ALL THINGS TECH

Brought to you by SYSCON

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

What's New

Early this month we will 'Spring Ahead.' Although we'll have a little extra sunshine at the end of the day, we'll lose an hour in the morning. At least the days are getting longer.

You've probably heard us talk about, or have received the Phoenix Rescue Mission Possible Cookies. This month, they have their annual Arise! Community Breakfast event, updating the business community on the many successes of their outreach to the homeless who struggle with addiction, and the special needs of women with children in this situation.

Count your blessings (it's not the luck of the Irish); hug your family members; give your time and talents! - *Catherine Wendt*

March 2020

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 Signs You're About To Get Hacked — And What You Can Do To Prevent It

Hackers love to go after small businesses. There are many businesses to choose from, and many don't invest in good IT security. Plus, many business owners and their employees have bad cyber security habits. They do things that increase their risk of a malware or a cyber-attack. Here are five bad habits that can lead to a hack and what you can do to reduce your risk.

1. Giving out your e-mail Just about every website wants your e-mail address. If you share it, it's usually not a big deal (though it varies by site – some are more than happy to sell your e-mail to advertisers). The point is that when you share your e-mail, you have no idea where it will end up – including in the hands of hackers. The more often you share your e-mail, the more you're at risk and liable to start getting suspicious e-mails in your inbox. Not convinced? I'll bet you don't give your cell phone out very often; same thing.

If you don't recognize the sender, then don't click it. Even if you recognize the sender but aren't expecting anything from them and do click it, then DO NOT click links or attachments. There's always a chance it's malware. If you still aren't sure, pick up the phone and call them before clicking anything.

2. Not deleting cookies Cookies are digital trackers. They are used to save website settings and to track your behavior. For example, if you click a product, cookies are logged in your browser and shared with ad networks. This allows for targeted advertising.

There's no good way to tell who is tracking online. But you can use more secure web browsers, like Firefox and Safari. These browsers make it easier to control who is tracking you.

Continued pg.2

(continued from page 1)
In Firefox, for example, click the three lines in the upper right corner, go into the Options menu and set your Privacy & Security preferences. Plus, every web browser has the option to delete cookies – which you should do constantly. In Chrome, simply click History, then choose "Clear Browsing Data." Done. You can also use ad-blocking extensions, like uBlock Origin, for a safe web -browsing experience.

3. Not checking for HTTPS Most of us know HTTP – Hypertext Transfer Protocol. It's a part of every web address. However, most websites now use HTTPS, with the S meaning "secure." Most browsers now automatically open HTTPS websites, giving you a more secure connection, but not all sites use an SSL certificate to secure the traffic.

If you visit an unsecured HTTP website, any data you share with that site, including date of birth or financial information, is not secure. You don't know if your private data will end up in the hands of a third party, whether that be an advertiser (most common) or a hacker. Always look in the address bar of every site you visit. Look for the padlock icon. If the padlock is closed or green, you're secure. If it's open or red, you're not secure. You should immediately leave any website that isn't secure.

4. Saving passwords in your web browser Browsers can save passwords at the click of a button. Makes things easy, right? Unfortunately, this method of saving passwords is not the most secure. If a hacker gets your saved passwords, they have everything they could ever want. Most web browsers require a password or PIN to see saved passwords, but a skilled hacker can force their way past this if given the chance.

Protect yourself with a dedicated password manager! These apps keep passwords in one place and come with serious security. Password managers can also suggest new passwords when it's time to update old passwords (and they remind you to change your passwords!). LastPass, 1Password, and Keeper Security Password Manager are good options. Find one that suits your needs and the needs of your business.

5. You believe it will never happen to you This is the worst mentality to have when it comes to cyber security. It means you aren't prepared for what can happen. Business owners who think hackers won't target them are MORE likely to get hit with a data breach or malware attack. If they think they are in the clear, they are less likely to invest in good security and education for their employees.

The best thing you can do is accept that you are at risk. All small businesses are at risk. But you can lower your risk by investing in good network security, backing up all your data to a secure cloud network, using strong passwords, educating your team about cyber threats, and working with a dedicated IT company. Good IT security can be the best investment you make for the future of your business.

Cathy and Larry Sightings

Catherine spent most of February in the Midwest. Snow, rain, cold!

Larry has been working on several orchestrations for various groups.

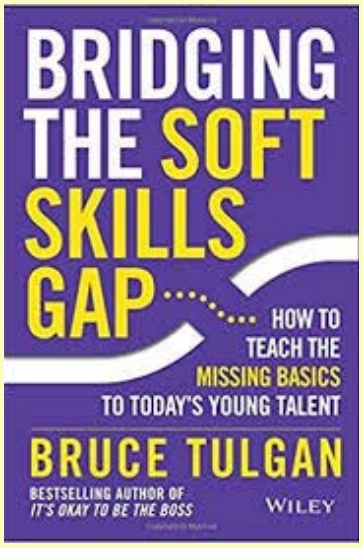
'You are Braver than you Believe, Smarter than you Seem, and Stronger than you Think.'
- Winnie the Pooh

Bridging the Soft Skills Gap by Bruce Tulgan

I find this title irritating, mostly because it implies that I'm responsible to teach the 'soft skills' if I expect them from our staff. But if I grew up with them, what's changed? Well, Mr. Tulgan starts with this question, and answers it pretty well.

As each chapter unfolds, there are sections where he clearly lays out the two points of view. He also gives some important historical background for each generation that we find in the workplace right now. Our view of soft skills and our responsibilities to use them in society and the work place are formed not only by world events, but by the generation that raised us. In other words, we have some culpability when it comes to the soft skills gap in the next generation.

The best part about this book is the lesson plans. Each skill is defined, given context as to why it is needed in the work place, steps to introduce it to our younger workers (and some of the older ones, too), then its practical application in the work place. I've got yellow highlights all over this book! Positive Attitude, Responsibility, Good Work Habits, and more. This is reality, so dig in and get started! - *CMW*



Shiny New Gadget Of The Month:

ThePhotoStick Mobile

Never worry about running out of memory on your smartphone again! It happens to all of us – you're trying to take a picture or record a video and you get a message saying your phone's storage is full. You don't want to buy another new smartphone, so what can you do besides delete old photos?

This is where ThePhotoStick Mobile comes in. It's a memory stick compatible with most Android and iPhone devices and will boost your phone's memory without your having to buy a new phone. ThePhotoStick Mobile is an insurance policy against lost photos and videos.

ThePhotoStick Mobile gives you more control. While most smartphones work without a hitch for years, you never know if something might happen or if you'll run out of memory. ThePhotoStick Mobile plugs into your device and allows you to copy photos over. You can keep them on ThePhotoStick or transfer them to another device. Learn more at GetPhotoStickMobile.io!

From the Techs

Too Much Data—What to Delete

Data sizes can grow out of control like bunnies (we did a fun stick-man video on this one). There are two places on your computer that may have data that can be cleaned out to buy back some of that drive space and improve performance.

The first one is easy – the Deleted folder in your email. **You actually have to delete the email in the Deleted Items folder; really**.

What we've learned over the years is that there are quite a few of you that use the Deleted email folder to save email, like an archive. When you need historical info, you search the deleted folder. I admit, I search this folder from time to time, and it can be helpful for recent items. But, we don't recommend using this folder to archive email messages. If it's worth saving, move it to an Archive folder. Besides, there are probably quite a few email messages in there that really could be deleted after all and it's tedious to sort through everything when you're running low on space and have to clean up (I've had to do this, BTW).

So, rather than delete an email to the Deleted folder, you can use the **Shift/ Delete key combination to permanently delete** any email you want deleted. At a minimum, this saves some extra steps. Besides, when it's time to clean out the Deleted folder, you'll have a lot less data to look through.

Second, when you're on the server and you delete files, or even on your workstation/laptop, they go to a Recycle Bin where they may sit for quite a while, taking up space. You think you threw them out, but you haven't emptied the trash can yet.

We recently had a client with a huge amount of data in the Recycle Bin, bringing their available drive space to critically low levels. The same thing can happen on your workstation/laptop, or even a server.

So why don't people empty the Recyle Bin? They **may not know about it**, which is why we write these articles. Sometimes we find that people are using this as a way to store files for future use, which is not the intent. When maintenance is done on the computer, **you may be in for an unexpected and potentially unwelcomed surprise**.

A computer maintenance checklist includes a step to 'empty' the Recycle Bin on the computer. This frees up space and cleans up the files. If you're using this as a file drawer, you may want to re-think your process and move important files to file folders, instead.

Sometimes files seem unnecessary, but you just don't feel comfortable deleting them. That's a great time to **move them to an external hard drive or thumb drive**. Don't forget to label these with dates and a general description of the contents, then put them in a safe place.

Running out of space can freeze-up a computer, corrupt data, and create unexpected and expensive work disruptions. Keep your computer data clean and organized which should allow you to have more days when you 'love' your computer rather than the alternative. – *CMW*

Construction Corner

Sage Upgrades, Enhancements

In late December, Sage came out with version 22.3.30 for 100 Contractor. This release had the Federal tax tables and quite a few states. In late January, Sage had another minor release that included a few more states. The list of states that were part of the release were included with the release email they sent.

When Sage announces a Release , they include highlights of things that have been changed. Not all releases need to be installed. You have some options, so here are some guidelines:

- If the release has a feature you've been waiting for, a 'fix' to something that you regularly use, a report you've been waiting for, or a tax update that impacts your payroll, go ahead and contact your IT group to arrange the upgrade.
- If it is a new Major release, the first number will be higher. For instance, in 2019, we were all running version 21, then mid-year, Sage released version 22 and wanted us all to be on it in 2020 (which is why the tax tables were only released in version 22).
- Sage only supports the last two Major releases.

When updates are announced, we usually get a couple of panic calls. Sage is very aggressive about getting everyone on the latest release. It's easier for Sage to support one or two releases, rather than having all their support people proficient on multiple versions of the program; completely understandable.

In mid-January, we had a call from a client who got the very dire-looking warning saying they had to upgrade. The new warnings are larger, red and black, and look very 'dangerous' if you don't comply. She panicked and started installing the upgrade. Unfortunately, she was installing it on her local workstation and created some new problems that required some emergency IT intervention.

If you're going to install the update, there are a couple of things to keep in mind here, too:

- Before you start, check the space on your server. The upgrade when installed takes additional space, and upgrading the datasets also requires more space.
- Plan ahead. Everyone will need to be out of the software, so a little planning will ensure everything goes smoothly.
- An upgrade requires Exclusive Access, so everyone is out.
- All datasets, including archives, need to be updated, as well.
- For those of you with local workstation/laptop installations, the new release is 'pushed' from the server rather than the old way of installing on each and every machine; a great time-saver, but an extra step during the upgrade process.
- Some of you have a separate SQL instance with the old archives; be sure the datasets on that separate instance are also updated; all datasets/archives need to be updated.

Lastly, there is a new Product Enhancement feature. Sage indicates that this helps them learn how their user base works within the software and what modules they use. With release 22.3.30, this feature automatically opted you 'in' for this tracking. We noticed it because we saw a Sage 'user' when we wanted Exclusive Access. It was turned 'on,' although we did not check the box. It's under the Home & Resources icon. You can take a look and see if you're marked as 'Opt In' and if you'd rather not participate, you can uncheck the box (which is what we did). Food for thought. – *CMW*

Who Wants To Win a $25 Amazon Gift Card?

This month's trivia question:

What computer virus replicates itself, shutting down the computer system in the process?

a) worm b) botnet c) Trojan Horse d) back door

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, 2020

Congratulations to last month's Trivia Contest winner, Tammy Pelchatt with **Tri-State Painting** in NH! Tammy's name was drawn from the fishbowl for last month's correctly answered question:

The computer scientist/MIT professor who invented the World Wide Web:

d) Sir Tim Berners-Lee

Visit www.syscon-inc.com/Trivia for contest rules.

FIELD INTEGRATED TIME SYSTEM

Collecting Time From the Field Just Got Exciting!

You won't find a better, fully integrated, field time collection solution than ours because we wrote it to do what our clients need! Interested? **Want to enjoy Mondays again?** Join us Friday, **March 27th at 11:30am Central Time** to hear all about it! Register at www.syscon-inc.com/events.