NUANCE | WHAT'S NEXT BLOG

Kundeninteraktion auf allen Kanälen, Verifizierung und Betrugsprävention

KI und Biometrie verhindern Sozialhilfebetrug schon im Ansatz

Nuance Communications

3 Juni 2021

Betrüger:innen haben in ganz Europa die Unsicherheiten rund um COVID-19 ausgenutzt, um Milliarden an Hilfs- und Konjunkturgeldern abzugreifen. Deshalb fragen sich Regierungen und Banken: wie können wir unsere Bürger:innen und Kund:innen besser schützen? Immer mehr setzen dafür auf intelligente Lösungen auf Basis von KI und Biometrie, um Sozialleistungsbetrug proaktiv zu erkennen und zu verhindern und gleichzeitig sicherzustellen, dass berechtigte Antragsteller:innen ihre Leistungen erhalten.

Fraud was already a serious problem before the pandemic: In an EU-wide "Scams and Fraud" study published by the European Commission in January 2020, the majority (56%) of Europeans said they had fallen victim to fraud in the past two years.

Und dann kam COVID-19. Die weitreichenden negativen Auswirkungen der Pandemie auf die Wirtschaft eröffneten Betrüger:innen viele neue Möglichkeiten – vor allem im Zusammenhang mit Leistungsbetrug bei Arbeitslosengeldern.

Unbürokratische Verteilung von Hilfsmitteln lockt

Kriminelle an

The crisis caused the EU labour market to shrink dramatically: in the second quarter of last year, 5.5 million jobs were lost across the EU. As governments rushed to implement new aid and stimulus programs – from Spain's ETRE to Britain's Furlough program – application processes were simplified in many places to reduce administrative burdens and provide timely support to citizens in need.

However, professional fraudsters quickly took advantage of this situation and submitted applications for unemployment benefits and company grants on behalf of strangers and companies. In France, for example, criminals stole 1.7 million euros, which were intended to support companies at risk. In Germany, fraudsters stole at least 31.5 million euros from a single state government. And in the UK, it is estimated that up to £3.5 billion in COVID aid has been fraudulently requested or falsely disbursed.

These are just a few examples that show how the COVID-19 pandemic has accelerated the need to rethink authentication and fraud prevention. Government agencies across Europe – including the UK – are taking note, allocating larger budgets to action and considering what else they can do to protect themselves and their citizens.

Verifizierung biometrischer Merkmale ist schneller und zuverlässiger

One possible solution is AI-based biometrics, which can authenticate citizens and quickly and securely detect fraudsters during telephone and digital interactions. Compared to security questions or on-the-phone verification, biometrics are faster and more reliable at authenticating and exposing fraudsters because they are not fooled by stolen information. Instead, they verify people based on individual characteristics. Even more effective is linking biometrics with other features such as environment detection (checking the device, network, channel, and location) and anti-spoofing measures (preventing ANI spoofing and detecting synthetic speech or audio playbacks).

Ein Beispiel: Eine Betrügerin oder ein Betrüger ruft dutzende Male in einem Contact Center an und gibt sich jedes Mal als eine andere Person aus, um Leistungsansprüche unter falschem Namen anzumelden. Wenn die Betrügerin oder der Betrüger über Identitätsdaten anderer Personen verfügt (die oft leicht im Dark Web erhältlich sind), kann sie oder er unentdeckt bleiben und sich Tausende Euro an staatlicher Unterstützungen erschleichen.

Wird das Contact Center jedoch durch eine Biometrielösung unterstützt, erkennt diese Betrüger:innen innerhalb von Sekunden und alarmiert die jeweiligen Contact Center-Mitarbeiter:innen in Echtzeit. In der Zwischenzeit kann das Sicherheitsteam historische Anrufaufzeichnungen analysieren und feststellen, ob dieselbe Stimme schon häufiger in Anrufen aufgetaucht ist. Das Team kann dann die Stimme einer Überwachungsliste hinzuzufügen, sodass die Betrügerin oder der Betrüger beim nächsten Anruf sofort erkannt wird. Das ermöglicht auch das Sammeln hochwertiger Beweise für die Strafverfolgung.

Investitionen in die digitale Zukunft

Auch der Blick in die Zukunft über die Pandemie hinaus zeigt die Bedeutung von Lösungen gegen diese Art von Betrug. Regierungsbehörden müssen ihre Bürger:innen in diesem Übergang zur "neuen Normalität" im Jahr 2021 proaktiv schützen. Vorausschauende Investitionen in Technologien der nächsten Generation wie KI und Biometrie können dazu beitragen, Interaktionen mit Bürger:innen und Kund:innen zu optimieren und zu schützen, sodass sie Leistungen schneller erhalten und Betrüger:innen keine Chance haben.

Learn more about Nuance's security and biometrics solutions. In addition, I am also available for a conversation to discuss the specific challenges of your authority and how our technologies can best be used for you.

Tags: Biometrische Authentifizierung