What is Multi-factor Authentication?

Multi-factor authentication is the process of requiring more than one method of identifying and validating a person’s identity before granting access. Multi-factor authentication requires using at least two of three categories of verification factors. The categories include: what you *know*, what you *have*, and who you *are*.

Reasons to Implement Multi-factor Authentication

Implementing multi-factor authentication adds an additional layer of security that further protects a firm from unauthorized access or data breach. Multi-factor authentication is implemented to:

* Reduce the risk of data breaches
* Assure clients of data security
* Satisfy regulatory requirements

Best Practices to Avoid Data Breaches

## To prevent unauthorized access to the network, know and follow firm policies on network access.

## Use secure passwords or passphrases as a first line of defense in preventing data breaches, as doing so strengthens the process of multi-factor authentication.

## Take the necessary steps to add multi-factor authentication to your social media and online accounts. Many of the leading online services offer multi-factor authentication.

## After connecting to a secure Internet site, verify that you are at a trusted site by clicking the lock icon located to the right of the site’s URL address to view the VeriSign certificate.