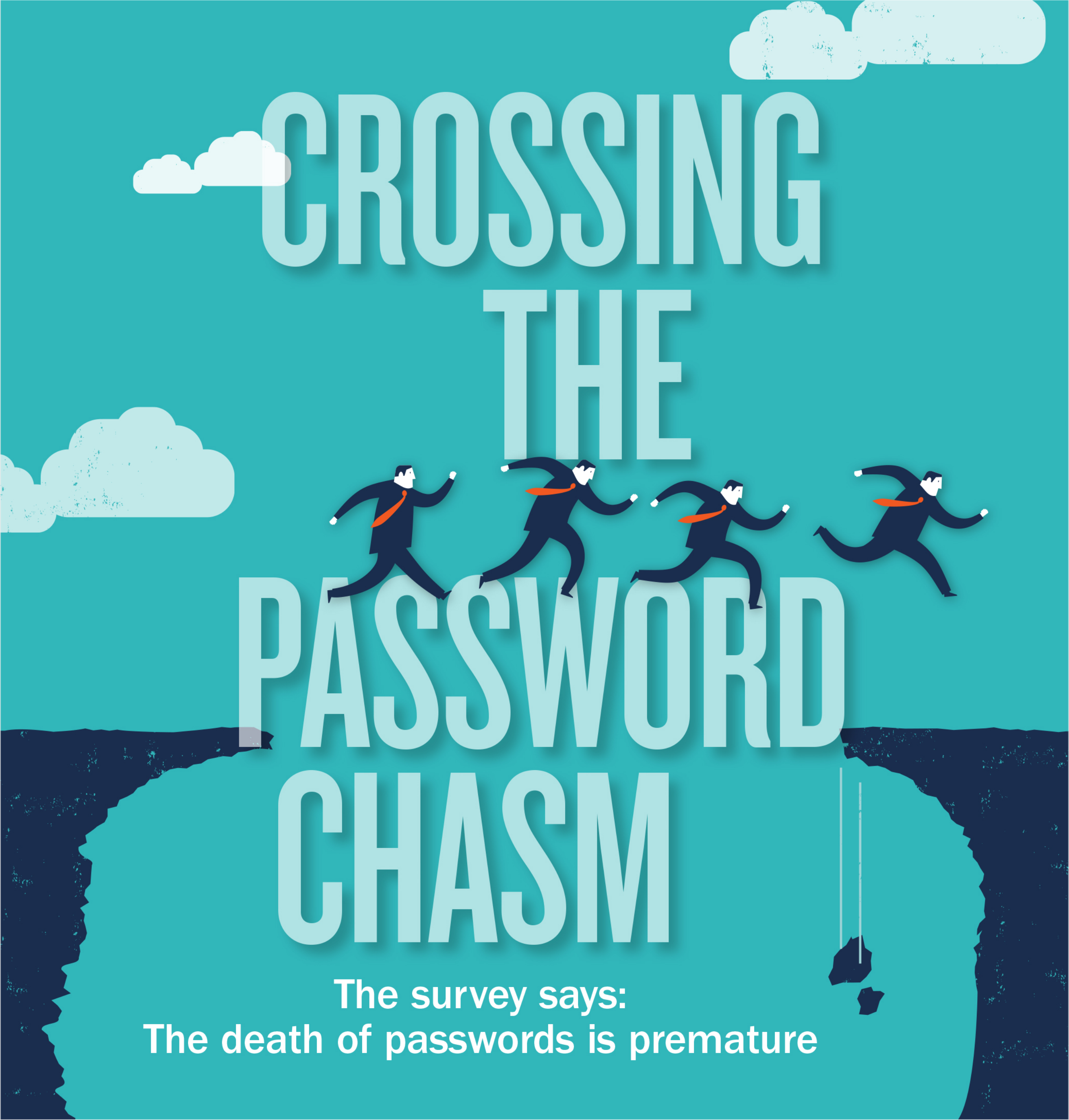
KEEPER®

7 pages of original research

MarketFocus

In-depth analysis from Keeper Security

January 2017



CROSSING THE PASSWORD CHASM

The survey says:
The death of passwords is premature

Confidence in password management is high

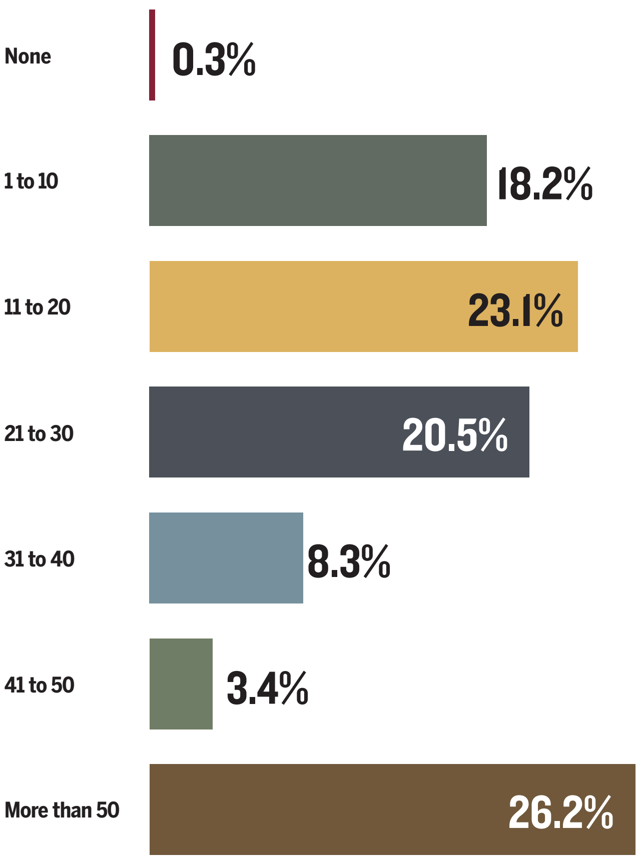
A survey of security pros shows confidence in password security and password managers remains high. Jesse Staniforth explains.

There is a popular belief that the traditional password as we've known it is dead. Passwords are too easy to crack, "they" say. It is too hard to keep track of passwords, "they" say. Biometrics and other new technologies will replace the password, "they" say. Whomever "they" are, apparently they are not among the growing group of users and IT professionals using password managers.

Those are the findings from a survey conducted by SC Media and the research firm of C.A. Walker Research Solutions in December 2016. The survey, commissioned by Keeper Security, shows there is good news about the future of the traditional password combined with the bad some pundits have been expressing for years.

The good news is that confidence in traditional password security remains high as more people than many experts anticipated are moving to the password manager model to create complex passwords and save them securely. The bad news should not surprise anyone; with users having more online accounts than ever before, those trying to memorize all their passwords end up using less complex passwords that are easier to crack and they are often reused for multiple accounts.

How many total online accounts do you have?



With 385 respondents, the survey weighed heavily toward representatives from companies with fewer than 1,000 employees (291) and revenues totalling less than $100-million (257). In fact, nearly half of respondents (163) worked for companies smaller than 100 employees.

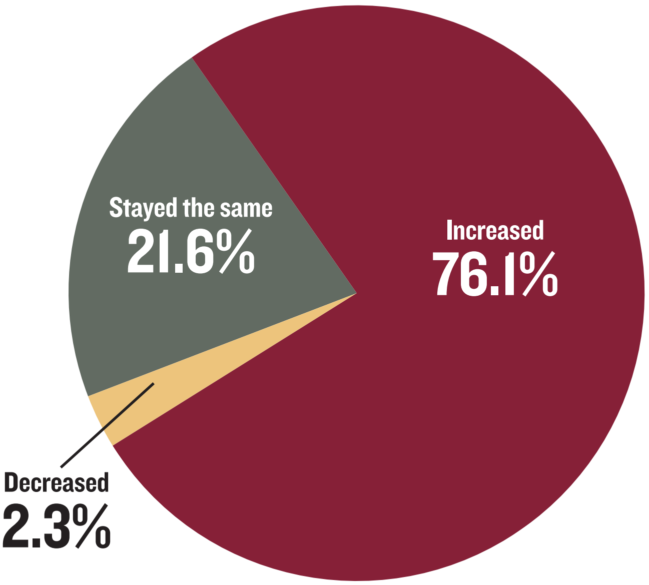
Those who took the survey reflected a high degree of speciality in technological fields: 26 percent worked in the Technological Services industry sector, 15.3 percent worked within finance, 9.1 percent worked in government (including military), and 7 percent worked in education.

Respondents' individual positions were notably specialized as well—11.9 percent were IT managers, 11.2 percent were systems/security administrators or analysts, 9.9 percent were consultants, and 9.6 percent were engineers/architects. While 7.5 percent were owners and 7.3 percent were CEOs/presidents, directors of security C-suites represented a sizeable portion of respondents—CSOs/CISOs, CIOs, and CTOs combined comprised 13.2 percent of the total response to the survey.

The good news

Whether this cross-section was more likely to contain early adopters, advanced users, and those with greater security maturity was a subject of some discussion, as analysts agreed this market split encouraged some of the survey's optimism. To begin with, there was a far higher level of confidence in password security than many expected. Responding to the question, "How confident are you that your passwords are protected from hackers?" 72.2 percent replied on the confident side, either "Very confident" (19 percent) or "Somewhat confident" (53.2 percent). By contrast, a total of only 25.2 percent identified themselves as not confident, either "Not very confident" (21 percent) or "Not at all confident" (4.2 percent).

Has the number of total online accounts you use increased, decreased or stayed the same over the past year?



"The statistics sound optimistic to me," says Adrian Lane, CTO of Phoenix-based Securosis. "Respondents may be measuring how confident they are in the way they keep their passwords safe.

Most people I talk with don't have trust in their passwords, but that's a proxy for not trusting companies with their passwords."

The sense of password insecurity is greatest, Lane notes, outside the realm of security. "People who are in security mostly use password managers," he quips, "so they might have answered that question with great confidence — your password is fine if it's on your own password manager."

Australian web-security expert and Have I Been Pwned blogger Troy Hunt adds, "I have a high degree of confidence that the passwords I create (that) I'm protecting well. I have them in a good password manager with a strong master password — that's about as strong as we're going to get within reasonable measures. However I have a very low degree of confidence that the vast majority of websites I give my passwords to are protecting them at all."

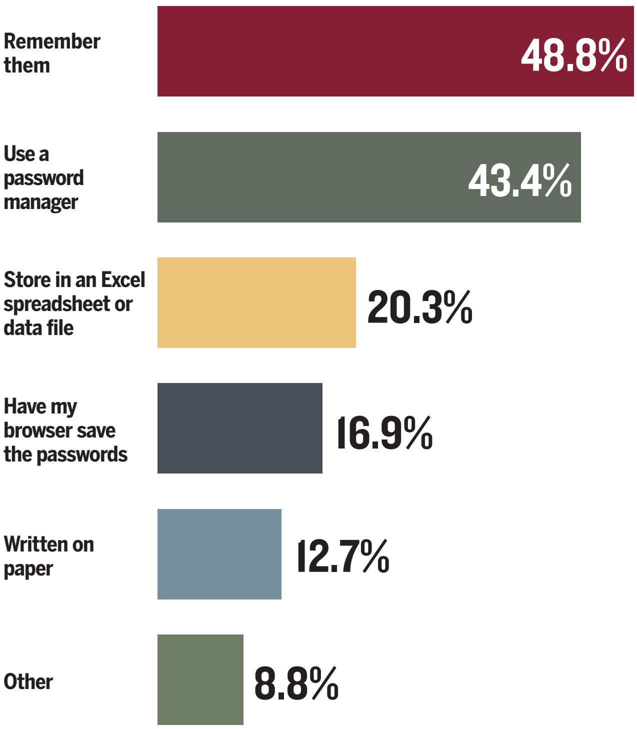
"Context is king," says Per Thorsheim, an independent security adviser in Bergen, Norway. "I feel very confident that my passwords are secure in the context of systems I own myself, operated at home, disconnected from the Internet. I also feel that my passwords are secure in the context of my personal accounts, since I'm using two-factor authentication wherever I can."

All agreed that outside the circumstances a person can control themselves, however, the landscape of password safety came nowhere near meriting the high level of confidence reflected in the survey.

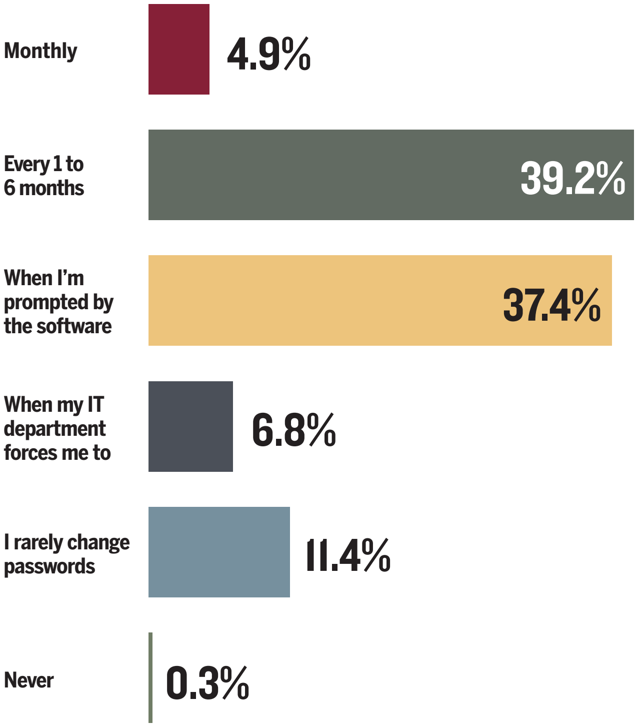
The bad news

Responding to the 19 percent who were "Very confident" that their passwords were protected from hackers, Hunt laughs sardonically. "Well, they're all wrong! It's not up for debate!" he says. "On the whole, our password exposure is ridiculously bad, even before we get into the discussion about how easy it is just to guess a bunch of them."

How do you store and/or remember the passwords you use?



How often do you change your passwords?



Larry Ponemon, chairman and founder of the Ponemon Institute in Traverse City, Mich., sees a potential danger behind the confidence. Excessive optimism about password security is widespread in the general public, he underscores.

"People feel that if they have a strong password, maybe special characters, a combination of alphanumeric, that somehow they're protected, and that's all they need to safely access their accounts and files," he says.

Recalling a study from several years ago, Ponemon remembered polling individuals who had been victims of identity theft or had had other negative experiences resulting from data insecurity about how those events changed their relationships with safety and privacy.

"Even a bad event, we noticed, basically didn't get people from the confident rates to the not-so-confident rates," he says. "People felt it was a random act that wasn't going to happen to them again. They even still felt safe with a sloppy password."

> I'm surprised only 50 percent of people are memorizing their passwords"
>
> – Darren Guccione, CEO, Keeper Security

That point could go a long way toward explaining why 48.8 percent of respondents reported memorizing their passwords, which was the core of the bad news in the survey. Remembering passwords led the pack of password-retention methods in spite of a plurality of 26.2 percent reporting having to juggle more than 50 accounts, and 75 percent overall saying their number of accounts has gone up in the past year alone.

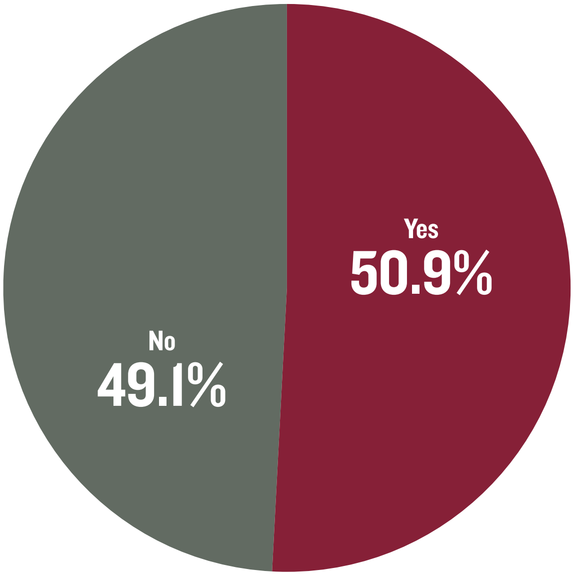
"I'm surprised only 50 percent of people are memorizing their passwords," says Keeper Security CEO Darren Guccione. "This sample has a high rate of response from fluent technology users, so that seems fair. In enterprises, it's different. But in the general public that percentage sounds low. Who knows?

Because I'm constantly doing trade shows, I meet a lot of people. I ask them all, ‘How do you remember your passwords?’ The number of people who memorize passwords could be as high as 90 percent. Maybe one in twenty, at best, tells me they use a password manager.”

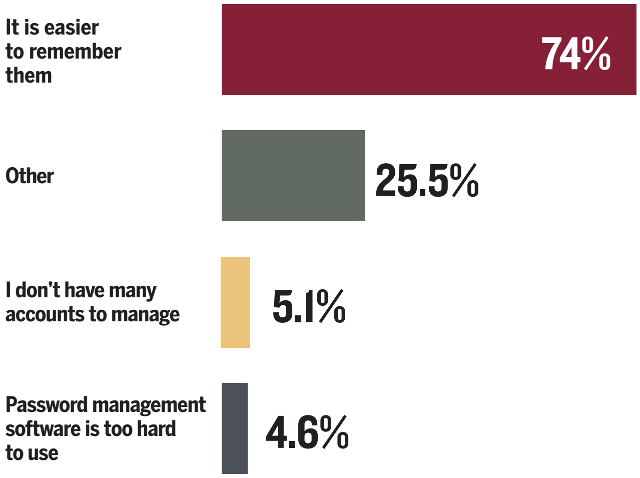
Of course, the factor that makes it possible for such a high number of respondents — with such a huge (and growing) number of accounts — to rely on password memorization, is what Hunt calls “the dirty little secret we all know:” Most people are reusing passwords, and reusing them widely.

“Look at the drivers for this. We're continually forced into creating new credentials,” Hunt says. “We've got the massive sprawl of websites that seem to be required for our everyday trivial tasks. Most people are going to use ‘their password’ to do that — ‘their password’ being that singular instance that they use everywhere.”

Do you reuse passwords?



Why do you reuse passwords?



The challenge

Results from a new study by Keeper of the past year's most common passwords show that the 2016's most popular choices were again the sequential-key classics “123456” and “qwerty” (and several longer variations upon each). Those are easy to remember and easier to crack. As the account landscape continues to sprawl across the internet, it's getting easier for the bad guys to compromise not only users of weak passwords, but also stronger passwords that are reused for multiple accounts.

Hunt gives the example of having recently purchased airport parking in advance and having to create an account with a password in order to do so. Because he uses a password manager, he easily created and stored a randomly generated password. But imagining the number of others who simply enter their email address and the password they use everywhere, he saw the seeds of disaster sown in a local parking website.

“Your local parking site was built by someone's brother's cousin's uncle's dog,” Hunt says. “It does absolutely no cryptographic storage and has injection flaws—and tomorrow that gets leaked. Now, because you needed to park your car, someone's in your Gmail.”

Even Securosis' Lane admits that before he had a password manager, he used the same password across dozens, if not hundreds, of sites. Though the advent of increased cascade failures encouraged a move to password managers for some users, Lane does not consider it shocking that nearly half of respondents in a survey so heavily weighted toward security professionals admitted password reuse.

“Even people in technical professions don't understand password managers, he says. “It's taken me years to get family members who hear me talk about security every day to adopt a password manager or something like that.”

The intervention of the online world in the everyday once again came to mind for Hunt, who says the more we're bombarded with the need to create accounts and secure them with passwords, the harder it becomes to keep passwords secure overall.

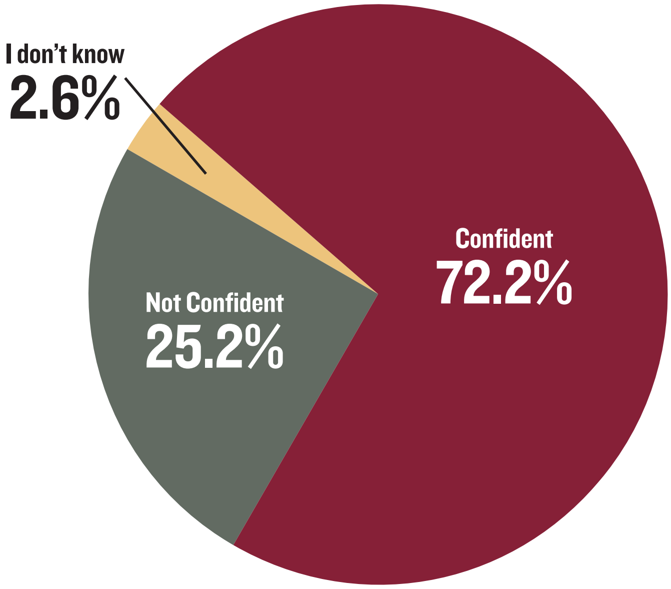
“Very often people talk about how to create a good password — use a passphrase, or random this, or random that,” Hunt says. “That's fine, but it's one-dimensional thinking. The problem is when we apply that to the other dimension, which is doing it uniquely across every single account, completely different for every account. How many accounts do you have? You have a lot. Unless you're Rain Man, you're not going to be able to remember all these unique streams you've used for every independent website.”

If respondents who commit passwords to memory aren't simply reusing one password but rather using simple variations on it, such as half of one password plus date of birth, those too can be easily broken by a hacker or rootkit, Ponemon notes.

But even a best-case-scenario read of the numbers on memorization, Ponemon cautioned, pointed in the direction of bad news. He hypothesized a stoic character that comes up with 50 strong passwords for 50 sites and commits them all to memory.

“What happens,” he posits, “when they get older and have memory problems?”

How confident are you that your passwords are protected from hackers?



> “Unless you're Rain Man, you're not going to be able to remember all these unique streams...”
>
> – Troy Hunt, web security expert

The most positive news of the study, and potentially the most controversial, was the 43.4 percent of respondents who say they use a password manager to keep track of their passwords (respondents could answer with more than one method of password retention). This suggests that those relying on their memory for password retention are only doing so with a handful of frequently used sites. However, the number was greeted with some suspicion.

“I cannot imagine 43.4 percent using a password manager, unless it includes passwords on paper, documents, spreadsheets and more,” says Thorsheim flatly.

Hunt concurs, adding, “I would love for that figure to be true, but it's just not true. Maybe we've got a really skewed sample group. But even when I speak at security conferences and run workshops and ask for a show of hands for people who have password managers, it's really rare to see above 50 percent — and these aren't just people who work in government and have an investment in security, they're people who really understand all the concepts we're talking about. Yet they just aren't acting on them.”

Others, however, suggest that the specific background of the survey respondents explain higher reports of password-manager use than expected.

“Given the targeted respondents, it's not surprising that it's more than 40 percent,” says Ponemon. “If the respondents have a background in technology, they probably have lots of passwords to manage, so they're more likely to use a password manager. If you asked that same question for the average person on the street, whether or not they had a background in IT, I think that number would be lower."

Context is key

For Lane, a deciding factor was enterprise size — the larger the enterprise, the more likely that password managers will be standard.

"It solves a lot of problems for enterprises. Ten years ago, if you asked IT what their biggest problem was," Lane recalls, "it would be password resets. It was a huge issue. Being able to have a password manager on the desktop, people never forget their passwords and it solves a lot of other problems about password strength by proxy and the ability to rotate passwords and not having users complain all the time."

Keeper's Guccione says that regardless of whether the study leaned toward technological speciality, it nonetheless shows that the popularity of password managers is growing, even if the market remains very young.

"The market for this is absolutely enormous," Guccione says, "but people are only finally becoming aware that there's a better way — there's software out there that's easy to use and very secure, which not only requires that you not remember passwords, but creates high-strength passwords for you, and authenticates you into all of your sites with ease."

While there is a chasm between technology specialists and the general public in terms of technology adoption, Guccione says, the positive news is that the general public seems to be crossing it in ever-greater numbers.

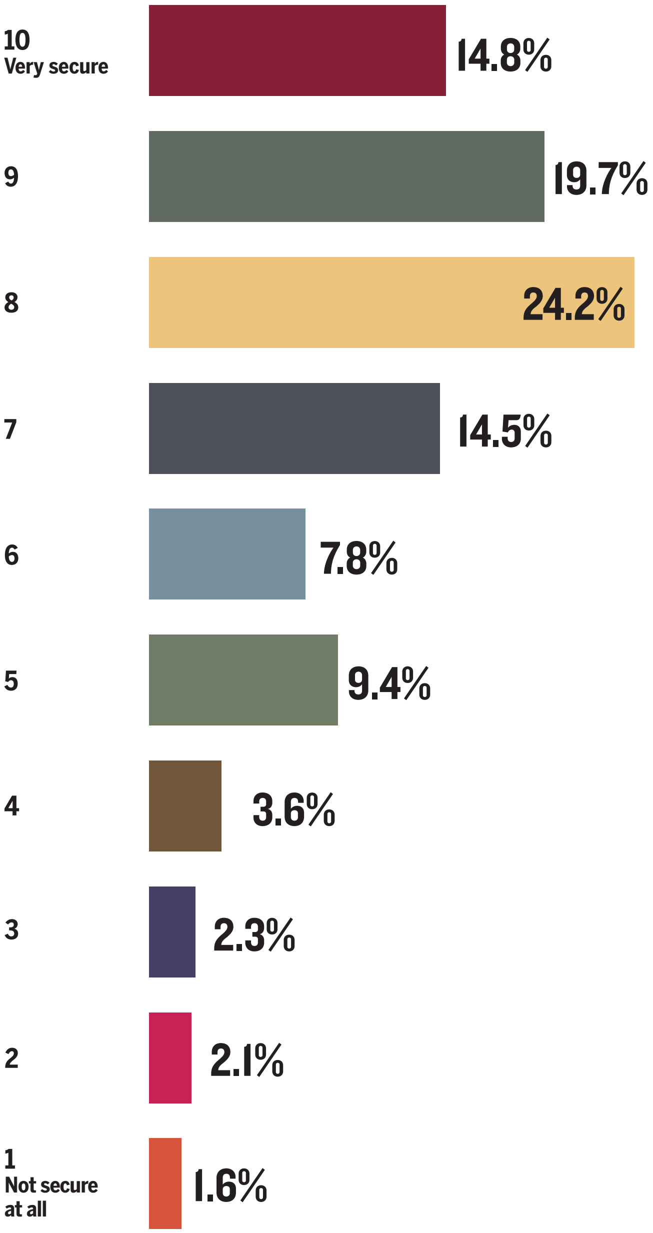
Another contentious issue was a question about the perception of the security of biometric logins (measured as a number out of ten). While a plurality (24.2 percent) of respondents rated biometric logins as offering 8 out of 10 security, those rating biometric logins as 10 out of 10, 9 out of 10, and 8 out of 10 added up to 58.7 percent.

Among the analysts, this led to a variety of responses. Noting that biometrics refers to a wide variety of different technologies, Lane says that in an aggregate sense, he felt the positivity was merited, though he places the security level closer to 7 out of 10.

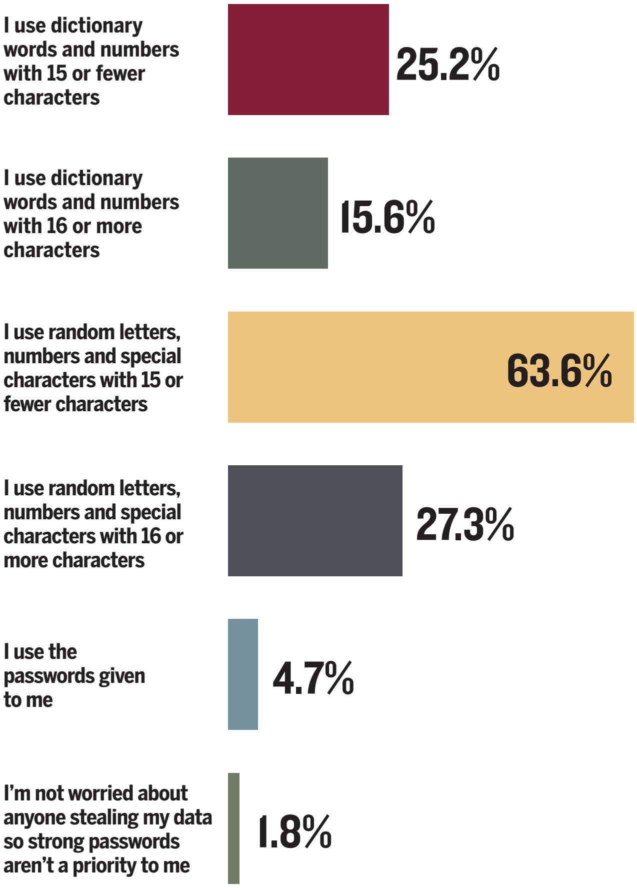
"All of those systems are hackable in some way," Lane explains, "but if you're just trying to keep your phone safe, a fingerprint is pretty good. If you're worried about nation-states, forget it, all bets are off. A lot of these technologies are in use and can do things well in most cases. But if they come under attack by really skilled individuals, they tend to fall over."

In the wake of the US election hacking debates and the knowledge that major breaches occurred through

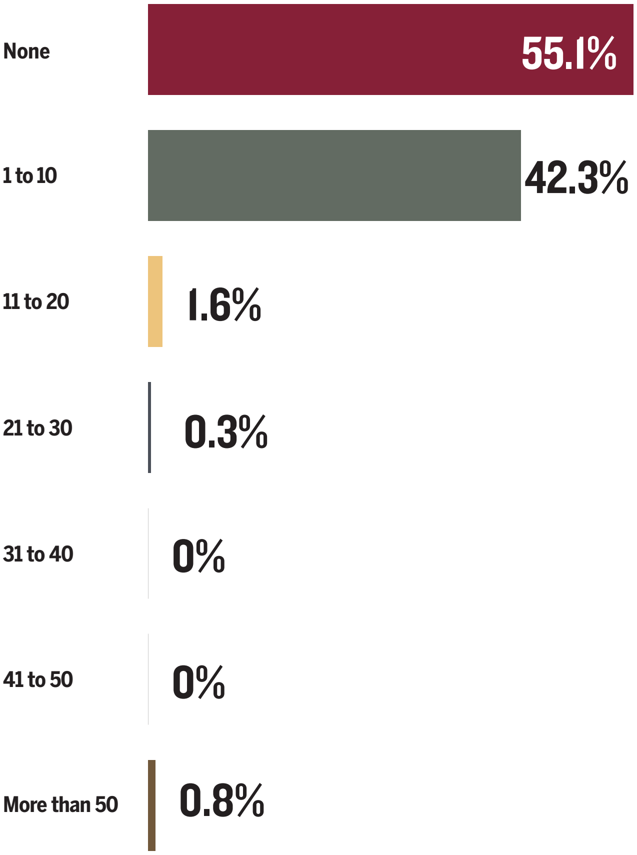
On a scale of 1 to 10, how secure do you perceive biometric login would be?



How do you select the passwords you use?



How many passwords have you shared with family, friends or colleagues?



phishing and social engineering, this was the final caution of the study. It is not biometric measures themselves, or strong passwords alone, that will do the protecting of data and it is not through those measures alone that we can work toward a more thorough understanding of security. The future of password security is in approaches and practices.

Yet even as we seek to outwit the bad guys' constant attempts at socially engineered hacks, the sharp end of the issue remains the passwords themselves. If products such as password managers propagate complex, entropy-proof passwords while driving down the temptation to reuse passwords, they may very well empower the state of password-entry landscape. Ultimately, the experts agree, the challenge is convincing users to employ appropriate security hygiene, even if it is a bit more inconvenient than simply remembering 123456.

Methodology

This survey was based on 385 responses from a broad, cross-section of company sizes and revenues and eight industry verticals, including federal and state and local government, technology services, finance, education, manufacturing, medical and health care, legal/real estate and retail and wholesale distribution. The survey was conducted in December 2016 by C.A. Walker Research Solutions, Glendale, Calif. The results of this survey might not equal exactly 100 percent due to the following reasons: rounding errors during the analysis phase of research; respondents who skip a question; and respondents who provide more than one answer to a question. This research has a confidence level of +/- 3.1 percent.

KEEPER®

Keeper Security is transforming the way organizations and individuals protect their passwords and sensitive digital assets to significantly reduce cybertheft and data breaches. Keeper is the leading provider of zero-knowledge security and encryption software covering password management, dark web monitoring, digital file storage and messaging. Named PC Magazine's Best Password Manager of 2018 and awarded the Publisher's Choice Cybersecurity Password Management InfoSec Award for 2019, Keeper is trusted by millions of people and thousands of businesses to protect their digital assets and help mitigate the risk of a data breach. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the Federal government through the System for Award Management (SAM). Keeper protects businesses of all sizes across every major industry sector.

Learn more at https://keepersecurity.com.

This supplement was commissioned by Keeper Security and produced by SC Media, a Haymarket Media, Inc. brand.