Is block chain technology the answer we have been looking for?

It is no secret that cryptocurrency has been taking the world by storm. Some of us see it as an investment opportunity with the potential of great financial gains, others are worried. Afterall, the technology that allows for secure financial transactions similar to cash transactions is the same technology that greatly affects cybercrime. Crypto has great potential, but is the way of the future?

This month we will be co-hosting a FREE seminar networking event with financial advisor Scott Lask (Wedbush Securities). We would love for you to join us to exchange thoughts, ideas, and answer questions while enjoying a meal of burgers and refreshments with you.

There is NO cost to attend, but seats are limited so please RSVP soon. The event will take place on **Thursday October 24th, from 5.30 to 7pm at the CoLab in Goshen.** Please email me at: mduci@meetingtreecomputer.com to let us know if you'll be attending.

We are looking forward to seeing you there!

This monthly publication provided courtesy of Meeting Tree Computer.

3 Ways To Prevent Your Employees From Leaking Confidential Information

A lot of businesses need to come to terms with the fact that their employees are their greatest IT threat. As a business owner, you may be aware of cyberthreats to your business, but your employees might not be. They might not know about the threat of cyber-attacks or malware. They might use unsecured WiFi on company equipment. As a result, your employees may be putting your business at serious risk.

What can you do to change that?

1 IT ALL STARTS WITH EDUCATION. One of the biggest reasons why employees put their employer at risk simply comes down to a lack of education. They don't know about the threats targeting businesses or that small businesses are a major target of hackers and scammers.

You need to do everything you can to train your employees. Give them the education and resources to be a line of defense rather than a risk. Develop a consistent training regimen. If you need to bring in IT professionals to help, do it. Don't make assumptions about critical IT security training if you aren't sure. Professionals can answer your questions and make sure you and your employees have everything you need to know to keep your business secure.

Another important thing is to hold this training regularly. Threats evolve, and you need to stay ahead of the curve. Keep IT security on the

minds of your employees. When they forget about it, that's when the risk is highest.

2 **SAY NO TO UNSECURED, PUBLIC WIFI.** This is a big problem for businesses with remote employees, employees who work from home or employees who use company technology outside of the business walls. According to a Spiceworks study, 61% of employees said they have connected to unsecured WiFi while working remotely.

This is cause for concern. Connecting to public WiFi is like leaving the front door of your home wide-open while posting on social media that you're going to be out of town for a week. You never know who is going to let themselves in and snoop around. Hackers use public hot spots to circulate malware and steal data. Sometimes they even set up fake hot spots with the same name as a legitimate hot spot to trick users into connecting to their WiFi, which makes data theft even easier.

> **"It's all about understanding the threats and taking a proactive approach to security."**

Discouraging your employees from using unsecured, public WiFi is a good step to take, but don't be afraid to take it further. Don't let them connect company equipment to unsecured WiFi at all. And place a bigger focus on endpoint security – make sure your equipment has up-todate software, malware protection, local firewalls, as well as a VPN (virtual private network). The more layers of security, the better.

3 **PROTECT ALL OF YOUR DATA.** Your employees should never save personal or business data on portable/ external hard drives, USB drives or even as printed material – and then take that data out of the office. The theft of these types of devices is a real threat. An external hard drive is a tempting target for thieves because they will search the drive for sensitive data, such as financial or customer information that they can use or sell.

If you have remote employees who need to access company data, put a method in place to do just that (it should be discussed as part of your regular company IT security training). They need to know how to properly access the data, save the data or delete it, if necessary. Many businesses go with a secure cloud option, but you need to determine what makes the most sense for your business and its security.

While these three tips are great, nothing beats helping your employees develop a positive IT security mindset. It's all about understanding the threats and taking a proactive approach to security. Proactivity reduces risk. But you don't have to go it alone. Working with experienced IT security professionals is the best way to cover all your bases – and to ensure your employees have everything they need to protect your business.

Healthcare Is An Easy Target With A Big Pay Off

Data breaches are on the rise. Most, if not all of us, will have heard of the data breach at Quest Diagnostic, the medical testing company, where 11.9 million patients were affected by a cyber incident a few months ago. What about the Michigan based ENT & hearing practice that was the victim of ransomware earlier this year? After they refused to pay the ransom cyber criminals deleted all their data. They had no reliable backup in place and had to permanently close their doors.

All of us are busy every day, running around trying to get through all our regular responsibilities. None of us are looking for added stress and so, discussing and planning data protection strategies and worrying about compliance regulations don't often make it to the top of our to-do lists.

Will the OCR some knocking on your door tomorrow if you're not compliant with HIPAA rules? No probably not. But having a robust security strategy in place shouldn't be something that you do for them, but for yourself, your practice and your patients.

As your IT provider, we wanted to make sure that we are well educated and equipped to help you with this. And so, we are proud to announce that as of this month we are fully HIPAA compliant and have services and coaches in place to support you even better than before.

If you are ready to discuss the security and compliance of your medical practice call us today at **845-237-2117**. Let's get the conversation started.

The Power Of Punctuality

Personally, I am not a fan of people who are always late. Sometimes, things happen that we have no control over, such as car accidents, traffic jams and unexpected family emergencies, to name a few. I am not addressing those situations.

**What I am addressing is how punctuality can do wonders for your success.**

Have you ever thought about what being punctual says about you? It shows you are in control, disciplined, able to keep track of things, trustworthy, reliable and respectful of another person's time. Being late demonstrates none of those things. In fact, being late shows you are unreliable, disorganized, disinterested and inconsiderate. When you look at it from that perspective, you would never want yourself described that way.

Do you want to hire someone who is unreliable? Not me. How about disorganized? A disorganized person will make mistakes — and mistakes cost money. Let's take a closer look at disinterested. One of the definitions of disinterested is having or feeling no interest in something, unconcerned, uncaring and unenthusiastic. That sounds like someone you NEVER want to have on your team. Then that leaves us with inconsiderate, defined as thoughtlessly causing hurt or inconvenience to others, unthinking, selfish, impolite and rude.

Associates, bosses and customers have NO fondness for lateness. I heard one person express it this way: "If you are chronically late, you are chronically rude." If you are looking to be promoted to a leadership position, it will be difficult to prove yourself reliable when people are having to wait for you to show up. Punctuality is a product of discipline, proper planning and respect for others. In simple terms, preparedness and punctuality are two of the most important qualities of a leader.

When you are late, you are saying, "My time is more valuable than yours." That is not a great way to start anything. The celebrated writer Charles Dickens once said, "I could have never done what I have done without the habits of punctuality, order and discipline." I feel that by being punctual, you are paying a courteous compliment to those you are about to see or serve; it's a respectful gesture of how you value their time.
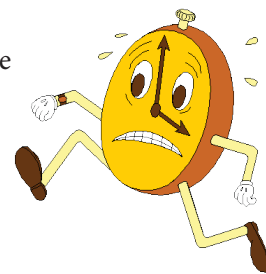
Chronic lateness sets a tone about accountability. If you want a culture in which people are accountable to customers, associates and even to themselves, then make punctuality a priority. Start all meetings on time regardless of who is missing. The word will get out, and people will start showing up on time.

Being on time may seem a bit trivial to some people, but it's a good idea to start making accountability part of your corporate culture. Shakespeare once stated: "Better three hours too soon, than a minute late." There truly is power in being punctual.

Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys and 52 Essential Habits For Success, he's shared the podium with esteemed figures from across the country, including former President George H.W. Bush, former Secretary of State Colin Powell, Anthony Robbins, Tom Peters and Steven Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.

■ THESE ARE THE BIGGEST PRIVACY THREATS YOU FACE ONLINE TODAY

Webcam Access – While it's rare, there are known exploits that allow others to access your webcam (such as malicious software or software security flaws). Putting electrical tape over your webcam isn't a bad idea, but more webcams are coming with kill switches and shutters for peace of mind.

Phishing Scams – Don't ever expect these to go away. People still fall for them. NEVER click links in e-mails from anyone you don't know (and even if you do know them, verify that they sent you a link — e-mail addresses can be spoofed).

Web Browser Plug-ins – Vet every browser plug-in and extension you install. Many extensions collect your browsing history and sell it. Read the terms of service before you click install (a good rule of thumb for software in general).

Ad Tracking – Web ads (and web ad providers, such as Facebook and Google) are notorious for tracking users. They want to know what you like so they can cater ads directly to you in the hopes that you'll click the ad, which gives them ad revenue. It's one of the many reasons why people use ad blockers.

Device Tracking – If you have a smartphone, chances are it's being used to track your every move. Again, it comes back to delivering ads that are relevant to you so you'll click on them. For companies like Facebook and Google, users are the product.
Inc., 7/19/2019

■ CAPITALIZE ON THIS STRATEGY TO IMPROVE YOUR BOTTOM LINE

Want to boost your bottom line? The answer may be in cashless payments. It's all about taking your current systems and updating them to current trends.

Outside of the U.S., particularly in Europe and much of Asia, cashless payments are king. More people are relying on smartphones as payment processing tools (both in the consumer and business worlds). Of course, you don't want to rely on cashless — you want to be able to accept any money your customers are spending, whether it's cash, card or electronic.

Look at your point-of-sale system — is it ready for cashless? If not, look into it, research your options, ask around and see what option makes sense for your business (and bottom line).
Small Business Trends, 6/26/2019

October is National Cyber Security Awareness Month!

Time to brush up on smarter security practices.

Follow us this month on Facebook and LinkedIn for tips and advice.

"I DON'T THINK YOU UNDERSTAND THE CONCEPT of CYBERSECURITY."

Follow Us On Social Media!

http://bit.ly/MeetingTreeComp-Facebook

http://bit.ly/MTC-LinkedIn

A referral from a friend, Client, or colleague is the highest compliment we can receive.

www.MeetingTreeComputer.com
Phone: (845) 237-2117