Could biometrics replace OTPS?

Andrew Bud, CEO & Founder

Perhaps we're coming to a moment of transition over the last 10 years, we've seen a significant enhancement in the cyber security of people and organizations, thanks to the use of text messaging to deliver one time passcodes. These one time passcodes assure that the user is actually in possession of the mobile device which they claim to have.

And that forms one leg of a two-factor authentication process, the other one of which is often a password, something you know, something you have - these are the elements of two factor authentication. And one time passcodes have become extremely familiar to users in numerous tests people have indicated that that is their preferred method, just because of the familiarity, the establishment of user behaviour.

But it's becoming increasingly clear that onetime passcodes have had their day. There are substantial security vulnerabilities, both at the network side where access to the signalling system seven network can enable attackers to access the onetime passwords to divert them and to read them. And also at the user side where one time passcodes can give rise to significant vectors for fishing and smishing attacks. As have recently occurred in a number of different countries. So the one time passcode has perhaps had its day, what will come next? Well, we believe that biometrics... facial biometrics will come next... cloud based facial biometrics will come next.

Why? Because if they enjoy the same incredible usability. That other established behaviors have I look at my device, it looks back at me. What could possibly be simpler? It's ubiquitous. It has the same ubiquity that one time passcodes have. A one time passcode can be delivered to any mobile device and a face biometric can be captured on any mobile device with a front facing camera, which pretty much means any user device and that includes laptops as well.

So you have ubiquity, you have usability and you also have security because a face cannot be stolen. It can be copied, but with good, genuine presence assurance technology copies can be detected and blocked. So I think we're on the verge of a transition from one time passcodes to the use of cloud based biometrics to deliver inclusive, ubiquitous, highly secure authentication for the next generation of online applications.