Password Limitation in Online Banking Domain

Online banking has become an essential part of everyday life. For many consumers, this means clicking into the application with something as simple as a face ID or password. However, consumers are limited in their options for passwords. The password to gain access to the records must present a capital letter, numbers, and hold no characters. Passwords that contain all numbers or symbols are not accepted. In the case of a forgotten password, a password used in the past is unable to be used and further limits the individual's ability to craft a new password. In addition, the password must not contain sensitive information such as customer information, answers to security questions, and passwords below a certain character limit. This password experience becomes an issue when a consumer repeatedly attempts to change their password due to their inability to recall the original password. Consumers then choose to create a simple password that will be easier to remember and weakens the strength of security. In limiting the password characteristics, the banking companies make an attempt to improve security, but the actual result is an easily hacked security system.

References

[1] D. M. K. L. H. Judith Gebauer, "Password Security Risk versus Effort: An Exploratory Study on User-Perceived Risk and the Intention to Use Online Applications," *Journal of Information Systems Applied Research ,* vol. 4, no. 2, pp. 52-62, 2011.

[2] N. N. S. T. Himika Parmar, "Generation of Secure One-Time Password Based on Image Authentication," *Computer Science & Information Technology (CS & IT),* vol. 1, no. 1, pp. 195-206, 2012.

[3] M. H. B. B. Viktor Taneski, "Systematic Overview of Password Security Problems," *Acta Polytechnica Hungarica ,* vol. 16, no. 3, pp. 143-165, 2019.

Hypothesis

With strict password requirement linked to online banking, consumers are able to choose to create a password that is completely personalized to them with the addition of certain requirements. However, many consumers are often unable to remember their passwords, thus using features such as Touch ID or Face ID. In addition, companies tend to put restrictions on the passcodes to improve overall security. The current solution to the issue of banking passwords is to use security questions as a way to help the user remember the complex password. This differs from my solution because a recent study showed that most participants in the study were able to answer the security questions for other people in their inner circle. This decreases the overall security as the users are now able to gain access to the application by answering the questions. I believe that by reducing the strict passcode rules and requirements, the consumer will remember the passcode. But lessening the requirements will weaken the password security. In order to address this issue, I propose a 2-step authentication to bridge this gap. The two step process would allow the consumer to authenticate their identity through using a secure server that utilizes push. In order to increase security, a third-party application should be used to hold information in a separate database or server outside of the banks application or network. My solution will fix this problem by using the 2-step authentication method. Consumers will no longer struggle to use access their account with a complicated password or fear for their information with a weaker one.

References

[1] A. Moallem, "Did You Forget Your Password?," *Lecture Notes in Computer Science ,* vol. 6770, pp. 29-39, 2011.