NUANCE | WHAT'S NEXT BLOG

Authentication & fraud prevention, Customer engagement

Shifting gears to drive down security risks in a virtual world: A solution in voice biometrics

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

December 15, 2021

Following the pandemic, the contact centre has more weaknesses than ever before. Agents work remotely, separated from their colleagues and more susceptible to attacks, while customers exhibit new behaviours that make them difficult to distinguish from fraudsters. Brett Beranek reveals some of the key insights from his conversation with Microsoft's Chief Cybersecurity Advisor on how brands can navigate these new security challenges.

The disruption and uncertainty of the past couple of years created new opportunities for fraudsters to retrieve personal information and impersonate customers, and it kickstarted a wave of account-based attacks that's continuing to rise today.

These recent attacks have put security front of mind for both brands and customers. But many organisations are still a few steps behind, lacking the measures to fight fraud effectively.

I was recently joined by Abbas Kudrati, Microsoft's Chief Cybersecurity Advisor, and my colleague Robert Schwarz, Managing Director of Nuance Australia, for a discussion on how the fraud landscape has changed and what it means for brands and their customers in 2022. We also spoke about some of the strategies brands will need to prioritise over the next few months, and how solutions like voice biometrics will play a crucial role in fighting fraud for years to come.

It was a valuable conversation—I'd recommend listening back to it if you missed it. But in the meantime, here are some of the key points we covered.

A Zero Trust approach is critical to keeping customers safe

So many attacks we're seeing today are based on stealing customer identities, which means it's more important than ever to ensure you know who you're talking to in every engagement.

It was interesting to hear Abbas talk about how Microsoft approaches this challenge, using a 'Zero Trust' approach to engagements. "Zero Trust isn't just a buzzword. It's an architecture model that forces brands to verify the user at every engagement, trust nobody, and always assume a breach has happened," he explained.

It's a two-pronged approach, involving participation from both customers and employees. Customers need to prove they're trustworthy every time they speak to an agent, access their account, or complete a transaction. Similarly, employees need to prove they're trustworthy throughout the working day.

Zero Trust also involves more than just authenticating individuals. It requires brands to know their architecture, including all the devices and services used across their network, and the digital health of those devices.

While it sounds simple in principle, Zero Trust can be a little trickier to put into action. In parts of the organisation like the contact centre, gauging the trust of agents and customers effectively—without causing too much friction in engagements—can be a major challenge.

The new threats and challenges in the contact centre

The contact centre has always been a weak security point for organisations and a prime target for fraudsters, and its security gaps have only grown since the pandemic.

Agents are no longer operating in heavily monitored environments. Instead, many contact centre models have changed, and agents work from home, use multiple devices, and share their working spaces with family members and housemates. These circumstances make it a lot harder for contact centre leaders to know whether the person interacting with customers is who they say they are, who has access to agents' devices—and in turn, who has access to valuable customer information.

Even if an agent is who they say they are, you can't guarantee they won't be a threat to your organisation. Many agents' circumstances will have changed during the pandemic, and some might be encouraged to turn rogue, even if they've been loyal employees for years.

Over the last year, we've seen fraudsters taking advantage of security gaps like these—my colleague Simon Marchand offers some prime examples in his recent blog post.

Long-established attack methods like phishing have made a strong return, preying on agents cut off from their colleagues and customers anxious about the effects of the pandemic. Also, with customer behaviour changing so frequently during the pandemic, many traditional fraud prevention tools have struggled to distinguish normal and abnormal behaviour. And in many cases, that's allowed fraudsters to go unnoticed, while agents and customers face more friction during engagements.

Navigating the move to password-less

To reduce customer friction and minimise the effectiveness of phishing attacks, we've seen many brands going completely passwordless over the past year. It's a move in the right direction—we've all seen how easily passwords are purchased on the dark web and compromised by fraudsters.

But during this move, the alternative authentication method mustn't expose customers and agents to new risks. For example, one of the most common alternatives to passwords is sending a one-time passcode by SMS messaging, but this method is easily thwarted by a simple SIM swap attack. Just look at my conversation with tech investor Robert Ross to see how damaging these attacks can be.

To truly protect customers and make agents' lives easier, you need a modern authentication solution like voice biometrics. For agents, it removes the burden of authenticating customers, and provides a fast and easy method to prove their trustworthiness to their organisation. And for customers, it eliminates the hassle of passwords and PINs, and offers an effortless way to authenticate during engagements.

But as we discussed in the webinar, no single solution should be used by itself. Tools like voice biometrics should be used alongside a holistic fraud prevention platform that integrates with the rest of your architecture and allows you to spread the Zero Trust mindset through your entire organisation.

Listen to the full conversation

I've only covered a fraction of what Abbas, Robert, and I discussed in the webinar—if you haven't already, I'd urge you to watch the full session. We closed the webinar sharing some of our best practices for brands rethinking their security strategies over the next year and offered a detailed insight into the effectiveness of voice biometrics solutions.

Tags: SIM fraud, Contact centre strategy

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