NUANCE | WHAT'S NEXT BLOG

Customer engagement, Authentication & fraud prevention

It's time to forget passwords for good, and rethink World Password Day

Brett Beranek | Vice President & General Manager, Security & Biometrics

May 5, 2021

Asking for a password has never been an effective way to verify someone's identity—as our recent global poll of consumers makes all too clear. But with fraud on the rise, brands have a responsibility to develop a more comprehensive approach to authentication. What's more, those that have already made the leap to biometric technologies are seeing better outcomes for their customers and their businesses.

When Intel created World Password Day in 2013, it was a global reminder to change and strengthen the words, numbers, and special characters which secured our accounts and protected our identities.

Eight years later, World Password Day reminds us that passwords are an archaic tool. It reminds us that passwords have become a commodity for sale on the dark web and that the fraud committed with them—not to mention the challenge of simply remembering them—regularly costs individuals vast sums of money.

But most of all, it reminds us that if you need to create a national day to shore up a form of security, that form of security will never be particularly secure.

Rethinking World Password Day

In Nuance's recent survey, more than three in ten (31 percent) of consumers in the US admitted to choosing only between three or less passwords for all their accounts. More than seven in ten (77 percent) said forgetting usernames, PINs and passwords and six in ten (60%) received notifications that their passwords have been compromised in the last 6 months. We've been doing similar research also two years ago, and despite having a World Password Day, the numbers have not significantly gone down.

This message is clear—it's on enterprises to find a more comprehensive method to protect their customers. And they need to move fast.

The leap in fraudulent activity so many organizations witnessed at the outbreak of COVID-19 has become even clearer in hindsight; global losses from payment fraud tripled from $9.84 billion in 2011 to $32.39 billion in 2020 and are expected to top $40.62 billion by 2027. What's more, 38 % of the consumers in the US we spoke to for our research said they had fallen victim to fraud in the last 12 months.

If brands are to maintain customer trust—and customers, period—they need to accelerate the transition to more robust, user-friendly forms of authentication. And for many, biometric technology will be the smartest solution.

Biometrics offers a proven alternative

The fundamental problem with password-based authentication and PINs has always been easy to understand; it tests what someone knows, not who they are. But back in 2013, the year Apple first introduced fingerprint scanners into the iPhone, such knowledge-based authentication (KBA) was still the best option available to most businesses.

Since then, biometric technology has come a very long way. And whether it's reading your fingerprint, listening to the sound of your voice, or analyzing the way you're swiping, tapping, and typing on your device, it's doing what KBA never does—checking the things that actually make you, you.

The recent survey has shown that nearly 6 in 10 (59 percent) feel more comfortable using biometric technology to authenticate myself when accessing accounts than before the pandemic**.** Today, biometrics are a proven and trusted technology. And as we all become more accustomed to life without the hassle and stress of KBA, it's rapidly becoming table stakes for brands determined to compete on customer experience.

The business case for banishing passwords

One brand that has embraced biometrics—and seen compelling benefits—is NatWest Group (formerly Royal Bank of Scotland Group). Its voice biometric solution delivered over 300% ROI in just 12 months while helping identify one in every 3,500 calls as a fraud attempt. As Jason Costain, Head of Fraud at NatWest, recently told the BBC TV program Frontline Fightback, the technology has also provided evidence to support 231 arrests and prevented £38 million from being stolen by UK criminals in a single year.

Other brands are finding that their move away from slow, stressful conversations about passwords and PINs is having a profound impact on customer experience. When Barclays Wealth and Investment Management implemented voice biometrics, customer and agent satisfaction increased, and it saw a 90% reduction in complaints.

In the US, voice biometrics is helping Virginia Credit Union to serve its members more quickly and efficiently; since deploying its Voice ID solution, it's seen average handle times fall by 37 seconds.

The expanding universe of biometric applications

While the opportunities once presented by knowledge-based authentication have been thoroughly exhausted, organizations are pioneering new applications for biometric technology all the time.

One of my favorite examples comes from global telecommunications company Telefónica. Following the outbreak of the pandemic, the organization wanted to give priority to its most vulnerable customers. Our research team worked to make this happen—allowing Telefónica to identify a caller's age by the sound of their voice, and fast-track service for any customer over 65.

Let's rethink World Password Day

Every year, I write a blog post to mark another World Password Day. And every year, World Password Day feels like more of an anachronism and needs rethinking. Here's hoping that more brands seize the opportunity presented by biometrics—giving a new dimension to this day.

Tags: World Password Day, Fraud prevention, Biometric authentication, Nuance Gatekeeper

More Information

About Brett Beranek

Brett Beranek is responsible for overseeing the security and biometric line of business at Nuance, a Microsoft company. In this role for the past 12 years, Beranek has brought Nuance to a leadership position in the biometric authentication and biometric fraud prevention space. A thought leader in the field of biometrics, Beranek is a frequent contributor in industry events and the media on the topic of AI technology and it's use by the fraud community, and how society can mitigate against these evolving threats. Prior to Nuance, he held various leadership positions in the biometrics and security industry. He has earned a Bachelor of Commerce, Information Systems Major, from McGill University as well as an Executive Marketing certificate from Massachusetts Institute of Technology's Sloan School of Management. Beranek is also a certified Master Fraud Prevention Black Belt professional.

View all posts by Brett Beranek