

Goodbye passwords!

—

Pier Luigi Rotondo
Security Architect

 **@PGRotondo**

#ECSMPerugia
#CyberSecMonth



123456

The password dilemma

- Short passwords easy to attack
- *AS2-Y#!t9@-a1lMYp@\$* way more secure
- **Growing number of accounts**
 - Need to keep passwords distinct
 - Lost revenues due to forgotten passwords ^[2]
- Password-based authentication is under attack!

Goodbye passwords!

<https://www.youtube.com/watch?v=vcsGu9ug9J4>

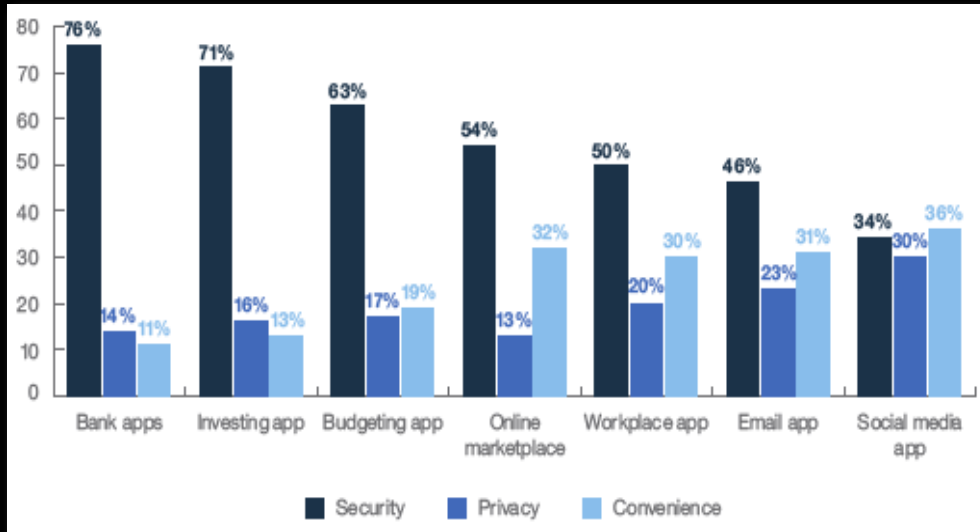
Welcome biometrics



A biometric characteristic

- No need to remember
- Always with you
- Fast and easy!
- More secure ... or at least this is what many people think!

How secure do you want to be?



Source: *Future of Identity Study 2018* - IBM Security



A screenshot of a login interface. On the left, there are three social login buttons: 'Accedi con Twitter' (blue), 'Accedi con Facebook' (dark blue), and 'Accedi con Google' (red). On the right, there is a form with an 'Email' field, a 'Password' field, and an 'Accedi' button. Below the form, there is a small disclaimer: 'Facendo clic su Accedi, accetto i Termini di Hootsuite, tra cui i termini di pagamento e Informativa sulla Privacy' and a link for 'Password dimenticata?'.

The right compromise



of respondents are comfortable using biometric authentication today.



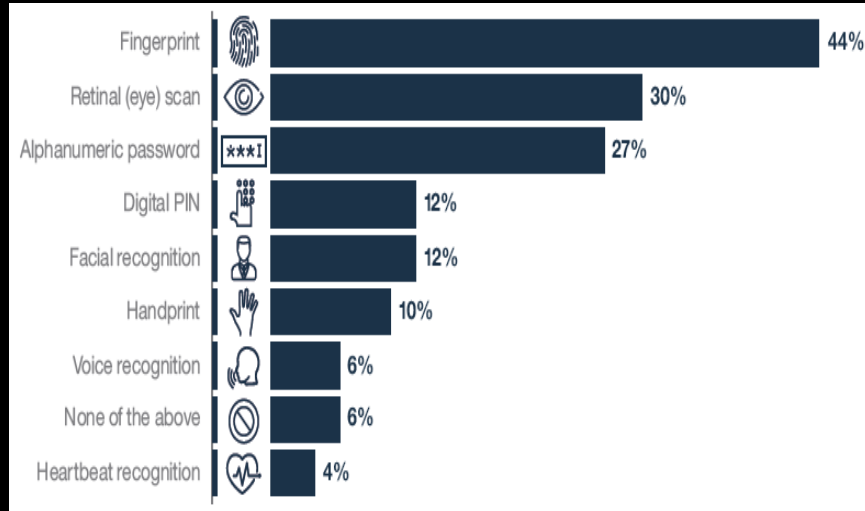
of respondents would consider using different types of biometric authentication in the future.



Source: *Future of Identity Study 2018* - IBM Security

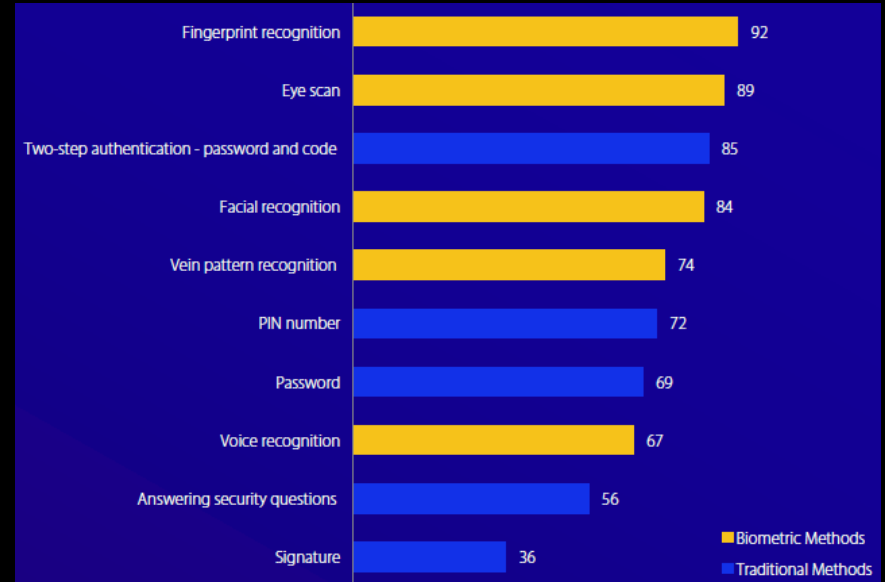
What biometrics

Authentication methods perceived as most secure



Source: *Future of Identity Study 2018* - IBM Security

Secure methods for authorizing payments

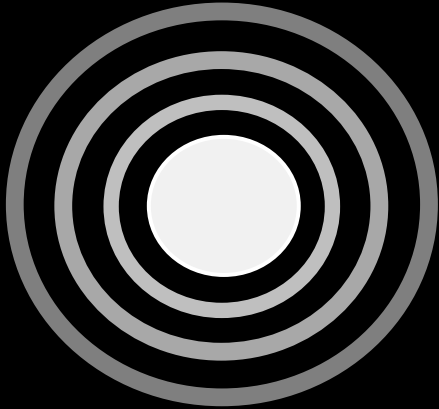


Source: *Goodbye, passwords. Hello, biometrics.* - VISA

How secure is
... biometric
security?

Multi-Factor Authentication (MFA)

- Multiple layers of defense
- *Visible vs invisible* authentication factors



Authentication-as-a-service (1/3)

1 Enrollment (once)

1.1 Device registration

1.2 Identity

> Watch the demo



Authentication-as-a-service (2/3)

2 Password-free login

> Watch the demo



Authentication-as-a-service (3/3)

3 Safer banking

3.1 Low value transaction

3.2 Medium value transaction

3.3 High value transaction
> Watch the demo



Conclusions

- Don't force your users. Engage them!
 - Manage user experience and acceptance, along with risks
- Make biometric authentication appealing
- One size fits all does not fit here
- Two is better than one. Especially when it comes to authentication!
 - And more is better than two!
- Risk-based authentication
- Behavioral biometrics

And your speaker is ...

Pier Luigi Rotondo

Security Architect



@PGRotondo



facebook.com/pierluigi@ibm



Thank you

Pier Luigi Rotondo
Security Architect
IBM Italia S.p.A.

—

pierluigi.rotondo@it.ibm.com
+39 335 7389699
ibm.com

References

- [1] L. Kessem *Future of Identity Study 2018* IBM Security, January 2018 - ibm.biz/FutureOfIdentity
- [2] *Goodbye, passwords. Hello, biometrics.* VISA, September 2017
- [3] J. Moar *3 steps to prepare for multimodal biometric payments* Juniper Research, March 2018
- [4] *About Face ID advanced technology* Apple Support, September 2018