Safeguarding your customers against the threat of identity theft

By Wynand Smit

17 Nov 2017

A recent data breach exposed the personal information of 30-million South Africans, including emails, ID numbers, addresses and contact numbers, and, in some cases, even passwords. A real estate agency owned up to having their data leaked - but really, it resulted in all of those customers and potential customers being placed in a vulnerable position.

© monsit jangariyawong – 123RF.com

Identity verification in contact centres across a number of industries relies heavily on security questions, questions that, in turn, rely on data to ascertain the individual's identity. If that data is leaked, it's relatively easy for an unscrupulous fraudster to pose as another person.

If you know enough about someone, you can answer all the questions correctly, so to the agent on the other end of the call, you've proven that you are that person. This can put you in a position of being a verified identity, allowing you to alter access requirements or passwords, effectively assuming ownership of online profiles and accounts.

If your company is still conducting business using a security question process as a means of identification verification, given the prevalence of large-scale data leaks, it's time to make your business more watertight.

Verifying identity without exposing data

Biometric identification is gaining traction, since it reduces the need for tedious security questions, and offers enhanced security and peace of mind for businesses and customers alike. Biometric means of verification include unique identifiers such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures.

In contact centres, voice authentication is an effective method, since it improves security, reduces time spent verifying identity by as much as 70% and cuts down on those frustrating minutes it takes for your customers having to answer questions, sometimes repeatedly.

Cutting down on time spent on calls makes sense, as it translates to improved efficiency and productivity, which is turn drives profitability and customer experience improvements.

Blockchain technology

The next possible step in identity verification is not rolled out in South Africa, but with the popularity Blockchain is gaining internationally, the trust economy could have an impact on how we do business eventually. Among many possible applications, in the contact centre environment it could allow two people to potentially verify each other's identities in seconds via multiple data points.

In addition to that potential application, Blockchain technology could also allow consumers the ability to store all sorts of information such as contracts, ID documents, driver's licenses many other forms of rendered documents online, with access to those only given to verified people for specific purposes.

This emerging technology is relatively far away from being seen in active applications, but it's part of an entire system that's evolving in response to connectivity and the opportunities that provides.

Let's begin at the beginning, though: if your company is storing customer data, ask yourself a couple of key questions: do we need to hang on to this information? Are we accessing, storing and using the data in a secure vacuum? Are there better ways of managing, storing and, if necessary, erasing this data, all the while with the protection of your customer's personal information?

If not, it's time to rethink your data management strategy.

ABOUT WYNAND SMIT

Wynand Smit is CEO at INOVO, a leading contact centre business solutions provider.

- Creating competitive experiences with cloud - 12 Apr 2022
- How to prepare your contact centre for an AI-driven future - 15 Oct 2019
- Tech won't kill the contact centre, it'll make it more powerful - 30 Apr 2019
- 2019 predictions: The CIO will govern - 14 Jan 2019
- Safeguarding your customers against the threat of identity theft - 17 Nov 2017

View my profile and articles...