2019 CONSUMER SURVEY: TRUST AND ACCOUNTABILITY IN THE ERA OF DATA MISUSE
INTRODUCTION

Data privacy and security are becoming central to the modern online experience. Globally, consumers are bombarded with headlines about rampant data misuse, while large-scale security breaches continue to be the new norm. To better understand how this turbulent environment is impacting consumer relationships with their service providers—and consumer security behavior in general—Ping Identity recently surveyed more than 4,000 people across the U.S., UK, Australia, France and Germany.

The results show that consumers are no longer confident in the ability of companies to protect their information online, and are ready to hold these organizations accountable for security lapses and other breaches of trust, such as data privacy violations. At the same time, however, consumers show a general lack of understanding of the risks to which they’re exposed, and a limited awareness about best practices for protecting their data online. These conflicting mindsets and actions are likely putting them at greater risk of diminished protection.

KEY FINDINGS

• **81% of people would stop engaging with a brand online following a data breach**, up slightly from 2018 (78%), including 25% who would stop interacting with the brand in any capacity.

• **63% of people say a company is always responsible for protecting user data**, even when users fall victim to phishing scams or use unencrypted Wi-Fi connections.

• **More than one half (55%) of people say a company sharing their personal data without permission is more likely than any other scenario to deter them from using that brand’s products**, even more than a data breach (27%).

• **Nearly one half (47%) of respondents have let others use their password for an entertainment or e-commerce service.** Additionally, nearly one quarter (24%) of that group say they are likely to reuse passwords from entertainment and e-commerce sites for a service that can unlock more personal information, such as email and banking.

• **65% of people are frustrated by login experiences**, which is no surprise considering the same percentage have been locked out of their accounts at least a few times a year. The frustration leads to action: One third (33%) of people have stopped using a device, app or service or have left a bad review following an inconvenient login experience.
**CONSUMERS ARE HOLDING COMPANIES RESPONSIBLE FOR DATA SECURITY**

**KEY TAKEAWAY**

Data security has become a major concern for consumers in recent years. Today, people are placing sole responsibility for data protection on companies and holding them more accountable. Increasingly, data breaches are driving people to change their relationships with affected companies, with a growing number of people disengaging completely in the wake of a breach. The findings below demonstrate the extent to which a data breach can deter potential customers from engaging with a brand, ultimately impacting the company’s bottom line.

**SUPPORTING DATA**

**GROWING SECURITY CONCERNS**

- 49% of people say they are more concerned about protecting their personal information today than they were one year ago, while another 49% are equally as worried as they were the previous year.

- The greatest percentage of anxiety is in the U.S., where 60% of people report being more concerned than they were one year ago, compared to less than 50% in other countries.

**THE STAKES ARE HIGH FOR HACKED COMPANIES**

- 63% of people say a company is always responsible for protecting user data, even when users fall victim to phishing emails or follow unsafe practices like using unencrypted Wi-Fi connections or reusing passwords. In many of these cases, companies will get the blame even though there is little or nothing they could have done to prevent it.

- Only 14% of respondents would readily sign up for and use an application/service following a breach.

- 81% would stop engaging with a brand online following a breach (up 3% from 2018), and 25% would stop all interaction whatsoever.

![What Would You Do to a Brand That Had a Data Breach?](chart)

- 56% would stop engaging with a brand online after a data breach
- 25% would stop engaging with a brand completely after a data breach
- 19% wouldn’t change my behavior toward a brand after a data breach
DATA SECURITY AND PRIVACY ISSUES INCREASE CONSUMER MISTRUST

SECURITY = PROTECT ME
Don’t let people steal my data.

PRIVACY = RESPECT ME
Don’t sell or share my data without my consent.

CONSUMER TRUST BY SECTOR

• Social media companies are the least trusted sector among five large sectors, with only 28% of people reporting they feel confident in these platforms’ ability to protect their personal information, which is not surprising given the privacy gaffes of recent years.

• Less than two thirds of people are confident in financial services’ ability to protect their data (63%), while healthcare (61%) fares slightly worse.

• Hospitality and retail rank in the middle of the aforementioned sectors, with 38% of consumers feeling confident in hospitality and 36% in retail.

GROWING TECHNOLOGY CONCERNS

• Of three key issues—online data security, online data exploitation and online account access—the majority (57%) of respondents report being most concerned with the security of their online data, followed by one quarter (25%) who are most concerned with companies exploiting their data for marketing and advertising purposes. This compares to only 12% who are most concerned with not being able to access online accounts quickly and easily, and 5% who are not concerned with any of these three issues.

• People expect privacy issues to get worse: 39% ranked data privacy as their number one technology concern for the next year, above security, surveillance, disinformation online or automation.

• People get more upset about companies abusing data than getting hacked: 54% say a company sharing data without their permission is most likely to damage their perception of that organization, compared with a hack (29%).

Interesting, Germany trends higher on concerns about surveillance than other countries, while the U.S. trends higher on data privacy. In fact, respondents from countries in the E.U. (the UK, Germany and France) were less concerned than those in the U.S. and Australia about data privacy, which likely shows the impact of GDPR.

KEY TAKEAWAY
Trust in companies’ ability to protect personal data and privacy is on the decline. Social media companies are the least trusted, but even financial services and healthcare firms—guardians of the most hallowed data—have their security cynics. The fact that banks aren’t more trusted is somewhat surprising given their reputation as being on the forefront of security protection. For healthcare companies, ransomware attacks impacting hospitals may be dragging consumer confidence down.
PRIVACY TRUMPS CONVENIENCE (AND EVEN SECURITY)

KEY TAKEAWAY

Consumers gravitate toward the data security techniques and practices they see as being more secure, rather than choosing the most convenient option. But privacy is the larger priority, with consumers forgoing options they see as more secure when those options are also seen as posing privacy concerns. Even so, consumers continue to be frustrated with login experiences and being locked out of their online accounts, and are taking action when confronted with an inconvenient login experience.

SUPPORTING DATA

SECURITY, PRIVACY AND CONVENIENCE: RANKED

- Amid growing security concerns, people are choosing security over convenience, yet prioritize privacy above all.

- Multi-factor authentication was ranked as the most secure login method by respondents, and is also among the most widely used.

- Maintaining a unique and strong password for each account was ranked as the third-most secure option, and it tied with multi-factor authentication as the most used method. Yet, inconvenience was cited as a common inhibitor: 38% of those who don't maintain strong and unique passwords said it was inconvenient, and 30% of those who don't use multi-factor authentication said it was inconvenient.

- Privacy issues outrank security for consumers when choosing a login method. Biometrics, for example, was ranked as the second-most secure login method and the second-most convenient. However, 49% report having privacy concerns with facial recognition, a common form of the technology, and biometrics is only used by 31% of respondents.

  > Of the people who have privacy concerns regarding facial recognition, the top worries are that the app will share their information with others and that the government will use it for surveillance.

LOGIN PAIN POINTS

- While consumers have deprioritized convenience, most (65%) are still frustrated by login experiences.

- 65% of people report having to change their passwords after being locked out of their accounts at least a few times a year or more, with 22% experiencing this more than once per month.

- One third (33%) of people have stopped using a device, app or service or have left a bad review following an inconvenient login experience.

How often do you have to change your password after being locked out of your account (e.g. because you forgot your password)?

- 8% Once a week or more often
- 14% A few times a month
- 15% Once a month
- 29% A few times a year
- 24% Once a year or less often
- 11% Never
CONSUMERS STILL FOLLOW RISKY SECURITY PRACTICES

KEY TAKEAWAY

Despite strong security and privacy concerns, consumers continue to make risky choices regarding their security. Younger generations in general take more risks with their security. Since companies are often blamed for fraud and privacy breaches, even if they result from potentially unsafe consumer choices, companies have to go the extra mile to protect their customer data.

SUPPORTING DATA

TOP SECURITY MISTAKES

• 43% do not maintain a strong and unique password for each account.

• Nearly one half (47%) have let others use their password for an entertainment or e-commerce service, and 18% do this often. Almost one quarter (24%) of those who have shared a password are likely to use that same password to log into a service that can unlock more personal information, like a bank or email account.

• One quarter (26%) of people do not change their password for an online service immediately after that service provider has been hacked.

BAD HABITS VARY BY AGE

Boomers are least likely to share their passwords (only 20%), while 71% of GenZ and 58% of Millennials do this.

Of those who reuse passwords, the worst offenders are GenZ (34%) and Millennials (31%).

THE DISCONNECT: CONSUMER THOUGHTS AND ACTIONS DON’T ALWAYS ALIGN

• People underestimate how difficult it is to maintain a strong and unique password for each account (or overestimate how good they are at it).

  > 46% of people rank this as the most or second-most convenient option, over biometrics, a password manager and single sign-on options, which in practice are easier to use and manage.

  > This is in spite of the fact that 65% report having to change their passwords after being locked out of their accounts at least a few times per year, which means they may be overconfident in their ability to remember unique passwords for each account.
WHY THE LACK OF SECURITY AWARENESS?

KEY TAKEAWAY
Misunderstandings and lack of awareness mean that consumers continue to engage in risky security practices despite being very concerned about security. People are not aware of many secure login options, or don’t know how to use them.

SECURITY BLINDSPOTS

• Multi-factor authentication is ranked as the most secure or second-most secure login option by 56% of respondents. Yet, 43% are not currently using it. Of those who don’t use it, 16% have no idea how to use it, 19% don’t think it’s available to them and 11% have never heard of it.

• Only 25% of respondents currently use a password manager. Of those who don’t, 22% don’t know how to use this login method, while 17% have never heard of it.

• Hardware tokens are the most under-used and misunderstood. Only 14% report using this option, and of those who don’t, 20% have never heard of a hardware token and 24% don’t know how to use it.

People place more confidence in passwords than they do in other security measures that are actually less likely to be defeated and compromised. For example, respondents ranked maintaining a unique and strong password for each account higher on security than using a hardware token or password manager. In reality, risky password practices are at the root of why breaches can cause so much damage. Not only are consumer practices lax, but passwords are easy to crack using automated tools. Password reuse enables criminals to easily break into other websites and user accounts.
CONCLUSION

Consumers everywhere increasingly are holding companies to higher standards when it comes to data privacy and security. At the same time, consumer confidence in the ability of companies to protect their data and privacy is low, and their own personal security practices and behavior are far from perfect. For companies that embrace the new realities of today’s post-breach digital landscape, there has never been a greater opportunity to win customer trust and loyalty—and it starts with creating the right balance of privacy, security and convenience.

To learn more about how identity and access management can help you protect customer data without sacrificing convenience, visit pingidentity.com.

METHODOLOGY

Ping Identity commissioned Market Cube to conduct a survey of 4,017 consumers in the United States, the United Kingdom, Australia, France and Germany who are at least 18 years old and use at least one of the following online sites or services: online shopping, online banking, movie/TV services, music services, government services, travel sites or transportation services. Additionally, respondents must have entered at least one of the following on a website or app in the past 12 months: address, date of birth, phone number, credit card number, bank information, social security number or driver’s license number. The geography breakdown of respondents is as follows: United States: 1,004, United Kingdom: 753, Australia: 755, France: 751, Germany: 754. The survey was conducted online between July 31 and August 6, 2019. The margin of error is plus or minus 1.6 percentage points.