Happy St. Patrick's Day!

March 2019

microTECH Times

Covered I.T. 24/7—Never Worry Again!

3 Ways To Secure Your Network Because Luck Is What Happens When Preparation Meets Opportunity

Ransomware has mostly faded from the headlines since WannaCry and NotPetya wreaked havoc across the globe in 2017. The attacks sparked so much alarm that more people than ever are backing up their files, which effectively deadens a ransomware attack, but are your efforts working and in place today?

Too many of us have short memories and as the WannaCry sobs become a faded memory, cybersecurity experts warn against getting lazy about backing up your files. The first instance of a ransomware threat was detected 30 years ago--in 1989--when an AIDS conference was "attacked" by floppy disks. Since then it has been a relentless duel of one-upmanship between the bad guys and the cybersecurity experts.

The reality is that most ransomware attacks are made at random despite the mountain of reports that indicate cybercriminals target specific institutions and organizations. The bad guys will go after anyone with a computer...including you. In 2017 Amit Serper, a principal security researcher at Cyberreason, became a hero for creating the first "vaccine" to slam the door on the devastating NotPetya attack. However, even as his vaccine was universally viewed as a shaft of light in the dark history of ransomware, Serper was a warning of the vaccines' limitations. "They're only useful," he said, "to contain a specific outbreak."

So what can you do? Back up off network. Then back up...and back up some more! Take a look at these three ways to clean up your network and prepare your company for a cyber attack.

1. Implement a comprehensive backup strategy. A multifaceted approach helps blunt the force of a ransomware attack. A company's information cannot be held hostage when it's stored securely off-network and ready for recovery. Tejaswini Herath, an associate professor of information services at Brock University, urges a "tiered" or "layered" backup strategy that includes redundancy. Use devices not connected to the network, keep a copy

(Continued on page 2)

microenterprises

PO Box 503
Deepwater, NJ 08023
877-540-6789
www.microent.net

What's Inside

Irish Toast

To all the days here and after—May they be filled with fond memories, happiness, and laughter.

♣

May your troubles be less and your blessings be more and nothing but happiness come through your door.

♣

A good employee is like a four leaf clover, hard to find and lucky to have.

♣

May the best day of your past be the worst day of your future.

Celebrate Spring

March is filled with fun observances to help us celebrate the new season. Take a look at the holidays coming up and great ways to get your business in shape for the new season.

March observances. The month of March is full of fun little observances. First up is Dr. Seuss's Birthday and Read Across America Day on March 2nd, then World Book Day on the 5th, National Pi Day on March 14th and, of course, St. Patrick's Day on March 17th. International Earth Day on March 20th, the first day of Spring and World Meteorology Day on March 23nd finish out the month with over a half dozen reasons to celebrate in March.

Put a little spring in your step. Spring will begin March 20th. This is the time of year to clear out all those old nooks and crannies to make room for a new season of growth in your business. What's in that old closet anyway? Why do we still have that old printer

(Continued on page 3)

3 Ways To Secure Your Network...

(Continued from page 1)
off-site and encrypt your back-ups. Recovery from an attack is only as good as the back-ups you store.

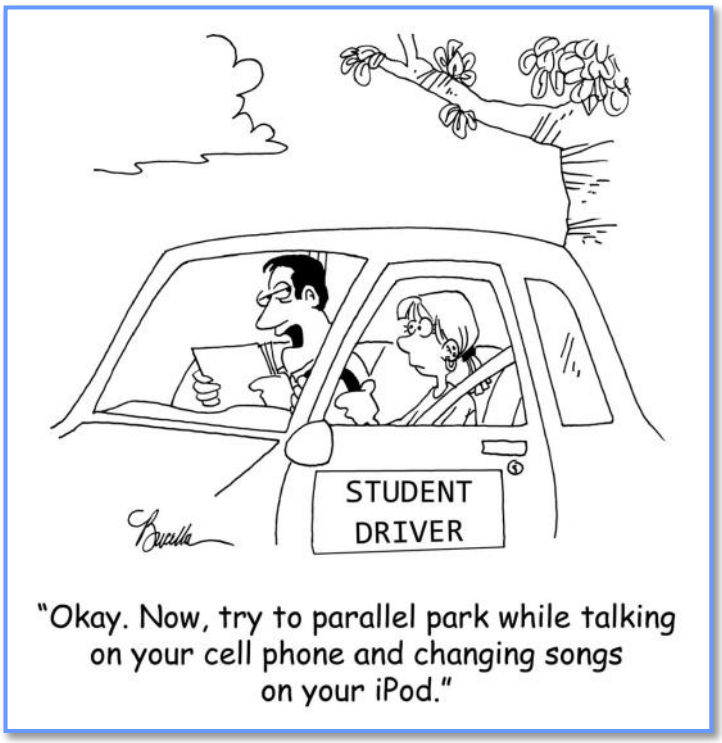
2. Choose cloud back-up options with threat-protection features. Many ransomware variants, Herath said, can infect any attached drives or network files that are accessible, including cloud-based. Not all cloud providers have the same features though. If you currently have data in a cloud, are looking for a new cloud provider or just aren't sure what's really included, inquire today. Ask questions about their security policy and their threat-protection features.

3. Consider the latest intrusion prevention products so you can be alerted of a breach and act quickly if one occurs. Ongoing 24/7/365 monitoring is a great way to stop an attack in it's tracks and ensure a swift recovery should the need arise. According to Herath, too often enterprises continue to follow the "patch once or twice a year" philosophy. This practice, he said, can leave them at enormous risk considering the lightning speed of ransomware's release.

Don't ignore the human element. Stay on top of current threats online and share your concerns with your staff. Everyone in your company is involved in keeping your company safe. There are a variety of next-generation products that are being developed to prevent recognizable malware, identify hidden malware activity, and destroy the intrusive files. However, none of these fancy tools can take the place of common sense.

Worried about network security? Stressed about back-ups? Unsure about your cloud solution? If this article sparked any concerns, give us a call today for a Network Security Audit. We will evaluate every nook and cranny of your technology and present you a full picture of your current setup. In addition, we will throw in our recommendations to secure your network.

Micro Enterprises LLC
877-540 -6789



"Okay. Now, try to parallel park while talking on your cell phone and changing songs on your iPod."

4 Dangerous Passwords

Even though remembering passwords is a pain, strong passwords can save you a bundle in damages. Make sure to stay away from these terrible passwords:

1. Password, no matter how you use it, is a bad idea. No using P@ssword or P@55w0rd! Just don't use it at all.
2. QWERTY passwords. Stay away from anything in a line with your fingers on a keyboard. These types of passwords are hacked very easily.
3. No birthdays or anniversaries. Anything in your social media is banned.
4. Your business name or information. Stay away from any common names for your business, your address, or phone number if you're putting a password on a company account. A good rule of thumb, anything on your website should be considered common knowledge.

Focus On Cyber Security

Did you know that roughly 58% of all cyber attack victims were small businesses (companies with less than 250 employees)?

It could happen to you. Change the mindset and culture in your company. Always assume you're at risk and a juicy target. Talk about active threats like the phishing scam on page 3 and keep everyone on the same page with proactive solutions.

Train your staff. Keep your employees informed with regular monthly discussions or trainings about how these risks can impact your business. Share stories about companies like yours that have struggled and encourage your staff to stay alert.

Find help. If you don't have a tech resource to monitor your systems, find one. There are a ton of outsourced IT providers here in our area. Have your network assessed, button up any loose ends, and create a plan for ongoing monitoring. Make sure everyone in your organization knows how to identify issues and who to call when there is a possible infection. Stop a cyber security threat in it's tracks with your best asset, your employees.

Celebrate...

(Continued from page 1)
over there in the corner? If you've been waiting to dispose of those old pieces of equipment, now's the time! Declutter your office and make room for your next new employee.

Hit the ground running. Clear a space for your newest addition. Make sure to order any new equipment you need too. A new computer for a fresh face or even a revamp of some of your old equipment can boost efficiency and ultimately help your company be more profitable.

Don't rely on luck! Be proactive about your company growth. Leprechauns won't help your company business grow even though a pot of gold would be nice. Business is about creating an environment for work to be completed efficiently and with good quality for your clients. Regardless of your industry, technology can help.

A little spring cleaning never hurts. Stop listening to your employees curse at the printer, scanner or even their computers and give us a call. We can evaluate your current setup and help you determine what steps will help you put a little pep in your step for spring time this year.

A Terrible Phishing Scam You Should Know About That's Impacting Business Just Like Yours

2019 has already become quite a year for Phishing scams. As many of you have seen, the newest ones are very deceiving; they seem to come from right inside your own company.

A new wave of invasions. Over the past few months we have seen thousands of e-mails come in from outside resources that are all dressed up to look just like your boss is e-mailing an urgent task. Many workers have been spoofed into purchasing items online like gift cards loosing a ton of company cash.

Who is getting hit? Well, we have see companies large and small. Everything from architecture firms, real estate companies, distribution organizations and even smaller service companies are receiving these socially engineered scams. No one is safe these days.

Typical scams we've seen. A few of the typical scams include requests from a member of management to purchase gift cards for a work related function or as a gift for a special occasion. Scammers will even be quick to reply if you e-mail back with questions, comments, and of course the gift card info. However, the gift cards are then stolen and used by the hackers for whatever they like.

What can you do to help protect your company? The messages really do look like they are coming from a coworker. Be aware and make an announcement in your office so everyone knows to just ask if anything looks off. Carefully assess any messages that include a request for multiple gift card purchases. Encourage your staff to call one another if there are any questions about purchases. A good phone conversation may save your company a boat load of money. In addition, some companies have started putting a warning on all e-mails that originate outside the company network. This helps people determine if the messages are legitimately from a coworker at a glance.

Interested in this new warning? Give us a call. We can take a look at your e-mail settings and work on getting your company notifications setup.

What Does A Port On A Firewall Actually Do?

Ever wondered why ports are so important if they are dangerous? The media has been flooded with stories about open ports causing back doors for hackers, so what do they actually do? What good are they if they can do so much harm?

What is a port? Well, here are the quick and dirty details about ports. You know, the Internet comes to your network over a big wire, right? So your network has to figure out the difference between videos, e-mails and other types of information. There are five major types information is sorted into and then pushed to your devices. The term "port" generally refers to a physical hole in your firewall or switch where something is plugged in like on the back of your firewall.

Then Internet gods created more... Sometimes the term "port" may be used in reference to an Internet Protocol or IP service. In this case, they can become dangerous. These non-physical ports are a logical construct of Internet stuff that allows data to flow in and out over an Internet connection. In order to address the data to the right location, the term "port" was used with a number designation to queue computers to recognize the Hyper-Text Transfer Protocol or HTTP.

Two things to remember, if we lost you here on the geek speak… 1. ports on your firewall should always be physically locked down so passer byers cannot plug in and hack your systems. Just like this physical threat, your virtual addresses or IP ports should be locked down so information cannot be passed through without your knowledge. If you are unsure if your IP ports are locked down, give us a call. We will look into it for you to ensure your company is secure.

"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...

How To Stay Sharp And Engaged At Work. Staying engaged with work has become a problem, according to staffing experts at Robert Half. Their Office Team survey showed that the typical employee feels disengaged or bored with their work for about 10.5 hours per week. In the winter months, 28% of workers feel disengaged.

It is possible to stay sharp and engaged in nearly any job, however, Lifehacker suggests a multifaceted approach to ensure you are ready for your work day and make work more challenging. Take a look at these steps to get yourself in gear:

1. Make sure to get enough sleep. The first steps happens before you even fire up your computer. Make time each evening to get a good nights rest. Most people need seven to nine hours of sleep each night, but many don't get that much which leaves them feeling sluggish through out the day.

2. Catch up while you commute. Look at your commute as an opportunity to jumpstart the day and center your thoughts. Mentally review your work for the day, noting the task that you will start first. Then, let go of work for a while and inject creativity with a podcast, audiobook or music.

3. Prepare your workspace for success. At the office, take a good look at your workspace and consider adding more ergonomic seating, better lighting, or even a plant to make your environment more comfortable. Sit-stand desks can be a great way to get the blood flowing throughout the day.

4. Challenge yourself. Not feeling challenged can also be a significant roadblock to staying engaged at work but there are many ways to increase responsibilities without adding extra stress. Perform a self-assessment. Identify your strengths and opportunities within the company, take steps to enhance your personal contributions, and share these efforts with a coworker or manager.

Ready for more? Focus during meetings, ask questions and take notes to stay engaged. Talk to your manager to see if there is room for an extra creative project or maybe time for skill enhancement. Use downtime to learn a new language or master an important computer application or even develop something new to streamline work for your company. No one likes to go to work each day and feel like a robot barely making it through their work. Be ready to take the initiative, bring yourself prepared for your day, create a work environment that encourages your personal success and challenge yourself to make your job even more engaging.

Secure Your Pot Of Gold

Worried about security? Concerned your backups are slipping through the cracks? Tired of struggling to ensure all the pieces of your network are getting the attention they really need? Our goal is to prevent computer problems before they escalate into unexpected downtime, data loss, and interruptions for your company.

Give us a call today for your *Network Security Audit* and learn how to button up your network. Ensure your pot of gold is monitored 24/7/365, back-ups are complete, and your data is recoverable when you need it most.

Micro Enterprises LLC 877-540 -6789

microenterprises

PO Box 503
Deepwater, NJ 08023
877-540-6789
www.microent.net