Saying goodbye to passwords reduces vulnerabilities

Why in the world is everyone going passwordless?

For starters, passwords create major security risks, are considerably more expensive, and, quite frankly, can be really hard to manage.

Data breaches, phishing, and brute force attacks
80% of hacking-related breaches are caused by compromised credentials,
and 80% of hacking-related breaches are caused by compromised credentials.

Passwords are expensive
50% of help desk costs are made up of password resets.

Workforce login issues
90% of end-users report policy violations as the #1 reason for going passwordless.

39% of organizations mention regional compliance mandates like PSD2 (EU) and SCA driving the change to 2FA and biometrics.

What does the future hold for passwordless?

By 2022, 60% of large global enterprises, and 90% of midsize enterprises will implement passwordless methods in 50% of use cases.

By 2023, 30% of organizations will leverage at least one form of passwordless authentication.

The average user has 90+ online accounts and manages 80 passwords.

Password management solutions for mobile devices will rise to $28+ billion by 2025.

The 5 technologies

Here are the technologies security and risk management tech professionals can use to go passwordless right now:

FIDO

FIDO is leading the fight against passwords. Not only is it a secure alternative, but it also has high adoption across industries – with 500+ certified solutions and support across browsers and platforms.

Biometric

82% of users identify biometric approaches as a solution for passwordless. The biometric authentication market is expected to reach $93B+ by 2025.

Decentralized digital identity

With 60% of the global GDP expected to be digitized by 2022, the economy will be highly dependent on identity. Decentralizing credential storage using blockchain along with secure passwordless authentication is the way forward.

Mobile

Smartphones have been a driving force in bringing biometrics to the masses. Consumers expect biometric authentication for their most sensitive information, especially when it comes to mobile banking and payments.

Learn more about our passwordless solutions at entrust.com/go/passwordless-login

SOURCES

1 “Embrace a Passwordless Approach to Improve Security,” March 2019, Gartner

2 “Cybersecurity investment priorities for organizations worldwide in 2020,” March 2020, Statista

3 “Passwordless is the future,” March 2020, CyberArk

4 “Why hackers still need master passwords,” February 2017, ZDNet

5 “Thieves steal 40% of U.S. email accounts through phishing to steal passwords,” Security Magazine, March 2020

6 “Companies Move ‘Beyond the Password’ to Strong Authentication,” 2019 survey by ThumbSignIn, One World Identity (OWI), and Gluu

7 Verizon 2020 Data Breach Investigations Report

8 “Passwordless Authentication: The next breakthrough in secure digital transformation,” January 2020, World Economic Forum white paper

9 “Passwordless Authentication: Bridging the Gap Between High-Security and Low-Friction Identity Management,” June 2019, Enterprise Management Associates research report

10 Poor password management puts US companies at risk, onelogin infographic

11 Online Security Survey, February 2019, Google/Harris Poll


13 “The digital future we need,” January 2019, Reuters

14 “The future of finance is now,” January 2020, Reuters