PALMTECH
I.T. SOLUTIONS FOR BUSINESS

THE PALMTECH TIMES

PalmTech Computer Solutions | January 2022

This monthly publication provided courtesy of Chuck Poole, CISSP, CEO of PalmTech Computer Solutions.

Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.

The Best IT-Related Resolutions For The New Year

The past couple of years have been difficult for just about everyone. Business owners and entrepreneurs have had to adapt and evolve to survive in an ever-changing climate. There's no telling when or even if things will go back to what we once thought was "normal." As we enter a New Year, many business owners are putting their resolutions in place to survive and hopefully thrive in 2022.

People will focus on plans for growth and ways to bring more profit in for their resolution, but it's important to include tech- and IT-related resolutions as well. Technology might not be an obvious approach to growing a business, but it goes a long way toward making your clients and employees feel more secure about everyday interactions. This can inadvertently lead to growth as you improve customer relationships as well.

Here are a few tech-related resolutions that we think can greatly improve any business.

Use Multiple Layers Of Cyber Security Protection - There is no security approach that covers every hole or flaw that cyber security threats are looking to exploit. The best way to keep your defenses protected is to put in place multiple approaches to cover every possible gap. By using multiple programs and layers, you will ensure that every individual component of your cyber security program has a backup to counter any issues.

Your first line of defense should be a firewall. Firewalls help monitor incoming and outgoing traffic and work as a barrier between networks you trust and don't trust. They essentially shield you from malicious or unnecessary network traffic. Multifactor authentication is an important layer as well. This prevents cyber-attacks that come from weak or compromised passwords. With multifactor authentication, you and your employees may have to receive

continued on page 2

a text to your cell phones to prove that the correct person is trying to access the network. This will help prevent the use of employee passwords to gain access to sensitive information.

Back Up Your Data And Replace Old Equipment - Unfortunately, preventive measures don't always work. An unexpected disaster could cause your network to go down or someone could accidentally delete some important files. Plus, if your data is not backed up, you could lose sensitive information as well as time and money down the road. Customers will also be upset if you lose information pertaining to them. This could devastate your brand's reputation and cost you customers. If you do not have a backup plan or program in place, you should definitely get one for 2022.

In addition to backup plans, it's important to have equipment that is up-to-date. Using slow and outdated technology can take away from productivity and will make your job more difficult. If some of your equipment goes down, think about replacing it with something new rather than repairing it. While it might be more expensive at first, this decision will save you time and money in the long run.

Employee Security Training - If you want to run a cyber security-aware business, you'll need to train your employees

> **"If you do not have a backup plan or program in place, you should definitely get one for 2022."**

in security awareness and create a culture that ensures information security. Providing your employees with training related to information security can make them more comfortable and confident in their decision-making and overall employment. This rubs off on your clients and makes them feel more comfortable about doing business with you. According to information from the UK Information Commissioner's Office, human error is to blame for 90% of cyberdata breaches. Getting your employees trained in cyber security awareness can help reduce the chance of human error.

As you lay out plans to make your business more successful throughout 2022 and beyond, ensure that your tech and information security practices are updated. There are simply no downsides to improving your technology and cyber security. Adopting these practices can go a long way toward making your employees and customers feel more comfortable and confident in their decisions. **Our team at PalmTech will be happy provide you with the guidance necessary to secure your business. Contact us at 561-969-1616.**

Hackers dedicate time EVERY week to keeping up with security news, trends, and technologies

Are your employees doing the same to stay one step ahead?

Call us about Security Awareness Training for your staff!
(561)969-1616

Are Your Employees' Credentials For Sale On The Dark Web?

Visit www.palmtech.net/darkweb/ For A Free Scan!

Don’t Give Up On You by Mike Michalowicz

As you venture through your business and personal life, you’ll have people tell you “no” or that your ideas aren’t good enough. But remember: you know your goals, dreams and aspirations better than anyone else, so why would you let their opinions have an impact on your vision? I certainly wouldn’t be where I am today if I had listened to all of the naysayers and critics. If you have a dream, don’t let anything hold you back from accomplishing it.

After I wrote my first two books, *The Toilet Paper Entrepreneur* and *The Pumpkin Plan*, I approached my publisher and said I had written another book: *Profit First*. They looked it over and said, “Nobody needs another accounting book.” I was a little stunned, but I wouldn’t let that stop me.

I knew that I had a really strong book, and my mentor at the time told me to “make them regret it,” so I doubled down and decided to publish *Profit First* myself. It ended up being a roaring success. I sold so many copies that my publisher reached out to me about buying the book after they had rejected it the first time!

We made a revised, extended edition for Penguin Books, and it is definitely my most popular book to date. If I had listened to my publisher the first time around, I never would have made *Profit First* or any of the other small business books I have written since then.

I get calls and e-mails all the time from small-business owners who have improved their businesses through things they learned in *Profit First*. All of the money these businesses saved and the lessons they learned from *Profit First* never would have happened if I have given up on my goal.

If you come up with a product, service or idea that you think can help people in any regard, try to push forward through any negativity or criticism. Critics don’t always see the big picture and may use preconceived ideas to form an opinion about your business or idea. If you think you are on the verge of something great, don’t let anyone or anything stop you from pursuing your vision. You absolutely cannot give up on yourself. Push on and continue chasing your dreams.

Mike Michalowicz has always believed that he had the formula to success and has proven it on multiple occasions. He is the creator of the book Profit First, *which is used by hundreds of thousands of companies across the globe to drive greater profits. Mike is a former small-business columnist for* The Wall Street Journal *and served as a business makeover specialist for MSNBC. Mike currently leads two new multimillion-dollar ventures as he puts his latest research to the test.*

How Can Identity & Access Management Benefit Your Organization?

Every technology you use — whether it's a cloud-based program, a mobile application, or on-premises servers — contains sensitive business data vital to conducting operations. So how can you ensure the security of such data from cyberthreats like identity theft, phishing attacks, and other forms of fraud? Identity and access management (IAM) is the answer to this.

What Is IAM?

Identity and access management is a system that secures, stores, and manages user identities and access privileges. It ensures that users are who they say they are and will grant access to applications and resources only to those who have permission to use them. System administrators can enforce this system to give employees access to only the apps and data they need for work.

Other solutions that go into IAM include single sign-on (SSO) and multifactor authentication (MFA). The former allows users to securely log in to multiple applications that they are authorized to access. Meanwhile, MFA sets an additional method of user verification other than passwords. This includes fingerprint scans, facial ID, or a one-time security code sent via SMS.

These security solutions are designed to protect digital assets even if users attempt to access company accounts through mobile devices and the cloud.

Centralize Access Control

Too much access to certain systems is risky, while too little can hamper productivity and frustrate users. IAM strikes the perfect balance by letting you set centralized policies for the right access privileges. For example, you can deny your design team access to the accounting system while granting it to your CFO.

Each user's role and attribute can be used to determine which resources they're allowed to access and to what extent. This not only offers better security, but also more flexibility and ease of management.

Lower Chances of Data Breaches

With SSO and MFA, your employees will no longer have to remember multiple passwords. Instead, they'll be able to prove their identity using evidence-based authorization such as answering a personal question that only they would know. IAM also comes equipped with advanced encryption tools to protect sensitive data, reducing the risk of compromised user credentials.

Improve User Experience

Customers today interact with your company across multiple channels, whether in the cloud or via third-party applications. This is where IAM helps provide a better experience through SSO, self-service capabilities, and unified customer profiles that make communication processes quick and easy.

Your employees, on the other hand, will be able to access the information they need securely and conveniently no matter where they are. This means productivity will no longer be confined to their office desk.

Achieve Regulatory Compliance

Businesses today must meet the constantly changing regulatory requirements concerning data access governance and privacy management. IAM was designed with exactly that in mind and provides control over who can access data and how it can be used and shared.

Reduce IT costs

IAM automates and standardizes many aspects of identity, authentication, and authorization management. This means you'll be able to minimize significant labor costs associated with keeping your business environment secure.

An identity and access management solution equips you with much-needed security without compromising on usability and convenience. To operate in a digital business environment, it's not a matter of if but when you'll adopt IAM within your company.

If you're looking to enhance company-wide security, whether with IAM or other solutions, why not give us a call? We're sure we can help. Email us at info@palmtech.net or call us at 561-969-1616.