PALMTECH
I.T. Solutions For Business
THE PALMTECH TIMES
PalmTech Computer Solutions
June 2022

Entrepreneurship Secrets: Beginner's Guide To Running A Successful Business

By Abdul Vasi

When you're first starting out on your entrepreneurial journey, you're probably looking for help and advice at every opportunity. Throughout the first few years, you'll come across challenging and unexpected situations. It would help to have a guidebook during these instances, and that's exactly where Abdul Vasi's Entrepreneurship Secrets comes into play. From employee management to setting the proper organizational goals, Vasi takes you through some of the most common problems that plague new business owners and entrepreneurs while giving you guidelines for how to handle each situation. With Entrepreneurship Secrets in your back pocket, you'll be ready to tackle any decision that arises during you first few years with your new business.

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.

How To Prepare For Gen Z In The Workforce

Be Proactive And Update Your Cyber Security Practices

Technology has evolved leaps and bounds over the last 20 years. In fact, in the next few years, the first generation to grow up with smartphones and social media, will join the workforce. It might seem like Generation Z will be the most cyber-secure generation, considering they've always had the Internet and other advanced technologies at the tips of their fingers, but reports are starting to show that this is not the case. Many business owners fear that Generation Z's desire to share content online will lead them to accidentally reveal sensitive information that can cause financial, legal and branding damage to their business.

Online scammers have surely taken note of the power that social media influencers have over their fans and followers. Steve Durbin, CEO of the Information Security Forum, believes that organized criminal groups will begin posing as influencers in an effort to manipulate tech-dependent individuals into giving up sensitive information related to their employer. He's not the only business leader who's concerned either.

According to a study from the UK's advisory, conciliation and arbitration service, 70% of surveyed managers were concerned about Gen Z entering the workforce. Instant gratification, resistance to authority and poor face-to-face communication were listed as the main concerns. Additionally, Entrepreneur magazine has stated that many Gen Zers struggle to differentiate between friends they've made online and those in the real world. The National Cybersecurity Alliance's Annual Cybersecurity Attitudes And Behaviors Report stated that millennials and Gen Zers are more likely to experience a cyberthreat. That report also stated that Gen Zers and millennials have had their identities stolen more often than baby boomers. There's good reason for

continued on page 2

business leaders to be concerned about the next generation entering the workforce.

If you’re a business leader who’s worried about cyber security and bringing the digital generation into your workplace, don’t fret quite yet. There are plenty of things you can do to prepare your business and ensure it stays cyber-secure. You must be proactive if you want your company to keep up-to-date with the best cyber security practices.

One of the first things you’ll want to do is implement or update a cyber-security training program. You need to have every member of your team buy into a cyber-secure culture, and the best way to get them on the same page is with a training program. That way there will be no questions, and cyber security practices won’t change from employee to employee. When new employees start, you will already have a cyber-secure culture established, so it will be much easier to train them on your processes.

Additionally, you want to ensure that all of your software is receiving its necessary updates. Failing to update software can leave your company vulnerable to cyber-attacks since those updates usually fill any holes that hackers can exploit. When a new software update is released, try not to wait. If your employees use smartphones for work, make sure they have the proper security software installed – and that it stays updated.

> **“When new employees start, you will already have a cyber-secure culture established, so it will be much easier to train them on your processes.”**

Another great option to take care of all of your cyber security and IT needs is to hire a managed services provider. With an MSP, your business will have its data backed up, the reliability and quality of your computer systems will be improved and you’ll save time that you can reallocate elsewhere in the business. There’s no better or more affordable way to improve your company’s cyber security than by hiring an MSP to take care of all of your technological needs.

While the new generation will certainly come with their own set of challenges and obstacles, you don’t have to worry about their cyber security practices if you’re proactive. Use password managers, hire an MSP and start a training program as soon as possible to jump-start the creation of your cyber-secure culture. We’ve introduced new generations to the workforce many times before, and Gen Z shouldn’t be more challenging than any of the others. There will just be slightly different challenges.

Phishy Social Media Quizzes

Quiz Time! If you have ever used social media, you have probably seen a “quiz” like the one below.

Which pet should you get? Answer these questions to find out:

- Have you ever traveled outside of the country?
- What town did you grow up in?
- Who is your favorite fictional character?

Now it’s time for your results: You got... **a phish**! That’s right, the answers to these simple questions could give cybercriminals the data needed to gain access to your sensitive information. The questions in a social media quiz may seem trivial, but your answers reveal a lot about you.

Have you ever traveled outside of the country? This question reveals whether you have a passport. Knowing which forms of identification you have could help a cybercriminal steal your identity.

What town did you grow up in? This question reveals a detail that can be used to verify your identity. The town where you grew up could also be where you were born or where you went to school. Cybercriminals could use this information to answer security questions and gain access to an important account.

Who is your favorite fictional character? This question reveals your interests. Knowing what books or movies you enjoy could provide cybercriminals with a hint to crack your password. Cybercriminals could also use this information to target you on social media, claiming to have a shared interest.

Remember These Tips to Stay Safe: 1) Don’t share info online that you wouldn’t want to make public. 2) Review social media security options and edit your privacy settings to be sure your info is kept safe. 3) When you see a family member post a quiz on social media, inform them of the risks involved. They may share sensitive info that you both have in common & criminals could realize the connection.

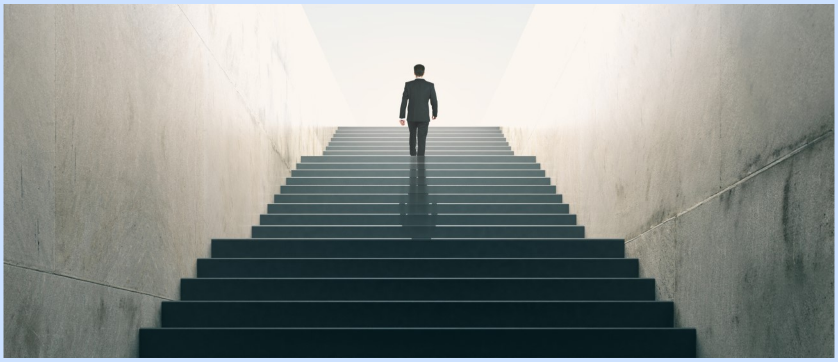
Shiny New Gadget of the Month

NeckRelax

Do you spend a lot of time hunched over your computer at work? Many people work on their computers for multiple hours a day and start to develop pain and stiffness in their necks because of it. While you can get a prescription to manage the pain or try to get a massage, these options aren't appealing to everyone. NeckRelax is the newest neck pain relief tool on the market and is working wonders for people who are using it. NeckRelax offers six distinct massage modes and infrared heat and also comes with a set of electrode pads to target specific muscles. NeckRelax sells for $119 but often goes on sale on their website: NeckRelax.io.

Get out of pain and take back your life with NeckRelax.

Confidence



By Dr. Geoff Smart

Confidence is an incredibly important trait in the world of business. You may think that all of the great CEOs and entrepreneurs of the last few decades never lose their confidence, but you'd be surprised. New CEOs usually have impostor syndrome and struggle with the idea that they're good enough for their role. Self-made billionaires often worry that their fortune will take an embarrassing hit. Even private equity investors look at the looming recession and grow concerned.

We often find that leaders are less confident when they obsess about things that are out of their control, rather than taking action in areas where they have some control. The Wall Street Journal recently reported that externally, most CEOs are most worried about a recession, global trade and politics. Internally, they're much more concerned about retaining top talent, dealing with disruptive technologies and developing the next generation of leaders. While it's good to be aware of the external issues, it's much more important to master the internal problems within your control.

In order to fully boost your own confidence, you must have a high level of confidence in your team. If you are already confident in your team, keep doing what you're doing to hire and develop top talent. If you aren't confident in them, then you should work on hiring the right people. If you've found yourself in this position and you're simply not confident enough in your team, there are a few things you can do to boost your confidence.

Your first option is to invest your own time into hiring, training and developing your team yourself. You'll need to set ample time aside so you can truly master the necessary skills to see the best results. Additionally, you can hire a company like ghSMART to do it for you. There are options for an immediate fix that will help adjust your confidence while also building your team's skills.

Confidence is not necessarily an inherent trait we get from our genes. We can build and grow our confidence skills by taking care of the things we can control. There will always be outside pressures that are out of our control, and there's simply nothing we can do about it. Instead, focus on hiring and maintaining top talent, developing your company's digital capabilities and training the next generation of leaders. You'll see positive results before you know it.

Dr. Geoff Smart is the chairman and founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times *best sellers. He stays active in his community and has advised many government officials.*

Your Employees: Your Biggest Cybersecurity Risk

Cybercriminals work round the clock to detect and exploit vulnerabilities in your business' network for nefarious gains. The only way to counter these hackers is by deploying a robust cybersecurity posture that's built using comprehensive security solutions. However, while you're caught up doing this, there is a possibility you may overlook mitigating the weakest link in your fight against cybercriminals — your employees.

With remote work and decentralized workspaces being more common, businesses like yours must strengthen their cybersecurity strategies to counter human errors and data breaches perpetrated by malicious insiders. All employees, irrespective of their designation/rank, can expose your business vulnerabilities to cybercriminals.

Implementing routine security awareness training for employees can help you prevent a vulnerability from escalating into a disaster. As the first line of defense against cyberattacks, your employees must be thoroughly and regularly trained to identify and deflate potential threats.

Why Employees Pose a Risk to Businesses?

According to IBM's Cost of a Data Breach Report 2020, 23 percent of data breaches in an organization occurred because of human error. An untrained employee can compromise your business' security in multiple ways. Some of the most common errors committed by employees include:

Falling for phishing scams: Cybercriminals are using improved techniques, like spoofed emails and text messages, to propagate the ongoing scam. Your employees must be well-trained to counter it.

Bad password hygiene: A section of your employees might reuse the same password or a set of passwords for multiple accounts (business and personal), which is a dangerous habit that allows cybercriminals to crack your business' network security.

Misdelivery: Even slight carelessness can lead to an employee sending sensitive, business-critical information to a hacker which can cause lasting damage to your business. You must be prepared to counter it.

Inept patch management: Often, employees can delay the deployment of a security patch sent to their device, which can lead to security vulnerabilities in your business' IT security left unaddressed.

The bottom line is that with cybercriminals upgrading their arsenal every day and exploring a plethora of options to trap your employees, security awareness training has become more important than ever before.

Security Awareness Training: An Essential Investment

A one-time training program will neither help your employees repel cyberthreats nor help your business develop a security culture. To deal with the growing threat landscape, your employees need thorough and regular security awareness training.

You must never back out of providing continual security awareness training to your employees just because of the time and money you need to invest in it. The ROI will be visible in the form of better decision-making employees who efficiently respond in the face of adversity, ultimately saving your business from data breaches, damage to reputation and potentially expensive lawsuits. The following statistics highlight why you must deploy regular security awareness training and consider it a necessary investment:

- √ Eighty percent of organizations experience at least one compromised account threat per month. [1]
- √ Sixty-seven percent of data breaches result from human error, credential theft or social attack. [2]
- √ Since the start of the COVID-19 pandemic, phishing attacks have gone up by 67 percent. [3]

Expecting your employees to train themselves on how to detect and respond to cyberthreats certainly isn't the best way to deal with an ever-evolving threat landscape. You must take on the responsibility of providing regular training to your employees to ensure you adequately prepare them to identify and ward off potential cyberattacks.

Every employee must realize that even a minor mistake can snowball into a terrible security disaster for the company. They need to understand that your business' cybersecurity is also their responsibility.

You can transform your business' biggest cybersecurity risk – your employees – into its prime defense against threats by developing a security culture that emphasizes adequate and regular security awareness training.

Making all this happen will require continued effort and may seem like an uphill climb, but with the right partner by your side, you can easily integrate security awareness training into your business' cybersecurity strategy. The first step towards training and empowering your employees starts with an email to us. Feel free to get in touch anytime: **info@palmtech.net**