



WAKE UP TO THE REALITY OF

cyber security

All across the world, hackers are targeting and exploiting security weaknesses and holding data hostage. In May, the Colonial Pipeline was hit by a cyber-attack that disrupted fuel supplies along the East Coast for several days. The company – and the FBI – paid hackers \$4.4 million in Bitcoin to regain control of the system.

Colonial Pipeline was not the only corporation that paid hackers an exorbitant amount of money. The NBA, Kia Motors and JBS Foods have also been victimized by cyber-attacks where hackers demanded millions of dollars. CD Projekt RED, a Polish video game developer, was also a victim of a cyber-attack, but since they had backups in place, they never had to pay the ransom.

While these are all big companies, that does not mean that small businesses are safe. These stories made the news because companies paid millions of dollars to regain control of their data. When a small or mid-size business gets attacked, they can't pay millions of dollars to recover stolen information. Instead, these hackers will usually go after customer and employee information as well as financial records and

statements. When a hacker attacks a small or mid-size business, it often ends in the business closing their doors for good.

The year 2021 set a record for cyber attacks, and 2022 is shaping out to be no different. If you're a business owner, you need to wake up to the reality of cyberthreats and cyber security before it's too late.

Here are a couple of the best cyber security practices you should put into place immediately.

Hire A Managed Services Provider For Your IT Needs

Cyber security awareness has grown over the past five years, but there are still plenty of companies who think there is no need for cyber security measures or that they're too expensive. The simple truth is that every business can be a victim of cyber-attacks. If you think it's too expensive to have your own IT team watching over your cyber needs, think again. Hiring an MSP is one of the best and most cost-effective ways to ensure that your network and information are protected.

MSPs can be incredibly beneficial to any business. They're designed to recognize and fix weak points in

TECH BYTES

FEBRUARY 2022

before
you hit  Send

Most of us are working virtually more often these days, but we want to remain just as professional as when we are face to face. So before you hit "SEND" - keeping email etiquette in mind is helpful.

- Write your email before entering the recipient's address
- Don't REPLY ALL; use it sparingly
- Proofread every email you send
- Reply to your emails; it is unprofessional to ignore or avoid your messages
- Keep your emails short and to the point
- Use a signature block if your recipient does not know anything about you or your company
- Enter a clear, concise subject line
- Always use a professional greeting
- Don't respond to an email when emotional/angry/upset
- Use a reputable email service provider



BLUE BAY
TECHNOLOGY

your IT infrastructure. MSPs work proactively to ensure that your business is fully protected in the cyberworld. They offer around-the-clock monitoring, data backup and recovery, firewall and network protection, real-time threat prevention and so much more. MSPs provide you with a dedicated team of IT professionals who are available to assist with any IT needs. If you have not looked into hiring an MSP for your business, you need to consider it.

If you're interested in hiring an MSP or want more information about the benefits, reach out to the Blue Bay Team and we will assist with any questions you may have.

Create A Cyber-Secure Culture

Many cyber-attacks stem from employee error or a staff member misunderstanding. You will want to make sure that your employees are aware of the risks associated with cyber-attacks. When you first hire an employee, train them on cyber security. In addition to this, your current employees should go through a reminder course at least

once a year. You'll need to inform your employees about the dangers of phishing e-mails and texts, downloading malware, scams and password protection. If you have remote employees, you should ensure that their devices have built in security measures. When employees are informed about the risks, they will be more observant and spot potential threats. Your entire team needs to buy into the cyber-secure culture if you want your training to be effective.

In today's day and age, you can never be too careful when it comes to your cyber security. You need to be proactive and put in all security measures you possibly can to protect your investment. The year 2021 saw cyber-attacks reach new heights, and it's likely that these numbers will continue to rise even higher. Take preventive action and don't let your business add to the cyber-attack statistics. If you're unsure of where to begin when it comes to buffing up your cyber security practices, give us a call, and our team will be glad to help make your organization cyber resilient for years to come.



**Why You
Should always
take your**

Vacation

Vacation - how vital can it be? It's absolutely a fact that rested employees are more productive employees. Taking time off reduces stress, prevents burnout and promotes a work-life balance by allowing for more time to be spent with family and friends. In addition, repeatedly working long hours and not taking time away from work can have an adverse effect on health and can negatively affect family life.

Some workers take great pride in never taking a vacation or paid time off in years. Some may feel that their company looks down on those that take time away from work. What has been proven time and time again is that taking those vacation days pays off: For both employees *and* the company.

212 million vacation days forfeited annually

- U.S. Travel Association

Staff members who use most or all of their earned vacation time each year are more productive, perform at higher levels, and are more satisfied with their jobs than those who do not, according to the Vacation's Impact on the Workplace report (from SHRM). Companies who encourage the use of vacation and other time off will have employees happier when they return to work, which translates into higher retention rates - and THAT can save a company thousands of dollars.



Get Different and avoid Defeat

When I released my first book, *The Toilet Paper Entrepreneur*, I hoped that it would be met with immediate success. Instead, nobody bought the book on its initial release day. Like most would be in this situation, I felt defeated. I had to think about my next step. Should I learn how to market effectively or simply give up on my hopes and dreams?

I knew that I wrote a good book and that it would help other entrepreneurs succeed, so it became my mission to properly market the book. The lack of good and effective marketing is what holds many businesses back from reaching their goals.

If you want to beat the competition, you must differentiate yourself from the rest. My book *Get Different* explains ways that you can make your company more visible in the business marketplace. I'd love to share the three main steps from this book, as they can help any business's marketing strategy be more engaging and effective.



Mike Michalowicz has always believed that he had the formula to success & 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* & 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.

- The first thing you need to do is differentiate your business from its competitors. If you rely on word-of-mouth marketing, you'll fail. Instead, you should get out there and use your marketing tools to ensure that people know your business is the best in the industry. Use your talents to stand out from the crowd. Be funnier or smarter than the rest, and consumers will surely take notice of your brand.
- After you get your consumers' attention, you need to attract and engage them. Give your campaign an authoritative, trustful, repetitive or socially significant approach so they feel comfortable using your business.
- Lastly, you need to be direct. After you get their attention, tell them what to do. Develop a call to action so customers and ideal prospects will take the next step. By picking a specific action, you can also measure the results and see how effective your marketing truly is.

Proper marketing can be very difficult to achieve, but with these steps, you will be on the road to business success.



WORK SMARTER NOT HARDER

In many cases, entrepreneurs try to do as much work as possible in order to meet their standards and succeed in their industries. Sometimes, these entrepreneurs do way more work than is necessary. Unfortunately, this may involve more busywork, on a daily basis, which will put any entrepreneur on the fast track to burnout and may even reduce profits.

If you feel like your days are bogged down with busywork, you should look into business automation tools. These will help get your business back on a profitable track while also alleviating stress.

Automation tools are available to boost nearly any aspect of a business. Google Workspace and Office 365 can help with various tasks, Mailchimp and Constant Contact can make e-mailing a breeze and FreshBooks can help automate billing. If you're not using any automation tools in your business, you should start now. Do your research and find the programs that will benefit your business the most.



"If you must work hard, work hard to find a smart solution."
- Alexander Woo



Prepare for a Hack Attack

Avoid Phishing Scams:

Train your employees to not open or respond to any suspicious texts or e-mails; and avoid clicking links that are not from verified, trusted sources.

Hide Your Data:

Keep your data in multiple online locations and separate data between multiple cloud providers to keep it secure. Hackers are likely to give up if it's too much hassle to get in.

Watch What You Post On Social Media:

Don't post any information on social media that a hacker could utilize to breach your security. If you're not sure, then just don't risk the post.

Check Your Finances:

Routinely examine your accounts. It's up to you -- not your accountant or your bank -- to keep up with your finances and watch for irregularities on your accounts.



600 Airport Road Winchester VA 22602
4451 Brookfield Corp. Dr, Ste. 100, Chantilly VA 20151

703 261-7200

www.bluebaytechnology.com