ALL THINGS TECH

Brought to you by SYSCON

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

What's New

The Fourth of July—a great day for celebration, fireworks, grilling with friends and family. This is also a great time to reflect on the courage of those men who wrote and signed the Declaration of Independence.

"We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness."

These well-educated, passionate men took action, together. Where could you make an impact for your family or community?

- Catherine Wendt

July 2018

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

We love this stuff! Our passion is helping businesses use technology to run their organization successfully and profitably.

Top 4 Ways Hackers Will Attack Your Network

And They Are Targeting You RIGHT NOW

Most small and midsize business (SMB) owners exist in a bubble of blissful ignorance. They focus on the day-to-day operations of their organization, driving growth, facilitating hiring, and guiding marketing, without a single thought given to the security of the computer networks these processes depend on. After all, they're just the little guy – why would hackers go to the trouble of penetrating their systems for the minuscule amount of data they store?

And eventually, often after years of smooth sailing through calm seas, they get hacked, fork out thousands of dollars to malicious hackers, and collapse beneath the weight of their own shortsightedness.

The facts don't lie. According to Verizon's annual Data Breach Investigations Report, a full 71% of cyber-attacks are aimed squarely at SMBs. And while it's unclear exactly how many of these attacks are actually successful, with the sad state of most small businesses' security protocols, it's a safe bet that a good chunk of the attacks make it through.

But why? As Tina Manzer writes for Educational Dealer, "Size becomes less of an issue than the security network … While larger enterprises typically have more data to steal, small businesses have less secure networks." As a result, hackers can hook up automated strikes to lift data from thousands of small businesses at a time – the hit rate is that high.

Today, trusting the security of your company to your son-in-law, who assures you he "knows about computers," isn't enough. It takes constant vigilance, professional attention and, most of all, knowledge. Start here with the four most common ways hackers infiltrate hapless small businesses.

Continued pg.2

(continued from page 1)

1. PHISHING E-MAILS

An employee receives an e-mail directly from your company's billing company, urging them to fill out some "required" information before their paycheck can be finalized. Included in the very professional-looking e-mail is a link your employee needs to click to complete the process. But when they click the link, they aren't redirected anywhere. Instead, a host of vicious malware floods their system, spreading to the entirety of your business network within seconds, and locks everyone out of their most precious data. In return, the hackers want thousands of dollars or they'll delete everything.

It's one of the oldest tricks in the hacker toolbox, but today it's easier than ever for an attacker to gather key information and make a phishing e-mail look exactly like every other e-mail you receive each day. Train your employees to recognize these sneaky tactics, and put in safeguards in case someone messes up and clicks the malicious link.

2. BAD PASSWORDS

According to Inc.com contributing editor John Brandon, "With a $300 graphics card, a hacker can run 420 billion simple, lowercase, eight-character password combinations a minute." What's more, he says, "80% of cyber-attacks involve weak passwords," yet despite this fact, "55% of people use one password for all logins."

As a manager, you should be bothered by these statistics. There's simply no excuse for using an easy-to-crack password, for you or your team. To check the strength of your password, type it into HowSecureIsMyPassword.net before you make it official.

3. MALWARE

As described above, malware is often delivered through a shady phishing e-mail, but it's not the only way it can wreak havoc on your system. An infected website (such as those you visit when you misspell sites like Facebook.com, a technique called "typosquatting"), a USB drive loaded with viruses, or even an application can bring vicious software into your world without you even realizing it. In the past, an antivirus software was all that you needed. These days, it's likely that you need a combination of software systems to combat these threats.

4. SOCIAL ENGINEERING

As fallible as computers may be, they've got nothing on people. Sometimes hackers don't need to touch a keyboard at all to break through your defenses: they can simply masquerade as you to a support team in order to get the team to activate a password reset. It's easier than you think, and requires carefully watching what information you put on the Internet – don't put the answers to your security questions out there for all to see.

We've outlined some of the simplest ways to defend yourself against these shady techniques, but the best way is to bring on a company that constantly keeps your system updated with the most cutting-edge security and is ready at a moment's notice to protect you in a crisis. Hackers are going to come for you, so do everything you can to prepare!

Cathy and Larry Sightings

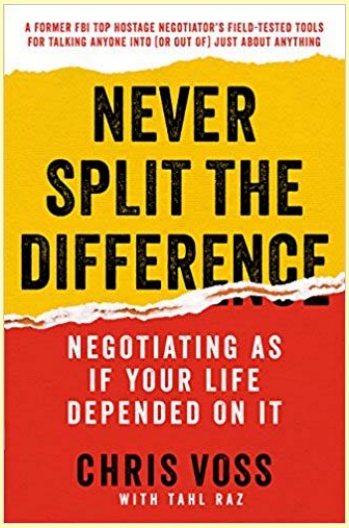
Syscon took the whole staff to Top Golf for an evening of good food and fun!

Larry is recovering from foot surgery. Turns out ankles aren't supposed to move like that after all!

'Your future is created by what you do today… not tomorrow'

- Anon

Never Split the Difference by Chris Voss



Earlier this year, I had the chance to hear Chris Voss speak at an industry event. He shared some FBI American hostage stories and his negotiation efforts; really eye-opening. He then went on to talk about the science of negotiating and how it has transformed in recent decades.

For Chris Voss and the families in distress, the stakes were very high—4 hostages, so just split the difference? Not acceptable in life and death situations. In the book, there are some great stories. There's also a wealth of specific, actionable information we can use in our businesses, our relationships, and our families. This is not a book about manipulation. This is an excellent book about communication, human nature, and how to negotiate. Highly Recommended!

Shiny New Gadget Of The Month:

Introducing The Snap SmartCam

Today, the security of your home is more important than ever before. Lawbreakers are constantly getting bolder, and as our technology advances, they switch up their tactics. With that in mind, all of us should be on the lookout for a security camera that's difficult to spot, is intelligent about the footage it collects, and grabs high-quality footage to identify burglars.

Enter the Snap SmartCam, a tiny little camera that looks — and operates — just like a phone charger. The innocuous-looking device uses motion-detecting technology to pick up when shady activity is going on in your house, and takes high-quality footage to catch a person in the act. If you're interested, the camera will cost you $57.00 at the time of writing, a great deal for a security camera of any type, much less one that seems so useful.

News From Our Techs

Tales from a Hacker turned White Night

At a recent industry event, we heard and watched Kevin Mitnick, reformed hacker who was wanted by the FBI. He got caught, went to jail, served his time, and now he does security penetration testing. He did a demo for us using 'simple' tools that hackers have available to them. We were amazed at what he shared, truly stunned by what we were seeing. There were quite a few takeaways; this month we'll share two of them.

When you're at the airport or the local coffee shop, you can usually see a list of available wireless options. There's often a free one for guests. Turns out, hackers know how to create a Wi-Fi option that looks just like the airline or the coffee shop you're visiting, but it isn't!

You log on to their bogus Wi-Fi and now they can see your computer, your camera, the keystrokes, the sites you visit, everything you're doing. They can even install software or spyware on your computer! In a matter of minutes, Mr. Mitnick had setup the fake Wi-Fi, logged into it, then hacked into his own computer; how unnerving!

Mr. Mitnick is very sure that the next big wave of ransomware attacks is going to hit Office 365. He brought up his own Office 365 email account on one screen, and the hacking software on the other. We could see the email messages and subject lines in his account. On the hacking software screen, he hacked into the email account, encrypted the email, and sent the message demanding the ransom payment. You could see all the email become encrypted—except the subject lines, so you can see what you're missing. He then 'paid' the ransom and released the encryption so the email was back to normal. This took less than 5 minutes!

What can you do? First, use your own Mobile Hot spot on your cell phone for a wireless connection, rather than public hot spots. You can also setup VPN tunnels between your computer and the server at your office. Use strong passwords (NOT password, or 12345, or your pet's name!), and change them every 90 days; NEVER share your password with others. If you really need to get on public wireless, limit what sites you visit and avoid any that might post a security risk to you. Be Cautious, Be Careful!

Will Google Flag Your Website as 'Not-Secure'?

In an official announcement on February 8th of this year, Google posted the following comment: 'Beginning in July 2018 with the release of Chrome 68, Chrome will mark all HTTP sites as "not secure." When they get to your website, it will say 'Not Secure' and they might leave.

You've probably heard about HTTP versus HTTPS and seen it in your Internet Browser. Bank sites are usually HTTPS, meaning they have a Security certificate in place. The additional encryption provided with an SSL Certificate protects you and the website you're visiting. With an SSL Cert in place, no one can modify the traffic or spy on the session. Without it, someone with access to the router could intercept the info or even put malware in place.

If you don't have an SSL Cert for your website, now's the time to buy it and get it applied. Give us a call and we'll help you get it done! - *CMW*

Construction Corner

S100C Version 21 To Upgrade or Not to Upgrade

Last month we shared some of the new features available with version 21! These include the ability to create recurring salaried payroll records; sending Direct Deposit vouchers at a later date (kind of); tracking employee raises; removing the 'Protected Sheet' flag when you print to Excel; a new Bank Feed for reconciliations; and more.

So, should you upgrade from 20.x to 21? If there's a feature on this list that you just have to have, go ahead. For the rest of you, no rush. We recommend waiting until they work out a few bugs (and there are always a few), then upgrade later this year.—*CMW*

Print Spooler Errors There are known issues with the print spooler. Sage acknowledges that sometimes the printer will 'hang.' For those of you in our hosted environment, we've created a script that runs each night that clears the print queue. Be sure you Log Off each night (not the X, but log out of the software, *and* Log Off of the server). Our script runs before you arrive in the morning, so you'll be all set! - *CMW*

Need Another License?

We have a GREAT problem! All of you are very busy this year, lots of projects, and adding staff. However, you are now battling over available S100C licenses, and some of you are hogging!

You may not want another out-of-pocket expense, but it's probably time to buy a license; not having it is costing you more than you think; lost productivity while people check around to see who can release a license so they can log on; delays in reports, data entry, review of paperwork by PM's because they can't log on until later or tomorrow; the nightly Tune Up isn't running, so your user experience will get slower; and I bet you can think of a few others.

It's about $2K to add licenses. We'd be happy to get you a quote and get the ball rolling.—CMW

Windows 7—Support Ending January 2020

Seem far away? 18 months, that's it. You might have to replace hardware. If your laptop/ workstation is 4 years old (or more), you may need to replace it. If it's more recent, let's talk about whether you should upgrade and when. Not all Windows 10 upgrades have gone well; FYI

Collecting Time From the Field Just Got Exciting!

We're helping our clients collect field time from mobile devices with Sage 100 Contractor v20.

We can collect cost code information, work order numbers, phases, client signatures, and a whole lot more. Your field can use iPhones, Androids, or Tablets.

Interested? Join us for a demo on **July 12th at 11:30am CT!**

Who Else Wants To Win a $25 Amazon Gift Card?

This month's trivia question:

Dec 3, 1967, Dr. Christiaan Barnard performs the first ever of which type of surgery that now saves thousands of people every year?

a) Lung Transplant b) Hip Replacement c) Angioplasty d) Heart Transplant

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: July 20, 2018

There were no entries for last month's Trivia Contest, so we are sending the $25 to the Phoenix Rescue Mission!

Which of the following search engines came first?:

d) WebCrawler