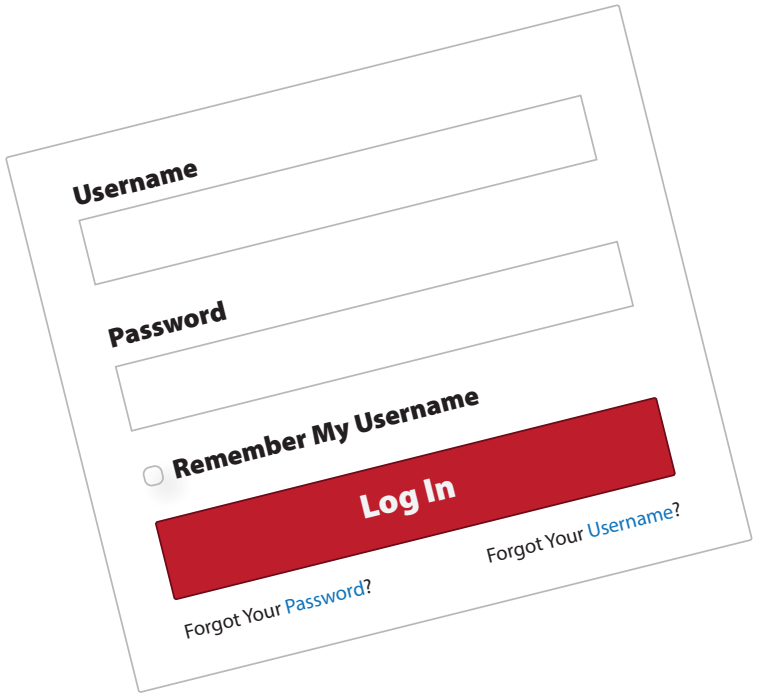
Beyond the Password:
The Future of Account Security



Sponsored by:

TeleSign

Independently conducted by:

LAWLESS ?ESEARCH!

Introduction

In 2015, nearly 800 data breaches occurred in the U.S., exposing more than 169 million records.[1] Compromised passwords were the port of entry for many of these attacks,[2] in large part because consumers frequently reuse passwords on multiple sites, making these accounts particularly susceptible.[3]

Selling credentials on the black market is big business, so cybercrime is an ever-present and growing concern for companies that provide consumer web and mobile accounts. Account takeover (ATO) has become one of the most prevalent types of fraud. An ATO occurs when an unauthorized party gains online access to an existing account and then conducts malicious activities.

Although imperfect, passwords are here to stay for the foreseeable future. To counteract fraud and address the problem of account vulnerability, companies are adding multiple layers of authentication to augment password security. Account security professionals are looking for solutions that enhance security and protect against ATOs without degrading the user experience. Behavioral biometrics is a promising new technology that may meet the dual demands for a solution that is effective and frictionless. And technologies such as two-factor authentication are seeing a rise in adoption as companies seek an additional layer of protection beyond passwords.

This study, conducted by Lawless Research and commissioned by TeleSign, the mobile identity company, describes the steps that medium-sized and large companies are taking to ensure the security of web and mobile accounts. Data are drawn from an online survey of 600 consumer account authentication professionals in U.S. companies with 100 or more employees. The report highlights companies' account security practices and concerns, quantifies their exposure to fraud, estimates the impact of fraud, and forecasts adoption rates of behavioral biometrics and two-factor authentication.

"The research shows that passwords aren't dead yet. Having said that, experts aren't resigning themselves or their users to password-only account security."

–Ryan Disraeli, Co-Founder of TeleSign

1 ID Theft Resource Center 2015 Data Breach Report, January 25, 2016

2 Verizon 2016 Data Breach Investigations Report

3 TeleSign Consumer Account Security Report, June 3, 2015

"The business of fraud has become public enemy number one for mobile and online companies."

–Ryan Disraeli, Co-Founder of TeleSign

Study Highlights

Passwords are no longer sufficient alone to protect accounts

- 69% of companies say that usernames and passwords alone no longer provide sufficient security.
- 3 in 4 companies employ usernames and passwords, but only 7% of companies rely solely on usernames and passwords.
- 36% of companies foresee that they will do away with passwords in 1 to 4 years, and another 36% predict they will no longer use them in 5 to 9 years.
- Passwords are a high-friction authentication method—companies say their users are frustrated by forgetting their username and password (58%) and entering their username and password (30%).

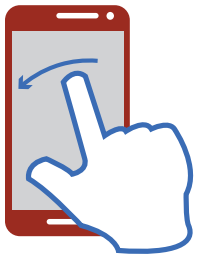
Fraud is pervasive and the impacts are high

- In the past year, 90% of companies experienced fraud—the most common types are spam or phishing attacks (42%), payment or credit card fraud (35%) and fake account fraud (29%).
- The impact of fraud is high, with 42% of companies saying they experienced financial losses.
- Fraud also increased employee time to correct the fraud (45%) and caused a loss of user trust (34%).
- 79% are extremely or very concerned about account takeovers (ATOs).
- 28% of companies were victims of account takeover and costs were higher for these companies—51% had financial losses, 42% lost customers or users, and 42% experienced damage to the company brand.

Multi-layer authentication is standard practice for augmenting password security

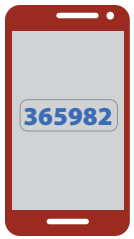
- Companies use an average of 3.4 methods to authenticate users; companies with 10 million or more users employ an average of 4.3 methods.
- 86% of companies are extremely or very concerned about authenticating the identity of web and mobile app users.
- After username and password (74%), knowledge-based authentication (50%), CAPTCHA (44%), and two-factor authentication (41%) are the most commonly used authentication methods.
- The top selection criteria for authentication solutions are effectiveness (53%), functional capabilities (28%) and user experience (26%).

Use of behavioral biometrics is poised to grow dramatically



- 76% of companies have implemented or plan to implement behavioral biometric: 22% are already using the technology and 54% plan to implement behavioral biometrics in 2016 or later.
- 90% of respondents rate behavioral biometrics as an extremely or very valuable technology for increasing account security beyond password protection.
- 83% agree that behavioral biometrics would increase security without adding friction to the user experience.

Majority of companies will be using two-factor authentication within the next 12 months



- 44% of companies are likely to implement 2FA within the year, adding to the 41% of companies that already have 2FA in place.
- 92% of respondents agree that 2FA combined with passwords increases account security.

More than eight out of ten companies are highly concerned about user authentication.

Overall, 86% of companies with consumer accounts are extremely or very concerned about authenticating the identity of web and mobile app users.

Three-fourths of companies employ usernames and passwords for account security.

While usernames and passwords are the most common authentication method, they are used by only 74 percent of companies.

Most Commonly Used Methods to Authenticate Web and Mobile App Users

74%

Username and password

50%

Knowledge-based authentication

44%

CAPTCHA

41%

Two-factor authentication

KEY FINDING: Passwords are no longer sufficient alone to protect and secure accounts

The first computer passwords were invented by Fernando Corbató in 1961 to protect accounts on MIT's Compatible Time Sharing System (CTSS). Only one year later in 1962, the system was hacked and the passwords stolen by MIT researcher Allan Scherr who needed more than his allotted four hours on the CTSS.

Fast forward to 2004, when Bill Gates predicted the death of the password at the RSA Security conference saying, "There is no doubt that over time, people are going to rely less and less on passwords. People use the same password on different systems, they write them down and they just don't meet the challenge for anything you really want to secure."[1]

Twelve years later the password is still an imperfect security technology and not yet extinct. Three-fourths of companies employ passwords to authenticate web and mobile app users, yet two-thirds agree that passwords are insufficient to protect accounts. Only a small number of companies (6 percent) rely solely on usernames and passwords to authenticate consumer accounts.

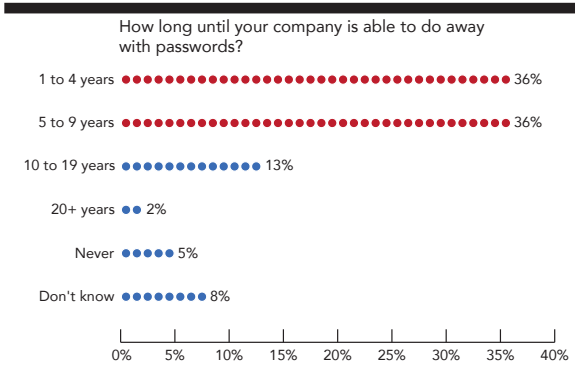
This study shows that passwords may show up on the endangered list within the next decade. One-third of respondents predict their companies will eliminate passwords in one to four years and another third say passwords will no longer be used in five to nine years.

1 CNET, February 25, 2004

A third of companies predict they will do away with passwords in less than 5 years.

More than one-third (36 percent) of companies see an end to passwords in the next four years and another third (36 percent) predict passwords will be obsolete in five to nine years.

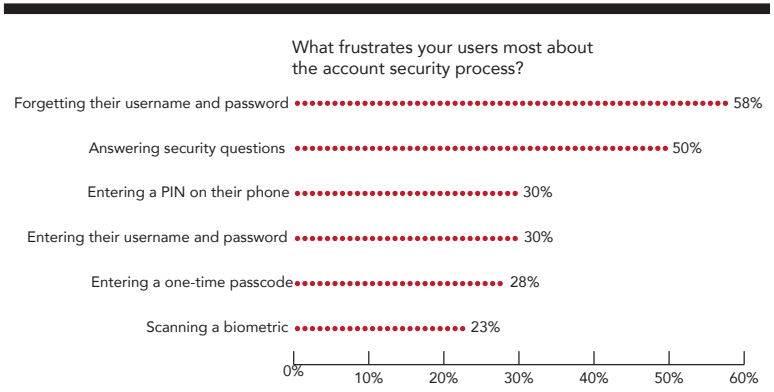
- Four in ten companies in eCommerce or retail (43 percent), software (42 percent) and business services (40 percent) predict that their companies will do away with passwords in the next one to four years. Only one in four companies (25 percent) in banking see an end to using passwords in the next four years.



Forgetting passwords and answering security questions frustrate users most about the account security process.

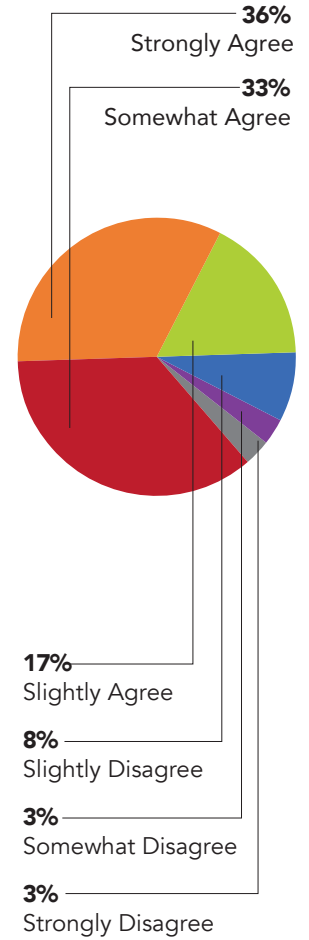
Half of account security professionals believe that forgetting usernames and passwords (58 percent) and answering security questions (50 percent) are the main sources of frustration for their users.

- Companies with 3 million or more users are more likely to say scanning a biometric, such as a fingerprint, is frustrating for their users (29 percent vs. 15 percent of companies with fewer than 3 million users).



Seven in ten companies believe that passwords alone do not protect accounts.

More than two-thirds (69 percent) of respondents strongly or somewhat agree that usernames and passwords no longer provide sufficient account security.

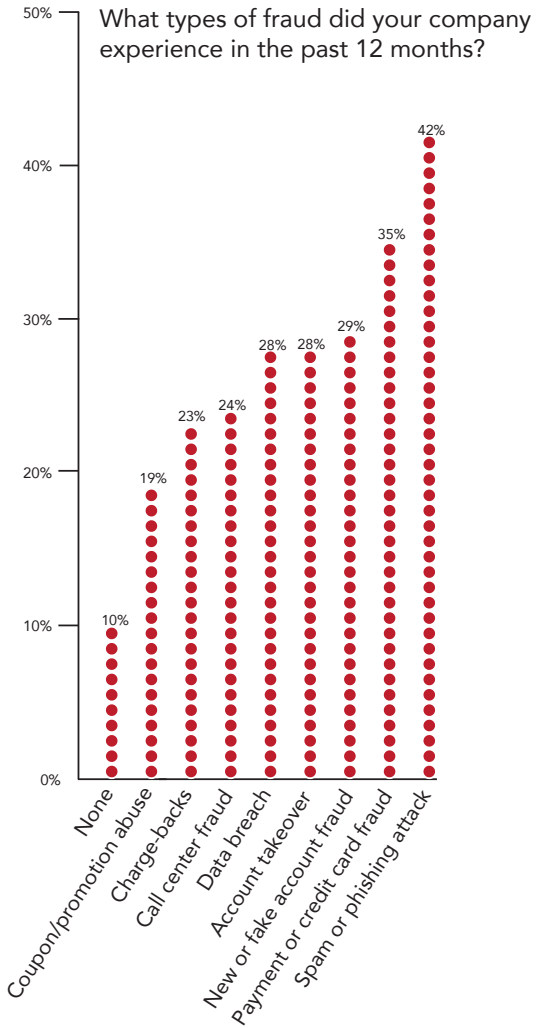


Usernames and passwords no longer provide sufficient account security.

Nine in ten companies experienced one or more forms of fraud in the past 12 months.

The most common types of fraud are spam or phishing attack (42 percent), payment or credit card fraud (35 percent), and new account or fake account fraud (29 percent).

- Companies experienced an average of two types of fraud in the past year.



KEY FINDING: Fraud is pervasive and the impacts are high

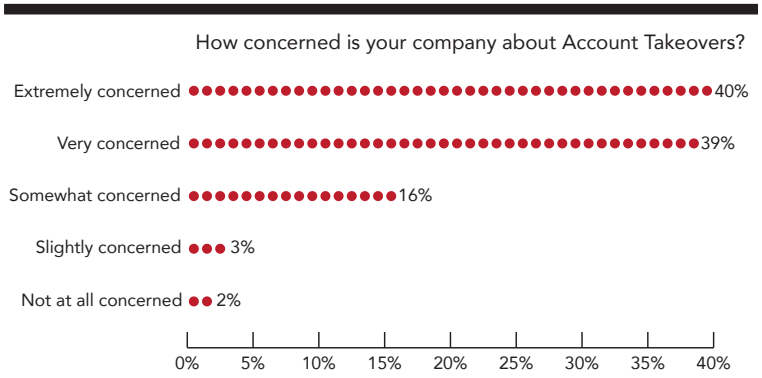
Combatting fraud and mitigating its effects are major challenges for companies that have web and mobile consumer accounts. Despite having multiple layers of security in place, 90 percent of companies fell victim to cybercriminals between April 2015 and March 2016. Attacks ranged from coupon abuse to data breaches and the fraud resulted in financial losses, damage to company brand, and loss of customers.

Of great concern is the prevalence of account takeover (ATO) fraud, which occurred in 28 percent of companies. The theft of hundreds of millions of consumer records by hackers has made account takeover a significant threat. Fraudsters use stolen consumer credentials to access accounts to launch phishing attacks, withdraw money, make unauthorized purchases, harvest virtual currency, and conduct other malicious activities. In an ATO attack, organized crime rings use bot armies to crack passwords on consumer-facing websites and mobile apps. At highest risk are accounts with passwords that are weak or reused on multiple sites. Verizon's 2016 Data Breach Investigations Report found that 63 percent of confirmed breaches involved weak, default or stolen passwords.[1]

1 Verizon 2016 Data Breach Investigations Report

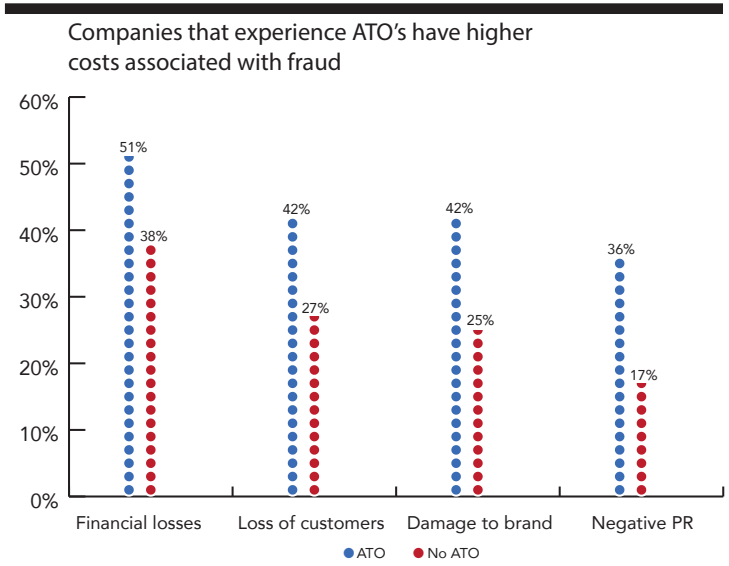
Eight in ten companies are extremely or very concerned about account takeovers.

An ATO occurs when an unauthorized party gains online access to an existing account and then conducts malicious activities. More than three-fourths (79 percent) of companies are extremely or very concerned about account takeovers.



Costs are higher for companies that experienced account takeovers.

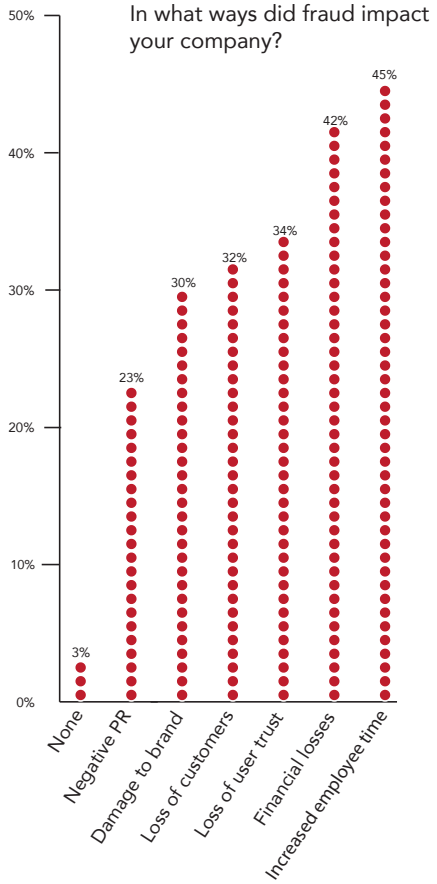
More than one in four companies (28 percent) had account takeovers in the past year. These companies experienced more impacts from fraud than companies without ATOs, including financial losses (51 percent vs. 38 percent), loss of customers or users (42 percent vs. 27 percent), damage to their company's brand (42 percent vs. 25 percent), and negative PR (36 percent vs. 17 percent).



Nine in ten companies that experienced fraud were impacted by the cyberattacks.

Among companies that experienced fraud, 97 percent reported one or more impacts. Four in ten (42 percent) respondents say the fraud caused financial losses and 45 percent say the fraud required employee time to investigate and correct the fraud.

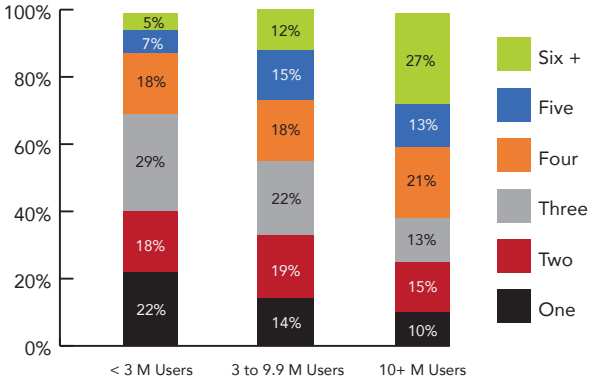
- **Three in ten (34 percent) companies say fraud resulted in loss of user trust, loss of customers or users (32 percent), or damage to their company's brand (30 percent).**



Companies use an average of three methods to authenticate account users.

Overall, companies use 3.4 authentication methods. The number of methods used increases with the number of web and mobile accounts from 2.9 for companies with fewer than 3 million account users to 4.3 for companies with 10 million or more account users.

Number of Authentication Methods Used vs. Number of User Accounts



KEY FINDING: Multi-layer authentication is standard practice for augmenting password security

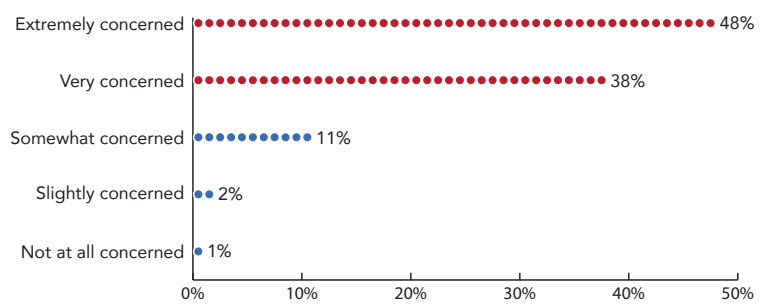
In TeleSign's 2015 Consumer Account Security study, 80 percent of consumers said they worry about their online security, 70 percent lack confidence that passwords can protect their accounts, and 68 percent want companies to provide extra layers of protection.[1]

In response to their users' demand for greater protection, businesses are implementing multiple technologies to authenticate accounts. On average, companies use three methods of authentication. After username and password protection, the most common technologies implemented are knowledge-based authentication, CAPTCHA and two-factor authentication.

More than eight in ten companies are highly concerned about user authentication.

Overall, 86 percent of companies with consumer accounts are extremely or very concerned about authenticating the identity of web and mobile app users.

How concerned is your company about authenticating the identity of web and mobile users?

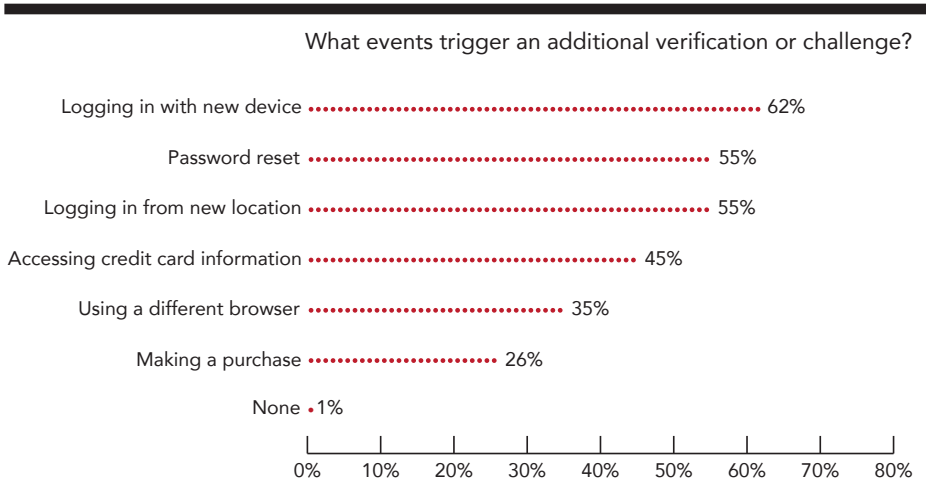


1 TeleSign Consumer Account Security Report, June 3, 2015

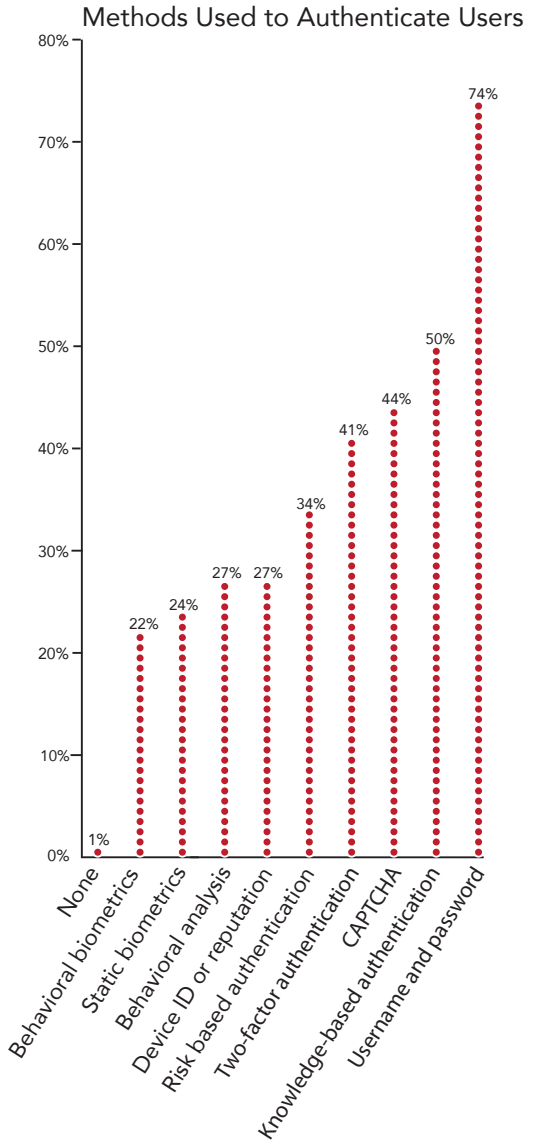
Only 7 percent of companies rely solely on username and password protection.
Companies with fewer than 3 million account users are more likely to use passwords only (10 percent vs. 3 percent of companies with 3 million or more users).

Companies that don't use passwords are less likely to use device ID or device reputation.
One in four companies do not use password protection for their consumer accounts. Companies that don't use passwords are also less likely to use device ID or device reputation (18 percent vs. 31 percent of companies that use passwords), CAPTCHA (35 percent vs. 48 percent) and knowledge-based authentication (34 percent vs. 56 percent).

Almost all companies set conditions for additional verifications or challenges.
Only 1 percent of companies do not have events that trigger an additional verification. Logging in with a new device is the most common trigger, used by six in ten companies. Over half of companies require additional verification when a password is reset or when users log in from a new location.



Seven in ten companies use passwords and five in ten companies use knowledge-based authentication.

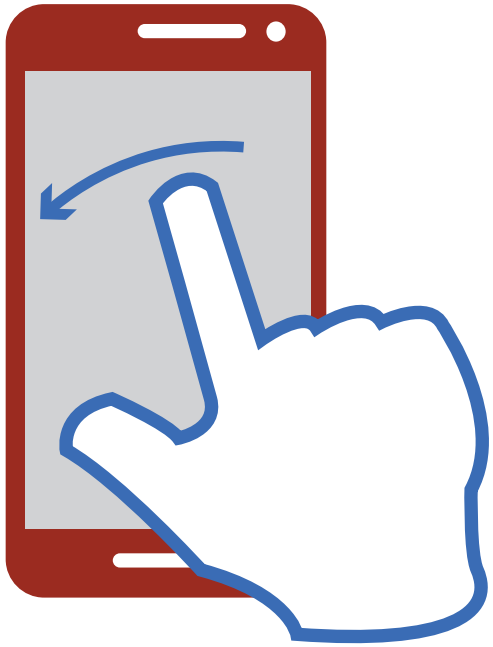


Over half of companies rank effectiveness among their most important selection criteria.

The top criteria for selecting authentication methods are security effectiveness (53 percent), functional capabilities (28 percent) and user experience (26 percent).

What criteria are most important when selecting user authentication solutions? (Choose your top 2.)	
1 Security effectiveness	53%
2 Functional capabilities	28%
3 User experience	26%
4 Ease of management	22%
5 Price	20%
6 Ease of integration	20%
7 Total Cost of Ownership	17%
8 Scalability	15%
Total	200%
N=600	

KEY FINDING: Use of behavioral biometrics is poised to grow dramatically



Behavioral biometrics has emerged as a secure, frictionless method to stop increasingly savvy fraudsters from hijacking legitimate user accounts. Behavioral biometrics is designed to prevent account takeovers by continuously authenticating web and mobile app users. The technology works by recognizing users based on their behavior patterns, such as keystrokes, mouse dynamics and screen interactions. It then uses these patterns to identify anomalies between "approved" users and "bad actors."

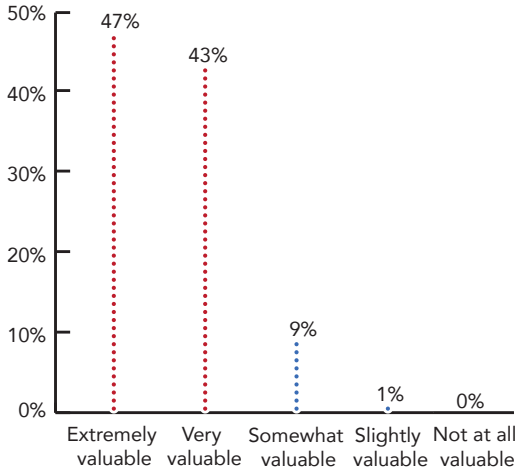
User experience is an important selection criteria and organizations recognize the value of behavioral biometrics as a way to increase account security without degrading the user experience. Two in 10 companies have implemented behavioral biometrics and another five in 10 plan to add it as part of their multilayer authentication strategy. The primary drivers for implementation are to prevent fraudulent transactions, add another layer of security and prevent account takeovers.

Almost all companies rate behavioral biometrics as valuable for increasing user account security beyond password protection.

Nine in ten companies (90 percent) say behavioral biometrics would be extremely or very valuable for increasing user account security.

- **Companies that are extremely concerned about account takeovers rate the value of behavioral biometrics higher (70 percent extremely valuable vs. 32 percent for those less concerned with ATOs).**
- **Companies that are extremely concerned about authenticating account users rate the value of behavioral biometrics higher (65 percent extremely valuable vs. 30 percent for those less concerned with authentication).**

How would you rate the potential value of behavioral biometrics for increasing user account security beyond password protection?



The chief reason for implementing behavioral biometrics is to prevent fraudulent transactions.

What are the reasons your company has implemented or would consider implementing behavioral biometrics?

Prevent fraudulent transactions	58%
Add another layer of security	56%
Prevent account takeovers	53%
Provide frictionless experience for users	43%
None of the above	0%

N=473 companies that have implemented or are considering implementing behavioral biometrics

Concern about cost is the top reason for not implementing behavioral biometrics among companies that have no plans to implement the technology.

What are the reasons your company would not consider implementing behavioral biometrics?

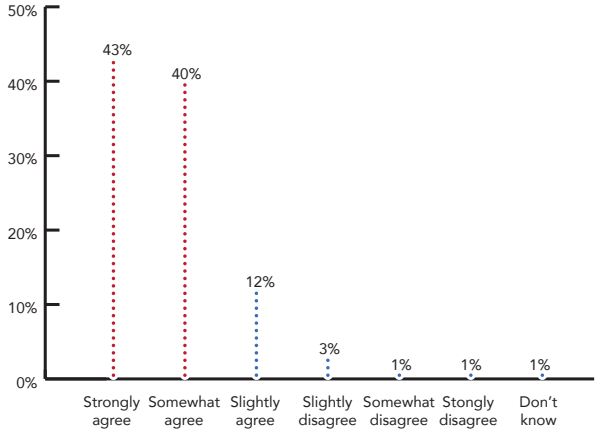
The cost is too high	42%
Uncertain of the effectiveness	37%
Concern about consumers' resistance	27%
Lack of knowledge of technology	23%
We build technology in-house	20%
Account Takeovers are not a problem	18%
None of the above	3%

N=71 companies that are not considering behavioral biometrics

Eight in ten companies say adding behavioral biometrics would increase security without degrading the user experience.

A total of 83 percent of respondents strongly or somewhat agreed that adding behavioral biometrics to traditional password protection would increase security without degrading the user experience.

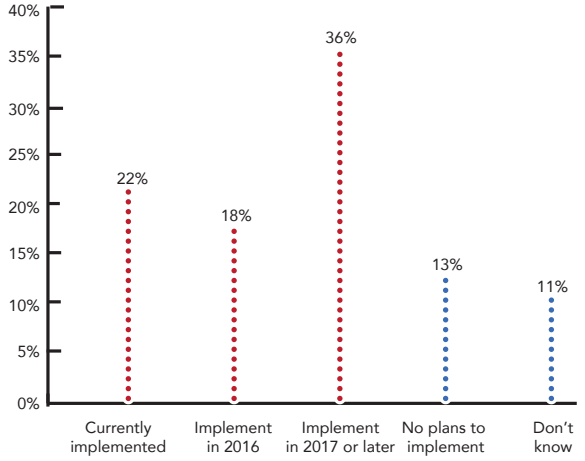
Adding behavioral biometrics to traditional password protection would increase security without degrading the user experience.



The majority of companies plan to implement behavioral biometrics.

Over half of companies (54 percent) plan to implement behavioral biometrics in 2016 or later. Two in ten (22 percent) companies have already implemented behavioral biometrics as an additional method to authenticate web and mobile users.

What are your company's plans for implementing behavioral biometrics as an additional method for authentication?



KEY FINDING: Majority of companies will be using two-factor authentication within the next 12 months

Two-factor authentication (2FA) is an additional layer of protection beyond passwords. 2FA commonly works by asking for something users know (their password) in combination with something they have (their mobile phone) to confirm their identity. When an event—such as logging in with a new device or from a new location—triggers an additional verification, a code is sent via SMS or voice to the phone number that was used to open the account. Users are verified when they enter the code on the website or in the mobile app. With 2FA enabled, a fraudster would need the user's mobile phone in hand, as well as their username and password, to hack into the account.

In their 2016 Data Breach Investigations Report, Verizon recommends that businesses protect their networks by offering or mandating two-factor authentication on top of standard password security.[1] Businesses are taking experts' recommendations seriously and implementing two-factor authentication. Currently, four in ten companies are using 2FA and in 12 months that will likely increase to eight in ten.

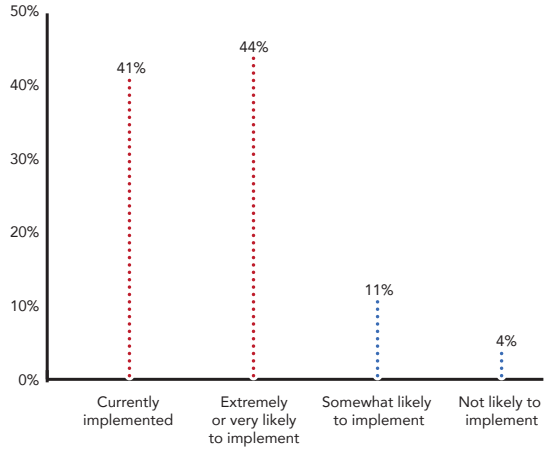
1 TeleSign Consumer Account Security Report, June 3, 2015

Most companies have implemented 2FA or plan to implement it in the next 12 months.

Four in ten (41 percent) organizations are using two-factor authentication for their consumer accounts and four in ten (44 percent) plan to adopt 2FA in the next 12 months.

- **The rate of implementation is higher for companies with 10 million or more users: 51 percent have 2FA in place vs. 38 percent of companies with fewer than 10 million users.**
- **46 percent of companies with fewer than 10 million users plan to adopt 2FA in the next year.**

What is the likelihood that your company will adopt two-factor authentication in the next 12 months?



The majority of companies with 2FA require users to participate.

Three-fourths (74 percent) of companies that have two-factor authentication for their consumer accounts require participation and 26 percent of companies make it voluntary for users to turn it on.

Among companies with voluntary 2FA, most have opt-in rates of 50 percent or more.

Two-thirds (66 percent) of companies with voluntary 2FA have opt-in rates of 50 percent or more.

What percentage of your users opt-in to voluntary two-factor authentication

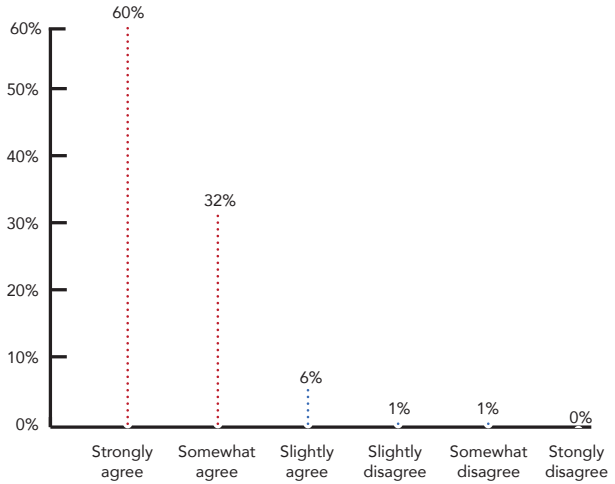
1 to 24%	3%
25% to 49%	31%
50% to 74%	36%
75% to 99%	19%
100%	11%
Total	100%

N=64 companies with voluntary 2FA

Nine in ten companies agree that 2FA combined with passwords increases account security significantly.

A total of 92 percent of respondents strongly or somewhat agreed that account security increases significantly with the addition of two-factor authentication to password protection.

Using two-factor authentication combined with password protection increases account security significantly



CONCLUSION

This research shows that passwords are no longer sufficient alone to protect and secure accounts. Stolen credentials and weak passwords have made companies vulnerable to online attacks, with nine in ten companies victimized by fraud in the past year. Cybercrime exacts a high cost on businesses in the form of financial losses, damage to brand and loss of customers. To protect their users and thwart fraudsters, businesses are using multiple layers of authentication including two-factor authentication and newer technologies such as behavioral biometrics. Companies are adopting behavioral biometrics to prevent fraudulent transactions, add a layer of security and prevent account takeovers.

ABOUT LAWLESS RESEARCH

Lawless Research designs online market research studies worldwide for clients across industries, including tech, banking, healthcare and consumer packaged goods. With 30 years of experience, Lawless Research provides valuable insights that help clients make strategic decisions about marketing, advertising, product development, and customer acquisition and retention. Thought leadership surveys, a specialty of Lawless Research, help companies identify emerging trends to use in PR and content marketing.
www.lawlessresearch.com

ABOUT TELESIGN

TeleSign is the leader in mobile identity solutions, helping customers secure more than 3.5 billion end user accounts worldwide and prevent registration fraud, while improving user experience and managing costs. TeleSign delivers account security and fraud prevention with two-factor authentication based on each user's mobile identity (phone number, device and behavior) and driven by real-time, global intelligence, including reputation scoring and device data. To find out more, visit www.telesign.com or follow us on Twitter – @TeleSign.

METHODOLOGY

TeleSign commissioned Lawless Research to design and conduct a study to determine how companies are authenticating web and mobile app user accounts. A total of 600 security, risk, and fraud professionals who are responsible for user authentication in companies with 100 or more employees completed the 10-minute online survey from April 18 through April 19, 2016. The respondents did not know who was sponsoring the research. The survey was hosted by Qualtrics and Survey Sampling International provided respondents from their online panel. Tests of significant difference were conducted at the .01 level (99% probability that the difference is real, not by chance).

Research Demographics

How many employees does your company have?

	N	%
100 to 499	152	25%
500 to 999	155	26%
1,000 to 4,999	163	27%
5,000 or more	130	22%
Total	600	100%

Can your company's users or customers create accounts on your website or through a mobile app?

	N	%
Website and mobile app	486	81%
Website only	103	17%
Mobile app only	11	2%
Total	600	100%

Does your company have online accounts for consumers or businesses?

	N	%
Both consumers and businesses	529	88%
Consumers only	71	12%
Total	600	100%

Which of the following do you have responsibility for in your job? (Select all that apply).

	N	%
Account security	384	64%
Identity management	340	57%
Payment security	340	57%
Risk management	338	56%
Fraud prevention	292	49%
User account registration	278	46%

N=600

What roles do you have in choosing technologies for user account security and identity? (Select all that apply.)

	N	%
Evaluate	441	74%
Recommend	428	71%
Select	314	52%

N=600

In what department or function do you work?

	N	%
IT Security	239	40%
Customer Relationship Mgt.	77	13%
Risk Management	75	13%
Engineering	47	8%
Product Management	46	8%
Internet Infrastructure	38	6%
Ecommerce	38	6%
Product Development	24	4%
Web Development	10	2%
Other	6	1%
Total	600	100%

About how many web and mobile account users do you have?

	N	%
Less than 1 million	113	19%
1 to 2.9 million	126	21%
3 to 4.9 million	111	19%
5 to 9.9 million	111	19%
10 to 19.9 million	68	11%
20 to 49.9 million	26	4%
50 million or more	27	4%
Don't know	18	3%
Total	600	100%

What is your organization's primary industry or sector?

	N	%
Computer Hardware or Software	108	18%
Banking, Finance, and Insurance	103	17%
Professional & Technical Services	103	17%
Business Services	97	16%
Retail or eCommerce	68	11%
Hospitality	33	6%
Social Networking	17	3%
Telecommunications and Internet Service Providers	17	3%
Online Gaming	15	3%
Instant Messaging/Chat	11	2%
Other	28	5%
Total	600	100%