ALL THINGS TECH

Brought to you by SYSCON

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

What's New

The two 'hot' topics this month are Super bowl LIII (53) and Valentine's day. Every store has themed munchies for the game, and boxes of chocolates with red roses, and Valentine cards.

Last month, we added computer resources to our hosted environment for speed and stability. We've been planning this for a while, so it's great to see it finally in place; great teamwork!

We also added some staff to our Network group, including Kevon Ward, our IT Director; Welcome!

- Catherine Wendt

February 2019

This monthly publication provided courtesy of Catherine Wendt, President of Syscon Inc.

We love this stuff! We are committed to helping businesses use technology to run their organization successfully and profitably.

Sneaky Ways Cybercriminals Access Your Network

And What You Can Do To Prevent It TODAY

Hackers prefer the little guy. The high-profile data breaches you read about in the news — your Facebooks and Equifaxes and T-Mobiles — are only the tip of the iceberg when it comes to the digital crimes being perpetrated day after day, especially against small businesses. Today, according to a report by the National Cyber Security Alliance, 70 percent of hackers specifically target small businesses. Attracted by the prospect of easy money, they search for those organizations who underspend on protection, who have employees untrained to spot security risks, and who subscribe to woefully out-of-date practices to protect their data. As a result, more than 50 percent of small businesses have been hacked, while 60 percent of companies breached are forced to close their doors within six months.

Most business owners have no idea the danger they're putting their livelihood in by leaving cyber security up to chance. According to a survey conducted by Paychex, 68 percent of small-business owners aren't concerned about their current cyber security standards, despite the fact that around 70 percent of them aren't adequately protected. In the face of an imminent, global threat to the very existence of small businesses everywhere, most CEOs offer up a collective shrug.

The tactics and software available to hackers become more sophisticated by the day, but with so many unwitting victims, most criminals don't even need to work that hard to net a six-figure income. By sticking to two tried-and-tested tools of the trade — phishing, ransomware ,and the subtle art of guessing users' passwords — they leech comfortably off the earnest efforts of small businesses all over the world.

So, what's to be done? Well, first things first: You need to educate yourself and your team. Protect your organization against phishing by fostering a healthy skepticism of any email that enters your inbox. Make it a habit of hovering over

Continued pg.2

(continued from page 1)
hyperlinks to check their actual destination before you click. If an email is coming from someone you know, but the email address is different, verify it with the other party. And never, ever send passwords or personal details to anyone over the internet if you can avoid it.

Speaking of passwords, you probably need to upgrade yours. The majority of folks use the same password for everything from their Facebook account to their business email. The fact that this includes your employees should make you shudder. It may not seem like a big deal — who's going to take the time to guess SoCcErMoM666? — but aside from the fact that simple software enables hackers to guess even complicated passwords in minutes, that's not even usually necessary. Instead, they can just look at the data dumps from a recent more high-profile breach — think the Equifax fiasco — pull your old website from there and type it into whatever profile they want to access. If you keep all your passwords the same across sites, it won't take them long to dig into your most precious assets. To avoid this, implement a strict set of password regulations for your business, preferably incorporating two-factor authentication, and mandatory password changes every few weeks.

"...implement a strict set of password regulations for your business..."

Of course, you can read up on hacking techniques and teach them to your team until you're blue in the face, and a data breach can still occur. Cybercrime is constantly evolving, and staying abreast of its breakneck pace takes a dedicated awareness of the latest protective tools and measures. That's why your single best weapon to defend you against the hackers at your door is to find a managed service provider (MSP) to partner with your organization, like us! These companies not only regularly monitor your network, they also keep it updated with the latest patches and measures to prevent the worst. And if crisis somehow still strikes, they'll be able to get your network back up in minutes rather than days, equipped with an expert knowledge of your systems and years of experience in the field.

In today's digital world, leaving your cyber security up to a subpar antivirus and some wishful thinking is irresponsible and a threat to your company. But with a little savvy, a bit of investment and a second opinion on the circumstances of your company's security, you can rest easy knowing that no matter what comes, you're protected.

Cathy and Larry Sightings

Catherine and Larry took a couple of trips together to Kansas for a new client, getting them 'live' on Sage 100 Contractor; lots of teamwork!

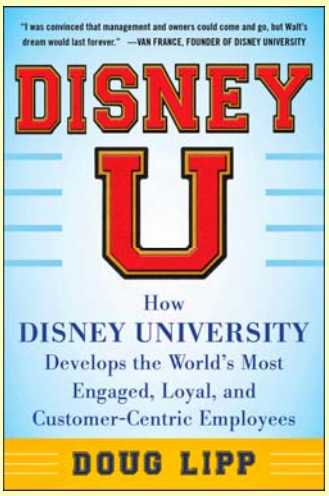
'Dance like no one is watching. Sing like no one is listening. Love like you've never been hurt, and live like it's Heaven on Earth.'
- Mark Twain

Disney U by Doug Lipp

I had an opportunity to hear Doug Lipp speak at an industry event. He has passion for his topic, and was ready to give us some specific take-aways to bring back to our businesses. What I remember the best is his statement, 'Snow White Never Has a Bad Day.' How do you pull that off?

The book is a nice combination of the history of the Disney dream and philosophies, along with the struggles they had over the years, primarily focused on personnel. There are quite a few reasons to have continuing education, such as success, growth pains, and outside circumstances. It starts with the initial orientation, but there's a lot more. The idea of 'walking the park,' seeing how your customers interact with your staff, with each other, and really spending a day side-by-side with your front line workers to see what they face, all great reminders!

Lots of practical take-aways, and a good read. Strongly recommended! - *CMW*



Shiny New Gadget Of The Month:

This Smartphone Is Also A Projector:

Sure, your big honking iPhone or massive Android is impressive, but does it have a screen the size of an entire wall?

The Movi is the first smartphone to integrate a built-in pico projector into its design, allowing users to project 720p images up to 200 inches in size wherever they are. At only $599, it's a bargain when compared to other comparable projectors.

However, there are caveats: the Movi's FHD phone screen can't compare to its higher-end OLED competitors, and its camera leaves something to be desired. But if you're an avid video buff with a mind for convenience, the Movi may be just what you're looking for.

From the Techs

Sick of the Robo calls? Here's an option...

We've been receiving dozens of calls to our cell phones, from lots of different phone numbers, telling us that the health care deadline has been extended and...; then we hang up, annoyed. Our Aunt in California is receiving a relentless amount of calls saying her Social Security number has been compromised and she needs to act. How do you stop these interruptions and the bullying? Is it just us?

According to NBC news, Americans received 30 billion (with a 'B') robo calls in 2017, up 19% from 2016, to both land lines and cell phones. Wow!

Turns out there are several services out there that are ready to address this very issue. For the cell phones, there are apps you can download; some have a fee, others have advertising. For the land lines, the phone has to have simultaneous ringing technology to use the services, something you can check into.

The services have a database of phone numbers they've collected. When their customers receive a robo call, the user flags it as a robo call and the service adds it to the database for everyone's benefit.

When a known robo phone number calls you, the phone rings once then the call is rejected. You get a message in your call log showing that the call came in, it was blocked, and the service may even show you the transcribed text from the call that was blocked.

When you have a whole community that's fed up with these interruptions, it can become a powerful database of info that can be shared for everyone's benefit; check it out!

Caribou Coffee Breach

In December, Caribou coffee announced that 239 of its 603 locations, 40% of its stores, had experienced a security breach. There was unauthorized access at its Point of Sale (POS) devices.

All customers who used a credit or debit card at one of the affected stores between August 28th and December 3rd, 2018, are at risk. Online purchases were not affected (the silver lining).

ID Agent, the company we use for Dark Web monitoring, included this event in its weekly Breach Updates, ranking this incident as 1.777 on its scale, a Severe threat to Small Businesses. For individual risk, it received a 2.428 ranking, also Severe.

Caribou Coffee has posted a list of the stores; might be worth checking - *CMW*

Do you get our weekly email blasts?

These are short, **2-minute video updates** on tech-related topics. There's often a **short blog** if you want to read more on the topic. If you don't get these, **please call Jonathan** at our office and we'll make sure you're on the list. You might have to 'white list' us, and we can tell you how to do that, too!

Construction Corner

Some Common Problems That Lit Up Our Phones Last Month

You should be on version 21.3 now. If you haven't already upgraded, it's time. Version 21.3 has the latest tax table updates and several feature enhancements (see previous newsletters for more details on these). When you install this update, be sure to have your Sage Customer ID number and the EXACT spelling of your Sage Client Name, since these will need to be re-entered at the end of the upgrade process.

Run the Payroll Audit, 5-3-7, every time you run a payroll. Then resolve all audit errors right away, before you go on to the next payroll cycle. AND, run it again before you create any quarterly or yearend reports. Be sure all audit errors are resolved BEFORE you create the quarterly reports.

Each Employee can only have <u>one</u> employee record in 5-2-1. This is the first year that I've had so many calls about this one. It seems many of our clients are crossing state lines and hiring old employees back, so they're creating a second employee record for the same person—do NOT do this. At the end of the year, each employee can only have one W-2 form. This also creates an over-accrual and over-stated expense for State and Federal unemployment, both of which have maximum base wage limits; this also makes lots of extra weekly steps to make split child support between the two checks, health premiums, and similar. Don't ignore the Sage warnings when you're doing something new in the system. If you have issues with State wages, State withholding, special fees for work in a specific district, give us a call and we'll work it through with you. Do NOT create a second employee number for the same employee.

When you use Paygroups (prevailing wage or union), there are rules about what rates will 'win.' If the paygroup has one rate, and the pay calc has another, the Paygroup rates win every time. Update the pay calcs so your reports print correctly, but know that whatever rate is in the Benefits tab of the paygroup, is the rate that will be used to calculate the benefits/ deductions for any employee in that paygroup.

Final Word— Sage 100 Contractor is an excellent program. If you're not getting the result you want, you may not be using the 'tool' correctly. Even if you give me the best trowel money can buy, my wall is NOT going to look very good because I don't know how to use a trowel! Get trained, ask questions, and go beyond the Sage 'Help' files since they're not always the best place to get the right answers. —*CMW*

Who Wants To Win a $25 Amazon Gift Card?

This month's trivia question:
At which university was the first computer mouse developed?

a) Stanford b) DeVry Tech c) MIT d) University of Phoenix

To enter: Go to www.Syscon-inc.com/Trivia and type in your answer. All correct answers will be put into a fishbowl and we'll randomly draw the winner. The Winner will be contacted shortly after the deadline and will be announced in next month's newsletter.
Deadline: February 20, 2019

Congratulations to last month's Trivia Contest winner, Sharon Brown with **Temp-Con**, KS! Sharon's name was drawn from the fishbowl for last month's correctly answered Question:

In 1998, software engineer Steve Gibson discovered a cookie in some e-commerce websites that tracked user browsing habits and sent them back to a server. What is the generic name for this wicked practice (not restricted to cookies)?

c) Spyware

FIELD INTEGRATED TIME SYSTEM

Collecting Time From the Field Just Got Exciting!

We collect time, cost code information, work order numbers, phases, client signatures, and a whole lot more. Your field can use iPhones, Androids, or Tablets. All the info is sent straight to Sage 100 Contractor, no copy-paste! Interested? Join us on Thursday, **February 21st at 11:30am Central Time**.