NUANCE | WHAT'S NEXT BLOG

Customer engagement, Authentication & fraud prevention

Five digital security trends to watch in 2021

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

December 21, 2020

Countless unsuspecting technology users are victims of a cybercrime or fraud each year. This number continues to increase during the pandemic, as online interactions such as banking and shopping take place in unprecedented volume. Against this backdrop, we offer our key cybersecurity predictions for 2021.

Here is a round up of five key digital security trends that span from cybersecurity, fraud prevention, and risk management

Forward-looking CISOs will transition to **password-less authentication** with the twin goals of customer convenience and enterprise security. Consumers want a digital experience that is easy, secure, and free of passwords. Daily passwords and pins (e.g., email, ATMs) are near relics. As more consumers shift to online channels in order to bank, socialize, play, and shop, users demand a more sophisticated and secure experience. Passwords have lulled consumers into a false sense of security for years, especially as the number and variety of devices on which apps are used skyrocketed, each requiring critical information to be entered repeatedly – and thus each instance an opportunity to track and steal that data. Companies will need to demonstrate to their customers that they take their security seriously. Consumers are now more conscious than ever of the risks surrounding their identity. They will start to demand more from the

businesses they deal with. Organizations can't afford to do things only based on ROI – better security is now a question of customer retention, loyalty, and corporate social responsibility.

An **integrated approach for fraud prevention and authentication** will be the key to protection against flimsy device-side biometrics. Customers are going to demand security protocols that identify themselves in particular, not just someone who may have their identification. We are seeing a noticeable shift away from technology that does not authenticate the identity of the actual person interacting with security measures. It is no longer enough to authenticate passwords, pins, or SMS confirmations, for example. That information is too easy to obtain. Biometrics such as voice recognition, behavioral recognition, fingerprints, and eye scans are critical to a secure online presence. Thanks to years of interacting with smart devices customers often already feel comfortable with fingerprint ID and facial recognition. Unfortunately, most of these device-side biometric authentication methods don't have any real impact on stopping fraudsters because, firstly, it is challenging to determine who has created the biometric print, and secondly, the prints are limited to a specific device, making them difficult to leverage across multiple channels and impossible to port from one device to the next. Their "value" begins and ends with being free. It is server-side biometrics, such as voice biometrics, that will have result in both significant fraud prevention and frictionless, convenient customer experiences

Cutting-edge artificial intelligence will enable biometrics to solve increasingly complex security challenges. Earlier this year, Telefónica, S.A., a Spanish multinational telecommunications company and one of the largest mobile network providers in the world, engaged Nuance to help them deploy voice biometrics to analyze the sound of clients' voices to determine whether they are 65 or over. This critical determination helps the bank provide world-class bank anti-fraud protection to an age group that is highly susceptible to fraud.

Harnessing state-of-the-art technology will allow organizations not only to prioritize or adapt services for specific customer demographics but also strengthens fraud prevention efforts by providing additional biometric factors to consider.

Customer care will take a drastic shift to video/virtual settings. As virtual consultations, transactions and interactions become the norm between brands and consumers, digital channels will need to be as secure and convenient as if these interactions were happening in person. Video customer care is a trend that we are starting to see emerge as a result of COVID-19, and voice biometrics is a critical aspect of authentication and keeping customers safe.

For example, IBK (Industrial Bank of Korea) has implemented Nuance's voice biometric technology to ensure robust, sophisticated customer authentication as virtual transactions are rising significantly. Reporting 100% consistenty in validation rates, IBK has been able to revolutionize the digital banking experience.

Security will need long arms to protect against increased fraud brought on by **remote work**. As companies extend work from home indefinitely in what Harvard Business Review's most recent cover tags as "The Work From Anywhere Future" (Nov-Dec 2020), fraud will only increase against remote workers and frontline agents, but remote work also represents a potential for increased occupational fraud. Unsupervised employees with access to PII have a new opportunity to defraud their employers and steal valuable information. Under increased pressure that difficult social and economic times brings, conditions are right for a surge in occupational fraud. Forrester Research echoes this sentiment, forecasting that thirty-three percent of data breaches will be caused by insider incidents, up from 25% today. Companies will need to work quickly to combat voice fakes (i.e. ultra-realistic speech cloning) and deep voices (i.e. the use of artificial intelligence to create speech, accents, and tones – effectively, a fake voice) to seamlessly secure interactions with workers worldwide. Traditional security measures will also need to operate at peak performance with so many individuals outside an organization's firewalls.

We can find comfort in 2021 that shepherds greater digital security and peace of mind. Traditional ways of doing things, even ones so rudimentary and fundamental as the online password, no longer suffice. Biometric security systems based on verifiable traits such as one's retinal scan, fingerprints, and voice patterns will replace subjective codes all too easily stolen and misused. Adopters will make a quantum leap in their security protocols and find a smooth transition to a more secure digital presence.

Tags: Customer experience

More Information

Learn more

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