Privacy-conscious South Africans may be exposing themselves to additional risk

Issued by Entersekt

17 Nov 2022

Banks, medical aids, insurance companies and many others have spent millions educating their customers about new and evolving security risks. But South African consumers are now so hyper aware of protecting their personal data, that many are inadvertently disabling their means to some of the strongest digital security available. Striking the balance between friction and security will require re-educating customers and making them part of the solution, says authentication expert, Entersekt.

Andries Maritz

“We all want our banks and other service providers to offer the best security possible, until that means we have to jump through hoops to complete the transaction we are trying to make. The big challenge for organisations now is to make their customers feel safe, without adding layers of friction to their customer experience,” says Andries Maritz, product manager at Entersekt.

Maritz says authentication is generally viewed as a one-size-fits-all solution. However, this approach is no longer appropriate and not only adds layers of friction that will hurt the customer experience, but also cuts the customer off from a better security option.

“Context-aware authentication looks at each transaction and each user profile and then makes a judgement call as to the most appropriate authentication journey for that transaction. The problem is that as customers take control of their data, many are switching off certain functions in apps, such as location data. While it’s understandable that users are mistrustful of being tracked, this could potentially force a shift in how authentication solutions operate and assess risk,” he explains.

Using multiple data fields delivers a better experience

Context-aware authentication, sometimes referred to as intelligent friction, is all about knowing who your customer is, where they are, and what device they’re using. By using as many data fields as possible, such as location, device biometrics, and IP address, companies can provide an additional layer of security that can prevent unauthorised access.

The authentication method has evolved to accommodate the move towards omni-channel customer experience. A survey conducted by PYMNTS and Entersekt shows that 25% of consumers will use multiple devices to check their bank accounts. Logically, this means that banks and others will need to build up data across all digital channels over a period of time in order to deliver accurate estimations of the legitimacy of users and transactions.

“Consumers are wary of the unknown. They may not immediately understand what companies are using their data for and this can cause panic. For instance, your banking app may access your camera in order to compare your face to the picture it has of you on file. Or, it may access your microphone, apply AI to emit a noise, and see if that noise bounces back to ensure it is not dealing with a recording of your voice. There are also other liveness detection features, which may be startling if the user is not aware of them. We believe that organisations should inform customers and make them part of the security solution,” Maritz says.

An involved customer is a safer customer

Entersekt believes that companies that involve their customers can fast track the move towards a more robust and mature security ecosystem.

“Fraud attack vectors are constantly evolving and it’s a war of escalation between bad actors and security departments. It’s time to make the consumer part of the battle. Nobody knows better whether a transaction is legitimate or not than the customer. Companies that inform customers about how and why their data is being collected are likely to get their buy-in for new authentication methods. This will deliver a more secure and frictionless experience, but it will also empower consumers to take charge of their digital security. Context-awareness will continue to evolve and businesses must prepare the consumer for the journey ahead,” Maritz advises.