Central Texas Technology Solutions
Your Business Partner

Technology Monthly Newsletter
December 2017

Happy Holidays

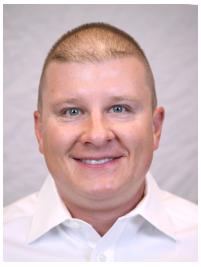
During this season, we would like to take time to reflect upon the good things we have… like our partnership with you!

We appreciate working with you and hope that the holidays and the coming year will bring you happiness and success.

Please note that our office will be closed on Monday, December 25th and Monday, January 1st, but if you have an emergency you can call us at (512) 388-5559.

Thank you from all of us at CTTS: Josh, Sara, Jamie, Kurt, Tony, Brandon, Kara and Dustin

Central Texas Technology Solutions
Your Business Partner For 15 Years



This monthly publication provided courtesy of Josh Wilmoth, CEO of CTTS, Inc.

"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!"

Cybercriminals Confess: The Top 5 Tricks, Sneaky Schemes And Gimmicks They Use To Hack Your Computer Network

The contemporary world is rife with digital thieves. They're penetrating the complicated data structures of huge credit-monitoring companies like Equifax, scooping up the personal information of millions of people. They're releasing sensitive customer data to the public from discreet businesses like Ashley Madison. They're watching webcam feeds of our celebrities without them knowing; they're locking down the systems of public utilities like the German railway system; they're even managing to steal thousands of gigabytes of information directly from high-profile government entities like the CIA.

They're also targeting small businesses exactly like your own and extorting them for thousands and thousands of dollars. When running a company, it's vital to have a dedicated security team, equipped with the most up-to-the-minute security technology, on your side to protect you from these malicious cyberthreats. But it's not enough to leave it to somebody else. You also need to be informed. Here are five of the most common ways hackers infiltrate your network:

1 Phishing Scams
You receive an e-mail in your work inbox coming directly from a high-ranking employee with whom you've been working on a project. Inside is a link he needs you to click to access some "vital information," but when you click it, it rapidly installs a host of malware on the computer, spreads through the network and locks out everyone in the company.

Phishing scams are the oldest trick in a hacker's book – ever received one

of those "Nigerian Prince" scams? – but they're still wildly successful. Not only that, but they're becoming increasingly more sophisticated. As Thomas Peters writes for "Newsweek," "The best messages look like they're trying to protect the company. One well-meaning system administrator even offered to post a PDF that could deliver malware on an internal server because it was called, 'How to avoid a phishing attack.'" How's that for irony?

2 Social Engineering
Social engineering is a type of "hacking" that uses real, well-intentioned people to carry out its schemes, rather than intricate lines of code. This is especially effective for gathering sensitive information that can later be used in another type of attack – e-mail passwords used for phishing scams, for example. Maybe your IT guy receives a call from the "secretary" of one of your clients, pretending that they're experiencing problems with your service due to some firewall, a problem that your IT professional is more than happy to help out with. Before you know it, the caller knows the ins and outs of your entire security system, or lack thereof. Social engineers have been known to use phone company customer service departments, Facebook and other services to gather Social Security or credit card numbers, prepare for digital robbery and even change the passwords to your central data network security.

"When running a company, it's vital to have a dedicated security team, equipped with the most up-to-the-minute security technology, on your side to protect you from these malicious cyber threats."

3 Password Hacking
You may think that your passwords are clever and complicated, filled with exclamation points and random numbers, but it's rarely enough. With information gathered carefully from social engineering or a simple check on your employees' social media accounts, hackers can easily use brute-force to figure out that your password is the name of the family dog, followed by your anniversary (for example). That's if they didn't already manage to steal your password through one of the techniques listed above.

4 Fault Injection
Sophisticated hackers can scan your business's network or software source code for weak points. Once they're located, they can surgically attempt to crash the system through snippets of code they splice in expressly for that purpose. Different commands can do different things, whether they want to deliver a devastating virus, redirect links on your website to malicious malware or steal and erase vast swathes of information.

5 USB-based Malware
At the last conference you attended, someone probably handed out free branded USB sticks to keep their business top-of-mind. Hackers will sometimes covertly slip a bunch of infected USB sticks into a company's stash. The instant somebody tries to use one, their computer is taken over by ransomware.

So What Can I Do About It?
It's a scary world out there, with virtually everyone left vulnerable to digital attack. Knowing the strategies hackers deploy is half the battle. But, frankly, these techniques are constantly changing; it's impossible to keep up by yourself.

That's why it's so important to utilize only the most up-to-date security solutions when protecting your business. Hackers move fast. You and your security technology need to stay one step ahead.

FREE Report: The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks

Eighty-two thousand NEW malware threats are being released every day, and businesses (and their bank accounts) are the No. 1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious reputational damage, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack, you MUST read this report and act on the information we're providing.

Claim your FREE copy today at **https://www.cttsonline.com/security/** or call our office at (512) 388-5559.

The Top 3 Things I Have Learned From John Mackey

By Josh Wilmoth

Recently, I had the honor of meeting John Mackey, CEO of Whole Foods and author of *Conscious Capitalism*. He has received numerous awards for his excellence in entrepreneurship and I wanted to share with you the top 3 things I learned from him:

Know the Value of Your Business

John Mackey describes business as a great force for good in the world, saying that businesses create value for all involved. *Conscious Capitalism* is a system for overcoming poverty and creating wealth. Unfortunately, most people do not view businesses and capitalism in this light, but instead as evil entities driven by greed and selfishness. That is why he decided to write the book, *Conscious Capitalism*, to change the negative perceptions of businesses and business owners. In his book he wants you, the business owner, to ask, "What value are you creating with your business? Is there a potential for a higher purpose?". Of course, we all want to make money—need to make money in order to survive—but that alone does not drive a business to success. Businesses need to create value for your customers, your employees, your suppliers, and investors. That common goal fuels the needs and desires of the organization as a whole, unifying the business as you work together to create prosperity for all.

Run Your Business on the Happiness Principal

If you want to be happy, John Mackey says you should cultivate these three things: gratitude, forgiveness, and love. By practicing these concepts on a daily basis, a healthy culture can be created at home and in the workplace. When building your company, take care to hire a Team of the very best employees possible, train them well and make sure they're happy. When your employees are happy, they serve the customers well and the customers, in turn, are happy. And when your customers are happy, business is good. But keeping your employees happy is easier said than done. First off, you want to make people feel secure in the workplace. If you manage your employees with threats causing them to fear you, it leaves no room for growth on either side. Practicing a servant-based leadership style and treating each other with respect and dignity will build a healthy work culture. One tip he gave was to end your weekly staff meetings with a voluntary round of praise. When appreciating each other, it allows the group to connect and form a stronger bond as a true Team. When you hire a good Team and keep them happy, your company will thrive.

There is No Magical Formula for Success

There are always going to be challenges that your business faces, but Mackey encourages us to embrace these challenges. The journey is what makes life so sweet, not the destination. If everything was easy, life would be boring. We need challenges to force us to change and evolve into the best person possible. So, while there is no true answer on how to be a successful business, make it your mission and commit yourself to being the best, to have the highest quality goods and services, have the happiest employees, and the success of your business can only follow.

What Is Two-Factor Authentication and Why You Should Use It

Having a strong, unique password might not be enough if hackers trick you into giving it away or steal it from your email provider or bank.

That's why for your most sensitive accounts—think your email or banking accounts—you should set up two-factor authentication (or 2FA). This simply means adding a second step to log into your accounts. First, the password. And, second: either a code sent to your cellphone via text message, or created by a special app on your phone.

With two-factor, even if the hackers steal your passwords, they still won't be able to get in.

If you have questions on how to set this up, call us today to speak with one of our Security Experts: **(512) 388-5559**

Become A Better Public Speaker With This App Americans are terrified of public speaking. In fact, in most surveys about our fears, talking in front of a crowd far outranks even our fear of dying. But if you, like millions of others, break out in a cold sweat when you imagine giving a speech, you're in luck. There's an app for that.

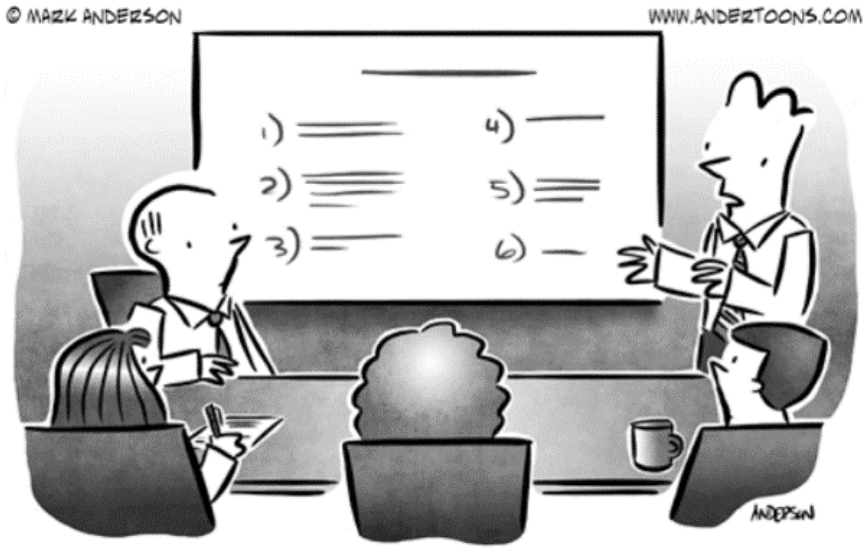
Developed during the Disrupt San Francisco Hackathon, Vocalytics is a comprehensive project dedicated to building an AI that will teach you to be a better public speaker. The ultimate goal is to develop a virtual trainer that can give feedback even better than what you'd get from a professional speaking coach.

The app – called Orai – uses machine learning to analyze your body language as you speak, ensuring that every word hits home. When paired with speech analysis project SpeechCoach.ai, you can take concrete steps toward killing it in front of any crowd. *TechCrunch.com 9/17/2017*

Top Tech Accessories To Make Your Life Easier The best gadgets help us navigate our lives with ease, making particular processes that much more hassle-free. With technology, it's often the little things that make all the difference in the world. Take AUKEY's car phone mount, for instance. At only $7.99 on Amazon, there's no reason you should be fumbling with your iPhone while you're using Google Maps on a road trip. The clip attaches directly to any air vent, putting your phone front and center for easy viewing and reducing the need for dangerous fiddling.

Or, pair an Amazon Echo with the Tp-Link Smart Plug Mini ($29.99), which allows you to activate all kinds of devices with your voice or your phone. It's the perfect first step toward a smarter home and a world of convenience.

If you've got a phone that's always dying, hook it up to an Anker battery case, which can extend the battery life of most phones by as much as 120%. For more small-scale tech solutions, check out Business Insider's list of "50 must-have tech accessories under $50." *BusinessInsider.com 9/28/2017*



"You're right, it is easier said than done. That's why I said it; because it's easy. Try and keep up."

Did You Know?

91% Of Cyberattacks Start With A Phishing Email

The majority of cyberattacks begin with a user clicking on a phishing email. Ever wonder why users continue to fall for phishing emails?

According to a new report from PhishMe that found that 91% of cyberattacks start with a phish, the top reasons people are duped by phishing emails are curiosity (13.7%), fear (13.4%), and urgency (13.2%), followed by reward/recognition, social, entertainment, and opportunity.