Password-Less Authentication Offers Safety and Convenience

cyber security digital banking

Summary: A recent survey indicates that 89% of IT security leaders at financial services firms think authentication systems that use biometrics, push notifications, and other alternatives are more secure than passwords. Though CFIs will have challenges implementing password-free systems, the reward could be safer data and better customer satisfaction.

What being has four legs, then two, and then three? According to the myth of Oedipus, the wrong answer to this riddle meant becoming the Sphinx's dinner. It also meant that travelers could neither enter nor leave the city of Thebes, which the Sphinx guarded, until someone guessed correctly. The correct answer, given by Oedipus in the story, is "*man, who crawls on all fours as a baby, then walks on two legs, and finally needs a cane in old age.*" The Sphinx then jumped from a cliff, freeing the citizens of Thebes, and allowing visitors into the city once more.

Thankfully, modern password protection doesn't involve risking your life to get past a cryptic monster. In fact, there's really no cost to getting a password wrong, aside from the account getting locked temporarily for too many failed attempts. Unfortunately, that means it's just as low of a risk for password thieves and hackers attempting to access an account as it is for the account's rightful owner to get the info wrong. Actually, our lack of imagination with passwords can make figuring out our login credentials simple.

According to a survey conducted by Google and the Harris Poll, a quarter of us have used such easily-guessed passwords as abc123, Password, 123456, iloveyou, 111111, qwerty, admin, or welcome. If the hacker knows you personally, it's even easier. A third of us incorporate a pet's name into our passwords, 59% use our own names or birthdates, and about 15% use a spouse or child's name.

Sometimes outsiders don't even have to guess our passwords. Almost half of the study participants have told someone their passwords, and 55% don't bother changing their passwords after a security breach. Around 42% of organizations use sticky notes to manage passwords, which means that anyone can log on.

Community financial institutions (CFIs) have especially good grounds to dislike password-based authentication. Verizon's 2022 Data Breach Investigations Report says that bank data breaches typically involve stolen credentials. This includes every method from brute force hacking to credential stuffing.

Moving Beyond Passwords

Password-free authentication, which involves logging into a system using biometrics, a USB key, or an app on a trusted device such as a smart phone, is much more secure. Another recent survey showed that 89% of IT security leaders at financial services companies think password-free phishing-resistant multifactor authentication is the gold standard for authentication security, better than either passwords or traditional multi-factor authentication (MFA), both of which can be compromised by sophisticated hackers. The difference is that phishing-resistant MFA methods eliminate that more hackable MFA option of something you know, such as answers to security questions, pins, and passwords.

Community financial institutions (CFIs) that are interested in password-free authentication could have a lot to gain from making the switch. CFI customers care profoundly about data security; a survey by the analytics company Verint showed that security and fraud protection are replacing fees as the top reason that people change banks.

In selecting password-free authentication methods, CFIs have a variety of choices. For CFIs who use vendors for their mobile or website technology, their alternative authentication options will depend on the vendor's offerings.

Here are some of the most popular choices:

- **Push notifications** provide an authentication code on the lock screen of a mobile device such as a cell phone. The method is significantly more secure than texting the customer a code. Alternatively, a system can push a QR code that is then used to authenticate when a trusted mobile device scans it.
- **Biometrics**, which include face and fingerprint recognition, are already popular on a variety of devices, including laptop computers and cell phones.
- **FIDO (Fast Identity Online)** puts authentication responsibility on a trusted device, such as a cell phone.

All these options offer CFIs and their customers multiple benefits, including enhanced cyber security and convenience. Password-free authentication is faster than using a password, doesn't rely on memory or written (and therefore, easy to compromise) credentials, and often employs techniques with which customers are already familiar. Because of the enhanced usability and security, it could be helpful to your staff as well as your customers to investigate how you can adopt password-less authentication methods.

COMMERCIAL LOAN GROWTH AND FLOATING RATE ASSETS

Does your institution need fully-funded, senior secured floating-rate loans to diversify your portfolio? Learn about our C&I Loan Program to meet your loan growth objectives.

ECONOMY & RATES

Rates As Of: 11/10/2022 05:48AM (GMT-0800)

Treasury	Yields	MTD Chg	YTD Chg
3M	4.29	0.07	4.23
6M	4.59	0.02	4.40
1Y	4.55	-0.07	4.17
2Y	4.38	-0.11	3.64
5Y	4.04	-0.19	2.77
10Y	3.92	-0.13	2.41
30Y	4.19	0.02	2.29
FF Market	**FF Disc**		**IORB**
3.83	4.00		3.90
SOFR	**Prime**		**OBFR**
3.78	7.00		3.82