The Password Isn’t Dead (and Will Never Die)

Part 1: Why Passwordless Authentication is Bad in Theory

HackNotice WHITEPAPER

If you’ve been keeping up with cybersecurity industry news lately, you’ve probably seen a few headlines unabashedly declaring the death of the password and the dawn of the passwordless era. A couple of security tech brands are hedging their bets, spending millions on software development for passwordless authentication, and forking out obscene ad budgets to evangelize the password’s supposed impending demise.

If it feels like déjà vu, that’s because a handful of thought leaders have been making that same bold claim for nearly 30 years. In fact, at the 2004 RSA Security Conference, Bill Gates also brazenly proclaimed the imminent death of the password.

But he was wrong. It didn’t happen then, it won’t happen now, and we’re willing to bet it won’t happen soon.

But why do tech leaders keep trying to kill the password, and what makes us believe it’s unequivocally here to stay?

As it turns out, these questions are part of a larger debate that has little to do with passwords and everything to do with security culture, employee autonomy, and the future of work (and cybersecurity) as we know it.

In this new series, we're diving head-first into this hotly contested and occasionally controversial topic to help you make the best decisions for your organization. And in this first installment, we're tackling the fundamentals: What passwordless authentication looks like and why, on a theoretical level, it's bad for business.

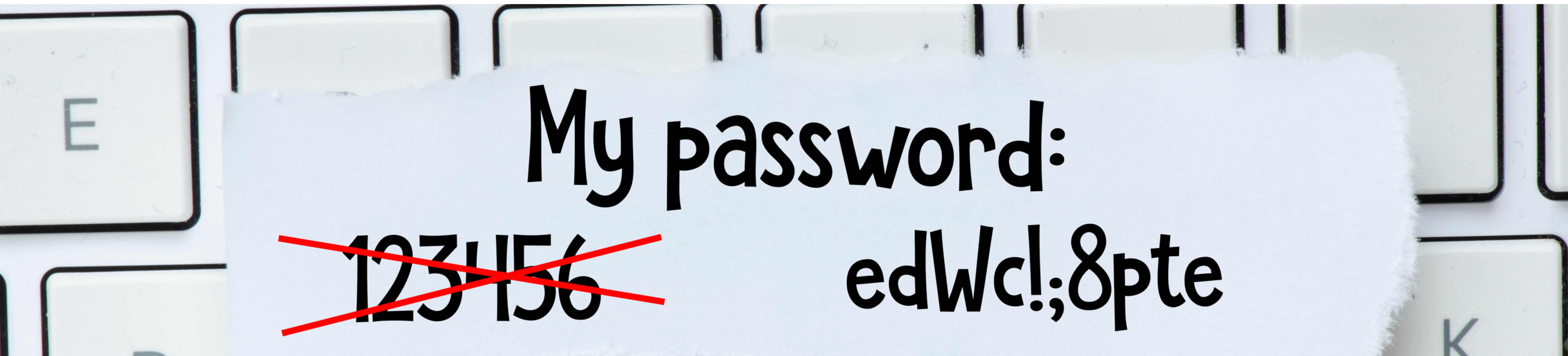
THE THEORY OF PASSWORD (AND PASSWORDLESS) AUTHENTICATION

In 1961, computer scientist Fernando José introduced The Compatible Time-Sharing System (CTSS), which was the first computer system to leverage a password login. Since then, this process has become ubiquitous. Nearly every digital experience — from your work email to your doctor's patient portal and your Netflix account — requires you to enter a username and password.

Over the past six decades, we've also become more sophisticated with our cybersecurity habits and password authentication processes.

Today, strong authentication has three components:

- Something you know (i.e., your password)
- Something you have (i.e., your device)
- Something you are (i.e., your biometrics)



Removing any of these three weakens the authentication, and that's precisely what happens with passwordless authentication. Instead of logging into a system with your username and password, passwordless authentication verifies your identity with physical or digital tokens, biometrics, or some type of third-party application.

And while it may sound pleasant in theory to relieve your workforce from the burden of remembering and regularly updating their passwords, removing the "something you know" part of the equation makes users more vulnerable.

That's because your password requires your consent, but the other two don't.

We've all heard the disturbing stories of law enforcement using people's fingerprints or facial recognition software to unlock phones without their permission, either by force or when an individual is unconscious. The idea of someone using your biometrics against your will is a terrifying prospect, especially considering how far a criminal might go to access your data.

But while you can't change your fingerprint, you can change your password.

ERADICATING THE PASSWORD IS NOT A FIX

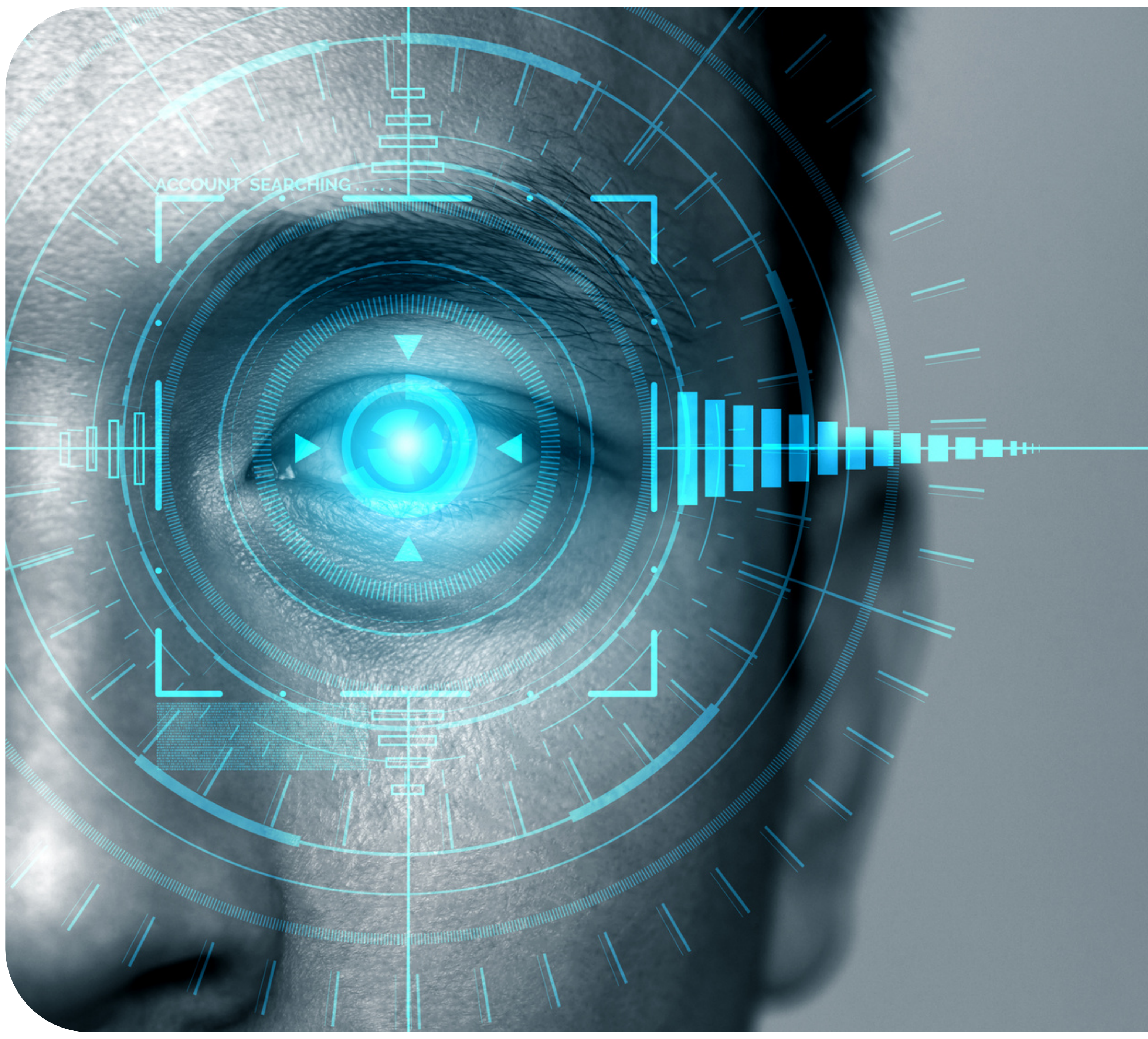
In all the debates around passwordless authentication, security thought leaders are missing one critical concern: eradicating the password is not a fix. It simply removes the symptom of a deeper and more pervasive issue. It’s akin to tossing back a couple of Tylenol for a raging toothache instead of going to the dentist to address the underlying cause.

Bad password habits stem from the fact that employees don’t fully understand online threats nor how their behaviors jeopardize the company’s or their personal privacy and security. And taking passwords away won’t bring you any closer to a strong security culture or a safer digital environment. In fact, removing this responsibility merely creates another layer of abstraction between employees and cybersecurity, which can worsen the problem.

When employees create short and easily guessable passwords or fail to regularly update those passwords, it’s usually because they don’t understand how cybercriminals might exploit their negligence. But educating employees on best practices and holding them accountable for their behaviors online will help foster better habits and ensures security remains top-of-mind for everyone in your organization.

BIOMETRICS ARE NOT AS RELIABLE AS YOU THINK

Not only does passwordless authentication fail to address the root cause of weak passwords (and poor cybersecurity habits in general), but it also relies on technology that's relatively new and not entirely foolproof.



But this isn't anything new. Hackers have fooled various face identification software with images, videos, and rudimentary masks of an original user's face.

And at the Chaos Communication Congress in Berlin, Germany, researchers fooled various types of biometrics authentication.

And while some tactics were more labor-intensive (like creating a lifelike wax model of a person's palm to trick vein authentication), others were disturbingly easy. For example, researchers discovered a simple latex replication of a fingerprint was enough to bypass most sensors on the market.

At the 2019 Black Hat convention, security researchers bypassed Apple's iPhone Face ID authentication in under two minutes by placing tape over the lenses on a pair of glasses and then slipping them on the user's face. By obscuring the person's eyes, the researchers circumvented the software's "liveness detection." This allowed them to not only unlock the user's phone but also transfer money via mobile payment.

And, if someone is willing to go through the trouble of creating a 3D printed copy of a user's head, research shows that can be enough to bypass several different types of Android facial recognition authentication software.

But what's most alarming about these discoveries is that once someone has been able to copy your biometrics, there's little you can do to prevent them from using it to access almost anything. Because while you can quickly and easily update a password, your biometrics won't change.

PASSWORDLESS AUTHENTICATION WON'T SAVE YOU IN THE EVENT OF DEVICE THEFT

Another challenge to consider is that most passwordless systems rely on a single device to store all credentials. This can create serious problems for users, especially in the event of theft.

Take SIM swapping, for example. In this scam, a criminal tricks your cell phone provider into transferring your number to a SIM card in their possession. This allows the criminal to intercept two-factor authentication texts or calls, which typically include one-time passwords, PINs, and magic links.

If you have a password protecting your device, the perpetrator won't be able to get in unless they know your password. And they won't be able to access other apps protected by different passwords. Plus, if you discover your device and/or password has been stolen, you can easily change it remotely.

But if you're relying on passwordless authentication, there's nothing you can do. Worse, once a criminal accesses the device holding all your credentials using a practice like SIM swapping or spyware to intercept authentication, they'll be able to get into everything. That means your banking information, various work and personal apps, social media networks, text message history, photos, and anything else stored or accessible via your device are all vulnerable.

PASSWORDLESS AUTHENTICATION IS NOT THE ANSWER

It's easy to be allured by the appeal of passwordless authentication. At first glance, it seems like a great way to streamline user experiences and exercise more control over your organization's security by taking the responsibility away from your employees. But the weaknesses in these processes can jeopardize your security and make it more challenging to foster a security-conscious workforce.

By recognizing that weak passwords are a symptom of a weak security culture and instead focusing your resources on strengthening that culture, you'll solve the password issue and improve security across the board.

READY TO TRANSFORM YOUR EMPLOYEES INTO SECURITY HEROES?

THE HACKNOTICE THREAT AWARENESS PLATFORM IS DESIGNED TO FOLLOW ALL OF THE PRINCIPLES SHARED ABOVE.

LET'S GET STARTED