BUSINESS CONSULTANTS WITH A TECHNOLOGY FOCUS ISSUE 89 July 2016

TECHSAGE TECH TALK

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"

Welcome Jesus Ramirez

Jesus joined the TechSage team as an intern mid-June.

In his spare time, Jesus enjoys music and playing guitar. He is also an avid car enthusiast and has cycled long distances around San Antonio.

Jesus is also furthering his education in the technical field.

TechSage Solutions is excited to have Jesus as part of the team.

July 2016

This Monthly Publication provided courtesy of John Hill, President of TechSage Solutions.

We are Business Consultants with a Technology Focus and have Leveraged Technology to Propel Our Clients Toward Competitive Success in the San Antonio area for sixteen years. Our goal is to Simplify the use of Information Technology for our Clients so that they can focus on managing and growing their businesses.

5 Ways To Spot A Social Engineering Attack

"I'm not going to make payroll – we're going to close our doors as a result of the fraud."

Unfortunately, that statement is becoming more common among smaller businesses, according to Mitchell Thompson, head of an FBI financial cybercrimes task force in New York.

The FBI reports that since October 2013 more than 12,000 businesses worldwide have been targeted by social engineering–type cyberscams, netting criminals well over $2 billion. And those are just the reported cases. Often, due to customer relationships, PR or other concerns, incidents go unreported.

These unfortunate events were triggered by a particularly nasty form of cyberattack known as "social engineering."

Social engineering is a method cyber con artists use to lure well-meaning individuals into breaking normal security procedures. They appeal to vanity, authority or greed to exploit their victims. Even a simple willingness to help can be used to extract sensitive data. An attacker might pose as a coworker with an urgent problem that requires otherwise off-limits network resources, for example.

They can be devastatingly effective, and outrageously difficult to defend against.

The key to shielding your network from this threat is a keen, ongoing awareness throughout your organization. To nip one of these scams in the bud, every member of your team must remain alert to these five telltale tactics:

1.**Baiting –** In baiting, the attacker dangles something enticing to move his victim to action. It could be a movie or music download. Or something like a USB flash drive with company logo, labeled "Executive Salary Summary 2016 Q1," left where a victim can easily find it..

continued on pg2

Once these files are downloaded, or the USB drive is plugged in, the person's or company's computer is infected, providing a point of access for the criminal.

2. **Phishing** – Phishing employs a fake e-mail, chat or website that appears legit. It may convey a message from a bank or other well-known entity asking to "verify" login information. Another ploy is a hacker conveying a well-disguised message claiming you are the "winner" of some prize, along with a request for banking information. Others even appear to be a plea from some charity following a natural disaster. And, unfortunately for the naive, these schemes can be insidiously effective.

3**. Pretexting** – Pretexting is the human version of phishing, where someone impersonates a trusted individual or authority figure to gain access to login details. It could be a fake IT support person supposedly needing to do maintenance…or an investigator performing a company audit. Other trusted roles might include police officer, tax authority or even custodial personnel, faking an identity to break into your network.

"The problem with social engineering attacks is you can't easily protect your network against them."

4. **Quid Pro Quo** A con artist may offer to swap some nifty little goody for information… It could be a t-shirt, or access to an online game or service in exchange for login credentials. Or it could be a researcher asking for your password as part of an experiment with a $100 reward for completion. If it seems fishy, or just a little too good to be true, proceed with extreme caution, or just exit out.

5. **Tailgating** – When somebody follows you into a restricted area, physical or online, you may be dealing with a tailgater. For instance, a legit-looking person may ask you to hold open the door behind you because they forgot their company RFID card. Or someone asks to borrow your laptop or computer to perform a simple task, when in reality they are installing malware.

The problem with social engineering attacks is you can't easily protect your network against them with a simple software or hardware fix. Your whole organization needs to be trained, alert and vigilant against this kind of incursion.

For more on social engineering as well as other similar cyberthreats you need to protect your network from, get our latest special report on this crucial topic:

The Top 10 Ways Hackers Get Around Your Firewall And AntiVirus To Rob You Blind

Don't let your organization be caught like a sitting duck! You've worked way too hard to get where you are today to risk it all due to some little cyberhack you didn't know about. Call us at **210-582-5814**, or e-mail me direct: **jhill@techsagesolutions.com** and get your copy of this crucial preventive guide today – before your company becomes yet another social engineering statistic.

Can You Answer this Security Question?

What type of malware do users inadvertently install with USB thumb drive?

A. Spam B. Trojans C. Buffer Overflow D. Logic Bomb

Answer: **B.** Users can unknowingly transfer and install Trojan horse malware onto their systems with USB thumb drives. Spam in unwanted e-amil filtered with anti-spamn software. A bugger overflow occurs when a system receives unexpected data or more data than program can handle. A logic bomb a program or code snippet that executes in response to an event, such as a specific time or date.

Ransomware: The Dangers & How to Protect Your Business

Ransomware is a growing problem around the world. In case you haven't heard of it before, ransomware is a particularly nasty type of malware that locks up your computers, but with a catch: If you pay a ransom, the villains will (sometimes) unlock your machine and you can continue on. The thieves normally demand payment of a few hundred dollars per machine to be paid using Bitcoin, an untraceable form of electronic currency. Obviously, a ransomware attack can bring your business to a standstill and end up being quite costly, assuming the perpetrators follow through on their promise to unlock your machines after you've paid the ransom.

The hackers are going after everyone, but some industries seem to be more vulnerable than others. For example, as 75% of hospitals in the US could have been hit with ransomware in the last year, according to the new survey released by Healthcare IT News and HIMSS Analytics. A lot of them might not even be aware that they've been hit — about 25% of them are either unsure or have no way of knowing whether ransomware attacks were perpetrated against them or not.

Why are the bad guys targeting healthcare providers? And why now? According to Chris Ensey, COO of Dunbar Security Solutions, the answer is simple. It's a quest for more revenue. ***"What we're seeing is the macroevolution of ransomware and the tactics that are being used by organized crime to continue to expand the revenue generated from ransomware. The most productive way to do that is by targeted campaigns."***

Healthcare organizations make good targets for hackers for several reasons, including often lax IT security and also because there is a market for patient data. Hackers that are able to get into a healthcare provider's IT system can make money two ways: They can retrieve and sell on any data they extract and as well as demand ransoms.

The ransomware epidemic is far from being limited to the healthcare industry though. Any organization with a substantial investment in IT equipment can make a good target. In fact, ransomware has gone from a niche attack to a booming criminal market since its introduction in 2013. Attacks are being reported in a number of organizations both large and small in several verticals. For example, in the past ten months, 29 different federal agencies detected and reported 321 incident reports of ransomware-related activity. One famous virus, "CryptoLocker," infected more than 250,000 computers around the world and was used to target businesses and consumers. The virus enabled the extortion of about $27 million from infected users in just a two month period.

Ransomware is now an industry unto itself and, like any forward-thinking tech vertical, there's a big emphasis on speed and innovation. Malware developers are looking to ramp up their infection volume while also coming up with new ways to slip past corporate defenses.

What To Do About It

Anyone working in IT today knows that one of the most difficult challenges involves getting people to be aware of hacking and ransomware threats, and to take reasonable security precautions as a matter of routine. However, people being people – and busy people at that – changing their behavior is difficult, and that's how ransomware infections spread.

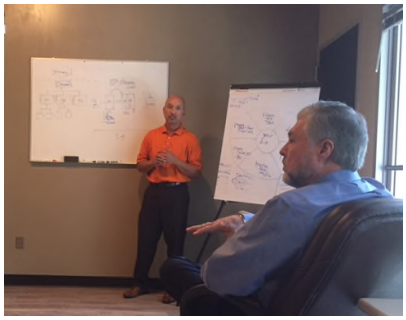
Here's a mantra that MSPs and IT admins within organizations need to keep in mind at all times:

Keeping your data safe means protecting it from your least technically savvy employee.

TechSage's new Workspace-as-a-Service protects our clients by making it harder to install ransomware in the first place. And if an employee does get hit, their machine won't contain any of the data the thief wants to grab. Wiping the PC gets rid of the ransomware and the previously infected machine can be returned to service in a few minutes. The platform also prevents the infection from getting to the servers and even if a black hat tries that, they won't succeed. A TechSage-enabled server is locked down and secured to prevent a server-based attack as well.

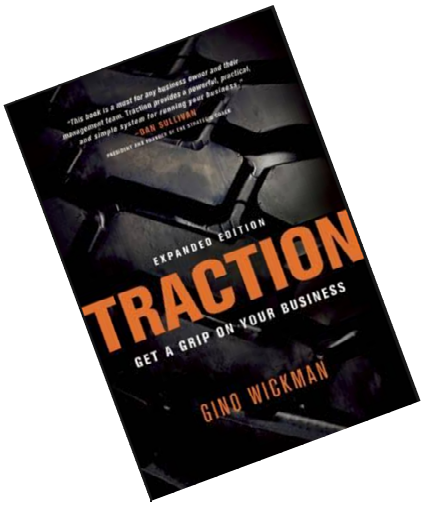
Contact us at **210-582-5814** or email at **info@techsagesolutions.com** to learn how you can use TechSage's Workspace-as-a-Service platform to improve the overall security of your IT systems.

We Are Always Learning For You!



Don Maranca is not only our business coach but also a certified EOS (Entrepreneurial Operating System) trainer. Don gave the TechSage team an overview of the EOS system, which is based on the book "*Traction*" by Gino Wickman.

In "*Traction*", you'll learn the secrets of strengthening the six key components of your business. You'll discover a simple yet powerful way to run your company that will give you and your leadership team more focus, more growth, and more enjoyment. Successful companies are applying "*Traction*" every day to run profitable, frustration-free businesses.



There is a companion book called "*Get A Grip*" that is a fictionalized story of a company actually implementing the ideas in "*Traction*". If you like content in a story line, I suggest readying this book first for better understanding the "T*raction*" principles.

TechSage's belief is to train all team members to propel to excellence in company practices and by serving our clients. John and I have both read this book several times and we are currently applying this concept to our business. Because of my belief in learning, I will send the first person who emails me at **ehill@techsagesolutions.com** a **free** copy of this book! Add Traction in the subject line.

Referral Contest!!

Refer a friend to TechSage Solutions between June 1, 2016 - August 31, 2016 for a chance to win an Amazon Echo.

How the Contest Works:

1) Call or email us with your referral information.
2) We will call to schedule an appointment.
3) We will pay you or donate $25 to your favorite charity for anyone that you refer to us, who we get an appointment with.
4) When your referral becomes a client (and spends $1,000 or more), we will pay you $75 more or donate $75 more to your favorite charity. Plus, we will give your referral $100 off the purchase.
5) What makes a good referral for TechSage Solutions? A business owner who has 10 or more PC's and needs help with their network, data backups, email server or is just interested in having a second opinion on how they are doing things now. We provide service to the San Antonio area and surrounding cities.

Send an email to ehill@TechSagesolutions.com or call (210) 582-5814.

Shiny New Gadget Of The Month:

Finally: An Easy Way To Control The Family Net

Got kids age 6 to 16?

Circle With Disney is a new device that helps make Internet struggles at home a thing of the past. Imagine: no more negotiating with kids to get off the web and come to dinner (or get their homework done).

This 3½-inch white cube with rounded corners (it's not exactly a circle…) lets you control Internet usage around your house with a tap on your iPhone. (Android compatibility coming soon.)

With presets by age group, or custom controls, Circle helps you restrict who in your family surfs what, and when. It also tallies how much time each person spends on any site. You might even want to monitor your own Facebook or Pinterest time (or maybe not…).

Circle also lets you put your whole home network on pause, sets up in about five minutes and works with your router.

Just $99 at MeetCircle.com may be all you need to win your family back from the web – at least for a few minutes a day.

Your Crystal Ball For Hiring

I don't know if what I'm about to share with you is impressive or pathetic…

First, a brief history to earn your trust. I studied in graduate school 20 years ago with the Father of Management, Peter Drucker. He estimated that managers make hiring mistakes 50% of the time.

This topic of hiring talented teams always intrigued me. My father was an industrial psychologist, so I had been around this topic for my whole life. In 1998 I finished my PhD dissertation on this topic of evaluating various methods for hiring. I had read about 50 years' worth of research and noted some interesting findings, like "Don't ask hypothetical questions." As it turns out, candidates give you hypothetical answers. Yet today, so many leaders pose hypothetical questions to their candidates – "How would you do this? How might you do that?"

During my PhD dissertation study, I found that, consistent with the field of research, there were a few key things that really worked in interviewing: 1) to have a specific set of criteria in mind (scorecard), 2) to collect not a little, but a lot – hundreds of data points – on a candidate's accomplishments and failures from their actual past experiences, and 3) then scoring candidates on a consistent set of criteria (apples to apples).

These "past-oriented interviews," as I called them in my PhD dissertation, were the most valid and reliable predictor of a candidate's future performance on the job (as opposed to "future-oriented" or hypothetical interview formats). I wanted to share this important insight with the world. To give leaders a crystal ball.

An interview process, if done right, gives you a crystal ball.

For the last 20 years, my colleagues and I have used this approach to evaluate over 15,000 candidates for leadership jobs in all industries. We have taught thousands of people how to use this method for hiring – business leaders, entrepreneurs, as well as government leaders, including three sitting US governors, and top brass in the military. It works. Clients who follow our methods achieve a 90% hiring success rate. And you can too. (Come to my SMARTfest event and I'll teach you how!)

And this approach follows a very simple structure of collecting highs and lows from a candidate's education years, then asking five questions about every job: What were they hired to do? What did they accomplish that they were proud of? What were mistakes in that job? Who did they work with and how were they viewed? And why did they leave that job?

This is straight out of our book Who, which has been – since its publication in 2008 – the #1 top-selling and most-acclaimed book on this topic in the world. And this topic, hiring talented teams, has become the #1 topic in business, if you look at any recent survey of what's on the minds of CEOs and investors.

We want you to apply this concept to improve your hiring success rate from 50% to 90%. That's why we're giving you free access to the Who Interview Template at GeoffSmart.com/smartthoughts.

Geoff is Chairman & Founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times bestselling book Who: The A Method for Hiring and the author of the #1 Wall Street Journal bestseller Leadocracy: Hiring More Great Leaders (Like You) into Government. Geoff co-created the Topgrading brand of talent management. Geoff is the Founder of two 501c3 not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring and The Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a B.A. in Economics with Honors from Northwestern University, an M.A., and a Ph.D. in Psychology from Claremont Graduate University

Want to know your Lyft or Uber passenger rating?

Ratings are a two-way street with both Uber and Lyft. Of course, as a passenger you can rate your driver. Yet passengers are rated too, by their drivers. To find your average Uber passenger rating, open your Uber app and tap the menu bar in the top left corner. Then follow this path: Help > Account > "I'd like to know my rating." Tap "Submit" on the explanation page and your rating should then appear. Lyft has no such system, however their support team may send your average passenger score to you if you request it. Want to improve your score? Be nice to your driver and show up at your pickup location on time.

-Glitterless.com

Forget apps…here comes the voice-controlled future.

Soon, we won't be fumbling around with a gazillion different apps, trying to figure out which one turns off the sprinklers in the front yard… Apple Siri, Amazon Echo and now Google Home all point to the future of digital living. When it comes to voice plus smart machines vs. finger taps on a phone, voice wins, hands down. You don't want to use a weather app, you just want the forecast. Your customers won't go to your website and download an app; they'll interact with your business in some way by voice. That future will arrive in the next five to 10 years. Will your business be ready?

-Inc.com

Skip the airport – just hop in your e-jet and fly!

By 2018, owning your own battery-powered VTOL (Vertical Takeoff and Landing) two-seater could be one step closer to reality. That's the plan for the Lilium Jet, being developed in Germany under the auspices of the European Space Agency. This Jetsons-looking aircraft sports "fly-by-wire" joystick controls, retractable landing gear and gull-wing doors. Its developers claim it will have a top speed of 250 miles per hour and could be available to the public as soon as 2018. Designed for daytime recreational flying, it's quieter – and safer – than a helicopter, thanks to its battery-powered ducted fan motors and intelligent, computer controlled takeoffs and landings. And pricing, according to its developers, will be far less than similar-sized aircraft.

-GizMag

Is your mobile website stressing people out?

Of course, page-load times can affect conversion and brand perception. But did you know they also affect user heart rate and stress levels? According to a 2016 study on mobility by Ericsson, page-loading delays lead to an average 38% jump in heart rate. Remember the last time you watched a horror movie? It's about that stressful… Not how you want your visitors to feel. To keep your page loads painless and your visitors happy, make sure your website is mobile-friendly. It needs to be quick and easy to navigate and engage with. You have a lot at stake in your website – and making it stress-free for visitors could make a big difference.

-HubSpot Blog

Who Else Wants To Win $25 Gift Card?

Last month, Tricia Garcia took the challenge by answering the trivia question correctly. She has a $25 Texas Roadhouse card coming her way.

Here is this month's trivia question. The winner will receive a $25 Google play card.

Which of the following worldwide computer viruses caused an estimated $5 billion worth of damage?

A) Code Red B) ILOVEYOU C) Melissa D) Cryptolocker

Email Megan Now With Your Answer!

mhernandez@techsagesolutions.com

With Subject: July Trivia Answer

At the end of July we will draw from the correct answers for the gift card