KEEPER®

Password Management Report

Unifying Perception with Reality

Intro

There is no getting away from the fact that passwords are still the cornerstone of modern cybersecurity practices. Despite decades of advice to users to always pick strong and unique passwords for each of their online accounts, Keeper Security found that only one-quarter of survey respondents actually do this. Many use repeat variations of the same password (34%) or still admit to using simple passwords to secure their online accounts (30%). Perhaps more worryingly, almost half (44%) of those who claimed all their passwords were well-managed also said they used repeated variations of them. One in five also admitted to knowing they've had at least one password involved in a data breach or available on the dark web.

At first glance, these results may come as a shock, especially to those in the cybersecurity industry who have been touting these simple best practices for years. However, when considering more than one in three people (35%) globally admit to feeling overwhelmed when it comes to taking action to improve their cybersecurity, and one in ten admit to neglecting password management altogether, the results are much less of a surprise.

The Keeper Password Survey looks at password habits of over 8,000 individuals across the US, UK, France and Germany and delves into what people say they do to ensure their cybersecurity, what they actually do and how they feel about cybersecurity in general. With just over one in four people describing themselves either as an ostrich burying their heads in the sand, careless as a bull in a china shop or a possum paralysed with fear - clearly, the industry still has much work to do to get more people more comfortable with cybersecurity and better protected as a result.

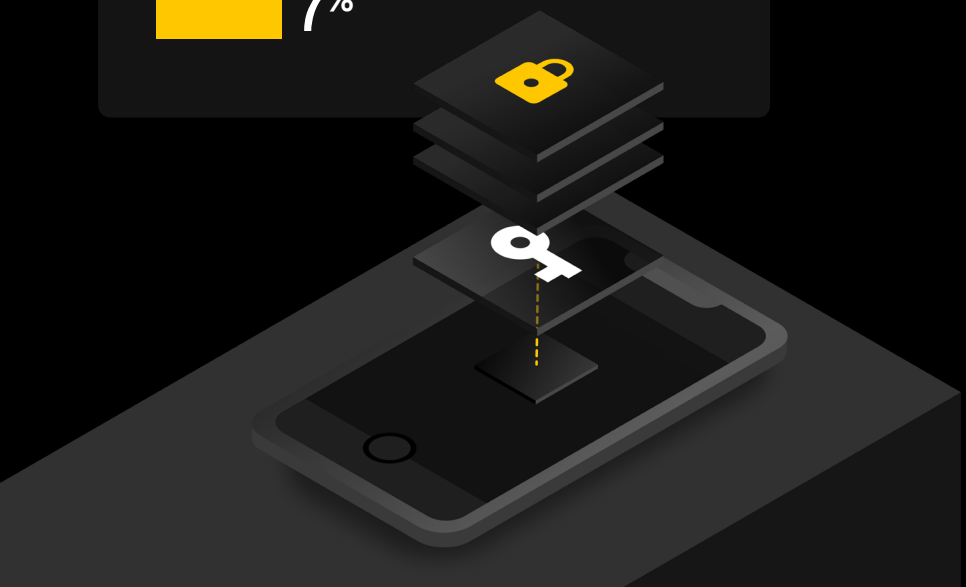
> More than one in four people describe themselves either as an **ostrich burying their heads in the sand, careless as a bull in a china shop or a possum paralysed with fear**

What is the best way to achieve personal cybersecurity?

Password Management

Up to 80% of successful data breaches stem from compromised login credentials according to the annual Verizon Data Breach Investigations Report. Keeper's survey respondents felt that strong passwords were the single best method to achieve personal cybersecurity, yet nearly three in four fail to implement industry-recommended password protection practices in their daily lives. Stranger still, only 7% of respondents globally recognised password managers as the best way to achieve personal cybersecurity.

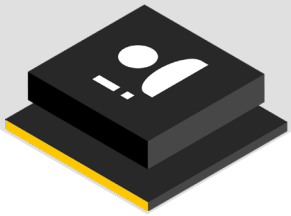
Considering password managers are widely promoted in security circles and recommended by leading government agencies as the safest and most convenient method of creating and storing strong passwords, it's clear the layman is under-informed. This is reflected in the respondents' own password behaviours. Just 25% globally said they use strong, unique passwords for all of their accounts. That means only a quarter of people have actually implemented strong password practices into their everyday lives.



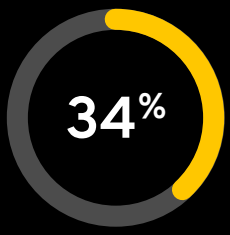
Thirty-four percent of respondents said they use strong passwords, but repeat variations of them. This makes them susceptible to credential-stuffing cyberattacks, in which a cybercriminal uses stolen credentials to access multiple accounts. This type of brute force attack is often successful and considered a hacker's "low-hanging fruit" - yet more than a third of respondents admit to the risky practice of repeating passwords that leads to these attacks. Nearly one in five (17%) Gen Z respondents use simple, repeat variations of passwords, making them the most susceptible to these types of attacks. The use of a password manager reduces credential-stuffing attacks by allowing users to create and store strong and unique passwords for every account, yet the data indicates respondents are not making use of this widely-available solution.

17%

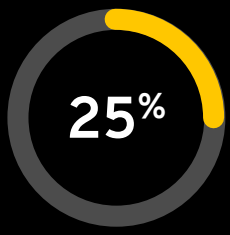
of Gen Z respondents use simple, repeated variations of passwords, making them the most susceptible to these types of attacks



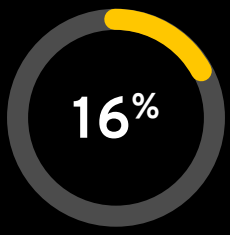
Which, if any, best describes your password practices?



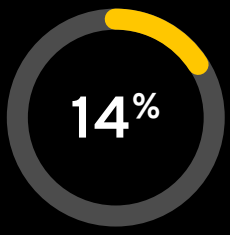
I use strong passwords, but repeat variations of them



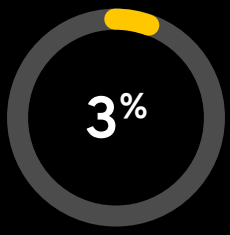
I use strong and unique passwords for every account



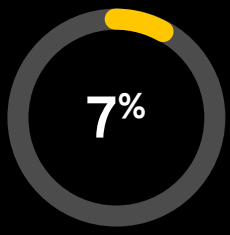
I use simple, but unique passwords for every account



I use simple passwords and repeat variations of them

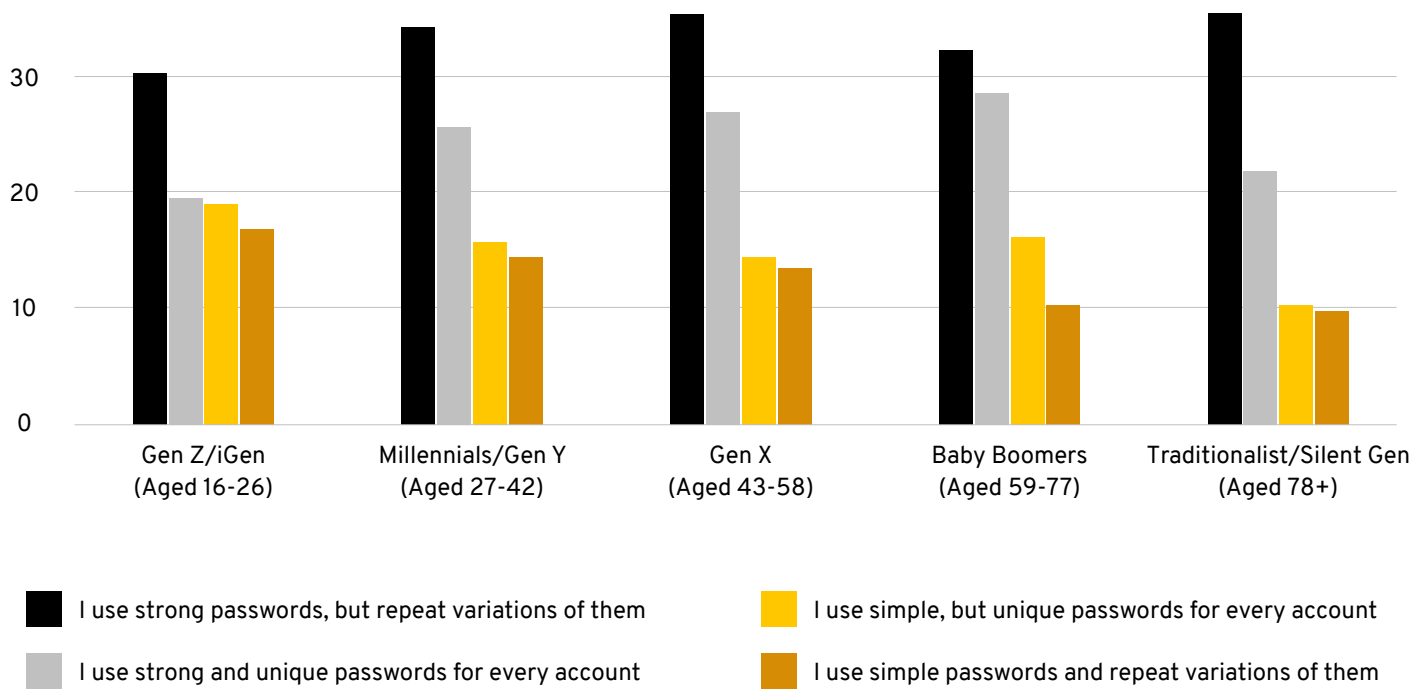


I do not know how to ensure my password-protected accounts are secure



None of the above

Which, if any, best describes your password practices?



It's not, as we might assume, young people who have the strongest password practices. In fact, 29% of Baby Boomers use strong and unique passwords for every account, compared to only 20% of Gen Z respondents. One possible reason is that Baby Boomers are more likely to be dealing with important data or documents, both in their personal and professional lives, and as such, recognise the need to protect them.

Despite only 25% of respondents using strong, unique passwords, 36% believed that all their passwords were well-managed. And of those who thought their passwords were well-managed, only one in three followed best practice advice to use strong and unique passwords for all of their accounts. This gap suggests those surveyed are still unaware of what good password practices are or are overconfident when it comes to their cybersecurity. Most likely, it's a mix of both.

KEEPER

Understanding of Cybersecurity

This overconfidence is reflected in our respondent's broader feelings about cybersecurity. Despite our results showing that a majority (75%) of respondents do not adhere to widely accepted password best practices, a staggering 51% thought that cybersecurity was easy to understand. However, of those who found it easy to understand, half said they used repeat variations of passwords. This suggests a large number of those surveyed are grossly overestimating their cyber-savvy or are wilfully ignoring password hygiene advice.

Our results suggest it may be the latter, with one in four respondents indicating that cybersecurity was easy to understand but overwhelming. Our results suggest that feeling of being overwhelmed is a major contributing factor to poor password hygiene. While it may be surprising that older generations generally implement better password practices than Gen Z, when we consider a staggering 40% of our youngest respondents found cybersecurity overwhelming, these results come as less of a shock. It's possible, in light of these results, that the more educated a person is about cybersecurity, the more overwhelmed they are likely to be. This is especially true for password practices.

Which of the following best describes your understanding of cybersecurity?

Cybersecurity is easy to understand (Net)

51%

Cybersecurity is easy to understand and I take steps to protect myself

25%

Cybersecurity is easy to understand but taking action feels overwhelming

25%

Cybersecurity is difficult to understand but I take steps to protect myself

32%

Cybersecurity is difficult to understand and taking action feels overwhelming

10%

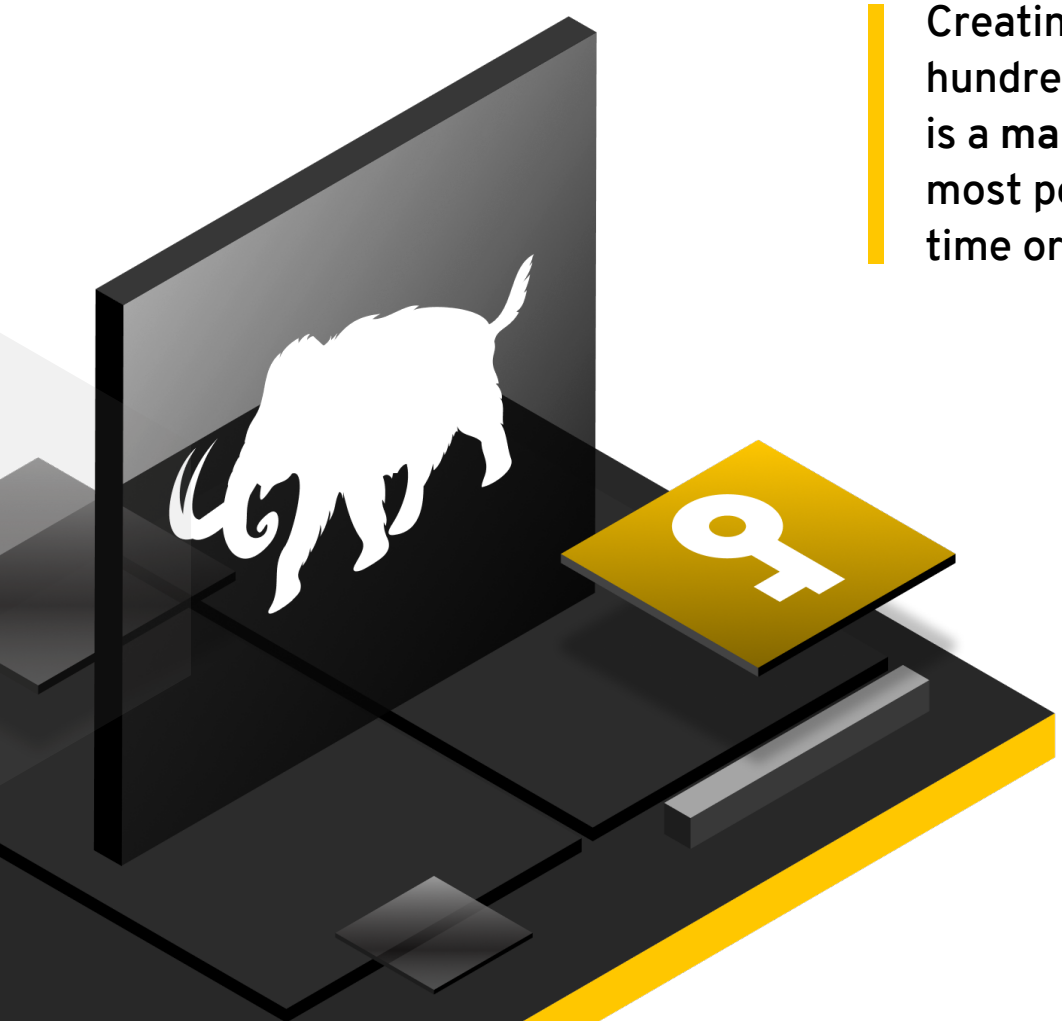
None of the above

8%

Cybersecurity is difficult to understand (Net)

41%

Users are constantly being told they must use strong, unique passwords for all their accounts, but aren't always told how to achieve this. Creating and remembering hundreds of unique passwords is a mammoth task, and one most people neither have the time or energy to tackle. When educating people on the importance of good password hygiene going forward, it is critical that security professionals speak of strong, unique passwords and password managers in the same breath – a failure to do so could result in people giving up on solid password practices entirely, as it feels like an overwhelmingly impossible feat.



Creating and remembering hundreds of unique passwords is a mammoth task, and one most people neither have the time or energy to tackle.

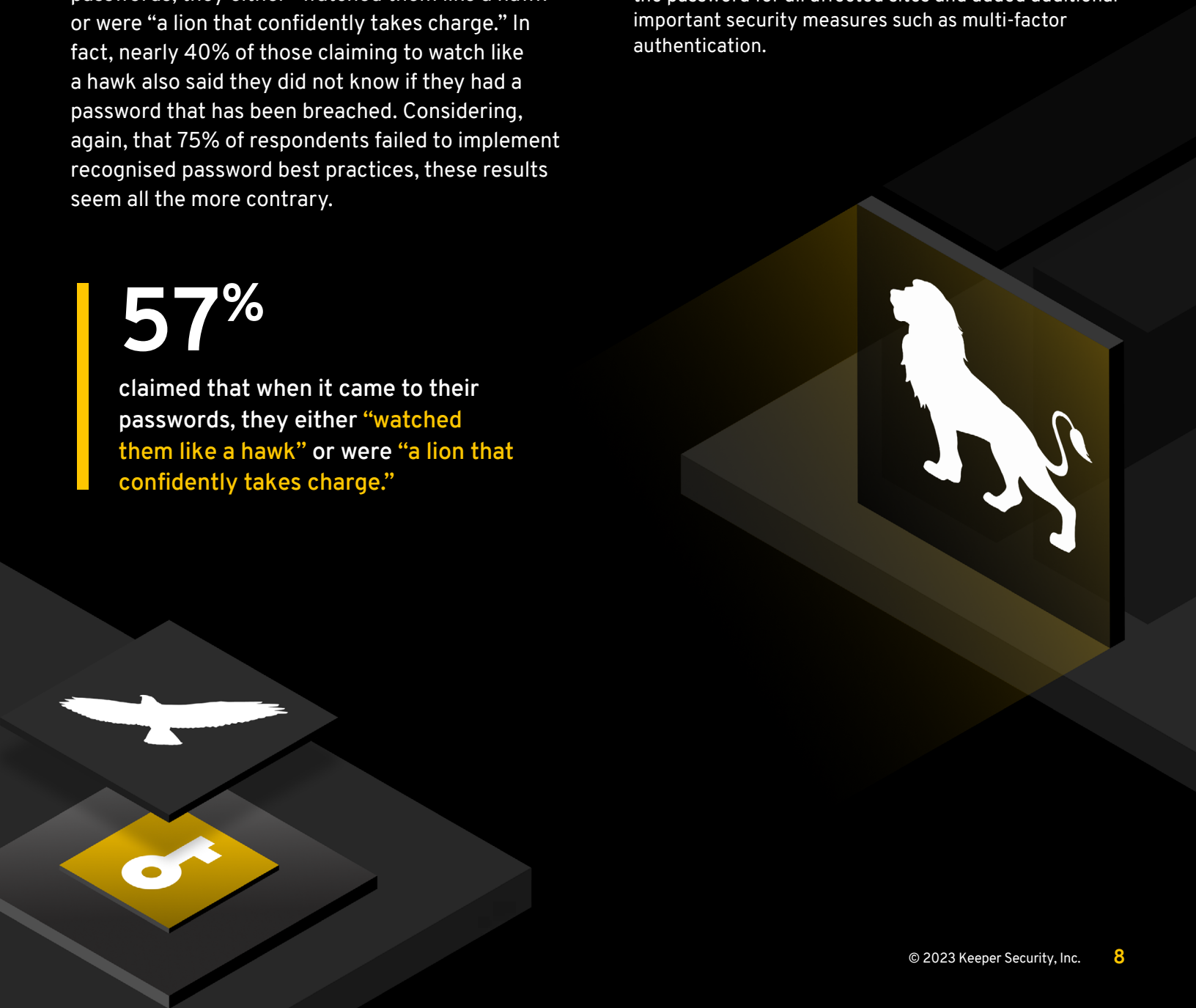
Approaches to Cybersecurity

Themes of overconfidence with underaction carry through to the latter part of our survey. Despite 39% of respondents being completely unaware of whether they've been breached, and 32% not knowing if they have a password available on the dark web, 57% claimed that, when it came to their passwords, they either "watched them like a hawk" or were "a lion that confidently takes charge." In fact, nearly 40% of those claiming to watch like a hawk also said they did not know if they had a password that has been breached. Considering, again, that 75% of respondents failed to implement recognised password best practices, these results seem all the more contrary.

Of those who did know they had a breached password or dark web exposure (20%), almost one in ten (9%) took no action whatsoever. One in three (32%) did a little better, changing the password for the affected website, and 31% did better still, changing the password for the breached site and all others in which they use the same password. Only one in four (24%) changed the password for all affected sites and added additional important security measures such as multi-factor authentication.

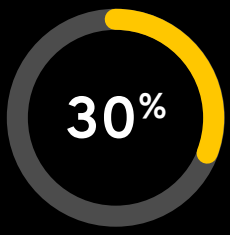
57%

claimed that when it came to their passwords, they either "watched them like a hawk" or were "a lion that confidently takes charge."

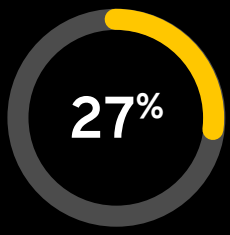


These results again indicate an astounding level of overconfidence in our respondents' password practices. **Only 27% of those surveyed felt they were "an ostrich burying their head in the sand," as "careless as a bull in a china shop" or "a possum paralysed with fear."** Considering a whopping three-quarters of respondents failed to take the correct course of action in the event of a breached or exposed password, it's obvious that many people seriously overestimate their cyber-savvy.

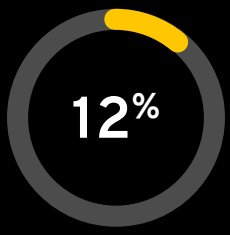
Which animal best describes your approach to cybersecurity?



I watch it like a hawk



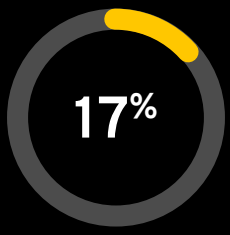
I'm a lion that confidently takes charge



I'm an ostrich burying its head in the sand

I'm as careless as a bull in a china shop

I'm a possum paralysed with fear



None of the above

Conclusion

There's no shortage of advice when it comes to cybersecurity, but our survey shows the onslaught of information available has become overwhelming for more than a third of people around the globe. While respondents tell us they believe strong passwords are the single best way to achieve personal cybersecurity, the majority fail to implement industry-recommended password protection practices in their daily lives. And despite our findings that three in four people do not adhere to password best practices, most believe cybersecurity is easy to understand.

Now is the time to bridge that gap.

Cybersecurity is a priority and cybersecurity solutions must also be. The threat landscape continues to expand as our lives shift from in-person banks, stores, and coffee shops to online banking, internet shopping, social networking, and everything in between. We have never been more dependent on our phones, computers and connected devices, yet we are overconfident in our ability to protect them and wilfully ignoring the actions we must take to do so. Perhaps we need more people to admit they're as careless as a bull in a china shop, burying their heads in the sand like an ostrich or simply paralysed with fear. Facing the reality and coming to recognise what's at stake, they can more confidently charge forward and take the necessary steps to protect their information, identities and online accounts.

Methodology

This survey was based on the Censuswide study conducted with 8,211 individuals aged 16+ in the US, UK, France and Germany in January 2023. Censuswide abides by and employs members of the Market Research Society which is based on the ESOMAR principles.