PacStates
Integrated Business Technology
One Company, One Call

Multi-Factor Authentication and its Benefits.

According to the TeleSign corporation, 54% of consumers use five or fewer passwords to secure all of their accounts. This is highly problematic, especially if a cybercriminal breaches one account, a domino effect will occur. One after another, all accounts that use the password will be breached, and all of the information stolen. This is where Multi-Factor Authentication (MFA) comes in. MFA is an additional layer of protection for your data. It utilizes an extra step when signing into your accounts, whether it is the system sending a one-use unique security code to your number or having a special PIN (Personal Identification Number). It is this added layer of security that makes hackers' lives exceedingly difficult as they have to take a lot more time and risk to get around the protection, most of the time they will move on to an easier target.

You may not realize it, but you use MFA on a daily basis. Every time you access an ATM with your card and enter your PIN is one of the most common examples of MFA. Another example is security questions that only you would know. For example. favorite teacher in middle school, father’s middle name, etc are another layer of protection that should be kept private for your protection. MFA can also be in a biometric form such as fingerprints or retinal scans. The two branches of MFA are "Who you are" (biometrics, your knowledge, etcetera.) and "What you have" (trusted devices, and key cards).

MFA will make your accounts more secure, although they are not impenetrable. Most companies are required to use MFA on their more critical data such as social security numbers, employee information, client data, etcetera. This protection is necessary for compliance with several federal regulations. It is important to note that even though you utilize MFA, you need to train your employees on how to use it properly, and why it is imperative to the company safety. There is always some form of user error that can cripple a system, and that comes from a small mistake, such as conducting business on an unsecured device or clicking on links in phishing emails.

There is still a chance of user error with MFA; however, it is significantly less probable. Some companies opt to use an application that either texts the account holder a code or another that the user must download onto their phone, which authenticates through similar methods.

If a user receives a sign-in notification but did not request one, then they must report it to your IT admin swiftly to prevent a data breach. Hence the importance of proper training for your full staff, on a regular basis. It is important to ensure that your employees know what to expect from the beginning of an attack, what to do if any situations arise, and how to prevent them in the first place. It is also essential to train them on the type of data that could be at risk if a breach does occur.

PacStates experts are always available and happy to answer any questions and if you need assistance we can take care of setting up an MFA system that works for your company.

Join our vCIO Ryan Baskharoon to review Safe practices and how to properly change your passwords in our Early Risers education webinar which occurs every fourth Thursday at 7:30am. (link this to our events page)

Give us a call for your stress-free conversation around any IT or technical issues and which MFA system will work for you. For over 30 years, we have been Northern Nevada's top "One Company, One Call" Integrated Business Solutions provider. We look forward to providing you solutions for your company.