IDEMIA

How do we finally say goodbye to passwords?

JUSTICE & PUBLIC SAFETY IDENTITY – NORTH AMERICA

POSTED ON 02.13.19

You've likely clicked that "forgot password" hyperlink far too many times to count. But industries have begun to respond to this consumer pain point by implementing secondary means of identification and in some cases replacing passwords all together. Given these developments, what is the future of passwords?

- With too many passwords to remember, we have adopted bad habits that render our tedious passwords useless
- Combining security and convenience are crucial in public and private sectors alike
- Constant innovation in biometrics and AI, and widespread adoption of the technologies, are changing user behavior and paving the way towards a password-free world

Passwords just aren't enough

Passwords are the most universal way to authenticate ourselves – requiring no specific equipment and providing a level of security that only the user should be able to unlock. Paradoxically, the password has become a victim of its own success. Instead of being the ultimate secret that protects us, passwords have become a hassle and often are no longer sufficient. Today, users can have as many as 200 passwords per person, leading many to adopt unsafe habits, such as using the **same password** for multiple sites (80% of millennials use the same password for all accounts) or creating **overly-simplified passwords** that are easy to guess. These unsafe habits render our **passwords useless**. And on top of it all, fraudsters are continuously inventing new ways to steal personal information.

Increasing security…

Our passwords grant us access to websites and services with varying levels of **security requirements**. While we can login to certain websites, such as social media or email using a claimed identity, i.e. without actually proving who we are, more **secure services**, such as banking or government sites, require a **verified identity**. In these situations, we must prove our identity with an official ID document at the enrollment phase in order to access these services. Service providers have also begun to integrate additional security measures such as **multi-factor authentication**; meaning combining at least two of the following: something we know (a password), something we own (e.g. our smartphone) and something we are (our **biometric data**). While it adds another level of security and protects highly sensitive transactions, multi-factor authentication tends to complicate the user experience.

Conveniently secure or securely convenient?

Security and convenience are crucial in public and private sectors alike; however prioritizing the two can vary. Governments, first and foremost, need to assure citizens that their identities are highly protected against fraud. So, while

they are willing to boost the convenience factor by digitizing services, security remains of utmost importance. For banks, e-merchants and mobile operators, a seamless experience that facilitates access to services and transactions is critical. Cumbersome security measures yield high abandonment rates, which can negatively impact business.

In both these spheres, **biometrics** is the best way to combine high security and a seamless user experience. We've already seen it create a virtuous cycle in the early days of smartphones. When users grew tired of unlocking their phones with a PIN code, many chose to leave their devices – and data – unprotected. Convenience was the key to changing user habits. With the massive adoption of **fingerprint scans**, users began protecting their device, and themselves, once again.

In banking and e-commerce sectors, the combination of biometrics with **risked-based authentication** techniques creates an even smoother experience. In this scenario, users are asked to prove their identity only when the transaction presents a real risk – for instance, an unusual delivery address or a particularly expensive purchase. In this case, what a more natural way to **prove who they are than a quick selfie** on their smartphone?

Advancements in Deep Learning and Artificial Intelligence (AI) algorithms can push the needle even further in the years to come. The mobile industry, for example, is investigating ways to make the authentication process even more invisible with **context-based authentication**. With explicit user consent, a service provider could for instance confirm a user's identity by analyzing their location and the unique way they swipe their smartphones – requiring zero additional effort on the part of users.

Towards a password-free world?

In the foreseeable future, passwords will still exist for specific scenarios such as account recovery operations; however their use will become significantly less common. In the coming years, as more devices integrate biometric and AI technologies, we could find ourselves in a (nearly) **password-free world** where your PC recognizes you (and only you) when you sit at your desk and where phishing threats are long forgotten. At IDEMIA, we invest in biometrics and AI to create highly secure and frictionless authentication solutions for the public and private sectors for a safer and password-free digital world.