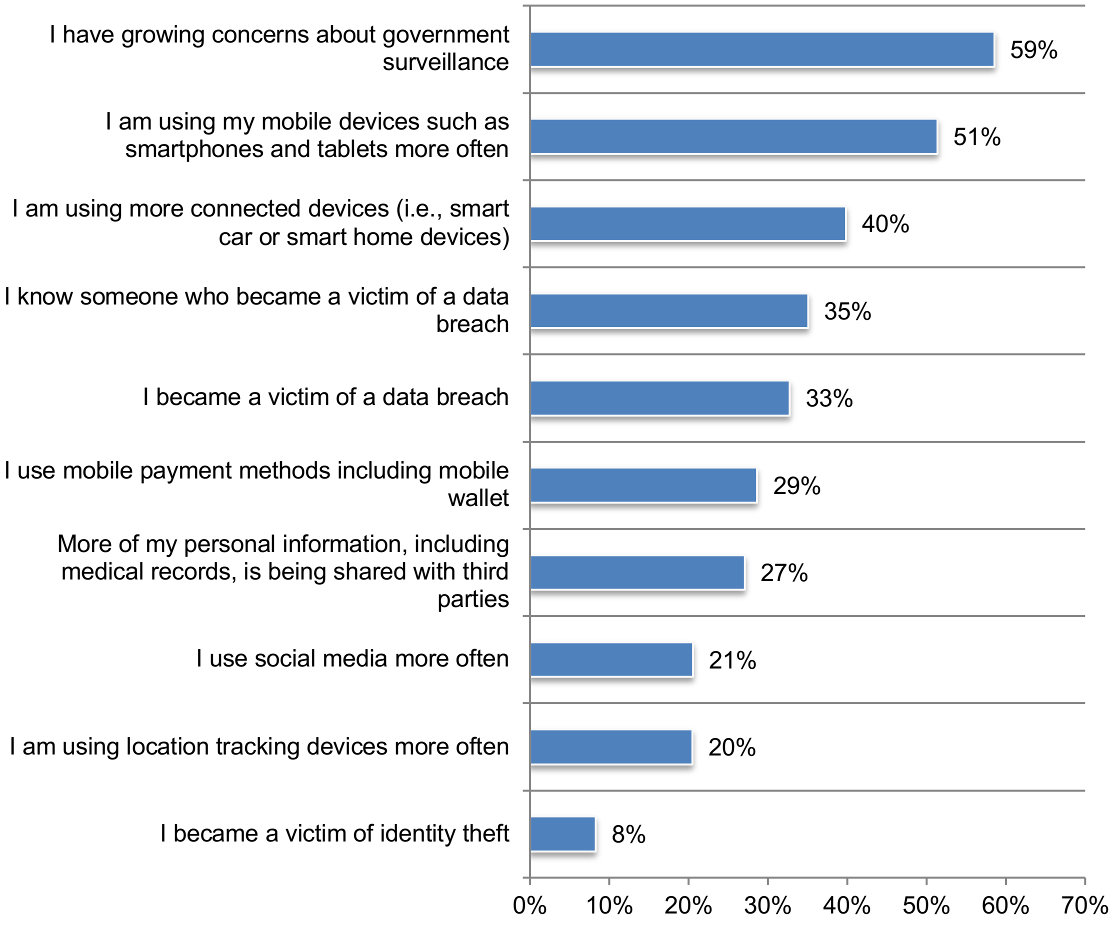
This section provides an analysis of the key findings. The complete audited findings of the research are provided in the Appendix of this report. We have organized the report according to the following themes:

- How privacy and security concerns affect personal password practices
- Risky password practices in the workplace
- Authentication and account security in organizations
- Differences in password practices and authentication security behaviors by age
- Differences in password practices and authentication security behaviors by country

How privacy and security concerns affect personal password practices

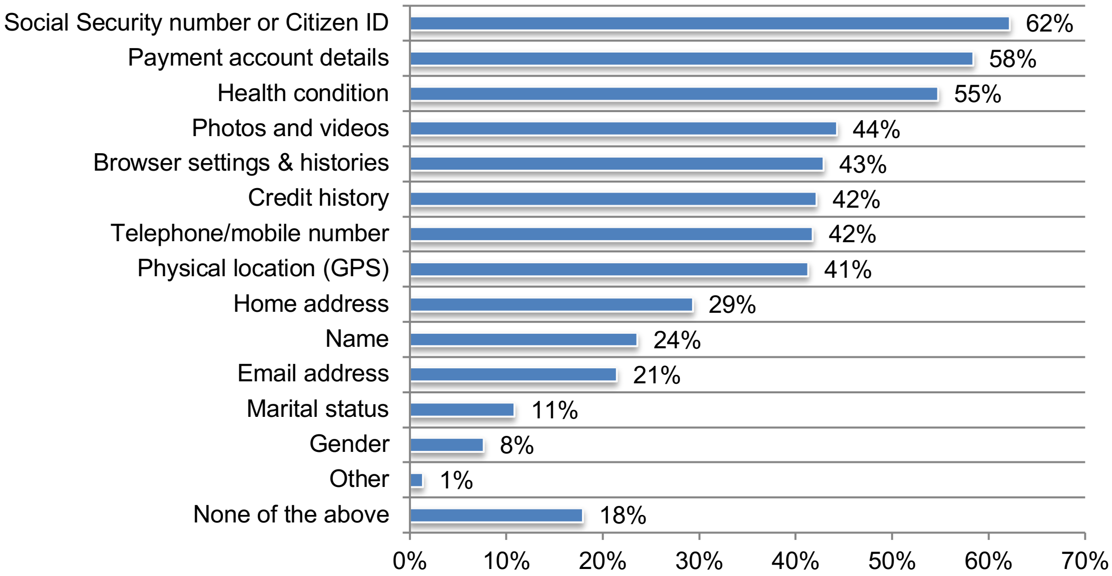
Privacy concerns increase. Sixty-three percent of respondents say they have become more concerned about the privacy and security of their personal data over the past two years. As shown in Figure 2, the number one reason for this is a growing concern about government surveillance (59 percent of respondents) followed by the increasing use of mobile devices, such as smartphones and tablets.

Figure 2. Why are you more concerned about your privacy?
More than one response permitted



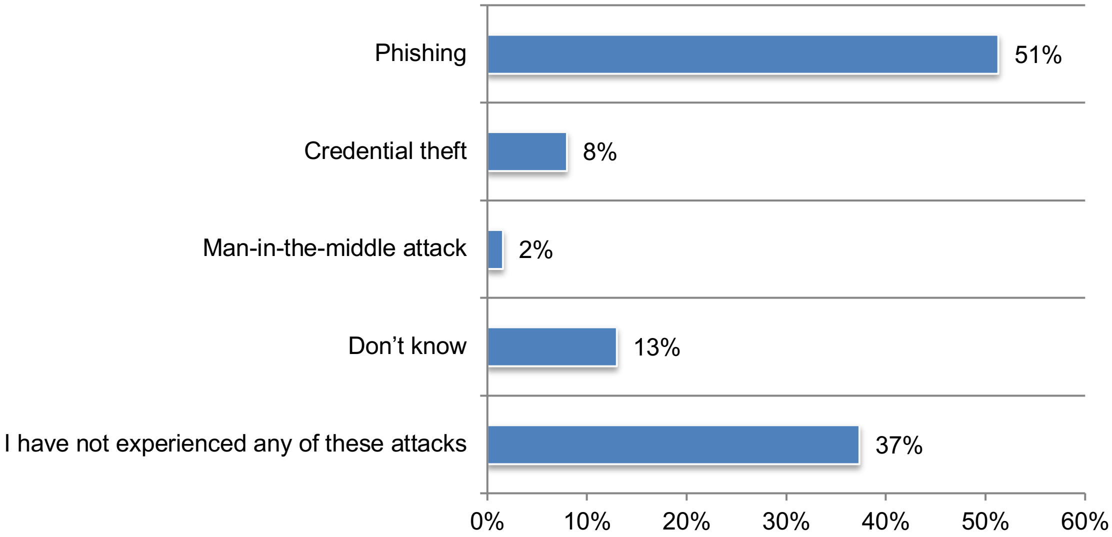
Protection of Social Security numbers or Citizen IDs and payment account details is considered most important. According to Figure 3, respondents are most concerned about protecting the data that is most vulnerable to identity theft.

Figure 3. What personal information are you most concerned about protecting?
More than one response permitted



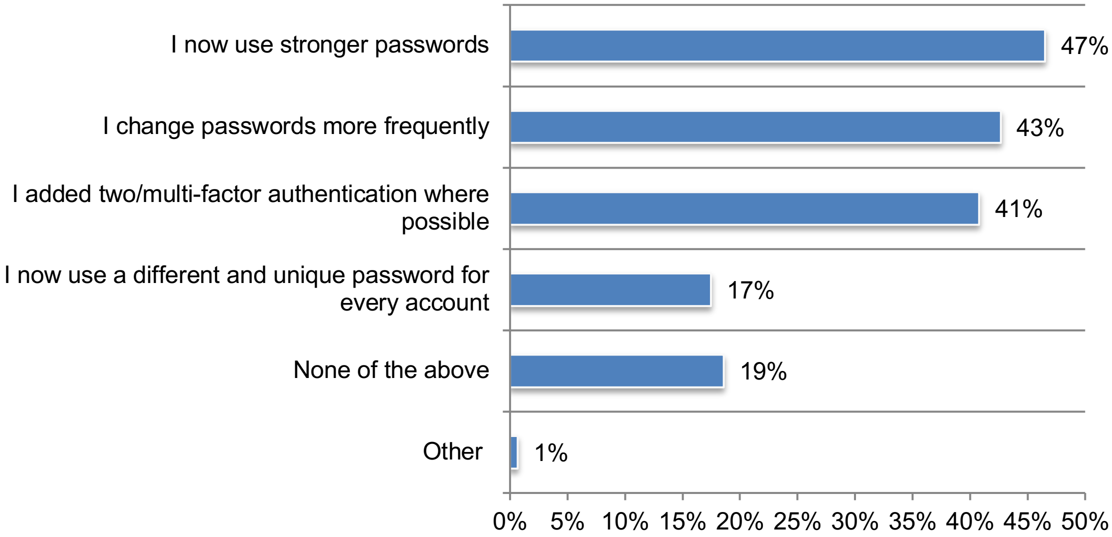
Phishing attacks are prevalent but do not change behavior. More than half of respondents (51 percent) say they have experienced a phishing attack but 57 percent of these respondents say it did not change how they manage their passwords. While very few respondents report they have experienced credential theft (8 percent) or a man-in-the-middle attack (2 percent), it is also important to note that it can be more difficult to really know if they have been targeted by these attacks.

Figure 4. Have you experienced any of the following attacks in your personal life?
More than one choice permitted



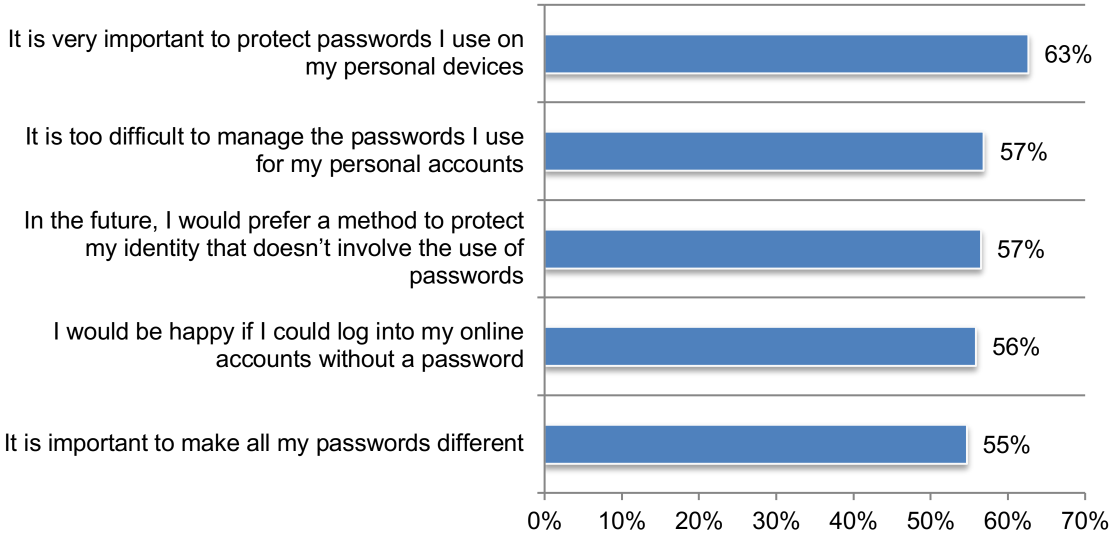
Following any of these attacks, stronger passwords are used. As shown in Figure 5, of the 43 percent of respondents who say they change how they manage passwords, 47 percent of respondents say they use stronger passwords and/or change them more frequently (43 percent of respondents).

Figure 5. If you changed how you manage your passwords, what did you do?
More than one choice permitted



Passwords are inconvenient and cumbersome. As shown in Figure 6, the majority of respondents would prefer an alternative method to protect their identity (57 percent) and would be happy if they didn't need a password to log into their online accounts (56 percent). Despite the difficulty in managing their passwords, 63 percent of respondents believe that the protection of passwords used on personal devices is important.

Figure 6. Perceptions about personal passwords
Strongly agree and Agree responses combined



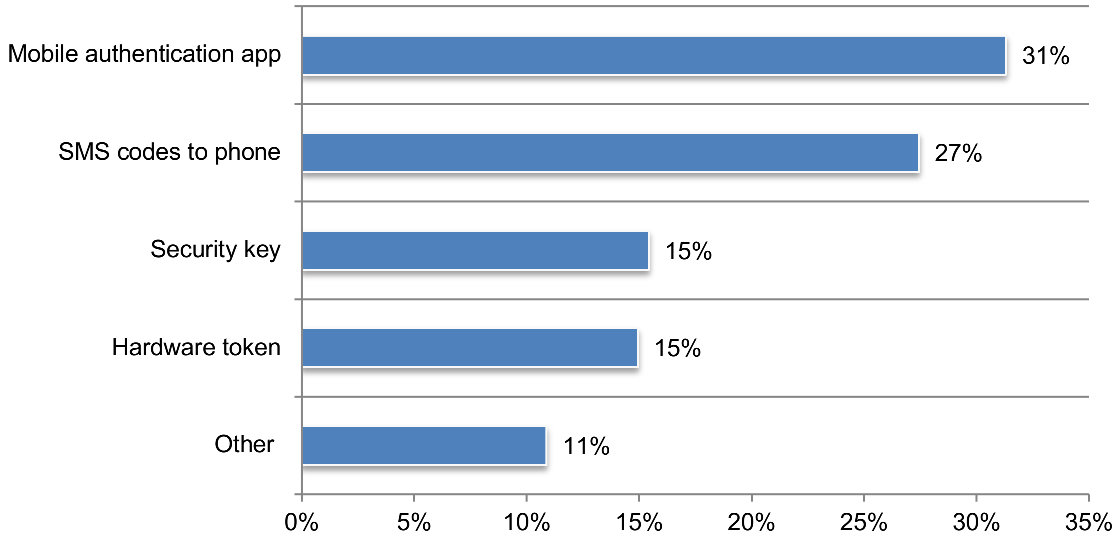
Managing passwords are costly to organizations. As shown in Table 1, on average, respondents report having to spend an average of 12.6 minutes each week or 10.9 hours per year entering and/or resetting passwords. Based on the average headcount in this research of almost 15,000, we estimate the cost of the loss of productivity and labor to organizations averages $5.2 million annually.

Table 1. How much time do you spend each week entering and/or resetting your passwords?	Notes to calculations	Calculus
Minutes each week	A=Computed from survey	12.61
Minutes each year	B=A x 52	655.72
Hours each year	C=B / 60	10.93
*Average labor cost per hour	D=Determined from benchmarks	$32.00
*Average labor cost per employee	E=C x D	$349.72
Average total headcount	F=Computed from survey	14,919
Annual cost of productivity and labor loss per company on average	G=E x F	$5,217,456

*An average hourly rate for a rank and file employee $32.00 (source: Ponemon Institute)

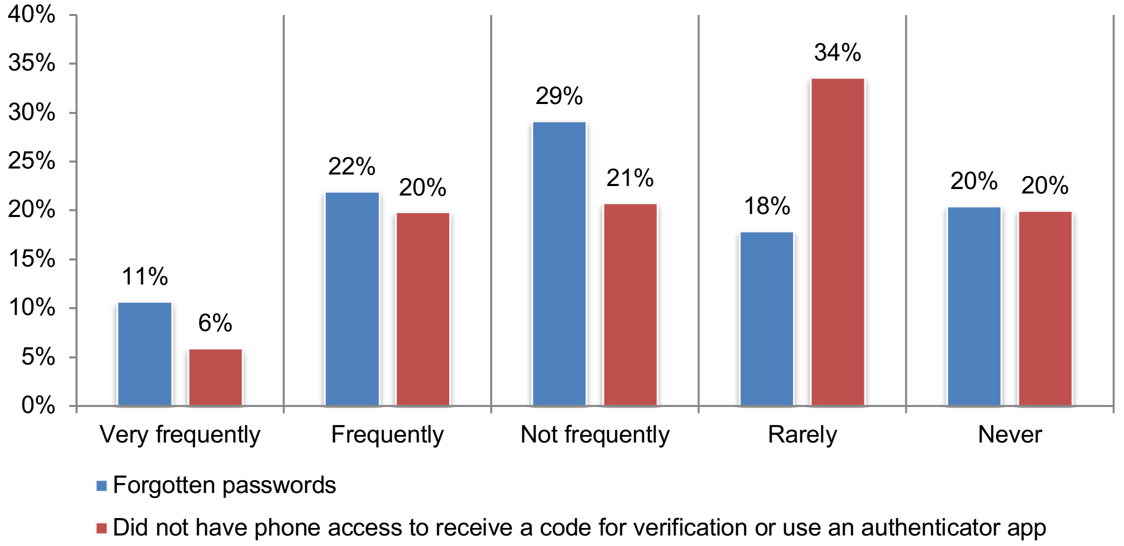
Thirty-three percent of respondents say they use two-factor authentication for personal use. The two most popular methods are mobile application app (31 percent of respondents) and/or SMS codes sent to phone (27 percent of respondents), as shown in Figure 7.

Figure 7. What type of two-factor authentication do you use for personal reasons?
More than one choice permitted



Most respondents were unable to complete a personal transaction because they forgot their passwords. According to Figure 8, 62 percent of respondents say they could not complete a purchase or other online transaction because they could not remember their passwords. Almost half (47 percent of respondents) say a transaction could not be completed because they did not have mobile phone access to receive a code for verification or were not able to use an authenticator app.

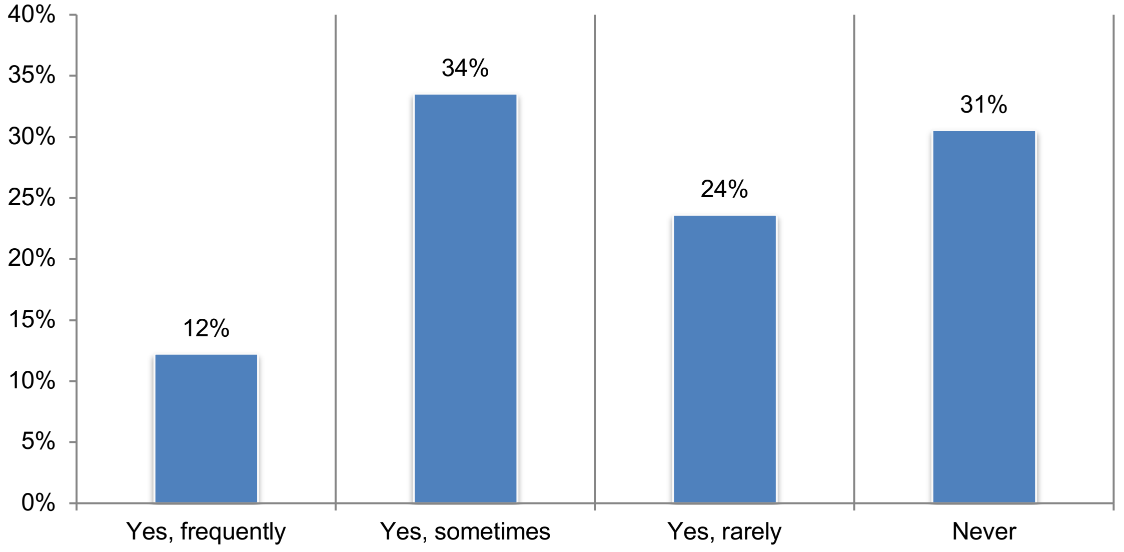
Figure 8. The frequency of not being able to complete personal because passwords were forgotten, mobile verification codes could not be received or mobile authenticator apps could not be used



Risky password practices in the workplace

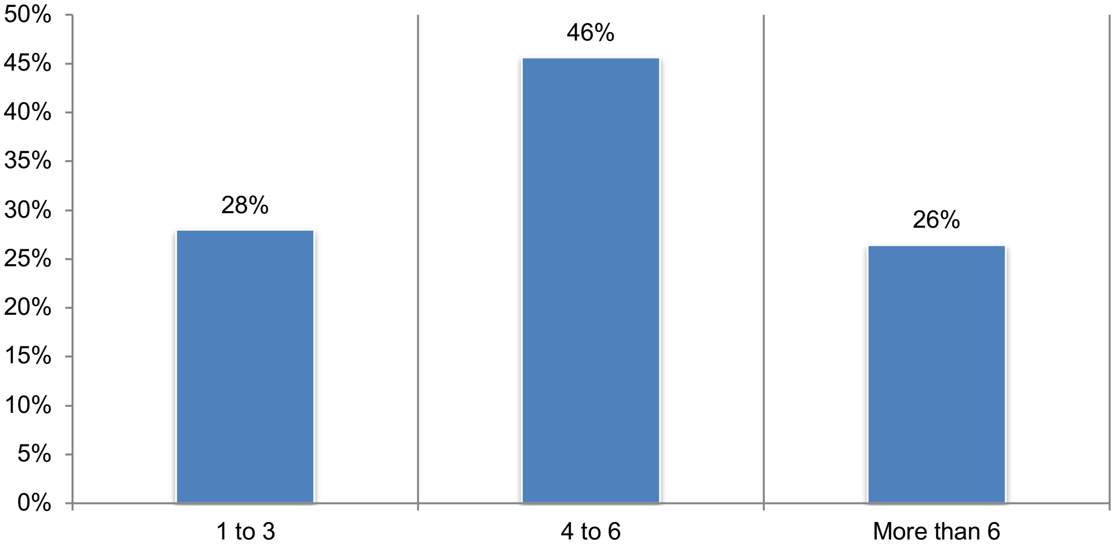
Passwords are being shared in the workplace. While respondents should know better, 69 percent say they have shared passwords with others in the workplace either frequently, sometimes or rarely to enable access to accounts, as shown in Figure 9.

Figure 9. Do you share passwords with colleagues to enable access to accounts?



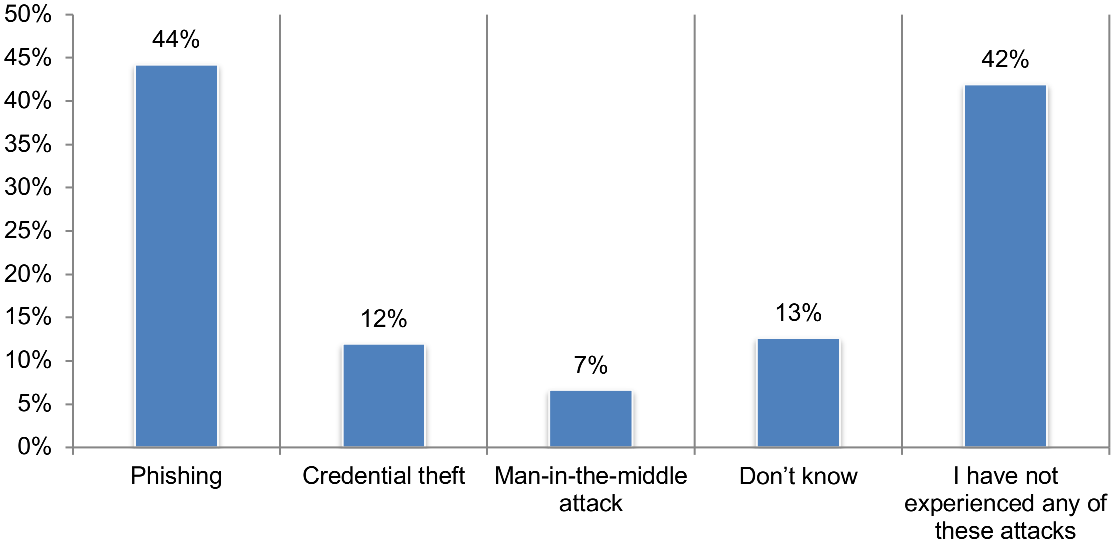
Passwords are reused an average of five times. More than half of respondents (51 percent) say they reuse passwords across any of their business and/or personal accounts. As shown in Figure 10, respondents reuse an average of 5 passwords.

Figure 10. The number of times a password is reused
Extrapolated value 4.69



Phishing attacks are prevalent in the workplace. Similar to what respondents report from their personal experience, the most frequent type of attack experienced in the workplace is also phishing. Fifty-seven percent of respondents say their colleagues are not careful to avoid phishing scams, putting their organizations at risk for such attacks as credential theft and ransomware. While fewer respondents report that they have experienced credential theft or a man-in-the-middle attack, it is important to note that it can be more difficult to really know if they have been targeted by these attacks.

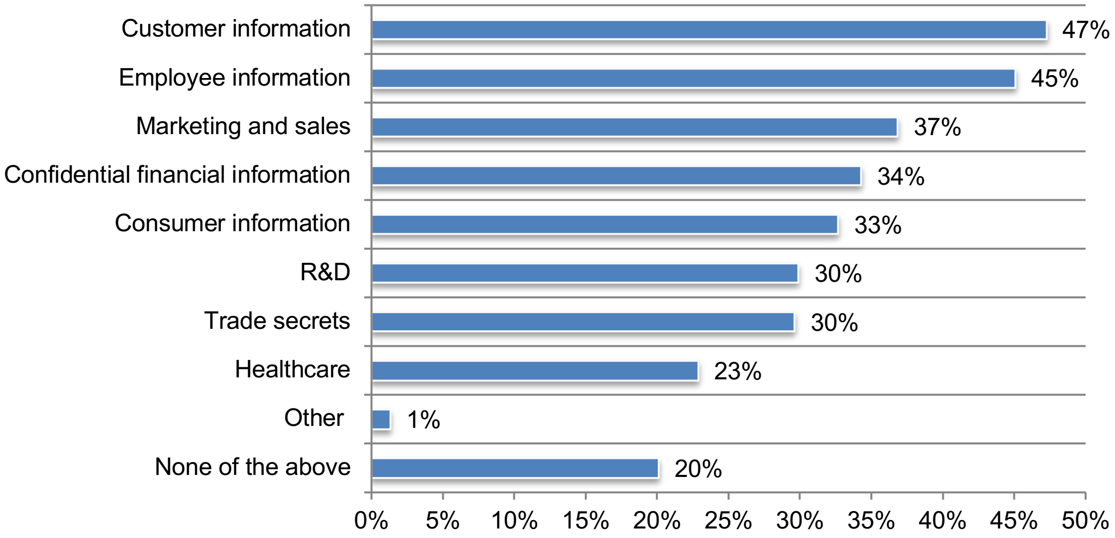
Figure 11. Have you experienced any of the following attacks in the workplace?
More than one choice permitted



Authentication and account security in organizations

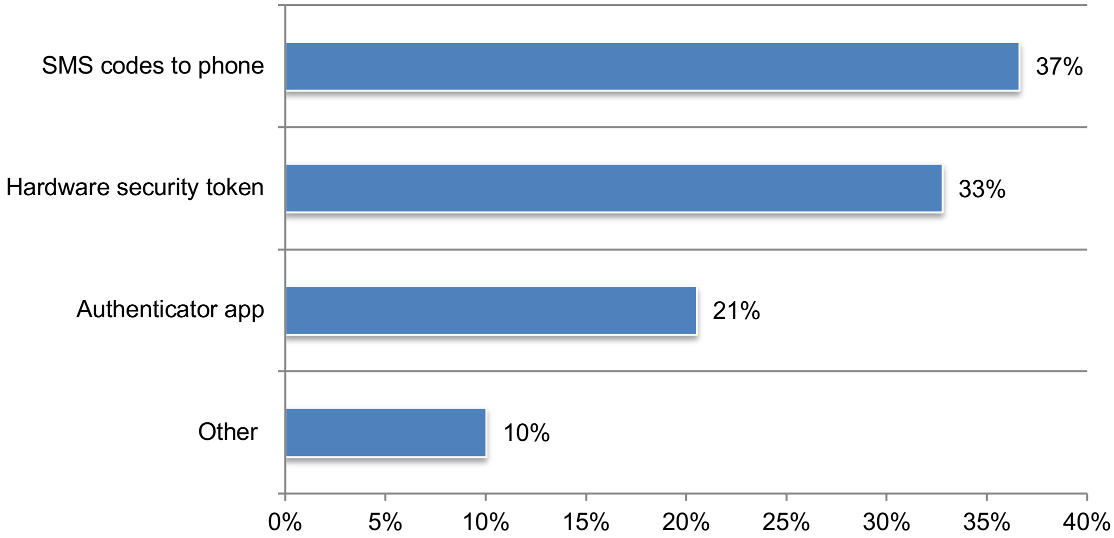
Customer and employee information are top priorities for organizations when it comes to data protection. Figure 12 presents a list of the types of business information respondents believe are most important to protect with effective authentication methods.

Figure 12. What business information are you most concerned about protecting?
More than one choice permitted



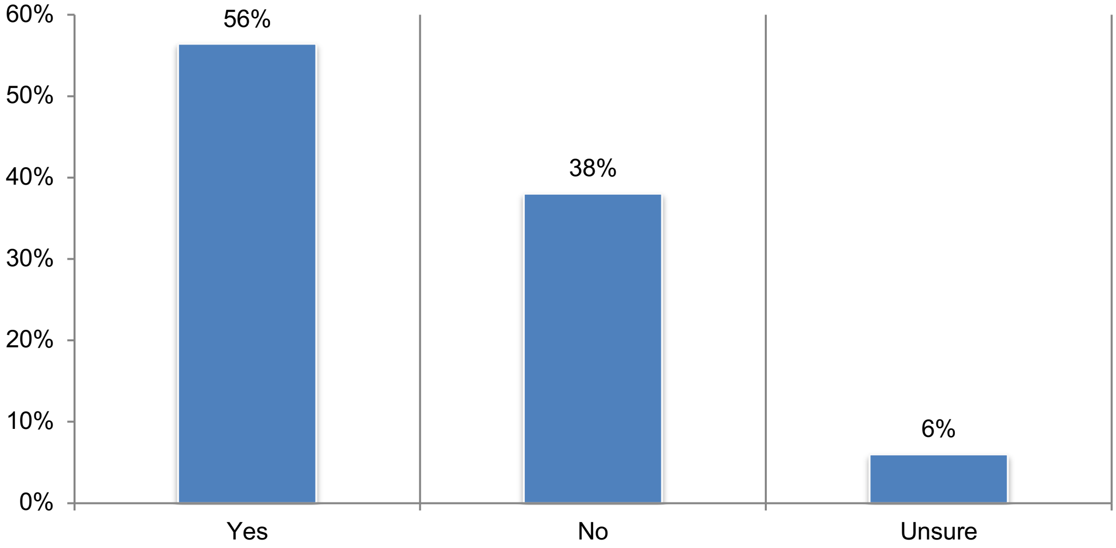
SMS codes sent to a mobile phone and hardware security tokens are the authentication technologies most often used in addition to passwords. According to Figure 13, the most frequently used authentication technology used are SMS codes (37 percent of respondents) followed by hardware security token (33 percent of respondents).

Figure 13. In addition to passwords, what authentication technologies do you or have you used?
More than one choice permitted



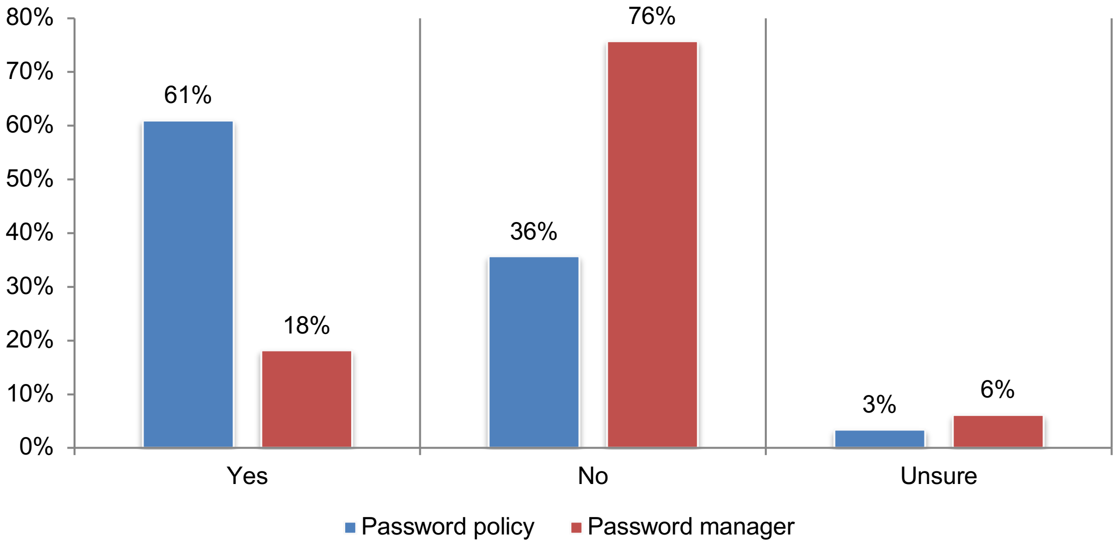
A preferred login is a physical hardware token. According to Figure 14, the majority of respondents for security purposes would prefer a physical hardware token for more secure login to business and/or personal accounts.

Figure 14. Would you feel you would get better security if offered a physical hardware token to login to business and/or personal accounts?



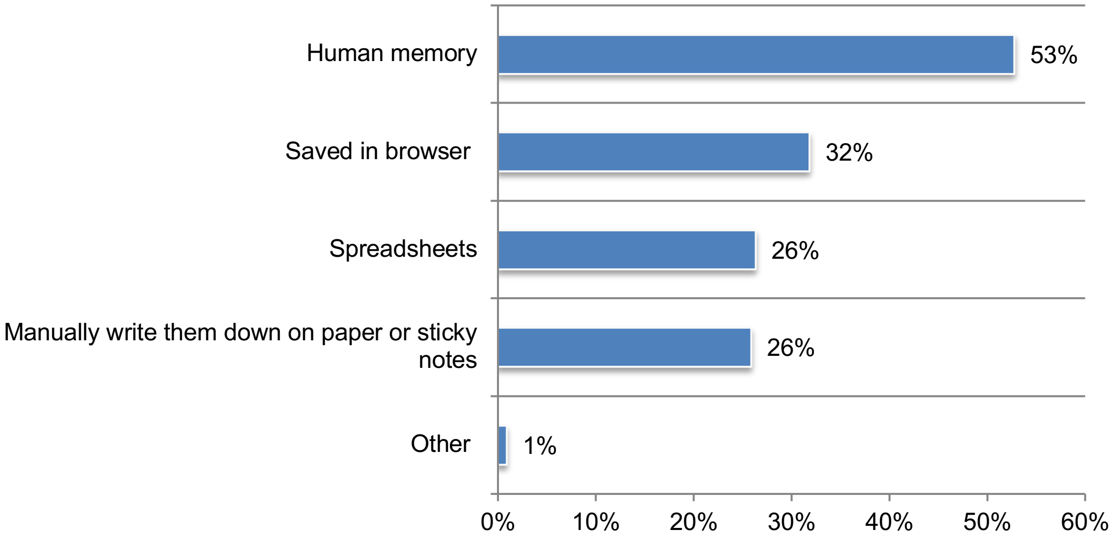
As shown in Figure 15, 61 percent of respondents say their organizations have a password policy. However, only 39 percent of respondents say the policy is strictly enforced. Only 18 percent of respondents say they require employees to use a password manager.

Figure 15. Does your organization have a password policy or require the use of a password manager?



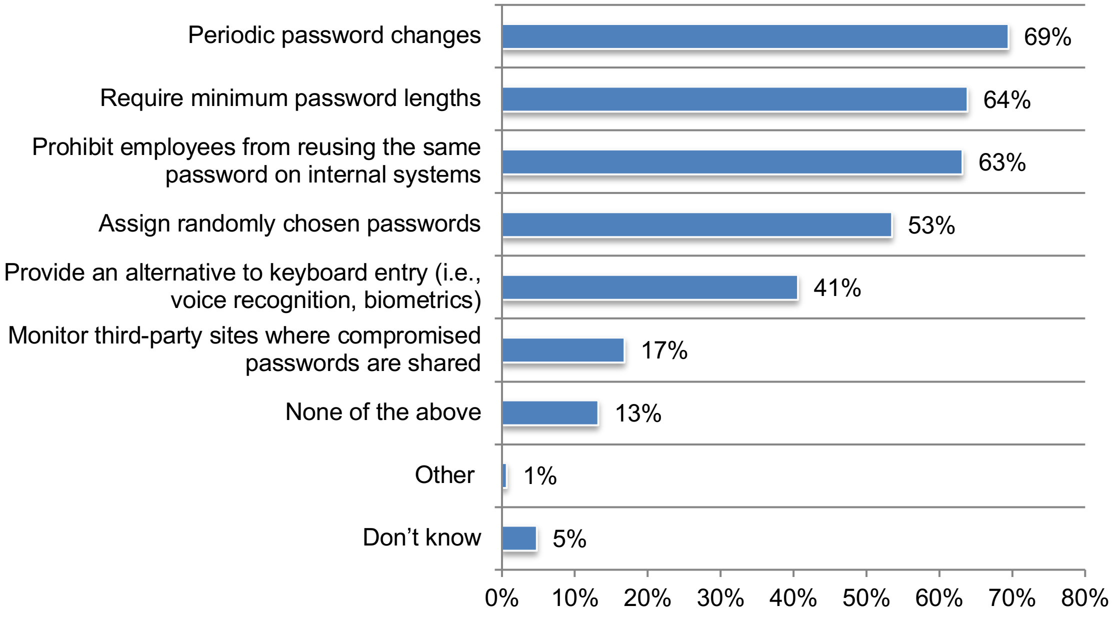
Human memory is most often used to manage and protect passwords. As shown in Figure 16, the most frequently used methods to protect passwords rely upon low or no tech methods as human memory, spreadsheets and sticky notes. Only 32 percent save passwords in browsers.

Figure 16. If password managers are not required, what does your organization use to manage and protect its passwords?
More than one choice permitted



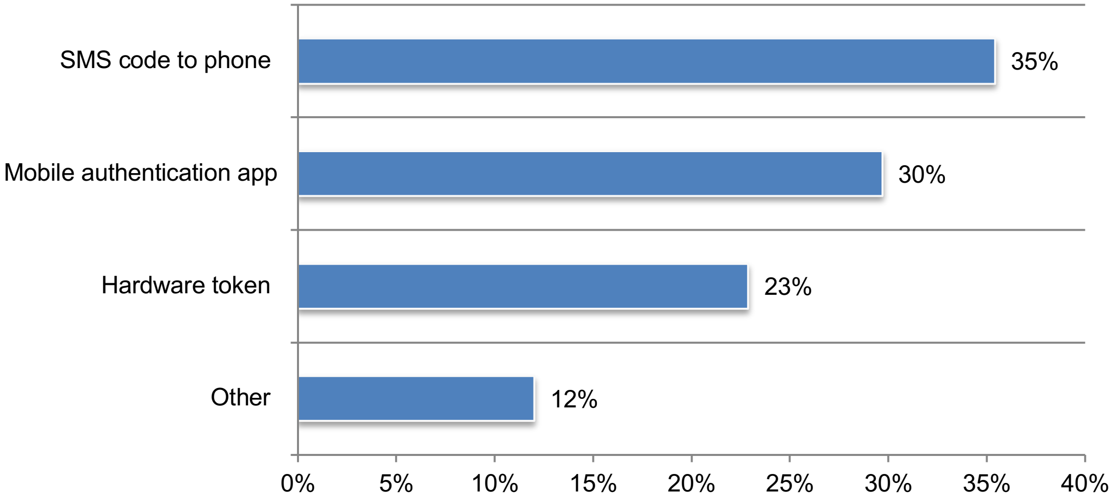
Periodic password changes and minimum password lengths are the steps most often taken by organizations to improve account security. As shown in Figure 17, 69 percent of respondents say their organizations require periodic password changes and 64 percent of respondents say they require minimum password lengths. Furthermore, 63 percent of respondents say their organizations prohibit them for reusing the same password on internal systems, yet 51 percent of respondents say they are reusing their passwords for business accounts.

Figure 17. Does your organization take any of the following steps?
More than one choice permitted



To control access to enterprise accounts, 45 percent of respondents say their organizations require employees to use two-factor or multi-factor authentication. According to Figure 18, SMS codes to phone and mobile authentication apps are the two types of two-factor authentication used most often in the workplace.

Figure 18. What type of two-factor authentication do you use in the workplace?
More than one choice permitted

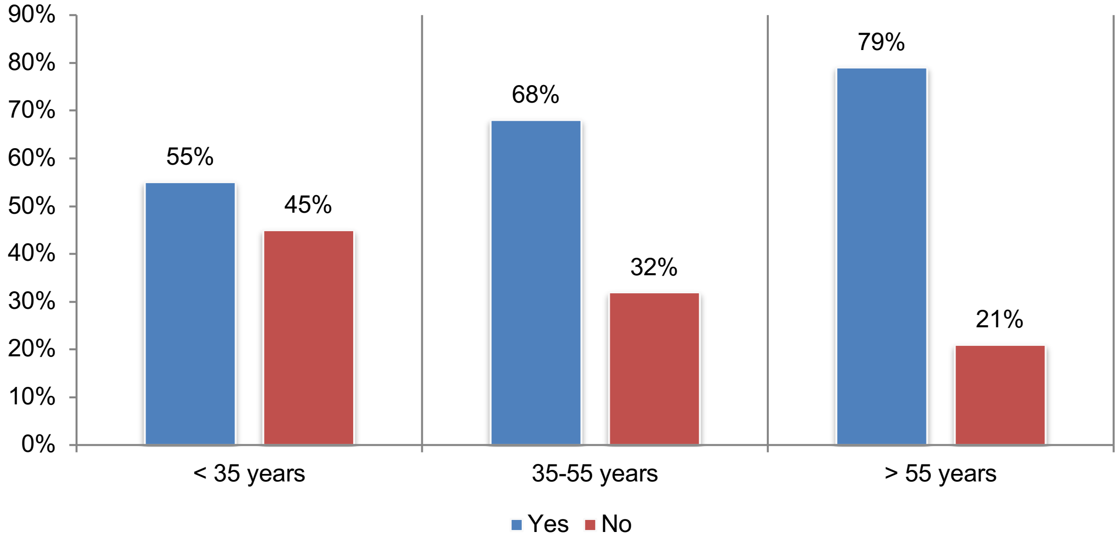


Differences in password practices and authentication by age

This section presents a special analysis of the findings according to the age of the respondent. Forty-five percent of respondents are 35 years or younger, 46 percent of respondents are between 35 and 55 years and 9 percent of respondents are 55 years or older.

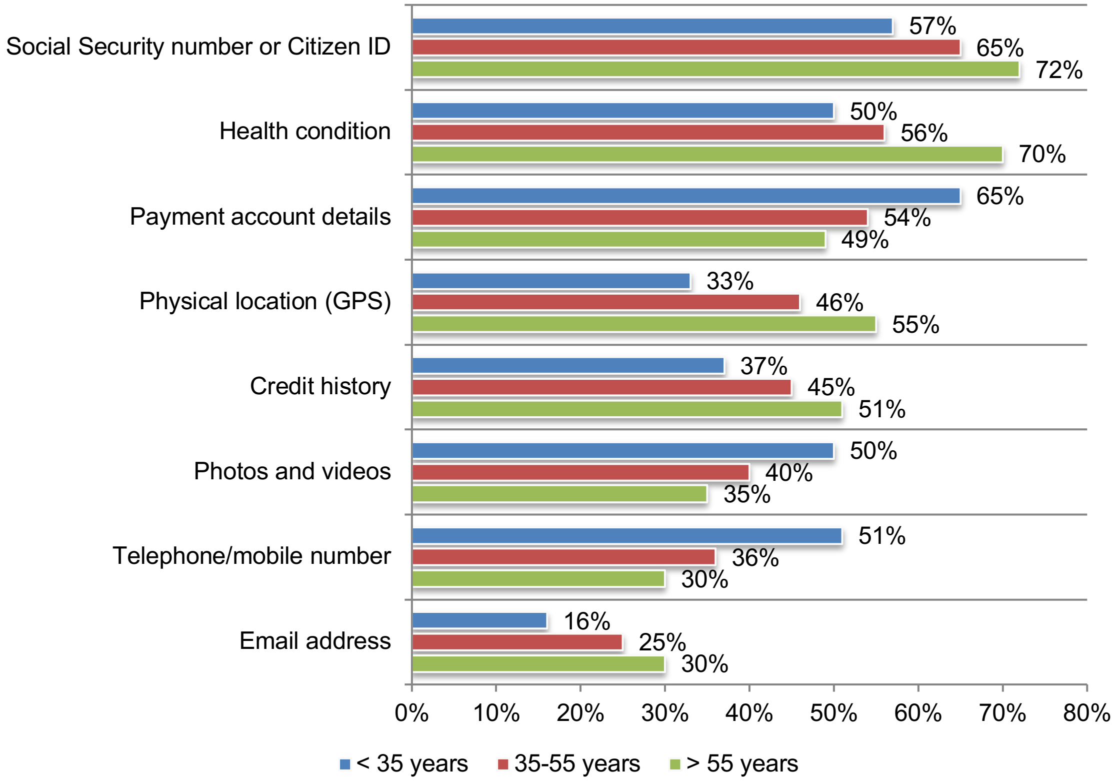
Younger respondents are less concerned about the privacy and security of their personal information than older respondents. Seventy-nine percent of respondents in the 55+ age say they are more concerned about their privacy, while only 55 percent of respondents 35 years and younger say they have become more concerned.

Figure 19. Have you become more concerned about the privacy and security of your personal information over the past two years?



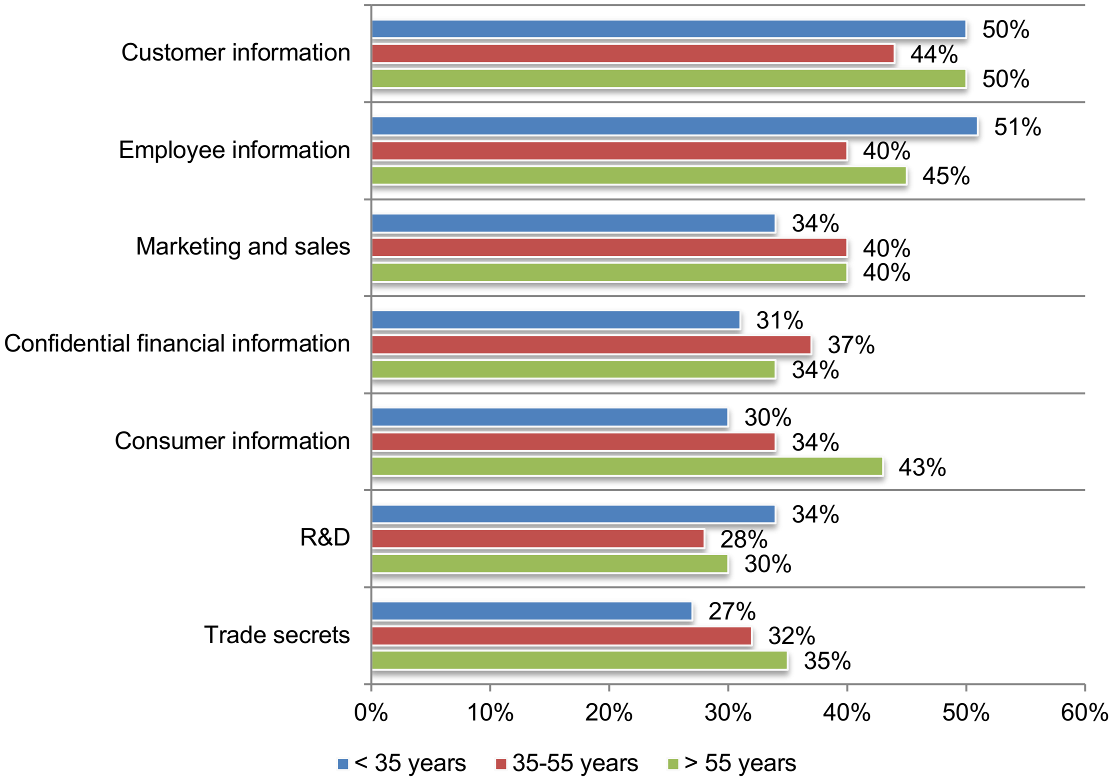
As shown in Figure 20, older respondents are more concerned about protecting their Social Security number or Citizen ID (72 percent of respondents) than younger respondents. Additionally, 70 percent are concerned about protecting health information, while only 50 percent of younger respondents are concerned about the protection of their health information. This could possibly be attributed to the fact that they typically require more medical attention than younger respondents. Younger respondents are more focused on protecting payment account details (65 percent) and telephone/mobile numbers (51 percent).

Figure 20. What personal information are you most concerned about protecting?
Five choices permitted



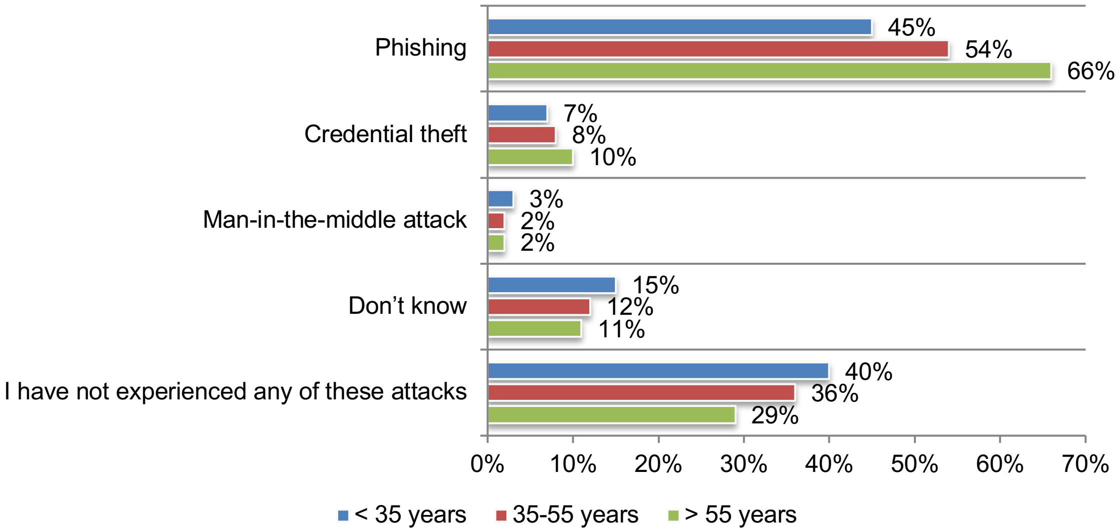
Both younger and older respondents agree that the business data that is most important to protect is customer information. Younger respondents are concerned about protecting employee information (51 percent) and customer information (50 percent). Of all the business data, older respondents believe it is most important to protect consumer information, as shown in Figure 21.

Figure 21. What business information are you most concerned about protecting?
Three choices permitted



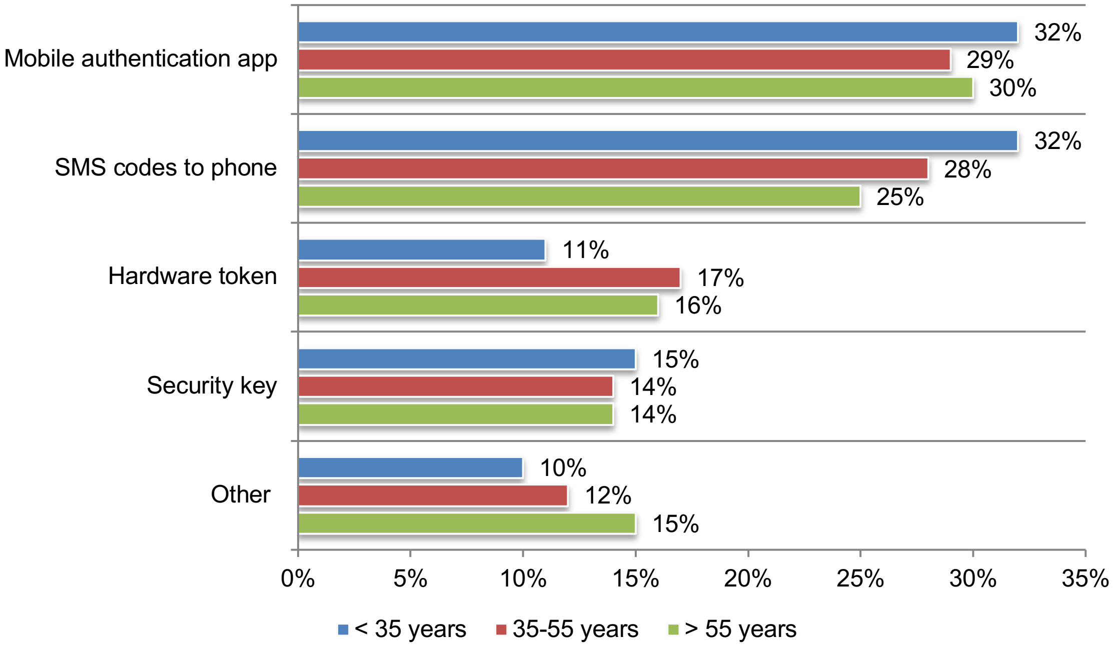
Older respondents are far more likely to have experienced a phishing attack. According to Figure 22, 66 percent of respondents who are older than 55 were victims of a phishing attack. In contrast, 40 percent of respondents 35 years or younger did not experience phishing, credential theft or a man-in-the-middle attack. While very few respondents report they experienced credential theft or a man-in-the-middle attack, it is important to note that it can be difficult to really know if they have been targeted by these attacks.

Figure 22. Have you ever experienced any of the following attacks?
More than one choice permitted



Mobile authentication apps are the most common type of two-factor authentication used by all age groups. According to Figure 23, younger respondents are most likely to use SMS codes as compared to other age groups.

Figure 23. What type of two-factor authentication do you use for personal reasons?

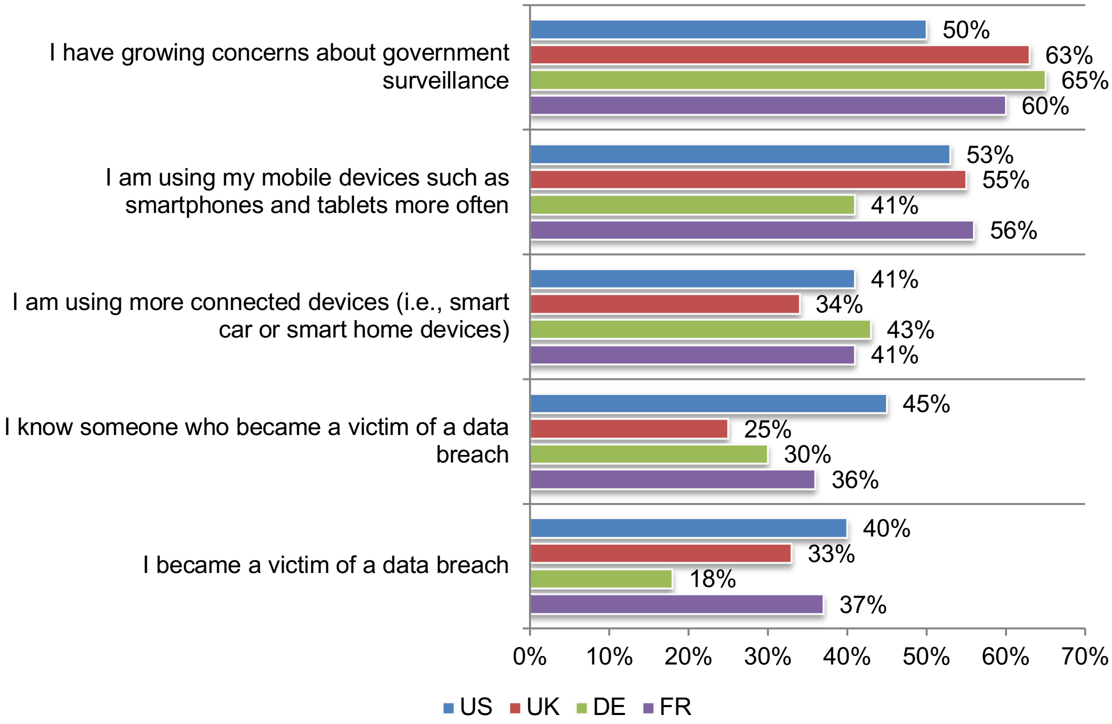


Country differences in password practices and authentication security behaviors

This section presents the most salient differences between respondents in the US (577 respondents), UK (404 respondents), Germany (400 respondents) and France (380 respondents).

Government surveillance is having the most impact on respondents' concerns about their privacy. Respondents in Germany are most concerned about government surveillance and respondents in the US are least concerned, as shown in Figure 24. The increasing use of mobile devices, such as smartphones and tablets, is also affecting respondents' concerns about their privacy, especially for those in the US, UK and France. With respect to data breaches, respondents in the US are far more likely to report that that they know someone who was a victim of a data breach or they were a victim of a data breach (45 percent). France is second at 36 percent of respondents. The UK is the lowest with only 25 percent of respondents saying they know someone who was a victim of a data breach or they were a victim.

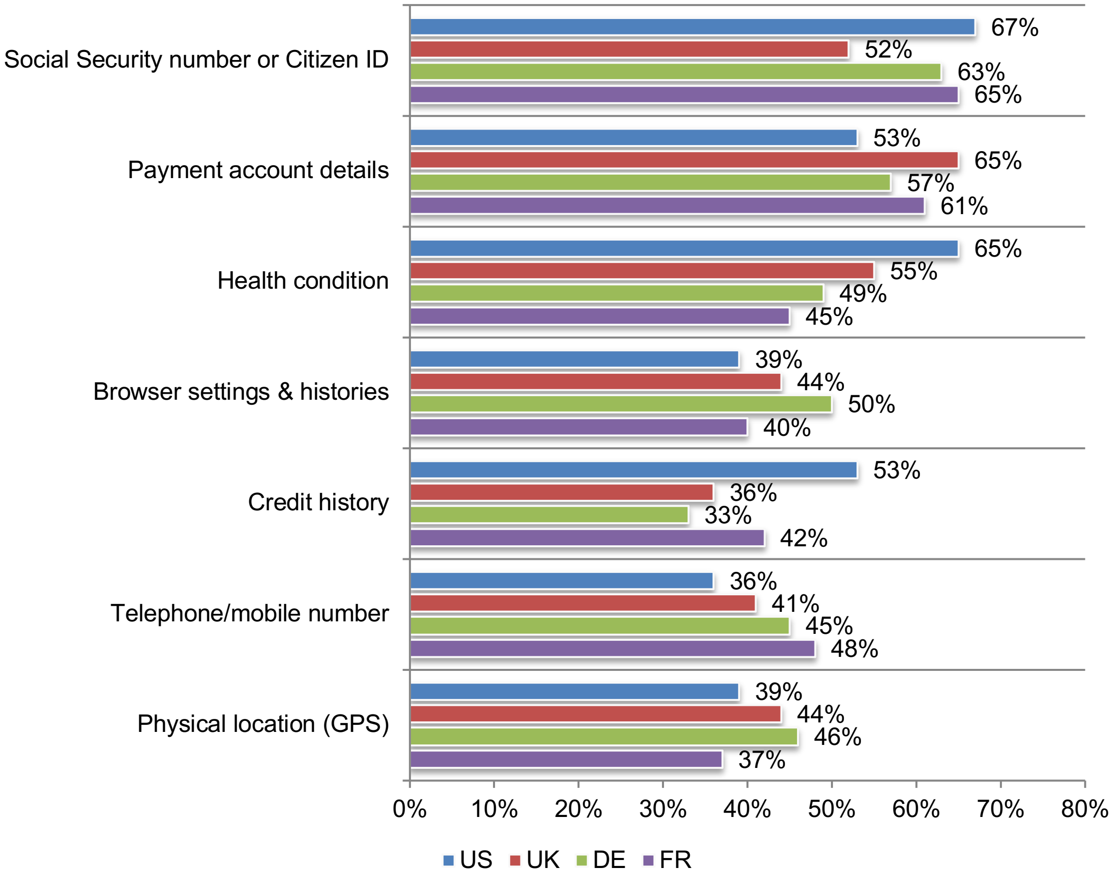
Figure 24. Why are you more concerned about your privacy?
More than one choice permitted



Social Security numbers, Citizen IDs, payment account details and information about health conditions are the types of personal information respondents in these countries are most concerned about protecting. According to Figure 25, respondents in the US are most concerned about safeguarding their Social Security number and information about their health. It is interesting to note that respondents in the US are much more concerned about credit history than respondents in other countries, which could be attributed to recent large-scale data impacting this type of information.

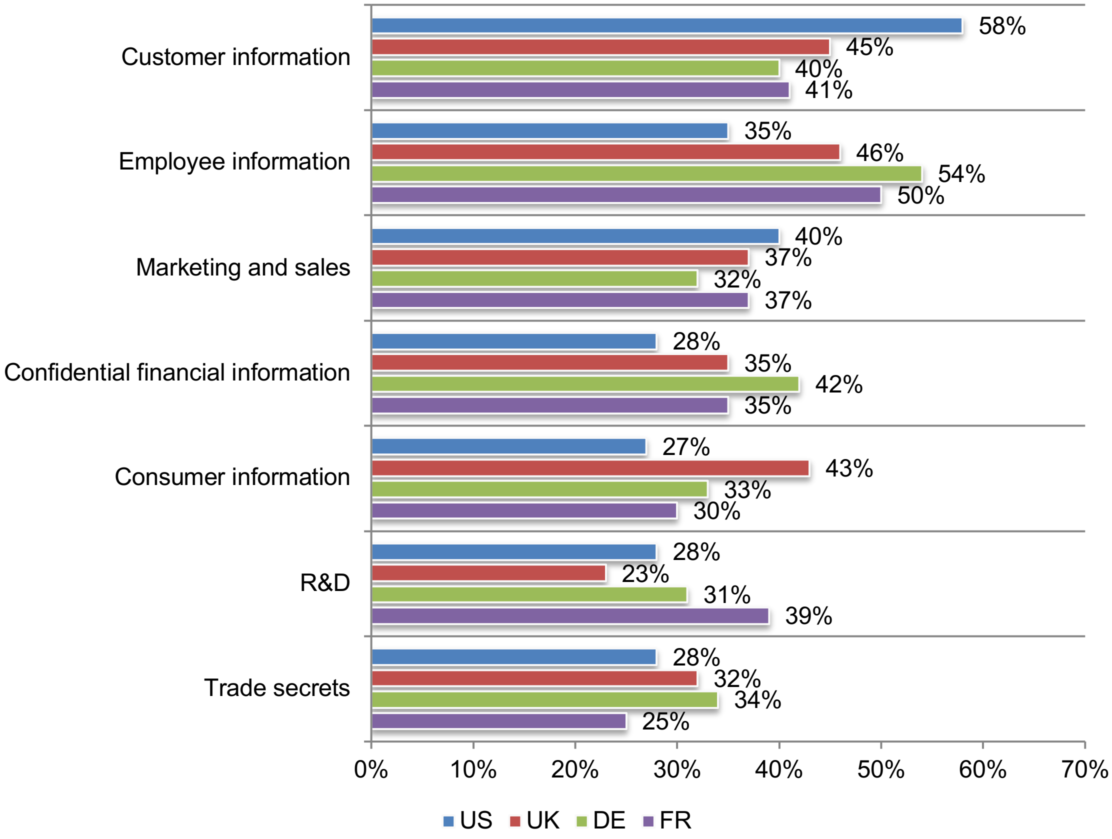
Respondents in the UK are concerned about protecting payment account details and their health information. German respondents are more concerned than others about browser settings and histories and French respondents are more likely to protect their telephone/mobile numbers.

Figure 25. What personal information are you most concerned about protecting?
Five choices permitted



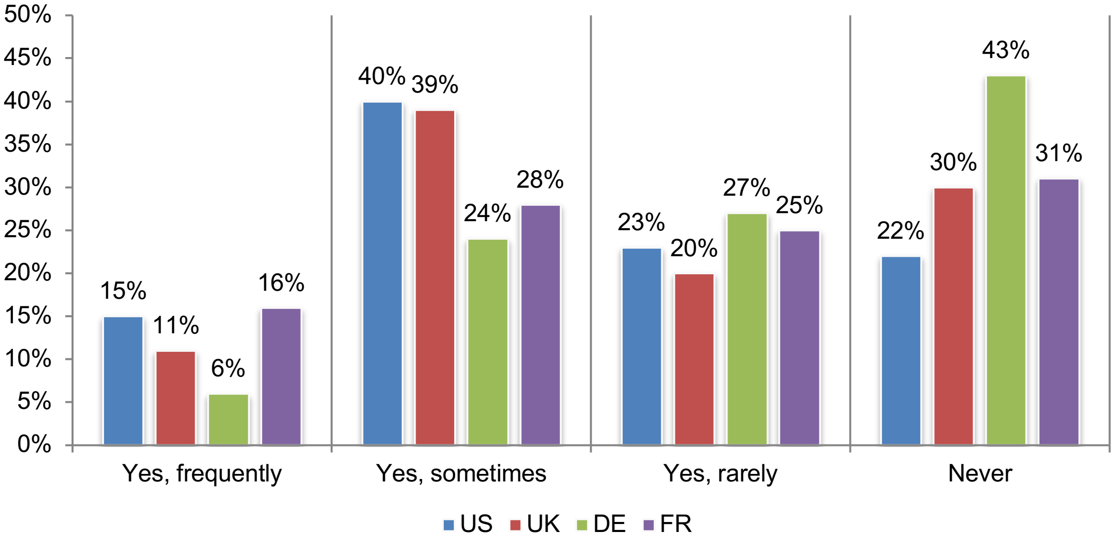
In the US, respondents are far more concerned with the protection of customer information than respondents in other countries. As shown in Figure 26, respondents in these four countries have different priorities as to what information should be protected. Respondents in the UK are more likely to protect consumer information and German respondents are more focused on protecting employee information. French respondents are concerned about the protection of research and development information.

Figure 26. What business information are you most concerned about protecting
Three choices permitted



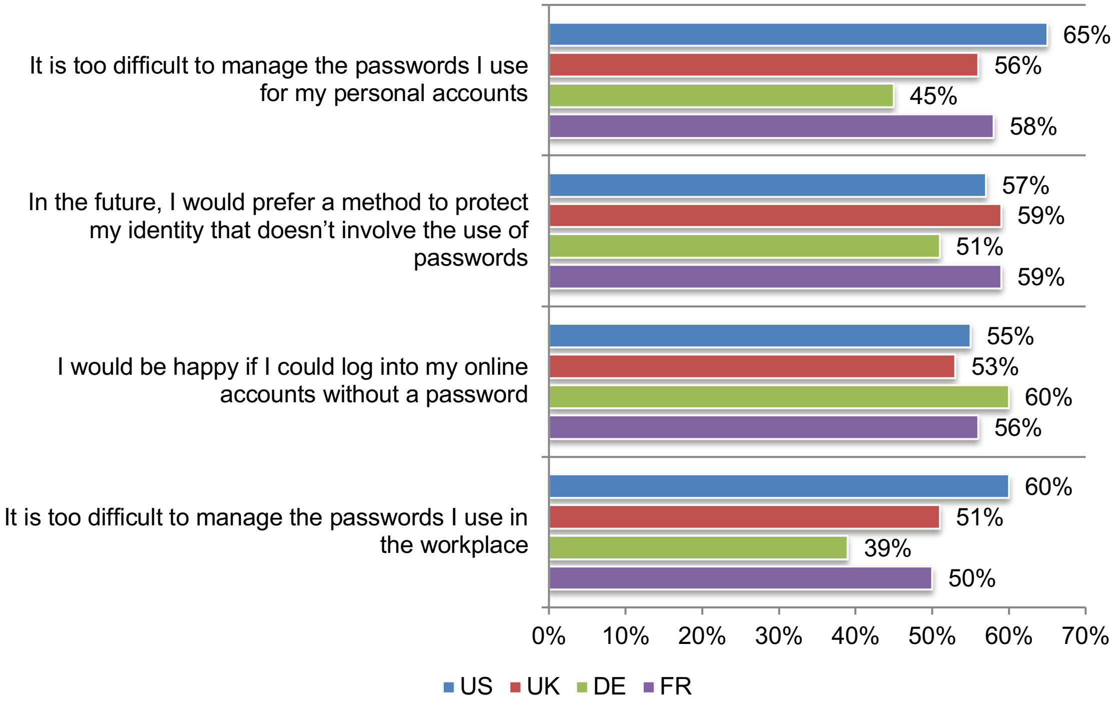
German respondents are least likely to share passwords with their colleagues. According to Figure 27, 55 percent of US respondents are most likely to share passwords frequently or sometimes. Only 30 percent of German respondents say they share passwords frequently or sometimes, and 43 percent of respondents never share their passwords.

Figure 27. Do you share passwords with colleagues



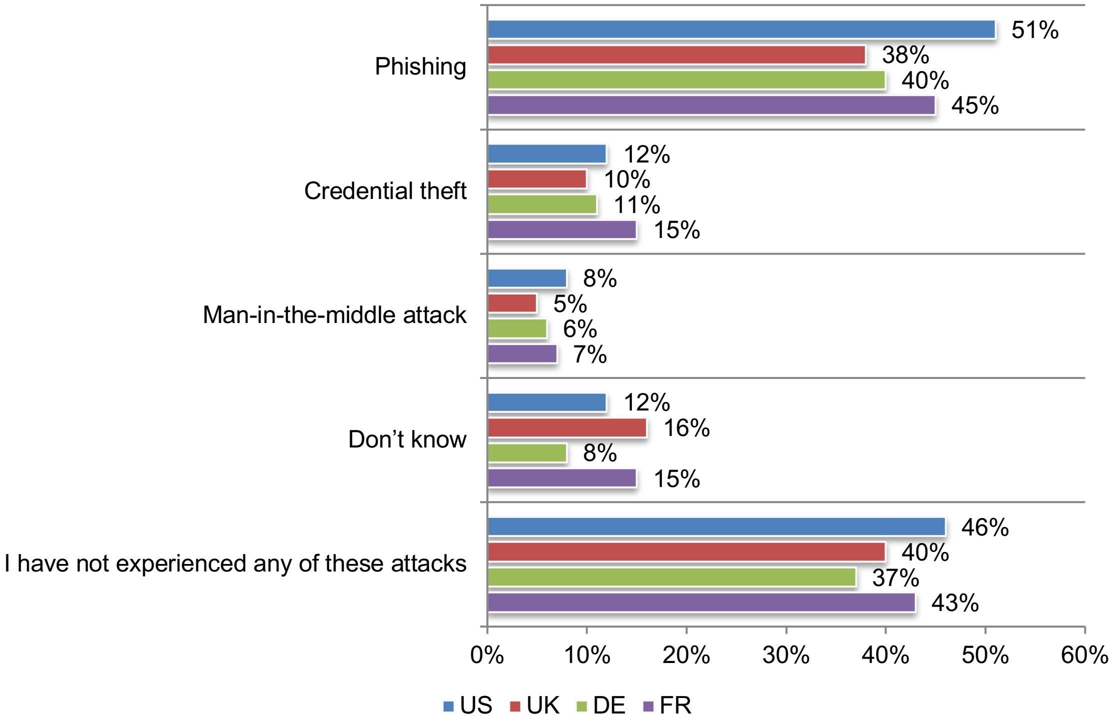
US respondents are most likely to say it is too difficult to manage the passwords used for personal accounts. As shown in Figure 28, US respondents are more likely to say it is difficult to manage passwords in their personal accounts (65 percent) or in the workplace (60 percent). In contrast, among all the countries, German respondents are least likely to think it is difficult to manage their passwords in their personal accounts (45 percent) and in the workplace (39 percent). Most respondents in all countries would prefer a method to protect their identity that doesn't involve the use of passwords.

Figure 28. Perceptions about password management and protection
Strongly agree and Agree responses combined



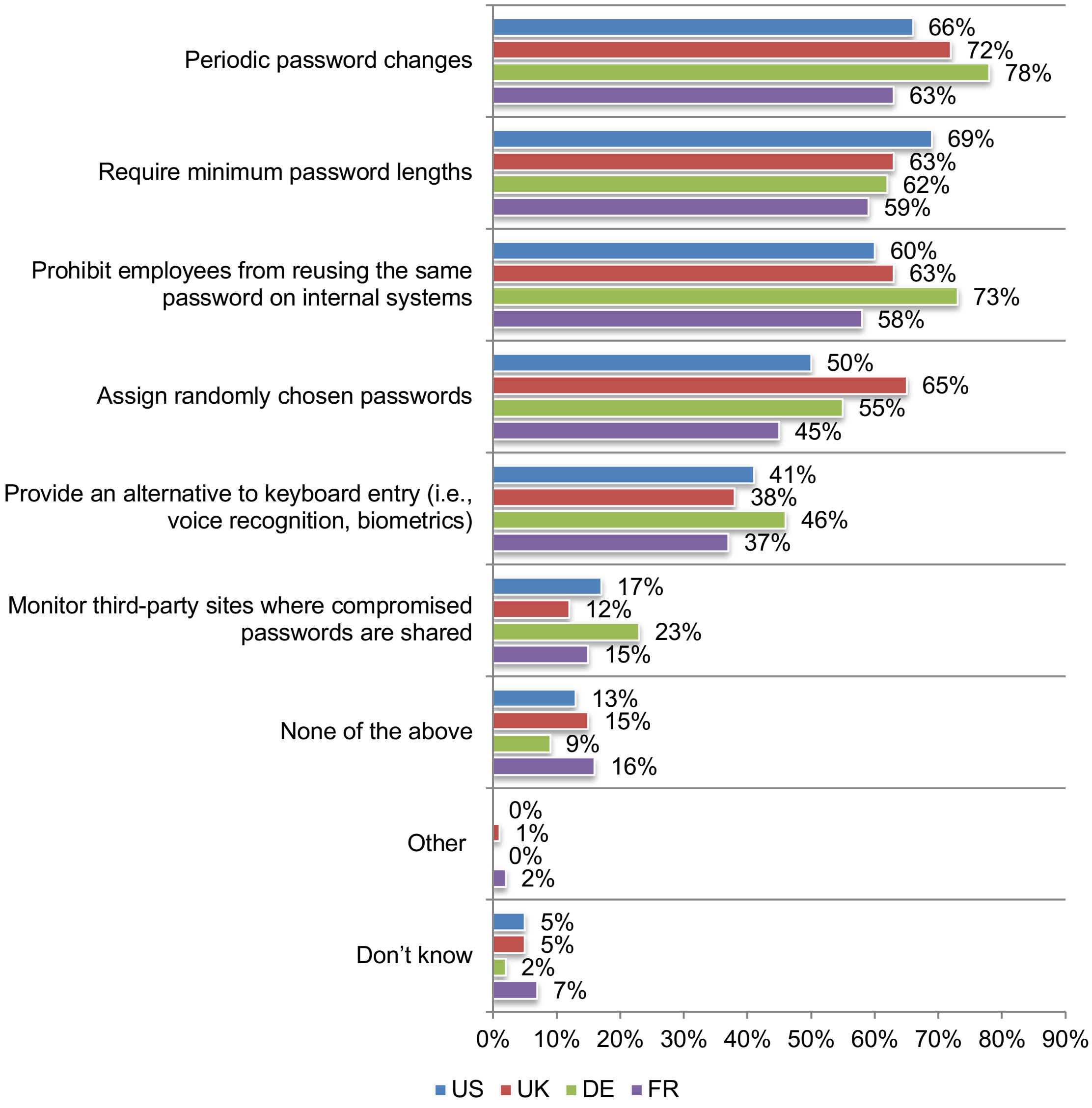
Phishing attacks are most prevalent in the US. According to Figure 29, 51 percent of respondents say they had a phishing attack in the workplace, but only 38 percent of the UK respondents report they had a phishing attack in the workplace. While very few respondents report they experienced credential theft or a man-in-the-middle attack, it is important to note that it can be difficult to know if they have been targeted by these attacks.

Figure 29. Have you experienced any of the following attacks in the workplace
More than one choice permitted



German organizations are most likely to require periodic password changes. Seventy-eight percent of respondents in Germany say they require employees to change their passwords periodically and 73 percent of these respondents say employees are prohibited from reusing the same password on internal systems. Sixty-five percent of UK respondents say their organizations randomly assign passwords.

Figure 30. Does your organization take any of the following steps to manage and protect passwords?
More than one choice permitted



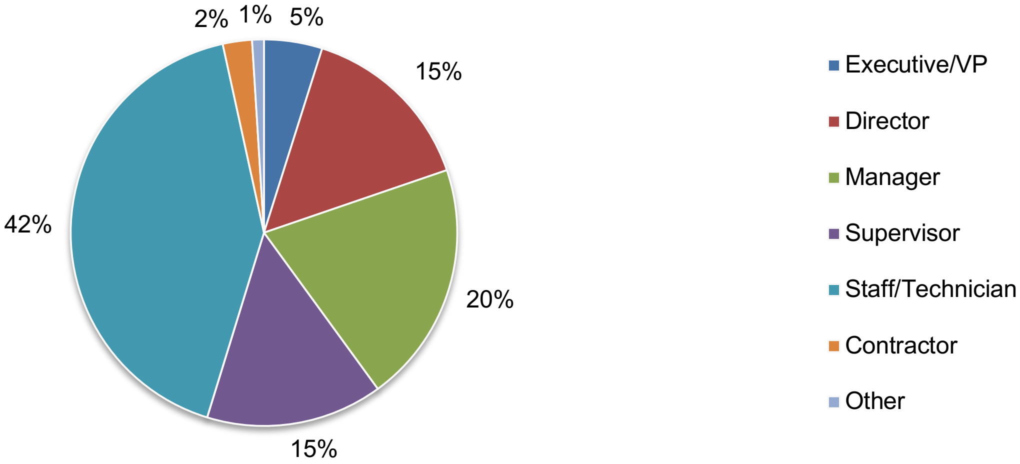
Part 3. Methods

A sampling frame of 51,207 IT or IT security practitioners located in the United States, the United Kingdom, Germany and France were selected as participants in the research. Table 2 shows that there were 1,972 total returned surveys. Screening and reliability checks led to the removal of 211 surveys. Our final sample consisted of 1,761 surveys, a 3.4 percent response.

Table 2. Sample response	Freq	Pct%
Sampling frame	51,207	100.0%
Total returns	1,972	3.9%
Rejected or screened surveys	211	0.4%
Final sample	1,761	3.4%

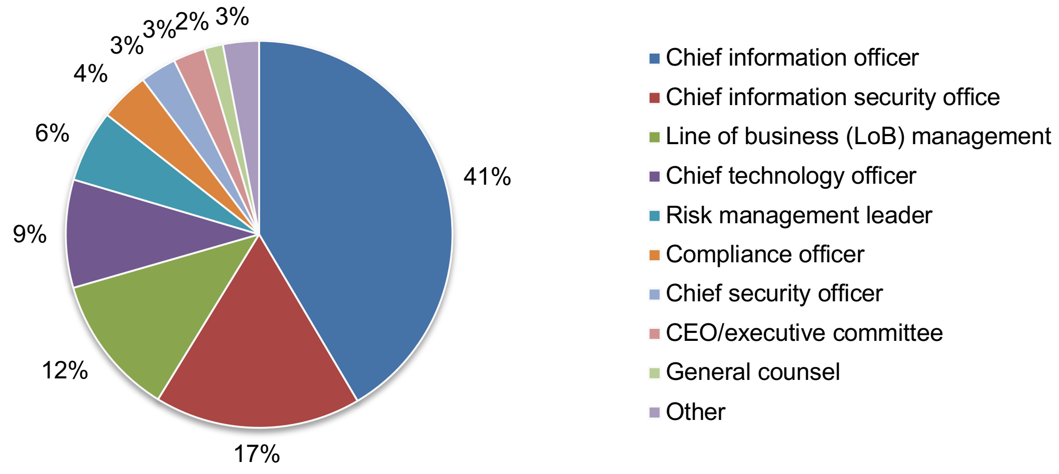
Pie Chart 1 reports the respondents' organizational level within participating organizations. By design, more than half of respondents (55 percent) are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



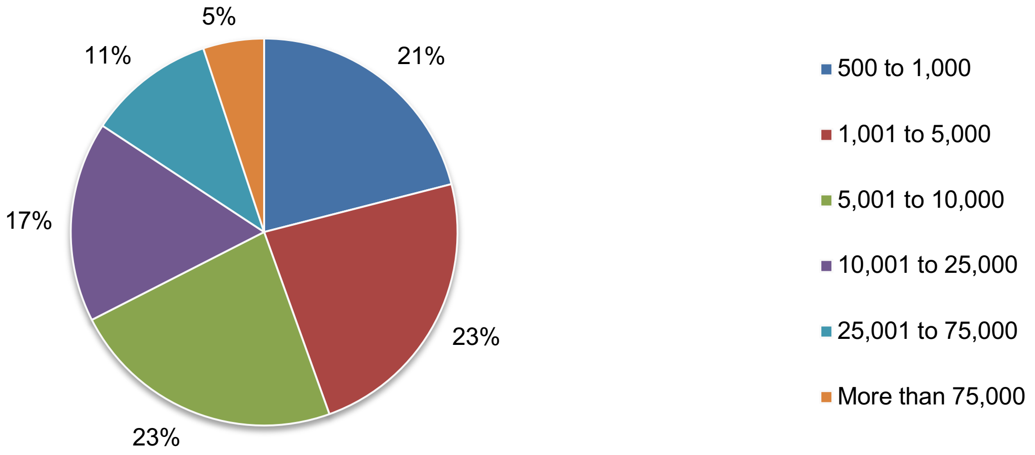
Pie Chart 2 identifies the primary person to whom the respondent reports. Forty-one percent of respondents identified the chief information officer as the person to whom they report. Another 17 percent indicated they report directly to the chief information security officer and 12 percent of respondents report to the lines of business leader.

Pie Chart 2. Distribution of respondents according to reporting channel



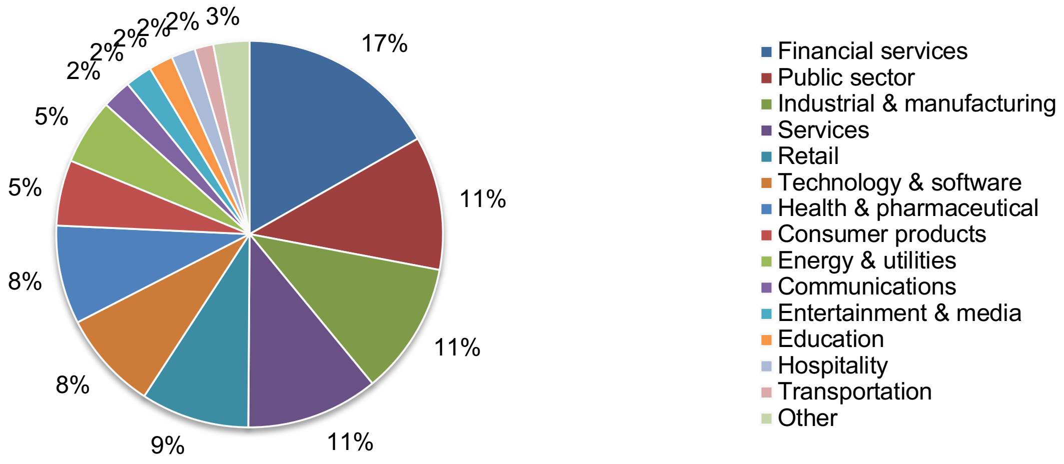
According to Pie Chart 3, more than half of the respondents (56 percent) are from organizations with a global headcount of more than 5,000 employees.

Pie Chart 3. Distribution of respondents according to full-time global head count



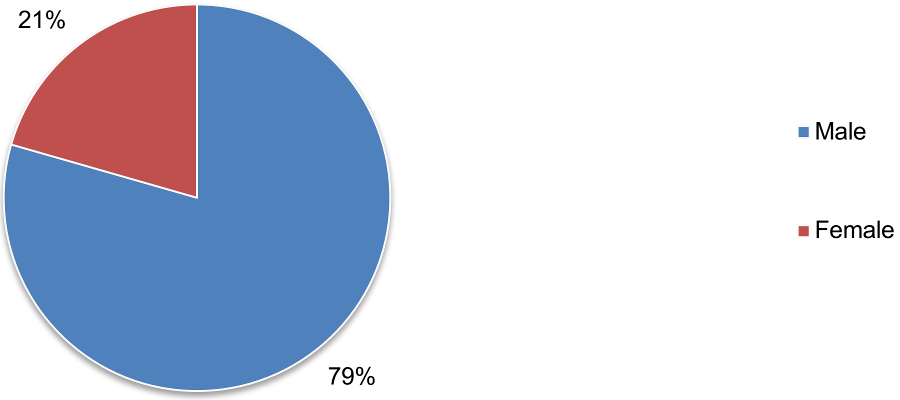
Pie Chart 4 reports the primary industry classification of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, followed by public sector (11 percent of respondents), industrial/manufacturing (11 percent of respondents), services sector (11 percent of respondents), and retail (9 percent of respondents).

Pie Chart 4. Distribution of respondents according to primary industry classification



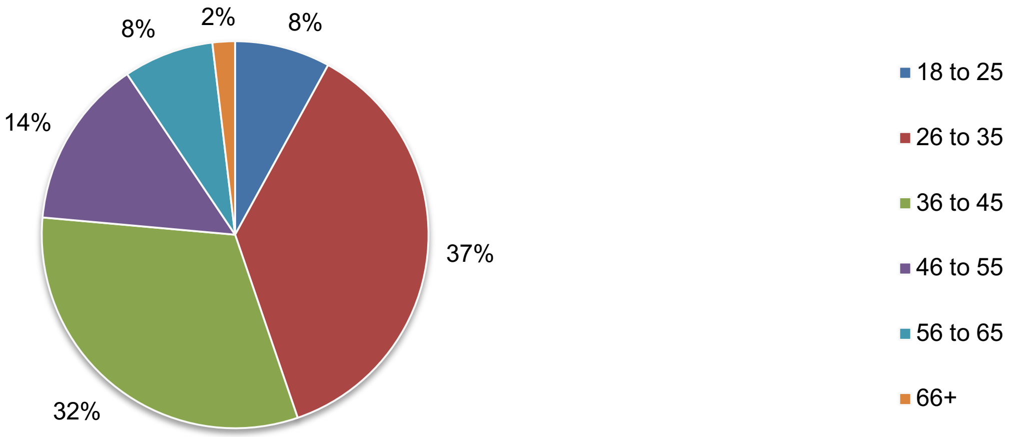
Seventy-nine percent of respondents are male and twenty-one percent of respondents are female, as shown in Pie Chart 5.

Pie Chart 5. Distribution of respondents according to gender



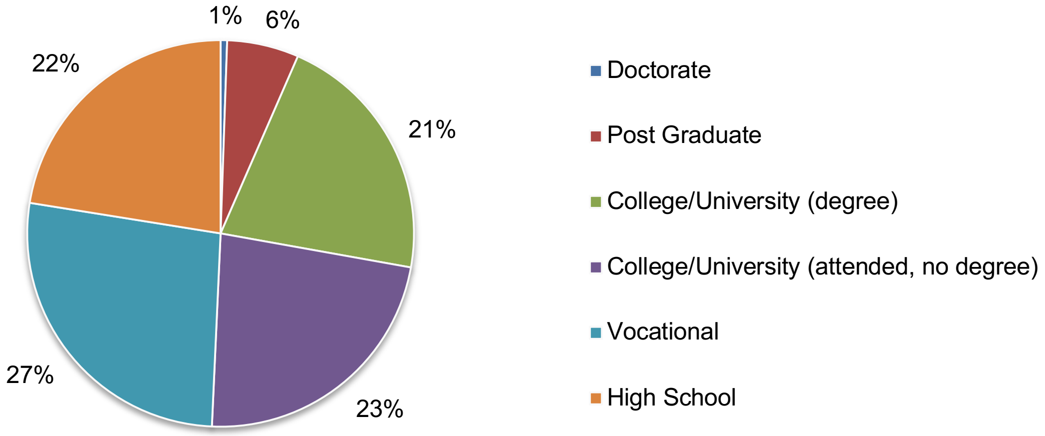
As shown in Pie Chart 6, the majority of respondents (69 percent) are between the ages of 26 and 45.

Pie Chart 6. Distribution of respondents according to age range



Pie Chart 7 reports the respondents' highest level of education. More than half of respondents (51 percent) have at least attended a college or university (23 percent of respondents), earned a degree (21 percent of respondents), completed post graduate education (6 percent of respondents) or doctoral education (1 percent of respondents).

Pie Chart 7. Distribution of respondents according to highest level of education



Part 4. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners in various organizations the United States, the United Kingdom, Germany and France. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured August 20 to September 4, 2018.

Survey response	Total
Total sampling frame	51,207
Total returns	1,972
Rejected surveys	211
Final sample	1,761
Response rate	3.4%
Sample weights	1.00

Part 1. The impact of privacy and security concerns on password and authentication practices

Q1a. Have you become more concerned about the privacy and security of your personal data over the past two years?	Total
Yes	63%
No	37%
Total	100%

Q1b. If yes, why are you more concerned? Please select all that apply.	Total
I became a victim of a data breach	33%
I became a victim of identity theft	8%
I have growing concerns about government surveillance	59%
I use social media more often	21%
I am using location tracking devices more often	20%
I am using more connected devices (i.e., smart car or smart home devices)	40%
I know someone who became a victim of a data breach	35%
I am using my mobile devices such as smartphones and tablets more often	51%
I use mobile payment methods including mobile wallet	29%
More of my personal information, including medical records, is being shared with third parties	27%
Total	323%

Q2. Have you ever been the victim of identity theft or had fraudulent changes on your bank statement due to someone accessing your account credentials?	Total
Yes	23%
No	65%
Don’t know	13%
Total	100%

Q3. Have you ever been the victim of an account takeover or hacking of a personal account?	Total
Yes	19%
No	67%
Don’t know	14%
Total	100%

Q4a. What personal information are you most concerned about protecting? Please select your top 5 choices.	Total
Browser settings & histories	43%
Credit history	42%
Email address	21%
Health condition	55%
Home address	29%
Marital status	11%
Telephone/mobile number	42%
Name	24%
Payment account details	58%
Photos and videos	44%
Physical location (GPS)	41%
Social Security number or Citizen ID	62%
Gender	8%
Other (please specify)	1%
None of the above	18%
Total	500%

Q4b. What business information are you most concerned about protecting? Please check your top 3 choices.	Total
Customer information	47%
Consumer information	33%
Confidential financial information	34%
Trade secrets	30%
R&D	30%
Marketing and sales	37%
Healthcare	23%
Employee information	45%
Other (please specify)	1%
None of the above	20%
Total	300%

Q5. Do you share passwords with colleagues to access accounts?	Total
Yes, frequently	12%
Yes, sometimes	34%
Yes, rarely	24%
Never	31%
Total	100%

Q6. How much time do you spend each week entering and/or resetting your passwords?	Total
Less than 5 minutes	16%
6 to 10 minutes	24%
11 to 20 minutes	23%
21 to 45 minutes	20%
46 minutes to 1 hour	14%
2 to 4 hours	2%
More than 4 hours	0%
Total	100%
Extrapolated value (minutes each week)	24.91

Q7. In addition to passwords, what authentication technologies do you or have you used? Please select one best choice.	Total
SMS codes to phone	37%
Hardware security token	33%
Authenticator app	21%
Other (please specify)	10%
Total	100%

Q8. Would you feel you were getting better security if you were offered a physical hardware token to login to business and/or personal accounts?	Total
Yes	56%
No	38%
Unsure	6%
Total	100%

Part 2. Attributions: Please respond to each statement using the five-point scale from strongly agree to strongly disagree. **Strongly Agree and Agree response combined**	Total
Q9. It is very important to protect the passwords I use in the workplace.	66%
Q10. It is very important to protect passwords I use on my personal devices.	63%
Q11. It is important to make all my passwords different.	55%
Q12. It is too difficult to manage the passwords I use in the workplace.	51%
Q13. It is too difficult to manage the passwords I use for my personal accounts.	57%
Q14. In the future, I would prefer a method to protect my identity that doesn't involve the use of passwords.	57%
Q15. I would be happy if I could log into my online accounts without a password.	56%

Part 3. Authentication and account security in organizations

Q16. Have you shared **your** passwords with others in the workplace?	Total
Yes	31%
No	69%
Total	100%

Q17a. Do you reuse passwords across any of your business and/or personal accounts?	Total
Yes	51%
No (skip to Q18)	49%
Total	100%

Q17b. If yes, how many passwords do you reuse?	Total
1 to 3	28%
4 to 6	46%
More than 6	26%
Total	100%
Extrapolated value	4.69

Q18. Have you experienced any of the following attacks in the workplace? Please select all that apply.	Total
Phishing	44%
Credential theft	12%
Man-in-the-middle attack	7%
Don't know	13%
I have not experienced any of these attacks	42%
Total	117%

Q19a. Have you experienced any of the following attacks in your personal life? Please select all that apply.	Total
Phishing	51%
Credential theft	8%
Man-in-the-middle attack	2%
Don't know	13%
I have not experienced any of these attacks	37%
Total	111%

Q19b. If you experienced any of these attacks did it change how you manage your passwords?	Total
Yes	43%
No	57%
Total	100%

Q19c. If yes, did you take any of these steps?	Total
I now use stronger passwords	47%
I change passwords more frequently	43%
I now use a different and unique password for every account	17%
I added two/multi-factor authentication where possible	41%
Other (please specify)	1%
None of the above	19%
Total	167%

Q20. Are your colleagues careful not to fall for phishing scams?	Total
Yes	43%
No	51%
Unsure	6%
Total	100%

Q21a. Does your organization have a policy pertaining to employees' use of passwords?	Total
Yes	61%
No	36%
Unsure	3%
Total	100%

Q21b. If yes, does your organization strictly enforce this policy?	Total
Yes	39%
No	56%
Unsure	5%
Total	100%

Q22a. Does your organization require employees to use a password manager?	Total
Yes	18%
No	76%
Unsure	6%
Total	100%

Q22b. If no, what does your organization use to manage and protect its passwords?	Total
Spreadsheets	26%
Manually write them down on paper or sticky notes	26%
Human memory	53%
Browser extension	32%
Other (please specify)	1%
Total	138%

Q23. Does your organization take any of the following steps? Please select all that apply.	Total
Periodic password changes	69%
Assign randomly chosen passwords	53%
Require minimum password lengths	64%
Prohibit employees from reusing the same password on internal systems	63%
Provide an alternative to keyboard entry (i.e., voice recognition, biometrics)	41%
Monitor third-party sites where compromised passwords are shared	17%
None of the above	13%
Other (please specify)	1%
Don't know	5%
Total	5%

Q24a. Does your organization require you to use two-factor or multi-factor authentication?	Total
Yes	45%
No	55%
Total	100%

Q24b. If yes, what type of two-factor authentication do you use in the workplace? Please select one best choice.	Total
SMS codes to phone	35%
Mobile authentication app	30%
Hardware token (e.g., RSA keyfob)	23%
Other (please specify)	12%
Total	100%

Q25a. Do you use two-factor authentication for personal use?	Total
Yes	33%
No	67%
Total	100%

Q25b. If yes, what type of two-factor authentication do you use for personal reasons? Please select one best choice.	Total
SMS codes to phone	27%
Mobile authentication app	31%
Security key	15%
Hardware token/security key	15%
Other (please specify)	11%
Total	100%

Q26. Have you ever lost or broken your mobile phone?	Total
Yes	52%
No	48%
Total	100%

Q27. Is it acceptable for online services to use biometrics such as your voice or fingerprints to verify your identity?	Total
Yes	42%
Yes, but only if the biometric data is not accessible to the organization	41%
No	14%
Unsure	4%
Total	100%

Q28. Are you worried about your biometrics (i.e., facial scan or fingerprints) being stolen or biometric data leaked in a breach?	Total
Yes	42%
No	58%
Total	100%

Q29a. Have you ever wanted to perform an online transaction, such as buying a product or service, but couldn't do so because you forgot your password?	Total
Very frequently	11%
Frequently	22%
Not frequently	29%
Rarely	18%
Never	20%
Total	100%

Q29b. Have you ever wanted to perform an online transaction, such as buying a product or service, but couldn't do so because you did not have access to your phone to receive a code for verification or use an authenticator app?	Total
Very frequently	6%
Frequently	20%
Not frequently	21%
Rarely	34%
Never	20%
Total	100%

Q29c. If either situation happened very frequently or frequently, how frustrated were you?	Total
Very frustrated	31%
Frustrated	35%
Somewhat frustrated	17%
Not frustrated	18%
Total	100%

Q30a. Have you ever needed access to information critical for your work but couldn't do so because of a forgotten password?	Total
Very frequently	12%
Frequently	30%
Not frequently	19%
Rarely	21%
Never	17%
Total	100%

Q30b. Have you ever needed access to information critical for your work but couldn't do so because you didn't have access to your phone to either receive a code for verification or use an authenticator app?	Total
Very frequently	19%
Frequently	29%
Not frequently	21%
Rarely	16%
Never	16%
Total	100%

Q30c. If you answered very frequently or frequently to either situation, how frustrated were you?	Total
Very frustrated	31%
Frustrated	31%
Somewhat frustrated	21%
Not frustrated	17%
Total	100%

Part 3. Organizational Characteristics

D1. What best describes your position level within the organization?	Total
Executive/VP	5%
Director	15%
Manager	20%
Supervisor	15%
Staff/Technician	42%
Contractor	2%
Other (please specify)	1%
Total	100%

D2. To whom do you report to within the organization?	Total
CEO/executive committee	3%
Chief operating officer	1%
Chief financial officer	1%
Chief information security office	17%
Chief security officer	3%
Chief information officer	41%
Chief technology officer	9%
General counsel	2%
Compliance officer	4%
Risk management leader	6%
Line of business (LoB) management	12%
Other (please specify)	1%
Total	100%

D3. What range best describes the full-time headcount of your global organization?	Total
500 to 1,000	21%
1,001 to 5,000	23%
5,001 to 10,000	23%
10,001 to 25,000	17%
25,001 to 75,000	11%
More than 75,000	5%
Total	100%

D4. What best describes your organization's primary industry classification?	Total
Agriculture & food services	1%
Communications	2%
Construction & real estate	1%
Consumer products	5%
Defense & aerospace	1%
Education	2%
Energy & utilities	5%
Entertainment & media	2%
Financial services	17%
Health & pharmaceutical	8%
Hospitality	2%
Industrial & manufacturing	11%
Public sector	11%
Retail	9%
Services	11%
Technology & software	8%
Transportation	2%
Other (please specify)	0%
Total	100%

Personal Demographics

D5. Gender	Total
Male	79%
Female	21%
Total	100%

D6. Age range	Total
18 to 25	8%
26 to 35	37%
36 to 45	32%
46 to 55	14%
56 to 65	8%
66+	2%
Total	100%

D7. Highest Level of Education:	Total
High School	22%
Vocational	27%
College/University (attended, no degree)	23%
College/University (degree)	21%
Post Graduate	6%
Doctorate	1%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.