MC Heartbeat

"Insider Tips to Make Your Practice Run Faster, Easier, and More Profitably"

How Do I Make MONEY?

By Justin Shelley

Kevin O'Leary and Justin Shelley

On April 23rd of this year, I had the privilege of meeting Kevin O'Leary, one of the investors on ABC's Shark Tank. I'm a huge fan of the show, and have been from day one. Kevin isn't known for being warm and cuddly, but he has always been one of my favorites. I guess that's because he gets right down to business. It's all about the MONEY!

In our society, it has almost become a crime to talk about money. "Rich" people are vilified and any organization that dares to turn a profit is dismantled by the media. "Corporate Greed" is the phrase of choice. It aggravates me to no end. If those evil corporations weren't greedy enough to make all those massive profits, there would be no jobs.

I was talking with a friend several years back who does not share my opinion about this subject. He said, "I'm all for spreading the wealth around a bit." There were other comments which I don't remember, but I do remember telling him how I loved rich people. At the time I was employed by a group of very rich people. Without them, I would have been unemployed.

In the end, opinions don't matter. The fact is that no organization can survive without money. Even non-profits have to pay the bills. So

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

- Justin Shelley, Master Computing

September 2015

DENTON, TEXAS

Inside This Issue…

what did I learn from Mr. O'Leary that can help *your* organization make money?

Kevin started off by talking about Shark Tank. He referenced a study conducted on all of the entrepreneurs that successfully closed a deal on the show. There were three characteristics that applied to all of them, without exception:

1) They were able to articulate their idea (value proposition) in 90 seconds or less.
2) They had the right team in place to execute their plan
3) They knew their numbers (margins, break-even point, etc.)

Let's take a look at each of these.

Value Proposition

I'm a member of an online community of fellow IT business-owners. Someone posted a question about how to sell the value of a new tool he had bought. "I still do not see the 'benefits' for clients, as a monthly fee." My response to him was, "You're thinking like a technician. You have a tool and want to know how to make the customer get excited about it. Do you care what type of socket set your mechanic uses to fix your car?" As a tech-junkie, I get excited about gadgets and tools. My clients generally do not.

The world of medicine is admittedly more complex than the world of technology, but you still have "customers" who are looking for value. Your customer might be the patient, it might be the provider, or it might be the insurance company. Maybe it's all three. In any case, what value do you provide? How are you making someone's life better? Remember, we're not talking about the "tools". We're not even talking about the procedures. We're talking about real value. The stuff that can only be measured on the warm-and-fuzzy meter.

This subject is a very deep, very complicated matter. I won't try to break it all down in the small amount of space I have here. But if you're looking for a place to start, just ask questions. Ask your customers (patients, providers, etc.) what they like about your practice. Ask them what they hate. And here's a tip, ask them what they hate about health care in general. They will rarely tell you to your face what they dislike about *you*. People naturally shy away from confrontation. But if you generalize the question, you'll be amazed at the feedback.

Your Team

Having a solid value proposition is great. But it's only step one. Even the organizations who think they have this one really dialed in might be surprised to learn that the rest of the team is not on the same page.

For a fun exercise, ask each member of your team what the organization's core values are. Or what your mission statement is. I've seen organizations with this information posted on the wall in large, fancy print, and still the team can't answer the question.

In order to really deliver consistent value, these three things *must* be in place:

- You must have the *right* team members
- Each team member must be doing the *right job*
- Everyone needs to have the *same vision*, with individual areas of responsibility and accountability

The Numbers

On the surface, you might think Kevin O'Leary is the definition of corporate greed. Honestly, my opinion of him wouldn't change even if that were true. But his opening line really resonated with me:

"It's not about greed. It's not about the money. It's about freedom." Did you catch that? Kevin said it's not about the money! If you watch Shark Tank, you will hear him talk a LOT about money. Why? Because money buys freedom. Freedom from overdue bills. Freedom from long, agonizing days because you are under-staffed. You may have your own version of freedom. But regardless, money can buy it.

Organizations do not have money by accident. It is a very deliberate, intentional process. But it starts with financial intelligence. Know your numbers! This will look different for every organization. It is also the difference between life and death.

So there you have it right from the mouth of my favorite shark. Here is your formula for making MONEY; here is your formula for buying freedom: know how you add value to the people around you, get everyone on board with the same vision, and know your numbers.

Here's to corporate greed and every ounce of freedom it buys! (For you, your team, your family, and society as a whole.)

5 Ways To Spot Phishing Emails

By Jessica Shelley

Unfortunately for most of us out there, phishing emails are a common and aggravating problem. If you're lucky enough to not know what phishing emails are exactly, they're scam emails sent by people trying to get personal information out of you such as your bank account information and social security number. However, not all of them are trying to get information about you. They're instead trying to trick you into downloading a virus on your computer so that they can gain access to all of your patient information. Not only would this be detrimental to your patients, but you could also get in trouble with HIPAA.

Hopefully, with these 5 tips, you'll never have to worry about being tricked by scam artists thanks to your amazing skills in spotting phishing emails.

1. **General Names:** When you receive an email supposedly from someone like Chase Bank or Facebook (someone that would know who you are) and it's addressed to "Dear Customer", that should be a giant red flag in your face. These big companies know your name and will always use a more personal greeting. However, you have to be careful with this one because scam artists can sometimes have access to your name. So even if they know your name, you should always be weary.

2. **Spelling Errors:** This may sound a little strange, but most of the time, obvious spelling or grammar errors can be a clue that the email is coming from an illegitimate source. There's no way a big company is going to send spelling errors out to their customers. They have people for that.

3. **Landing Pages That Are Wrong**: If an email is asking you to click on a link, it is almost always a phishing email. A good way to tell if the link is a trusted website is by hovering over the link. Doing this shows you exactly where the landing page is. If there is a spelling error in the landing page, or it's just completely wrong (says it's from Bed Bath and Beyond but the link goes to pugs.net), never ever click on the link. Even just clinking on the link can download a virus onto your computer which then can have complete access to all of your secure patient information.

4. **Incorrect URL**: If by some trick of fate you end up clicking on the link and you find yourself on a website that looks almost exactly like what it says it is, pay close attention to the URL. Often times on a phishing website the URL will either be misspelled or something will wrong (like missing the s in https//). If you see either of these signs you should immediately close the page and delete the email.

5. **Try To Log In Using an Incorrect Password**: If you end up on the landing page, you can't find any errors in the URL and everything looks up to par, try logging in using the wrong password. If it is in fact a phishing website, it's going to log you in because it's trying to get your password from you. But if it's the legitimate website it'll tell you that your password was incorrect and no harm done!

It's always better to be safe than sorry, especially if you're dealing with something as sensitive as PHI. If you notice too late that you've been tricked into giving away confidential information, be sure to contact your HIPAA Security Officer immediately as well as your IT provider. Letting the right people know as soon as possible can really help you out in the long run.

Turn Your Biggest Weakness Into Your Greatest Strength

You know the standard approach – first, identify your company's weakness and then do everything you can to fix it. Practice at it relentlessly, feed your team (and yourself) with constant affirmations, do anything you can to dive deep into your weakness and fix it once and for all. If you can't fix it, then go to Plan B by burying the weakness in hopes that none of your prospects or competitors find out.

Well, here's the dealio: the business down the street that is naturally strong at the same thing your company is weak at is working just as relentlessly to improve their strength. While you are fixing something that's broke, they are getting better at something that already works. While you may improve your weakness, their strength gets better too. At the end of the day they are still ahead of you. You lose. That is, unless you know the power of spin.

Instead of trying to fix weaknesses, smart leaders will turn the tables and make their weakness or even an industry weakness a competitive advantage. A wonderful example in the restaurant industry is Dick's Last Resort. Like all restaurants that struggle with the occasional rude waiter, Dick's could have tried to fix this industry-wide weakness. Instead they turned the weakness into their greatest strength. Known to have the "most obnoxious waitstaff in the world," Dick's built a whole system around exploiting an industry weakness. They hire and train people to be obnoxious (while the competition tries to fix it), and Dick's has grown explosively.

I have found that exploiting a weakness can draw droves of prospects. So, let's do it with your weakness. Here are the three simple steps you need to take:

Step 1

Know what your (or your industry's) weakness is. The process is simple: ask your customer and prospects what they don't like about your industry. Ask more customers the same question. Very soon you will know exactly what weakness they see.

Step 2

Instead of brainstorming ways to fix it, brainstorm ways to make the weakness absurdly weak. Can you make fun of it? Can you make it the core experience for your customers (think Dick's Last Resort)? How can you make the weakness a good thing?

Step 3

Now that you have a new and improved weakness, let the world know all about it. Market it to your prospects, inform your customers and even leverage all that work your fiercest competitor put into highlighting your weakness in the past.

The process of spinning a weakness takes courage, and that is exactly why it works. It is likely you have been afraid of doing this in the past, and it is highly likely your competitors are just as afraid too. If you have the courage to spin your weakness into an über-weakness (a.k.a. a big-time strength), you might just blow your competition out of the water once and for all.

MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford—a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group, a consulting firm that ignites explosive growth in companies that have plateaued; a former small-business columnist for *The Wall Street Journal*; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book *The Toilet Paper Entrepreneur*. His newest book, *The Pumpkin Plan*, has already been called "the next *E-Myth*!" For more information, visit http://www.mikemichalowicz.com/.

Shiny New Gadget Of The Month:

Nest Cam: Keeping An Eye On Things While You're Away

Have you ever worried about what's happening at home when you're away? The Nest Cam can keep you informed. This wide-angle camera streams sound and video to your smartphone. It will even warn you about any unusual activity.

If the Nest Cam detects sudden movement or loud noises, it instantly alerts you by phone. The video feed lets you see what's happening and even scold kids, pets or burglars through a speaker.

This product integrates with other Nest equipment. For example, smart smoke alarms can activate the Nest Cam. It also saves alerts and footage in a convenient archive. The camera even makes it easy to share fun video clips online.

If you already have WiFi, setup is a breeze. This gadget comes with a stand that lets you put it on any flat surface. It also sticks to metal objects or screws onto a regular camera tripod.

5 Ways To Protect Patient Information

Tip #1 – Encrypt all laptops

We are not going to get into the details of data encryption and you don't need to fully understand what data encryption is to understand the benefits. The HIPAA Security Rule states that if patient data is encrypted and the data is lost or stolen there is no need to notify patients or report the breach. The official description of encryption is that it is a Safe Harbor under the HIPAA Security Rule but we like to call it the "get out of jail free card". If you lose a laptop with patient information and it is encrypted you can act, for HIPAA compliance purposes as though it was never lost. It costs less than $100@year to encrypt a laptop. Encryption usually has no noticeable effect on using the laptop and only requires a password to be entered when you first startup the laptop.

We have heard arguments from clients that "our laptops don't have any patient data on them so why should we encrypt them?" While it may be true that you did not intend the laptop to contain patient information, the fact is it COULD contain patient information. There could be emails with patient information; spreadsheets, documents or PDFs with patient information could be stored on the laptop; reports downloaded from an EMR could be on the laptop. If a laptop is lost or stolen the process of trying to figure out what data was stored on the laptop would likely cost you much more than the cost to encrypt the laptop in the first place.

Bottom-line, if your laptops are encrypted you no longer have to worry about a HIPAA breach if they are lost or stolen

Tip # 2 – Minimize the use of portable devices and the amount of data on portable devices

In order to reduce the risk of losing patient information stored on a portable device, make it a practice to not use portable devices. Raise your employee awareness of the risks of portable devices. Write a memo or send an email to all employees stating that the use of portable devices to store patient information is frowned upon. If employees must use portable devices then the amount of patient information stored on the devices should be only the minimum needed.

Tip #3 – Encrypt all backup tapes

If you are still using tapes to backup your data then ensure that they are encrypted. Backup tapes hold all your data. If a backup tape is lost or stolen you could have a very large data breach. Don't assume your IT people are using encryption on your backup tapes. Have a conversation with your IT people and confirm that they are encrypting your tapes. Most backup software supports data encryption but it must be enabled first.

Tip #4 – Ensure you have a startup password and inactivity timeout on your smartphone

Smartphones such as iPhone, Android, Windows Phone and BlackBerry may contain patient information. More and more smartphones are used to access EMRs, imaging systems, etc. In addition, more and more patient information is contained in emails between physicians, physician assistants, billing departments, etc. Smartphones are easily lost or stolen and represent a risk to the patient information that they may contain. So what can be done to protect the information in the event that a smartphone is lost or stolen?

Tip #5 – Implement good password controls

Passwords are the key to protecting systems that contain patient information. The stronger the passwords that your employees use the more secure your systems are. Here are a few inexpensive ways to ensure you implement good password controls.

Complex Passwords

Encourage employees to use complex passwords that have upper and lower case letters, special symbols such as "@ ! $ % &" and numbers. The more complex the password the harder it is to guess or crack. Keep in mind that your employees probably have so many different passwords that they will not be too happy to have another password especially if it is hard to remember. You will have to ensure they understand the importance of protecting patient information and the importance of using complex passwords in order to respond to any employees' resistance.

Don't write passwords down

Passwords should not be written down. They should not be stuck to monitors on yellow sticky notes. They should not be on a piece of paper under the keyboard. Passwords, like credit card and social security numbers should be protected and not shared.

Conclusion

We mentioned a few simple and inexpensive tips that you can easily implement to protect patient information and help you toward HIPAA security compliance. Following these tips will go a long way toward providing increased protection of your patient information.

Do You Accept Credit Cards? Watch Out For These 5 Pitfalls That Could Lead To Lawsuits

If your company is not fully compliant with Payment Card Industry (PCI) Security Standards, you could be at risk of a serious tangle with attorneys. Technically, PCI guidelines are not a hard-and-fast set of laws. However, merchants can still face hefty liabilities for not meeting them. Avoid these mistakes to keep your company out of hot water with attorneys:

1. Storing Cardholder Data In Noncompliant Programs
Many states have laws regarding data breaches and, depending on where you accept cards, you may be subject to many of them. For example, Massachusetts has 201 CMR 17.00, which requires companies keeping any personal data from Massachusetts residents to prepare a PCI-compliant plan to protect that data. If a company then fails to maintain that plan, the business may face state prosecution.

2. Fibbing On The Self-Assessment Questionnaire
If you have considered tampering with the reports from your company's Approved Scanning Vendor, think again. Time invested now to fix any holes in your data security system could save you big-time from the penalties your company could suffer if there's ever a data breach.

The same thing applies to simply "fudging the truth" on self-prepared compliance reports. Even if you think it's a harmless stretch of the truth, don't do it.

3. Not Using The Right Qualified Security Assessor
Many companies use Qualified Security Assessors to help them maintain their PCI compliance. Every QSA does not necessarily know as much as another, however. It's important to select someone who both understands your business and stays up-to-date on the latest version of PCI Security Standards.

4. Trying To Resolve Data Compromises Under The Radar
You may be tempted to fix a customer's complaint yourself if they inform you of a data compromise. Not informing credit card companies of data breaches, however small, can lead to you no longer having access to their services. Those credit card companies can then file suit against your company, costing you big bucks in the end.

5. Not Checking ID For Point-Of-Sale Credit Card Use
Sometimes it seems like no one checks IDs against the credit cards being used, so merchants tend to be lax about doing so. Unfortunately, running just one unauthorized credit card could cost you a lot in the long run.
Even if the state in which you do business does not have specific laws regarding PCI compliance, a civil suit may come against your company for any data breaches. The court will not favor you if you have not been PCI-compliant.

All in all, it pays to pay attention to PCI compliance – a little time invested today could save you big-time tomorrow.

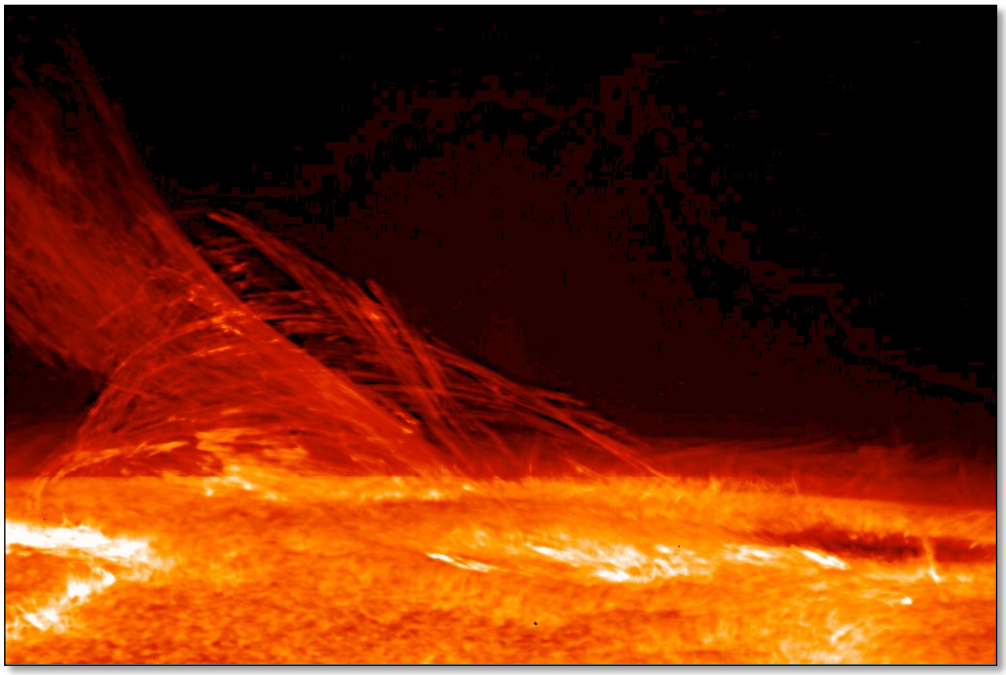
Help Us Out And We'll Give You A Brand-New iPad For Your Trouble

We love having you as a customer and, quite honestly, wish we had more like you! So instead of just wishing, we've decided to hold a special "refer a friend" event during the month of September.

Simply refer any medical practice with 10 or more computers to our office to receive a FREE Computer Network Assessment (a $397 value). Once we've signed an agreement with your referral, we'll rush YOU a free iPod Nano of your choice as a thank-you (or donate $100 to your favorite charity … your choice!). Simply call us at 940-220-7817 or e-mail us at connect@master-computing.com with your referral's name and contact information today!

The Beginnings Of Autumn

By Jessica Shelley



I think I can speak for just about everyone out there when I say that North Texas has been literally hot as hell lately. I mean, really, seven 100 plus days in a row! What's up with that?! Now I know that there are those crazy people out there that actually enjoy the heat and I have one thing to say to those people: you can go ahead and stop reading this article right now because you're crazy and should probably just move to the sun where you'll be happy.

Every year when September rolls around, I start to get a little excited because it FINALLY starts to cool down a little. And I say a little because instead of upper 90's and solid 100's we move down to like lower 90's. This may not seem like such a drastic change, but hey, I'll take what I can get.

It also renews my hope that eventually, just maybe, we'll see the 80's and dare I say it the gorgeous 70's. How people survived the Texas heat without A/C is just beyond me. Because if you're like me, you spend your day moving from one air conditioned building to another, spending as little time as possible outside in Hades' backyard.

So hopefully the realization that fall is just around the corner is enough to keep you going even though it would be much nicer to just stay home and take an ice bath.

Stay strong and count down the days to cooler weather.

Did Your Web Site Ranking Just Go In The Tank Because It's Not Mobile-Friendly?

As of last April, mobile-friendly web sites were given a big leg up on competitors. Known as "responsive" web sites, these sites instantly adapt to whatever device you are viewing them on.

As users were turning to smartphones and other mobile devices to surf the web, Google realized that most sites didn't display well on mobile devices. Therefore, Google updated the way they list sites, giving mobile-friendly sites a higher ranking.

Google hasn't removed all non-responsive pages from its top smartphone listings. But it's quickly heading in that direction.

According to Searchmetrics, many rankings have suffered as a result. Non-responsive yet high traffic sites such as SearchBug, Reddit and Webs.com lost visibility, while responsive sites such as Advance Auto Parts and Grist moved up in the ranks, gaining more traffic.

In addition to getting higher search rankings, responsive sites are easier for visitors to use. Happy visitors engage more, increasing the rate at which they turn into customers.

There are three ways to make your web site mobile-friendly:

1) Build a separate mobile edition that fits small screens and loads quickly.

2) Adapt your current web site design to be more mobile-friendly. In some cases it may be difficult to make such a design responsive on all devices.

3) Convert your current web site design into a responsive one. Going this route, you won't need a separate mobile version, and you avoid potential penalties from Google for having the same content on multiple domains.

Find out if your web site is mobile-friendly at www.google.com/webmasters/tools/mobile-friendly.

Who Else Wants To Win A $25 Gift Card?

The Grand Prize Winner of last month's Trivia Challenge Quiz is Jill Burns from American Airlines Credit Union! She was the first person to correctly answer my quiz question from last month: **What is the hottest place on earth: a.)Wadi Halfa, Sudan, b) Death Valley, California, c) Tirat Tsvi, Israel, d) Timbuktu, Mali** The correct answer was **b) Death Valley, California**

Now, here's this month's trivia question. The winner will receive a gift card to Barns and Noble!

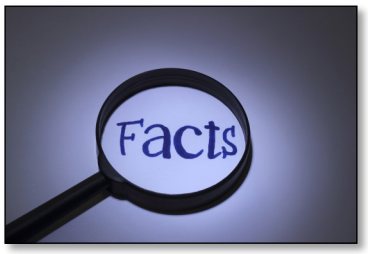
What were the first featured menu items at McDonald's?

a) Hamburgers **b) Hot Dogs**

c) Grilled Cheese Sandwiches **d) Tacos**

Email Us Right Now With Your Answer!
Trivia@Master-Computing.com

The Lighter Side:
IT Fun Facts



Technology has forever changed our lives and our world more than you know. Here are some numbers to put that fact into perspective:

1. About 4 billion people worldwide own a mobile phone, but only 3.5 billion people own a toothbrush.

2. Computers and other electronics account for 220,000 tons of annual trash in the U.S. alone.

3. About 300 hours of video are uploaded to YouTube every minute.

4. Around 100 billion e-mails traverse the Internet every day, and about 95% of those messages go straight to spam folders.

5. The annual amount of electricity it takes for Google to handle a billion search queries every day is around 15 billion kWh, which is more than most countries consume.

6. About 500 new mobile games appear on the Apple App Store each day.

7. The "father of information theory," Claude Shannon, invented the digital circuit at age 21 while he was in college.

8. Regular computer users blink only half as often as non-users.

9. Over 1 million children can say their parents met on Match.com