The Tech chronicle

What's New

February is the month of love! Here are some favorite Valentine's Day quotes for you to write to your special someone.

Love is composed of a single soul inhabiting two bodies ~ Aristotle

How do I love thee? Let me count the ways. ~ Elizabeth Barrett Browning

The best and most beautiful things in the world cannot be seen or even touched. They must be felt with the heart. ~ Hellen Keller

Love is the voice under all silences, the hope which has no opposite in fear; the strength so strong mere force is feebleness: the truth more first than sun, more last than star. ~ E.E. Cummings

February 2022

This monthly publication provided courtesy of Dennis Jock of DenBe Computer Consulting.

Did You Know?

Michigan has the longest freshwater shoreline in the world.

Cyber Security Is More Important Now Than Ever – Is Your Business Prepared?

Over the past few years, instances of cyberthreats have increased at an alarming rate, and they don't seem to be slowing down anytime soon. Awareness around cyber security has certainly improved over the past year, with 9 in 10 Americans stating that they are somewhat concerned about hacking that involves their personal information, financial institutions, government agencies or certain utilities. But while awareness has increased, so have the rates of cyber-attacks.

Last year, people had more data breaches from January to October 2021 than in all of 2020. As we continue through 2022, there's no reason to assume this year will be any different. In order to ensure that your business is protected this year and every year after, you should take the proper precautions regarding cyber security. If your business falls prey to a cyber-attack, you risk tarnishing your brand's reputation and will have customers questioning whether it's safe to do business with you.

Below are a couple of the best cyber security practices you can put in place to fully prepare for cyber-attacks and threats.

HIRE A MANAGED SERVICES PROVIDER

Small and mid-size businesses have seen an increase in cyber-attacks since 2018, but larger corporations are no exception for hackers. The NBA, Kia Motors and the Colonial Pipeline are just a few examples of big businesses that fell victim to cyber-attacks last year. No matter if your business is big or small, hiring

Continued on pg.2

Continued from pg.1

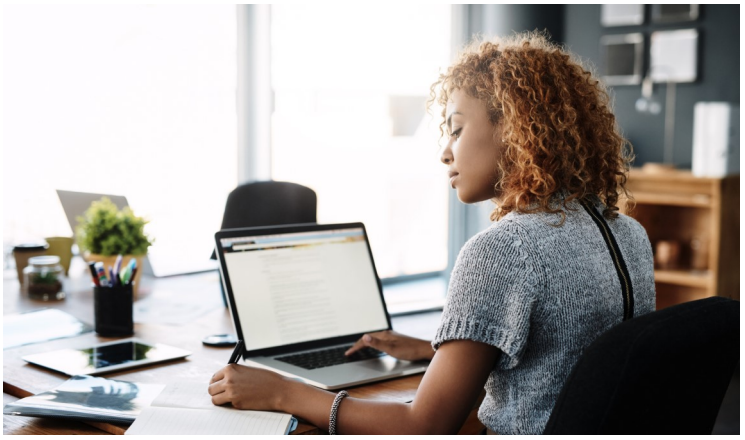
an MSP is the most affordable and best way to protect your business.

MSPs are designed to identify and resolve any weak points in your IT infrastructure. MSPs are focused on being proactive and will also focus on IT support and advanced security. You'll get around-the-clock monitoring, data encryption and backup, network and firewall protection, security awareness training and so much more. With MSPs, you get a team of dedicated IT professionals who are available to assist with any tech dilemmas that may arise. It's the quickest and most cost-efficient way to fully protect your business.

TRAIN YOUR EMPLOYEES

If your employees have not been trained to be cyber-secure, they need to be trained on this subject immediately. Security should also be built into the devices they use to access company data. This becomes even more important if your employees are working remotely. Multifactor identification and ensuring that your employees create complex and non-repetitive passwords go a long way toward keeping your business protected.

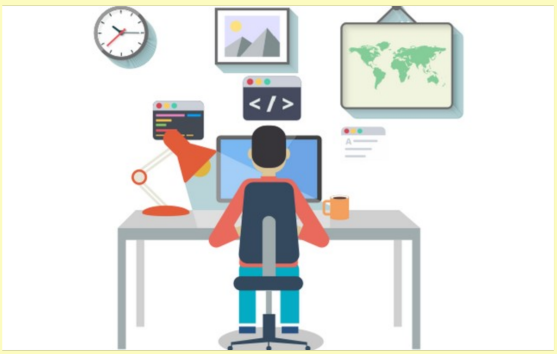
"Multifactor identification and ensuring that your employees create complex and non-repetitive passwords go a long way toward keeping your business protected."



Educate your employees about the most common forms of cyber-attacks. They should be aware of phishing e-mails and texts and should be taught to never open any links if they don't know who the sender is. Hackers have also started to frequent social media, and they often target small businesses through various platforms. Make sure your employees aren't clicking on any social media spam links that could put your network at risk. Lastly, make sure they aren't accidentally downloading any malware that could create disastrous outcomes for your company.

A cyber-attack can have cataclysmic effects on a small business, and every business owner needs to make sure their network is protected. If you don't know where to start, give us a call and we will find a way to help you make your company as cyberprotected as possible.

Wouldn't it be nice to have a one stop shop for all your IT needs? Let us give you a quote for Website Hosting, Design, SEO and SMM.



Why not let DenBe be your one stop shop for everything IT?

- We can design your new website or transfer your existing site to our infrastructure
- We'd love to grow your business by handling your Search Engine Optimization
- Who has time for all that posting– we'd love to create content and handle all your Social Media Management
- DenBe Consulting can take all this off Your plate so you can run Your business

Cybercrime on the Rise

There's no denying that cybercrime is on the rise. All it takes is a glance at a few big news stories from the past couple years. Equifax gave up the information of over 100 million people, many of them not even users, to a surgical hacker attack. Recently over 57,000 infections spread from a single ransomware source across 99 separate countries, with damage reaching everything from hospitals and businesses to vital public utilities. In your company's battle against cybercrime, it's essential to stay abreast of the rapidly shifting digital landscape. Only the most up-to-date security technology can even hope to protect you from the ever more sophisticated thieves pounding at your digital door. However, it's also important to stay informed. Here are a few of the sneakiest and most common tricks thieves use to snatch your vital data:

Social Engineering Hacking, though it can cost you thousands of dollars and do just as much damage as its digital counterparts, doesn't require a single line of code. Instead, they find weaknesses in the "human network" of a business. For example, skilled scammers can call your business's cell phone provider, posing as the CEO's spouse, and convince the customer service rep to hand over passwords, Social Security numbers, and sensitive personal information. Many IT departments are susceptible to this same scam. Often, social engineering is used to gather information that will later be used for a different strategy. Such as …

E-mail Phishing, which hijacks an e-mail account with trusted authority and sends users an e-mail requesting they click a particular link. Maybe the e-mail looks like it's from the service department of your company's time-tracking software, seeking to remedy an error. But when the link is clicked, ransomware or other malware spreads like wildfire through the system, and the user is at the mercy of the hackers. Usually, this is used to extort exorbitant sums of money out of small businesses or individuals. Symantec reports that just last year, over 7,000 businesses of all sizes fell prey to some form of phishing scam, costing them more than $740 million in total.

Brute-Force Password Attacks Or Password Guessing are just what they sound like. Either a hacker uses a software that, after putting in some data about the target (for example, the name of their dog or their anniversary), runs through potential keys ad infinitum. With sufficient information about the target, it's only a matter of time before the software breaks through. Or, more often than you might think, hackers can simply guess the password. Infiltrators have common passwords that use real words or common structures memorized and can run through hundreds before giving up.

How To Protect Yourself Against These Threats

It's not enough to keep your eye out for common hacker strategies. As the progress of technology marches on, so do the techniques and softwares used by hackers, resulting in an infinite number of permutations of ways they can penetrate your system. The only way to be truly secure is by utilizing leading-edge security solutions to ensure you stay ahead of the breakneck developments in hacker technology. With constantly updating software dedicated to security, along with some know-how, you can rest a lot easier knowing your data is safe.

How To Create More Opportunities

To put it simply, in life, perspective is everything. Every activity, job and situation usually has multiple angles, depending on how you view it. By changing our perspective in our business and personal lives, we are creating a very positive mindset that will open us up to a plethora of new opportunities.

There's a rocky cliff that rises up at the back of my property, and atop that small cliff is a boulder. I normally wouldn't give a second thought to this giant rock that sits in my yard since it's nonliving. I mean, it's just a rock, right? But as I observed it more and more, my perspective completely changed.

You see, while the rock itself may be nonliving, it is actually thriving with life. There are beautifully colored skinks that live in the crevices of the boulder, and I even saw a big black rat snake make its home there, too. When I took a second to think about it, I realized that this boulder sustains its own ecosystem.

By simply taking a moment to drop your own preconceived notions and making an effort to observe, you will find life and opportunities in something you may have previously missed. But changing your perspective is easier said than done. In order to change your perspective, you may have to do a little digging. You'll have to evaluate why you see things the way you do. You may need to reach out to others and consider their perspectives to get an idea of how others think. And lastly, you'll have to reform your own perspective so you can grow and find new opportunities.

Dig deeper within yourself and truly concentrate on what you're focusing on so you will see so much more. You'll quickly discover that the opportunities are endless.

Mike Michalowicz has always believed that he had the formula to success and has proved it on multiple occasions. He is the creator of Profit First*, which is used by hundreds of thousands of companies across the globe to drive profit. He is the author of multiple books, including* Get Different *and* The Toilet Paper Entrepreneur. *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. He also is a highly sought-after keynote speaker on innovative entrepreneurial topics.*

Break Through The Digital Dilemma And Take Your Business To The Next Level

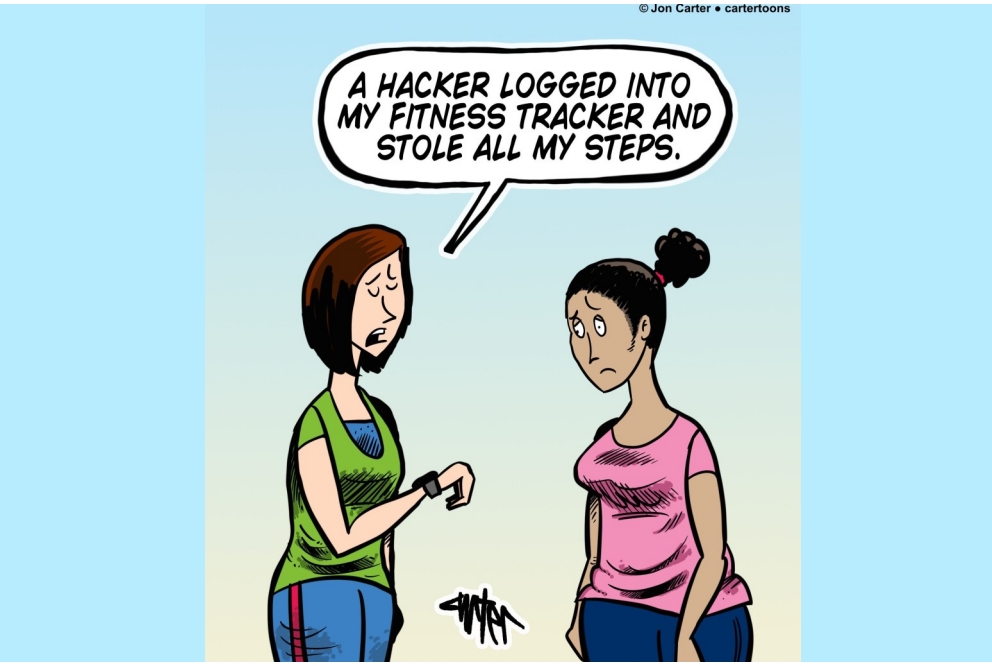
In the digital age, companies are growing faster than ever before, and the companies that are succeeding all have one thing in common: a growth mindset.

Companies that aren't looking to grow get stale quickly, and this becomes more apparent with each technological advancement. In order for your business to succeed, you will need to develop a growth mindset within your company. There are a few things you can do to adapt and create a mindset that will catapult you to the top of your industry.

The first thing is to continue promoting a learning and mentoring ideology within your business. There's always room for growth; you just need to encourage it. You should also encourage innovation by establishing areas where external and internal sources can communicate. Also, stay informed and ahead of your industry by paying attention to new technology. Lastly, don't be afraid of feedback. It can help your company grow and help you to discover any shortcomings.

Facebook Recently Launched Its Metaverse, And it's A Privacy Nightmare!

Facebook is in the process of unveiling hardware and other technology to support its metaverse, even calling this new network "Meta." The social media platform has seen a recent decrease in users who cite mistrust as a key factor in their departure. A Facebook whistleblower, Frances Haugen, has stated that the virtual reality world could give Facebook another opportunity to steal even more personal information from its users. Haugen said users will be required to set up many sensors throughout their home, which will encourage them to detract from reality and enter the virtual world. The idea of adding sensors into users' homes is a privacy nightmare. It gets even worse if you consider the fact that employers who use Meta may require their employees to have the sensors in their homes so they can participate in meetings. Trust in Facebook is already low, and Meta will have to ensure their system is safe if they hope for success.



It's Been Coined The 'Great Resignation,' But Why Are Employees Walking Out In Droves?

Everywhere you look, it seems like more businesses are putting out "Help Wanted" signs. Limeade, an organization that specializes in employee well-being, recently released the results of a study that focused on why people were leaving their jobs. Burnout was the top reason most employees quit. Through surveys and conversations with your team, you can discover if burnout is an issue in your business. Introducing mental health days and finding ways to equally distribute workloads can help prevent burnout.

People who recently left their jobs also stated that they wanted a more flexible or caring culture. Employees need time for themselves and will become unhappy if they feel work is taking away from that time.