Every swipe tells a story

AYELET ELIEZER: BIOCATCH

Digital behaviour patterns, combined with artificial intelligence-powered risk models, are changing the way financial institutions detect fraud in the mobile channel

In an age where the use of smart devices has skyrocketed and consumers require the convenience of instant services, it is no surprise that mobile banking is becoming the preferred method for customers to engage with their banks. While this shift has now presented financial institutions with an opportunity to acquire new customers and capture additional revenue, it has also created new risks in a digital channel that has generally been viewed as more vulnerable to attack than its online sibling. Today, BioCatch data shows that nearly half of all confirmed fraud cases originate in the mobile channel.

Behavioural biometrics deliver a fresh approach to mobile banking fraud protection. Leveraging machine learning algorithms that consider mobile interactions such as swipe and scrolling patterns, tap gestures, and touch and gyroscope events, behavioural biometrics learn about unique user behaviours and compare them at the user and population levels. When significant variations are detected, the likelihood of fraud risk increases.

The most common type of mobile account takeover is a manual act where a cybercriminal attempts to log in to a bank account through a mobile browser or mobile app using stolen credentials. Behavioural biometrics detect instances where a user's current behaviour shows significant variations from their unique user profile. For example, a legitimate user who consistently uses both thumbs equally when scrolling but suddenly uses only their left thumb is one example of an inconsistent behavioural event that could indicate risk.

Cybercriminals also attempt account takeover using technology such as mobile emulators or remote access tools (RAT). Behavioural biometrics detect fraudulent sessions run over mobile emulators by cross-correlating accelerometer data and touch events where there is no physical device or touch movement at all. In the instance of RATs, behaviours such as latency or a lack of device movement are often observed.

Behavioural biometrics have also been successful in uncovering advanced social engineering voice scams by looking for differences in actual human behaviour that are statistically significant enough to determine intent or emotional state. For example, continuous movement of a phone or changes in device orientation often suggest a user is acting under duress such as picking the phone up to take instructions and placing it back down to perform actions instructed by a cybercriminal.

Mobile devices are the future of digital banking, but increased mobility and frequent device changes make it hard to validate user activity based solely on location, device and network attributes. One thing that cannot be stolen, spoofed or replicated, however, is digital behaviour. Every swipe, tap and scroll tells a story – one of fraudulent activity or that of genuine user behaviour. ■

Ayelet Eliezer is vice president of product management at BioCatch