

# Two Factor Authentication: What is it and how do I get it?

Geoff Humes, Principal, Vulnerability Research & Analysis Digital Defense, Inc.

During the month of October, the FFIEC issued guidance titled Authentication in an Internet Banking Environment\*. This guidance document updated the previous document titled Authentication in an Electronic Banking Environment, released four years earlier. This new guidance outlines specific requirements for multi-factor authentication where high-risk transactions occur in an electronic format, and furthermore discusses various methods for implementing multi-factor authentication.

In their guidance document, the FFIEC states that single-factor authentication is not adequate protection for access to customer information or funds transfer transactions. This new guidance document differs from the older document in that the older guidance **recommended** multi-factor authentication and this guidance **requires** it for these types of transactions.

## What is Multi-Factor Authentication?

Multi-factor authentication at its most basic level means using more than one of the three types of authentication which are:

- Something you know
- Something you have
- Something you are

A combination of these types of authentication can form multi-factor authentication, or duplication can form single-factor multi-tier authentication.

The idea of multi-factor authentication is not new to the financial institution industry. When a member enters a branch to conduct a transaction, they must provide their account number (something you know) along with some form of identification such as a driver's license (something you have). Requiring members to provide a password (something you know) and a PIN (something you know) is not multi-factor authentication because this method of authentication relies only on knowledge of data. Requiring members to provide multiple instances of the same type of authentication (multi-tier) provides improvement over a single instance of authentication but fails to meet the requirements of the new FFIEC guidance. Some proposed solutions may advertise compliance with this guidance but use multi-tier rather than multi-factor authentication, so it is important to evaluate any proposed solution for its compliance with multi-factor authentication. Compliance with this guidance will ensure nearly the same level of protection to internet banking transactions that in-person transactions currently require.

## How Do I Implement It?

To implement a solution that is compliant with this guidance, there are a few steps to follow. First, you should conduct a risk assessment that clearly identifies the risk posed to both the member and the institution by the available Internet banking systems. Only by first understanding the current risk posed by these systems, can you gauge the effectiveness of any improvements. After the completion of this initial risk assessment, you should address mechanisms to improve to the security of the Internet banking systems. At this stage, it is important to consider general ideas such as intrusion detection/prevention systems, secondary authentication, or even firewalls rather than a specific vendor's version of a product. Once you have made the determination regarding the general improvements that you should put into action, it is time to look at the specifics of implementation. This two-step process to determine improvements is necessary because it is too easy to be overwhelmed with the myriad of "security products" available today without at least a general idea of the type of improvements that would be the most beneficial.

Many financial institutions either outsource existing Internet banking applications to third party vendors or house them at the institution as proprietary applications from one of many vendors. In these instances, the onus will be on the third party vendor or the application developer to recommend a solution that will satisfy these new requirements and will not affect any existing functionality or contracts. However, auditors will still look for compliance with this guidance from the institution, not the external vendor, which means that the institution must still show that they are making progress toward the end goal of multi-factor authentication.

## Is There Anything Else I Should Consider?

This new guidance document also states that any authentication system currently in place or planned as an improvement should have auditing capabilities. The goal of this capability would be to protect against unauthorized access to computer systems and member accounts. While evaluating proposed solutions that incorporate multi-factor authentication, it is imperative that this auditing capability is available. Once instituted, it is just as imperative that you use this capability.

## What about My Members or Customers?

Finally, the document recommends that financial institutions employ an effort to educate their members. Furthermore, it recommends that institutions evaluate the effectiveness of this education program by comparing metrics on several member actions such as reported phishing attempts, usage of information security links from the institutions public web page, or even the dollar amount relating to losses incurred from identity theft.

## In Conclusion

You may at first view the implementation of multi-factor authentication on Internet banking systems as a daunting task, but with careful investigation and evaluation, it can provide a more secure environment for financial institutions and their members or customers. There is and will continue to be many different implementations to reach this goal, and many different opinions on which specific implementation is "the best", but only through a process that determines your risk and your goals can you discover which solution is the best for your needs.

\* Guidance available [HERE](#)