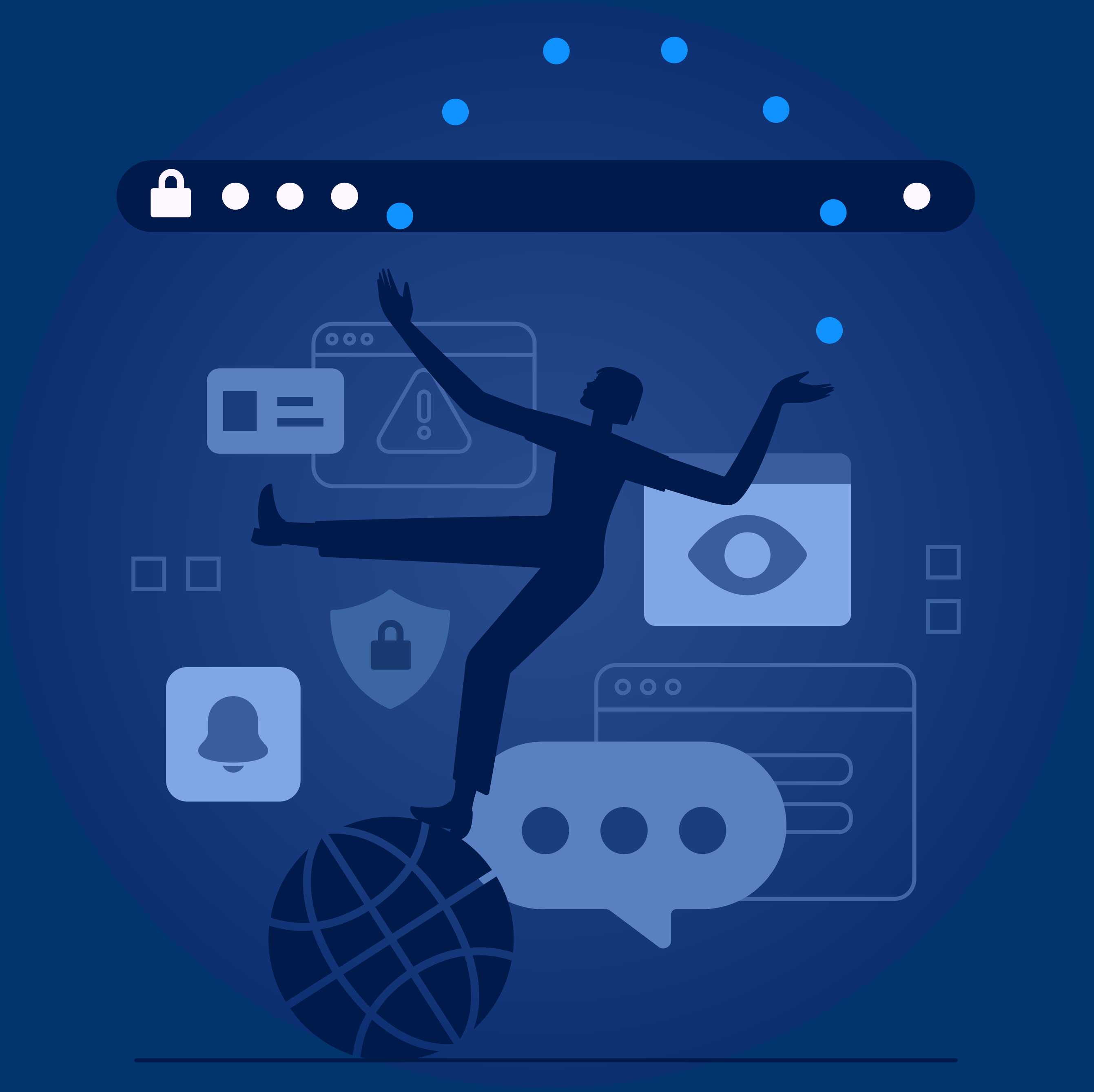
2022 STATE OF ACCESS REPORT

Distraction on overdrive

Security in a time of permacrisis



1Password

Executive Summary

1Password's 2022 State of Access Report, an annual survey of North American workers' sentiments and behaviors around cybersecurity and other critical aspects of modern work, reveals that the acute burnout detected in last year's survey has paved the way for a widespread sense of distraction in a time of "permacrisis."

Collins Dictionary recently declared "permacrisis" the official word of 2022, defining it as "an extended period of instability and insecurity, especially one resulting from a series of catastrophic events."

The darkest days of the Covid-19 pandemic appear to be behind us. Schools are back in person, new forms of remote and hybrid work have become familiar, and society has reopened. Yet as workers face pressures ranging from whipsawing markets to record-setting inflation to the first land combat in Europe since World War II, workers conveyed a vivid picture of distraction on overdrive.

One in three employees (32%) say they're the most stressed they've ever been in their lives, while four in five (79%) feel distracted on a typical working day. A quarter of employees (26%) say that distractions from world events make it hard to care about their jobs.

This proliferation of distractions has vast implications for workplace security. Verizon's 2022 Data Breach Investigations Report reveals that 82% of breaches involve a human element. When security protocols and practices aren't automated, even the most well-intentioned employees can unwittingly cause a breach. Distracted employees, we found, are more than twice as likely as others to say they do only the bare minimum at work when it comes to security (24% vs. 10%).

Even so, there's cause for some optimism. Security systems are improving. Large numbers of workers are using solutions like password managers, single sign-on, and multi-factor authentication. And employees have a broad understanding of the impact their own actions can have on their employers' ability to safeguard valuable company assets.

Key findings

Unprecedented stress

One in three employees (32%) say they're the most stressed they've ever been in their lives.

Distraction dilemma

Four in five employees (79%) feel distracted on a typical working day.

Global distractions

One in four workers (26%) – and **nearly half of workers in the tech/IT/telecom industry (46%)** – say that distractions from world events make it hard to care about their jobs.

Flouting the rules

45% of distracted employees don't bother following all security rules at their organizations, compared to **29% who are not distracted.**

Falling for phishing

There's growing awareness that bad actors preying on human psychology can make companies vulnerable: **A full half of employees (50%)** say the biggest security threat their company faces is the prospect of employees falling for scams or phishing attempts.

Password memory overload

Popular ways of storing work passwords include practices such as "just remembering them" **(40%)**, writing them down **(24%)**, and using a password manager **(29%).**

Evolution of authentication

70% of workers use two-factor or multi-factor authentication, **30%** use biometrics, **29%** use a password manager, and **24%** use single sign-on.

The easy way can be the secure way

There's a misperception that if security is too easy, it's not safe: Two-factor/multi-factor authentication is trusted **three times as much** as single sign-on **(65% vs. 19%).** While opinions can vary, both systems are considered valuable layers in the security stack.

Senior security snafus

Password hygiene is worse among senior leaders: **Half of workers at the level of director and above (49%)** use personal identifiers in their passwords, compared to **a third of individual contributors (34%).**

Tech workers' inconsistencies

Nearly half of tech/IT/telecom industry workers (49%) say they're more careful about online security at home than they are at work.

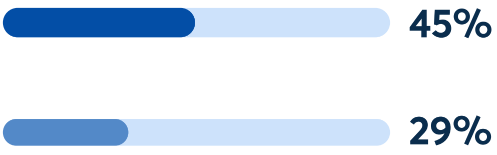
01

The distraction vortex

"Permacrisis: An extended period of instability and insecurity, especially one resulting from a series of catastrophic events."
– Collins Dictionary, 2022

Workers have faced what can feel like an avalanche of crises and concerns during the past year. They reported that their top sources of distraction are related to economics (53%) and Covid-19 (44%). But other concerns range from personal relationships (29%) to politics (22%) to climate change (15%).

Distraction can have serious security implications



We found that **45% of distracted workers** don't bother following all of the security rules at their organization, compared to **29% of those who aren't distracted.**

Unprecedented stress

One in three employees (32%) say they're the most stressed they've ever been in their lives.

Daily distractions

Four in five employees (79%) feel distracted on a typical working day.

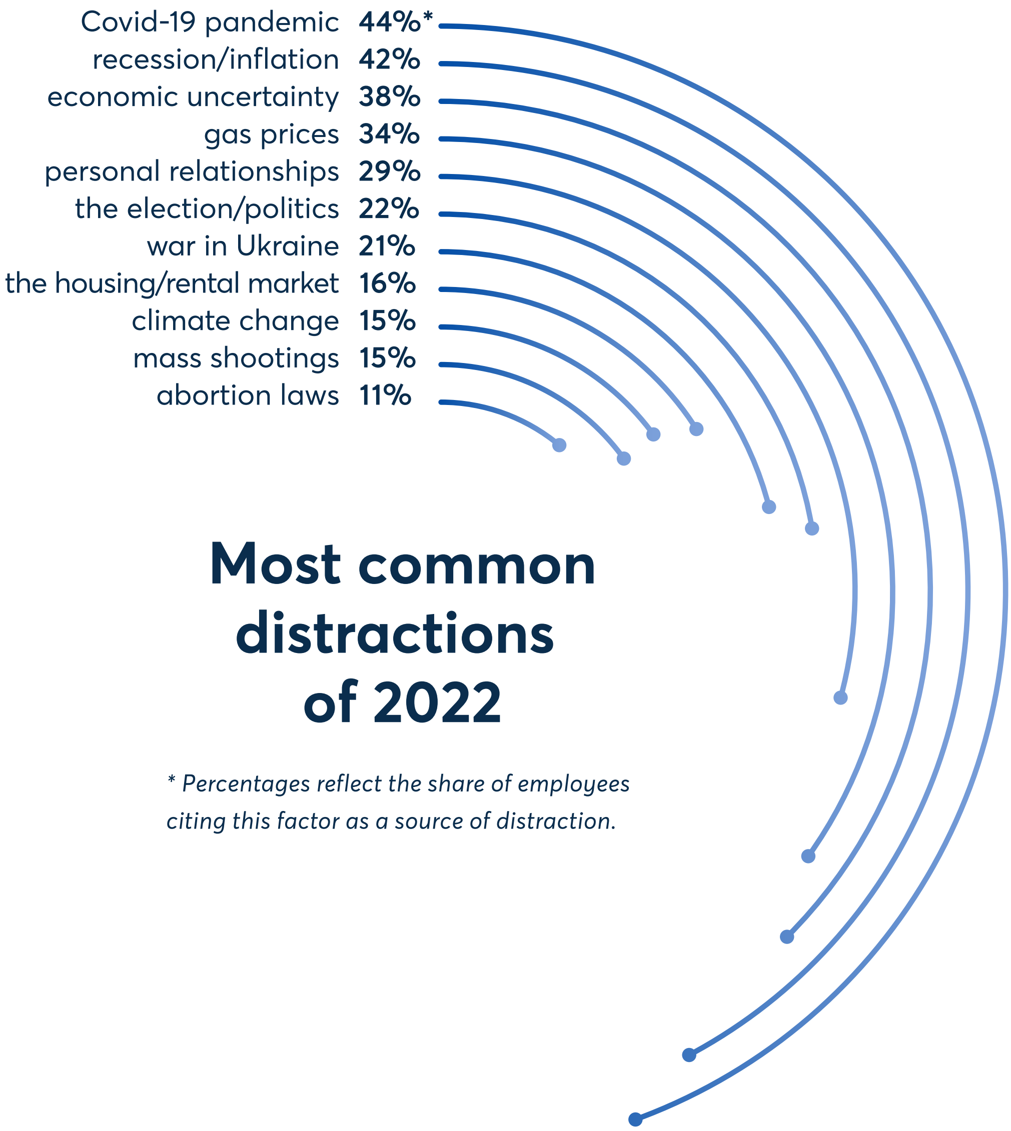
Missing motivation

One in four employees (26%) say that distractions from world events make it hard to care about their jobs.

A perfect storm

Workers have been bombarded by an array of distractions over the past year, from economic instability to the lingering Covid-19 pandemic to changes in abortion law.

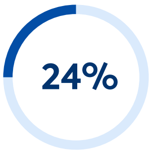
53% **of employees** say they've been distracted from work by economic or monetary concerns over the past year.



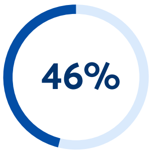
Most common distractions of 2022

** Percentages reflect the share of employees citing this factor as a source of distraction.*

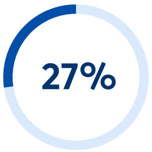
Security slips



of distracted employees say they do only the bare minimum when it comes to security at work, compared to **10% of those not distracted.**



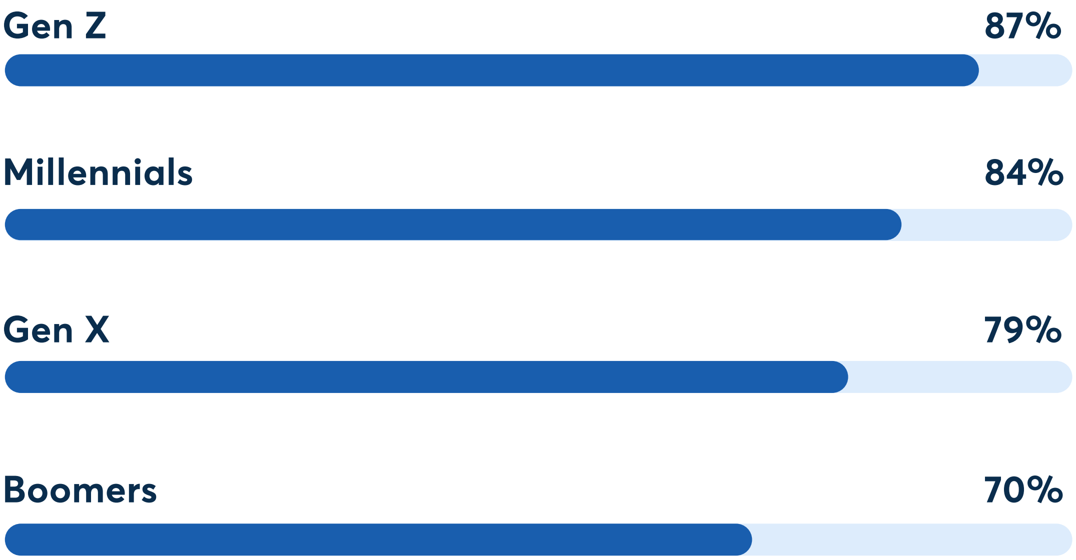
of distracted employees say, "I know it's risky, but I reuse passwords anyway," compared to **29% of those not distracted.**

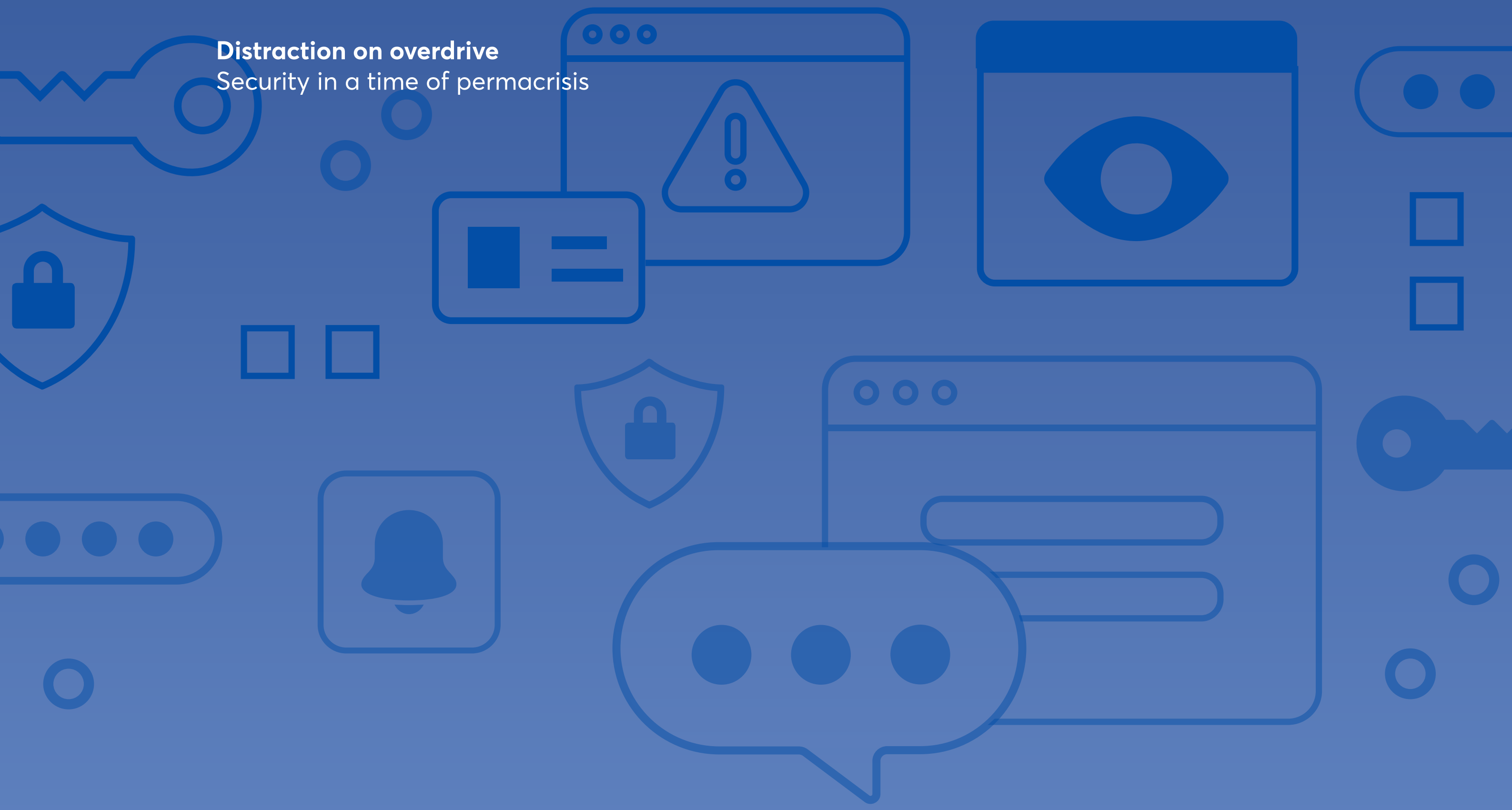


of distracted employees say, "I don't think my bad security habits could cause harm to my company," compared to **17% of those not distracted.**

Cross-generational distraction

All generations feel at least a little distracted on a typical working day, but younger generations are more likely to experience daily distractions.





02

Security is sinking in

As high-profile breaches and ransomware attacks splash across media headlines on a weekly basis, awareness of cyberthreats is rising. Because coverage of these developments is often accompanied by expert commentary on best security practices, people are coming to recognize that secure practices and technologies can make a difference.

When it comes to workplace security in particular, employees are largely aware of the role they play. Many now use solutions like multi-factor authentication. This is critical, as automation and systems can help counterbalance our natural human shortcomings around security. By removing human discretion from the equation, security tools and services can automate away the variability that results from stress and distraction.

Rising awareness

76% of workers are aware their individual actions have an impact on their company's overall security.

82% of workers would care if they caused a security breach.

Widespread use of security tools

89%
use password security products or services.

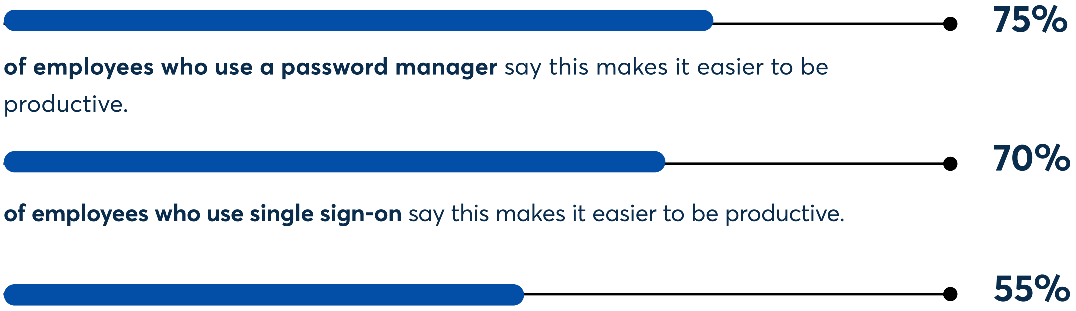
70%
use two-factor or multi-factor authentication (2FA/MFA).

30%
use biometrics.

29%
use a password manager.

24%
use single sign-on (SSO).

Powering productivity



75%

of employees who use a password manager say this makes it easier to be productive.

70%

of employees who use single sign-on say this makes it easier to be productive.

55%

of employees who use biometrics say this makes it easier to be productive.

Trusted tools

Among employees, two-factor authentication or multi-factor authentication are the most trusted security measures to keep accounts safe **(65%)**,

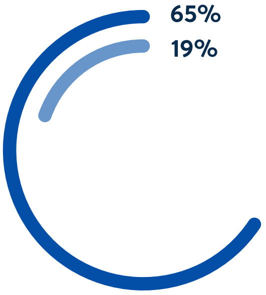
followed by biometrics **(35%)**,

and automated, forced password resets **(32%).**

Mythbusting: complexity ≠ security

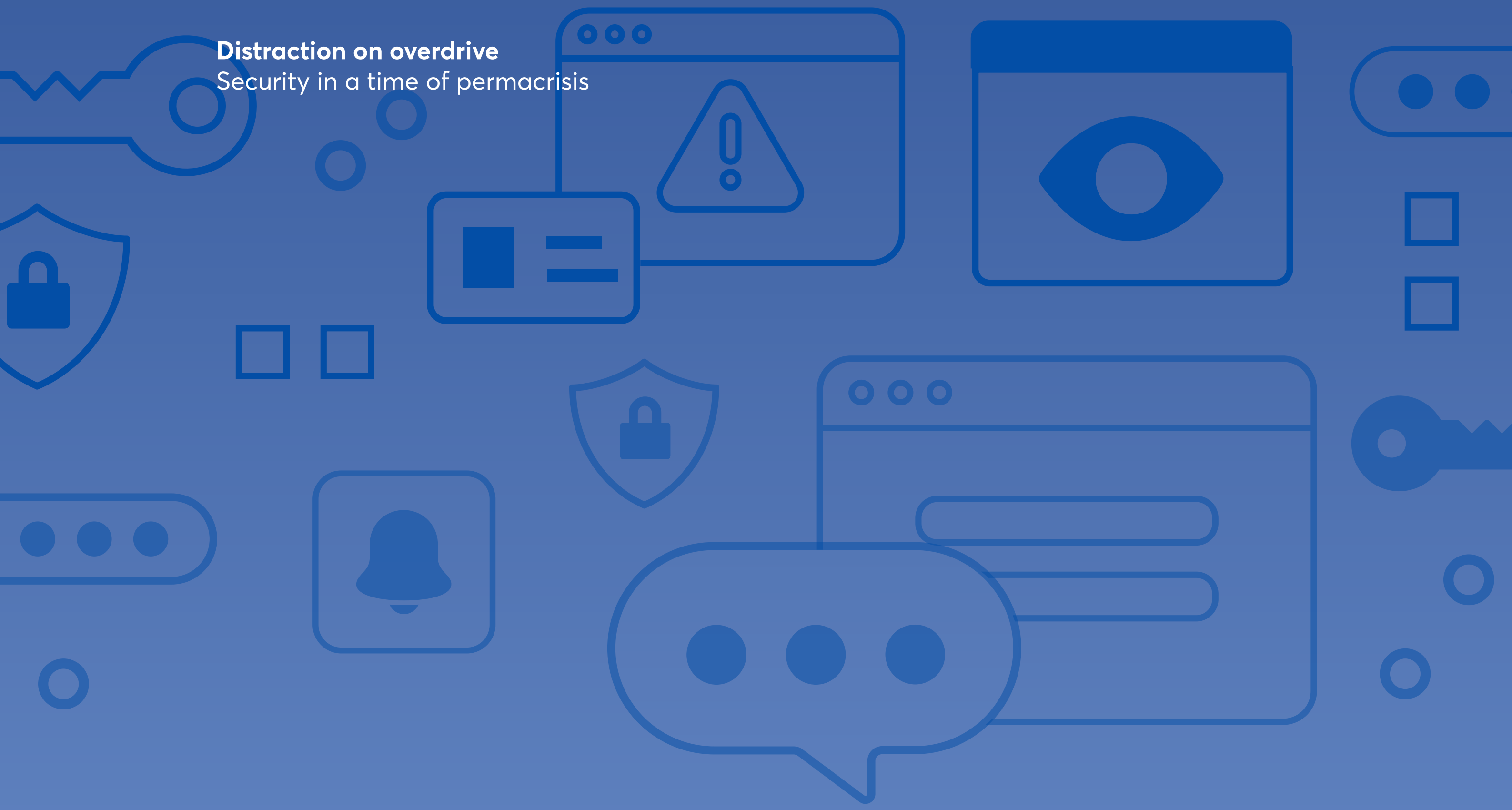
Our survey underscores the extent to which people continue to erroneously equate effort with security.

Our data shows that **employees are three times as likely** to trust two-factor or multi-factor authentication, which involve multiple steps, as they are to trust single sign-on – which involves the use of a single password to access multiple accounts and is notably easier to use **(65% vs. 19%).**



- ● **65% of workers** trust two-factor or multi-factor authentication to keep their accounts and information safe.
- ● **19% of workers** trust single sign-on to keep their accounts and information safe.

While opinions can vary, both 2FA/MFA and SSO are considered valuable layers in the security stack. The wide disparity in survey respondents' perceptions, therefore, reflects that many users remain unconvinced that seamless, human-centric solutions can also be trustworthy and secure.



03

Security slippage

While we've seen notable security improvements in recent years, there's much that needs to be done. Poor password practices persist, even as employees are increasingly aware of rising cyberthreats.

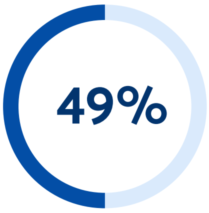
Half of employees (50%) say the biggest security threat their company faces is the prospect of employees falling for scams or phishing attempts, 41% cite external threats from bad actors, and 36% cite employees not following security rules. Nearly three-quarters of employees (72%) say they've received spam or been targeted by a phishing attack in the past year.

Password reuse

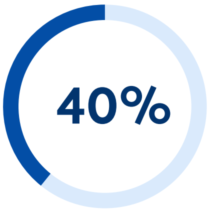
One in three employees (34%) reuse passwords despite knowing the risk.

Senior security snafus

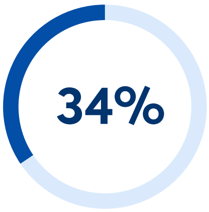
Poor password hygiene is notably worse among senior leadership, with directors and above more likely than individual contributors to use personal identifiers when creating passwords.



of employees at the level of director and above use personal identifiers in their passwords.



of managers/team leads use personal identifiers in their passwords.



of individual contributors use personal identifiers in their passwords.

Unclear consequences

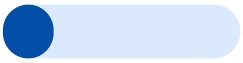
40%

of workers say bad security habits aren't punished at all – or they don't know what the consequences are.

70%

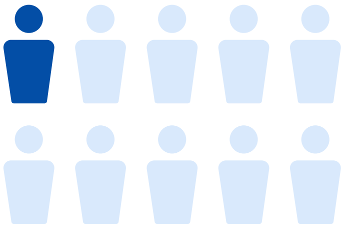
of workers don't know of anyone who has been reprimanded for improper use of a company computer or device.

15%

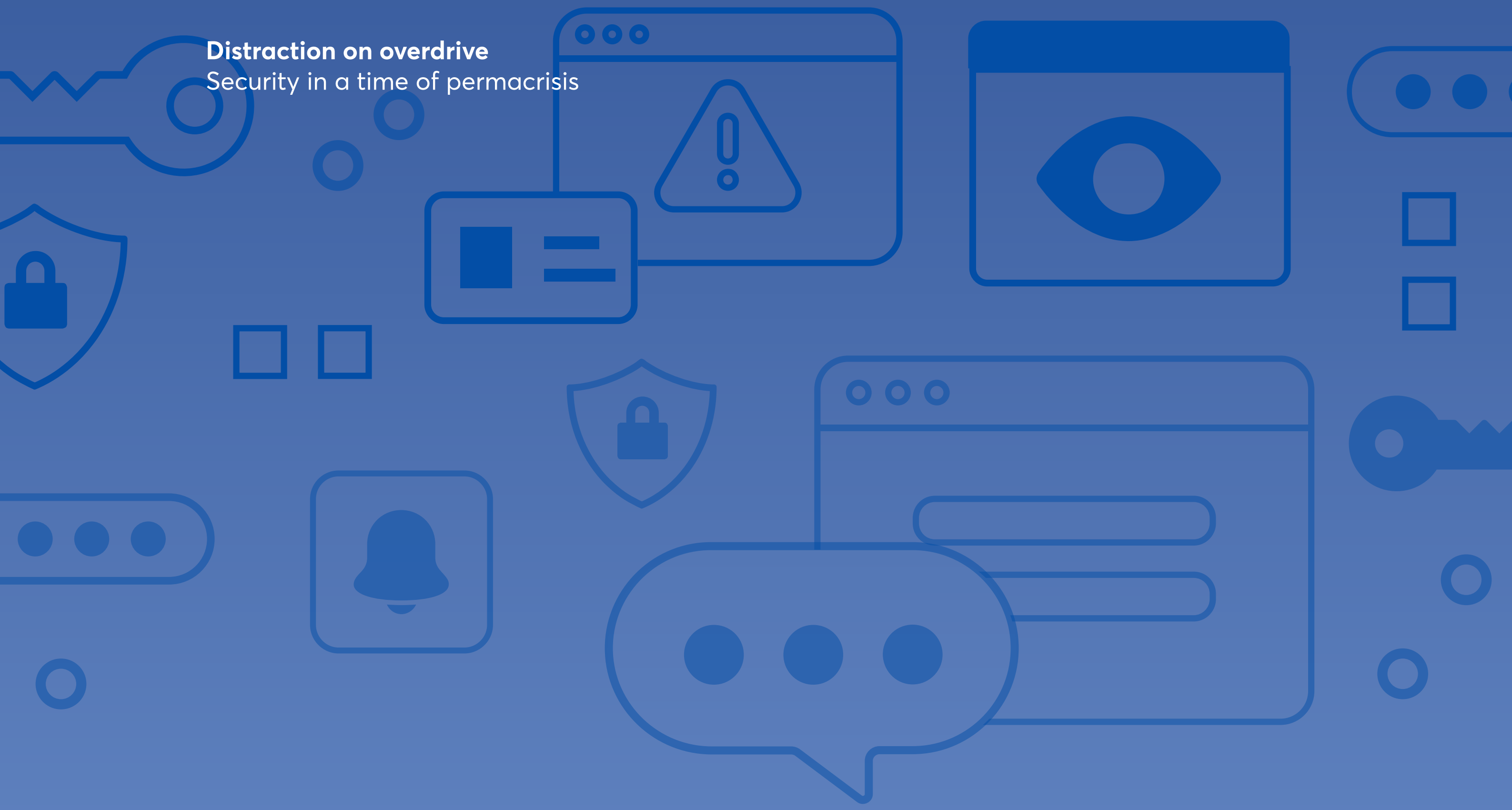


of workers are concerned about the possibility of being reprimanded for poor security habits, while **nearly half (47%)** say they aren't worried at all.

Blurring boundaries



One in 10 employees (10%) have used their work computers or devices for a side gig or another job.



04

Distraction escalation in tech

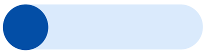
Among tech, IT, and telecom industry workers, the tendency toward distraction is more pronounced. Employees in these industries are nearly twice as likely as those in non-tech industries to say that distractions from world events make it hard to care about their jobs – and they are more than three times as likely to do only the bare minimum around security.

Domino effect

46%

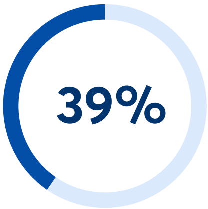
of tech industry employees say that distractions from world events make it hard to care about their jobs.

23%

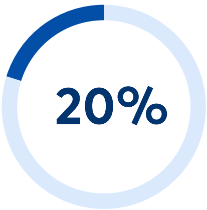


of employees in other industries say that distractions from world events make it hard to care about their jobs.

Distraction dependency



of tech industry workers say their coworkers are less productive at work because they're distracted by world events.



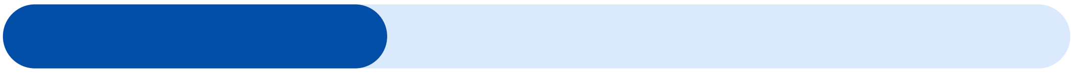
of workers in other industries say their coworkers are less productive at work because they're distracted by world events.

Security inconsistencies abound

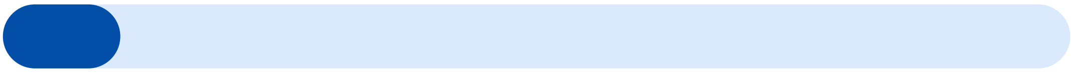
Nearly half of tech industry workers (49%) say they're more careful about online security at home than they are at work.

Phoning it in with workplace security

36% **of tech industry employees** say they do only the bare minimum when it comes to security at work.



11% **of employees in other industries** say they do only the bare minimum when it comes to security at work.



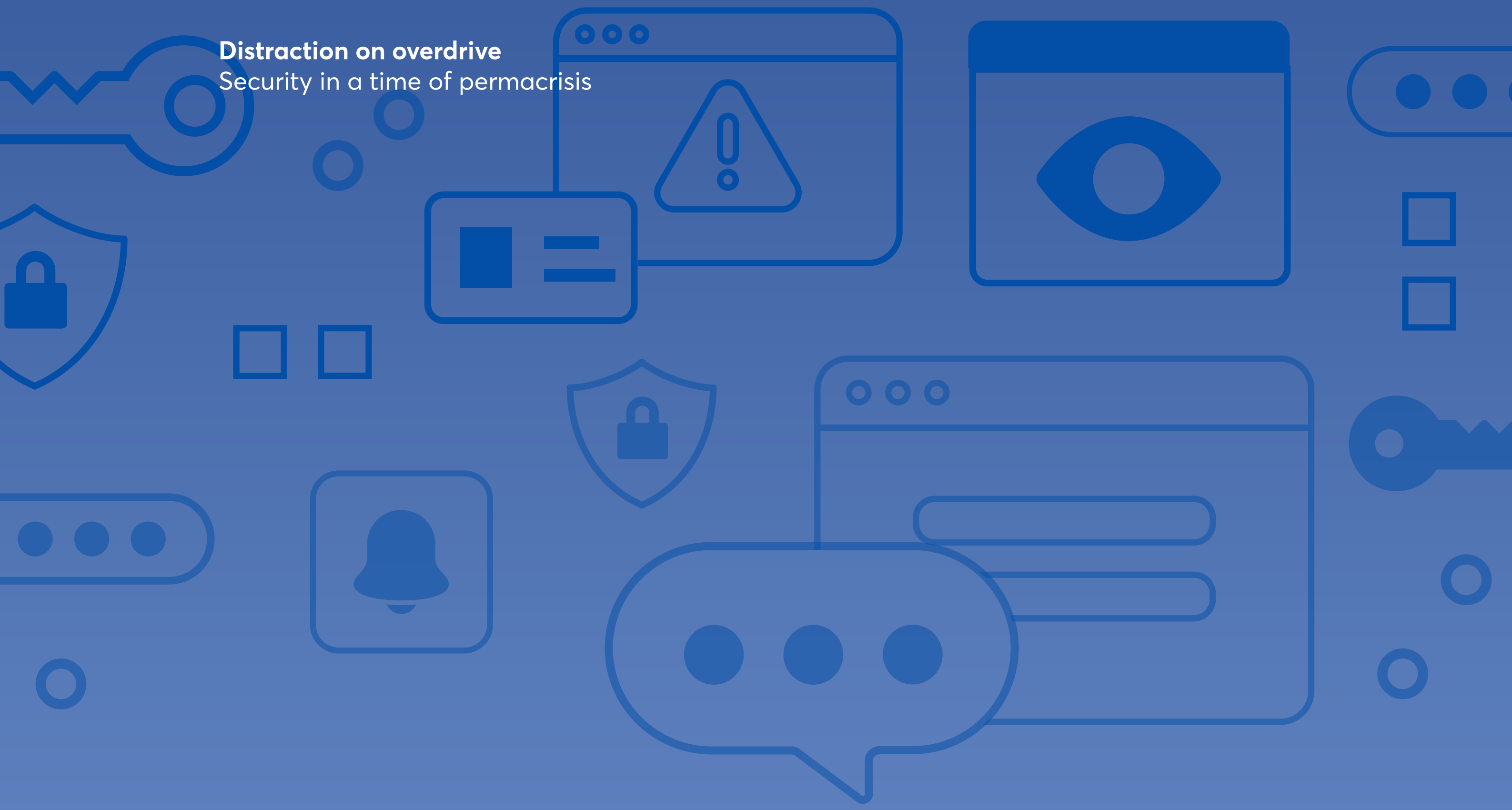
Same device, different gig

19%

of workers in the tech industry have used their work computers or devices for a side gig or another job.

9%

of workers in other industries have used their work computers or devices for a side gig or another job.



05

A look ahead:

In an age of uncertainty, security systems can save the day

Permacrisis, and widespread distractions, may be here to stay. Because we know that security takes a backseat when people get distracted, it's important to deploy easy-to-use, human-centric security solutions – ones that adapt to how we work and that provide protection without adding friction.

For a glimpse into the future, we asked experts in cybersecurity and human-centric solutions what they see as the most urgent threats, the most promising solutions, and the most critical imperatives for companies seeking to protect their valuable assets and reputations in 2023.

> “The research shows that 30% of folks are already using biometrics, and we'll continue to see the appetite for passwordless increase among both consumers and businesses in 2023. As big tech and other industry leaders put more muscle behind passwordless and passkeys, there needs to be a simultaneous push on the education front to show people that the simple thing can be the most secure thing. It won't happen with the flip of a switch – but by working together to achieve a frictionless authentication process that's secure, we'll be doing everyone a favor.”

Andrew Shikiar
Executive Director, FIDO Alliance

> “While we hope the worst of the pandemic is behind us, world events continue to unsettle and distract employees. Mishaps are inevitable – it's not a case of if world distractions will make employees more vulnerable to human error, it's a matter of when. That's why it's vital that businesses take security off people's plates by implementing seamless systems that eliminate the need for human action. The easier we can make security, the less it will become yet another distraction. It's a win-win for employees and companies.”

Jeff Shiner
CEO, 1Password

> Every crisis creates an opportunity for criminals to exploit victims via social engineering as they take advantage of psychological weaknesses. Many of the traditional human vulnerabilities are at greater risk in a time of permacrisis; curiosity, the power of authority figures, manufactured urgency, greed, and other weaknesses will continue to be used to the attackers' advantage. As the level of sophistication increases, even the most tech-savvy of us can fall victim to a well-crafted attack, and it's our job in the industry to build more resilient systems and tools."

Troy Hunt
Founder, Have I Been Pwned

> Moving forward, it's incumbent upon cybersecurity providers, and organizations across industries, to create and adopt solutions that are human-centric and, ideally, automated – solutions that are intuitive, seamless, and user-friendly. As workers come to trust these new systems, companies can continue to protect themselves despite what distractions lie ahead."

Dr. Karen Renaud
Chancellor's Fellow and faculty member, University of Strathclyde, Glasgow, Scotland
Expert in human-centric security

> The main problem with passwords is simple and straightforward: it's hard for people to create (and remember) strong ones. As our own neuroscience researchers understand well, the human brain is not built for this kind of activity. By automating password security, we can keep our systems safe while freeing up our valuable brain trust to pursue higher-order thinking. The beauty of automated solutions is that they work even when people have global crises or other pressing matters on their minds."

Nick Tripp
Senior Manager, IT Security Office, Duke University

2022 STATE OF ACCESS REPORT

Distraction on overdrive

Security in a time of permacrisis

Methodology

1Password conducted this research using an online survey prepared by Method Research and distributed by Dynata among n=2,000 adults ages 18+ in North America (n=1,400 U.S. + n=600 Canada) who work full-time primarily at a computer. The sample consisted of respondents from any department and title within their company. The sample was equally split between gender groups with a balanced spread across age groups. Data was collected from October 14 to October 24, 2022.

About 1Password

1Password's human-centric approach to security keeps people safe, at work and at home. Our solution is built from the ground up to enable anyone – no matter the level of technical proficiency – to navigate the digital world without fear or friction. The company's award-winning security platform is reshaping the future of authentication and is trusted by over 100,000 businesses, including IBM, Slack, Snowflake, Shopify, and Under Armour. 1Password protects the most sensitive information of millions of individuals and families across the globe, helping consumers and businesses get more done in less time – with security and privacy as a given. Learn more at 1Password.com.