



BRINGING NEW TECHNOLOGY TO YOUR BUSINESS

CoreTechs Consulting, Inc
4303 Clearbrook Lane
Kensington, MD 20895
301-949-2553
contact@coretechs.com
www.CoreTechs.com
 @CoreTechs_Inc

Could your company benefit from securing some of its resources with two factor authentication?

Data Security

Company's are increasing the information they collect from consumers at a rapid rate. Securing that data, as well as other privileged and business-essential information, is critical to ensuring that your business' information is safe.



Two Factor Authentication

The Background

Two factor authentication is a very broad name for any form of authentication requiring more than just memorized data. In the simplest form of authentication to a system, a user needs only one factor to prove they are who they say they are, generally a password. With this username and password a user is able to log in to whatever system that pair works for. The inherent problem with one factor authentication is that there is little or no way to tell if someone other than the intended user is logging in with the credentials presented. This is where two factor authentication comes into play.

The Details

True two factor authentication requires both something you know, such as a password and a second form of authentication. This second form is generally something you have, such as a code generating token or cell phone application; or something you are, such as a fingerprint or other biometric

scan. Requiring one of these pieces to log in makes it more difficult for unauthorized users to gain access to a system, because doing so requires not just virtual theft of a password, but real world theft as well.

Real World Application

Using this method of authentication to a system has caught on in recent years due to ever more intelligent password collecting scams and malware; but two factor authentication itself is nothing new. You probably use a two factor authentication system fairly often, if you ever visit an ATM. The first piece of authentication is your PIN, something you know. The second piece of authentication is your ATM card, something you have. For an unauthorized user to obtain access to your ATM account they would need not just your password data, but your physical ATM card. Imagining how this system works with an ATM is easy: no card – no access; no PIN – no access either.



Data thieves will look for the easiest systems to access. Adding additional security to your systems can keep them at bay.

Computers don't generally have ATM card slots, so the second factor has found a few other forms for laptops and desktops. So far, the most popular second factor has been an ID token. This token displays a four to ten digit code that the user types in as a second password. Unlike a users' primary password however, this one changes – constantly. There are two main types of token: one of them displays a password based on the current time, calculated using a large internal algorithm. The second type calculates a password based on the push of a button.

Every button push or time interval yields a new password in an order that only the token, and its corresponding software or hardware know. Knowing the current token password is useless to an unauthorized user, as the time based password will expire within a minute or so, and the button based password can generally only be used once. This is why two factor systems are so secure, a user needs physical possession of a token to gain access, even after knowing a user name and password.

Controversy

Some detractors say that the best way to protect data is to make it accessible only from a few set

places, and put tighter security around those physical places. While this is a great way to protect access to a system, two factor authentication systems are popular for protecting email, work applications, and data storage servers that a group needs accessible from anywhere, not just a set place.

“Two factor authentication can help make a system more secure”

Conclusion

While no security system is perfect, it is easy to see how two factor authentication can help make a system more secure, while remaining accessible from anywhere it needs to be reached from. Two factor systems allow companies and individuals to access data and systems from anywhere while keeping access to their systems more secure than is possible using only a basic username and password.

Next Steps

If you'd like to try out a basic two factor system today, why not try updating your Gmail account to use a cell phone generated pin today, just by going [here](http://bit.ly/o5ZSx7) (<http://bit.ly/o5ZSx7>) If you have something a bit more complex that is in need of some security, feel free to give us a call or [email us](mailto:emailus) (contact@CoreTechs.com) today, and we'll provide you with the help you need.



CoreTechs Consulting, Inc
4303 Clearbrook Lane
Kensington, MD 20895
301-949-2553
contact@coretechs.com
www.CoreTechs.com
[@CoreTechs_inc](https://twitter.com/CoreTechs_inc)