AlwaysOn IT

TECHNOLOGY TIMES

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

VoIP Services

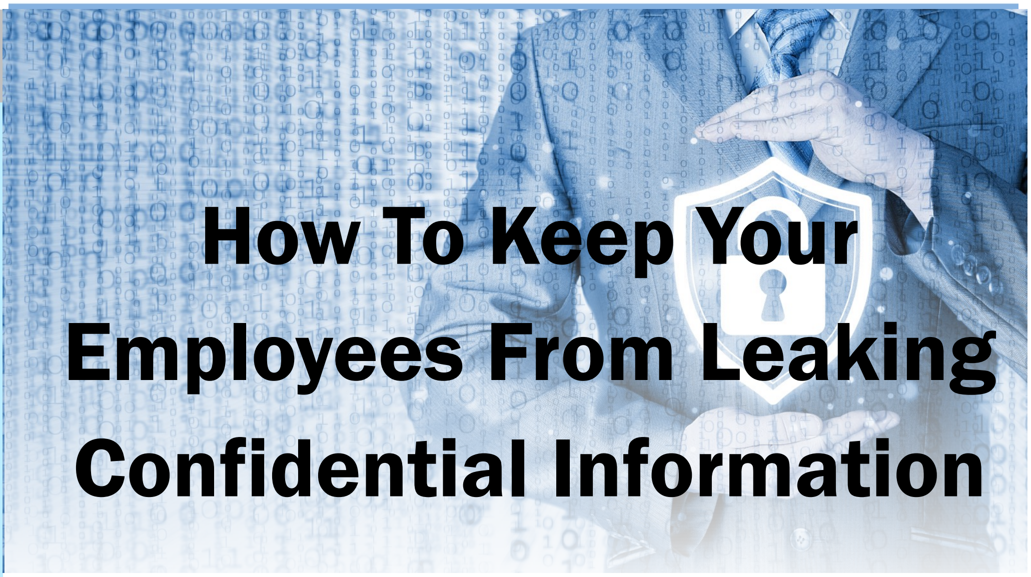
As we've met with our clients over the past few months, we've heard more and more concerns about costly phone bills. We've been testing a cutting-edge solution over the past several months and have found one that meets our extremely high standards. We are rolling this out to a few clients each month, and they have seen an average 40% cost savings on their monthly phone bill. If you want to be one of the first to experience this savings, call quality and ability to use cutting-edge features, just give us a call.

www.alwaysonit.com/voip-assessment/

June 2017

This monthly publication provided courtesy of Chris Benson, CEO of AlwaysOnIT.

Our Mission: To leave those we encounter better than we found them.
Our Vision: To become the company that others use and an example of world class service, community support, and giving.



How To Keep Your Employees From Leaking Confidential Information

Back in 2014, Code Spaces was murdered. The company offered tools for source code management, but they didn't have solid control over sensitive information — including their backups. One cyberattack later, and Code Spaces was out of business. Their killer had used some standard techniques, but the most effective was getting an unwitting Code Space employee to help — likely via a phishing attack.

When it comes to cybercrime that targets businesses, employees are the largest risks. Sure, your IT guys and gals are trained to recognize phishing attempts, funky websites, and other things that just don't seem right. But can you say the same thing about the people in reception, or the folks over in sales?

Sure, those employees might know that clicking on links or opening attachments in strange emails can cause issues. But things have become pretty sophisticated; cybercriminals can make it look like someone in your office is sending the email, even if the content looks funny. It only takes a click to compromise the system. It also only takes a click to Google a funny-looking link or ask IT about a weird download you don't recognize.

Just as you can't trust people to be email-savvy, you also can't trust them to come up with

>>

Continued pg.2

good passwords. It may sound so 2002, but plenty of people still use birthdays, pet names, or even “password” as their passcodes — or they meet the bare-minimum standards for required passcode complexity. Randomly generated passcodes are always better, and requiring multiple levels of authentication for secure data access is a must-do.

When it comes to cybercrime that targets businesses, employees are the largest risks.

Remember, that’s just for the office. Once employees start working outside of your network, even more issues crop up. It’s not always possible to keep them from working from home, or from a coffee shop on the road. But it is possible to invest in security tools, like email encryption, that keep data more secure if they have to work outside your network. And if people are working remotely, remind them that walking away from the computer is a no-no. Anybody could lean over and see what they’re working on, download malware or spyware, or even swipe the entire device and walk out — all of which are cybersecurity disasters.

Last but not least, you need to consider the possibility of a deliberate security compromise. Whether they’re setting themselves up for a future job or setting you up for a vengeful fall, this common occurrence is hard to prevent. It’s possible that Code Space’s demise was the result of malice, so let it be a warning to you as well! Whenever an employee leaves the company for any reason, remove their accounts and access to your data. And make it clear to employees that this behavior is considered stealing, or worse, and will be treated as such in criminal and civil court.

You really have your work cut out for you, huh? Fortunately, it’s still possible to run a secure-enough company in today’s world. Keep an eye on your data and on your employees. And foster an open communication that allows you to spot potential — or developing — compromises as soon as possible.

Free Report: What Every Small-Business Owner Must Know About Protecting and Preserving Their Company’s Critical Data and Computer Systems

PROTECT YOUR NETWORK

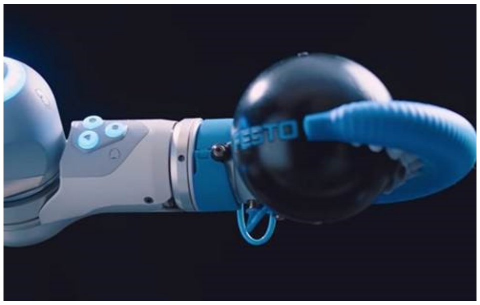
“What Every Business Owner Must Know About Protecting and Preserving Their Network”

Don’t Trust Your Company’s Critical Data And Operations To Just Anyone!

This report will outline in plain, nontechnical English common mistakes that many small-business owners make with their computer network that cost them thousands in lost sales, productivity and computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at www.AlwaysOnIT.com/protect or call our office at (503) 601-4335.

Shiny New Gadget Of The Month:



OctoGripper, the Octopus-Inspired Robotic Arm, Is Here

The animal kingdom is a reliable place to turn for mechanical inspiration. The German automation company Festo just made a robotic arm that takes its cue from an octopus. Meet the OctoGripper!

Festo figured it's hard to beat the octopus' flexibility. Built with a soft silicone structure that can be pneumatically controlled, the device bends inward to grip an item with two rows of suction cups. These create a vacuum, allowing the gripper to hold onto objects tightly while moving quickly Ñ a common challenge in robotics.

This isn't the only thing Festo is taking from nature. They want to see the OctoGripper incorporated into their BionicMotion Robot, which is inspired by an elephant's trunk. These could work side by side with humans, perhaps speeding up work.

Or they could pair up with Boston Dynamics and start the best robotic zoo this side of "Horizon: Zero Dawn."

5 Ways To Avoid Ransomware

With the WannaCry ransomware attack all over the news this week here are some quick tips on how to avoid ransomware in general. The best solution is layered protection that starts at the edge of your network and continues down to your users. Here are 5 quick tips on keeping your business network secure.

Firewalls: Who Is Knocking At Your Network's Door?

An intelligent security appliance (firewall) is a critical part of protecting your network. Not only will it prevent most malware from making it 'past the gates', it will give you details insight into what sorts of things are going on inside your business network. All clients protected by an AlwaysOnIT Sentry Perimeter Security Appliance have been protected from the WannaCry exploit since April 20th. Does your business have automatic, cloud-based proactive protection in place?

Backups: Who, What, When & Where?

A TESTED, MULTI-LAYERED backup solution is essential to your business – you should keep at least 3 copies of any data you don't want to lose. Are you prepared for when the inevitable happens? How much does it cost per hour If you cannot access key systems, service customers, or keep employees productive? You will sleep better at night knowing your backup is monitored and managed by professionals who can have your business up and running quickly. The proper solution can have your business back up and running in less than an hour.

Servers & Workstations: Keep Your Patching Up-To-Date

Microsoft patched this latest exploit back in March. That means all those affected by WannaCry were missing critical security updates that had been available for nearly 2 months. Knowing which patches to install and then making it a priority is time-consuming. A properly managed network automates this process and keeps systems protected without making you worry about it. ALL our managed clients were protected weeks ago – automatically without them having to even think about patching. How do you know if your systems are all updated and secure?

Email: Looking For Phishing Scams

Email remains the most common way ransomware attacks propagate. A "phishing scam" is an email that is usually disguised as a trustworthy source, designed to trick a user into clicking on or opening something they ordinarily wouldn't. Phishing emails may look like they come from a reputable business like UPS or Amazon, or could even appear to come from a co-worker. The best protection is to never click on links or attachments in emails unless you were expecting it. If you think you need to visit a link that appears in a questionable email, open your web browser and manually type in the address instead of clicking the link in the email. Office 365 is a great option to help filter out malicious emails – ask us if you are interested in learning more about migrating your email to Office 365.

User Education: The Biggest Business Threat

The BIGGEST threat to your business that technology cannot protect you from – THE USERS (and this includes you, Mr. CEO)! From clicking on phishing emails, to visiting inappropriate websites, downloading apps and programs from who-knows-where – your employees can be your biggest, and most expensive threat. One thing you can (and should) do is configure your firewall to document and monitor which web sites employees are visiting. Consider an Acceptable Use Policy (AUP) for your business, TRAIN employees on what is and isn't acceptable and then get them to sign the AUP. Ask us for a free AUP template!

Don't let your company become yet another statistic. Just one ransomware attack can result in a serious financial blow if you're not prepared. Visit www.AlwaysOnIT.com/DataTragedy TODAY or call 503-601-4335 by June 30th for a FREE Data Recovery Review ordinarily a $300 service.

Use This App To Pinpoint Dangerous Drivers. The open road is full of jerks and road rages, and a new app is taking them on. Nexar asks you to mount your phone to your dashboard, and it will monitor surrounding traffic. If someone starts driving dangerously, it will ask if you want to record what's going on with a 30-second video. The goal is to capture license plates of bad or hostile drivers. This is useful if you witness a crash or a criminal offense. According to trafficsafetystore.com, Nexar also uploads data to a central database. It will let you know if someone with a bad driving history enters the camera's field of vision, helping you spot potential bad drivers. In the future, Nexar plans to use GPS to identify dangerous cars to the side and behind them, too. *Safety Resource Center - December 1, 2016*

Where Have Tablet Sales Gone? Remember when they said tablets would outsell desktop and laptop computers? That now seems a tad optimistic. In March, Techcrunch.com reported that tablet sales are going down. But why? It turns out that folks treat tablets like computers Ñ meaning they don't upgrade them nearly as often as smartphones. "The iPad 2 is still in use today," IDC Senior Analyst Jitesh Ubrani tells TechCrunch. "The [original] iPad Minis and Air are all still in use today. They were being supported by Apple until very recently. People have been hanging onto these devices and they're finding that they work just as well as they did when they were released.". That's bad news for the tablet giants, who are still releasing new versions of tablets at least once a year. In the future, don't expect big releases or online unveilings for slates. *Techcrunch.com March 21, 2017*

Should You Have A Mobile App For Your Business? One of the great things about apps is that you don't need to be a big developer or company to build one. In fact, according to www.smallbusinesscomputing.com, 42 percent of small businesses in the United States have their own mobile app. By the end of the year, that figure is expected to hit 67 percent! Somewhat unsurprisingly, the most cited reason SMBs said they decided to build mobile apps is to increase sales (39 percent), followed by improving customers service (30 percent). Others turn to mobile apps as a competitive advantage in specific markets (22 percent) while for some organizations, their parent company suggested an app (10 percent). But with apps becoming more affordable than ever, there are lots of reasons to invest in your own app Ñ and lots of ways to recoup that investment. What would your ideal app do? *SmallBusinessComputing.com March 09, 2017*

Awesome tech you can't buy yet: Airport Jacket – Cargo jacket for Travel. If you always find yourself forking out for excess baggage every time you take a flight, then an Aussie-based startup has come up with an ingenious solution that'll have you confidently packing the kitchen sink for your next trip. The "Airport Jacket" is, for all intents and purposes, a wearable suitcase. With a whopping 14 pockets and two detachable pocket panels capable of taking up to 15 kgs. (about 33 lbs.) of stuff, your only concern will be ensuring your legs don't give way as you stagger toward the check-in desk. The jacket Ñ with all the stuff inside Ñ can be quickly transformed into a small bag so you only need to put it on when you arrive at the airport. Once you're through check-in and on the plane, you can fold it back up again before throwing it into one of the overhead bins. *Digital Trends – February 26, 2017*

Who Else Wants To Win Movie Tickets?

The winner of last month's drawing was Sue of Clackamas!
The correct answer was **B) $35 (https://en.wikipedia.org/wiki/Swoosh)**

Here's this month's trivia question. The winner will receive (2) tickets to Cinetopia.

What is Oregon's official state dance?

a) Waltz b) Jive c) Tango d) Square Dance

Email your answer to:
trivia@alwaysonit.com
Correct answers will be entered into our monthly drawing.
Drawing held on June 20th