Ponemon INSTITUTE

The 2020 State of Password and Authentication Security Behaviors Report

Research sponsored by Yubico

Independently Conducted by Ponemon Institute LLC

February 2020

The 2020 State of Password and Authentication Security Behaviors Report

Ponemon Institute, February 2020

Part 1. Introduction

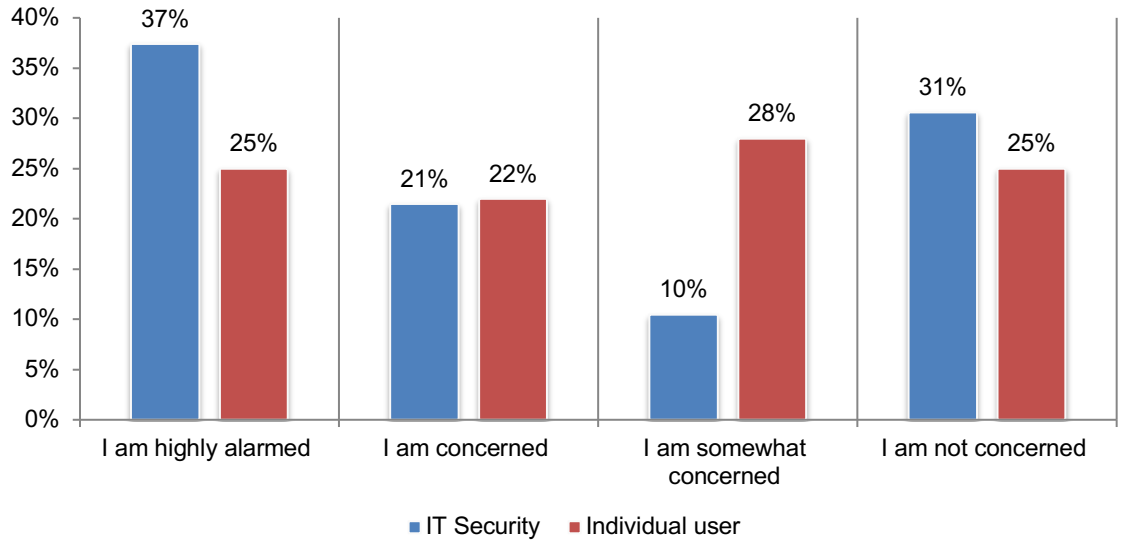
Cyber threats and attacks on individual users and organizations have not diminished. Phishing scams, stolen credentials, and account takeovers continue to rise, making it imperative for businesses to have policies and practices in place to reduce the risks created by poor password and authentication behaviors. What is perhaps more important is that the security policies and practices being deployed by businesses align with the preferences and behaviors of employees and customers (hereafter referred to as individual users). Without user adoption, businesses will remain vulnerable to cyber threats.

Ponemon Institute presents the results of *The 2020 State of Password and Authentication Security Behaviors Report,* sponsored by Yubico. Ponemon Institute surveyed 2,507 IT and IT security practitioners (hereafter referred to as IT security respondents) in the United States, United Kingdom, Germany, France, Sweden and Australia. This year, we also surveyed 563 Individual users to better understand the differences in security behaviors and preferences between IT security practitioners and Individuals.

Contrary to popular belief, IT security professionals— who we'd expect to take the utmost precaution when it comes to security—aren't much better than the individual users represented in this study. In fact, both groups are engaging in risky practices, including reusing and sharing passwords in the workplace and accessing workplace apps from their personal mobile devices without using two-factor authentication (2FA).

IT security professionals are more concerned about the privacy and security of their personal information than Individuals. As shown in Figure 1, 37 percent of IT security respondents are highly alarmed about possible risks to the security of their personal information. Individuals are more likely to be "only somewhat concerned". These differences can perhaps be explained by the fact that IT security respondents are in the trenches protecting their organizations from attacks and, therefore, better understand the current threat landscapes.

Figure 1. Have you become more concerned about the privacy and security of your personal data over the past two years?



Following are the most salient findings of this research.

- Individuals report better security practices in some instances compared to IT professionals. Out of the 35 percent of Individuals who report that they have been victim of an account takeover, a whopping 76 percent changed how they managed their passwords or protected their accounts. Of the 20 percent of IT security respondents who have been a victim of an account takeover, 65 percent changed how they managed their passwords or protected their accounts. Both Individuals and IT security respondents have reused passwords on an average of 10 of their personal accounts, but individual users (39 percent) are less likely to reuse passwords across workplace accounts than IT security respondents (50 percent)

- Fifty-one percent of IT security respondents say their organizations have experienced a phishing attack, with another 12 percent of respondents stating that their organizations experienced credential theft and 8 percent say it was a man-in-the-middle attack. Yet, only 53 percent of IT security respondents say their organizations have changed how passwords or protected corporate accounts were managed. Interestingly enough, Individuals reuse passwords across an average of 16 workplace accounts and IT security respondents say they reuse passwords across an average of 12 workplace accounts.

- Additionally, mobile use is on the rise. Fifty-five percent of IT security respondents report that the use of personal mobile devices is permitted at work and an average of 45 percent of employees in the organizations represented are using their mobile device for work. Alarmingly, 62 percent of IT security respondents say their organizations don't take necessary steps to protect information on mobile phones. Fifty-one percent of Individuals use their personal mobile device to access work related items, and of these, 56 percent don't use 2FA.

- Given the complexities of securing a modern, mobile workforce, organizations struggle to find simple, yet effective ways of protecting employee access to corporate accounts. Forty-nine percent of IT security respondents and 51 percent of Individuals share passwords with colleagues to access business accounts. Fifty-nine percent of IT security respondents report that their organization relies on human memory to manage passwords, while 42 percent say sticky notes are used. Only 31 percent of IT security respondents say that their organization uses a password manager, which are effective tools to securely create, manage and store passwords.

- IT security respondents say they are most concerned about protecting customer information and personally identifiable information (PII). However, 59 percent of IT security respondents say customer accounts have been subject to an account takeover. Despite this, 25 percent of IT security respondents say their organizations have no plans to adopt 2FA for customers. Of these 25 percent of IT security respondents, 60 percent say their organizations believe usernames and passwords provide sufficient security and 47 percent say their organizations are not going to provide 2FA because it will affect convenience by adding an extra step during login. When businesses are choosing to protect customer accounts and data, the 2FA options that are used most often do not offer adequate protection for users.

- IT security respondents report that SMS codes (41 percent), backup codes (40 percent), or mobile authentication apps (37 percent) are the three main 2FA methods that they support or plan to support for customers. SMS codes and mobile authentication apps are typically tied to only one device. Additionally, only 23 percent of individuals find 2FA methods like SMS and mobile authentication apps to be very inconvenient. A majority of Individuals rate security (56 percent), affordability (57 percent) and ease of use (35 percent) as very important.

- It is clear that new technologies are needed for enterprises and Individuals to reach a safer future together. Across the board, passwords are cumbersome, mobile use introduces a new set of security challenges, and the security tools that organizations have put in place are not being widely adopted by employees or customers. In fact, 49 percent of Individuals say that they would like to improve the security of their accounts and have already added extra layers of protection

beyond a username and password. However, 56 percent of Individuals will only adopt new technologies that are easy to use and significantly improve account security. Here's what is preferred: biometrics, security keys, and password-free login.

- A majority of IT security respondents and Individuals (55 percent) would prefer a method of protecting accounts that doesn't involve passwords. Both IT security (65 percent) and Individual users (53 percent) believe the use of biometrics would increase the security of their organization or accounts. And lastly, 56 percent of Individuals and 52 percent of IT security professionals believe a hardware token would offer 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:

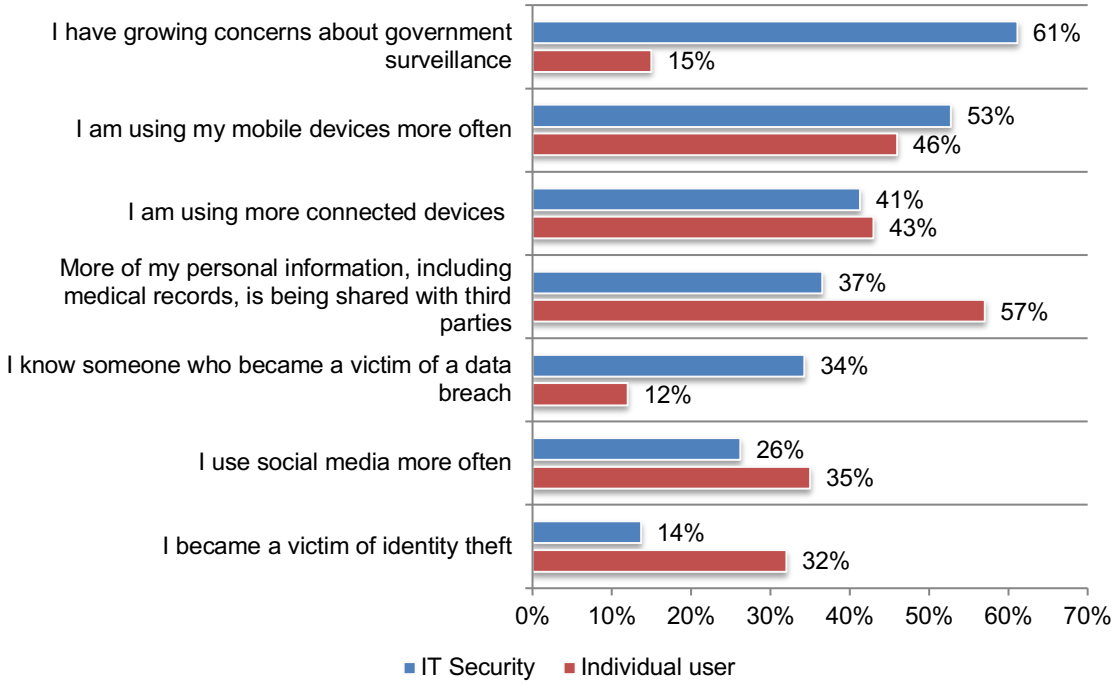
- How IT security respondents and Individuals approach personal security
- Security behaviors and practices in the workplace
- Authentication mechanisms
- The popularity of passwordless authentication
- Protecting customers' accounts with two-factor authentication
- The increase in personal mobile devices is bringing risk to the workplace
- How IT security behaviors and beliefs vary by country

How IT security respondents and Individual users approach personal security

IT security respondents have growing concerns about government surveillance. Figure 2 presents a list of reasons why most respondents are concerned about the privacy and security of their personal information. As shown, there are interesting differences between the two groups. The top two reasons of concern to IT security respondents are government surveillance (61 percent) and an increase in the use of mobile devices (53 percent).

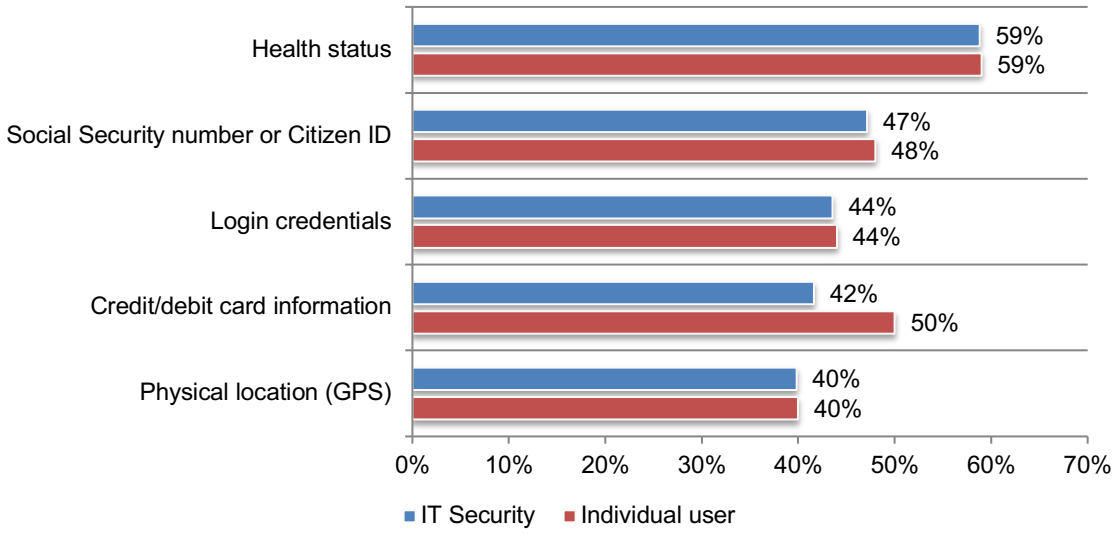
While Individuals are more concerned about the sharing of their personal data with third parties, especially their medical records (57 percent of respondents). Individuals agree with IT security respondents that the increase in the use of mobile devices is a top concern (46 percent and 53 percent of respondents, respectively).

Figure 2. The top reasons for the increase in concern about privacy and security
Four responses permitted



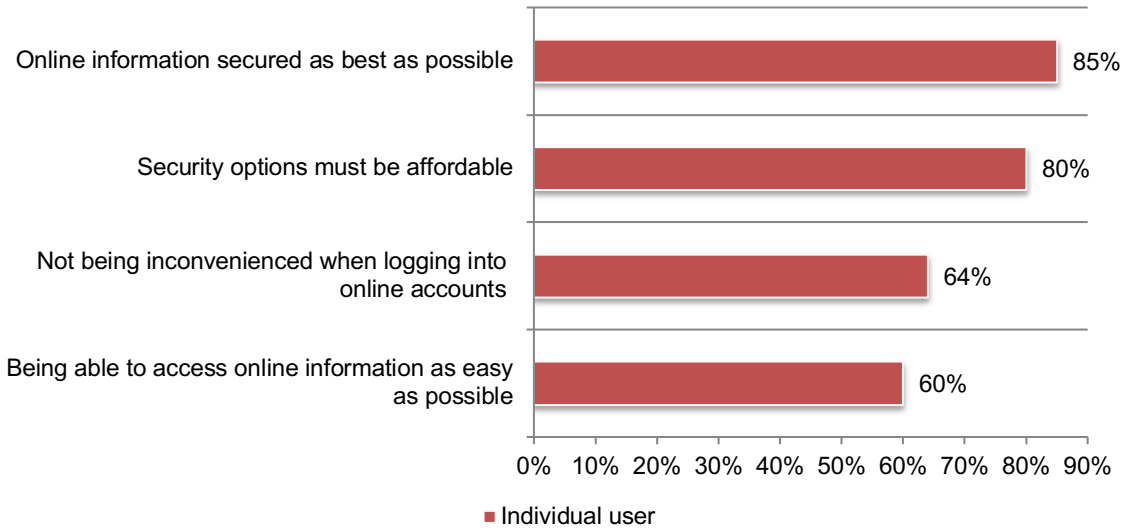
Perhaps because of the large and highly-publicized healthcare data breaches both groups are concerned about the protection of their health status (59 percent of respondents), as shown in Figure 3. However, Individuals are more concerned than IT security respondents about protecting credit/debit card information.

Figure 3. What personal information are you most concerned about protecting?
Four responses permitted



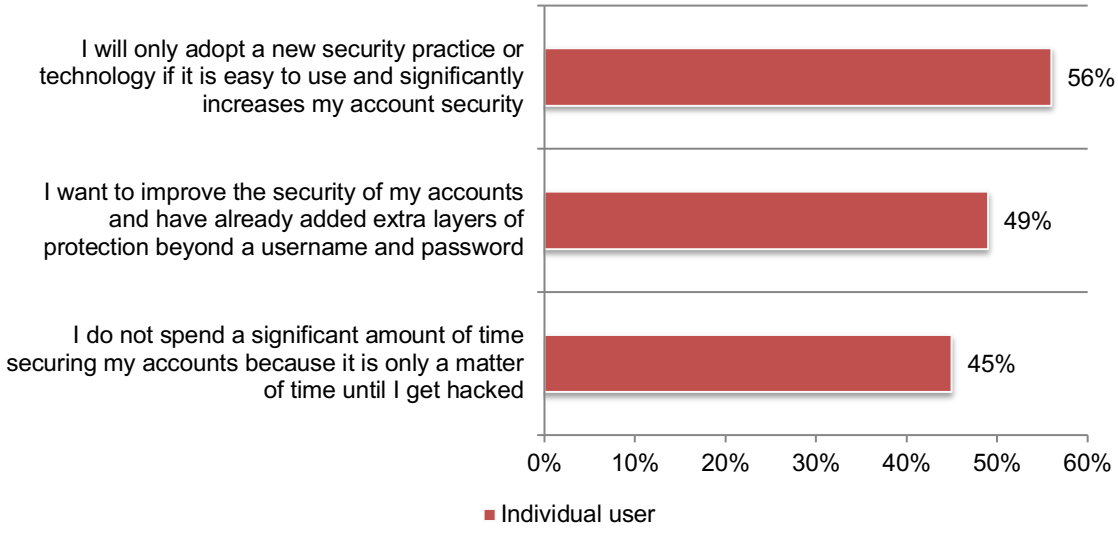
Individuals want the best online security but don't want to be inconvenienced. Sixty percent of individuals would spend $50 to $60 to have the highest form of security across all of their online accounts. Individuals were asked to rate the importance of various features of online security on a scale from 1 = not important to 10 = very important. Figure 4 presents the 7+ responses (important and very important responses combined). Eighty percent of Individuals say it is important to have affordable security options. The most important, according to 85 percent of respondents, is an option that provides the best online security.

Figure 4. Perceptions about the importance of online security
On a scale of 1 = not important to 10 = very important, 7+ responses presented



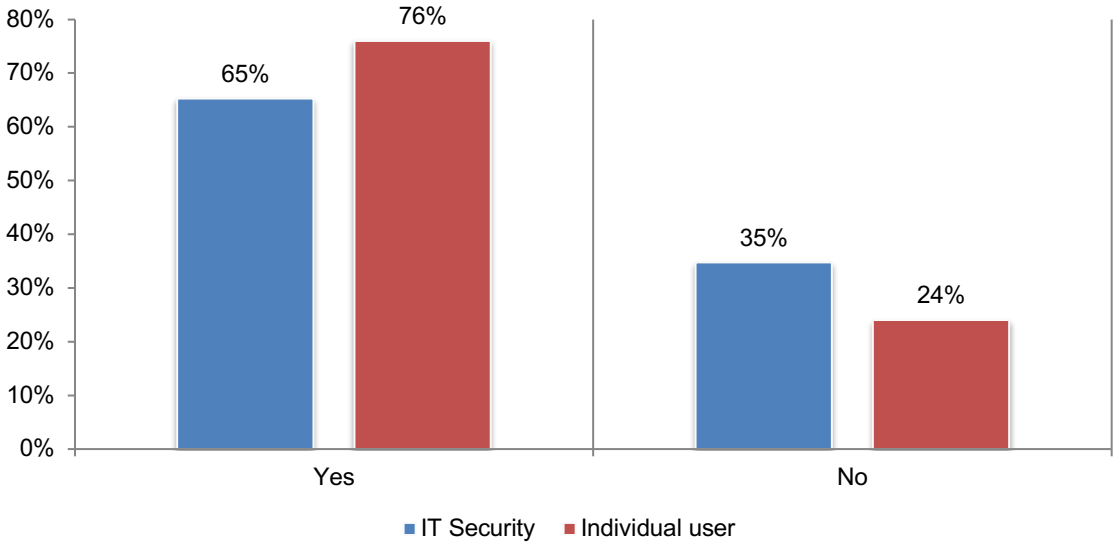
Despite growing concerns about the security of their personal information, less than half of Individuals (49 percent) are improving the security of their accounts and adding an extra layer of protection beyond a username and password, as shown in Figure 5. Fifty-six percent are only willing to adopt a new security practice or technology if it is easy to use and significantly increases account security.

Figure 5. Individuals' attitudes about protecting their online accounts
Strongly agree and Agree responses combined



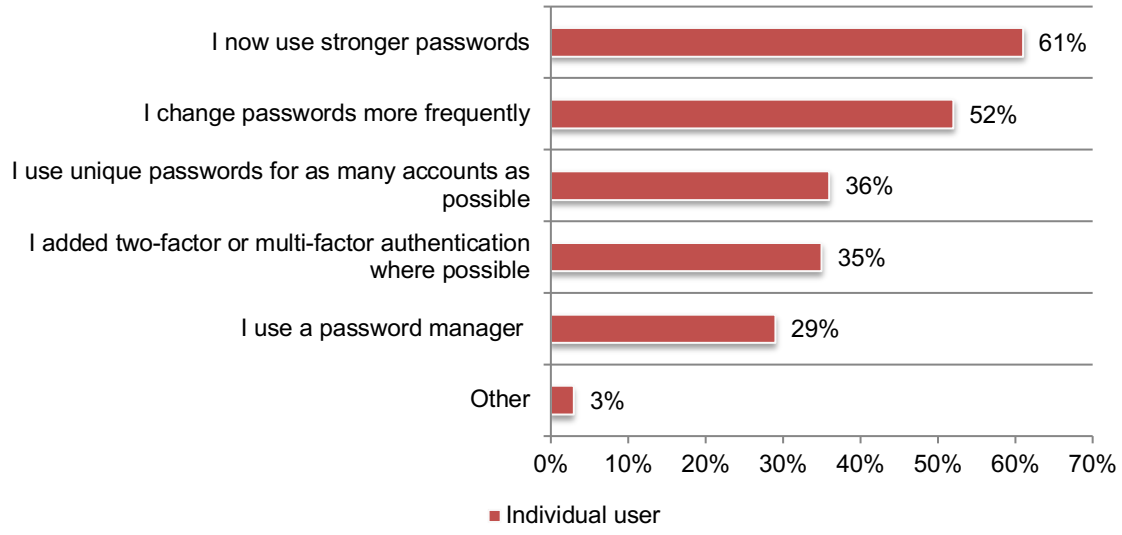
When attacked, most respondents will change their password practices. Twenty percent of IT security respondents and 35 percent of Individuals experienced an account takeover or hacking of their personal account. As shown in Figure 6, the majority of both groups did make changes as to how they protect their accounts. Something interesting to note is that more Individuals than IT security respondents made changes to their security posture after experiencing a compromised personal account.

Figure 6. Did an account takeover or hacking of your personal account change how you manage your passwords or protect your account?



According to Figure 7, the top two changes Individuals made were to use stronger passwords and change passwords more frequently.

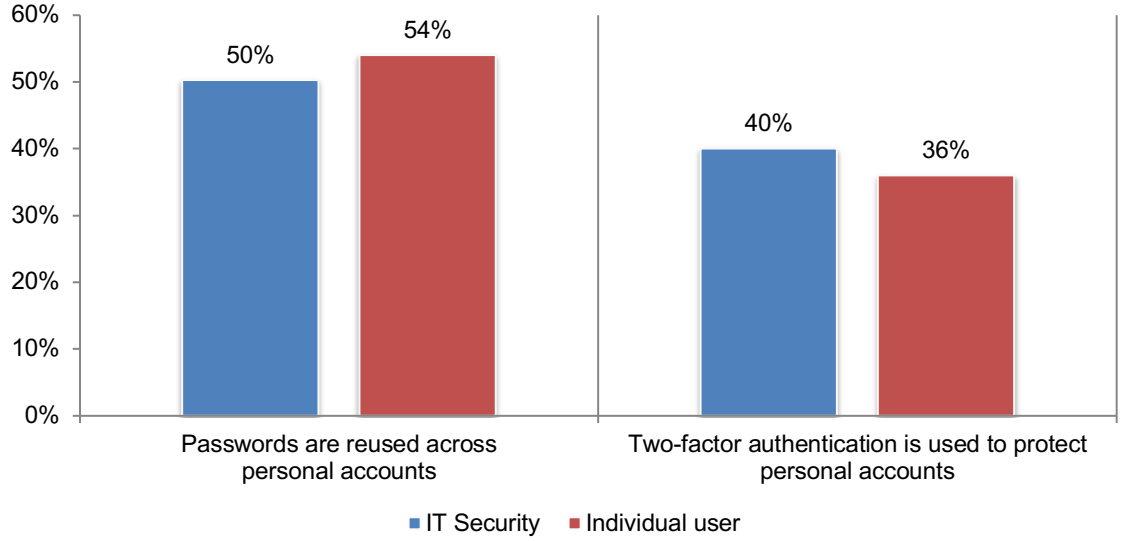
Figure 7. How did you change the way you manage passwords or protect your accounts?
More than one response permitted



Two-factor authentication (also known as 2FA or two-step verification) is a method to confirm a user's online identity by using a combination of two different types of factors. This can include something you know (a PIN or password), something you are (a fingerprint, iris, or facial scan), or something you have (a hardware security key or mobile phone). With 2FA, a password is typically the first factor and it is combined with one of the other factors to increase login security.

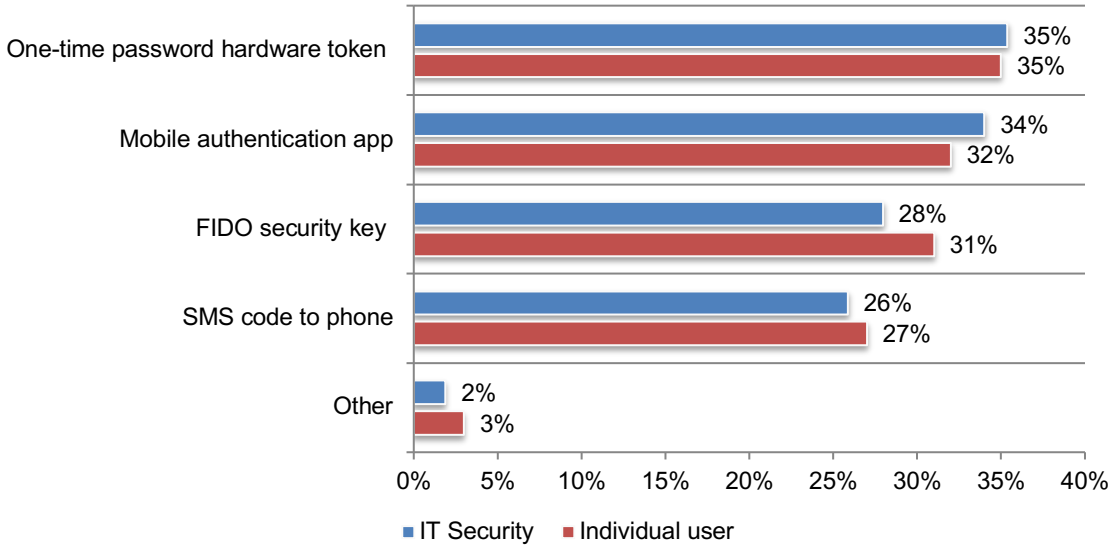
Both groups are reusing passwords across personal accounts and not implementing two-factor authentication. As shown in Figure 8, because many respondents do not want to be inconvenienced they are more likely to reuse their passwords and they are less likely to use two-factor authentication to protect their personal accounts. Both Individuals and IT security respondents reuse passwords on an average of 10 accounts.

Figure 8. Do you reuse passwords across any of your personal accounts and do you use two-factor authentication to protect your personal accounts?
Yes responses presented



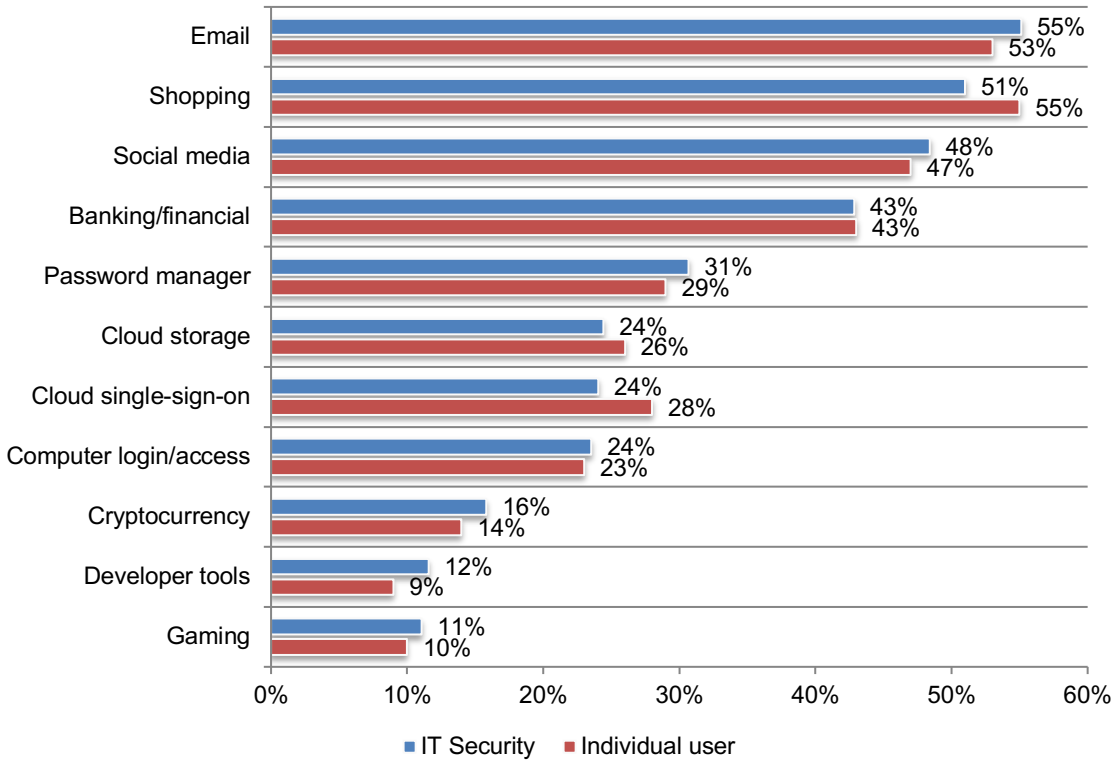
Of those respondents who use two-factor authentication to protect their personal accounts, the most popular method for both IT security and Individual users respondents is a one-time password hardware token (both 35 percent), as shown in Figure 9.

Figure 9. What type of two-factor authentication do you use for your personal accounts?



Individuals and IT security respondents both report that the top two personal accounts they secure with two-factor authentication are email and shopping accounts, followed closely by social media and banking/financial accounts as shown in Figure 10.

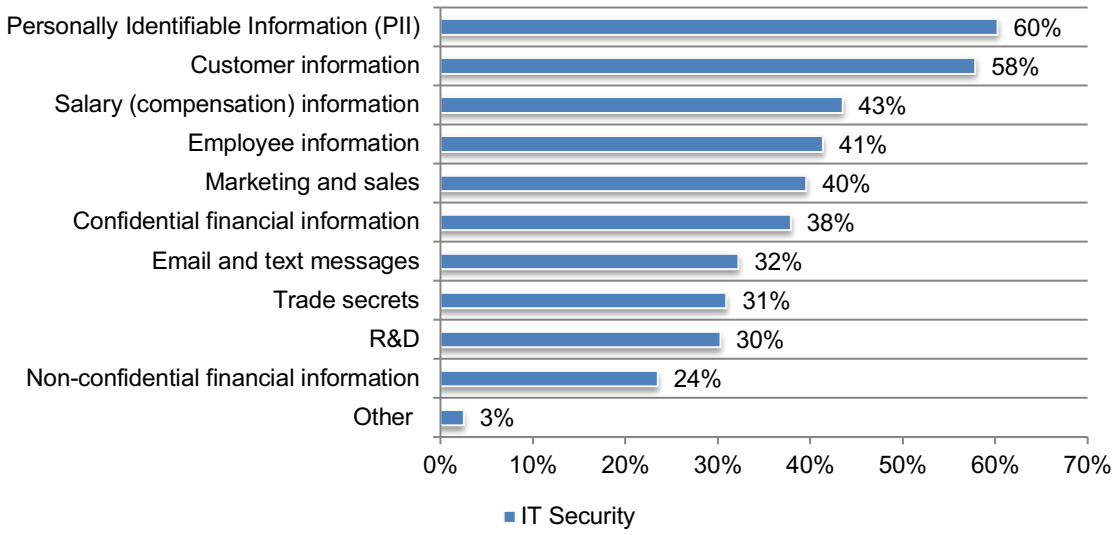
Figure 10. What type of personal accounts do you secure with two-factor (or multi-factor authentication?
More than one response permitted



Security behaviors and practices in the workplace

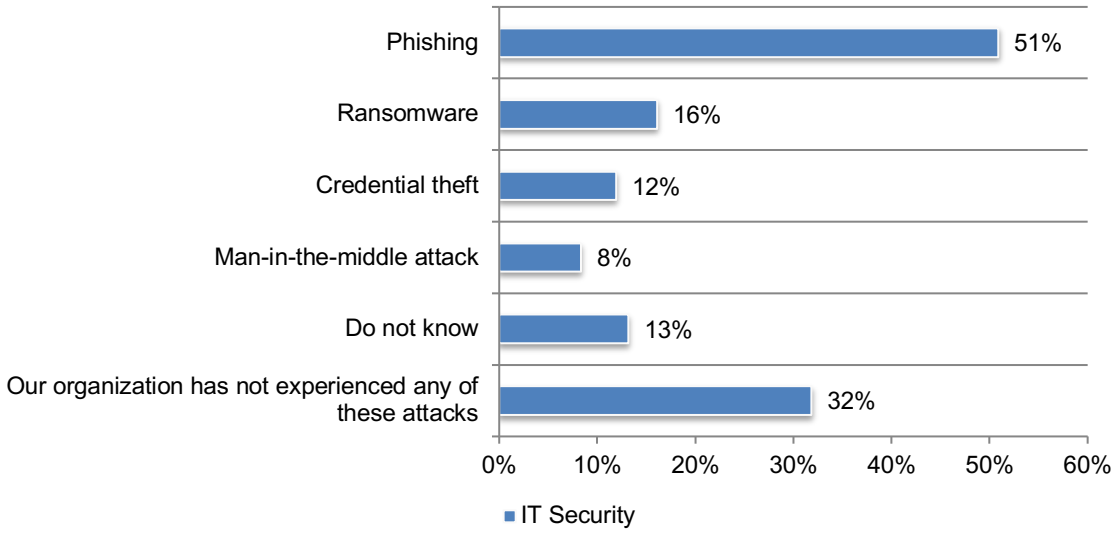
The priority for IT security respondents is protection of personally identifiable information (PII) and customer information over confidential financial information and trade secrets. Figure 11 presents the types of business information that respondents believe must be protected. Sixty percent of IT security respondents say PII is most important to protect, followed closely by customer information (58 percent) Thirty-eight percent of IT security respondents say they are concerned about confidential financial information and less than one-third say they are concerned about trade secrets and R&D.

Figure 11. What business information are you most concerned about protecting?
Four responses permitted



Phishing is a significant threat to business information. As shown in Figure 12, 51 percent of IT security respondents say their organizations experienced a phishing attack with another 12 percent say their organizations experienced credential theft and 8 percent say it was a man-in-the-middle attack.

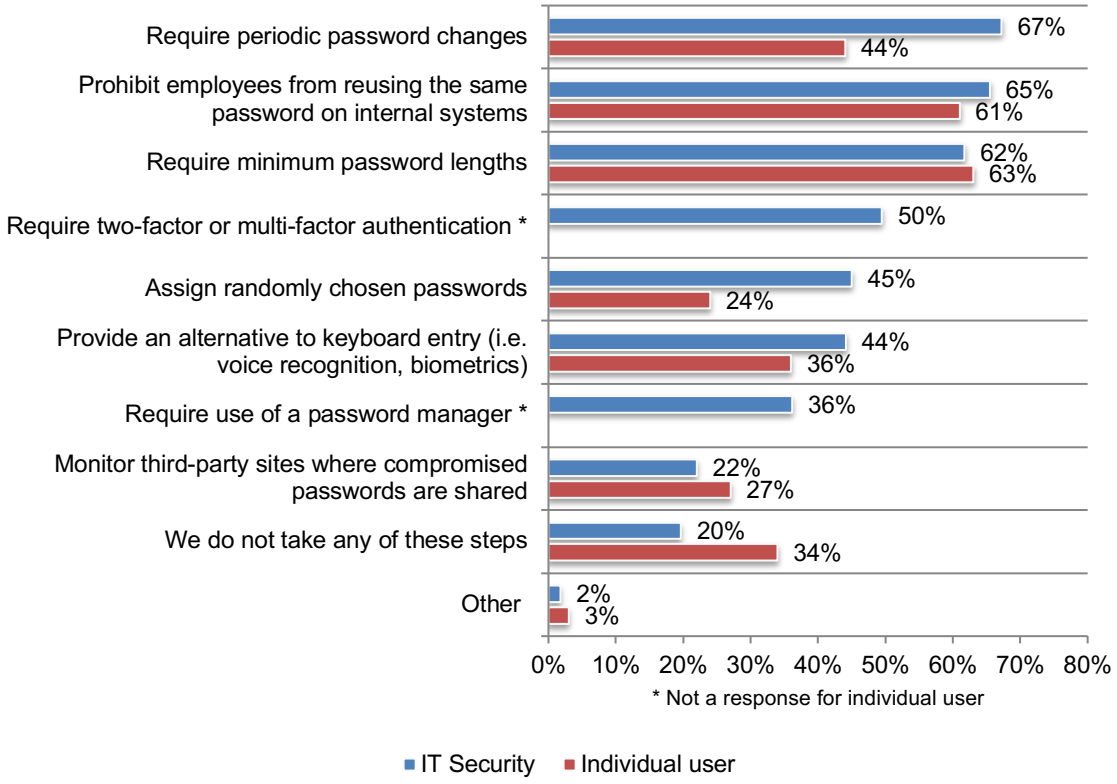
Figure 12. Has your organization experienced any of the following attacks?
More than one response permitted



To increase security, IT security respondents say their organizations require periodic password changes (67 percent). This is followed by prohibiting employees from reusing the same password on internal systems (65 percent of respondents). Most individuals (61 percent of respondents) say organizations are prohibiting employees from reusing the same password on internal systems, as shown in Figure 13. Sixty-two percent of IT respondents and 63 percent of Individuals say their organizations are requiring minimum password lengths.

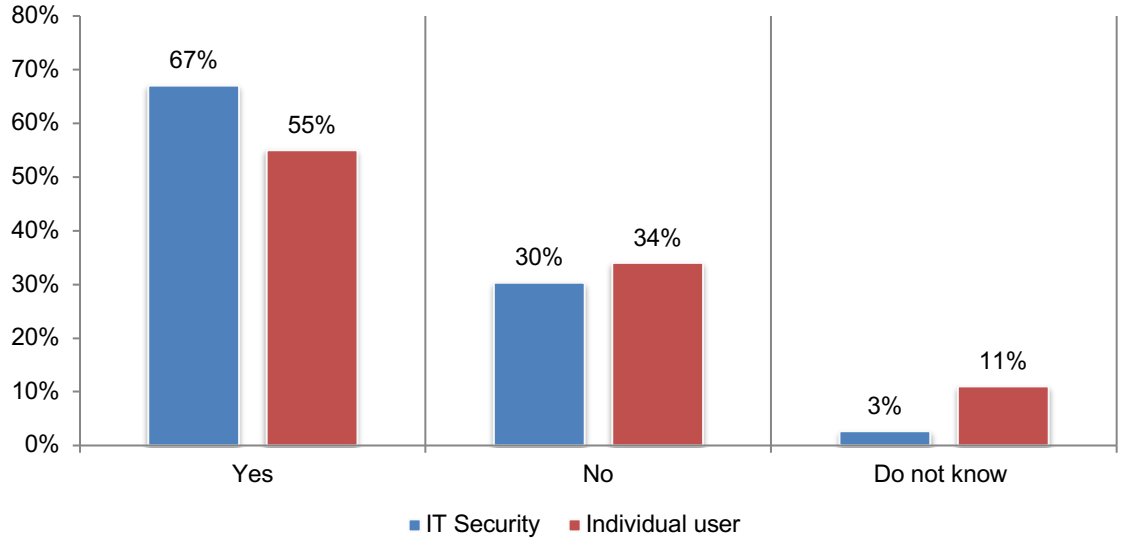
Only 36 percent of IT security respondents say their organizations require a password manager, which assists in generating and retrieving complex passwords, potentially storing such passwords in an encrypted database or typing them on demand.

Figure 13. Does your organization take any of the following steps to increase corporate security?
More than one response permitted



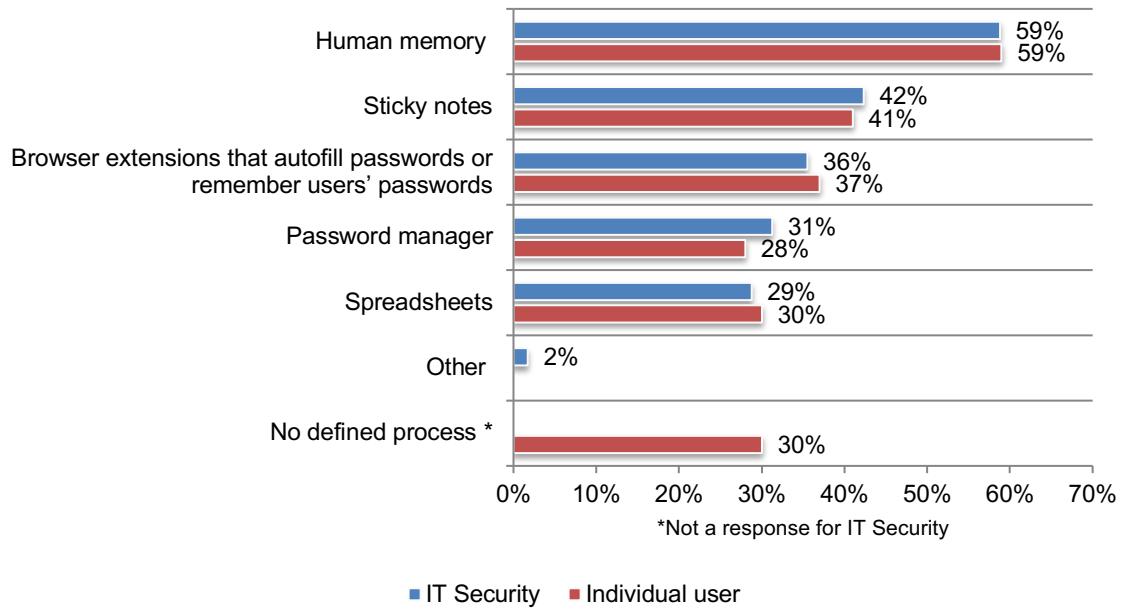
There is a significant gap between IT security respondents and Individuals who say their organization has a password policy for employees. According to Figure 14, 67 percent of IT security respondents and 55 percent of Individuals say their organizations have a password policy. However, only 41 percent of IT security respondents and 35 percent of Individuals say the password policy is strictly enforced.

Figure 14. Does your organization have a password policy for employees?



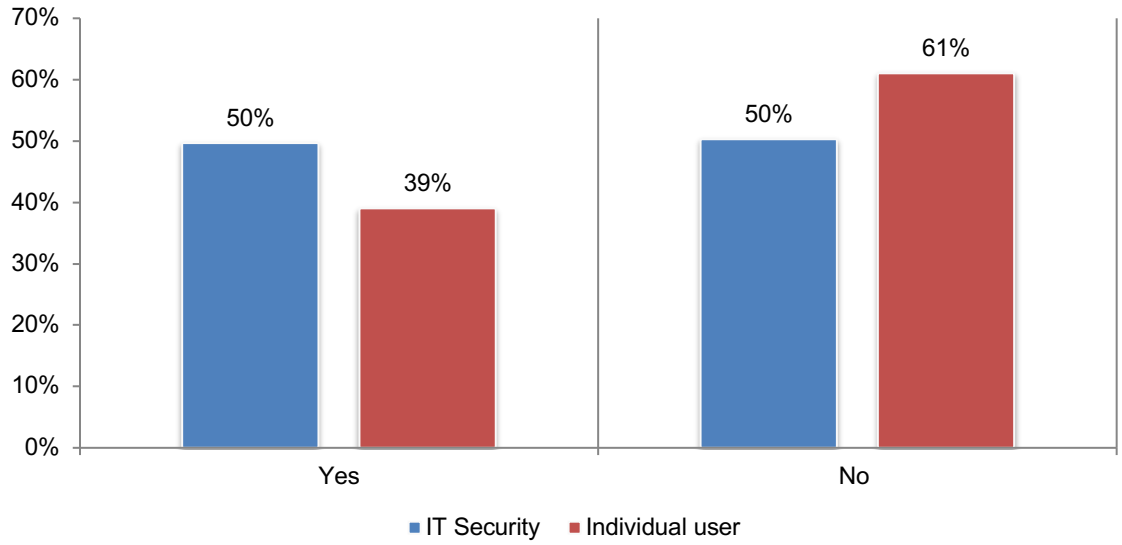
How organizations manage and protect passwords is putting them at risk. Despite concerns about protecting workplace accounts, both groups say human memory and sticky notes are used to manage and protect their passwords. As shown in Figure 15, only 36 percent of IT security and 37 percent of Individuals say their organizations use browser extensions. Even fewer respondents say their organizations are using a password manager.

Figure 15. What does your organization use to manage and protect its passwords?
More than one response permitted



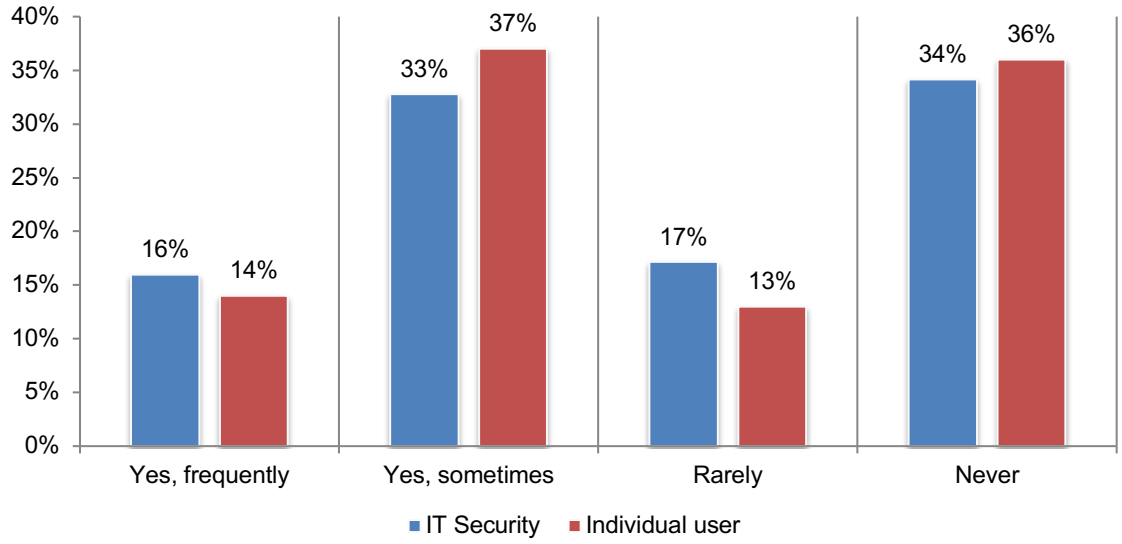
Another cause of risk is the reuse of personal or business passwords for workplace accounts. According to Figure 16, those who should know better (IT security respondents) are more likely to reuse their passwords for workplace accounts. Individuals have or have had an average of 22 workplace accounts and report reusing passwords on an average of 16 of those accounts. IT security respondents have or had an average of 16 accounts and report reusing passwords on an average of 12 of those accounts.

Figure 16. Do you reuse personal or business passwords for any of your workplace accounts?



Forty-nine percent of IT security respondents and 51 percent of Individuals say they are sharing passwords with their fellow employees.

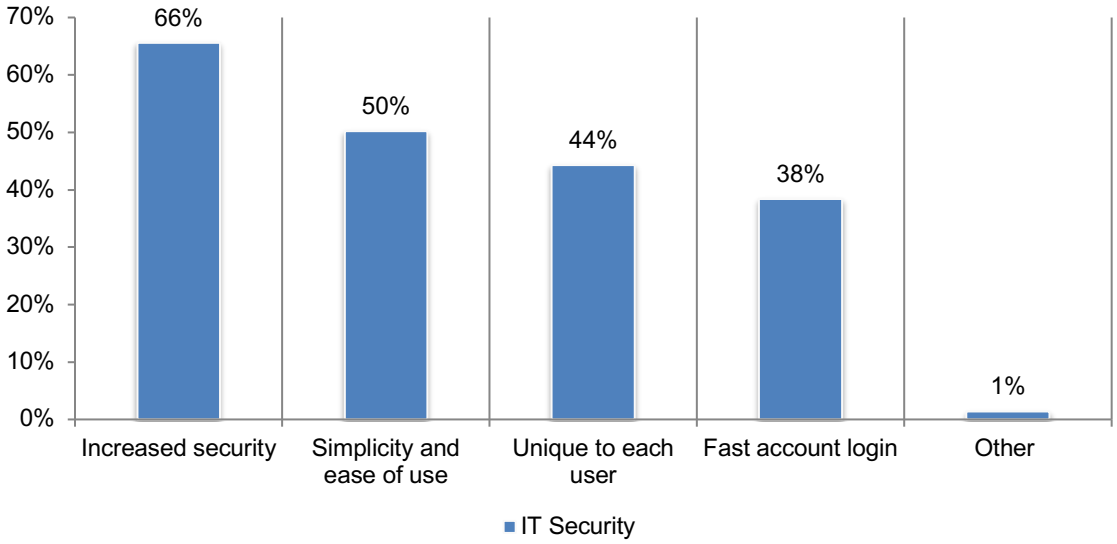
Figure 17. Do you share passwords with colleagues to access business accounts?



Authentication mechanisms

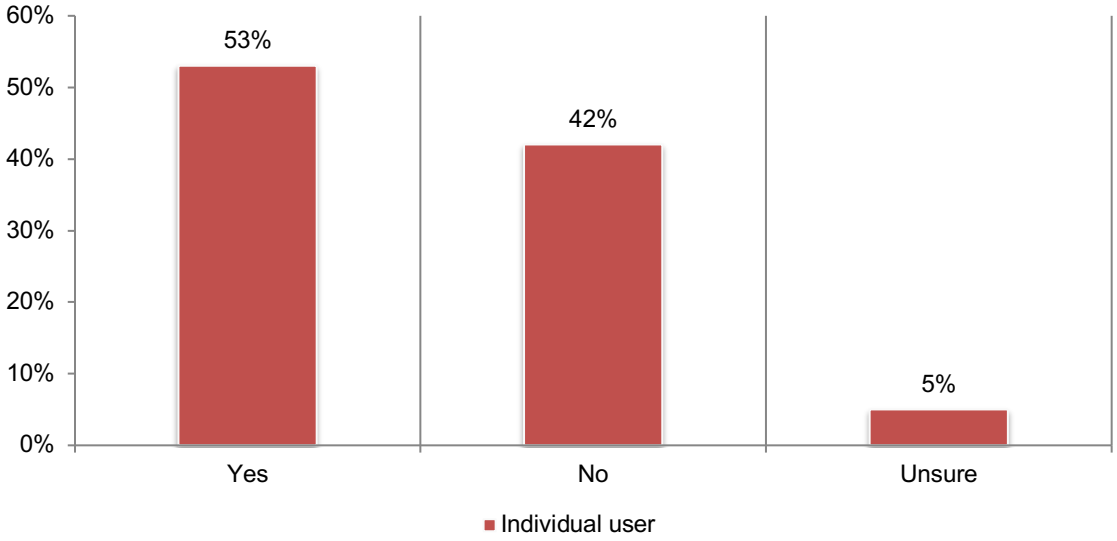
Biometrics are believed to increase the security of authentication processes. Sixty-five percent of IT security respondents believe that biometrics would reduce the risk of workplace accounts being compromised. According to Figure 18, increased security and simplicity and ease of use are the two biggest perceived benefits of using biometrics for account login.

Figure 18. What are the two biggest benefits of using biometrics for account login?
Two responses permitted



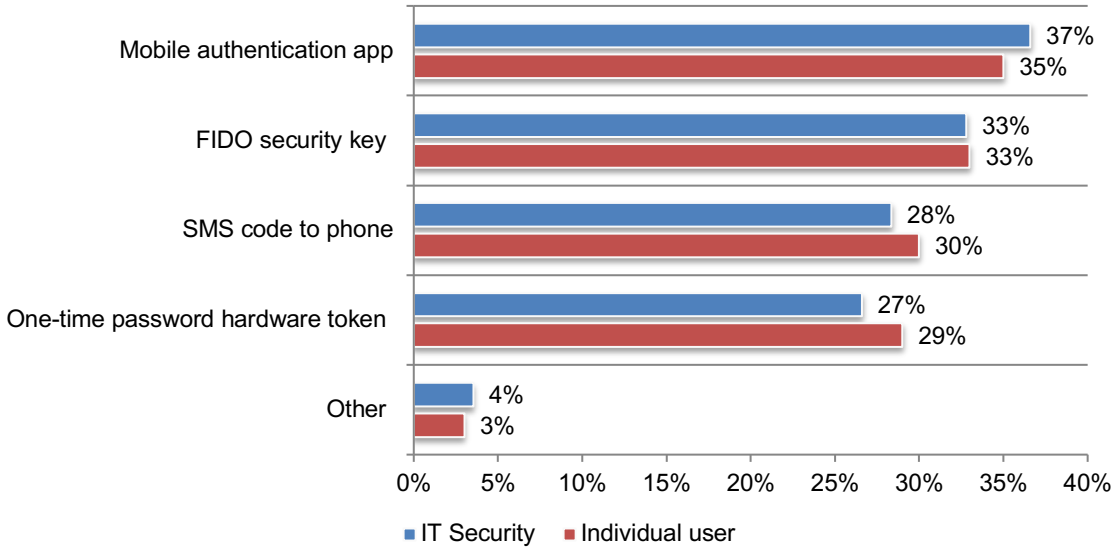
Individual respondents agree that biometrics improves their security. According to Figure 19, more than half of individual respondents (53 percent) think that biometrics improves their security. Because these respondents value convenience, it seems they would favor their organizations' adoption of biometrics.

Figure 19. Would you feel you were getting better security if you were able to use your fingerprint or facial scan to login to business and/or personal accounts?



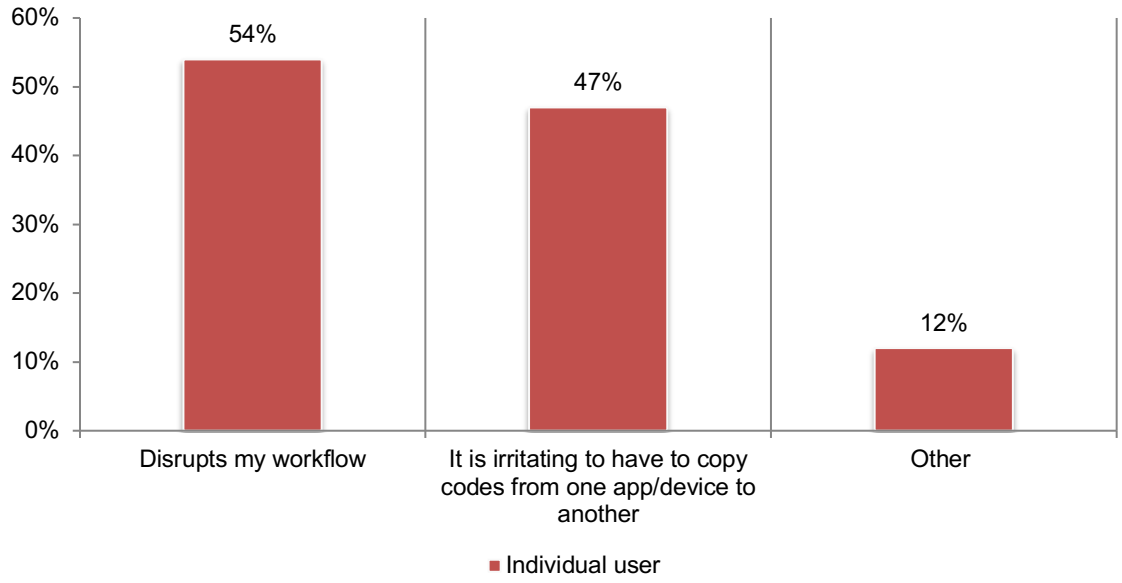
Forty-six percent of IT security respondents and 43 percent of Individuals say their organizations require two-factor authentication to gain access to business accounts. As shown in Figure 20, mobile authentication apps and FIDO security keys are the two-factor authentication types most often used. According to the findings, respondents believe one-time password hardware tokens would improve security. Yet, only 27 percent of IT security respondents and 29 percent of Individuals say their organizations use one-time password hardware tokens for authentication.

Figure 20. What type of two-factor authentication do you use to access business accounts?
More than one response permitted



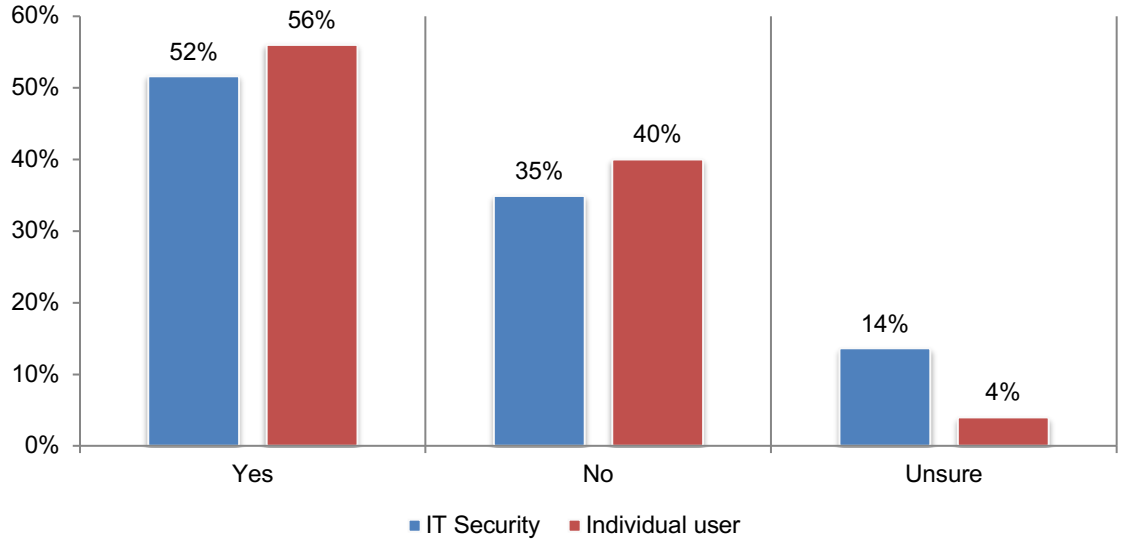
Individuals were asked to rate the convenience of two-factor authentication from 1 = highly inconvenient to 10 = very convenient. Twenty-three percent of respondents say two-factor authentication is highly inconvenient (responses 1 to 4 on the 10-point scale). According to Figure 21 of these respondents, 54 percent say it disrupts their workflow and it is irritating to have to copy codes from one app/device to another (47 percent).

Figure 21. Why is two-factor authentication not convenient?



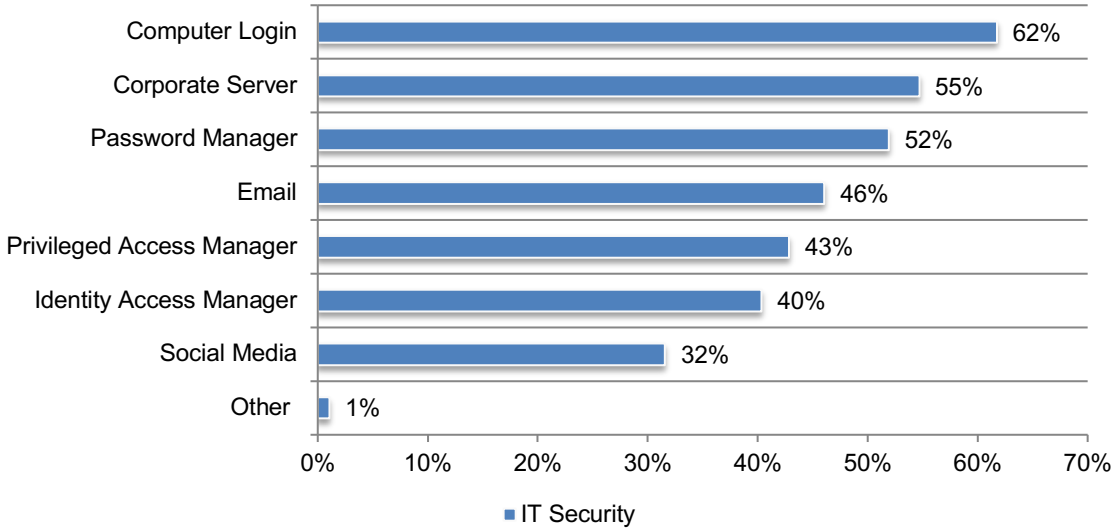
Both IT security respondents and Individuals believe security would improve with the use of a physical hardware token to access their accounts, as shown in Figure 22.

Figure 22. Do you believe security would improve if you were offered a physical hardware token to login to business and/or personal accounts?



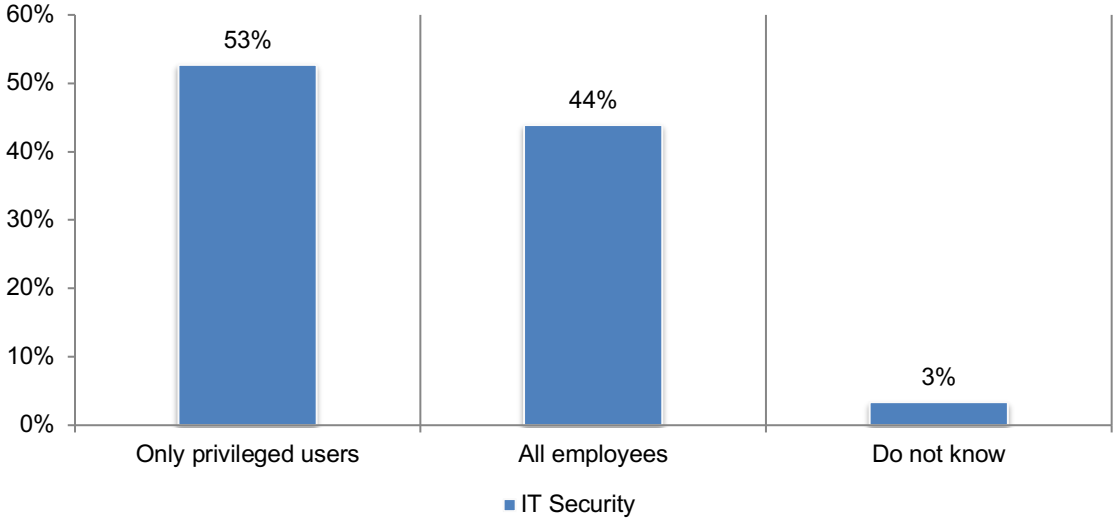
Computer login and corporate servers are the business accounts most often protected with two-factor authentication, as shown in Figure 23.

Figure 23. What types of business accounts or information are protected with two-factor authentication?
More than one response permitted



An average of 23 percent of employees are privileged users. According to Figure 24, 53 percent of IT security respondents say their organizations only require privileged users to use two-factor authentication. Only 44 percent say two-factor authentication is required for all employees.

Figure 24. Does your organization enable two-factor authentication for all employees or just privileged users?

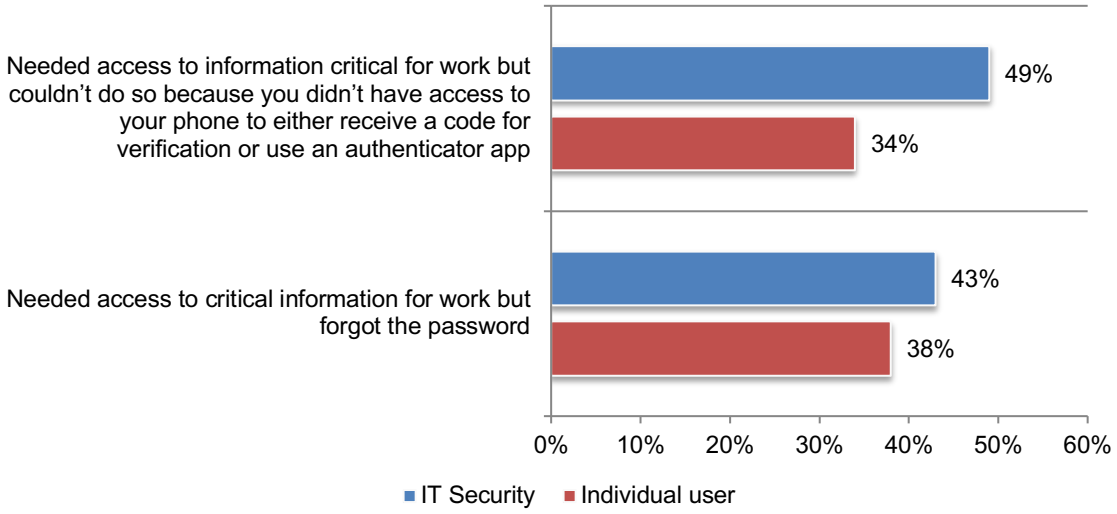


The popularity of passwordless protection

Many respondents are frustrated they could not access information because of a forgotten password or didn't have access to their phones. According to Figure 25, almost half of IT security respondents say they frequently or very frequently could not access information critical for work because they didn't have access to their phones to either receive a code for verification or use an authenticator. Forty-three percent of these respondents frequently or very frequently could not access information they needed for their work because they forgot their password.

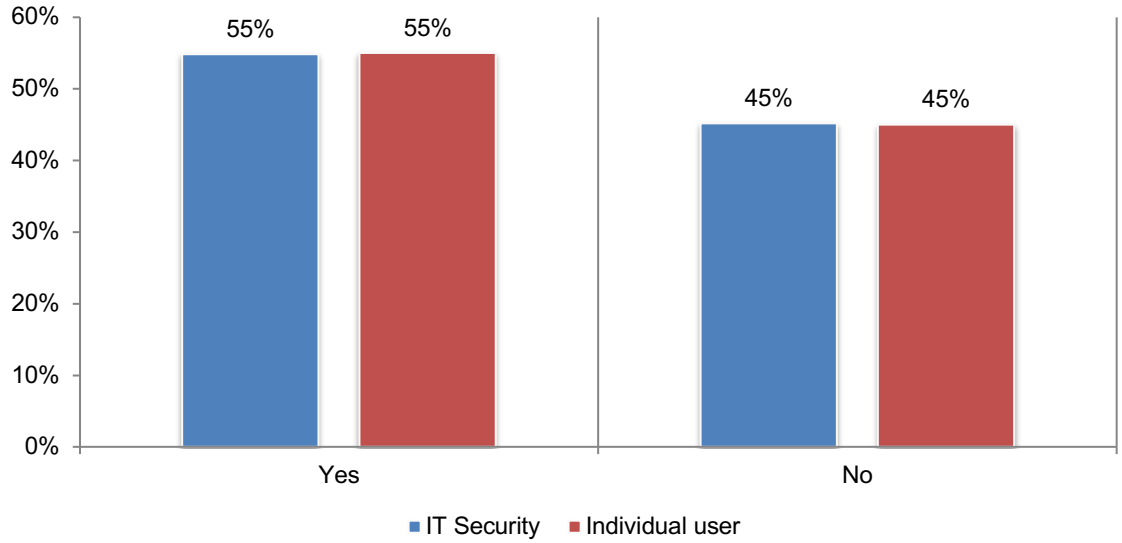
Figure 25. Have you ever needed access to critical information but forgot the password or didn't have access to your phone to either receive a code for verification or use an authenticator app?

Very frequently and Frequently responses combined



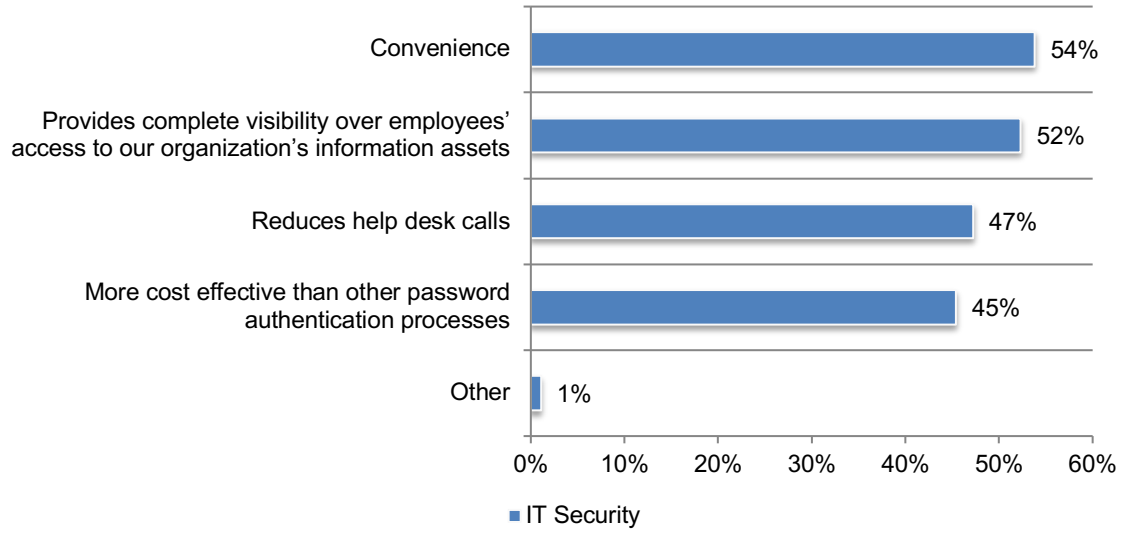
As a consequence of not being able to access critical information because of a forgotten password, 55 percent of respondents would prefer a method of protecting their personal or business accounts without having to remember their passwords, as shown Figure 26.

Figure 26. Would you prefer a method of protecting your personal or business accounts that doesn't involve the use of passwords?



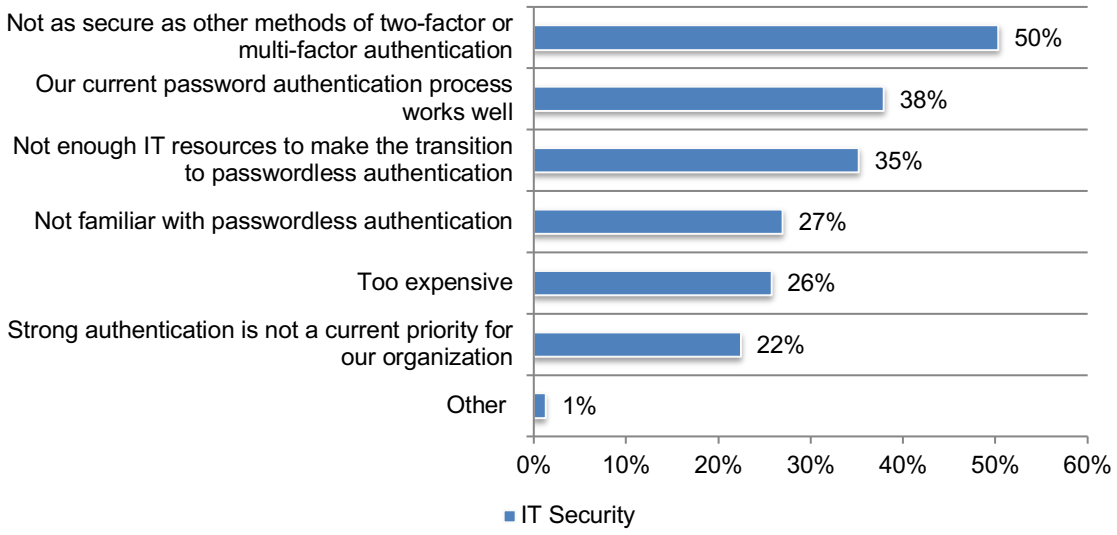
Fifty-six percent of IT security respondents say their organizations would adopt passwordless authentication because it would increase the security of their organizations' authentication processes. The perceived benefits are shown in Figure 27. Convenience and visibility over employees' access to information assets are reported as the primary benefits.

Figure 27. What are the primary benefits of passwordless authentication?
Two responses permitted



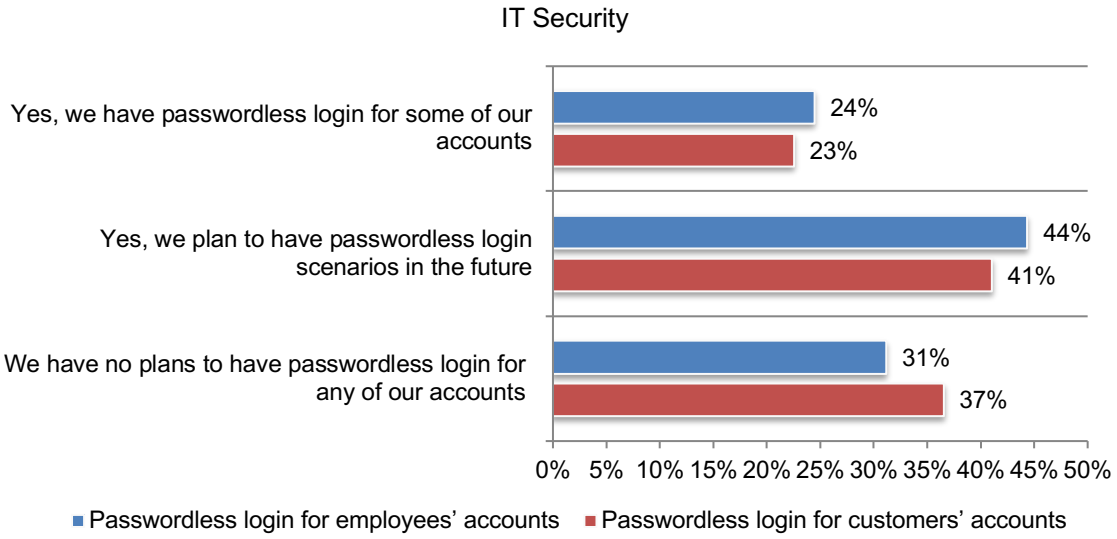
Of the 44 percent of IT security respondents who do not believe passwordless authentication increases security, 50 percent say it is not as secure as other methods of two-factor or multi-factor authentication. Thirty-eight percent of respondents say their current password authentication process works well, as shown in Figure 28.

Figure 28. Why would your organization not use passwordless authentication?
Two responses permitted



Most organizations plan to adopt passwordless authentication for both employees and customers. According to Figure 29, 68 percent of IT security respondents say their organizations have or eventually will have passwordless authentication for employees and 64 percent say they will have it for customers' accounts.

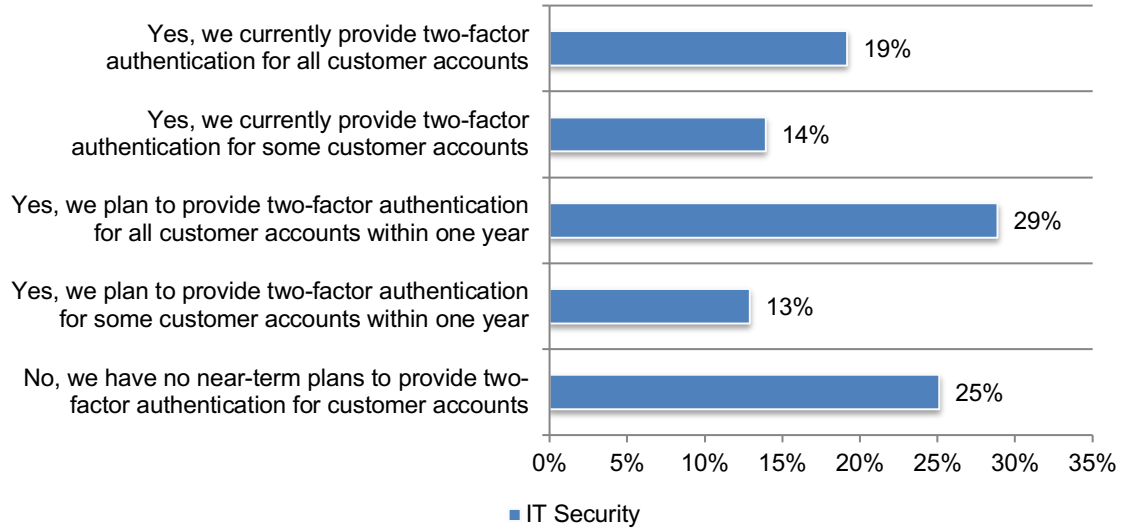
Figure 29. Does your organization have or plan to have passwordless authentication for employees and customers?



Protecting customers' accounts with two-factor authentication

The majority of organizations provide or plan to provide two-factor authentication for all or some customer accounts. As shown in Figure 30, 33 percent of IT security respondents say they currently provide two-factor authentication for all or some customer accounts. Another 42 percent plan to provide two-factor authentication.

Figure 30. Does your organization provide or plan to provide two-factor authentication for your customers?



Of those organizations that provide or plan to provide two-factor authentication for customers' accounts, the primary reason is to increase security. As shown in Figure 31, 62 percent of IT security respondents say it improves security and 58 percent of respondents say it reduces account takeovers.

Figure 31. What are the primary reasons to provide two-factor authentication?
Two responses permitted

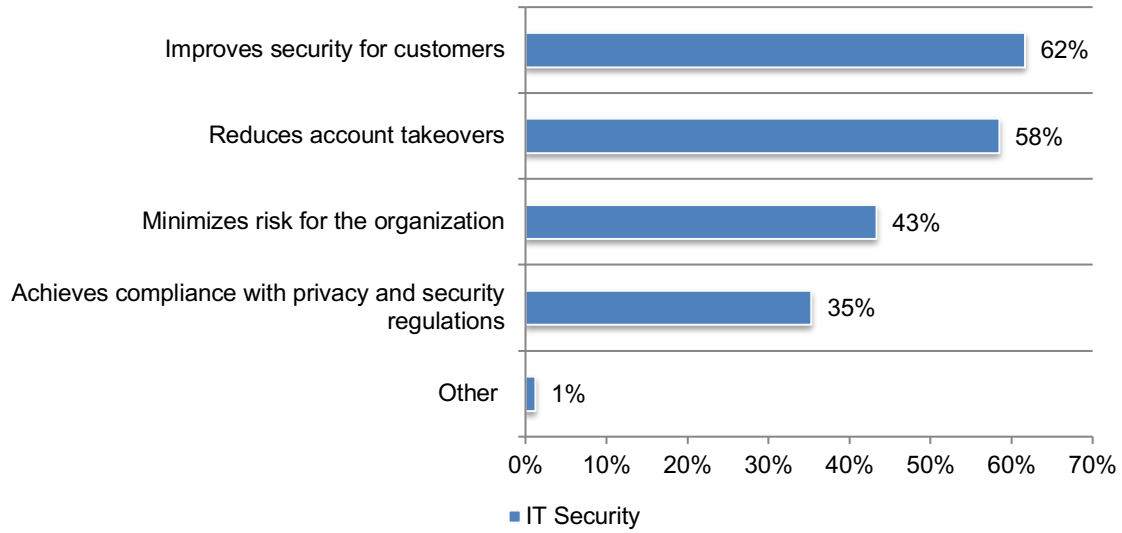
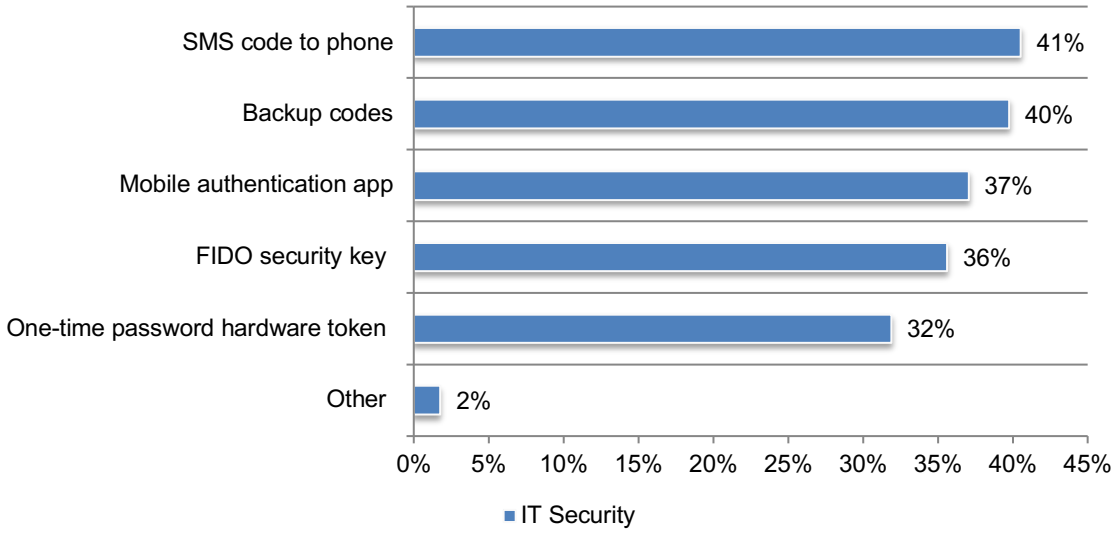


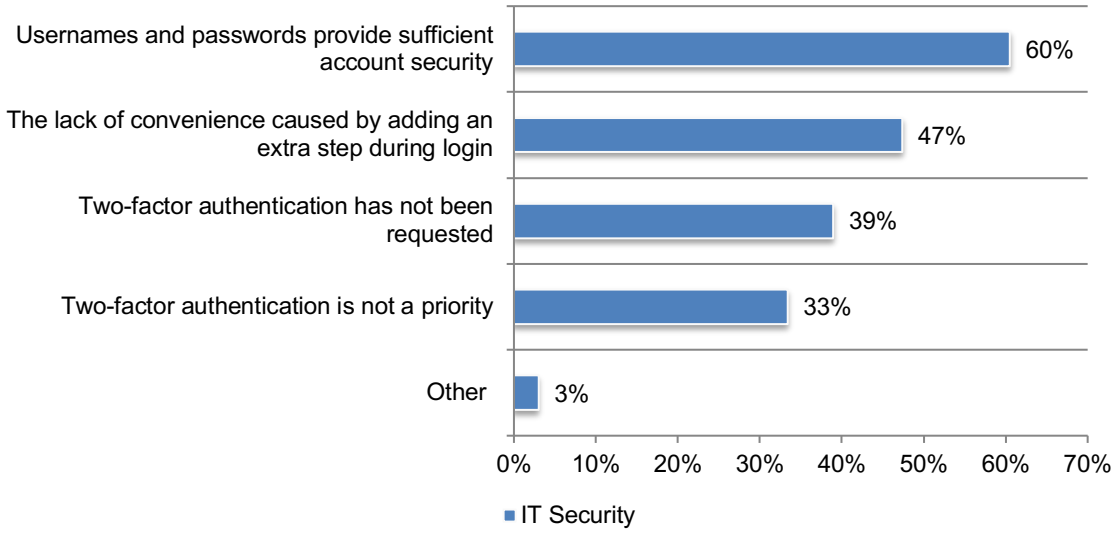
Figure 32 shows the two-factor authentication options organizations plan to provide. The top two-factor authentication options are SMS code to phone and backup codes.

Figure 32. What two-factor authentication options do you provide or plan to provide?
More than one response permitted



Twenty-five percent of respondents say their organizations do not plan to provide two-factor authentication for customers. According to Figure 33, 60 percent of respondents say usernames and passwords provide sufficient account security and 47 percent of respondents say they don't want to provide two-factor authentication as it may make it inconvenient for customers.

Figure 33. Why would your organization not provide two-factor authentication?
More than one response permitted

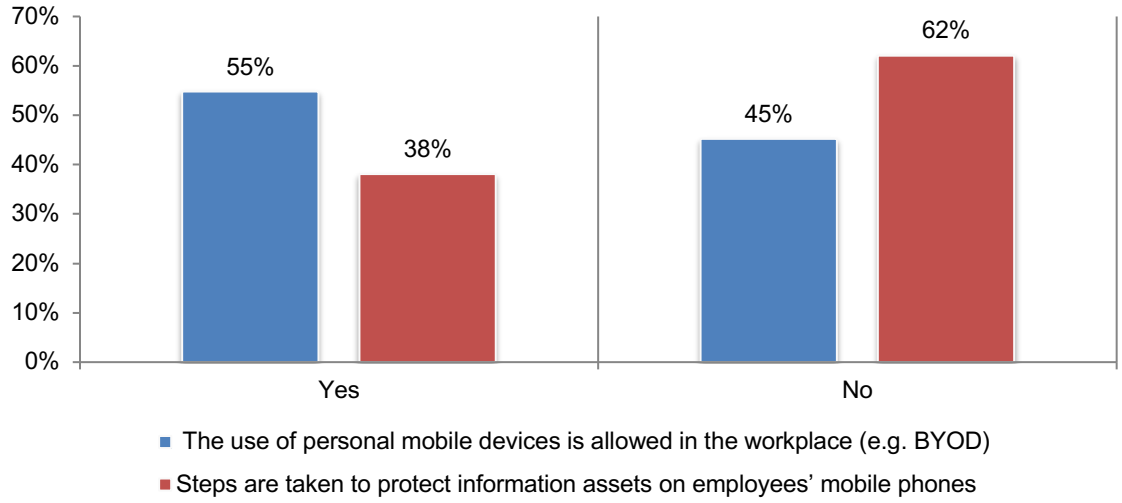


The increase in personal mobile devices is bringing risk to the workplace

Organizations allow personal devices in the workplace but many are not taking steps to protect information on these devices. IT security respondents were asked to rate the effectiveness of their organizations' ability to protect its information assets on employees' mobile phones on a scale of 1 = low effectiveness to 10 = high effectiveness. Only 27 percent of respondents say the steps they take are highly effective.

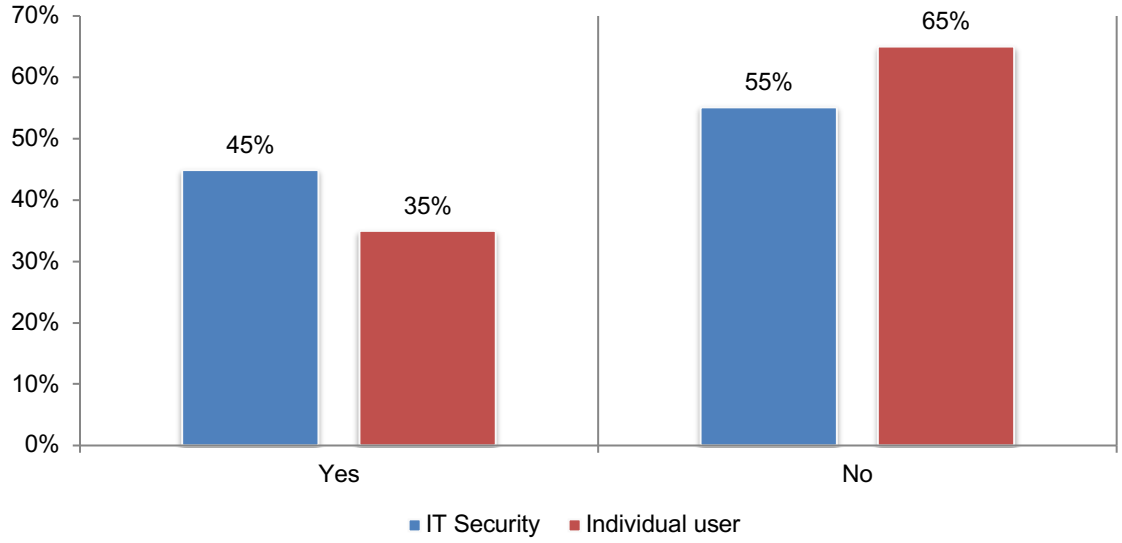
The reason effectiveness is rated low is that only 38 percent of IT security respondents say their organizations take steps to protect information assets on employees' devices, according to Figure 34. Fifty-five percent of IT security respondents say their organizations allow personal devices in the workplace.

Figure 34. Does your organization allow the use of personal mobile devices and does it take steps to protect its information assets on employees' mobile phones?



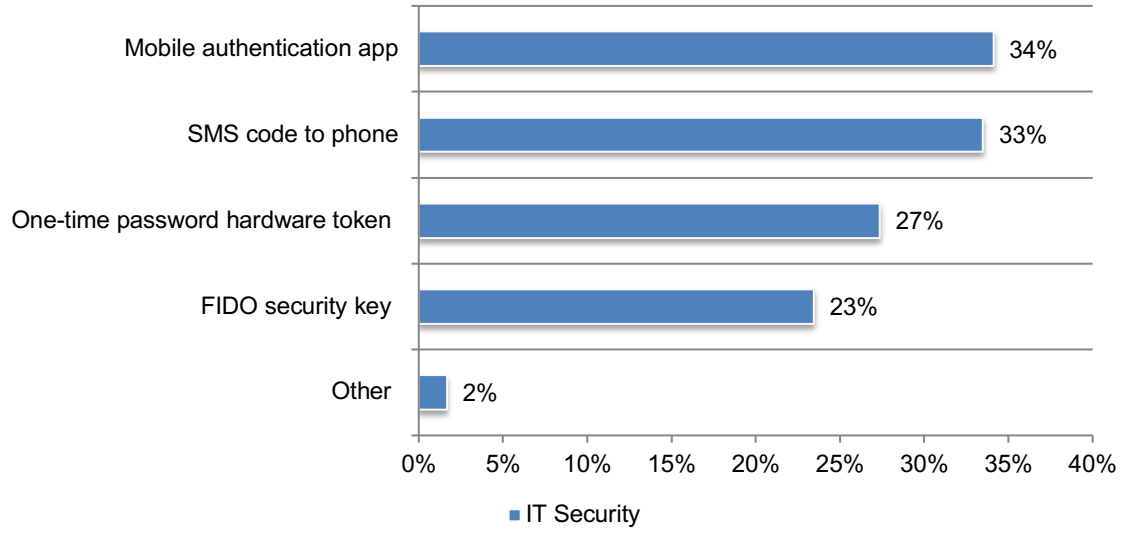
To improve effectiveness, employees should be required to use two-factor authentication when logging into work apps on their mobile devices. As shown in Figure 35, only 45 percent of IT security respondents and 35 percent of Individuals use two-factor authentication in the workplace.

Figure 35. Do you use any two-factor/multi-factor authentication methods when you log into your work apps on your mobile device?



According to Figure 36, 34 percent of IT security respondents say mobile authentication apps and 33 percent of respondents say SMS code to phone are the top two methods used.

Figure 36. If yes, which method do you use?
More than one response permitted

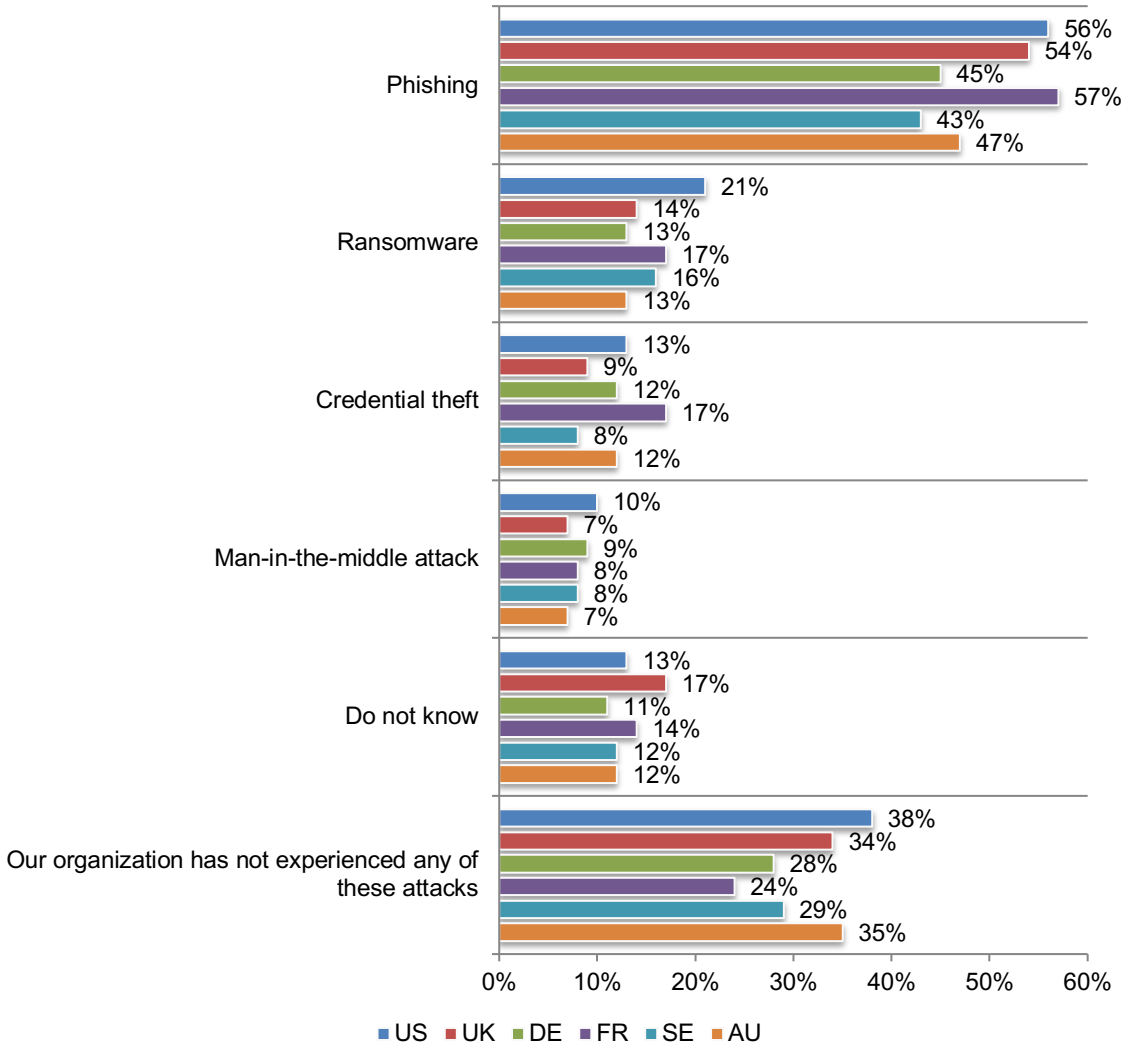


How IT security behaviors and beliefs vary by country

More than 2,500 IT and IT security practitioners were surveyed in the following countries: United States (593), United Kingdom (413), Germany (423), France (377), Sweden (365) and Australia (336). In this section, we present country differences in the research findings.

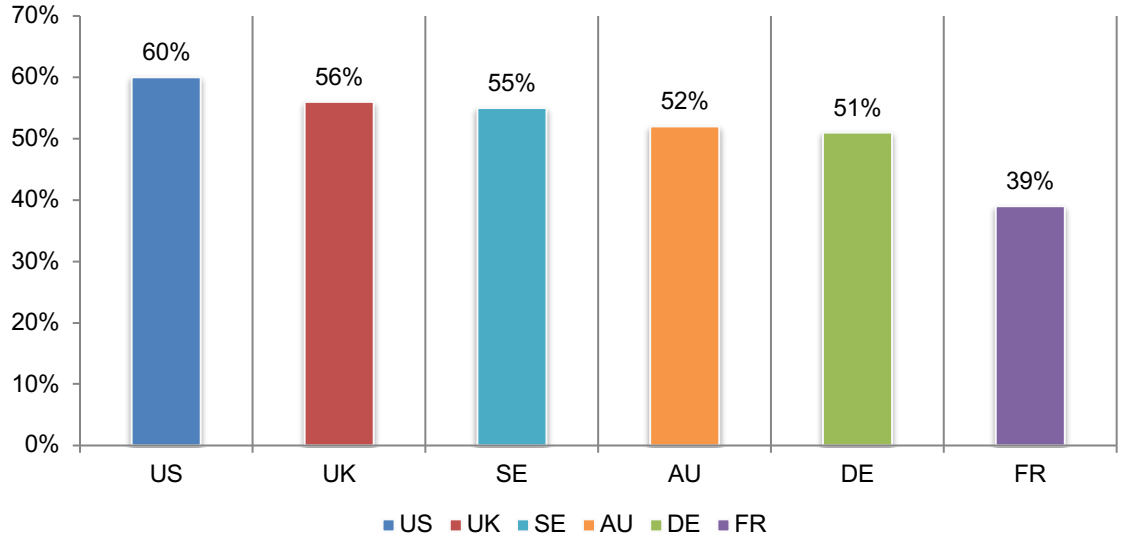
Phishing is the most prevalent type of attack in each country. As shown in Figure 37, more respondents in France, US and UK say their organizations had a phishing attack. Ransomware is most prevalent in the US (21 percent of respondents) and more respondents in France report that they had credential theft (17 percent of respondents.

Figure 37. Has your organization experienced any of the following attacks?
More than one response permitted



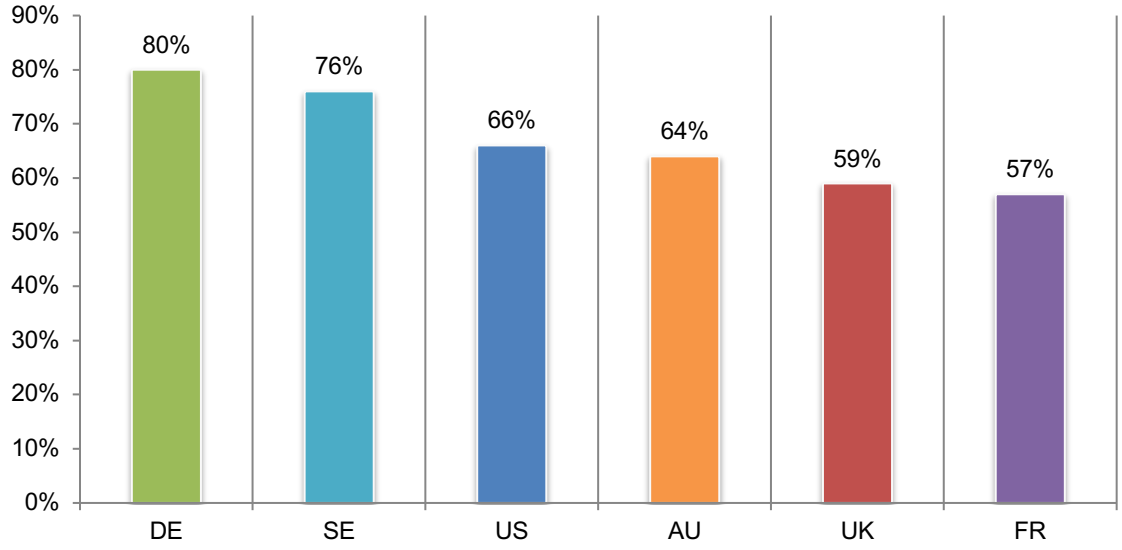
More US respondents (60 percent) say their organization changed their password practices following an attack. Only 39 percent of respondents in France say their organizations changed how it manages passwords or protects corporate accounts, as shown in Figure 38.

Figure 38. Did your organization change how it manages passwords or protects corporate accounts?
Yes responses



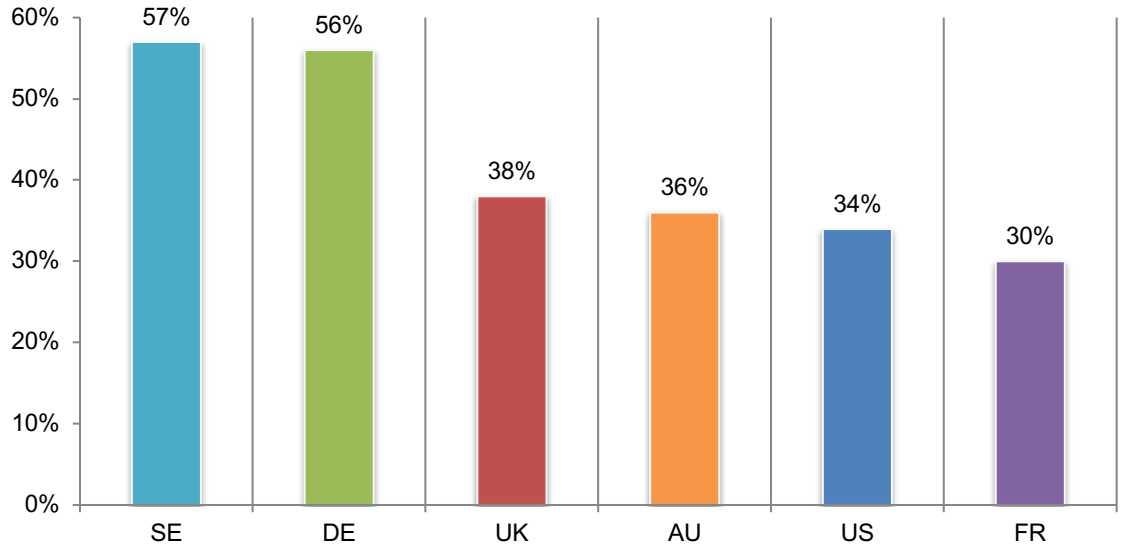
More German organizations have a password policy for their employees (80 percent of respondents) followed by Sweden (76 percent of respondents). Fifty-seven percent of respondents in France say their organizations have a password policy.

Figure 39. Does your organization have a password policy for their employees?
Yes responses presented



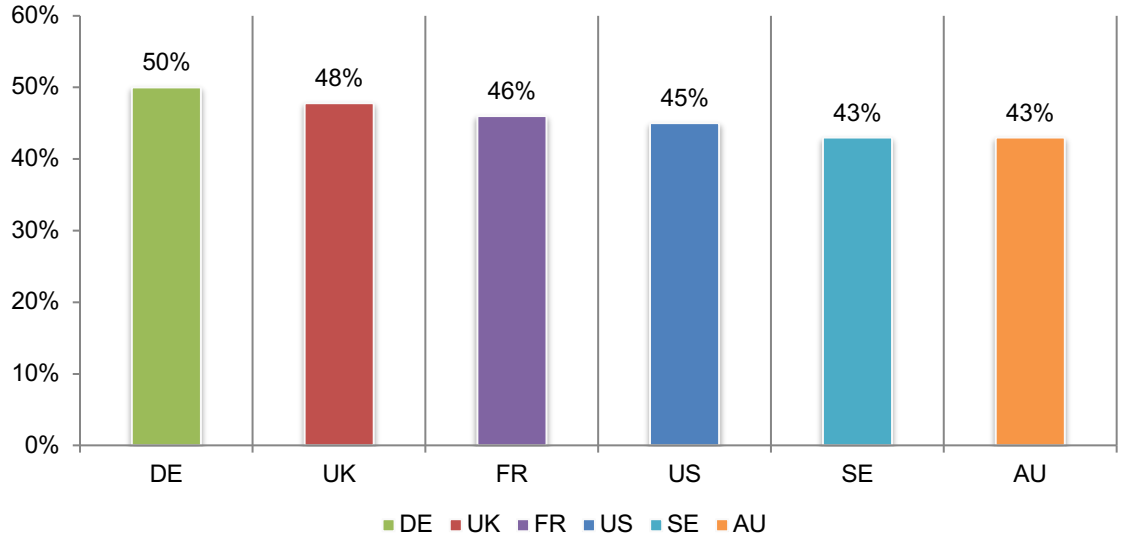
Sweden (57 percent of respondents) and Germany (56 percent of respondents) are most likely to strictly enforce the policy as shown in Figure 40.

Figure 40. If yes, does your organization strictly enforce this policy?
Yes responses permitted



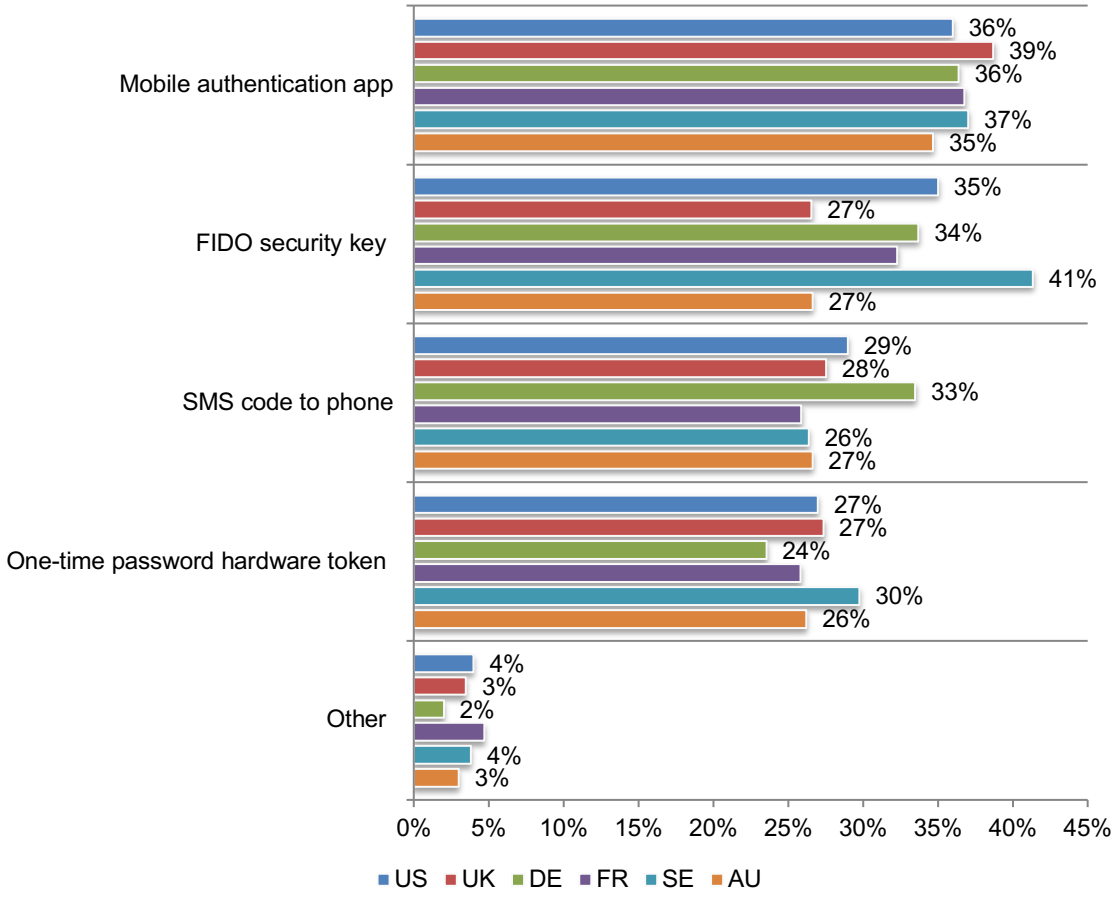
With the exception of German respondents (50 percent), less than half of respondents in the other countries say their organizations require the use of two-factor authentication to gain access to business accounts, according to Figure 41.

Figure 41. Does your organization require the use of two-factor authentication to gain access to business accounts?
Yes responses presented



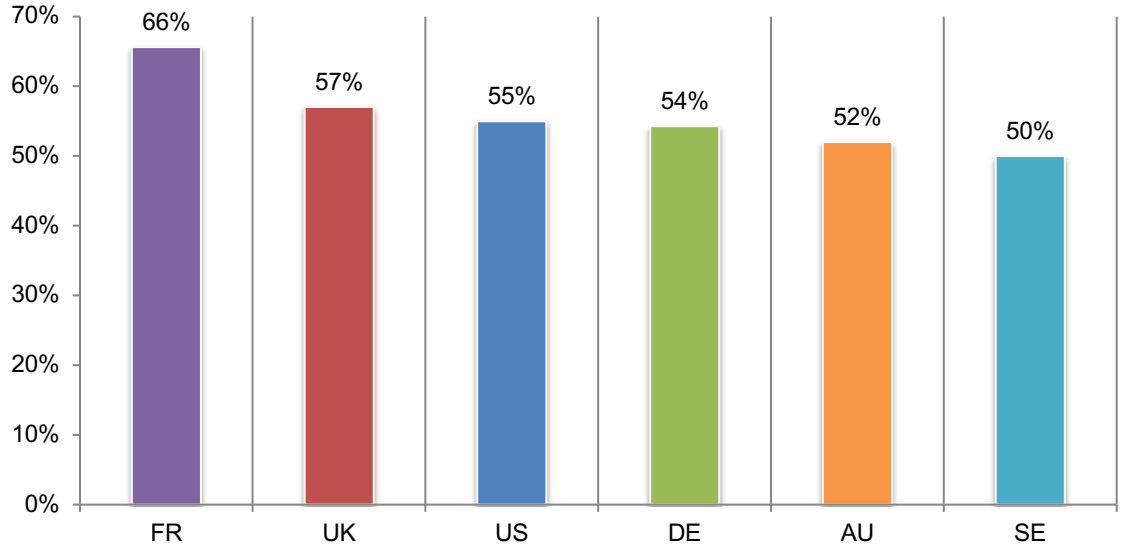
The type of two-factor authentication used to access business accounts varies by country. According to Figure 42, more respondents in Sweden say their organizations use a security key and respondents in Germany say their organizations primarily use mobile authentication apps (36 percent) and SMS code to phone (33 percent).

Figure 42. What type of two-factor authentication do you use to access business accounts?
More than one response permitted



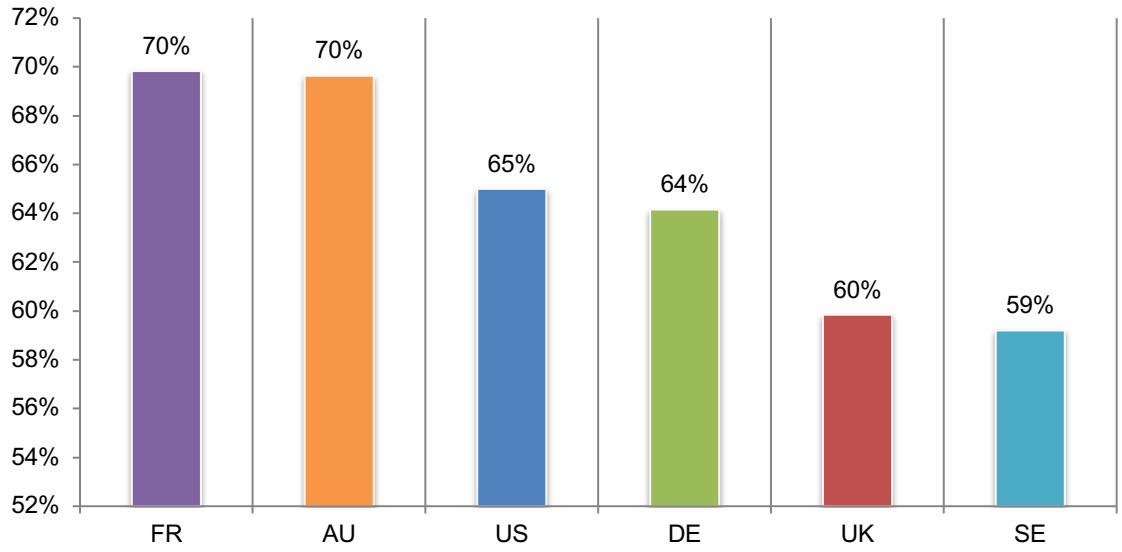
Passwordless authentication is considered to increase the security of authentication in the majority of companies. According to Figure 43, respondents in France are most likely to believe that the security of the authentication process is improved when using passwordless authentication.

Figure 43. Do you believe that passwordless authentication would increase the security of your organization's authentication processes?
Yes responses presented



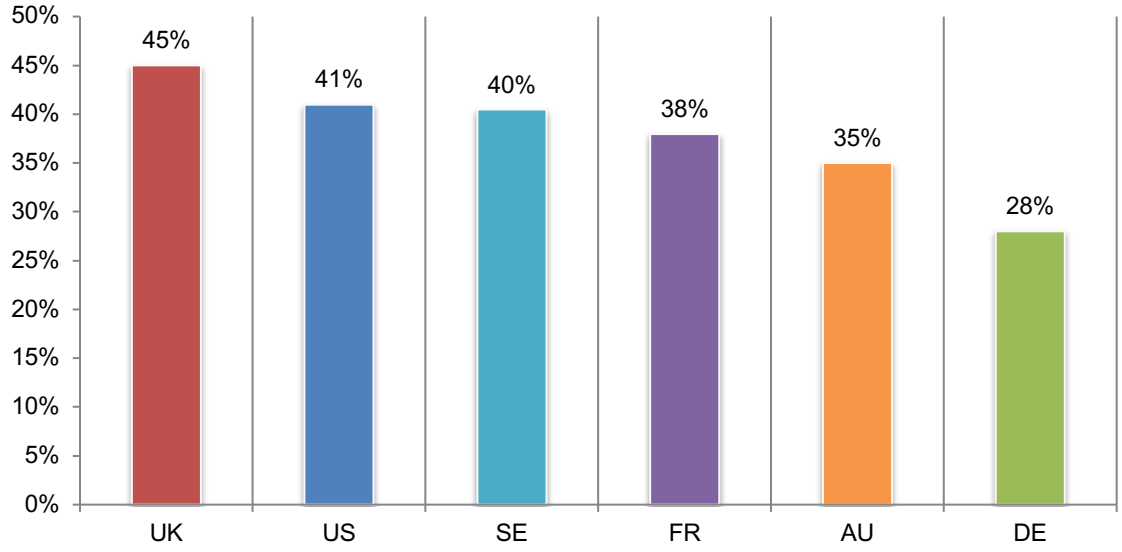
Seventy percent of respondents in France and Australia, as shown in Figure 44, say biometrics improves the security of the authentication process.

Figure 44. Do you believe the use of biometrics would increase the security of your organization's authentication process?
Yes responses presented



Organizations in all countries are failing to take steps to protect their information assets on employees' mobile phones. According to Figure 45, the majority of organizations in France, Australia and Germany do not take steps to protect their information assets on employees' mobile phones.

Figure 45. Does your organization take steps to protect its information assets on employees' mobile phones?
Yes responses presented



Part 3. Methods

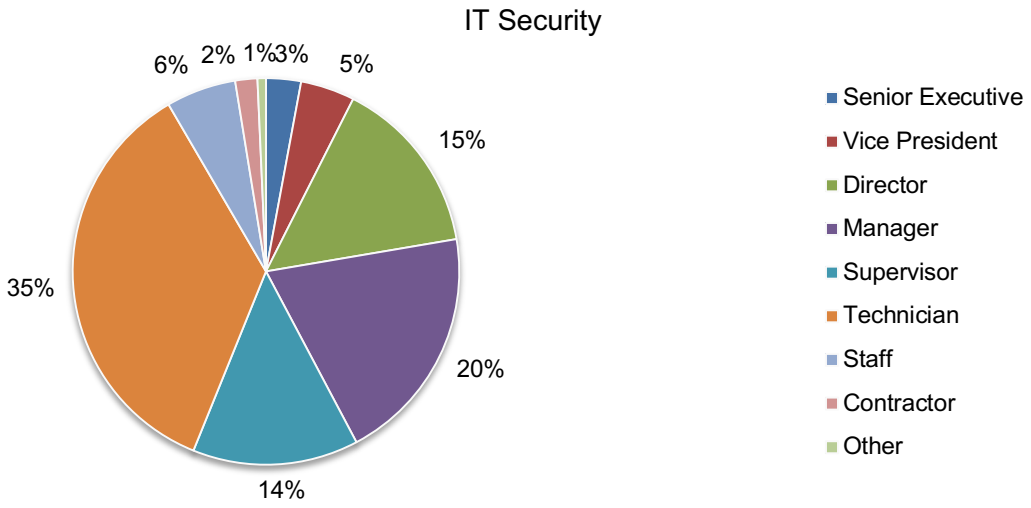
A sampling frame of 66,358 IT or IT security practitioners located in the United States, the United Kingdom, Germany, France, Sweden and Australia were selected as participants in the research. Table 1 shows that there were 2,787 total returned surveys. Screening and reliability checks led to the removal of 280 surveys. Our final sample consisted of 2,507 surveys, a 3.8 percent response.

A second sample of 15,878 individual users were also selected as participants in the research. =Table 1 shows that there were 625 total returned surveys. Screening and reliability checks led to the removal of 62 surveys. Our final sample consisted of 563 surveys, a 3.5 percent response.

Table 1. Sample response	IT Security	Individual User
Sampling frame	66,358	15,878
Total returns	2,787	625
Rejected or screened surveys	280	62
Final sample	2,507	563
Response rate	3.8%	3.5%

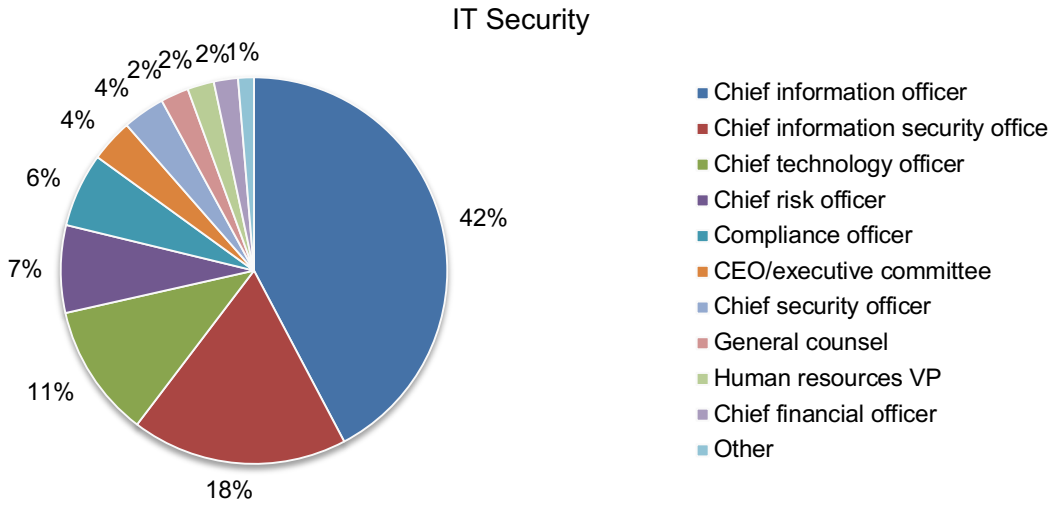
Pie Chart 1 reports the IT security respondents' organizational level within participating organizations. By design, more than half of these respondents (57 percent) are at or above the supervisory levels. Thirty-five percent of these respondents report their position level as technician.

Pie Chart 1. Position level within the organization



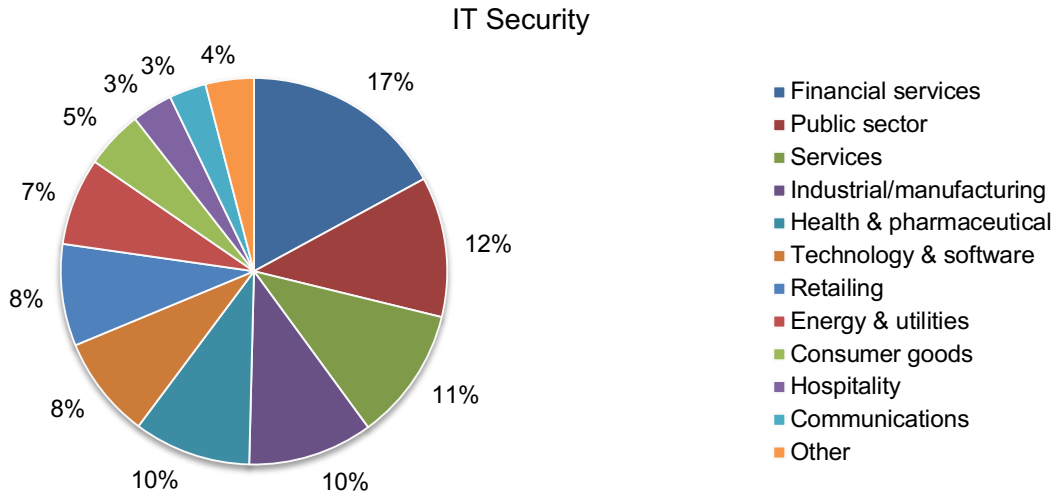
Pie Chart 2 identifies the primary person to whom the IT security respondent reports. Forty-two percent of IT security respondents identified the chief information officer as the person to whom they report. Another 18 percent indicated they report directly to the chief information security officer and 11 percent of these respondents report to the chief technology officer.

Pie Chart 2. Distribution of respondents according to reporting channel



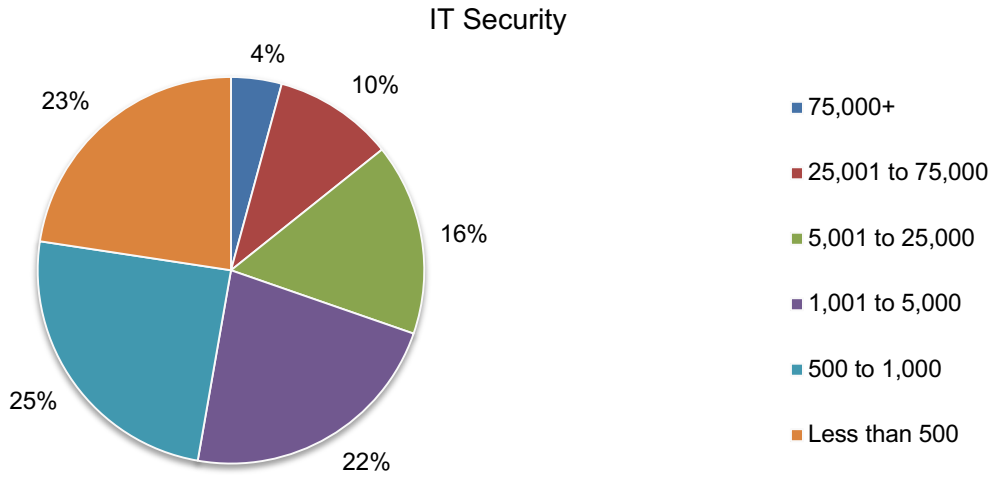
Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by public sector (12 percent of respondents), services (11 percent of respondents), industrial/manufacturing (10 percent of respondents), and health and pharmaceutical (10 percent of respondents).

Pie Chart 3. Distribution of respondents according to primary industry classification



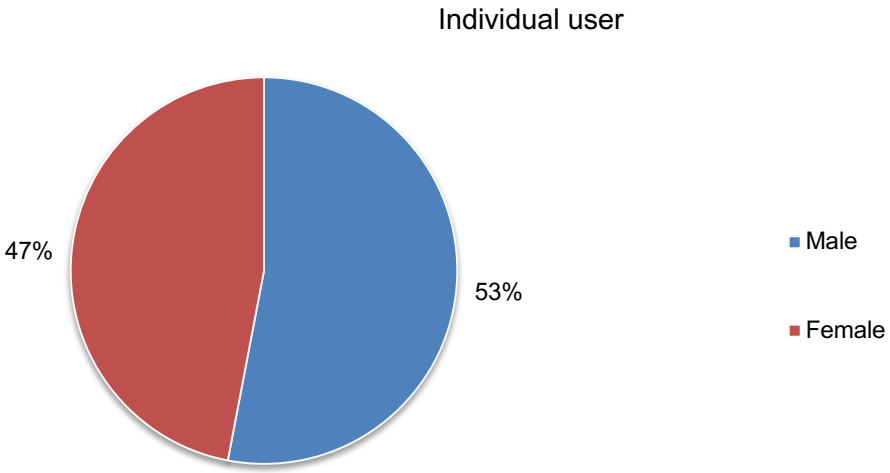
According to Pie Chart 4, more than half of IT security respondents (52 percent) are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 4. Distribution of respondents according to full-time global head count



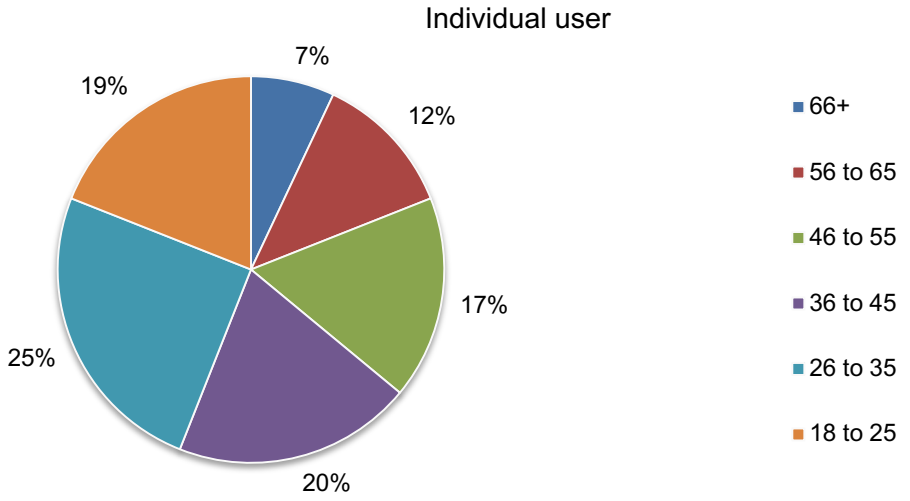
Fifty-three percent of Individual user respondents are female and forty-seven percent of Individual user respondents are male, as shown in Pie Chart 5.

Pie Chart 5. Distribution of individual user respondents according to gender



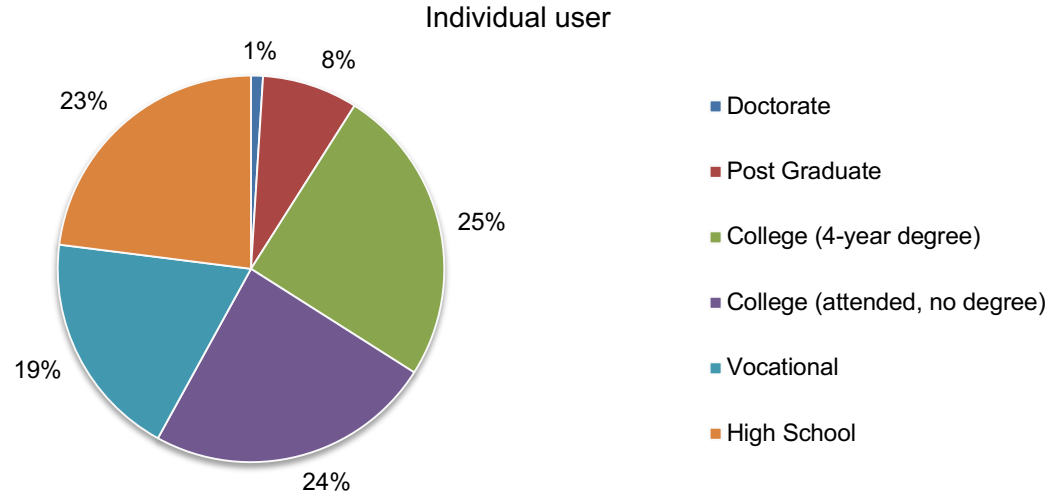
Sixty-four percent of Individual user respondents are between the ages of 18 to 45, as shown in Pie Chart 6.

Pie Chart 6. Distribution of individual user respondents according to highest level of education
Extrapolated value 38.2



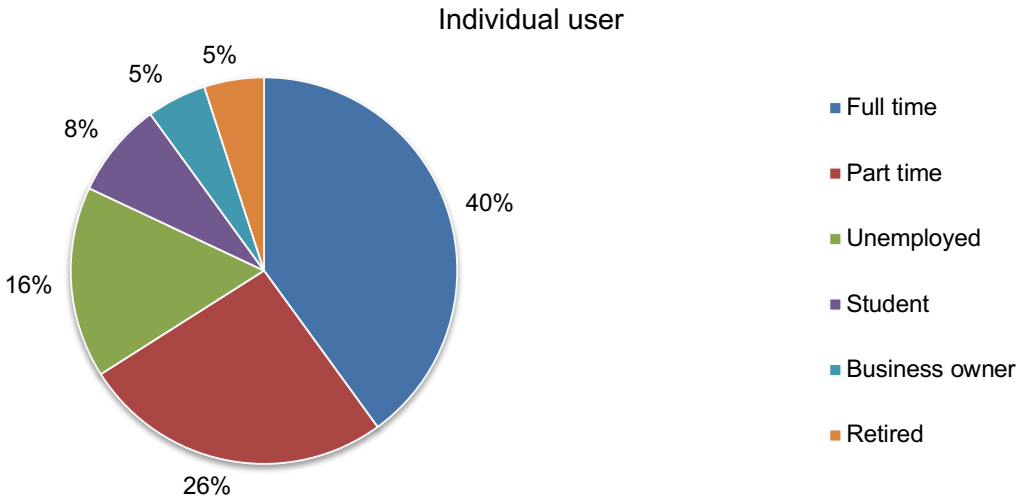
More than half (58 percent) of Individual user respondents reported their highest level of education as at least attending a college (no degree) to doctorate, as shown in Pie Chart 7.

Pie Chart 7. Distribution of individual user respondents according to age



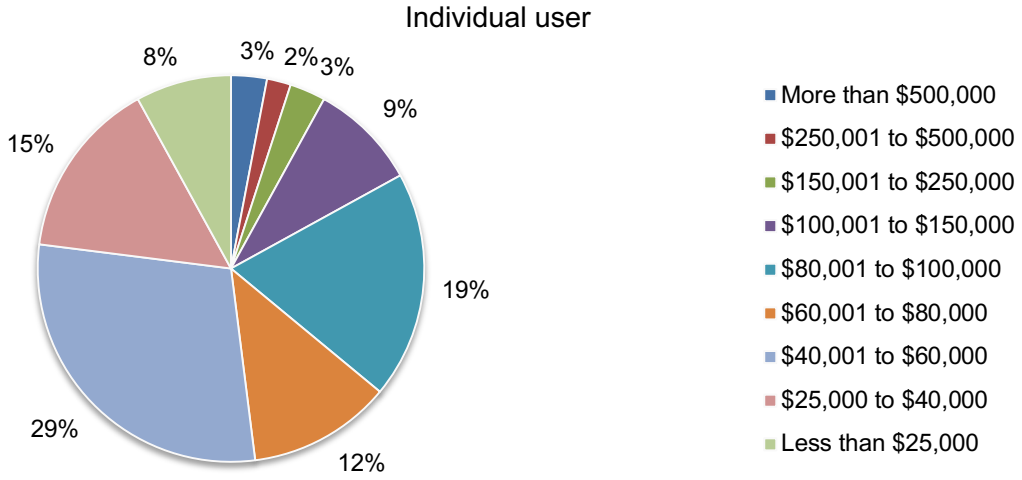
Forty percent of Individual user respondents reported their employment as full time, 26 percent of individual respondents reported part time employment and 16 percent of Individual respondents reported they are unemployed. Eighteen percent of Individual respondents are students (8 percent), business owners (5 percent) and retired (5 percent), as shown in Pie Chart 8.

Pie Chart 8. Distribution of individual user respondents according to employment status



The majority (75 percent) of Individual user respondents reported their income levels to be between $25,000 and $100,000, as shown in Pie Chart 9.

Pie Chart 9. Distribution of individual user respondents according to household income
Extrapolated value $88,625



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 two samples of survey returns. We sent surveys to a representative sample of IT and IT security and 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 IT and IT security practitioners who are IT or IT security practitioners in various organizations the United States, the United Kingdom, Germany, France, Sweden and Australia. 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. Similarly, the accuracy is based on contact information and the degree to which the list is representative of Individuals.

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 October 24 to November 15, 2019.

Survey response	IT Security
Total sampling frame	66,358
Total returns	2,787
Rejected surveys	280
Final sample	2,507
Response rate	3.8%

Part 1. Screening

S1. In your organization, which of the following are you responsible for or supervise? Please select all that apply.	IT Security
Information security	49%
Data privacy	19%
Governance, risk and compliance	41%
Incident response & management	39%
Network security architecture	32%
Security for virtualized or cloud networks	41%
Threat detection and remediation	41%
Vulnerability assessment and penetration testing	37%
Identity management	46%
Security operations management (SOM/SOC)	58%
None of the above	0%
Total	402%

Part 2. The impact of privacy and security concerns on password and authentication practices

Q1a. Have you become alarmed or more concerned about the privacy and security of your personal data over the past two years?	IT Security
Yes, I am highly alarmed about the privacy and security of my personal data	37%
Yes, I am concerned about the privacy and security of my personal data	21%
Yes, I am somewhat concerned about the privacy and security of my personal data	10%
No, I am not concerned about the privacy and security of my personal data	31%
Total	100%

Q1b. If yes, why are you alarmed or more concerned? Please select your top four reasons.	IT Security
I became a victim of a data breach	29%
I became a victim of identity theft	14%
I have growing concerns about government surveillance	61%
I use social media more often	26%
I am using location tracking devices more often	25%
I am using more connected devices (i.e. smart car or smart home devices)	41%
I know someone who became a victim of a data breach	34%
I know someone who became a victim of a identity theft	22%
I am using my mobile devices such as smartphones and tablets more often	53%
I use mobile payment methods including mobile wallet	33%
More of my personal information, including medical records, is being shared with third parties	37%
My concern about the privacy or security of my personal data has not changed	26%
Total	400%

Q2. What personal information are you most concerned about protecting? Please select your top five choices.	IT Security
Browser settings & histories	23%
Credit/debit card information	42%
Login credentials	44%
Email address	26%
Health status	59%
Employer/job information	19%
Investment information	19%
Home address	7%
Marital status	0%
Name	2%
Payment account details	36%
Photos and videos	35%
Physical location (GPS)	40%
Social Security number or Citizen ID	47%
Total	400%

Q3a. Have you ever been the victim of an account takeover or hacking of your personal account?	IT Security
Yes	20%
No	67%
Do not know	12%
Total	100%

Q3b. If yes, did it change how you manage your passwords or protect your accounts?	IT Security
Yes	65%
No	35%
Total	100%

Q4a. Do you reuse passwords across any of your **personal** accounts?	IT Security
Yes	50%
No	50%
Total	100%

Q4b. If yes, on average how many of your **personal** accounts have passwords that have been reused?	IT Security
1 to 5	28%
6 to 10	25%
11 to 15	30%
16 to 20	14%
More than 20	3%
Total	100%
Extrapolated value	10.0

Q5a. Do you use two-factor authentication to protect your **personal** accounts?	IT Security
Yes	40%
No	60%
Total	100%

Q5b. If yes, what type of two-factor authentication do you use?	IT Security
SMS code to phone	26%
Mobile authentication app	34%
FIDO security key	28%
One-time password hardware token	35%
Other	2%
Total	125%

Q5c. If yes, what type of accounts do you secure with two-factor or multi-factor authentication?	IT Security
Banking/financial	43%
Cloud single-sign-on	24%
Developer tools	12%
Password manager	31%
Cloud storage	24%
Email	55%
Shopping	51%
Social media	48%
Cryptocurrency	16%
Gaming	11%
Computer login/access	24%
Total	338%

Part 3. Security practices in the workplace

Q6. What business information are you most concerned about protecting? Please check your top 4 choices.	IT Security
Customer information	58%
Personally Identifiable Information (PII)	60%
Confidential financial information	38%
Non-confidential financial information	24%
Salary (compensation) information	43%
Email and text messages	32%
Trade secrets	31%
R&D	30%
Marketing and sales	40%
Employee information	41%
Other	3%
Total	400%

Q7a. Has your organization experienced any of the following attacks? Please select all that apply.	IT Security
Phishing	51%
Credential theft	12%
Man-in-the-middle attack	8%
Ransomware	16%
Do not know	13%
Our organization has not experienced any of these attacks	32%
Total	132%

Q7b. If your organization experienced any of these attacks, did it change how it manages passwords or protects corporate accounts?	IT Security
Yes	53%
No	47%
Total	100%

Q8. Does your organization take any of the following steps to increase corporate security? Please select all that apply.	IT Security
Require periodic password changes	67%
Require use of a password manager	36%
Assign randomly chosen passwords	45%
Require minimum password lengths	62%
Prohibit employees from reusing the same password on internal systems	65%
Require two-factor or multi-factor authentication	50%
Provide an alternative to keyboard entry (i.e. voice recognition, biometrics)	44%
Monitor third-party sites where compromised passwords are shared	22%
Other (please specify)	2%
We do not take any of these steps	20%
Total	413%

Q9a. Does your organization have a password policy for employees?	IT Security
Yes	67%
No	30%
Do not know	3%
Total	100%

Q9b. If yes, does your organization strictly enforce this policy?	IT Security
Yes	41%
No	54%
Do not know	5%
Total	100%

Q10. What does your organization use to manage and protect its passwords?	IT Security
Password manager	31%
Spreadsheets	29%
Sticky notes	42%
Human memory	59%
Browser extensions that autofill passwords or remember users' passwords	36%
Other	2%
Total	198%

Q11. What is the **total** number of workplace accounts do you have now or had at one time? Include those accounts you don't access or use that often.	IT Security
1 to 5	11%
6 to 10	16%
11 to 15	28%
16 to 25	32%
26 to 35	10%
More than 35	4%
Total	100%
Extrapolated value	15.5

Q12a. Do you reuse personal or business passwords for any of your workplace accounts?	IT Security
Yes	50%
No (skip to Q18)	50%
Total	100%

Q12b. If yes, how many workplace accounts have reused passwords?	IT Security
1 to 5	26%
6 to 10	22%
11 to 15	22%
16 to 25	18%
26 to 35	11%
More than 35	0%
Total	100%
Extrapolated value	12.0

Q13. Do you share passwords with colleagues to access business accounts?	IT Security
Yes, frequently	16%
Yes, sometimes	33%
Rarely	17%
Never	34%
Total	100%

Q14. Does your organization require the use of two-factor authentication to gain access to business accounts?	IT Security
Yes	46%
No	50%
Unsure	4%
Total	100%

Q15. What type of two-factor authentication do you use to access business accounts?	IT Security
SMS code to phone	28%
Mobile authentication app	37%
FIDO security key	33%
One-time password hardware token	27%
Other	4%
Total	128%

Q16. What types of business accounts or information are protected with two-factor authentication?	IT Security
Email	46%
Identity Access Manager	40%
Privileged Access Manager	43%
Password Manager	52%
Social Media	32%
Corporate Server	55%
Computer Login	62%
Other	1%
Total	330%

Q17. Does your organization enable two-factor authentication for all employees or just privileged users?	IT Security
All employees	44%
Only privileged users	53%
Do not know	3%
Total	100%

Q18. What percentage of your employees are privileged users?	IT Security
Less than 5 percent	18%
5 to 10 percent	24%
11 percent to 25 percent	25%
26 percent to 50 percent	19%
51 percent to 75 percent	9%
76 percent to 100 percent	5%
Total	100%
Extrapolated value	23%

Part 4. Security for customers

Q19. Does your organization provide or plan to provide an online service or application for customers that requires authentication?	IT Security
Yes	59%
No	41%
Total	100%

Q20. Have your customer accounts ever been subject to account takeover?	IT Security
Yes	59%
No	42%
Total	100%

Q21a. Does your organization provide or plan to provide two-factor authentication for your customers?	IT Security
Yes, we currently provide two-factor authentication **for all** customer accounts	19%
Yes, we currently provide two-factor authentication **for some** customer accounts	14%
Yes, we plan to provide two-factor authentication **for all** customer accounts within one year	29%
Yes, we plan to provide two-factor authentication **for some** customer accounts within one year	13%
No, we have no near-term plans to provide two-factor authentication for customer accounts	25%
Total	100%

Q21b. What are the primary reasons that your organization provides or plans to provide two-factor authentication for customer accounts? Please select your top two choices.	IT Security
Improves security for customers	62%
Minimizes risk for the organization	43%
Reduces account takeovers	58%
Achieves compliance with privacy and security regulations	35%
Other	1%
Total	200%

Q21c. If yes, what are the two-factor authentication options you provide or plan to provide to your customers?	IT Security
Backup codes	40%
SMS code to phone	41%
Mobile authentication app	37%
FIDO security key	36%
One-time password hardware token	32%
Other	2%
Total	187%

Q22. If no, why would your organization choose not to have two-factor authentication for customers?	IT Security
Usernames and passwords provide sufficient account security	60%
Two-factor authentication has not been requested	39%
The lack of convenience caused by adding an extra step during login	47%
Two-factor authentication is not a priority	33%
Other	3%
Total	195%

Part 5. Passwordless authentication in the workplace

Q23. Have you ever needed access to critical information for your work but forgot the password?	IT Security
Very frequently	13%
Frequently	30%
Not frequently	24%
Rarely	20%
Never	14%
Total	100%

Q24. 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?	IT Security
Very frequently	19%
Frequently	30%
Not frequently	21%
Rarely	16%
Never	14%
Total	100%

Q25. Would you prefer a method of protecting your business accounts that doesn't involve the use of passwords?	IT Security
Yes	55%
No	45%
Total	100%

Q26a. Do you believe that passwordless authentication would increase the security of your organization's authentication processes?	IT Security
Yes	56%
No	44%
Total	100%

Q26b. If yes, what are the primary benefits? Please select your top two choices.	IT Security
Reduces help desk calls	47%
Convenience	54%
More cost effective than other password authentication processes	45%
Provides complete visibility over employees' access to our organization's information assets	52%
Other	1%
Total	200%

Q26c. If no, why would your organization not use passwordless authentication? Please select your top two choices.	IT Security
Too expensive	26%
Not as secure as other methods of two-factor or multi-factor authentication	50%
Not familiar with passwordless authentication	27%
Not enough IT resources to make the transition to passwordless authentication	35%
Strong authentication is not a current priority for our organization	22%
Our current password authentication process works well	38%
Other	1%
Total	200%

Q27. Does your organization have or plan to have passwordless login for employees' accounts?	IT Security
Yes, we have passwordless login for some of our employees' accounts	24%
Yes, we plan to have passwordless login scenarios for employees in the future	44%
We have no plans to have passwordless login for any of our employee accounts	31%
Total	100%

Q28. Does your organization have or plan to have passwordless login for customers' accounts?	IT Security
Yes, we have passwordless login for some of our customers	23%
Yes, we plan to have passwordless login scenarios for our customers in the future	41%
We have no plans to have passwordless login for any of our customers	37%
Total	100%

Q29a Do you believe the use of biometrics (i.e. fingerprint, facial scan) would increase the security of your organization's authentication processes?	IT Security
Yes	65%
No	35%
Total	100%

Q29b. If yes, what are the two biggest benefits of using biometrics for account login?	IT Security
Unique to each user	44%
Increased security	66%
Simplicity and ease of use	50%
Fast account login	38%
Other	1%
Total	200%

Q30. Do you believe that the use of biometrics provides enough security to be used as a single form of account login?	IT Security
Yes	44%
No, it should be combined with another form of authentication	56%
Total	100%

Q31. Do you believe you would have better security if you were offered a physical hardware token to log in to your business and/or personal accounts?	IT Security
Yes	52%
No	35%
Unsure	14%
Total	100%

Q32. How familiar are you with hardware security keys based on FIDO2 and other similar authentication protocols?	IT Security
Very familiar	16%
Familiar	34%
Somewhat familiar	35%
Not familiar	15%
Total	100%

Q33. Does your organization use FIDO security keys?	IT Security
Yes	29%
No	71%
Total	100%

Part 6. The use of personal mobile devices in the workplace

Q34a. Does your organization allow the use of personal mobile devices in the workplace (e.g. BYOD)?	IT Security
Yes	55%
No	45%
Total	100%

Q34b. If yes, what type of mobile device is allowed? Please select only one.	IT Security
Personal mobile device (e.g. BYOD)	45%
Corporate office sanctioned device	32%
A combination of both	23%
Total	100%

Q35. What percentage of employees use their mobile device for work?	IT Security
Less than 10 percent	6%
10 percent to 25 percent	19%
26 percent to 50 percent	37%
51 percent to 75 percent	22%
76 percent to 100 percent	16%
Total	100%
Extrapolated value	45%

Q36. Does your organization take steps to protect its information assets on employees' mobile phones?	IT Security
Yes	38%
No	62%
Total	100%

Q37a. Do you use any two-factor/multi-factor authentication methods when you log into your work apps on your mobile device?	IT Security
Yes	45%
No	55%
Total	100%

Q37b. If yes, which method do you use?	IT Security
SMS code to phone	33%
Mobile authentication app	34%
FIDO security key	23%
One-time password hardware token	27%
Other	2%
Total	120%

Q38. Using the following 10-point scale, please rate the effectiveness of your organization's ability to protect its information assets on employees' mobile phones on a scale from 1 = low effectiveness to 10 = high effectiveness.	IT Security
1 or 2	7%
3 or 4	10%
5 or 6	27%
7 or 8	29%
9 or 10	27%
Total	100%
Extrapolated value	6.69

Part 7. Organizational Characteristics

D1. What best describes your position level within the organization?	IT Security
Senior Executive	3%
Vice President	5%
Director	15%
Manager	20%
Supervisor	14%
Technician	35%
Staff	6%
Contractor	2%
Other	1%
Total	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization	IT Security
CEO/executive committee	4%
Chief financial officer	2%
General counsel	2%
Chief information officer	42%
Chief technology officer	11%
Compliance officer	6%
Human resources VP	2%
Chief security officer	4%
Chief information security office	18%
Chief risk officer	7%
Other	1%
Total	100%

D3. What industry best describes your organization's industry focus?	IT Security
Agriculture & food services	1%
Communications	3%
Consumer goods	5%
Defense & aerospace	1%
Education & research	1%
Energy & utilities	7%
Financial services	17%
Health & pharmaceutical	10%
Hospitality	3%
Industrial/manufacturing	10%
Public sector	12%
Retailing	8%
Services	11%
Technology & software	8%
Transportation	1%
Other	0%
Total	100%

D4. What is the worldwide headcount of your organization?	IT Security
Less than 500	23%
500 to 1,000	25%
1,001 to 5,000	22%
5,001 to 25,000	16%
25,001 to 75,000	10%
75,000+	4%
Total	100%

Survey response	Individual user
Total sampling frame	15,878
Total returns	625
Rejected surveys	62
Final sample	563
Response rate	3.5%

Part 1. Personal Security Behaviors and Beliefs

Q1a. Have you become more concerned about the privacy and security of your personal data over the past two years?	Individual user
Yes, I am highly alarmed about the privacy and security of my personal data	25%
Yes, I am concerned about the privacy and security of my personal data	22%
Yes, I am somewhat concerned about the privacy and security of my personal data	28%
No, I am not concerned about the privacy and security of my personal data (please skip to Q2)	25%
Total	100%

Q1b. If yes, why are you more concerned? Please select your top four reasons.	Individual user
I became a victim of a data breach	40%
I became a victim of identity theft	32%
I have growing concerns about government surveillance	15%
I use social media more often	35%
I am using location tracking devices more often	25%
I am using more connected devices (i.e. smart car or smart home devices)	43%
I know someone who became a victim of a data breach	12%
I know someone who became a victim of identity theft	27%
I am using my mobile devices such as smartphones and tablets more often	46%
I use mobile payment methods including mobile wallet	33%
More of my personal information, including medical records, is being shared with third parties	57%
My concern about the privacy or security of my personal data has not changed	35%
Total	400%

Q2. What personal information are you most concerned about protecting? Please select your top four choices.	Individual user
Browser settings & histories	19%
Credit/debit card information	50%
Login credentials	44%
Email address	21%
Health status	59%
Employer/job information	20%
Investment information	12%
Home address	6%
Marital status	3%
Name	4%
Payment account details	34%
Photos and videos	35%
Physical location (GPS)	40%
Social Security number (SSN)	48%
Other (please specify)	5%
Total	400%

Part 2. Attributions. Please select **one statement only** and rate it using the agreement scale provided. **Strongly agree and Agree.**	Individual user
Q3a. I do not spend a significant amount of time securing my accounts because it is only a matter of time until I get hacked.	45%
Q3b. I want to improve the security of my accounts and have already added extra layers of protection beyond a username and password.	49%
Q3c. I will only adopt a new security practice or technology if it is easy to use and significantly increases my account security.	56%

Part 3. Personal Security Behaviors and Beliefs

Q4a. Have you ever been the victim of an account takeover or the hacking of a personal account?	Individual user
Yes	35%
No (please skip to Q5a)	63%
I do not know (please skip to Q5)	2%
Total	100%

Q4b. If yes, did it change how you manage your passwords or protect your accounts?	Individual user
Yes	76%
No	24%
Total	100%

Q4c. How did you change the way you manage passwords or protect your accounts? Please select all that apply.	Individual user
I now use stronger passwords	61%
I change passwords more frequently	52%
I use unique passwords for as many accounts as possible	36%
I use a password manager	29%
I added two-factor or multi-factor authentication where possible	35%
Other (please specify)	3%
Total	216%

Q5a. Do you reuse passwords across any of your **personal** accounts?	Individual user
Yes	54%
No (please skip to Q6)	46%
Total	100%

Q5b. If yes, on average how many of your **personal** accounts have passwords that have been reused?	Individual user
1 to 5	24%
6 to 10	31%
11 to 15	29%
16 to 20	10%
More than 20	6%
Total	100%
Extrapolated value	10.21

Q6. Do you use two-factor authentication to protect your **personal** accounts?	Individual user
Yes	36%
No (please skip to Q8)	64%
Total	100%

Q7a. If yes, what type of two-factor authentication do you use? Please select all that apply.	Individual user
SMS code to phone	27%
Mobile authentication app	32%
FIDO security key	31%
One-time password hardware token	35%
Other (please specify)	3%
Total	128%

Q7b. If yes, what type of accounts do you secure with two-factor or multi-factor authentication? Please select all that apply.	Individual user
Banking/financial	43%
Cloud single-sign-on	28%
Developer tools	9%
Password manager	29%
Cloud storage	26%
Email	53%
Shopping	55%
Social media	47%
Cryptocurrency	14%
Gaming	10%
Computer login/access	23%
Total	337%

Part 4. Workplace Security Behaviors and Beliefs

Q8. What is the **total** number of workplace accounts do you have now or had at one time? Include those accounts you don't access or use that often.	Individual user
1 to 5	5%
6 to 10	10%
11 to 15	20%
16 to 25	25%
26 to 35	24%
More than 35	16%
Total	100%
Extrapolated value	22.40

Q9a. Do you reuse personal or business passwords for any of your workplace accounts?	Individual user
Yes	39%
No (please skip to Q10)	61%
Total	100%

Q9b. If yes, how many workplace accounts have reused passwords?	Individual user
1 to 5	13%
6 to 10	18%
11 to 15	32%
16 to 25	20%
26 to 35	13%
More than 35	4%
Total	100%
Extrapolated value	15.66

Q10. Do you share passwords with colleagues to access business accounts?	Individual user
Yes, frequently	14%
Yes, sometimes	37%
Rarely	13%
Never	36%
Total	100%

Q11a. Does your organization have a policy pertaining to employees' use of passwords?	Individual user
Yes	55%
No (Please skip to Q12)	34%
Unsure (Please skip to Q12)	11%
Total	100%

Q11b. If yes, does your organization strictly enforce this policy?	Individual user
Yes	35%
No	57%
Unsure	8%
Total	100%

Q12. What does your organization use to manage and protect its passwords? Please select all that apply.	Individual user
Password manager	28%
Spreadsheets	30%
Sticky notes	41%
Human memory	59%
Browser extensions that autofill passwords or remember users' passwords	37%
No defined process	30%
Do not know	4%
Other (please specify)	0%
Total	229%

Q13. Does your organization take any of the following steps to improve corporate security? Please select all that apply.	Individual user
Require periodic password changes	44%
Assign randomly chosen passwords	24%
Require minimum password lengths	63%
Prohibit employees from reusing the same password on internal systems	61%
Provide an alternative to keyboard entry (i.e. voice recognition, biometrics)	36%
Monitor third-party sites where compromised passwords are shared	27%
Other (please specify)	3%
We do not take any of these steps	34%
Total	292%

Q14. Does your organization require the use of two-factor authentication to gain access to corporate accounts?	Individual user
Yes	43%
No (please skip to Q16)	51%
Unsure (please skip to Q16)	6%
Total	100%

Q15. What type of two-factor authentication are you required to use?	Individual user
SMS code to phone	30%
Mobile authentication app	35%
FIDO security key	33%
One-time password hardware token	29%
Other (please specify)	3%
Total	130%

Q16. Using the following 10-point scale, please rate the convenience of two-factor authentication methods such as text message verification codes and mobile authenticator apps from 1 = highly inconvenient to 10 = very convenient.	Individual user
1 or 2	8%
3 or 4	15%
5 or 6	28%
7 or 8	26%
9 or 10	23%
Total	100%
Extrapolated value	6.32

Q17. If not convenient (1 to 4 responses) why?	Individual user
Disrupts my workflow	54%
It is irritating to have to copy codes from one app/device to another	47%
Other (please specify)	12%
Total	113%

Part 5. Security Preferences and Views

Q18. Would you spend $50 to $60 to have the highest form of security across all of your online accounts?	Individual user
Yes, it would be worth it	60%
No, because it is too much money to spend on security	37%
Other (please specify)	3%
Total	100%

Q19. Using the following 10-point scale, please rate the importance of having your online information secured as best as possible 1 = not important to 10 = very important	Individual user
1 or 2	3%
3 or 4	5%
5 or 6	7%
7 or 8	29%
9 or 10	56%
Total	100%
Extrapolated value	8.10

Q20. Using the following 10-point scale, please rate the importance of being able to access online information as easy as possible 1 = not important to 10 = very important	Individual user
1 or 2	5%
3 or 4	8%
5 or 6	27%
7 or 8	25%
9 or 10	35%
Total	100%
Extrapolated value	7.04

Q21. Using the following 10-point scale, please rate the importance of not being inconvenienced when logging into online accounts 1 = not important to 10 = very important	Individual user
1 or 2	9%
3 or 4	12%
5 or 6	15%
7 or 8	37%
9 or 10	27%
Total	100%
Extrapolated value	6.72

Q22. Using the following 10-point scale, please rate the importance of having security options that must be affordable from 1 = not important to 10 = very important	Individual user
1 or 2	3%
3 or 4	6%
5 or 6	11%
7 or 8	23%
9 or 10	57%
Total	100%
Extrapolated value	8.00

Q23. Have you ever needed access to critical information for your work but forgot the password?	Individual user
Very frequently	16%
Frequently	22%
Not frequently	21%
Rarely	26%
Never	15%
Total	100%

Q24. 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?	Individual user
Very frequently	13%
Frequently	21%
Not frequently	29%
Rarely	23%
Never	14%
Total	100%

Q25. Would you prefer a method of protecting your personal or work accounts that doesn't involve the use of passwords?	Individual user
Yes	55%
No	45%
Total	100%

Q26. Would you feel you were getting better security if you were offered a physical hardware token to login to business and/or personal accounts?	Individual user
Yes	56%
No	40%
Unsure	4%
Total	100%

Q27. Would you feel you were getting better security if you were able to use your fingerprint or facial scan to login to business and/or personal accounts?	Individual user
Yes	53%
No	42%
Unsure	5%
Total	100%

Part 6. The Use of Personal Mobile Devices for Account Login

Q28. How often do you access your online accounts from a mobile device?	Individual user
Very frequently	33%
Frequently	21%
Somewhat frequently	18%
Rarely	14%
Never	14%
Total	100%

Q29. Do you use any two-factor/multi-factor authentication methods when you log into your personal apps/accounts on your mobile device?	Individual user
Yes	35%
No (please skip to Q31a)	65%
Total	100%

Q30. If yes, how many devices (i.e., phones, computers, tablets, etc.) do you have to access your online accounts?	Individual user
1 to 2	17%
3 to 4	28%
5 to 6	27%
7 to 8	20%
9 to 10	6%
11 to 12	2%
More than 12	0%
Total	100%
Extrapolated value	5.02

Q31a. Do you use your personal mobile device to access work related items?	Individual user
Yes	51%
No (please skip to Q33)	49%
Total	100%

Q31b. If yes, do you use any two-factor/multi-factor authentication methods when you log into your work apps/accounts on your mobile device?	Pct#
Yes	44%
No	56%
Total	100%

Q33. What mobile platform do you use?	Individual user
Android	33%
iOS	37%
Both Android and iOS	25%
Do not know	5%
Total	100%

Part 7. Organizational Characteristics and Demographics

D1. Gender:	Individual user
Female	47%
Male	53%
Total	100%

D2. Age Range:	Individual user
18 to 25	19%
26 to 35	25%
36 to 45	20%
46 to 55	17%
56 to 65	12%
66+	7%
Total	100%
Extrapolated value	38.23

D3. Highest Level of Education:	Individual user
High School	23%
Vocational	19%
College (attended, no degree)	24%
College (4-year degree)	25%
Post Graduate	8%
Doctorate	1%
Total	100%

D4. Employment status	Individual user
Business owner	5%
Full time	40%
Part time	26%
Student	8%
Retired	5%
Unemployed	16%
Total	100%

D5. Household income	Individual user
Less than $25,000	8%
$25,000 to $40,000	15%
$40,001 to $60,000	29%
$60,001 to $80,000	12%
$80,001 to $100,000	19%
$100,001 to $150,000	9%
$150,001 to $250,000	3%
$250,001 to $500,000	2%
More than $500,000	3%
Total	100%
Extrapolated value	$ 88,625

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.