

# Unlocking the Login Challenge

How Login Fatigue Compromises Employee Productivity, Security and Mental Health

1Passw@rd



# Executive summary

Logging in: It's the most elemental aspect of work, the digital equivalent of unlocking the office door. But accessing the essential software we need to do our jobs is still too complicated, disruptive and downright annoying—leaving employees frustrated and putting essential data and information at risk.

To better understand workers' attitudes, behaviors, beliefs and pain points around logging in, 1Password surveyed 2,000 North American adults who work full-time primarily at a computer. Our survey, conducted in June 2022, found that complex, multi-step login processes are frustrating workers, wasting their time, hindering productivity and prompting them to give up entirely—abandoning important work-related tasks simply because logging in was too cumbersome. To circumvent the hassle of logging in, we found, employees often seek risky workarounds like borrowing a colleague's password.

More broadly, our survey found that there are widespread misunderstandings around what constitutes a safe and secure login process. While the majority of employees (89%) think they generally follow their employer's login rules, there is a great deal of confusion around what "secure" looks like in 2022.

The average security breach costs a company more than \$4 million, according to the latest *Cost of a Data Breach Report* from IBM and the Ponemon Institute. While many companies invest heavily in security apps and software, Verizon's 2022 *Data Breach Investigations Report* reveals that 82% of breaches involve a human element. Our own research indicates that while employees are terrified of

being hacked, they grossly underestimate the value of the information that they have access to, and could leak through such a breach. And they are egregiously misguided about what secure login practices look like.

Taken together, these misunderstandings and frustrations leave companies vulnerable, rob them of productivity and unnecessarily deplete employees' energy at a time of widespread burnout.

## What is single sign-on?

Single sign-on (SSO) allows employees to log into a range of accounts with one strongly vetted identity, rather than having to create unique usernames and passwords for each site and service they access. By consolidating the number of credentials employees need to keep track of, SSO dramatically reduces companies "attack surface," or the number of entry points that IT needs to secure. SSO also allows organizations to enforce blanket security protocols like multi-factor authentication. On the consumer side, SSO allows users to access a broad range of accounts and websites by signing in through third-party accounts like Google, Apple or Facebook. Because these personal accounts are outside the purview of companies' IT departments, they are not considered secure when signing in for work purposes.



*When it comes to security, organizations say, 'Follow these guidelines,' then they add more rules every time something goes wrong. But every new rule creates new friction for employees, which acts as a bar on full productivity. This research confirms the serious toll that this friction is taking on employee well-being and, as a result, on organizations' security. Security has become such an onerous and arduous task that people don't even want to log in—that's a significant problem.*



### Dr. Karen Renaud

Chancellor's Fellow and Faculty Member  
University of Strathclyde, Glasgow, Scotland | Expert in Human-Centric Security

# Key findings

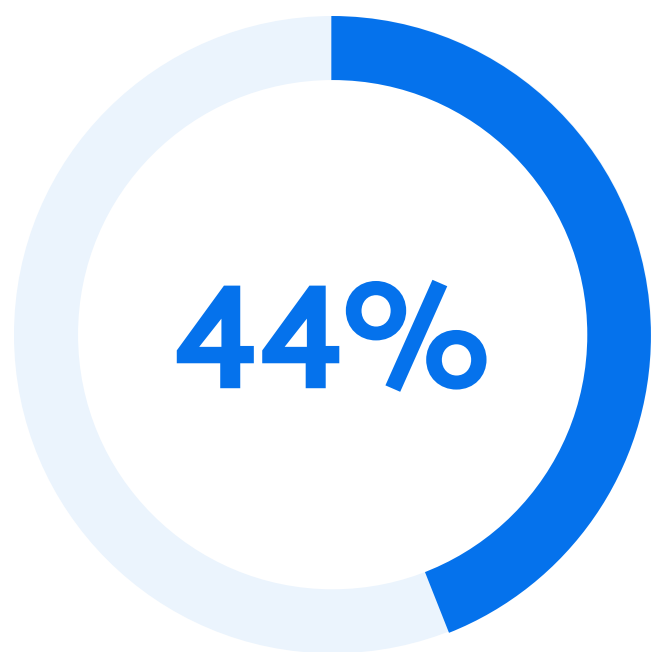
Today's work login processes aren't just frustrating—they're slashing productivity and putting companies at risk.

Fatigue and frustration	44%	Nearly half of employees say that the process of logging in and out at work harms their mood or reduces productivity.
Falling behind on day one	37%	More than a third of employees say that the onboarding process at their current job was time-consuming, confusing or challenging when it came to logging into work-related accounts.
Incomplete work product	26%	More than a quarter of employees have given up on doing something at work to avoid the hassle of logging in.
Negligent insider threats	38%	More than a third of employees have procrastinated, delegated or skipped setting up new work security apps because of burdensome login processes.
Missing meetings	62%	Nearly two-thirds of employees miss parts of meetings on a regular basis because of login issues.
Blurring work and home	45%	Nearly half of employees use personal accounts such as email or Facebook for single sign-on at work. This leaves companies vulnerable, as they cannot monitor personal accounts for security risks.
Major confusion abounds	27%	More than a quarter of employees think there's no difference between single sign-on (which boosts security by limiting the entry points that need to be secured) and reusing passwords (which increases exposure to hackers).
Fear of hacking	61%	Nearly two-thirds of employees think they're more likely to be hacked now than they were a year ago because of their increased online presence.

# The secret state of login agony

Logging in is an ongoing source of frustration across workplaces—spurring employees to seek risky workarounds and causing them to abandon certain work-related tasks altogether.

## Bad moods



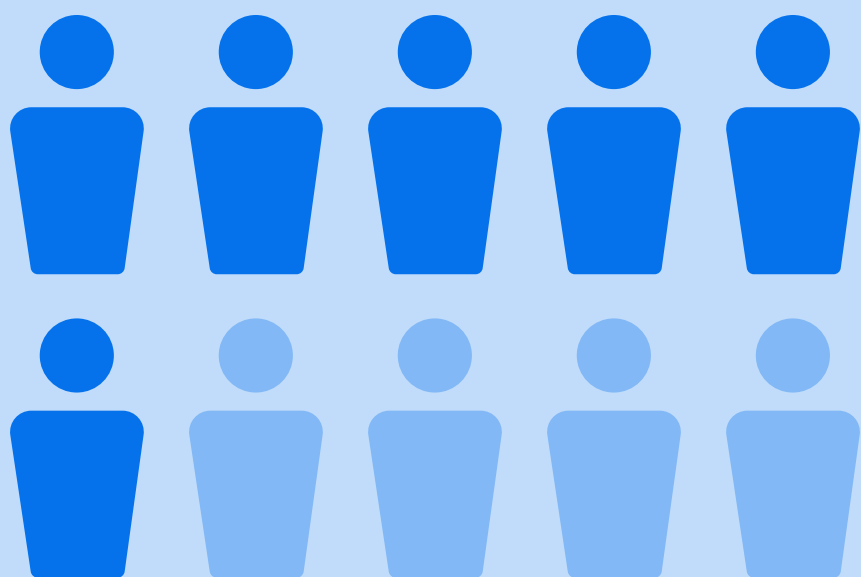
Nearly half of employees (44%) say that the process of logging in and out at work harms their mood or reduces their productivity.

## Outsized impact on Gen Z

Gen Z	59%
Millennials	49%
Gen X	47%
Boomers	33%

Gen Z respondents were **nearly twice as likely** as Boomers to say the process of logging in and out at work negatively impacts their mood or productivity (59% vs. 33%).

## Disrupted meetings



62% of employees miss parts of meetings on a regular basis because of login issues.



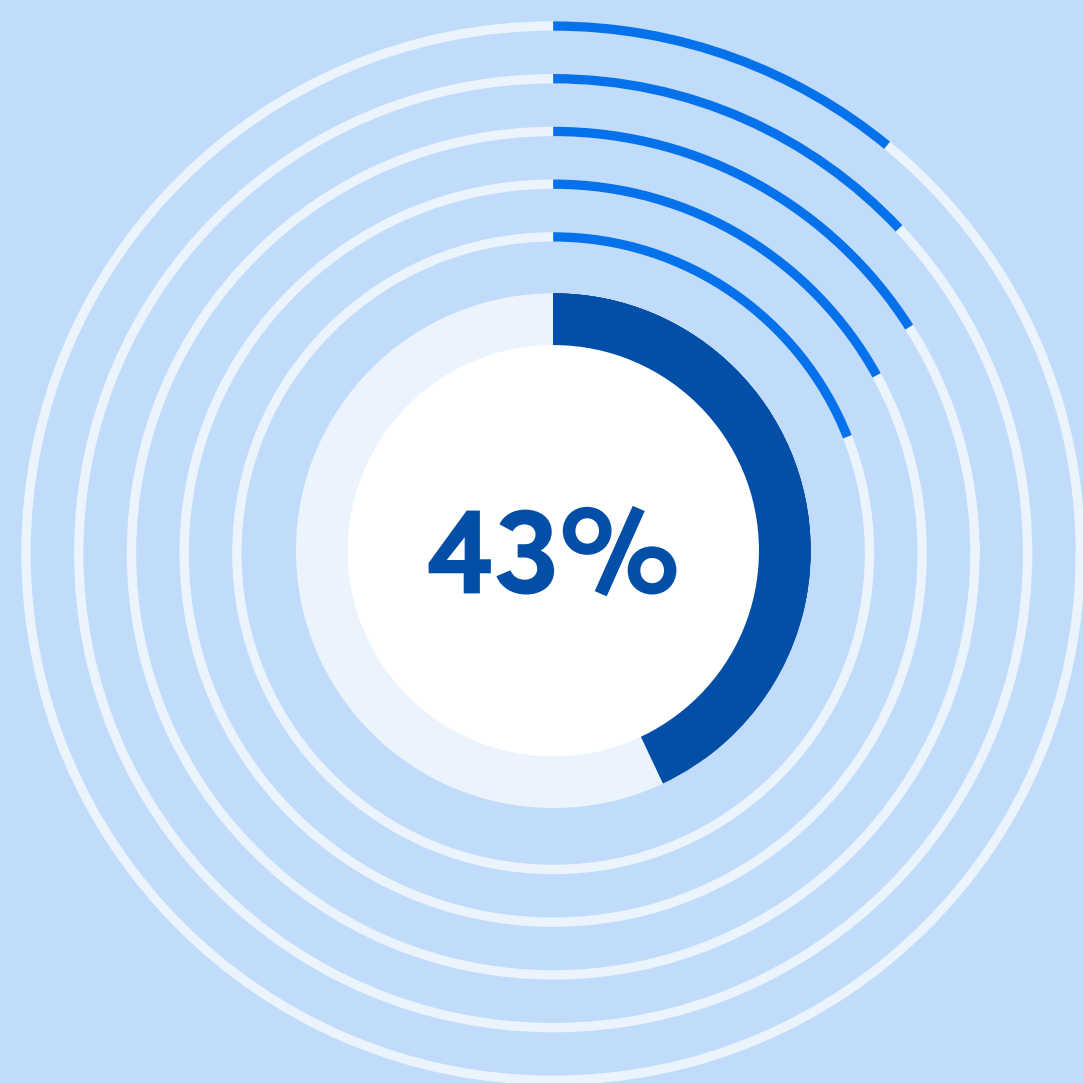
Each year, login issues cause employees to **miss over 10 hours** worth of meetings, on average.



# The secret state of login agony **continued**

## Incomplete work

**43% of employees** have figured out a workaround or given up on a task at work due to login challenges.



- 11%** **offloaded a task** to a colleague so they didn't have to deal with logging in.
- 13%** **abandoned a work task** so they didn't have to deal with logging in.
- 16%** **shared a login** or used somebody else's login to access an account or app at work.
- 17%** **figured out a workaround** to complete a task so they wouldn't have to log in.
- 19%** **gave up** on logging into a non-critical work app because it was taking too long.

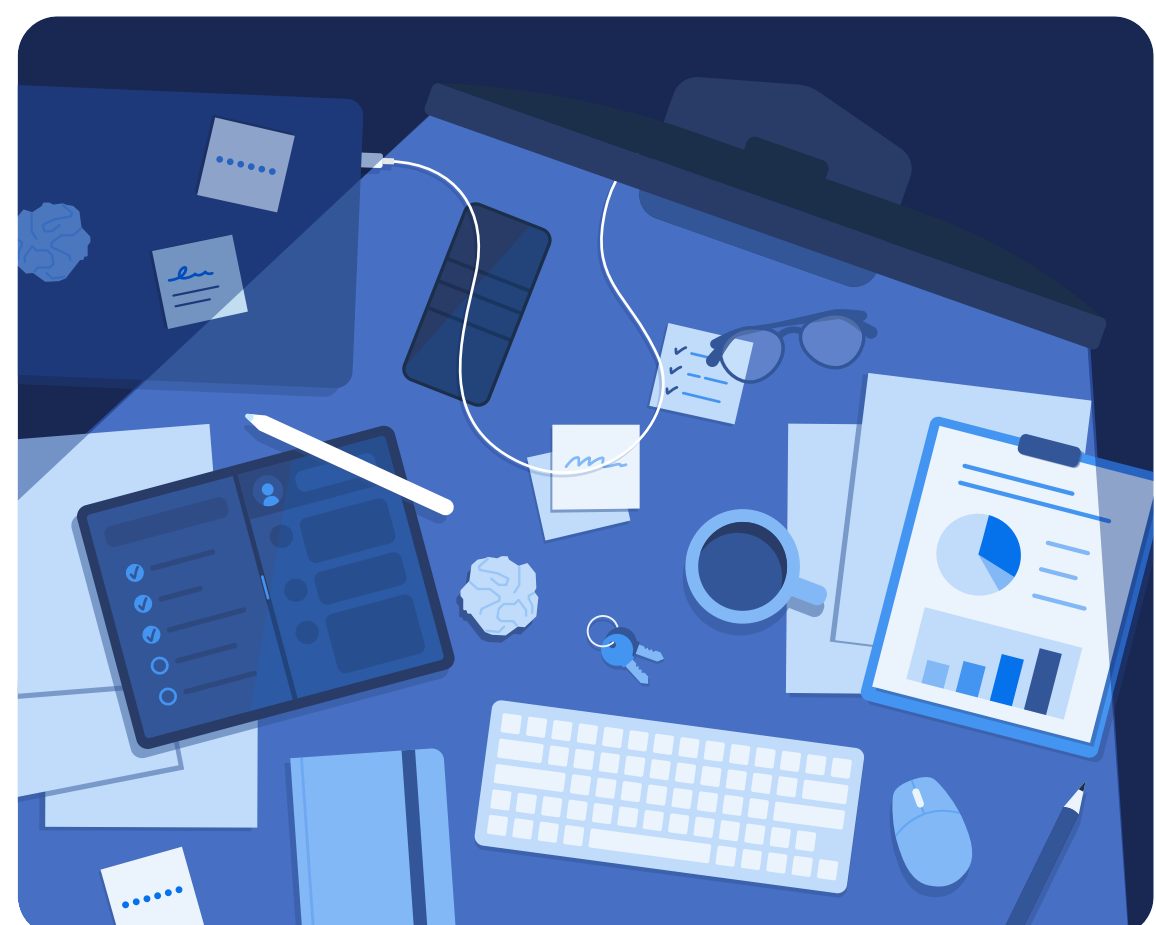
## Giving up on security

**Nearly 1 in 3 workers (30%)** say the process of logging in and out at work diminishes their view of their company's security policies or tech stack—making them care less about trying to maintain good security practices or embittering them towards certain apps and services.

## Blurring work-home boundaries

As a result of this headache, employees often take the path of least resistance by using personal logins to access work accounts.

**Nearly half of employees (45%)** use their personal email, LinkedIn, Facebook, or other personal account for a single sign-on at work. These accounts can't be properly managed under IT security policies and often circumvent IT management controls that keep companies safe. This leaves workers and their employers vulnerable.

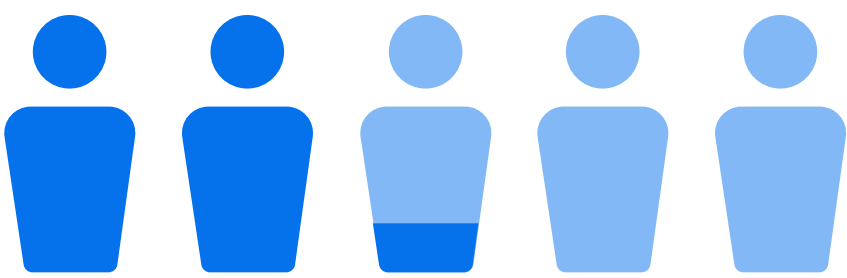


# Day one and already burned out

Cumbersome login processes affect employees' mental health from the moment they start their workdays.

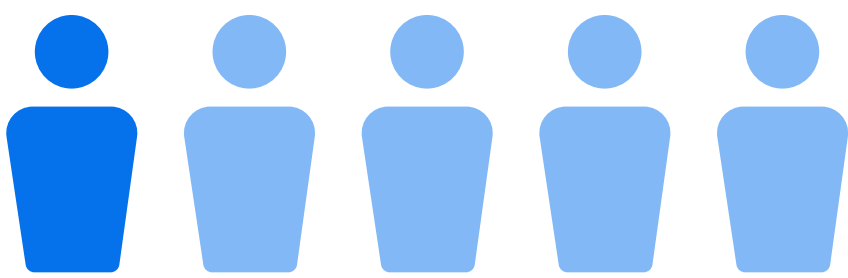
At a time when companies are struggling to attract, onboard and retain talent, login challenges are stressing out workers from day one—diminishing their view of their employers before they even get going. While companies are responding to widespread burnout and mounting mental health concerns by ramping up employee benefits, some employees are foregoing these critical benefits simply because it's too arduous to log in.

## Login overload



**More than a third of employees (41%)** say having to remember multiple logins heightens their stress levels and strains their mental health.

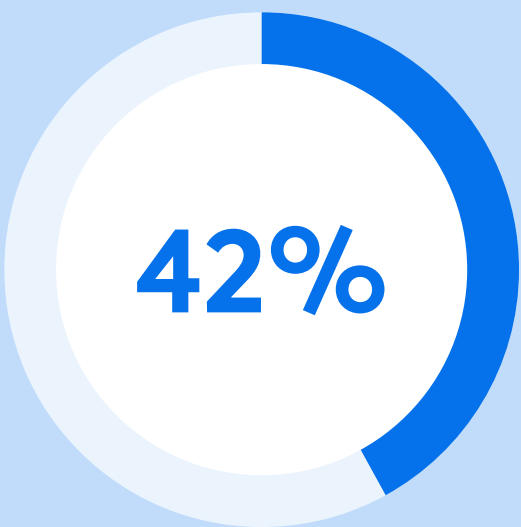
## Benefits breakdown



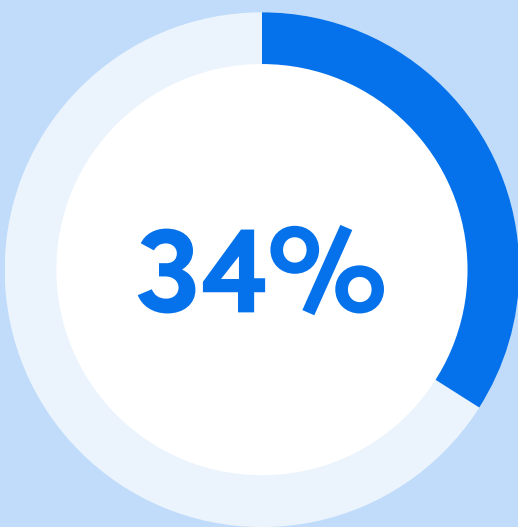
**1 in 5 workers (19%)** have entirely skipped open enrollment, requesting time off, free perks or access to discount marketplaces provided by their employer because it wasn't worth the challenge of logging in.

## Unwelcome and behind

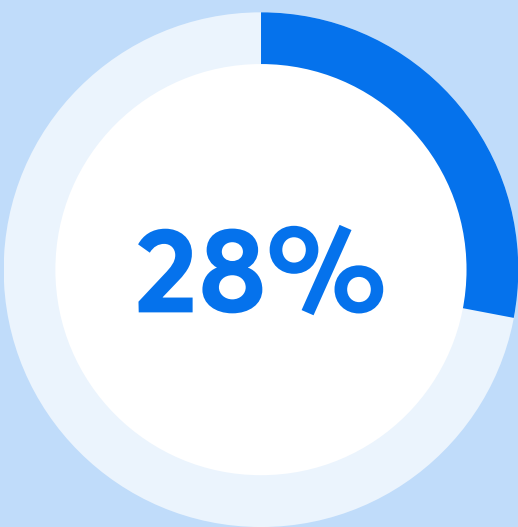
Logging in should be the simplest part of starting a new job. Instead, the process is leaving brand new team members feeling behind and unwelcome on day one. **Only 12% of employees** say that all of their logins were set up for them during their last onboarding experience. Those who did not have a quick and easy experience say they were left feeling:



overwhelmed and stressed



behind on work



frustrated and annoyed with their new company

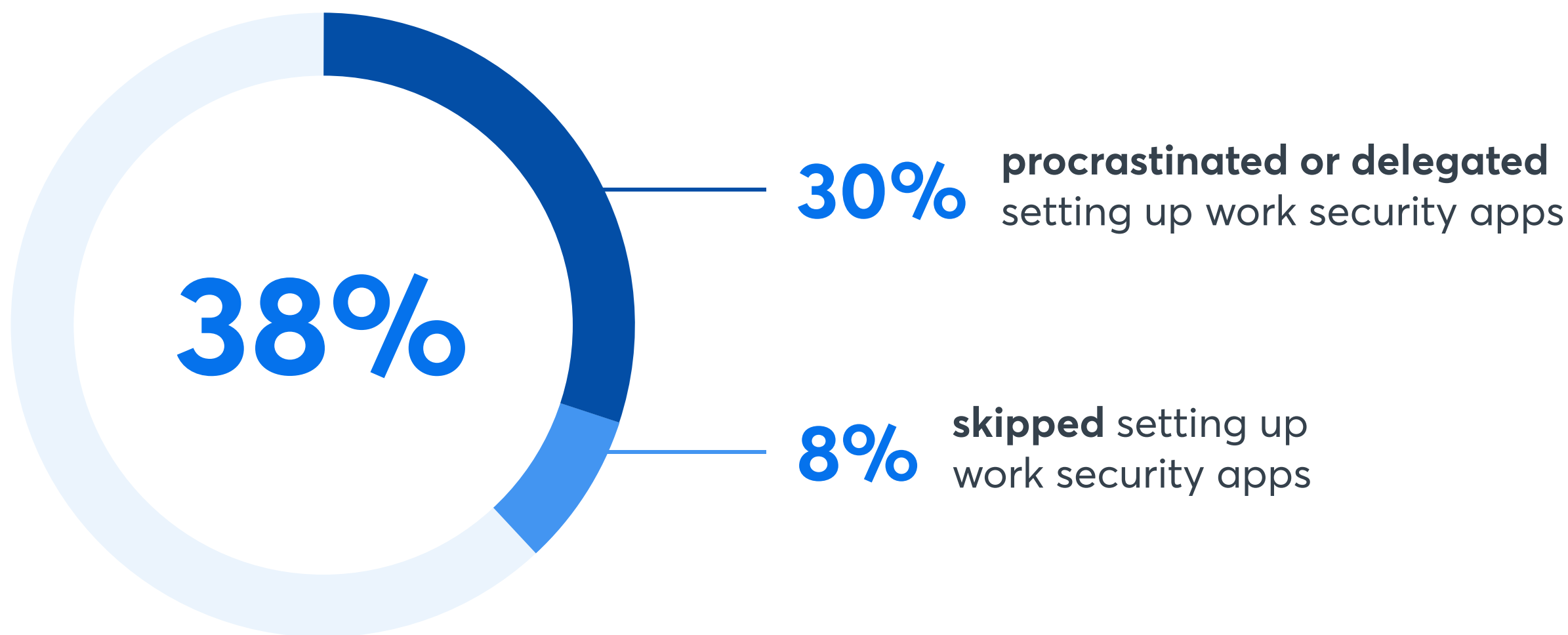


unwelcome

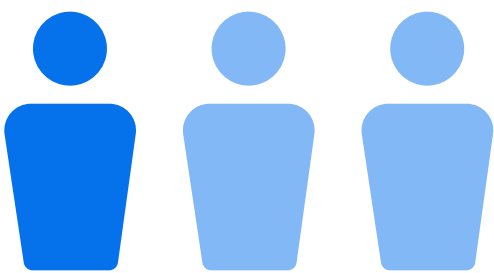
# Day one and already burned out continued

## Skipping out on security

Faced with multiple workplace apps to set up, many have procrastinated conducting the activity or have delegated it to a colleague. Incredibly, **nearly 2 in 5 workers (38%)** have procrastinated or delegated setting up even the most crucial of these—work security apps—or have skipped this activity altogether. This combination of uninstalled security apps and poor login practices leaves companies especially vulnerable.

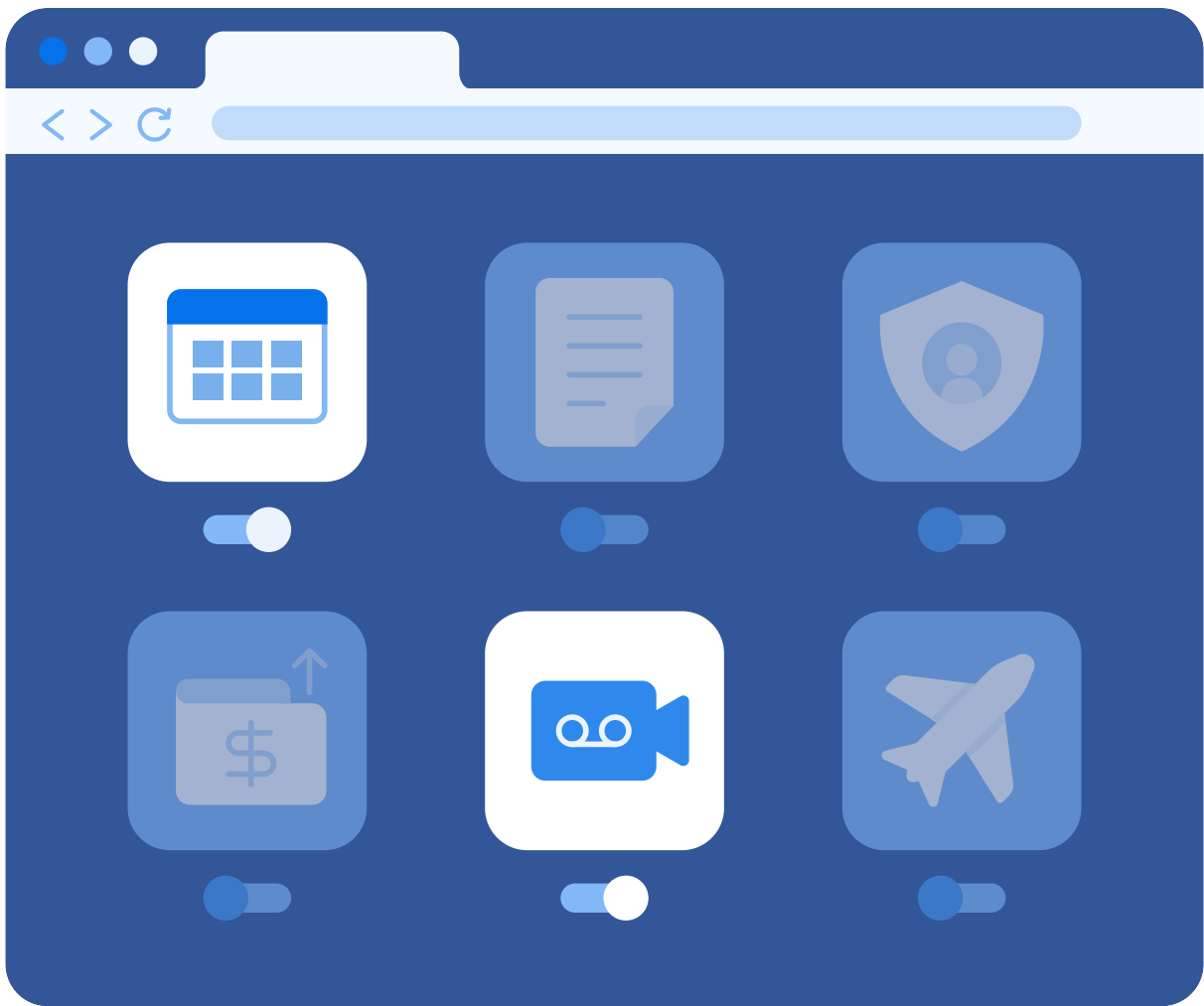


## Untapped tech tools



**1 in 3 employees (36%)** have procrastinated, delegated or skipped setting up new workplace accounts such as expense reporting software or travel accounts.

**1 in 3 employees (32%)** have procrastinated, delegated or skipped setting up paid video-conferencing software, hampering their participation in remote work.









# SS I Don't Know... time for a little mythbusting

As logging in has become more complicated and arduous, confusion over best practices has become widespread.

While **3 in 4 employees (75%)** say that using single sign-on (SSO) logins at work saves a lot of time and effort, many misunderstand how SSO works and what secure practices look like—and senior leaders are the most confused.

## Myth vs. Fact

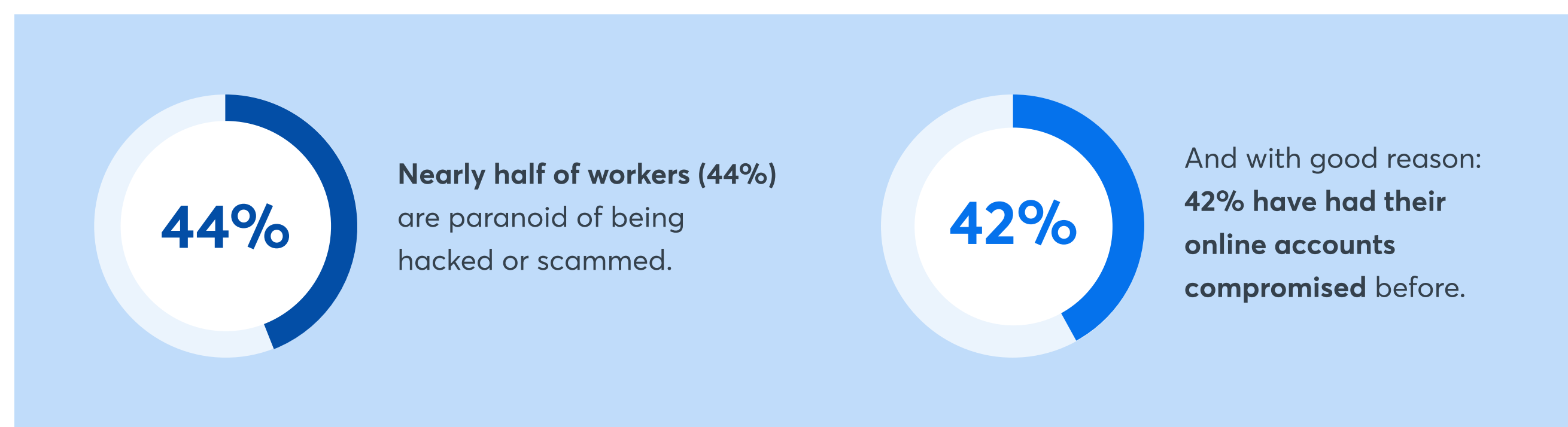
 <b>SSO is less secure</b>	 <p><b>Half of employees (50%)</b> believe that using SSO leaves a person more vulnerable to hacking, and 44% think SSO is less secure than traditional logins. In fact, by consolidating the number of credentials employees need to keep track of, SSO reduces the number of entry points that IT needs to secure. <b>In one analogy, SSO is akin to gathering all of your treasured logins into a castle, then building an alligator-filled moat around it.</b></p>
 <b>Effort equals security</b>	 <p><b>Nearly half of employees (48%)</b> think the more steps a login process has, the more secure it is—conflating effort with security. <b>But complexity does not necessarily translate into better security.</b> Human-centric security solutions are specifically designed to make it as easy as possible to securely log into online services. With SSO, users delegate identity verification to the SSO provider, and IT can focus on strengthening security at a single attack point.</p>
 <b>Senior leaders will set the tone on security</b>	 <p><b>Executives are actually performing worse on security than their lower-ranking peers.</b> Our research reveals that <b>41% of leaders at the level of vice president and above</b> say there's no difference between single sign-on and reusing the same password across multiple platforms, compared to 29% of team leads/managers and 21% of individual contributors.</p>



# Well-founded paranoia

Employees are painfully aware of the rise of cyberattacks and are terrified of being hacked or scammed, particularly as the amount of time people spend online has skyrocketed since the COVID-19 pandemic began. But workers are at a loss in terms of knowing what to do about it—expressing confusion around what safe login practices look like and how they can mitigate the risks.

## Helpless against hackers



## Feeling more vulnerable in 2022

### Increased online presence

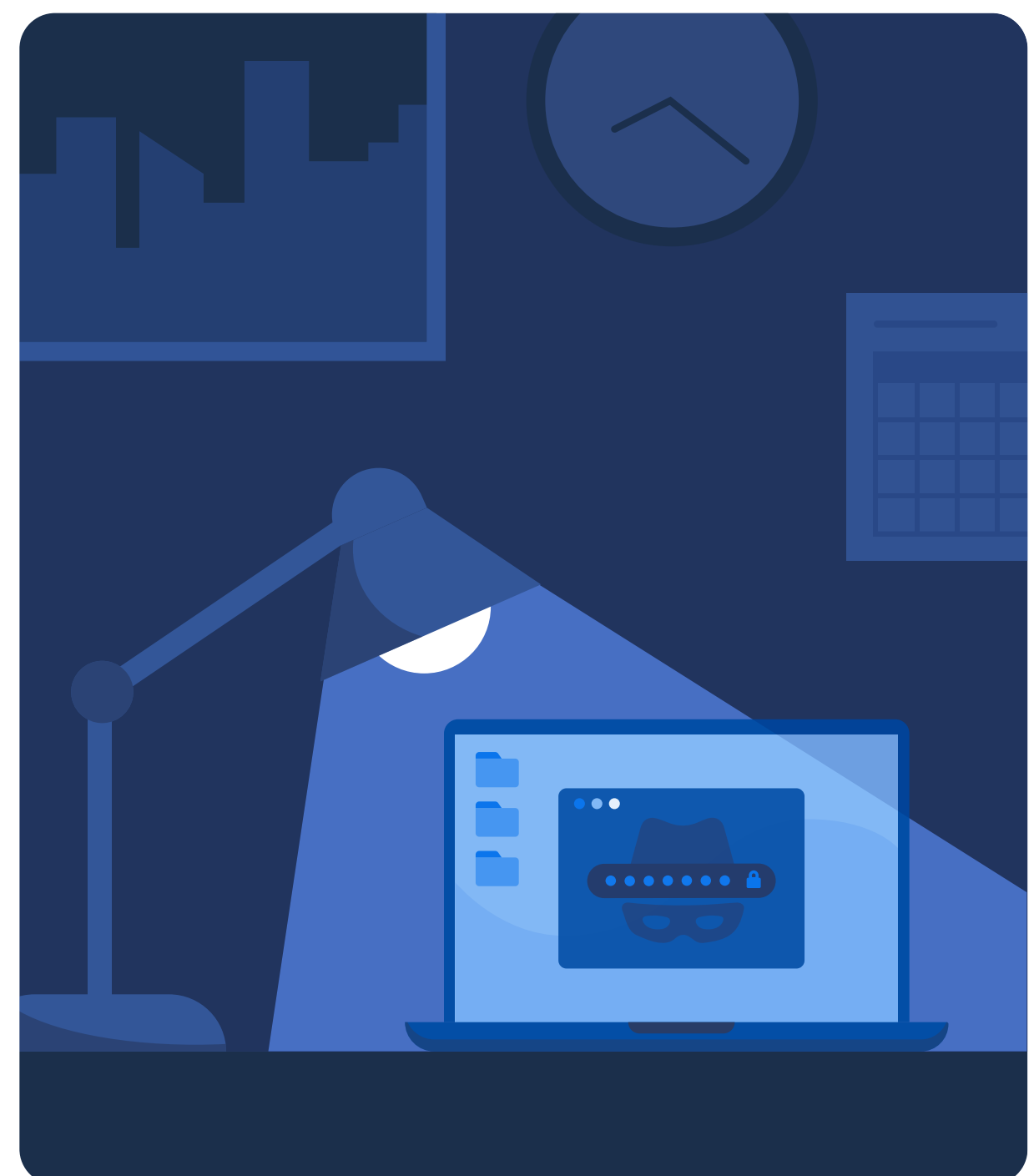
**Nearly two-thirds of workers (61%)** think they're more likely to be hacked now than they were a year ago because of their increased online presence, including online shopping and games.

### Password security habits

**1 in 3 workers (36%)** think they're more likely to be hacked now than they were a year ago because of their password security habits, such as sharing account access with friends and family and reusing the same password across multiple accounts.

### Global conflict

**1 in 3 employees (37%)** think they're more likely to be hacked now than they were a year ago because of global conflict. 15% blame the war in Ukraine for a higher likelihood they'll be hacked.



# Today's login fatigue makes the case for human-centric security

Companies implement complex logins for good reason: Today's cyberattacks are more sophisticated than ever.

With more companies operating larger parts of their business online—everything from restaurants to retailers to real estate agencies—any breach can directly harm operations, not to mention customer trust and brand reputation.

It's with great irony, though, that the very tools meant to protect company information and infrastructure are now putting companies at risk. Even as companies strive to make the online experience easier and more intuitive for customers, security is going the opposite way—interrupting workflows, sparking mass confusion and causing stress when employees just want to do their jobs.

Today's stringent login protections usually put the onus on employees, saddling them with lengthy and seemingly ever-changing password requirements, disruptive multiple

authentication channels and an array of third-party apps and services. While these are intended to keep employees and companies secure, everyone agrees they're often a headache—and heartache—to manage. It's no wonder that many employees are trying to get by with the absolute minimum in security, if not ignoring it altogether. In a world that caters to users, security software seems to be the single area where apps are actually getting harder to use.

That's a serious problem. Beyond putting companies at risk of attack, today's state of affairs calls into question whether employers are living up to their stated concern for employees' mental health. Good intentions have led to a situation where security is actively undermining businesses and the employees who build them. This research confirms that it's long past time for businesses to step back and redesign their approach, putting the same care into making online services easy to use and human-centric for their employees as they do for their customers.



“Humans minimize effort—not because we're lazy, but because we wouldn't be able to get through the day without automating many of the things that we have to do. Single sign-on eliminates as much friction as possible from the login process, making security second-nature and turning our employees into our most valuable assets, security-wise. The best security solutions are those that embrace the humanity of our employees. That's what human-centric security is all about.”

## Dr. Karen Renaud

Chancellor's Fellow and Faculty Member  
University of Strathclyde, Glasgow, Scotland | Expert in Human-Centric Security

### Methodology

1Password conducted this research using an online survey prepared by [Method Research](#) and distributed by [Lucid](#) among n=2,000 adults 18+ who are full-time employees at a company with 250+ employees and primarily use a computer for work. The sample consisted of n=1,500 U.S. respondents and n=500 Canadian respondents, with an even split between gender groups. Data was collected from June 7 to June 21, 2022.