IT'S TIME TO STOP TALKING ABOUT PASSWORDS

> Digital transformation is a cornerstone of most enterprise strategies today, with user experience at the heart of the design philosophy driving that transformation. But most user experiences—for customers, business partners, frontline employees and executives—begin with a transaction that's both annoying and, in terms of security, one of the weakest links.[1]
>
> - Deloitte Review Issue 19

The authors of this excerpt are grumbling about the weakness of password-based authentication. And they're not the only ones.

Whether you get your information from Deloitte, Gartner, KuppingerCole or dozens of other reputable sources, they're all saying the same thing: static authentication (the dreaded password) just doesn't cut it any more. And worse, it's putting your enterprise at risk.

Yet, so many enterprises still rely on this outdated and insufficient approach. Why? Because it's easy. But easy for who? And at what potential cost? Let's take a closer look at usability and security to find out.

1 Irfan Saif, Mike Wyatt, David Mapgaonkar, "A world beyond passwords: Improving security, efficiency, and user experience in digital transformation," Deloitte Review Issue 19, July 25, 2016.

01

USABILITY

Some may argue that passwords are easy for the user. That may have been true when the only ones we had to remember were the PIN for our ATM card and the combination for our gym locker. But those days are behind us.

Did you know that the average person has 27 discrete logins?[2] That's a lot of passwords to manage. And it's only going to get worse. Some predict that we'll each have 200 online accounts requiring a unique password by the year 2020.[3]

Since you're reading this, we're going to bet that you're smarter than the average bear. So you might be using a password manager or other technology to deal with this challenge. But what about the vast majority of users who aren't? They're typically using the same password for everything. Or they have a few passwords that they rotate. Even then, remembering which one they used for each account presents its own problems. Both for them and your organization.

It's been estimated that as many as 30% of helpdesk calls are about forgotten passwords. The expenses associated with maintaining this outdated system are not only on the rise but they're exacerbated by the associated losses in productivity. And the frustration "cost" to users is equally high and just as important.

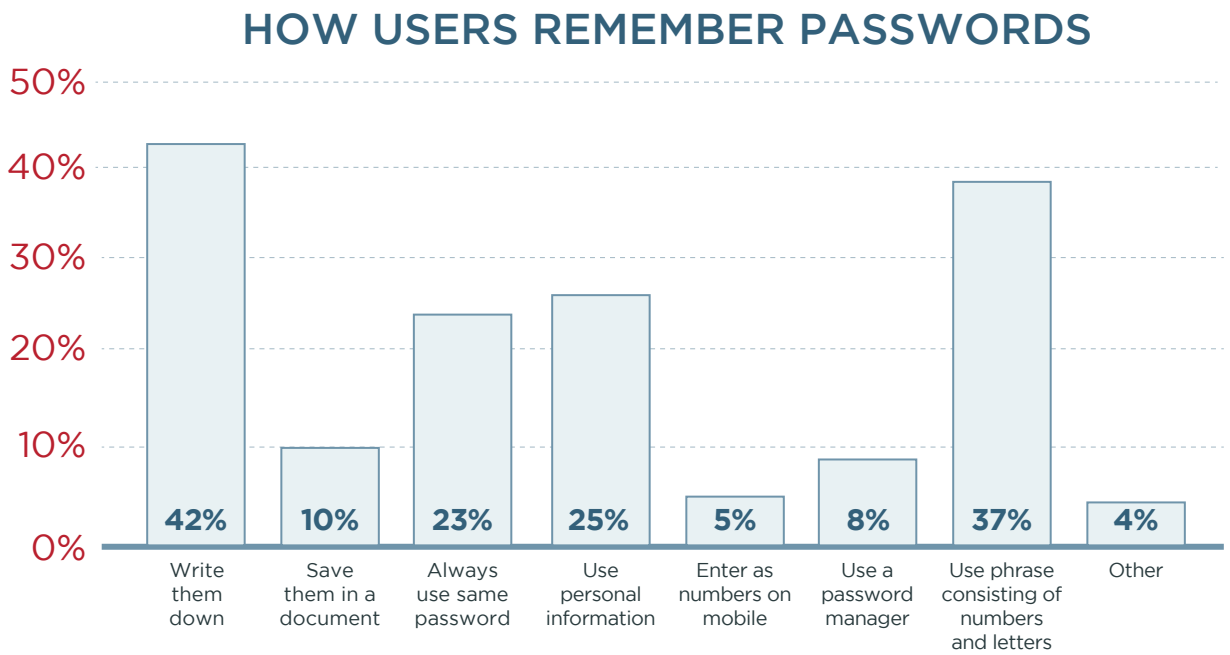

Figure 1: A recent study from password manager RoboForm reveals the most common techniques used to remember passwords.

2 Joseph Bernstein, "Survey Says: People Have Way Too Many Passwords To Remember," BuzzFeed News, May 4, 2016.
3 Guillaume Desnoës, "How will we manage 200 passwords in 2020?," ITProPortal, September 13, 2015.

02

SECURITY

We bet you cringed at the mention of users relying on a single password. But the one-password-for-everything approach is more common than you may want to believe. As RoboForm found (Figure 1), almost 25% of users rely on a single password for every login.[4]

Others estimate that it's even more common, with as many as a third of people using one password for everything.

The obvious dangers of that aside, the risks inherent in password-centric static authentication are huge. Verizon feels so strongly about it that they added a new credentials section to their annual 2016 Data Breach Investigations Report. Why? Because the use of stolen credentials is so prevalent in security incidents and breaches. In fact, Verizon reports that 3 out of 5 confirmed data breaches involved weak, default or stolen passwords.[5]

From phishing to web app attacks to POS intrusions, the bad guys are capitalizing on the weakness of static authentication, and they show no signs of slowing down. The costs to your organization—both in hard dollars and reputation damage—could be disastrous.

Static credentials continue to be targeted by several of the top hacking action varieties and malware functionalities.[5]

4 RoboForm, "Password security survey results," accessed Sept. 14, 2016.
5 Verizon 2016 Data Breach Investigations Report.

03

THE PROBLEM IS REAL

Once the cornerstone of security, passwords alone are indisputably insufficient. They lack the usability that today's users demand. They can't scale to deal with the number of apps users access. And as the basis of a static authentication protocol, they create very real security vulnerabilities.

Brett McDowell, Executive Director of the FIDO Alliance, summarizes it pretty well: "The password puts users into a no-win situation, where they either create different, complex passwords for all of their accounts—in which case they can't remember them when they need them, or they have to store them (typically somewhere that's not safe)—or they create only one or very few simple passwords that are easy to remember, which puts them at greater risk of having a single stolen or broken password result in many account takeovers, identity theft, and fraud."[6]

04

THE SOLUTION IS CLEAR

Just as the experts agree on the problem with passwords, they also agree that the solution can be found in multi-factor authentication (MFA). MFA is a form of two-factor authentication (2FA), but has several advantages in both usability and security over 2FA. MFA isn't a cure-all, but it can mitigate the risk of cyber attack, while also providing a frictionless user experience.

MFA solutions that leverage context extend beyond the traditional "what you know, have or are" to include "where you are" and "what you're doing" parameters. This is especially effective when MFA utilizes the mobile device to passively collect data points about users and their context to define use in dynamic authentication. These data points can include their location (both physical and network), their network environment and the resources they're trying to access.

If a user's behavior or the context of their request has a higher risk, contextual MFA can step up authentication requirements to apply the correct level of security based on the associated risk. Extra credentials are required only as warranted, delivering an optimal user experience and quite often lowering costs by utilizing more expensive authentication only when risk deems it necessary.

6 Brett McDowell, "The Problem with Passwords," The Cipher Brief, January 11, 2016.

05

THE CHOICE IS YOURS

According to Deloitte, new technologies like contextual MFA "offer companies the opportunity to design a fresh paradigm based on bilateral trust, user experience and improved system security."[7] They suggest that doing so provides not only a strong security posture for your enterprise, but can provide a strategic advantage and accelerate your digital transformation to boot.

Despite what the experts say, it's ultimately up to you to determine how to best protect your enterprise and serve your users. But if you're unwilling to sacrifice usability or security, then the choice seems pretty clear.

If you're tired of all the talk about passwords and want to learn about protecting your enterprise with contextual MFA, read our white paper.

MORE INFO

Visit our website
pingidentity.com
To speak with a Product Specialist in the U.S. call toll-free 1 (877) 898-2905

7 Irfan Saif, Mike Wyatt, David Mapgaonkar, "A world beyond passwords: Improving security, efficiency, and user experience in digital transformation," Deloitte Review Issue 19, July 25, 2016.

ABOUT PING IDENTITY: Ping Identity leads a new era of digital enterprise freedom, ensuring seamless, secure access for every user to all applications across the hyper-connected, open digital enterprise. Protecting over one billion identities worldwide, more than half of the Fortune 100, including Boeing, Cisco, Disney, GE, Kraft Foods, TIAA-CREF and Walgreens trust Ping Identity to solve modern enterprise security challenges created by their use of cloud, mobile, APIs and IoT. Visit pingidentity.com.

#3142 | 10.16 | v.002