NUANCE | WHAT'S NEXT BLOG

Customer engagement, Authentication & fraud prevention

The case for password-less authentication: Forgotten passwords lead to lost crypto investments

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

January 28, 2021

Forgot your password? You're not alone. Industry research suggests that about 80% of people have forgotten their passwords and had to reset them. This is more than just a frustrating experience for customers; it's a potential fraud and cybersecurity risk for organizations. We hear more and more catastrophic stories of lost passwords, all while we know that there are, in fact, far more secure and simple mechanisms for confirming users' identities. It's a topic we explored in our recent virtual roundtable on the evolution of authentication.

We all have that one person in our life who's forever forgetting their passwords to their online accounts. The saved login feature in their browser is their lifeline; so too is the face ID that lets them into their bank accounts from their mobile device. Perhaps, though, no story is more dramatic – or more illustrative of how damaging lost passwords can be – than the story of Stefan Thomas, whose investment in cryptocurrency is all but lost in the ether.

He protected his investment, today valued at about $220 million, with an anonymous digital wallet … the password to which he has lost.

This all too familiar phenomenon of forgotten passwords not only risks impacting buyers in the bullish cryptocurrency market but can prevent the safekeeping of any investment.

Passwords have, for too long, been a hallmark of customer authentication, but we're now seeing a noticeable shift toward password-less authentication platforms. Namely, we're talking about biometric authentication, which serves two primary goals. First, it's a frictionless, better customer experience. Second, multimodal biometrics help improve security and fraud prevention efforts.

It's a topic we explored recently in our ongoing virtual roundtable series with Zenkey. We know that PINs, passwords, and challenge questions fall short in terms of security. These credentials can be purchased online by fraudsters. What's more, inadequate measures like One Time Password (OTP) resets via SMS messaging to your smartphone are easy avenues for bad actors. And for people hoping to bolster their credentials with two-factor authentication, the bad news is that SIM swapping is unfortunately growing in frequency. For example, we recently sat down with Rob Ross, a tech investor who lost nearly $1 million of his life savings at the hands of fraudsters.

Biometric authentication helps to overcome these challenges and today has risen to become a very important component of authentication processes. By using a uniquely identifying aspect of the human body (fingerprints, voiceprints, facial recognition, etc.), artificial intelligence can be applied to automate the authentication process and confirm the user's identity—all while providing the security and convenience that customers and organizations depend on.

More, by creating an identity profile for the user's specific device, something done in partnership with the wireless providers in an effort to prevent SIM swapping scams, organizations can create a powerful and portable multi-factor authentication process that puts the end-user in control of their data and transactions. It's an effort that requires collaboration and trust, but one that can ultimately help avert millions of dollars in losses for organizations and consumers alike.

Tags: Fraud prevention, SIM fraud, Nuance Gatekeeper

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