Passwords – Are Their Days Numbered?

cyber security risk management

Summary: Passwords have long been the chief method of authentication for users. Yet, the human elements of memorization difficulty and affinity for convenience coupled with the new risks of the work-from-home environment have pushed several financial institutions to consider two-factor authentication. Is it time for your institution?

Experts say that the best time for the brain to learn is between 10 a.m. and 2 p.m. and then again from 4 p.m. to 10 p.m. This timing could be helpful to know when learning new passwords. Yet, many bankers and experts alike are looking at other options for passwords as well.

Financial institutions have always been a top target for cybercriminals. But as online compromises have spiked the past year in the face of the pandemic, many experts are questioning whether the ubiquitous password is enough in securing work-based access.

The human element. Entering a user name and password is, without a doubt, still the most familiar and popular form of authenticating the identity of a device, system, or website user. But, even before the pandemic, some security professionals questioned if the use of passwords was secure enough. After all, it is well-documented that the weakest security link is the human, and employees have the greatest security control over creating their passwords. Hence, it's not surprising that eight out of 10 breaches are born out of stolen or shared passwords, according to the Verizon Breach Investigations Report.

Further, industry research continually finds that the most popular passwords even in business settings are easily guessed ones, such as "12345" or even "password." If employees are forced to set more complex passwords, they often reuse the same alphanumeric combinations at many business and personal access points, making them more easily compromised across various sites and systems. With the typical user needing to remember dozens of (often tricky or random) passwords, many employees resort to storing passwords sometimes in an obvious place — in a Word or PDF document, or on a Post-It note.

The WFH factor. With the pandemic forcing millions of people to work from home since last March, bank employees may be interacting much differently with their work systems and files, as well as with their colleagues and bank customers. These massive abrupt changes have exacerbated password weakness in three major ways:

1. in the wake of chaos, cyber-criminals and scammers have been much more aggressive, as much as **tripling fraud attempts** in 2020;
2. working from home has allowed (or encouraged) many employees to become **more lax in their security hygiene** and password practices; and
3. the isolation and stress of the lockdown, job loss fears, and illness concerns have driven people to desire greater connection, even at the risk of letting down their defenses and **sharing privileged information** (like passwords) more easily.

Two-factor authentication. In the long run, the most secure solution is likely to implement two-factor authentication (or 2FA for short), which could utilize a combination of two or more non-password means of

identity verification. These could include:

- sending a one-time password or code to a user's mobile device separate from their work PC;
- hardware tokens such as a physical access card (as most branches of government already use);
- captcha questions that use visual recognition to discern a real human user from an automated fake;
- biometrics, like fingerprint, iris or facial geometry recognition;
- using a series of security questions based on rarely shared information, such as the street you grew up on.

Advocates of password-less authentication appreciate seeing more financial institutions put 2FA in place for employees — especially now when many are still working from home and the threat level remains high. As long as passwords exist, experts believe they will continue to represent the most likely point of attack. At least one FL community financial institution (CFI) has moved its employees off passwords and onto biometric authentication — an increasingly popular alternative, particularly as the technology improves and decreases in cost. Last year, the pandemic compelled many CFIs to shift gears (and technology dollars) to support employees' pressing remote work needs. This shift may ultimately drive more CFIs to "by-pass" the oldest authentication of passwords for more secure alternatives in coming years.

OUTSOURCE ALM SERVICES AND REST EASY

Regulators have raised the bar on interest rate risk and liquidity analysis, yet there is more to do than there are hours in a day. To see how easy it can be & get expert help, contact us today.