1Password

EBOOK

Why you need a password manager now

If you're not using a password manager for work, you're encouraging poor security habits.

Suppose you already know that you need a password manager for your business. Weak credentials continue to be the primary access vector for bad actors, with 22% of breaches related to credential abuse and 88% of basic web application attacks tied to stolen credentials. The cost of a data breach rose to $4.9 million in 2024, continuing to increase year over year. And you know that your employees are juggling dozens or even hundreds of accounts … far too many to safely keep track of themselves.

Let's say you know all that, but rolling out a password manager isn't at the top of your priority list at the moment.

But here's the thing: the longer you wait, the harder it will be to undo the damage wrought by developing bad organizational security habits.

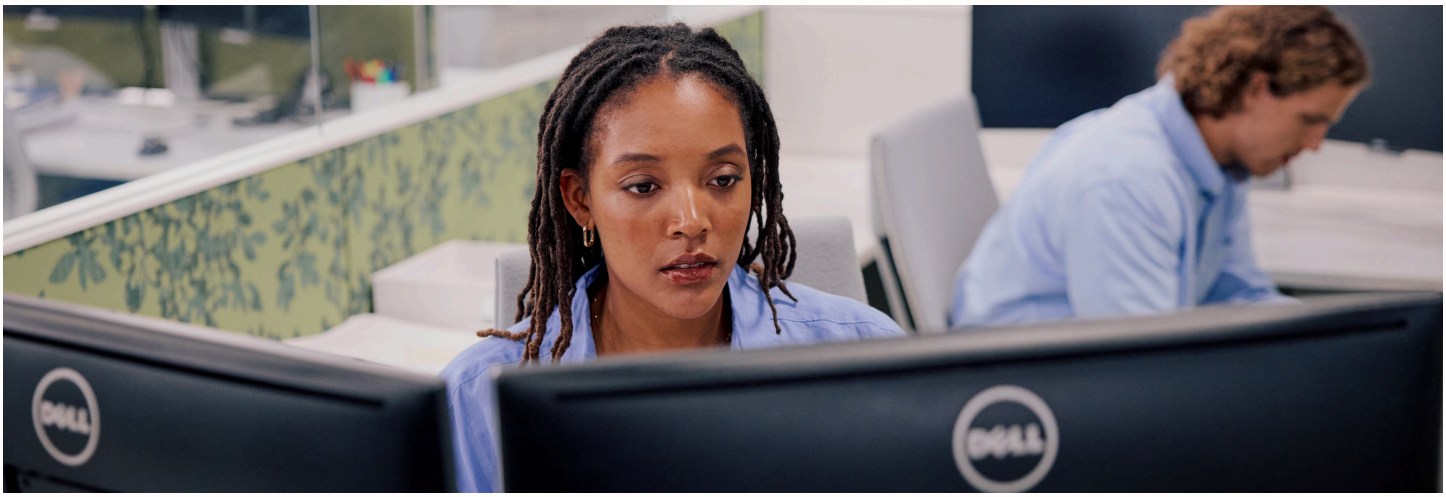
There are so many accounts you don’t know about

You can’t throw a rock on the internet without it bouncing off two or three new productivity tools and accounts used. They help us work more efficiently – but if workers are signing up for them on their own, they create an untraceable trail of accounts that IT doesn’t know about, a phenomenon known as shadow IT. And if IT doesn’t know about them, they can’t protect those accounts.

2.6% *of workers who use a unique password for each account*

It’s not a small problem. According to 1Password research, 63 percent of adults who work in an office with an IT department and use a computer for work have created at least one account in the past 12 months that IT doesn’t know about.

Of those, just 2.6 percent said they use a unique password for each account. And every time Jim creates an Airtable for his email campaigns, or Jennifer runs a legal document through a Grammarly check, they’re handing potentially sensitive data over to third parties with zero oversight.



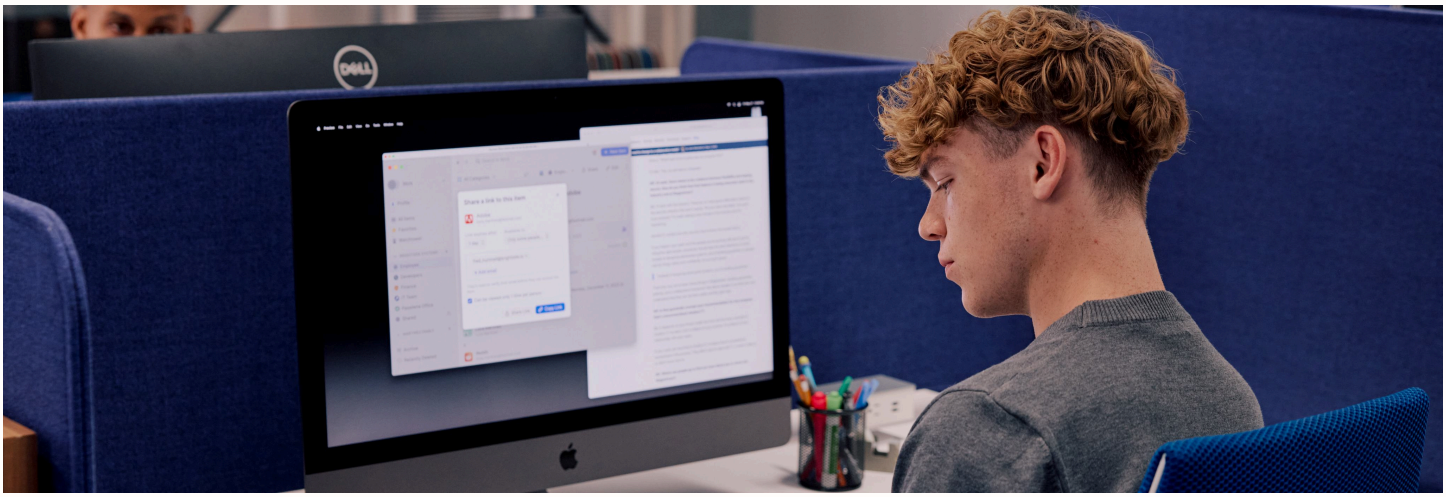
Your people are burned out, & that's a security risk

In our State of Secure Access Report, 1Password looked into the state of burnout among office workers and found that an astounding 80 percent of them reported feelings of burnout. Security professionals reported even higher burnout levels at 84 percent.

That's no surprise, given the stress we've all been under for the past two years or so. Less obvious is the effect of pervasive levels of burnout on your business risk.

Burned-out employees are three times as likely to claim that security policies "aren't worth the hassle." Even more alarming, significantly burned-out security professionals are more than twice as likely to say the same. And burned-out security professionals are twice as likely to say that, because of burnout, they're "completely checked out" at work and are "doing the bare minimum."

If everyone's cutting corners, the security protocols that you already have in place probably aren't providing the level of protection you think they are.



We’re forcing workers to choose between security & productivity

Of course, no one creates these accounts with the intention of putting their company at risk. We do so because we have jobs to do, and these apps help us do them better, faster.

Historically, therein lies the rub: You can be productive, or you can do things securely … but you can’t do both.

According to a report from security software platform ShiftLeft, 96 percent of developers believe that disconnected security and development workflows inhibit their productivity.

It’s not a giant leap to assume that the same holds true for office workers in general.

When we’re constantly forced to choose between security and productivity, many of us sometimes let our guards down a bit in the name of getting things done. Especially when we’re feeling burned out.

If you're not using a password manager, you're doubling down on bad security habits

Let's recap: Your employees are burned out, they're juggling more accounts than they can handle, and they often have to make a choice between productivity and security.

In other words, poor security practices are becoming an organizational habit.

Contrast this with what we at 1Password like to call a culture of security. A culture of security is the collective habits of employees who consistently do things in a secure way, actively helping to protect an organization and its sensitive data.

If you're serious about protecting your company, the first order of business should be creating a culture of security – so that good security becomes second nature.

To build a culture of security, you need two things: education and the proper tools. Education, so that people know the right thing to do. Tools, so that they can do the right thing without compromising their productivity – ideally, without even thinking about it.

A good password manager eliminates the tradeoff between security & productivity

That's where a good password manager comes in. If we tend to take the path of least resistance to get things done, then we need to secure the path of least resistance.

Password managers like 1Password remove the friction of logging into sites manually. Rather than hunting down the Post-It note that they jotted their password down on –or worse, reusing the same password across multiple services – 1Password fills in that information for them.

When a worker signs up for a new service, 1Password generates a strong, unique password, automatically fills in the relevant field, and then saves it to their 1Password vault. The next time they log in to that site, they don't have to remember their password, or even know it. 1Password logs them in automatically.

Nothing could be easier.

That ease of use gets at one of the most common misconceptions about good security: It's not about technology, it's about people. If you make your peoples' day-to-day lives easier, security and productivity tend to follow.

And it's not just logins. 1Password can autofill payment card information, store sensitive documents, and even mask their email address.

Ready to create a culture of security in your organization and eliminate the tradeoff between security and productivity? Get in touch with your MSP to learn more about how 1Password can protect your organization.