Cyber Times

Newsletter by Secure ERP, Inc.

LAST CHANCE

October Lunch & Learn Series

IN CPA SOCIETY

October 23rd I'll be presenting on Cyber Threats & Solutions for the Indiana CPA Society.

Although this provides CPE for CPAs, we would love to have law firm partners, medical practice managers and business owners attend to learn how best to defend against hackers & ransomware.
Space is limited.

REGISTER HERE:
https://www.incpas.org/home/cpe-and-events/eventdetail?evt_key=58ea3be7-8c6b-4ff6-8a60-eb791cd64862&SSO=true

October 2019

This monthly publication is provided courtesy of Rick Rusch, CEO of Secure ERP, Inc. Secure ERP is a network security & ERP integration specialist in central Indiana with over 25 years of experience supporting small to medium sized businesses. Founded by a CPA and Cybersecurity Evangelist, Secure ERP is dedicated to protecting our clients' data and supporting their people and growth.
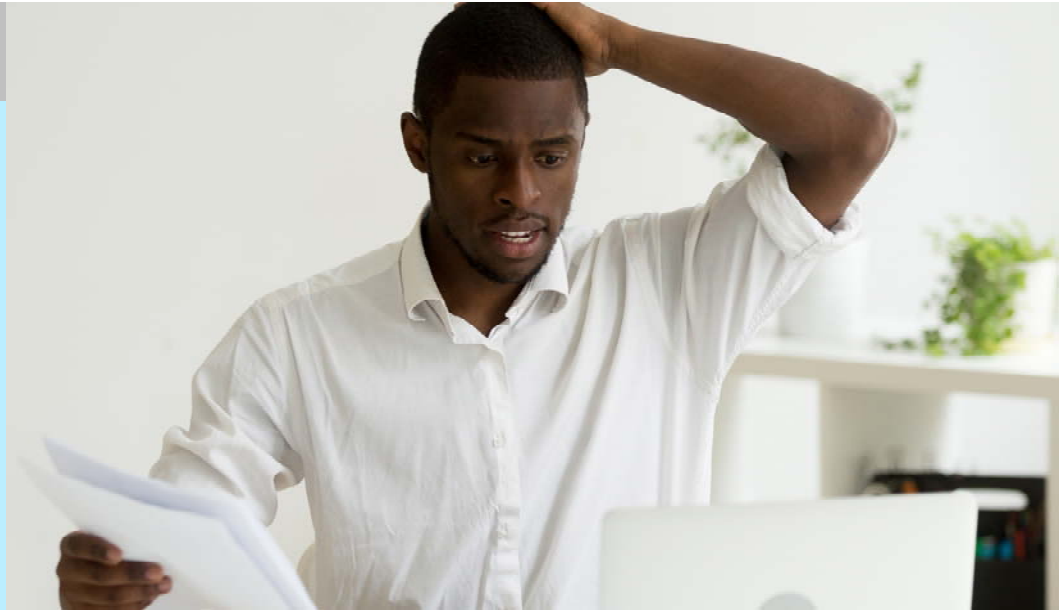
Employees Keeping Your Data Safe?
... Don't Count On It

In any business, big or small, employees can be your biggest IT threat, and they might not even realize it. Businesses already face countless cyberthreats, like data breaches, cyber-attacks, online viruses and malicious e-mails. But despite all these outside threats, the real problem can come from the inside.

One of the biggest threats to your business's security is simply a lack of awareness on the part of your employees. It comes down to this: your employees just aren't aware of current threats or how to safely navigate e-mails and the web. They might not be aware when they connect to an unsecured WiFi network or if they're using a firewall. They may be haphazard in all things IT. *There are a lot of variables.*

Your best defense, in this case, is training. Get all of your employees on the same page. Look at your current training and find the gaps, or start putting together training if

you don't have it. You want a training program that covers all your bases and gives your employees the knowledge and tools they need to keep themselves and your business secure. (Don't know where to begin? Work with cybersecurity specialists, **Secure ERP**. We know what your employees NEED to know!)

Another major security threat is phishing e-mails. On any given day, you and your employees can be on the receiving end of dozens, if not hundreds, of fraudulent e-mails. Data from Symantec shows that 71% of targeted cyber-attacks stem from phishing e-mails. While awareness regarding phishing scams is better than ever, it's still far from perfect. And it doesn't help that phishing e-mails have gotten more advanced.

Phishing e-mails are typically disguised as messages from a legitimate source, such as a
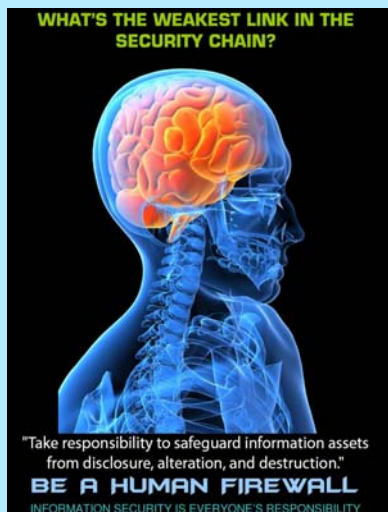
colleague, a bank or an online retailer. They try to trick recipients into clicking a link or opening a file (which you should NEVER do if you are not 100% sure about the source). But there are easy ways to identify scam e-mails:

1. They're impersonal. They may be addressed to "customer," "to whom it may concern" or "my friend." But be careful – sometimes they are addressed properly and use your name.

2. They're full of spelling and grammar errors. Not every phishing e-mail will have these errors, but it's good to read e-mails word for word rather than just glancing over them. Unusual errors often mean a scam is lurking.

3. The "from" e-mail address is unfamiliar. This is one of the easiest ways to pinpoint a scam e-mail. Look at the sender, and if the address is filled with numbers, letters, misspelled words or is weirdly long, there's a good chance it's from a scammer.

The other major issue facing your business is your employees connecting to unsecured WiFi hot spots. It is such an easy mistake to make. Whether it's a remote employee or an employee working during lunch at a corner café, you never know when they might connect to unsecured WiFi (it doesn't help that it's everywhere these days). One Spiceworks study found that upward of 61% of employees connect to unsecured public WiFi while working remotely.

The problem is, you never know who is watching or if the public

WiFi is really the network you intend to connect to. Hackers can easily set up a "fake" network to divert traffic to their hot spot to circulate malware and steal data.

Another WiFi threat might be right at home. If you have employees who work from home, you need to make sure their home WiFi connection is secure. Too often, homeowners leave their WiFi wide-open because it's home. They think no one's going to sneak onto their WiFi or they keep it unsecure because it's easier to connect a lot of devices.

While it might be easier to connect to, it can cause *huge* problems. For one, WiFi signals can reach hundreds of feet. It's easy to sit outside of an apartment or out on the street and find dozens of WiFi signals. If any of these signals are unsecure, a hacker can sit outside undisturbed and go to work accessing data and planting malware.

It all comes back to this: Work with your employees to establish IT best practices. Educate them on threats and how to protect themselves and your company. Help them develop a positive IT security mindset at the office, at home or anywhere they work, whether they're using company equipment or their own.

Don't know where to start? Don't worry – one phone call and we can help get you started. Don't wait. Let's secure your business today.

"71% of targeted cyber-attacks stem from phishing e-mails."

Our passion is your cyber protection, worry free tech is what we deliver.
www.secureerpinc.com • (317) 290-8702

Why Cyber Security

"Take responsibility to safeguard information assets from disclosure, alteration, and destruction."
BE A HUMAN FIREWALL
INFORMATION SECURITY IS EVERYONE'S RESPONSIBILITY

Awareness Training?

It's the very first thing I ask any owner, "Are you training your employees?" Often I get a shrug or they will happily say "YES, we test them once a year." Numerous studies have shown the national average of **30 minutes of training a year** isn't enough to prevent an accident which could severely damage your firm.

From the FBI, to national cybersecurity experts, they ALL agree, that you MUST continually train employees about cyber threats and defenses. Roughly 5 minutes a week or a whopping 20 minutes a month at a cost of a few dollars per employee a month.

I have a standing guarantee that if you offer coffee to all your employees, the cost of the coffee will be a larger expense. If I lose I'll pay for 2 months of your training for free and you won't have to buy the service.—R²

Creating The Perfect Team

Google has collected endless amounts of data, conducted countless studies, spent millions of dollars and logged thousands of hours all in the name of trying to better understand their employees. One initiative was to try and understand what makes a team effective. Specifically, **Google wanted to know why some teams excelled while others didn't.** The study was called Project Aristotle, and they gathered up some of Google's best talent to try and understand, codify and decipher how to create high-functioning teams.

The results of Project Aristotle may forever change how you go about assembling a team. Before the study, Julia Rozovsky, Google's people analytics manager, felt that the best teams came from compiling the best people. The "best of the best" would surely be the way to go. As she later stated, *"We were dead wrong."*

Google assembled organizational psychologists, sociologists, statisticians, engineers and researchers to attack this issue. For over two years, Project Aristotle studied 180 Google teams and analyzed over 250 different team attributes, looking for the magic dream-team formula, but they came up empty. Nothing was standing out to ensure you would be putting together an outstanding team.

They stumbled across some research by psychologists and sociologists that focused on what are known as "*group norms*": the traditions, behavioral standards and unwritten rules that govern how teams function when they work together. Following this new line of thought, they went in search of behaviors that magnified the effectiveness of a team and found five key characteristics of enhanced teams. Julia Rozovsky listed their findings as follows:

1. DEPENDABILITY: Team members get things done on time and meet expectations.

2. STRUCTURE AND CLARITY: High-performing teams have clear goals and have well-defined roles.

3. MEANING: The work has personal significance to each member.

4. IMPACT: The group believes their work is purposeful and positively impacts the greater good.

But #5 is the most important of all of them:

5. PSYCHOLOGICAL SAFETY: Imagine a setting where everyone is safe to take risks, voice their opinions and ask judgment-free questions; imagine a culture where everyone can let down their guard. That's psychological safety. Google found that teams with psychologically safe environments were more successful.

Psychological safety is dependent on team dynamics. There is no concern about authority or power. Everyone is focused on the clearly defined goal and *open* to whatever will help them obtain it. They are comfortable with the people on their team. The chemistry is proactive. They chat, they laugh, they have fun and they enjoy each other's company. There is no pecking order, no interest in titles, power or credit.

If you want an effective team, focus more on chemistry, diversity, balance and camaraderie. Then stir in talent, subjective and objective people, introverts and extroverts, fast and steady people, young and old and some brilliant nerds. A team full of quarterbacks will never win a Super Bowl.

Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys *and* 52 Essential Habits For Success, *he's shared the podium with esteemed figures from across the country, including former President George H.W. Bush, former Secretary of State Colin Powell, Anthony Robbins, Tom Peters and Steven Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.*

3 Ways To Make Your Business Grow

Invest In Advertising: Look at what's available and what makes sense for your niche. Need to go local? Newspapers combined with Facebook ads may make sense. Online advertising through Google and Facebook are a crucial way to reach customers, local, regional or global. It can take some experimenting to get it just right.

Invest In Training: As the world changes, so does business. Ensure your employees are at the top of their game when it comes to both industry standards and the way you do business. Keep them educated on best practices and make sure training is consistent across the board.

Invest In Your Team: Your employees make your business work. You want to make sure they're operating at their best. Offer a healthy work environment that promotes their well-being. It can be as simple as offering great perks like flexible hours, remote work, professional development, catered lunches – the list goes on. Happy employees are the best employees. *Smallbiz Technology, 2/12/2019*

Are You Making These Mistakes When Texting In Your Business?

Do you text clients? Do you text clients after business hours? A recent report by Carphone Warehouse found that 73% of respondents had no problem texting with clients after business hours. However, this can lead to serious issues, namely when it comes to drawing the line when communicating with clients (or employees). It breaks the professional barrier. After-hours texting says you're available 24/7. It can intrude on your personal life, and when you don't text back, it can harm that professional relationship. If you must text, treat it like an email: stick to working hours and keep it business-focused.

Don't open doors to unprofessional behavior. Texting is a very casual form of communication, and it's easy to forget you're chatting with a client or employee. You must be careful about what you say, especially if you're in a management position. Keep it professional and courteous. *Small Business Trends, 7/8/2019*

Use These Top Tips To Fuel Your Productivity

Stress can be a burden on your productivity, but there are ways you can use it to your advantage and turn it into something positive. Here are three tips to do just that:

1) Recognize your stress. You must come to terms with the fact that you need to manage your stress. If you don't, you won't be able to fuel your productivity.

2) Change your mindset. Most of us view stress as a negative. Instead, remind yourself you can manage your stress. It's not a brick wall but rather a door you can open to new possibilities.

3) Find new motivation. With a new outlook on stress, you can use it to take action and get things done. Tasks and deadlines will always be there, and when you feel stress, you can buckle down to get those tasks done, because once you are done, you will feel great. *Inc., 7/19/2019*

"You know, in the tech world being disruptive is seen as a positive."