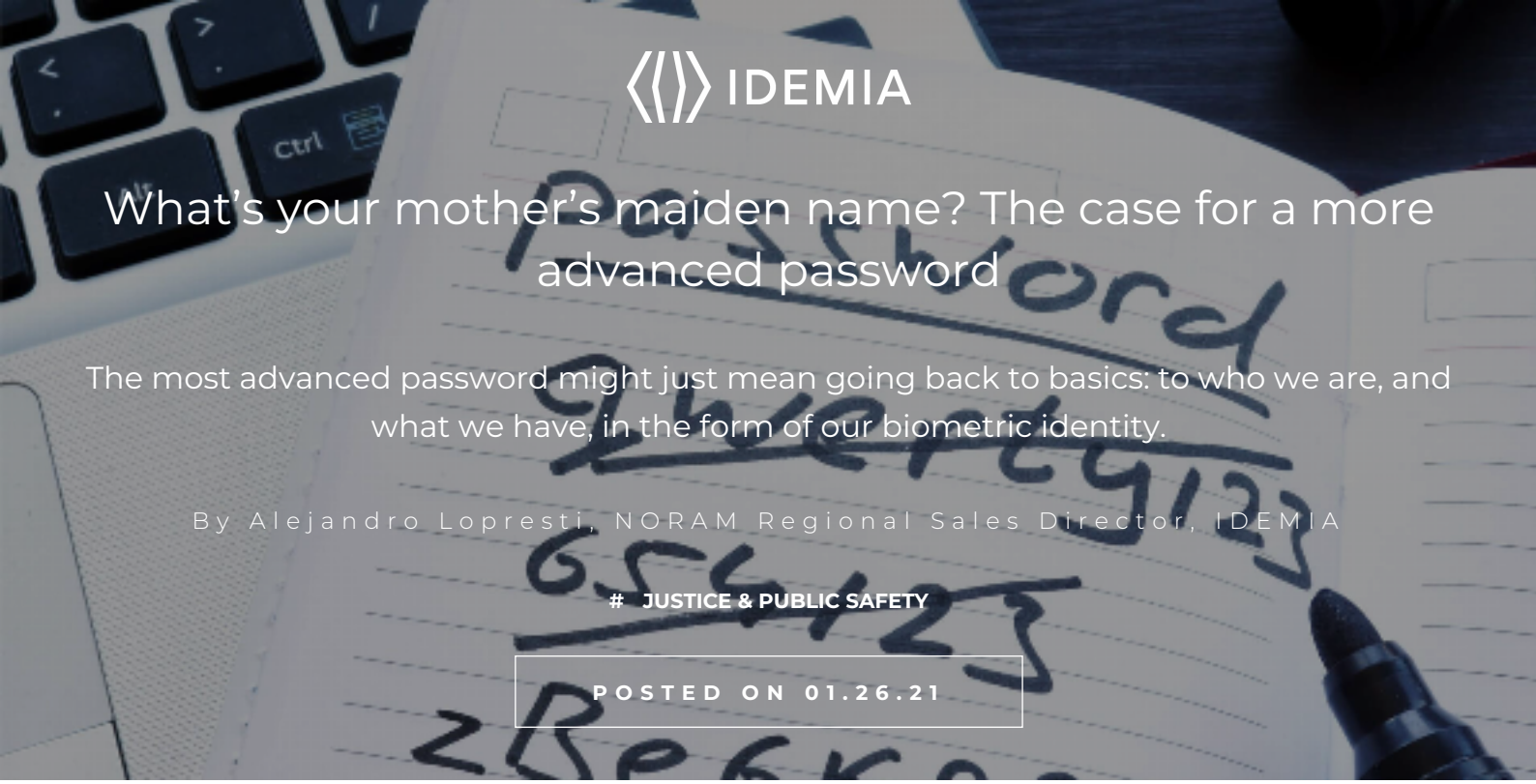


What's your mother's maiden name? The case for a more advanced password

The most advanced password might just mean going back to basics: to who we are, and what we have, in the form of our biometric identity.

By Alejandro Lopresti, NORAM Regional Sales Director, IDEMIA

JUSTICE & PUBLIC SAFETY

POSTED ON 01.26.21

The astronomer Carl Sagan once said, "You have to know the past to understand the present."

In a not too distant past, about 35 years ago, IBM deployed the first ATMs in Argentina. I remember that, at the time, the idea of walking up to a machine and being able to withdraw money at any time of day, using a four-digit number was such a revolution! Essentially, the ATM card and a user's four-digit PIN were part of an encryption process underneath the pad – and this was a really good example of a deep, broad, and secure authentication mechanism that could be used to provide a fairly simple operation for a customer.
That construct of ease of use was a driving force for business but… was it scalable?

Fast-forward 35 years, the reliance on passwords has shifted from a convenience to a liability, both in terms of security and customer experience. While back then, we were all fascinated by the practicality of using an ATM to withdraw money or pay a utility bill, such fascination with technology quickly plummets as authentication processes get more and more complicated. Ironically, as we continue to add measures to "secure" our passwords, the more we introduce security risks to customers and the organizations providing the endpoint capabilities. Why is this?

1 – **Passwords are everywhere**
The average person is required to perform 25 logins per day[1] – and each password is subject to various restrictions in reusability, length, character types, and reset policies. According to a 2019 Harris poll[2], 66% of Americans reuse the same passwords for their online banking, email and social media networks. The same poll also found that 75% of Americans have trouble keeping track of all their passwords.

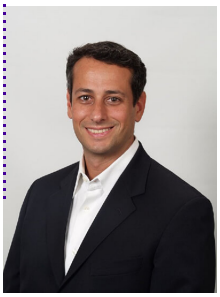
2 – **We have to note them somewhere**
With so many of us living in fear of forgetting our passwords or getting locked out of our accounts, we resort to basic solutions – writing it down. Ultimately, many digital asset are relying on the post-it stuck under our desks.

3 – **We often prioritize convenience over security**
As a result of this, many users prioritize convenience over security. In fact, statistics from the same Harris poll show that less than half of Americans (45%) change their password even after a data compromise or breach. When you consider that 75% of omni-channel customer-facing organizations will endure a targeted, cross-channel fraud attack, this creates a huge security risk for today's digital customer.

Furthermore, years of successive data breaches leaked customer's private information onto the dark web, becoming an attractive market for fraudsters. For example, NBC News reported[3] not too long ago that:

- Bank account passwords reportedly cost approximately $160.15;
- Airbnb and Uber credentials sell for an average of $8;
- A customer's entire digital profile can be purchased for just $1,200.

So passwords and challenge questions are not only frustrating for customers – they're ultimately insecure and vulnerable.



We can exchange knowledge, in the form of passwords, PINs, memorable data or personal details, but these verification methods come at a price, not least the loss of privacy, inconvenience, insecurity and identity fraud.

Alejandro Lopresti, NORAM Regional Sales Director, IDEMIA

Today, fraud, risk, and customer experience experts spend a lot of time wrangling over some key questions:

- How do I identify someone I don't know, can't see and isn't physically present without creating more friction?
- Can we replace big databases of users when we're exchanging shared secrets?
- Could we replace SMS verification and find a more reliable proof of identity?

The answer to these questions might just be going back to basics: to who we are and what we have, in the form of our biometric identity.

In my next article, I will go into some of the use cases for biometric authentication, and show why biometric passwords are a safer – and more logical alternative to traditional passwords.

---

[1] Microsoft Research. https://www.microsoft.com/en-us/research/publication/a-large-scale-study-of-web-password-habits-2/

[2] Google, in collaboration with Harris. https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf

[3] Dark Web Market Price Index (US Edition) by TOP10VPN
