ALL THINGS TECH

Brought to you by SYSCON

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

What's New

March is supposed to 'Come in like a lion, go out like a lamb'; well, I hope so! As March rolls in we're looking forward to longer days of sunshine. We also 'Spring ahead' on Sunday March 12 for Daylight Savings Time.

Back at the office, we're replacing our Firewall and adding redundancy to our infrastructure. We're very excited about this next step!

Our offer to scan your domain name for compromised user names and passwords has caused a few people's hearts to skip a beat when we showed them their password out there for sale. Haven't checked it out yet? Just give us a call!

- Catherine Wendt

March 2018

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.

5 Ways Your Employees Will Invite Hackers Into Your Network

Whether they're criminals or heroes, hackers in the movies are always portrayed as a glamorous group. When it comes down to the wire, these are the individuals who crack into the ominous megacorporation or hostile foreign government database, hitting the right key just in the nick of time. They either save the day or bring down regimes, empty the digital vault of the Federal Reserve, or disable all the power plants in the country. It's always a genius up against an impenetrable fortress of digital security, but no matter what, they always come out on top.

In real life, it's rarely that difficult. Sure, if you look at the news, you might believe hackers are close to their Hollywood counterparts, stealing data from the NSA and nabbing millions of customer records from Equifax. But the majority of hacks aren't against the big dogs; they're against small to mid-sized businesses. And usually, this doesn't involve actually hacking into anything. A lot of the time – approximately 60% according to the *Harvard Business Review* – an unwitting employee accidentally leaves the digital front door open.

The biggest threats to your company aren't teams of roaming hackers; they're your employees. Here's why.

1 They'll slip up because they don't know any better.

With the proliferation of technology has come an exponential rise in digital threats of such variety and complexity that it'd be impossible for the average person to keep track of it all. Each of your employees' lives are a labyrinth of passwords, interconnected online accounts, and precious data. If their vigilance slacks at any point, it not only leaves them vulnerable, but it leaves your company vulnerable as well. For

Continued pg.2

(continued from page 1)
this reason, most cyber-attacks come down to a lack of cyber security education.

2 They'll let you get hacked on purpose.

It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data to malicious groups. Whether it's info vital for your competitive advantage, passwords they can sell to hacker networks to make a quick buck, or sensitive data they can make public simply to spite your organization, it's difficult to protect against a double agent.

3 They'll trust the wrong person.

For many hacks, little code is needed whatsoever. Instead, hackers are notorious for posing as a trusted member of your own team. And if you believe that you'd be able to spot an impostor from a mile away, you may want to think again. Not only is it easier than ever to crack individual users' e-mail passwords and login credentials, personal info is now littered throughout social media. A simple visit to Facebook can give a hacker all they need to know to "social hack" their way into the heart of your business.

4 They'll miss red flags while surfing the web.

Clickbait is more than a nuisance plaguing your social media feeds. It can be a powerful tool for hackers trolling for easy prey. If an employee doesn't understand what exactly makes a site or link look dubious, they may open themselves – and your company – to browser exploits or other types of attacks.

5 They're terrible at passwords.

According to Entreprenuer.com, "3 out of 4 consumers use duplicate passwords, many of which have not been changed in five years or more." Even more, those passwords are simply weak, inviting easy access for unsavory elements. Many people brush off the importance of strong passwords, but the risks posed by the password "123456" or "password" cannot be overstated.

When it comes to defending your precious assets against digital threats, it can seem impossible to protect yourself at every turn. But there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people. Through a comprehensive security training program, including specific examples of methods hackers use – particularly phishing – you can drastically minimize the risk of an employee accidentally opening up a malicious e-mail or posting sensitive info. When you make a concerted effort to make the entire organization vigilant against cyber-attacks, you're much less likely to be targeted.

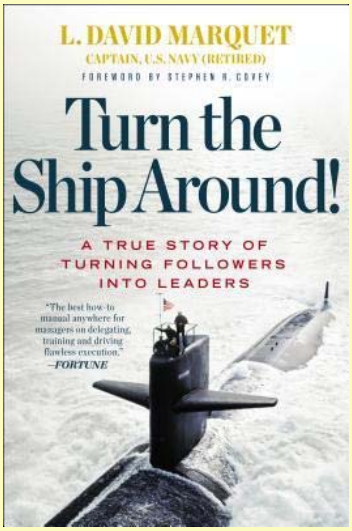
Cathy and Larry Sightings

Catherine had two flights cancelled due to Chicago weather! Larry is wrapping up version 20 programs.

'When you talk, you are only repeating what you already know. But if you listen, you may learn something new.'

- Dalai Lama

Turn the Ship Around! by L. David Marquet



At an industry event in Phoenix, AZ, Mr. Marquet was a featured speaker, sharing his first-hand experience on the USS *Santa Fe*, a nuclear submarine. He finds himself taking over a crew that had trouble getting underway on time and the worst retention record in the submarine force. The challenge was to use the same people and support team while changing the way they interacted and behaved, all with the goal of increasing the combat effectiveness.

During this assignment, David observed the men, asked questions, listened, and put together steps toward rebuilding the team, ultimately earning glowing accolades in the Navy, and a visit by Stephen Covey! Really enjoyed the story and the insights; Recommended! —*CMW*

Shiny New Gadget Of The Month:

FIXD

When was the last time you turned on your car, pulled out of the driveway and suddenly noticed the engine light pop up on your dashboard? You probably just ignored it and drove to your destination. Maybe the next day you spent some time trying to get to the bottom of the issue, only to come up short. Everything seems fine, so what's going on?

A new device called FIXD aims to figure that out. After plugging in the $59, palm-sized widget into your car's onboard diagnostics port – the same one mechanics use to find potential issues – it can communicate with a free app to tell you precisely what's wrong with your vehicle. You can determine why your engine light is on, how serious the problem is, and whether it requires emergency repairs, all without risking being ripped off by shady mechanics. If necessary, the device can actually turn off your engine light right from the app, making it a nuisance of the past.

The "Not Me!" Problem... And Why This Is Almost Guaranteed To Happen To You

Security this, password that—now they want a password with 14 characters with two symbols? And I have to change it every three months?

As difficult as it is to remember 24 different passwords, four PIN numbers and a slew of new cyber security processes, we still manage to instantly recall most of the tangible things in our lives. The code for the company door and alarm system, the passcode to our phones, the garage code, the other garage code—you get the idea.

But these numbers are based upon a time when the most "real" threat seemed to be someone busting in our door and threatening our families in the middle of the night. In 2018, those kinds of physical threats are far less statistically prevalent than cybercrime. In fact, data breaches and identity theft are occurring at three times the rate that home burglaries occur in the U.S. according to a 2016 study by the University of Kentucky.

Don't succumb to the "Not me!" approach to the shift in crime. Understand that it can happen to you, and approach all aspects of physical and electronic security with the attention they deserve.

Google Is Making Some Changes...

Beginning in July this year, Google Chrome will flag all HTTP websites as "not secure," according to a blog post published by Chrome security product manager Emily Schechter. This change will be timed with the release of their Chrome 68 version.

When you visit a website that displays as HTTPS, it has additional security. HTTPS encryption provides protection between your browser and the website you're visiting. This protection ensures that no one can modify the traffic or spy on the session. Without this level of encryption, someone with access to the router could intercept the information sent to the website or even put malware in place.

So, it's time to purchase an SSL Certificate for your website (check out our Trivia question on page 4). This will allow Chrome to flag your site as secure to those who visit. Give us a call and we'll be happy to give you more details about this change and discuss the steps you need to take. - *CMW*

Did you know we have a **You Tube Channel**? It's full of short videos about IT-specific topics for your business. Why not subscribe so you can see the latest update?

We have a **Syscon Linked In** page. If you're on Linked In, let's get connected!

We have a Twitter feed, too. It's **Syscon_Inc**— check it out!

Construction Corner

What's New in Sage 100 Contractor

Get ready for version 21—in a recent Sage webinar, Sage shared three (3) new features for version 21 which is targeted for release in early March. There will be enhancements to the 9-5 screen; you'll be able to enter by employee in the 5-5-1 Daily Payroll screen; they will have a 'Bank Feed' connected with the Bank Reconciliation screen.

They only had a mock up of the new Bank Feed, but basically you can select your bank and pull up the bank activity on your account and compare it to the entries in the software. The mock up showed a split-screen with the bank details on the left and the S100C entries on the right. It will be interesting to see how this plays out.

ASA Chicago Expo, March 6th

If you're in the Chicago area, come join us at this year's ASA Chicago Expo at the Drury Lane Theater in Oak Brook. It will be held Tuesday March 6th from 9:00am to 4:00pm.

We'll be at booth #907. Come by to say 'hi,' play the game, earn a prize, and see some of our IT services, along with our construction-specific services. Hope to see you there!

The User Group—TUG

We'll be at the TUG Expo in Orlando, Florida this May. This user-specific show is always well-attended, focusing on specific Sage software and add-ons for the Construction industry.

The event is May 15-17 in Orlando. We'll feature our Field Integrated Time (F.I.T.) System, and some of our Sage 100 Contractor-specific analytical tools such as Over/Under Billing, Indirect Cost Allocation (ICAP), and a few others. Look forward to seeing you in sunny Orlando!

An Odd Thing in S100C v20 that we've come across...

When you're in a screen with information displayed in the various fields, and you hit F7 to make a security or format change to the field, the fields in the F7 menu are grayed-out! Don't worry, just clear the record being displayed (blank screen), then go back to the field, hit F7, and the options will all be there.

Collecting Time From the Field Just Got Exciting!

We're helping our clients collect field time from mobile devices, and we're fully integrated (really!) with Sage 100 Contractor version 20.

We can collect cost code information, work order numbers, phases, client signatures, and a whole lot more. Interested?

Your field can use iPhones, Androids, or Tablets. Join us for a demo on **March 15th**!

Who Wants To Win a $25 Amazon Gift Card?

This month's trivia question: **What does SSL stand for?**

a) Superuser System Login b) Secure Socket Layer
c) System Socket Layer d) Secure System Login

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: March 20, 2018

Congratulations to last month's Trivia Contest winner, **Beth McCormick**, with **Polhemus Savery DaSilva**, MA! Beth's name was drawn from the fishbowl for last month's correctly answered Question:

In what year did the Wright Brothers successfully design and fly a motorized aircraft?

d) 1903