No, SMS OTP Isn't Dead

Stay Calm and Assess the Situation

31 July 2016 By: Al Pascual

Last week's announcement from NIST that SMS one-time-passwords (OTP) were deprecated as a form of out-of-band (OOB) authentication put the industry in a tizzy. Funny thing was that NIST did hedge a bit in its language, but it seemed that the agency was relegating SMS OTP to the junk pile when reading some of the posts out there.

While NIST has since clarified the statement further in a blog of its own ("2FA is better than no 2FA, and SMS OTP isn't prohibited"), there are questions as to what it all means for financial service providers as NIST guidance is closely followed by the industry (especially by forward-looking institutions).

There's understandably some concern among our clients about existing investments and what a change would mean for customer experience (as consumers in general have just started to become accustomed to SMS OTP). And you can bet that authentication vendors in the biometrics space were raising their glasses after the announcement, but they should put the glasses down. My position is that while I agree with NIST's assessment that SMS OTP is deprecated, SMS OTP isn't going away.

Why? Three reasons:

- On its own, SMS OTP still has value for low risk transactions
- It can be bolstered to mitigate shortcomings
- It is so broadly integrated across the industry (not quite like passwords, but you don't sunset something like this overnight)

Instead of tossing the baby out with the bath water, FIs should continue to consider a risk-weighted approach to authentication. Lower risk activities are safe in the near term, but any doubts around the suitability of standalone SMS OTP for use in higher risk transactions should be settled – banking Trojans and phone forwarding have long been effective in intercepting these messages. Supplemental forms of security can raise the level of assurance provided by SMS OTP – such as verifying the status of the receiving device or utilizing anti-malware to detect infected browsers where the OTP is to be entered.

So, will SMS OTP enjoy the same zombie-like status as "memorized secrets" (i.e., passwords – a solution that won't die, despite already being dead)? No, because it isn't dead (not even half dead for all you Billy Crystal fans). So if you use or are considering SMS OTP for OOB authentication, my suggestion would be stay calm and assess the situation. Examine the use cases, the inherent levels of risk, and how supplementing SMS OTP with other solutions affects the underlying ROI.

If you work at NIST on the other hand, I have a few suggestions for language around passwords that would really get everyone excited. But you have to mean it this time.

---

javelinstrategy.com inquiry@javelinstrategy.com 925.225.9100