# The Tech chronicle

## What's New

## October 2020

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.

# The #1 Mistake Your Employees Make That Lets Cybercriminals Into Your Network

We all make mistakes—it's a fact of life. But as we all know some mistakes can have serious and lasting consequences especially when it comes to business and cyber security.

While some businesses have invested heavily in cyber security, many have not. When it comes to network and data security one of the most vulnerable areas of the economy is small businesses.

More often than not, small businesses simply don't go all-in when it comes to IT security. Some fear they don't have the budget and worry that IT security is too expensive. Others don't take it seriously they have an "it won't happen to me" attitude. Then there are those who invest in *some* security, but it's limited and leaves them vulnerable in the long run.

But there is one area of IT security

where *every* business is vulnerable. You can have the greatest malware protection in the world and still fall victim due to this one big mistake.

Your employees lack IT security training.

It's as simple as that. When your team isn't trained on IT or network security *and* they aren't aware of today's best practices, you open yourself up to major risk. Here's why: We all make mistakes.

Scammers and cybercriminals have the most success when they are able to trick people or play on the emotions of their victims. One common emotion they use is fear.

No one likes to get a message telling them that their bank account has been compromised. This is how phishing e-mails work. The scammer sends an e-mail disguised as a message from a bank

---

Continued from pg.1

or financial institution. They may tell your employee that their account has been hacked or their password needs to be changed immediately. They use fear to trick them into clicking the link in the e-mail.

So, concerned about their bank account, your employee clicks the link. It takes them to a web page where they can enter their username, password and other credentials. Sometimes it even asks for their full Social Security number.

As you guessed, the web page is fake. The link in the e-mail directs your employee to a page that allows the scammer to collect their data. Some thieves use it to access their bank account, but others sell the information. No matter the situation, the information has fallen into the hands of crooks.

> **"Your employees are your first defense against outside cyber-attackers."**

The challenge is that phishing e-mails have gotten harder to spot. Scammers can spoof legitimate web addresses. They can make fake e-mails look like the real deal. But there are still plenty of minor details that indicate the e-mail is a fake. This is one of the MANY reasons why comprehensive employee IT training is so important. Training helps employees identify red flags and stay up to date on *changing* red flags. A phishing e-mail from 2010 looks nothing like a phishing e-mail from 2020. Scammers stay ahead of the curve. They know the trends and how to adapt. Your employees need to know the trends and need to be ready to adapt as well. Good IT training covers much more than phishing e-mails. It helps your employees identify security red flags across the board, including:

- Phishing e-mails and phone calls
- Poor or outdated passwords
- Malicious software hidden in links, attachments or online ads
- Poorly configured security on employee devices (a big deal for remote employees!)
- Lack of guidelines related to Internet or social media usage on employee devices
- Outdated software or hardware

Good training is also continuous. Cyber security training isn't a one-and-done deal. It's something you do every quarter or twice a year. Just as you keep your business's equipment maintained, you have to keep your employees' cyber security knowledge maintained. After all, your employees are your first defense against outside cyber-attackers. When they know what they're dealing with, they're better equipped to stop it in its tracks and protect your business.

The bottom line is that a lack of training is the biggest threat against your computer network and the health of your business. You need to have a strong training program in place to make sure your employees stay up-to-date. But you don't have to do it yourself. We can help. Along with your team, let's protect your business together.

# Improve Your Cash Flow With These Tips

*Have Better Billing Processes:* Make it as easy as possible for customers to pay their bills. Incentivize them to pay before the due date with a small discount or offer. Be diligent about sending invoices as soon as possible after customers buy with you.

*Get Cooperative:* If it's possible or practical, work with other businesses to form a buyers' co–op. This gives you more buying power when buying in bulk.

*Credit Check Customers:* When dealing with higher-priced goods or services and a customer can't pay in cash, don't be afraid to run a credit check. Customers with poor credit can be a liability and cost you big.

*Audit Your Inventory:* Identify what costs you money by sitting around. If you're stuck with inventory that isn't moving, you may need to discount it to get rid of it.

*Pay Online:* Pay all of your bills online. This way you can select the exact date when those bills are paid each month, giving you more control over your cash flow.

*SmallBiz Technology, Jan. 27, 2020*

# What Makes A Leader Successful Today?
## *Intentionality And The 3 Shifts*

Have you ever wondered what one thing all successful leaders have in common? First, consider what all *unsuccessful leaders* have in common: they lack focus.

Either they aren't clear on what they're trying to do or they know what they need to do but aren't doing the right things to achieve their objectives. Both waste money and resources and leave organizations stuck in the status quo. This affects leaders regardless of the size or type of organization, and that's why I wrote *The Intention Imperative.*

What all great leaders have in common is intentionality — *being crystal clear on what you're trying to achieve and taking the right actions every day to achieve it.*

Why do many business leaders lack clarity?

1. They inherited an unclear vision or never had one to begin with.
2. They value operations over objectives: doing things without questioning why.
3. They were distracted by problems, or even opportunities, which took them off course.
4. They were unwilling or unable to look at what was consistently being done with a fresh perspective.

What are the symptoms and signs of a leader who lacks clarity?

1. Constant changes in focus or direction
2. Lack of momentum
3. Confusion among employees and what to do
4. Many team members asking "Why?"
5. Frustration at every level
6. Inconsistent action or behavior

In my book, I explain intentionality and then share what I believe are imperative changes leaders need to take today to succeed: the shift from *structure to culture,* from *motivation to inspiration* and from *experience to emotion.*

### IMPERATIVE 1 – CULTURE

*"Culture is what we think and believe, which then determines what we do and what we accomplish."*

In *The Intention Imperative,* I teach the five levers you have for creating and maintaining the culture you desire. Creating it is the job of a leader.

### IMPERATIVE 2 – INSPIRATION

*"Inspiration doesn't have to be mysterious or complicated to create."*

What is inspiration? It is motivation to the power of purpose. It is linking meaning to motives. Inspiration doesn't come from outside force or artificial causes. It develops from the work itself and how the leader is able to demonstrate importance and impact.

### IMPERATIVE 3 – EMOTION

*"Emotions are everywhere and they are the single biggest factor in how we make decisions."*

A negative emotional experience can be offset with a positive one. The customer experience is important, but how the customer feels about that experience is critical. Few companies design and deliver for positive emotion.

*Now, try these three things:*

1. Focus on building a culture that powers the right actions to create the right results you, your team and customers need for breakthrough success.
2. Couple purpose with motivation so your team is inspired.
3. Design your product and service delivery around positive emotions.



*Mark Sanborn, CSP, CPAE, president of Sanborn & Associates, Inc., an "idea studio" seeks to motivate and develop leaders in and outside of business. He's a best-selling author of books like* The Potential Principle. *A noted expert on leadership, team building, and company change, he holds the Certified Speaking Professional designation from the National Speakers Association. Check out his video series "Team Building: How To Motivate And Manage People" or his website, MarkSanborn.com, to learn more.*