

## Two Factor Authentication

These days spending time online can be dangerous regardless of whether you're a private individual checking things out at home or the proprietor of a business. Admittedly there is more potential danger and loss to be had by a business who operates a network that stores client and business sensitive data. If this same company also has employees using the internet and email for any reason this opens the network and your data to even bigger and more damaging threats.

Danger has always lurked just around the corner for those who enjoy spending time online and since the inception of the Internet there have been various companies out to prove that they provide the very best in online security both for businesses as well as for the private sector. As someone who's been using the Internet for the better part of fifteen years I can tell you that there are very good, middle of the road and very bad security programs available through different vendors.

The one portion of online security I find disconcerting however is the oversight many of the larger publishers have when dealing with the common computer user. The typical computer owner knows how to do little more than open a browser and peruse a few favorite websites. With the majority of people falling into this category I often wonder why security programs are continually churned out that are overly difficult to use, have poor interfaces, or require extensive computer knowledge to use. Businesses really aren't affected by this however as they hire knowledgeable professionals who come to work already educated about such things.

Having spent the last couple of weeks researching online security programs I came across [Two Factor Authentication](#) which in layman's terms ups your online security and protects valuable and private data by using a digital fingerprinting system to determine what is and isn't safe and/or legitimate for you and any business who might use such security. This type of security can keep those individuals interested in practicing unscrupulous activities from doing so which in turn keeps valuable information safe.

Interestingly enough a few of the companies I looked into offered Two Factor Authentication services that required no tokens and required no installation of additional servers. I can see this as a big selling point for those businesses who might be interested in keeping their sensitive materials out of hands that might do harm, such as a man-in-the-middle looking to pull off phishing attacks. I was further surprised to find that some companies offer this type of security making use of retinal scans though I found these to be much more expensive than those utilizing fingerprints and the like.

So just how much security do you need? That's actually a matter of how big your business is and how many people have access to the data and equipment you want protected. Should everyone with access actually have those privileges or do they have access simply because you don't have the time to implement these types of security features? There's no price you can put on security and peace of mind so those of you who may not have yet to look into Two Factor Authentication security should do so.

## About the Author

Scott is an avid tech enthusiast who has recently become aware of the importance of [Two Factor Authentication](#).

Source: <http://www.articletrader.com>