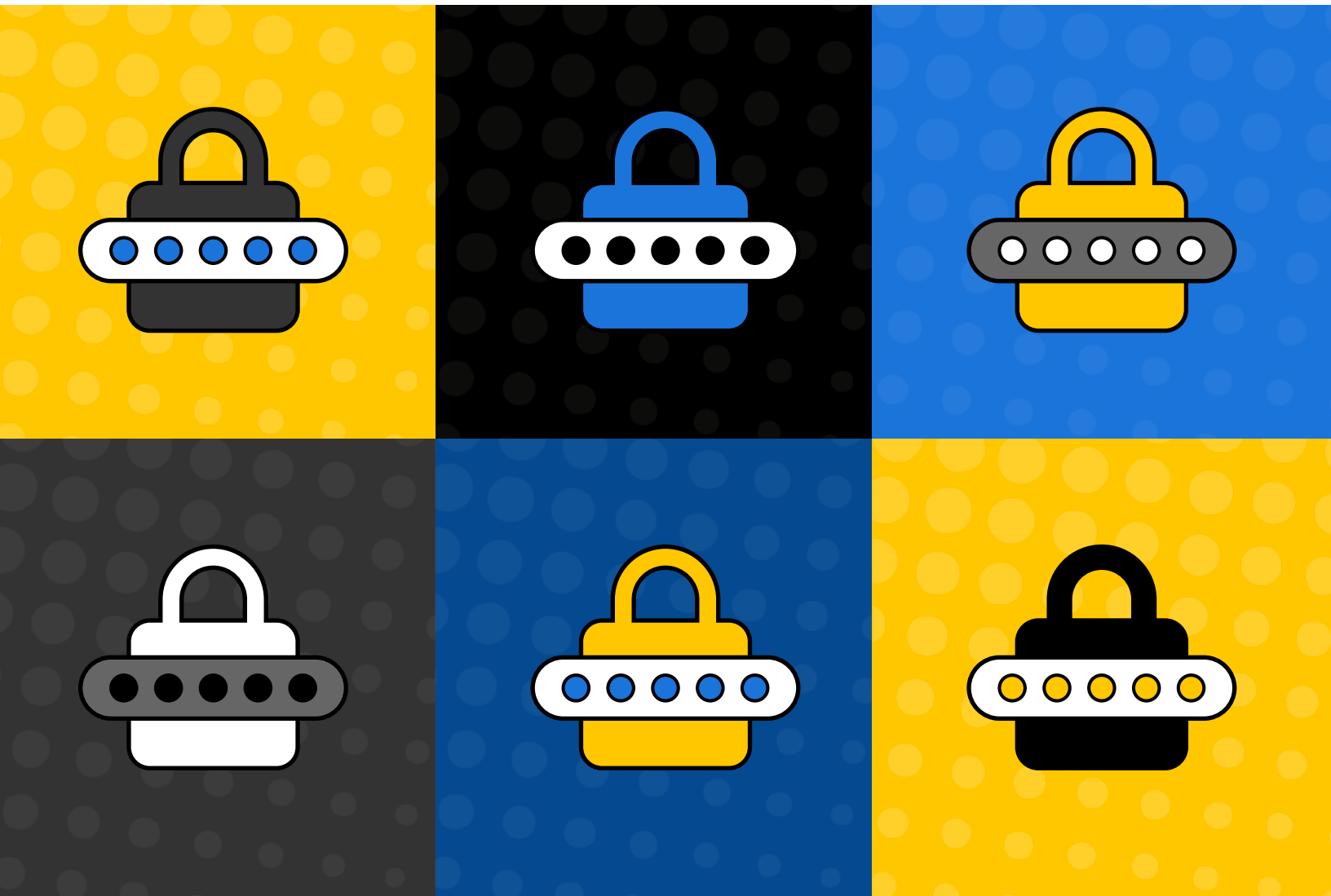
KEEPER
Cybersecurity Starts Here®

2022
US PASSWORD PRACTICES REPORT



FOREWORD

Online passwords are used for many critical aspects of our lives. They are needed when we communicate, work, transact and travel. We use them to access our most sensitive data, from banking to health records. Digital passwords are the keys to our lives.

Yet we are surprisingly negligent about password protection, from our choice of passwords to the means we use to remember them, and troublingly, our willingness to share sensitive passwords with others.

Keeper Security's survey of 4,000+ respondents in the US and UK unearthed negligent attitudes toward password protection, in which passwords are being shared with spouses, written down on bits of paper, changed too often, and forgotten over 50 times per year!

The result: nearly half of our 2,000 US survey respondents had been hacked at least once, with an average of $378 stolen per cyberattack.

The consequences of poor password protection can be disastrous in an era of growing online crime and identity theft. A hacked password can result in ransacked bank accounts, obliterated credit ratings, damaged personal lives and severed business relationships.

As we are more digitally dependent than ever, poor password protection only contributes to the growing threat of cyberattacks. In a 2020 survey, the average American had **access to 10+ connected devices** in their household, and **85% own a smartphone**. As a result, the chances of a critical personal data breach are very real, particularly when over **2,000 cyberattacks** are reported to the FBI every day, with countless more going unreported.

To raise awareness about the scale of the problem of weak passwords, **Keeper Security**, the leading provider of zero-trust and zero-knowledge cybersecurity software, is sharing our findings about Americans' password habits and practices. By raising awareness of the personal finances and data put at risk every day by weak, duplicate and shared passwords, we hope to reduce the risk of cybercrime and promote better password practices among Americans.

EXECUTIVE SUMMARY

Our research was conducted by Censuswide, an independent market research consultancy, between August 11th and 15th, 2022. The survey took place via an online link with 4,007 nationally representative respondents (18+) in the UK and US. Censuswide are members of the British Polling Council, abide by and employ members of the Market Research Society which is based on the ESOMAR principles.

Through this data, we found that despite the growing awareness of cybercrimes, Americans continue to ignore basic password hygiene, unwittingly offering up information to cybercriminals and scammers, leading to breaches of personal information and loss of funds.

In an alarming finding, we found that approximately 56% of respondents reuse their passwords. Once one account's password is compromised, victims are putting themselves at a high risk of other accounts being breached.

Keeper's survey found a major cause of cyberattacks is the troublingly casual attitude to password protection. Close to 7 out of 10 respondents are concerned about what would happen if they were hit with a cyberattack, but nearly one-fifth of respondents only change their password if notified. Meanwhile, 15% of respondents admitted they know their passwords are already compromised on the dark web.

Gauging the level of importance people attach to their passwords in the US, we asked respondents what they would rather have happen, compared to losing all their passwords.

Over a third say they would rather be stood up on a date or not have access to TV for a week! When you sit down and think about it, a lot of our day-to-day lives are password protected. Resetting or creating all-new passwords for every password-protected account would be a labor-intensive activity!

Given the attitudes and behaviors on display in the study, it's alarming that US consumers are turning a blind eye to password hygiene. It demonstrates a pressing need for the public to adopt better cybersecurity by using a trusted password management system.

FINDINGS

Poor password management and the consequences

Poor password protection

Just over a third (34%) of respondents aged 45-54 have trusted their partner/spouse with their passwords, compared to over a fifth (22%) of respondents aged 18-24 who said the same.

Those surveyed leave themselves vulnerable to cybercrime with easy-to-guess passwords. 18% of respondents use a pet's name, 13% of respondents use their family member's name, 12% use their birthday, 11% use their own name, and 9% use a consecutive number (e.g. 123).

Just under a quarter (24%) of respondents aged 18-24 use their birthday when creating passwords, while 1 in 14 (7%) respondents aged 55-64 said the same, pointing to a more relaxed attitude to password hygiene among the young.

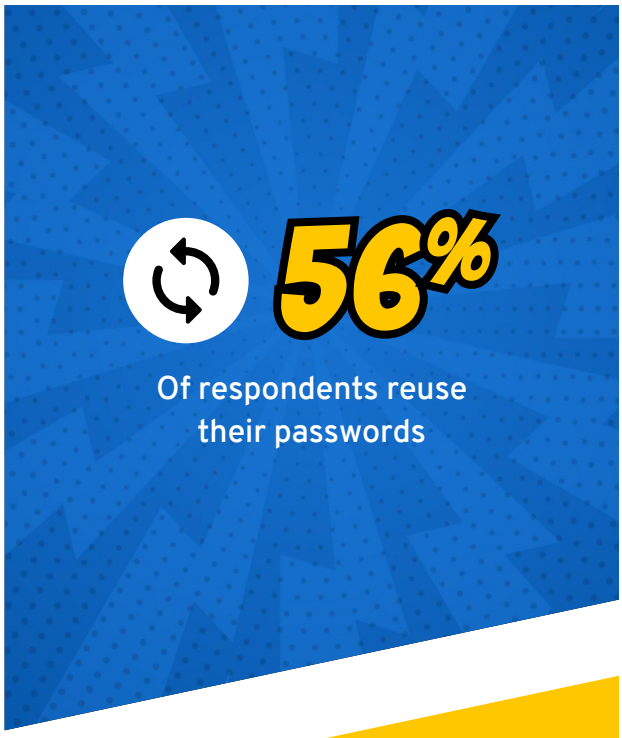
These findings also point to the availability of easy-to-guess passwords by other family members or close friends.

Password duplication

56% of respondents use the same password for multiple sites/apps, and on average, respondents use the same password for four different sites/apps.

When broken down by age group, on average, respondents aged 25-34 use the same password for five different sites/apps, while respondents aged 65+ use the same password for three different sites/apps.

As a result, the likelihood of having multiple accounts affected by a cyberattack is a real possibility in the US.



The impact of being hacked

55% of respondents in our survey have been the victim of a cyberattack at least once, with almost a fifth (18%) of respondents saying money was stolen as a result. On average, respondents lost $378.

Almost one-third (32%) of respondents said their social media account logins have been stolen, with an even higher percentage for those 18-24. Over 2 in 5 respondents in that group have had their social media logins stolen as a result of a breach.

Meanwhile, 15% of the total population surveyed said they know their passwords are compromised or available on the dark web.

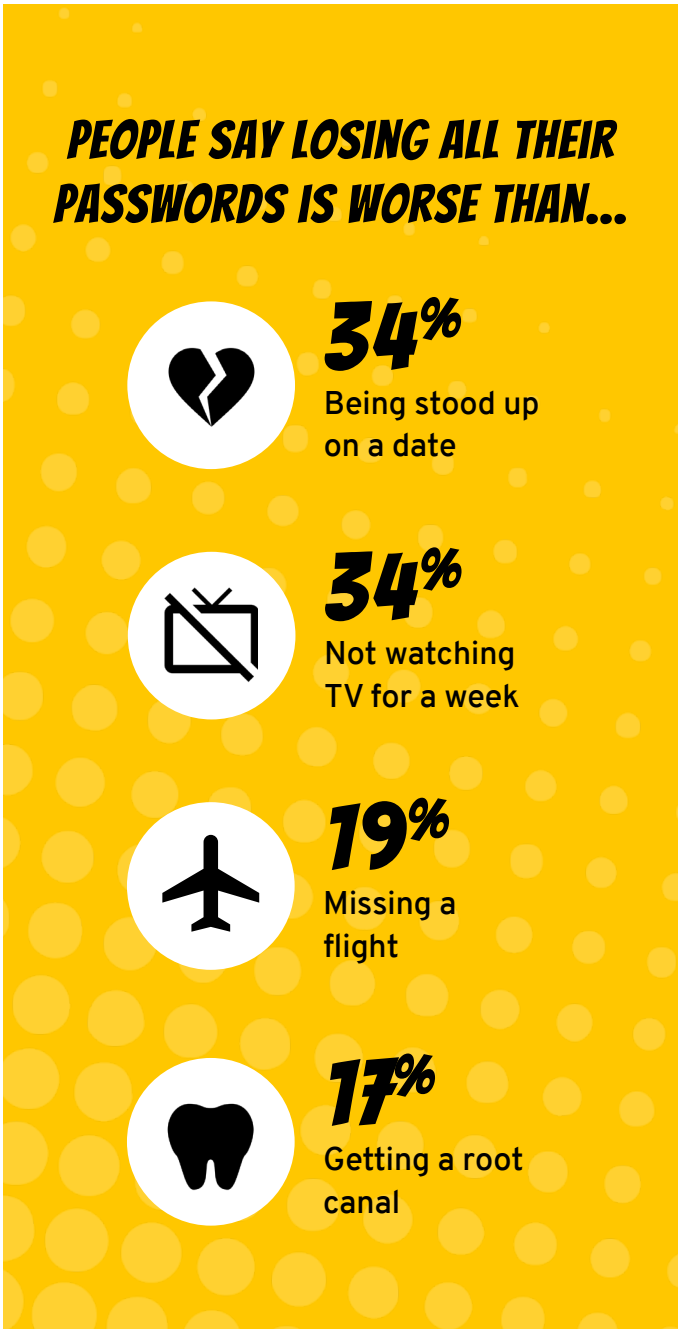
How much do we value our passwords?

Over one-third (34%) of respondents aged 25-34 would rather be stood up on a date than lose all their passwords.

A little over one-third of respondents would rather not watch TV for a week than lose all their passwords.

19% of respondents would rather miss a flight than lose all their passwords, and 17% of respondents shared they would rather get a root canal than lose all their passwords!

Over three-quarters (77%) of respondents aged 65+ said, when thinking of passwords, security is most important to them, while 66% of respondents aged 18-24 said the same.



MAINTAINING GOOD HYGIENE AND REDUCING PASSWORD OVERLOAD

Remembering and changing passwords

We found that on average, respondents forget their passwords 51 times per year.

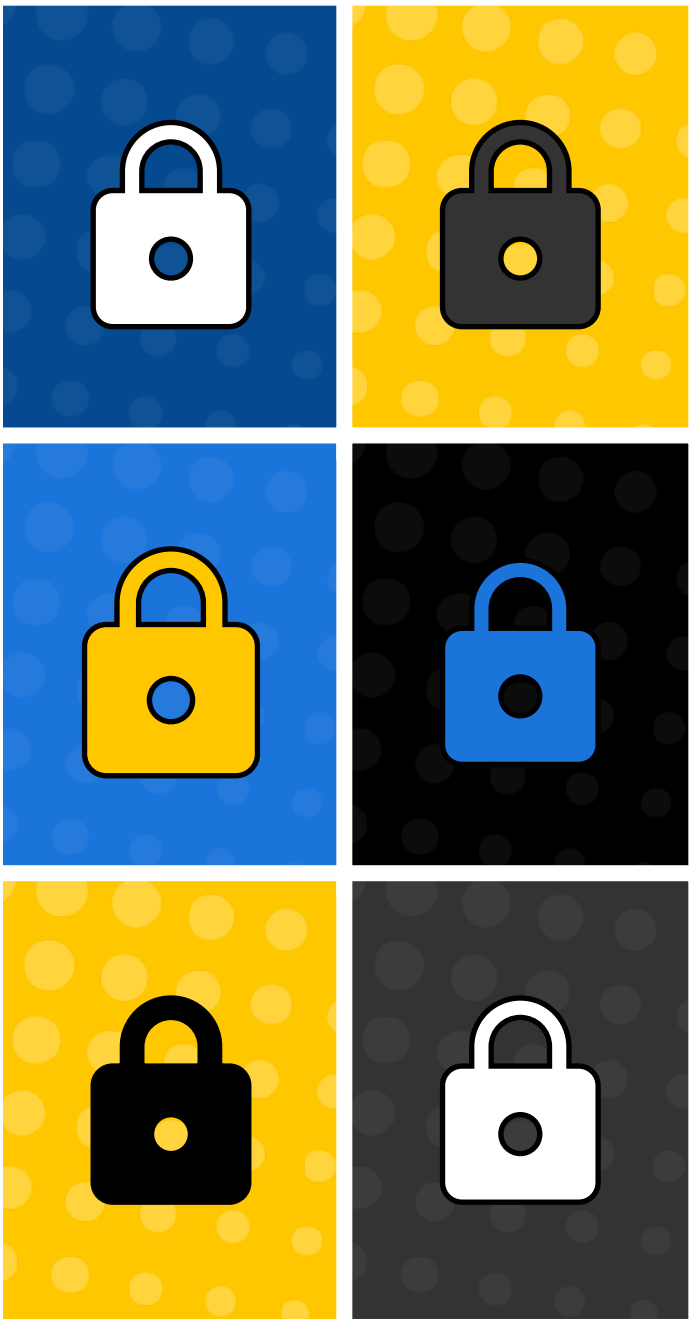
Respondents aged 18-24 forget their password close to 50 times a year, compared to respondents aged 65+ who forget theirs 62 times a year.

On average, respondents in our study change their password 10 times per year, and just about 1 in 9 (11%) respondents change their password once a month. Remembering and changing passwords is clearly problematic and points to widespread security loopholes.

22% of the survey say they 'just remember' their passwords, but the results were troubling for the more forgetful among us.

The most common method of remembering a password, particularly among older age groups, was physically writing a password down. Over half (53%) of respondents aged 65 + said they keep their passwords on sticky notes, in a diary, or on a notepad. 24% of respondents aged 35-44 said the same. 16% of those surveyed use password management software, yet 12% choose to store passwords in their web browsers.

These instances show that potential cybercriminals have ready access to our most sensitive devices and data.



How many password-protected accounts/ apps do we have?

On average, respondents report having 20 password-protected accounts/apps. Respondents aged 65+ reported having an average amount of 22 password-protected accounts/apps.

With accounts and apps we use daily being password protected, there is a pressing need for solid password protection across a number of devices.

Using password locks

Many individuals are not protecting their devices at all. Only about three in five (64%) respondents use a passcode to protect access to their phones.

Roughly half (53%) of respondents use a passcode to unlock their computers.

Using multi or two-factor authentication (MFA/2FA)

Almost one in six respondents have used the second step to secure their accounts, known as multi or two-factor authentication, but report that they find it difficult.

Likewise, a fifth (20%) of respondents have not used multi-factor authentication simply because they're worried it will be too difficult.

KNOW THE RISKS AND STAY VIGILANT

Spotting and identifying cyberattacks

62% of respondents said they would be confident in identifying a phishing email.

60% of respondents were confident they could spot a phony social media message coming from a friend who didn't send it.

57% of respondents would be confident in identifying pop-ups as a sign of a cyberattack; however, 18% would not be confident in doing so.

54% of respondents said they would know if their online passwords suddenly stopped working, it could be a sign of a cyberattack, while 18% would not be confident in making that identification.

Are we worried about being hacked?

Almost seven in ten (68%) respondents are concerned about what would happen if they were to be hacked, but just a third (33%) were very concerned, pointing to a casual attitude towards the implications of a cyberbreach.

Almost a third (32%) of respondents think they are likely to be hacked, with just over one in 12 saying it's very likely. This tallies with a separate survey carried out in 31 countries around the world between October and November 2020, which revealed a third of respondents thought at least one of their online accounts (e.g. email, social media, banking) would be hacked the following year.

62%
Of respondents are confident in identifying phishing emails

60%
Of respondents were confident they could spot a phony social media message

57%
Of respondents would be able to identify pop-ups as a sign of a cyberattack

CONCLUSION

Our findings show a troubling disconnect between the value people attach to their passwords and the means they use to protect them. In the US, people would rather see a dentist than lose their passwords, yet safe selection, storage, and management of passwords were found to be severely lacking in this study.

It is of great concern to see passwords being shared and duplicated across multiple platforms. It's equally concerning to see the use of overly simple passwords, relying on publicly-available data, such as names and birthdays. This will remain an acute challenge as we continue to use a range of devices and platforms to access the internet.

The impact of poor password protection was evidenced by the number of people in the survey reporting they've personally fallen victim to a cyberattack, resulting in financial loss and compromised social media profiles.

The report showed, most of all, that cybersecurity relies on attitudes. Despite demonstrating a high awareness of cybercrime, we noted a reluctance to take action against it, ranging from forgoing multi-factor authentication to not responding to a cyberbreach, despite knowing it had taken place. What we are seeing, therefore, is a strong sense of apathy developing, in which cyberattacks are viewed as an everyday inconvenience, part of modern life.

Yet, unchecked, cybercrime will only get worse. According to the Federal Bureau of Investigation's 2021 Internet Crime Report, potential losses from cybercrime cost the American public $6.9 billion. The FBI also reported two of the top cybercrimes of 2021 were personal data breaches and phishing attacks.

It's easy to be negligent about our password hygiene, but the threat of cybercrime is ever present. It's important to raise awareness of the preventative and simple solutions that can alleviate the stress of potential cyberattacks. Safeguarding your personal data can be as easy as implementing a password manager and using multi-factor authentication.

About Keeper Security

Keeper Security, Inc. ("Keeper") is transforming the way organizations and individuals protect their credentials, secrets, connections and sensitive digital assets to significantly reduce the risks of identity security-related cyberattacks, while gaining visibility and control. Keeper is the leading provider of zero-trust and zero-knowledge security cloud services trusted by millions of people and thousands of organizations for password management, secrets management, privileged access, secure remote infrastructure access and encrypted messaging.

Keeper's products are the highest-rated in the industry across G2, Trustpilot, PCMag and U.S. News & World Report. For the last several years, Keeper has received several InfoSec Awards from Cyber Defense Magazine for its cybersecurity enterprise software. Keeper is SOC 2 and ISO 27001 certified, FIPS 140-2 validated and FedRAMP Authorized. Keeper is backed by Insight Partners, a leading venture capital and private equity firm with $90b AUM.