CONSUMER SURVEY: PASSWORD HABITS

A study of password habits among American consumers

September 2012

csid.com

CSID®

A part of **Experian**

SUMMARY

The inherent problem with data security is human fallibility. Even with the most advanced security systems in place, if there is a human component to that system, there will be vulnerabilities. People create weak passwords, reuse these passwords across multiple sites, share information on social networks and inadvertently click on phishing links that download malware or viruses.

Furthermore, an email address or password compromised from one company's data breach can open up vulnerabilities across a multitude of completely unrelated websites such as banking, financial, online retailers and the like. To hackers, a simple credential like a password is like the missing piece to a puzzle. With that one piece, they can uncover other credentials and accounts, and in some cases, gather enough information to create an identity profile of the victim.

CSID, a part of Experian, enlisted help from research firm Research Now to conduct a survey about the password habits of a typical American consumer.

CSID found that consumers are careless about password creation, management and safety, even in a world where security breaches and identity fraud make headlines daily. They believe they are safe — an alarming disconnect that can leave many businesses open to data or security breach.

More than half of respondents (61%) admitted to reusing the same password for multiple sites, a practice that leaves consumers and businesses vulnerable. When a consumer reuses a password and login combination across multiple sites and one site is hacked, it opens the other sites to risk as well.

While nearly three-quarters (73%) of consumers claim to be concerned with strength and security when creating passwords, they often overlook the security consequences that can result from reusing passwords across multiple sites.

61% of people reuse the same password on multiple websites.

Interestingly, at 76%, 18 to 24-year-old consumers admit to reusing passwords more than any other age group. This may stem from the fact that this age group is also more concerned with easily remembering passwords than any other — when creating passwords, 76% of 18 to 24-year-olds consider making them not only secure, but easy to remember.

Despite these risky password habits, 89% of consumers say they feel secure with their current habits, indicating that consumers may not be aware of the associated risks and repercussions. In fact, one in ten consumers has had an online account compromised.

This report outlines the survey results, providing a glimpse into American consumer password and security habits, and presents recommendations for consumers and businesses to mitigate the risk of poor password habits.

KEY FINDINGS

54% of consumers have only five passwords or less.

44% of consumers change their password only once a year or less.

89% of consumers feel secure with their current password management and use habits.

21% of consumers have had an online account compromised.

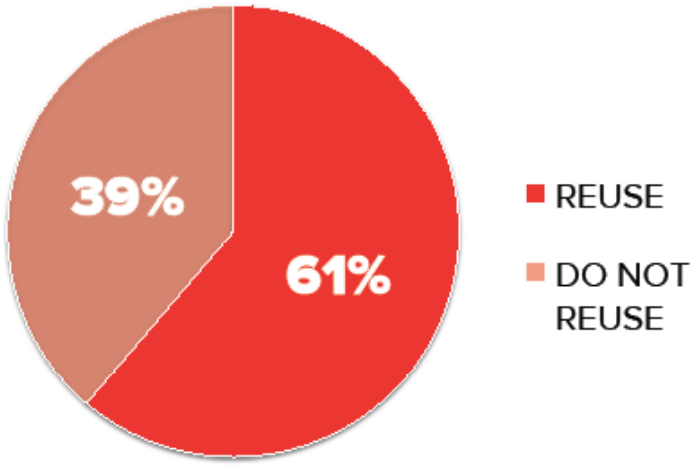
GRAPHS & CHARTS

PASSWORD HABITS

THREE FIFTHS OF INTERNET USERS REUSE PASSWORDS ON MULTIPLE WEBSITES.

61% of respondents admitted to reusing the same passwords among multiple sites.

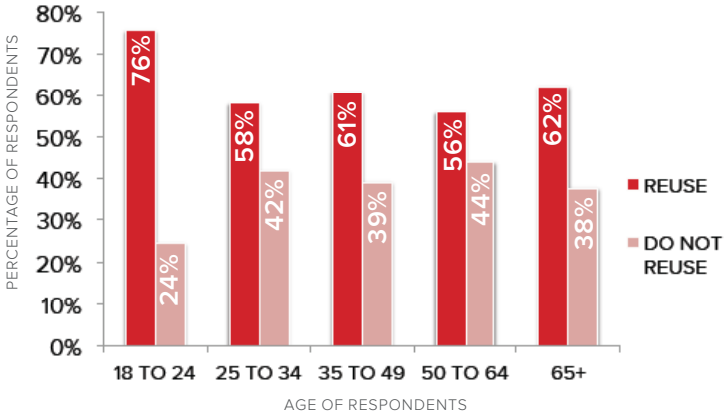
PERCENTAGE OF RESPONDENTS WHO REUSE VS. DO NOT REUSE PASSWORDS ACROSS SITES



18 TO 24-YEAR-OLDS ARE MORE LIKELY TO REUSE PASSWORDS THAN ANY OTHER AGE GROUP.

This graph shows that 76% of respondents in the 18 to 24-year-old age group reuse passwords among multiple sites — the highest percentage of any age group.

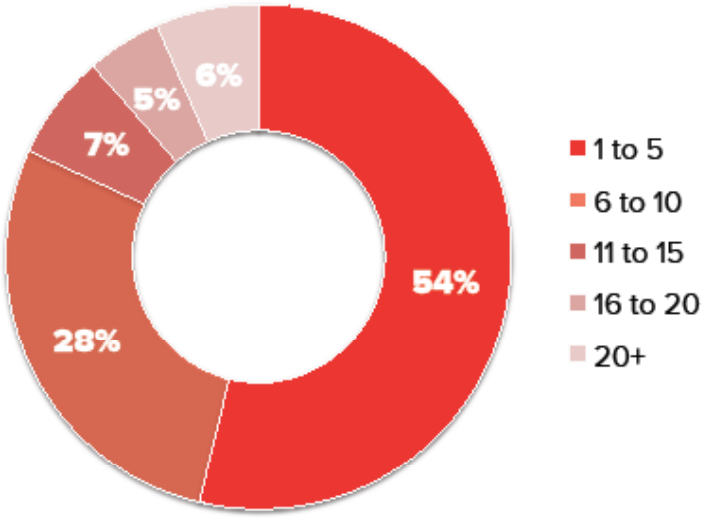
PERCENTAGE OF RESPONDENTS WHO REUSE PASSWORDS - BY AGE



MORE THAN HALF (54%) OF INTERNET USERS HAVE FIVE PASSWORDS OR LESS.

54% of respondents reported having only one to five passwords, while 28% reported having six to 10 passwords. Only 18% have more than 10.

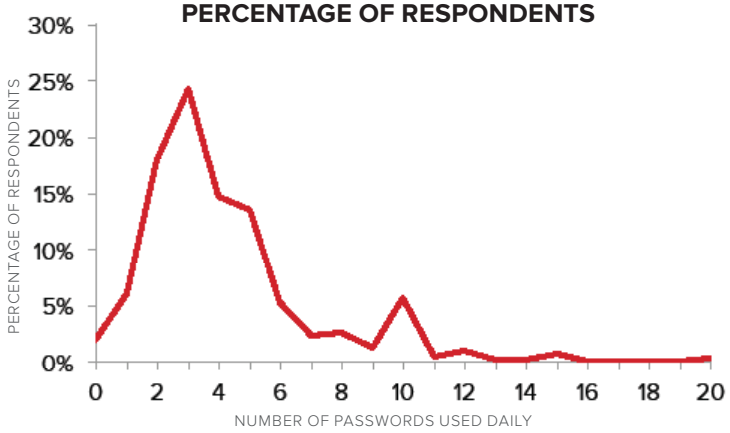
NUMBER OF PASSWORDS RESPONDENTS HAVE VS. PERCENTAGE OF RESPONDENTS



ON AVERAGE, PEOPLE USE 4 OR 5 PASSWORDS PER DAY.

77% of respondents type only one to five passwords daily, with 24% of that at three per day.

NUMBER OF PASSWORDS USED DAILY VS. PERCENTAGE OF RESPONDENTS



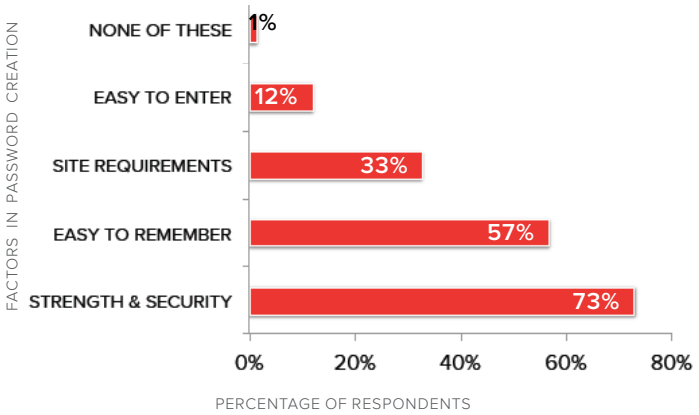
PASSWORD CREATION

STRENGTH IS THE TOP CONCERN IN PASSWORD CREATION.

Nearly three fourths (73%) of respondents consider strength and security when creating passwords, making this a top concern— more frequent than ease of memorization (57%), site requirements (33%) and ease of entering (12%).

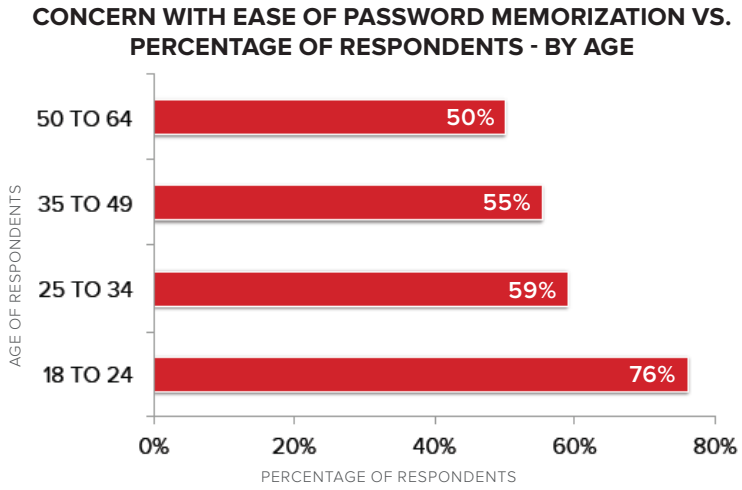
Note: Respondents were able to choose multiple answers to this question.

FACTORS IN PASSWORD CREATION VS. PERCENTAGE OF RESPONDENTS



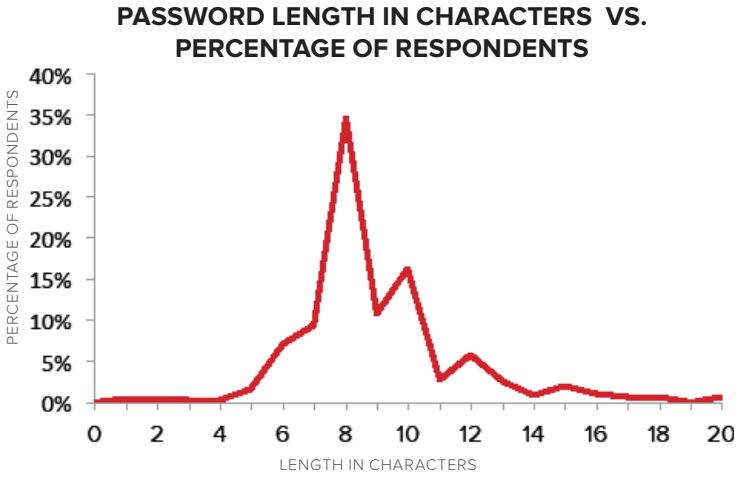
18 TO 24-YEAR-OLDS ARE MORE CONCERNED WITH CREATING PASSWORDS THAT ARE EASY TO REMEMBER THAN ANY OTHER AGE GROUP.

This graph shows the age of respondents vs. percentage of respondents who are concerned with having passwords that are easy to remember. Three quarters (76%) of 18 to 24-year-olds strive to create passwords that are easy to remember—a higher percentage than any other age group.



THE AVERAGE PASSWORD IS BETWEEN 8 AND 10 CHARACTERS IN LENGTH.

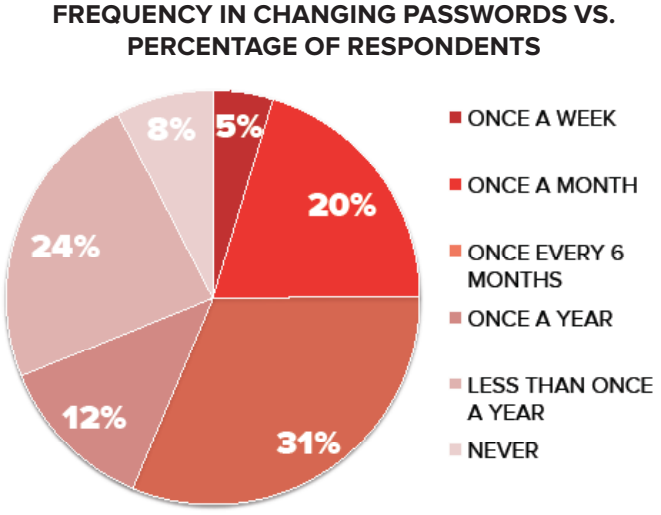
Most respondents (62%) create and use passwords that are eight to 10 characters long, making the average password 9.57 characters in length.



PASSWORD MANAGEMENT & SECURITY

44% OF PEOPLE CHANGE THEIR PASSWORDS AT MOST ONCE A YEAR.

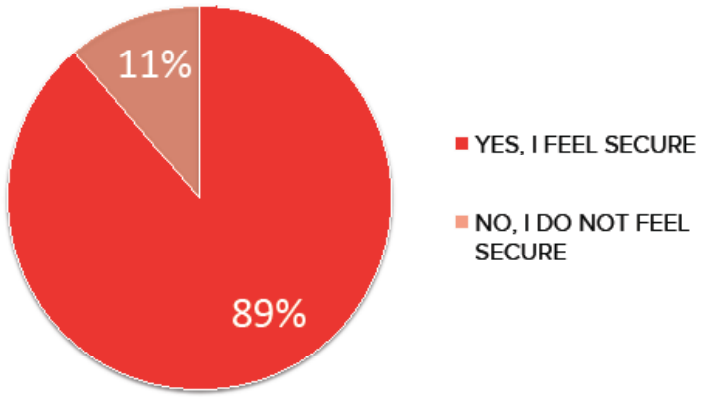
The graph to the right shows the percentage of respondents vs. frequency in changing passwords. 44% of consumers change their password only once a year or less, with only 12% at once a year, 24% at less than once a year, and 8% never changing their passwords.



NEARLY 90% OF PEOPLE FEEL SECURE WITH THEIR CURRENT PASSWORD HABITS.

89% of respondents claimed to feel secure with their current password creation and management habits.

PERCENTAGE OF RESPONDENTS WHO FEEL SECURE VS. DO NOT FEEL SECURE WITH CURRENT PASSWORD HABITS

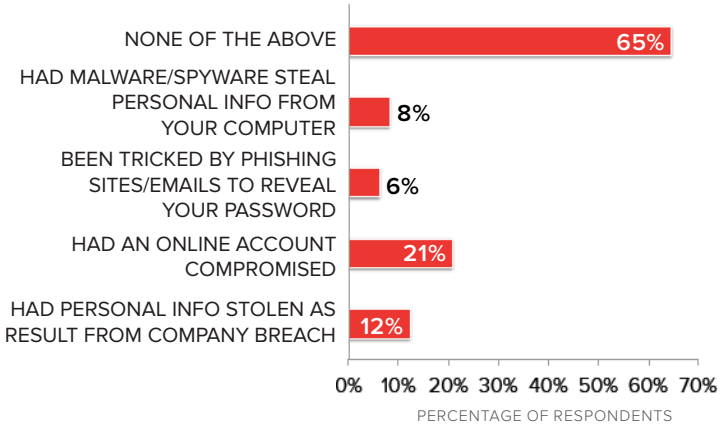


1 IN 5 PEOPLE HAS HAD AN ONLINE ACCOUNT COMPROMISED.

35% of respondents report having security issues with their computers and passwords: 1 in 5 (21%) had an online account compromised; 12% had personal information stolen as a result of a company breach; 8% had malware or spyware steal personal information from their computers; and 6% had been tricked by phishing sites or emails to reveal their passwords.

Note: Respondents were able to choose multiple answers to this question.

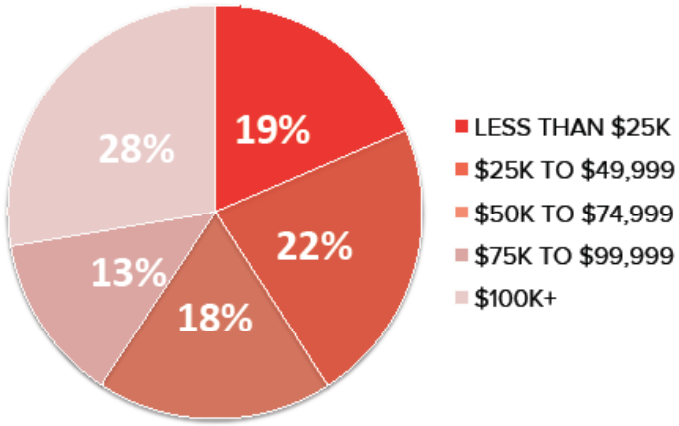
PERCENTAGE OF RESPONDENTS WHO HAVE FACED VARIOUS COMPUTER SECURITY PROBLEMS



THOSE WITH ANNUAL INCOMES OF $100K AND ABOVE ARE MORE LIKELY TO BE COMPROMISED THROUGH A COMPANY BREACH THAN OTHER INCOME BRACKETS.

This graph shows the percentage of respondents who have had passwords compromised as a result of company breach vs. annual income. Those with incomes of $100K and above make up more than a fourth (28%) of the respondents who have been affected by breach, the highest percentage of any income bracket.

LIKELIHOOD TO BE COMPROMISED THROUGH A COMPANY BREACH VS. INCOME



TAKEAWAYS

This survey revealed that there is a disconnect between intention and action when it comes to consumer password habits. Consumers largely feel secure with their password habits and consider security the most important factor of password creation, but are not practicing secure password techniques.

This perceived sense of security may be one reason why 61% of consumers feel comfortable reusing passwords across multiple sites—a behavior that in reality puts consumers and businesses at increased risk for compromise.

In fact, 18 to 24-year-olds make up the age group most likely to reuse passwords. Password reuse among 18 to 24-year-olds may be more common because they are more concerned with creating passwords that are easy to remember — and it is easier to reuse the same passwords across websites than it is to remember distinct passwords for each.

This survey also revealed that the average password is between eight and 10 characters in length. This may be attributed to the fact that websites often require a minimum password length of eight or 10 characters, and so the majority of consumers meet minimum password requirements but rarely more.

These results show that while consumers have secure intentions for their passwords, their actions typically do not follow suit, putting themselves and businesses at increased risk for compromise. To minimize this risk, we must diminish this disconnect between intention and action through the recommendations that follow.

The average consumer takes minimal action to secure online accounts.

RECOMMENDATIONS

BUSINESSES:
EDUCATE, MONITOR AND AUTHENTICATE

Human fallibility continues to be a major risk factor for businesses. People—including employees, customers and partners—that have risky password habits are making themselves and businesses vulnerable to breach and compromise. A business is only as strong as its weakest link, or weakest password connected to that business, whether belonging to a customer, partner or employee. To mitigate the effect of weak passwords, businesses should consider ongoing education, monitoring and authentication techniques, including:

- DO educate employees about the potential consequences for poor password habits, as well as proper password creation and management techniques.
- DO consider compulsory education for passwords and understand the risk-to-cost ratio for implementing these protocols.
- DO monitor employee credentials for compromise, and offer identity monitoring packages to employees and/or customers.
- DO research and implement two-factor authentication techniques for online accounts. Consider physiological and behavioral biometrics or location based authentication.
- DO have a plan in place in case of a company breach.

CONSUMERS:
ADOPT MORE SECURE PASSWORD HABITS

These survey results tell us that average consumer is concerned with password and online account security, but takes minimal proactive action to secure him or herself, such as using a variety of passwords that are long and strong. Adopt more secure password habits, such as:

- DO use long passwords with a mix of letters, numbers and symbols. They are hardest to crack. Create passwords that are 10 characters or longer that include uppercase letters, lowercase letters, symbols and numbers.
- DO use a unique password for each account and vary the email addresses you use for accounts.
- DO use a secure password management system to keep track of your login information for various sites.
- DO NOT store your account information in an unsecured document on your computer or network.
- DO NOT share your password — even with friends and family.

METHODOLOGY

CSID and consumer research firm Research Now teamed up to survey a demographically representative sample of 1,200 U.S. adults (age 18 and above) from the Research Now Consumer Panel. The sample framework is selected based on U.S. Census data for age, ethnicity, gender, region and income. The survey also collected demographic data for education level and marital status.

ABOUT CSID

CSID, a part of Experian, is a leading provider of global identity protection and fraud detection technologies for businesses, their employees, and consumers. With CSID's enterprise-level solutions, businesses can take a proactive approach to protecting the identities of their consumers all around the world. CSID's comprehensive identity protection services extend beyond credit monitoring to include a full suite of identity monitoring and fraud detection services; identity theft insurance provided under policies issued to CSID; full-service restoration services; and proactive data breach services.

WWW.CSID.COM

ABOUT RESEARCH NOW

Research Now, the leading digital data collection provider, powers market research insights. We enable companies to listen to and interact with the world's consumers and business professionals through online panels, as well as mobile, digital and social media technologies. Our team operates in 24 offices globally and is recognized as the market research industry's leader in client satisfaction. We foster a socially responsible culture by empowering our employees to give back.

WWW.RESEARCHNOW.COM