

February 2022



Connection



Quote of the Day:

"TODAY'S ACCOMPLISHMENTS
WERE YESTERDAY'S
IMPOSSIBILITIES."

– ROBERT H. SCHULLER

Our Mission

is to deliver outstanding
IT support to your
business in order to improve
uptime, productivity, and
profitability.
You take care of running your
business. We'll take care of
your technology.



This monthly
publication provided
courtesy of Michelle
Sherman, President
of Computer Services
Unlimited.



It's Time To Wake Up To The Reality Of Cyber Security In 2022

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 demanded ransom.

While these are all big organizations, 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 (SMB) 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.

Many cybercriminals look at small businesses like blank checks. More often than not, small businesses just don't put money into their cyber security, and hackers and cybercriminals love those odds. They can target small businesses at random, and they are all but guaranteed to find a business that has no IT security – or the business does have some security but it isn't set up correctly.

At the same time, cybercriminals send e-mails to businesses (and all the employees) with links to phishing websites (websites designed to look like familiar and legitimate websites) or

Continued on pg.2

Get More Free Tips, Tools and Services At Our Website: www.csuinc.com
(703) 968-2600

Continued from pg.1

links to malware. They hope employees will click on the links and give the criminals the information they want. All it takes is ONE employee to make the click.

Or, if the business doesn't have any security in place, a cybercriminal may be able to steal all the data they want. If you have computers connected to the Internet and those computers house sensitive business or customer data – and you have NO security – cybercriminals have tools to access these computers and walk away with sensitive data.

It gets worse! There are cybercriminals who have the capability to lock you out of your computer system and hold your data hostage. They may send a link to ransomware, and if you or an employee clicks the link or downloads a file, your business could be in big trouble. The criminal may request a sum of money in exchange for restoring your PCs or data. When a hacker attacks an SMB, it often ends in the business closing their doors for good.

2021 set a record for cyber-attacks, and 2022 is shaping up 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.

“2021 set a record for cyber-attacks, and 2022 is shaping up to be no different.”

Create A Cyber-Secure Culture

Many cyber-attacks stem from employee error or misunderstanding. You need to make sure that all of 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 keep cyber security top of mind, by completing 2 to 5 minute training modules at least once a month.

You'll need to inform your employees about the dangers of phishing e-mails and texts, downloading malware, social media scams and password protection. If you have employees working remotely, you should ensure that their devices have security measures built into them. If your employees are informed about the risks, they will be more observant so they can spot any 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 into effect all of the security measures you possibly can.

The year 2021 saw cyber-attacks reach new heights, and it's likely that these numbers will continue to rise even higher this year. 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, visit online at www.csuinc.com/cybersecuritytraining/ or give us a call at 703-968-2600, and we will be glad to help.

Shiny New Gadget Of The Month: Kailo – The Future Of Pain Relief



Nearly everyone has felt pain so intense that they had to take a painkiller to calm the discomfort. Sometimes orally administered painkillers can take too long to be effective, or they simply fail to dull the pain at all. The people at Kailo realized this and made it their mission to help people manage pain with a nanotech patch.

Kailo interacts directly with your brain's electrical system, telling it to calm down and reduce pain. Kailo doesn't use medicine or drugs, and there are zero side effects. In addition to this, it works anywhere on your body, and you'll start feeling the effects within the first minute. If the usual painkillers aren't working for you, give Kailo a try.

Get Different and Avoid Defeat

By: Mike Michalowicz



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.

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.



*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.*

■ Prepare For A Hack Attack TODAY

Every business owner, big and small, should be prepared for a cyber-attack. It's not a matter of if, it's a matter of when. Luckily, there are five strategies you can implement to better protect your company from hackers.

1. 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.

2. Routinely Check Your

Finances: It can be nearly impossible to recover from a hack if too much time has passed. It's not your bank's or accountant's responsibility to keep up with your finances, it's yours. Get in the habit of regularly checking your finances.

3. Utilize Multifactor

Authentication: Make sure your employees use multifactor authentication to protect company information.

They should change their passwords often and make them complex.

4. Avoid Phishing Scams:

Train your employees to not open or respond to any suspicious texts or e-mails.

5. Watch What You Post On Social Media: Don't post any information on social media that a hacker could utilize to breach your security.

■ Inspiration Station

Discover the secrets to overcoming challenges as you pursue your hopes and dreams. Dreams are like precious gems and should always be protected. If you lose sight of your dream, a big part of your life also will be lost. Chasing your dream requires a belief in yourself. It needs you to be the type of person who is comfortable blazing his or her own trail in life.

Here are some of the most common challenges a dream chaser MUST overcome:

It's taking too long—When you are actively chasing your dream and thinking about it regularly, it's like the watched pot that never boils. You know in your heart that the long-awaited goal is coming, but it usually takes much longer than you expect.

Failure is necessary—Failing is part of pursuing your dream. But it can stunt your excitement for a bit. When you lose your excitement, your forward movement slows down.

It's difficult—It's impossible to expect all the difficulties involved in achieving your dream. These setbacks can make you question your ability to succeed.

You're on an island—You feel like you are on an island of your own or a pioneer discovering a new land. There is no roadmap to follow the trail you are making. So it's easy to question your direction.

Change is required—In order to successfully achieve your dream, you will need to be open to change. Your course or direction will be modified and new ideas will require implementation to make that dream come true.

You must focus—You must continue to focus on your dream and pursue it with passion because there are many others that don't share it. They don't believe you will succeed. Sometimes, in their efforts to help you, they will steer you off your path to success.

WHY are you doing this?—It is easy to forget why you're doing something when difficulties arise. Pursuing your dream and successfully achieving it will require commitment, persistence, and genuine belief in yourself.

You will sometimes feel you are going crazy, and those around you might agree with you. But the trick is to NEVER give up.



We believe that experienced, reputable and fast responding IT support should be the standard.

CSU SERVICES



- Data Backup & Recovery
- Managed Services
- IT Consulting
- Network Security
- Cloud Computing
- Remote IT Services
- VoIP Telephone Services
- Cyber Security Training
- Mobile Device Management