HAPPY HALLOWEEN!

JR-Tech Times

October 2017

Congratulations to Brandy T. at Axxis Corporation for winning our Customer Service drawing! Brandy wins a $100 Amazon Gift Card! See below how you can win!

3 Frightening Ransomware Tactics That Could Take Your Company Out Of Commission For Days

Ransomware is on the rise. Most companies that become infected just want to get their systems back online. CNBC reports that over 70% of businesses infected end up paying the ransom just to get things up and running again. To ad further insult to injury, many companies never retrieve all their data back, even when they pay. Take a look at these three key ransomware tactics that take companies down every week and how to protect your company from these horrifying attacks.

Hair-raising ransomware. Ransomware attacks are on the rise and so are the ransom amounts. From 2015 to 2016 the number of ransomware attacks quadrupled and this year it looks like we will at least double over last year. Infections are projected to continue rising. So, how are these attacks happening with such frequency? Where do they even come from? And, what can you do to safeguard your company from disaster?

Frightening ransomware tactics. There are quite a few ways ransomware can wiggle into your network, but here are three of the most prominent we've seen this year.

1. Infected e-mail messages open the door. According to a recent IBM study, almost 40% of all spam messages contained ransomware last year. This is a staggering number considering there were over 30 trillion spam e-mails sent out. Don't become a statistic. Keep your company safe with a solid spam filtering solution in place to knock out those spam messages before users can open and read them. Also, inform your staff of the risks associated with spam messages and advise them to report suspicious messages. Make sure they know not to click on links in the message or open any attachments. Links and attachments are the preferred method for hack-

(Continued on page 2)

JR-Tech
Delivering Trouble-Free IT

JR-Tech
506 W. Graham Ave. Ste. 207
Lake Elsinore, CA 92530
951-319-4040
www.JR-Tech.com
youtube.com/c/JR-Tech

What's Inside

Don't Fake Professionalism…….Pg. 2

Scalable Business Solutions To Give You Eight More Arms And Legs……..Pg. 3

End Of Life For Office 2007……..Pg. 3

Is My Computer Really Being Monitored At Work?.....Pg. 4

Ghostly Technology Struggles……...Pg. 4

Enter to Win a $100 Amazon Gift Card!

You can have a chance to win too! Simply enter your name on the Customer Satisfaction Survey. At the end of every job close notification e-mail, we include a link to a brief survey. Each time you complete a survey about your job ticket and enter your name you are entered to win a drawing for a **$100 Amazon Gift Card!**

Where Does Candy Even Come From?

I haven't met a person yet who doesn't have an answer when I inquire about their favorite candy. However, I've always been curious where the concept even came from. So, here you go—a few fun candy facts for the Halloween.

The first candy. While cavemen were said to have used dried honey in a taffy-like concoction to satisfy their sweet tooth cravings, the concept of actual candy came later around 2,000 B.C. Egyptians mixed honey with figs, nuts, dates and even spices to create candy treats for their worship ceremonies — an offering to the gods.

Evolving over the years. Candy evolved over the next few centuries as sugarcane spread around the globe. Chinese people began adding sugar and nuts to ginger and licorice root to create small candies. Indians were really the first to make actual sugar candy though. About 3,000 years ago they figured out how to make brown sugar. By

(Continued on page 3)

3 Frightening Ransomware Tactics...

(Continued from page 1)

ers to deliver ransomware to your computer and network.

2. Browsing websites online can put a spell on you. Osterman Research found that 24% of all ransomware infections came through websites that were unassociated with an e-mail. People simply browsing online trip over a horribly infected site that latches onto their computer. Unfortunately, these types of ransomware don't just stop at one computer, they feed off the entire network and if they can will spread like wildfire.

3. Social media and storage drives deliver a jump-scare. Keep your personal life at home. Storage drives and social media websites can be risky for businesses. Osterman Research also found that roughly 17% of the assessed ransomware attacks were rooted from social media, storage devices, and business applications.

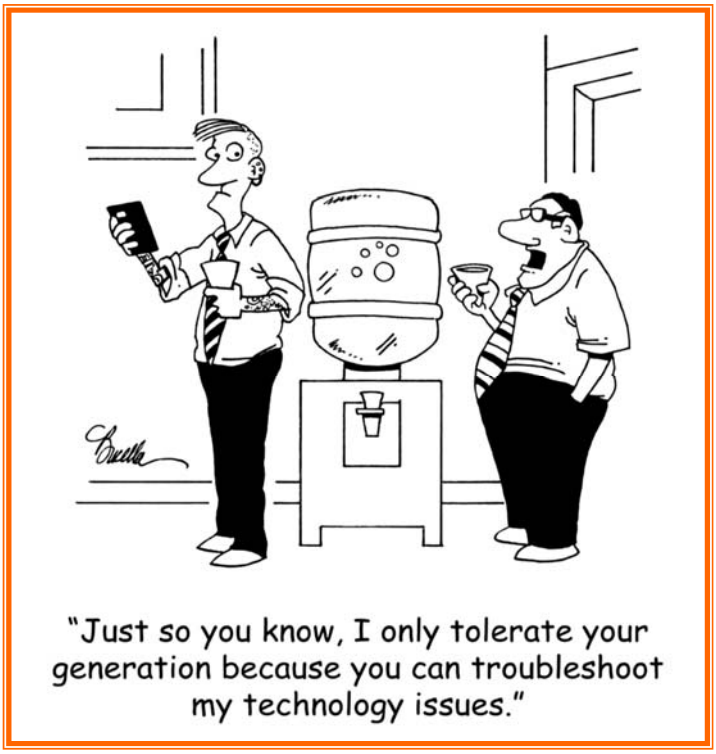
Are you prepared? We have handled our fair share of ransomware attacks this year and the best advice we have to give is be prepared. Regardless of how much money you spend on security, there is no sure fire way to safeguard your office from all threats. Here are a few things you can do to prepare and recover quickly from a ransomware attack.

Lock down your network tight. Make sure you have security protocols in place to only allow users access to necessary systems for their positions. This user level access will prevent their computers from infecting more critical systems should something happen originating on their workstation.

We've found a sweet solution. Good back-ups! The only businesses who have been able to quickly resolve a ransomware attack without paying the ransom, close to 100% of the time, are those who had dependable back-up and recovery solutions in place.

A few short hours of prevention can give you back two days of operations. Ok, so that just sounds silly right, but it's not. On average, most businesses face a minimum of two days down time when there is an infection and there are no viable backups. You would be surprised at the number of unmonitored and failed back-ups we find when running network assessments for new clients. Incremental backups are also a major concern. Some companies only back-up once a week or a few times each month. This means, all the time between the infection and the last back-up will be lost unless you break open your pocket book, fork over the ransom, and cross all your fingers and toes.

Ready for a FREE Network Security Assessment? Give us a call today if you are concerned about any of these terrifying tactics giving you a jump-scare. We will go through all the aspects of your network to measure how well each piece is performing. Then we will present you with a full report of our findings so you can easily see where your systems can be improved. No tricks, no treats, just a full audit that includes checks on your firewall, antivirus, security policies, and much more.



Don't Fake Professionalism

Many people talk about professionalism as if it's some fancy costume to wear. Professionalism is truly being respectful, skilled and reliable.

The service industry. Showing your professionalism, as an individual and as a representative of your organization, can actually improve your odds of obtaining new business.

R-e-s-p-e-c-t. It's not just about 'yes, ma'am' or 'no, sir', but more about listening, dressing appropriately, and conversing accordingly. Respect others and treat them the way you would like to be treated.

Presentation. Treat every encounter with clients and colleagues as an opportunity to show your best self. Always dress a bit over the general dress code for the setting and come prepared with the facts you need to hold an intelligent conversation.

Listen and converse smartly. Your communication method, listening or being heard, is extremely important. Stay away from difficult topics like politics or religion and focus on current events that hit home for your audience. Don't forget to acknowledge the human you're talking to as well. If you are all business you may come off too bold.

Where Does Candy Even...

(Continued from page 1)
250 A.D. they began making actual candy.

The first to manufactured candy. Arabs invented caramel by 950AD, however they used it initially as a hair product. They built the very first sugar refinery in the world.

A growing market for candy. In the 14th century, Venetians began importing sugar and making small candies too. Everyone seemed to love and crave these sugar sweets. During the middle Ages, sugar candies became very popular and were even thought of as a drug. Often candy was highly sought after and reserved for the very wealthy people as sugar had become very expensive.

Machines make candy affordable. During the 14th century, cocoa became a staple ingredient in the candy making with a whole string of new confections coming to life. All these rich ingredients helped push the mass production of candy beginning in the 18th century.

A rose by any other name is just as sweet. Candy, also called sweet treats or lollies, are quite tempting and delicious. Don't fill up too much this Halloween.

Scalable Business Solutions To Give You Eight More Arms And Legs When You Need Them

Ramsomware infections are truly a costly pitfall for businesses. Let us lighten the mood with a little view of the other side. Get ready! This is a classic, laughable, business mistake made by the WannaCry ransomware hackers that we all can learn from. This is a prime example of why all businesses should rely on scalable solutions to support their company.

From 2 to 20 in the blink of an eye. Is your business growing? Are you ready? Many companies struggle to add staff and equipment one by one as needed. What if you could have a solution in place that makes adding staff as easy as a quick phone call? After all, we are all in the business of growing our businesses.

Hackers WannaCry classic mistake. Obviously our companies are a much higher caliper than a cluster of hackers trying to attack others for personal gain, but I couldn't help but share a little laugh at their expense. WannaCry is a ransomware program put together by a band of hackers to infect computers and hold data hostage for a ransom much like CryptoLocker. WannaCry spread like wildfire hitting hundreds of thousands of targets in a relatively short amount of time. While this was the ultimate goal of their malicious attack, it backfired when WannaCry creators couldn't handle the volume of potential payments on the back end. The WannaCry program just couldn't keep up tracking the ransoms sent and payments received. So, hackers were reduced to basic bookkeeping tasks. The program couldn't match the payment with the unique address for the ransom, so the creators had to sit and figure out which of their victims paid and should be sent their encryption key. This wastes a ton of resources they probably didn't even have. I'll bet they were scrambling for warm bodies to put in front of computers just to process the information.

Growing pains. If the creators ran a legitimate company, a few scalable solutions could have saved the day. If only those hackers had a plan in place to efficiently spin up new computers for new employees to help manage this unexpected growth. This is a prime example of how an influx of business can bring a surge of needs. Make sure your technology solutions are ready for growth so you can eliminate growing pains like this and add staff when you need them most.

End Of Life For Office 2007

There have been quite a few announcements over the past year about the end of life for specific products. Office 2007 has finally reached its dreaded end date.

October 10th, 2017 marks the end of life for Microsoft Office 2007. Why is this such a big deal for businesses? Office 2007 has been a widely used set of programs in businesses around the world. However the support lifecycle end means there will be no new security updates, additional support options or technical content updates. This means, your company may be vulnerable to attack. Security weaknesses and bugs that come up will no longer be addressed by Microsoft and this will allow hackers to exploit users in various ways.

Many people had been waiting for a better version of Office and truly didn't see any reason to switch from Office 2007 over the past decade. Now with the end of life this month, it is critical to dive into a newer Office suite. We recommend Office365 or Office 2016.

Plan for your upgrade. It will take time to get all your workstations up to speed and if you are moving to an Office365 solution, the e-mail migration needs to be scheduled so it won't interrupt your regular flow of business. Need help? Give us a call today for your upgrade project.

$1,000 CASH Referral Program

We strive to provide exceptional customer service and as a natural result, we hope business owners who know us, would refer JR-Tech to other business owners in their community.

That's why when you refer a business owner to us and they become a client, we will give you

$1,000 CASH!

For more about our referral program, please visit our website:
JR-Tech.com/$1000referral

"We make all of your computer problems go away without adding additional full-time I.T. staff!"

Ask about our fixed price service agreements — Computer support at a flat monthly fee you can budget for, just like payroll!

Inquiring Minds...

MSPmentor 501 2017 WINNER

Is My Computer Being Monitored At Work? Yes, your computer is being monitored at work, but don't get too paranoid. Sure, in 1940, it would have been frowned upon to use the company typewriter to type a personal letter. Back then, monitoring meant a human hired to walk around the room and look over the shoulder of each typist. Most companies are much more understanding these days.

In the 21st century, monitoring is largely electronic, but the rules have not changed. Keep your professional and personal spaces separate. Many organizations monitor for both intellectual and network security. Personal laptops that aren't managed by company IT could be vulnerable to hacking. They also could be used to take confidential data offsite or become infected by personal data and this could easily bleed into the company's network.

Acceptable Use policy. Read and follow your organizations Acceptable Use policy. Most companies ask users to reframe from downloading movies, pictures, and large files that take up a tremendous amount resources on the network. Bandwidth is generally monitored for use and security issues so don't be surprised if you are approached about downloads. Excessive use by any one user can slow down the entire office killing productivity.

Unsecured apps and websites pose a risk to confidential data. Many companies let employees know what applications are acceptable for business transactions and block unsecured sites in-house. Sometimes it is easier to use them when you're working outside the office, but keep in mind using them at any time for company business can put proprietary information at risk.

Advocate for your Acceptable Use policy. Be an advocate for the proper use of tools in your business. Regardless of your position, security always begins with those who use the systems presented. If you're worried everyone isn't on the same page or don't have an Acceptable Use policy, take time to put one together. Keeping everyone informed about the dangers will ultimately keep your data safer.

Ghostly Technology Struggles. Here are a few silly tech accounts to tickle your funny bone. Enjoy!

- A user called in and said their monitor wasn't working. After the standard protocol for debugging, the user said, "There are no lights and he could not find the power button." The tech finally asked, "Is there actually a monitor on the desk?" Seemed like a crazy question, but the user replied "No." New monitor delivered; problem solved.
- We received a call from a business owner who had been vacationing over the summer and when she returned, she frantically called in. She explained that everything was different on her computer and she didn't know why. The machine had been turned off for a few weeks. Turns out she had been working on her Mac laptop all week and was then confused by her Windows machine at the office. Brain retraining.

JR-TECH
Delivering Trouble-Free IT

JR-Tech
506 W. Graham Ave. Ste. 207
Lake Elsinore, CA 92530
951-319-4040
www.JR-Tech.com
youtube.com/c/JR-Tech


Zombie Hackers

They're Coming For Your Data Through Open Ports!

Hackers have become more crafty about their attacks these days. Even firewalls can be a point of entry. That's right! The very device you put in place to keep your network safe and filter data coming and going could be a HUGE security risk. Open ports on your firewall leave a backdoor open for sneaky attackers. Worried about your firewall? Not sure if it is being maintained appropriately? Give us a call today. We will review your current systems and make suggestions to increase security.

Give us a call today to claim your CyberSecurity Audit.

JR-Tech • 951-319-4080