



# Security: Which Two-Factor Works Best?


As the risk of account hijacking and Internet fraud have grown, the Federal Financial Institutions Examination Council has recommended that financial institutions establish two-factor authentication, which uses a challenge/response methodology to help lessen vulnerabilities during online transactions. Two-factor authentication comes in many forms and numerous levels of security.

When you visit a typical online banking application, you are prompted to enter your user name and a password. However, this approach does not offer the most secure solution. Consider the rise in phishing scams: users are tricked into typing their user name and password into a malicious website that records the information. That information is then used by the owner of that malicious site to gain access to the real account.

Some claim that even with two-factor, an account could still be breached through a man-in-the-middle attack. This is where a malicious site catches all the data entered while allowing it to pass to the real destination. Then, once a user has passed the point of login, the malicious site in the middle takes over the communication completely and drops the real user. In reality, however, this type of attack is far less common than phishing and significantly more difficult to perform, especially in large volumes.

The real issue with two-factor authentication is not if it works, but which product is best. With so many products claiming to offer two-factor authentication, it can be difficult to understand which to choose. As with any technology, some versions are simple to use while others are so confusing they become more of a liability than an asset.

When considering two-factor authentication, you should be mindful of how you will deploy and manage the product. For example, if a credit union with 30,000 members chooses a solution that requires a token or key fob, they will have to send that device out to each of those members and then manage and maintain those devices when they expire, the battery dies, or are lost, stolen, or broken. Yes, it's proven, but is it worth the cost?

Ultimately, when selecting a provider of two-factor authentication, your credit union should take price, management, deployment, and customer satisfaction into account. It is not a one-size-fits-all. TraceSecurity is a provider of enterprise-class vulnerability management solutions and security assessments, including two-factor authentication. For more information, contact Candy Sims at 800.472.1202, ext. 3401. 

## Fulfilling Your Diverse Technology Needs TAKES A NUMBER OF PROVIDERS.



**That number is one.**

The task of trying to interface all the technologies required to run your credit union can be inefficient and expensive. When you partner with Fidelity National Information Services we'll deliver a suite of products to seamlessly handle all your needs. We offer a range of core processing solutions plus business intelligence, card services, item capture and imaging, EFT and debit services, eBanking and fraud solutions.

**Be efficient.**



FIDELITY NATIONAL INFORMATION SERVICES

[www.fidelityinfoservices.com](http://www.fidelityinfoservices.com)  
877.482.8786

Serving credit unions from the millions to the trillions.

