The Tech chronicle

What's New

While she may not be all that new, Elizabeth (Liz) Gonzalez has been adding a lot of new functionality to our company. Liz was hired last year part time to help with some of the admin work. It didn't take very long to realize she was going to amount to much more than we bargained for. In no time Liz streamlined our ordering, scheduling and billing systems. She then set to task completely revamping our project management system. As if that wasn't enough Liz has her hands in much of the new marketing initiatives we have undertaken. Truthfully, she is the one who makes this newsletter a reality each month. We are very excited to have Liz on our team and look forward to the next big project we throw her way.

October 2019

This monthly publication provided courtesy of Craig Covington co-owner Canon Capital Technologies

Our Mission

To enhance our customers quality of life and the health of their business

Are Your Employees Keeping Your Data Safe?

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 professional IT specialists. They 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

Continued on pg.2

Continued from pg.1

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.

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

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.

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To get started and claim your free assessment now, call 267-381-2025.

Texting for Business

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 could harm that professional relationship.

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. If you must text, treat it like an email: stick to working hours if possible and keep it business-focused.

Small Business Trends, 7/8/2019

Creating The Perfect Team

Google has collected endless amounts of data, conducted studies, and spent millions of dollars in order to try and understand employees. One initiative was to try and determine what makes a team effective. Google wanted to know why some teams excelled and others didn't. The study, titled Project Aristotle, gathered some of Google's best talent to try and understand how to create high-functioning teams.

The results were striking. Before the study, Julia Rozovsky, Google's people analytics manager, felt that the best teams came from compiling the best people. As she later stated, "We were dead wrong."

Google assembled organizational psychologists, sociologists, statisticians, and researchers to attack this issue. Over two years, Project Aristotle studied 180 Google teams and analyzed over 250 different team attributes, looking for the magic formula, but nothing was standing out to ensure you could put 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 together. Following this line of thought, they went in search of behaviors that magnified the effectiveness of a team and found five key characteristics. Julia Rozovsky listed their findings as follows:

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

2. STRUCTURE AND CLARITY: Teams have clear goals and well-defined roles.

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

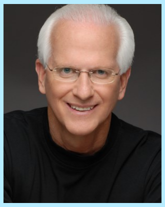
4. IMPACT: The group believes their work is purposeful and positively impacts the greater good.

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

5. PSYCHOLOGICAL SAFETY: Imagine, everyone feels safe to take risks, voice their opinions and ask judgment-free questions; this is 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 have fun and enjoy each other's company. There is no pecking order, no interest in titles, power or credit.

If you want an effective team, focus on chemistry, diversity and camaraderie. 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 a widely recognized professional speaker. Author of 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.