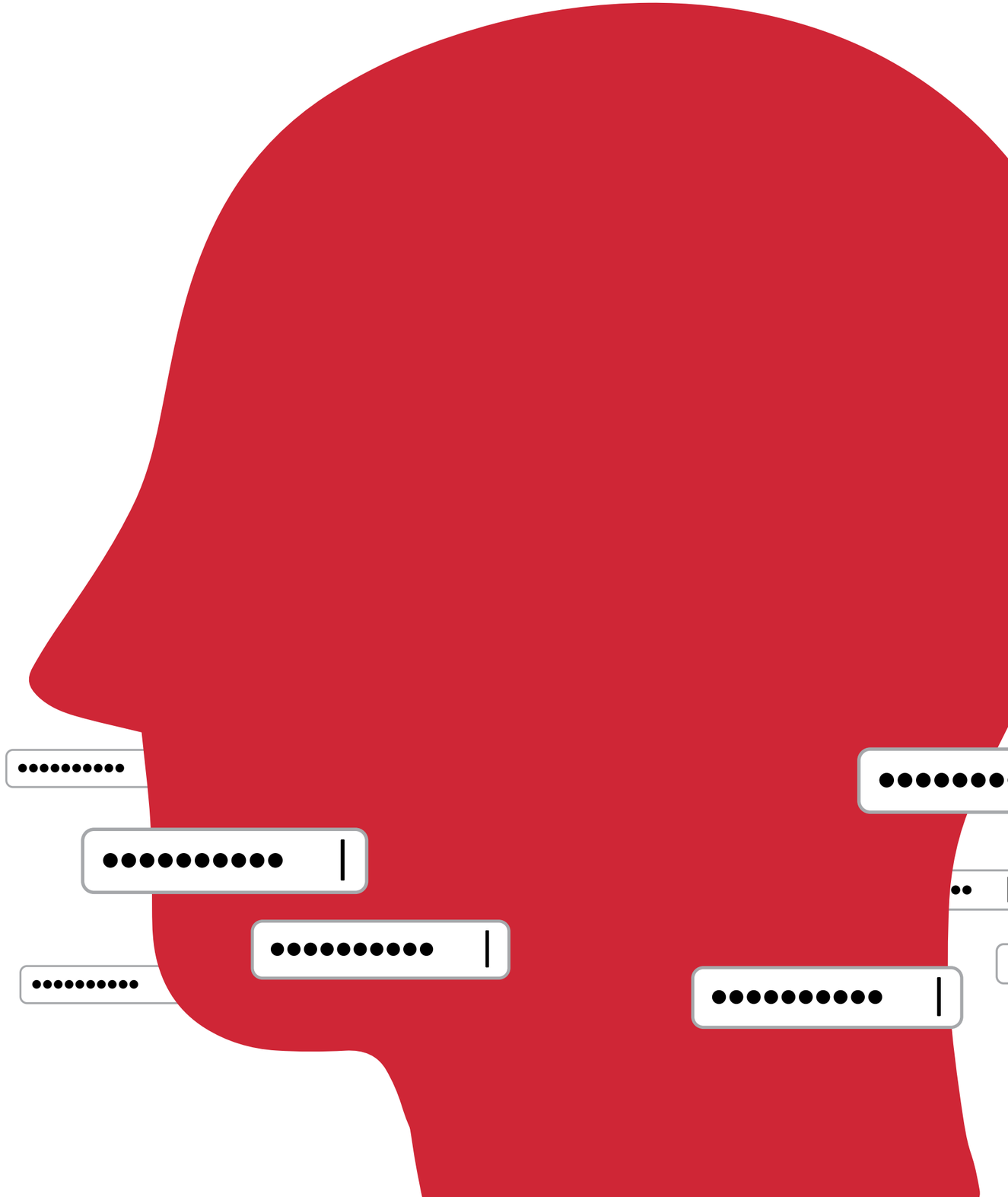
LastPass •••|

Psychology of PASSWORDS|

2022



Overview

In our new 2022 Psychology of Passwords report, we explore what people think they know about cybersecurity and what that means for how they choose to protect themselves online. For the first time in this annual report, we also analyze how people learn about cybersecurity topics and the generational differences in approaching digital security.

Given our proximity to and reliance upon technology in everyday life, some cybersecurity awareness inevitably filters down to the general public. In fact, **65%** of people say they've had some cybersecurity education. Yet despite most people receiving some cybersecurity education, our report found that many **(62%)** are still reusing passwords. **Why is that?** It turns out that education and awareness might not be enough.

So, what exactly does cyber awareness look like in 2022? And for the average person, does awareness translate to meaningful action? As cyber threats continue to evolve in their nature, we found what motivates people to change their online habits, and how the different generations approach cybersecurity.

Regardless of generational differences across Boomers (born between 1946-1964), Millennials (1981-1996), Gen X (1965-1980) and Gen Z (1997-2010), our research shows a false sense of password security runs rampant given current behaviors.

Key Takeaways

No generation is immune to password mishaps:

Gen Z is confident when it comes to their password management, while also being the biggest offenders of poor password hygiene. While Gen Z is also more likely to recognize that using the same or similar password for multiple logins is a risk, they use a variation of a single password **69%** of the time, alongside Millennials who do this **66%** of the time.

Confidence is creating a false sense of security:

89% of respondents acknowledged that using the same password or variation is a risk, but only **12%** use different passwords for different accounts, and **62%** always or mostly use the same password or a variation. In good news, people are now increasingly using variations of the same password, clocking in at **41%** in 2022 vs. **36%** in 2021.

Awareness doesn't translate to action:

With **65%** of those surveyed claiming to have some type of cybersecurity education, the majority **(79%)** found their education to be effective, whether formal or informal. But of those who received cybersecurity education, only **31%** stopped reusing passwords. And only **25%** started using a password manager.

While only 12% of respondents admit to always using unique passwords,

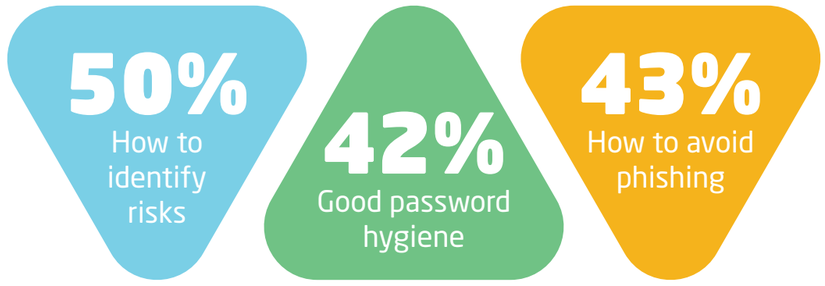
89% know that reused or similar passwords are a security risk.

Disconnect between cyber awareness and cybersecurity practices

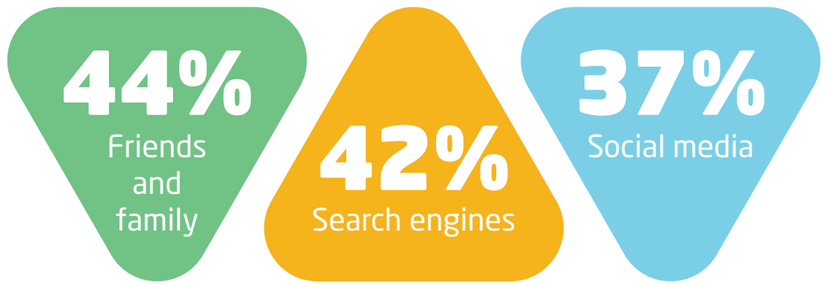
With nearly two-thirds **(65%)** of respondents sharing that they have some type of cybersecurity education, only **31%** stopped reusing passwords and only **33%** create strong passwords for their work accounts. While awareness does not translate into action, there's a need to combine this cybersecurity education with the appropriate tools, like a password manager, along with multi-factor authentication (MFA) and single sign-on (SSO) to drive action and accountability toward safer online habits.

The majority of respondents **(44%)** claimed to have received informal training, and learned how to identify risks **(50%)**, good password hygiene **(42%)**, or how to avoid phishing **(43%)**. While most who answered were also aware of malware **(74%)**, phishing **(68%)**, and ransomware **(47%)**, very few had heard of other cybersecurity threats, such as brute force attack, credential stuffing, or a drive-by attack.

Those who received informal or formal cybersecurity education learned:

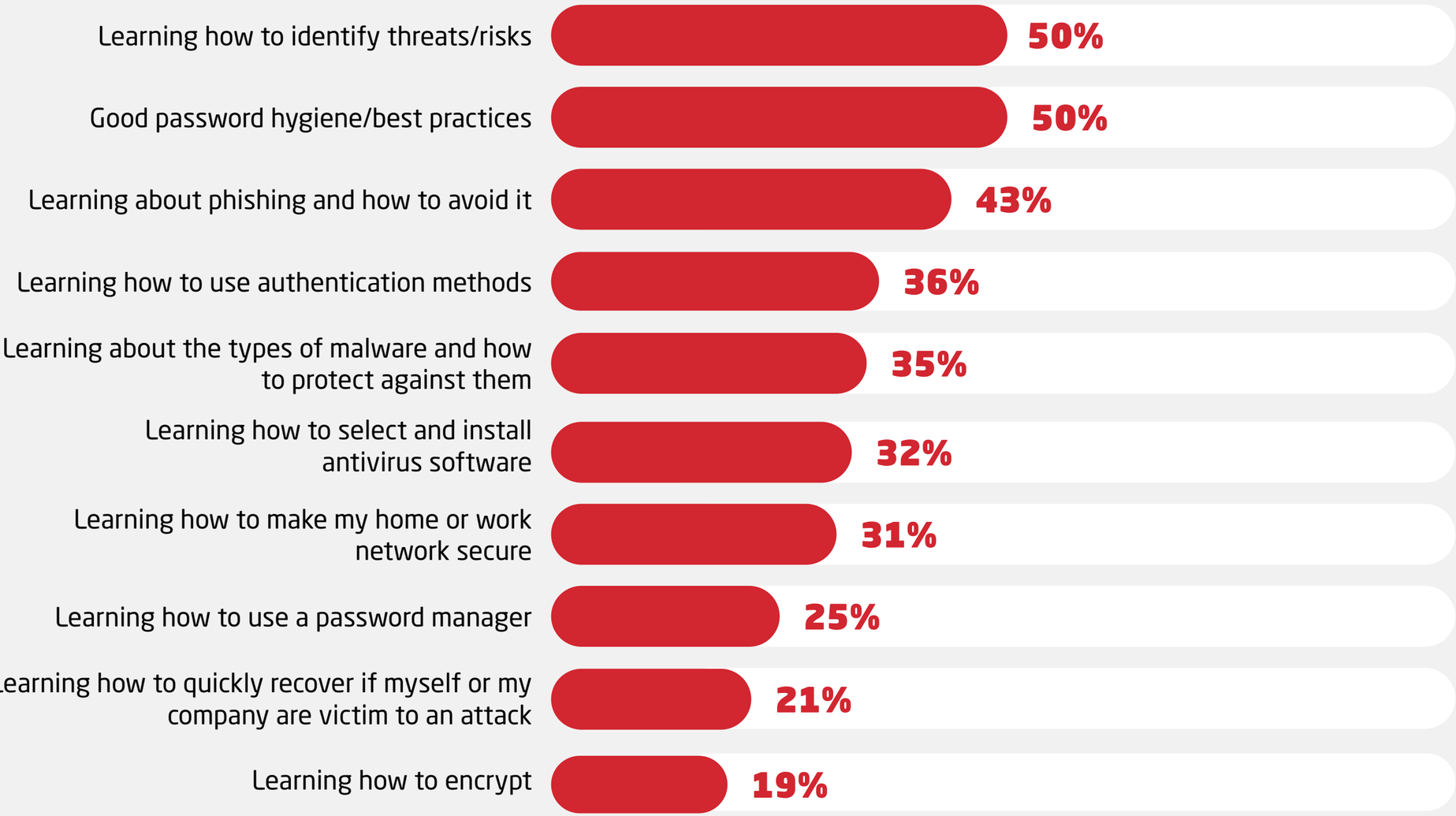


The majority 44% have informal training, which includes learning cybersecurity best practices from:



The majority **79%** found their education - whether formal or informal - to be effective.

What type of cyber education did people receive?



Of those who received a cybersecurity education,

Only

stopped reusing passwords**.**

And only

started using a password manager.

This lack of positive action may be connected to the fact that most

did not seek out a cybersecurity education on their own.

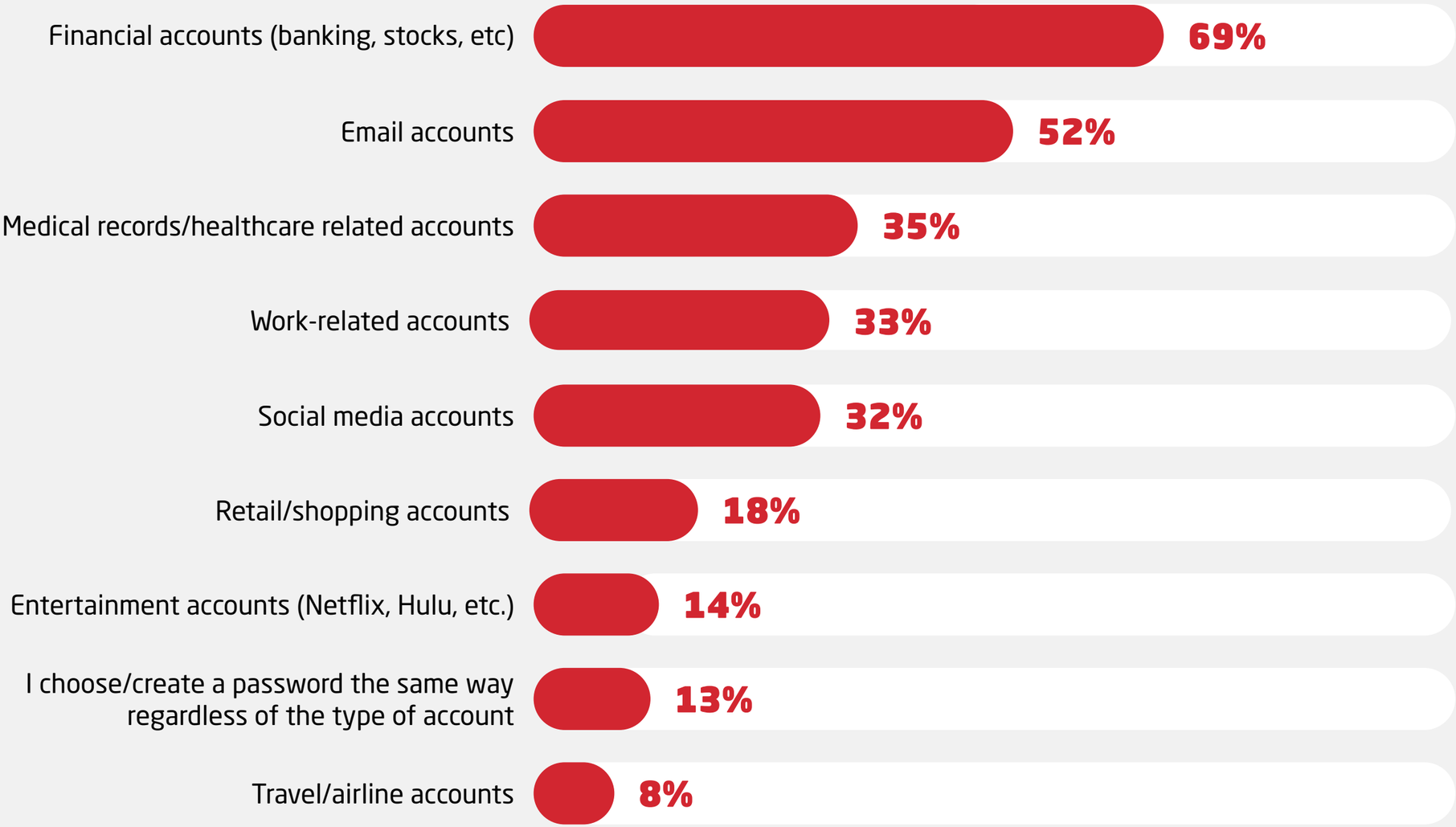
Add to that fact that less than half

of people think about cybersecurity weekly or more.

So, what about putting this education into practice? That's a different story.

And consumer perception of security importance varies by the source they are interacting with online – when all digital instances should be treated with the same level of security.

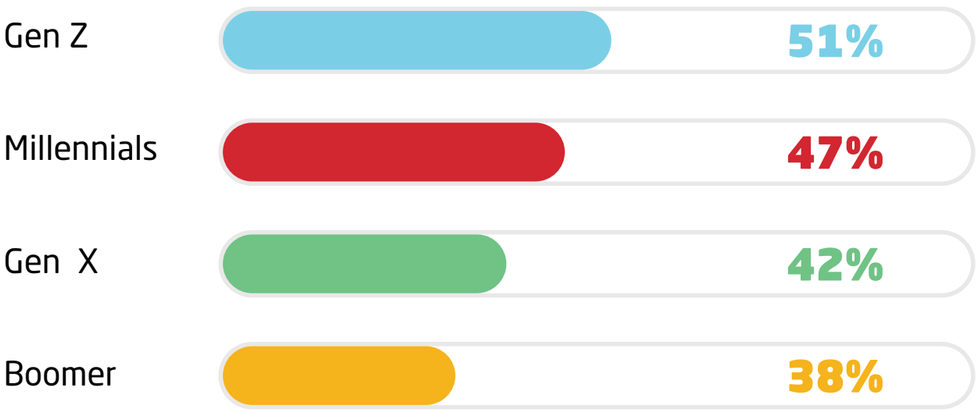
What online accounts would people create a stronger/more complex password for?



No generation is immune to mishaps

With Gen Z and Millennials having spent most of their lives online, the confidence and perception of themselves as online experts has created a blind spot when it comes to the reality of their behavior. Gen Z is the most assured generation when it comes to their password management skills while also being the biggest offenders.

Most Likely to Memorize Passwords:



Gen Z believes their password methods to be **“very safe.”**

Gen Z is more likely to recognize that using the same or similar password for multiple logins is a risk, alongside Millennials.

On the other hand, Gen Z is the generation most likely to use memorization to keep track of their passwords.

Baby Boomers are less confident about their password management but more cautious - and with the best password hygiene across generations.

They've had to catch up to their younger counterparts when it comes to the digital landscape, and they're also in a better position financially than Millennials and Gen Z - and thus, have more to lose online. While Baby Boomers are least likely to rate their password tracking methods as **"very safe"** and more likely to deem them **"neither safe nor risky,"** they are actually the most likely to create unique passwords and the least likely to use the same password or a variation of that.

77% **of consumers, regardless of age, noted the security tools they use for work, including MFA and password managers, are easy to implement**

When it comes to securing different types of accounts, Gen Z leads the pack with creating stronger passwords for social media and entertainment accounts.

Interestingly enough, Millennials and Gen Z create stronger passwords than Boomers when it comes to their work accounts, though this could also be attributed to many Baby Boomers retiring.

When it came to BREACHES, proximity drove the younger generations to change their passwords.

Millennial + Gen Z

change their passwords because of personal identity theft or identity theft of someone they know.

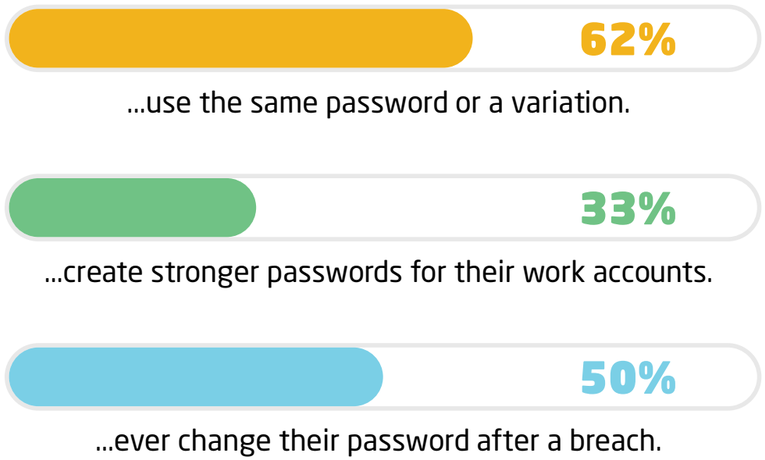
Baby Boomers

were more likely to change their password in event of a major bank breach, for example.

Knowledge workers have a false sense of password security

High confidence doesn't translate to better behavior for knowledge workers[1]. In fact, it may even create a false sense of safety that is detrimental to good password hygiene. With **73%** of respondents rating their current password behaviors as safe, and **89%** aware that using the same password or variation is a risk, respondents are switching from one bad habit to another in their quest to make password management as easy as possible.

Yet...



1 Knowledge worker is 30-55 years of age, employed full-time or as a contractor or freelancer, and has 5+ passwords.

Conclusion

Online users still need to level up cybersecurity by taking action versus a passive stance to protect their digital lives. No generation is immune to password mishaps, confidence is creating a false sense of security and awareness doesn't translate to action. Password managers can provide an easy way to bridge the gap between perceived and real safety online, transforming your knowledge into positive action.

Methodology

LastPass commissioned the market research firm Lab42 to reveal the current state of password behaviors in the new era of remote work. The responses were generated from a survey of 3,750 professionals at organizations across a variety of industries in the United States, United Kingdom, Germany, Australia, Singapore, and India. The survey asked the professionals surveyed about their feelings and behaviors regarding online security.

The result? An increase in time spent online with continued poor password behavior and cognitive dissonance.

LastPass is an award-winning password manager which has helped more than 33 million registered users organize and protect their online lives. For more than 100,000 businesses of all sizes, LastPass provides password and identity management solutions that are convenient, easy to manage and effortless to use. From enterprise password management and single sign-on to adaptive multi-factor authentication, LastPass for Business gives superior control to IT and frictionless access to users.

For more information, visit: https://lastpass.com.