CST TECHNOLOGY TIMES

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

Tech Talk...

with Lisa Brown, CEO of CST Group Inc.

Trick-or-Treat Cybersecurity: Don't Get Spooked This October! October is Cybersecurity Awareness Month, and just like Halloween, the digital world is full of tricks and treats. The scary truth?

Cybercriminals are always knocking at your door, but the good news is, you can fill your cybersecurity "candy bag" with tools and habits that keep the tricks away and the treats flowing.

Trick: Phishing Emails That Lure You In. Cybercriminals love disguises. Just like someone showing up at your door pretending to be a friendly neighbor, phishing emails try to trick you into clicking dangerous links or handing over sensitive information.

Treat: Always check the sender's address carefully, hover over links before clicking, and when in doubt - don't open the door – instead use the delete key! Adding some security to your email

continued on page 4

CST Group Inc.

This monthly publication is provided courtesy of Shawn & Lisa Brown, Owners.

OUR MISSION:

CST Group Inc. is a PROACTIVE technology management firm who's mission it to SECURE, PROTECT and MANAGE technology for Small to Medium Businesses like yours.

There are many common myths when it comes to cybersecurity, and, unlike harmless stories, these myths can leave you with gaping holes in your company's cybersecurity defenses. Here are five common myths and the truth behind them.

Myth #1: It Won't Happen To Us.

There's a common belief among Small and Medium-sized Businesses that they are too small to be a target for attackers. But this isn't the case; in fact, some cybercriminals target SMBs specifically, with the knowledge that SMBs are less likely to have the resources for reliable cybersecurity.

Cyberattacks happen to organizations of all sizes, in all verticals and geographies, and hit 80% of businesses. The global financial toll? A projected $9.5 trillion. And while large corporations can take the hit and recover, a single ransomware attack has the potential to put an SMB out of business.

So, regardless of what type of business or organization you have, you must protect yourself from cyberattacks and reduce your exposure. Always assume you are a target – because you are one.

Myth #2: If It Worked Then, It'll Work Now.

It's very common for decision-makers to reason that since they've never been breached in the past, they won't be breached in the future either. However, that belief doesn't account for the rapid pace at which technology – and cybercrime – are evolving.

The threat landscape is constantly changing and there is a very real game of cat-and-mouse at play. If you're not moving forward, you're moving backward. Effective security is a cycle of anticipation, adaptation and action.

Myth #3: Once Secure, Always Secure.

Unfortunately, technology is fluid – just like your business. Every time you bring on a new staff member and add new devices, your technology's configuration shifts. As it does, it creates new avenues of attack from cybercriminals.

continued on page 2...

...continued from cover

and management are necessary to maintain security integrity. The attack surface stretches beyond common focus areas. Because of this, strong cybersecurity demands a holistic, proactive, continuous approach.

Myth #4: Business Optimization Is Incompatible With Security.

Many organizations still assume that security initiatives create operational friction – delaying releases, adding red tape and increasing costs. This outdated thinking frames security and business optimization as mutually exclusive, as if improving one compromises the other.

While these perceptions may have roots in the past, they don't reflect modern practices. Today, security enables optimization. That means minimizing both waste and risk – including security risk.

In the end, secure systems are more resilient, predictable and cost-effective. This makes security a driver of business performance, not a barrier.

Myth 5: A Strong Password Is All I Need.

Creating a strong password (at least 16 characters long and a blend of letters, numbers and special characters) for each account is important, but it's not the only step needed to keep your data secure. For one, every account and device needs a unique password. If you reuse passwords, it means that if one of your accounts is hacked, all of your other accounts are at risk. To store all your unique passwords, we recommend a password manager!

Enabling MFA for every account will double your protection. The few seconds required to enter a code sent to your phone is well worth the extra security. That said, there are plenty of other vulnerabilities that savvy hackers can exploit to attack your business's data. That's why working with an MSP is a critical component of maintaining your company's cybersecurity.

CARTOON OF THE MONTH

DR. PHIL

PUSHES BUSINESS OWNERS TO "OWN IT"—IN LIFE AND IN BUSINESS

In a recent interview, Dr. Phil McGraw, celebrity psychologist and talk show host, gave frank advice on what it really means to be in business—and how business owners stay true to themselves while doing it.

Staying True To Passion And Standing Out

"I don't do anything that I'm not a hundred percent passionate about. And I never wanted to be a member of the herd. I didn't want to be a face in the crowd," McGraw said. "I wanted to market my education in a way that set me apart from the rest of the industry. I think you have to do that [in business]."

Define And Articulate Your Differentiator

"You have to know what separates you from everybody else that thinks they do what you do. What do you bring to the table that nobody else does? What do you do that's different than everybody else? If you don't know what your differentiator is, if you can't articulate it and don't market it in an easily perceptible way, then you aren't really in business yet."

You Are Your Own CEO

"I think every one of us is a company of one," said McGraw. "I don't care if you work for the United States post office. Every one of us is a company of one—and you are your own CEO. Then the question becomes: how are you doing in managing your career? How are you doing in managing your stock? How are you advancing your game? What is the world willing to compensate you for? If you can't articulate that with clarity and precision, then you're not really in business yet. You haven't gotten the courage."

Define, Commit And Own Your Brand

"No one is going to confuse me with anyone else, just like you're not going to confuse McDonald's with a great steakhouse. That's important to me," he said. "Define your brand, decide what it is, make a commitment to it and ride that horse to the finish line. You've got to decide what it is that you're selling and own it. Be who you are on purpose. Don't just get up and react to the world. Decide who you are and do that on purpose. Don't apologize for it. Own it."

Authenticity Is Key To Facing Criticism

"In the pursuit of that, you will face criticism. Not everyone will like you and your brand. But that's exactly why you have to believe in what you're doing passionately," says McGraw. "You can't just put it on. You have to believe it. A lot of people don't like some of the things I do. And I get that. But how boring would this world be, if we were all the same? We have a divisive world, in terms of ideas. But you have to believe what you believe. Then when somebody disagrees with you, if you're authentic in your position, you won't have a problem standing with it."

SHINY NEW GADGET OF THE MONTH

BenQ ScreenBar Halo Monitor Light

The BenQ ScreenBar Halo is a sleek USB-powered LED monitor light designed with an asymmetric optical system that directs soft, glare-free illumination onto your desk while avoiding screen reflection. With adjustable brightness and color temperature, you can dial in the perfect lighting using the wireless controller. It even has a backlight to reduce contrast with your surroundings. Plus, the auto-dimming feature adapts to your room's lighting, so it's always just right. No messy cords or mounts – just clean, functional lighting that protects your eyes and keeps your setup looking sharp.

Welcome, Victor!

We're excited to introduce you to the newest member of the CST team!

Victor Ortiz, our new IT Technician! Victor brings strong technical knowledge, a love of learning, and an upbeat, positive attitude that fits perfectly with our culture of excellence.

We know our clients will enjoy working with him as much as we do. Please join us in giving Victor a warm welcome to the CST family!

5 SIGNS

YOU'RE DUE FOR A TECH UPGRADE

At first, hanging on to old technology for as long as possible seems like a great way to stretch your IT budget. However, the cost of doing so is much higher than simply replacing the tech.

Continuing to use old hardware and outdated software can cost your business in productivity, budget and security.

The Real Cost

There are a few ways that outdated technology is costing your business. First, old systems move slower, causing your team to move slower and impacting productivity. These systems can also fail completely, causing unexpected downtime and putting a major dent in your deliverables.

There's also the risk factor to consider.

Outdated software and hardware are more vulnerable to cyberattacks, because they are no longer being patched to protect against known vulnerabilities.

Hackers are able to exploit these vulnerabilities and access your business's data. Because of this latent risk, your business also runs the risk of failing compliance audits. That's why it's so important to update to the latest software or hardware to stay secure.

Here are a few signs it's time to upgrade your technology:

1 Your Systems Are Still Running On Windows 10 Or Older

Windows 10 is rapidly approaching end of life; Microsoft will end support for it in October 2025. This means any new vulnerabilities will no longer be patched by security updates. Continuing to use Windows 10 past its end-of-life date is a major cybersecurity and compliance risk. To keep your business protected, start planning your upgrade path now and make the switch to Windows 11.

2 You Frequently Call IT For The Same Tech Problems

Frequent crashes and lagging systems aren't just annoyances, they're also indicators that your technology is failing. Slow systems, crashes, frustrated team members and constant tech support add up – and mean a significant impact on your productivity.

3 Your Existing Software Isn't Compatible With New Tools

If you're still using legacy software, it may not integrate with mobile apps or cloud platforms. This limits your ability to adopt new technologies, serve clients efficiently and scale your business.

4 Your Devices Are Slowing Down Your Team

If your team's computers are taking ages to boot up, or freeze or crash during video calls, they're slowing down your entire workflow. At the end of the day, time is money. Inefficient systems harm both. Devices more than three to five years old should be audited for performance and energy efficiency to ensure they aren't having a negative effect on your productivity and energy consumption.

5 You're Relying On Outdated Security Mechanisms

If your business's firewall or antivirus hasn't been updated in years, you're taking serious risks with your data. Cyberthreats evolve quickly; to keep your business safe, your defenses need to evolve too. Outdated systems are often the first point of entry for ransomware attacks.

If you're worried that upgrading tech will break the bank, we hear you. But hanging on to slow, outdated systems can cost more in lost productivity, security gaps and patchwork fixes. The good news is there are plenty of affordable, strategic upgrade paths to keep your business running smoothly without blowing your budget.

IT for Local Government – Powered by CST Group Inc.

You already know the level of protection, expertise, and peace of mind CST Group delivers. Now, we're bringing that same gold standard to municipalities and local government through our new division: IT for Local Government, Powered by CST Group Inc.

We are proud to be the #1 cybersecurity service provider for towns, municipalities, and government compliance. From ironclad security to regulatory peace of mind, we make sure public services stay protected and communities stay safe.

Here's where you can help: if you know a town, village, or municipality struggling with outdated IT, constant cyber threats, or compliance headaches, connect them with us.
You'll be giving them the same trusted partner you already rely on.

Have a referral in mind? Call us at 877-954-4100 or share www.cstsupport.com—let's make sure every community has the protection they deserve.

Let's Keep Our Defense Strong

Every football team knows the season isn't won in one game—it's built week after week with consistent practice, smart plays, and solid defense. The same is true for cybersecurity.
If You're already part of the CST Group team, that means you have a strong playbook and a dedicated coach in your corner. But just like the best teams, we can't get comfortable—we've got to stay alert and keep refining our strategy.

This month:

- **Check your equipment: If you've spotted "benched" devices in your office, let us know before they fumble your productivity.**
- **Tighten the defense: Make sure everyone on your team is using multi-factor authentication (MFA).**
- **Review the game film: If something feels "off" or suspicious, send it our way. No play is too small when it comes to protecting your business.**

Passionate NOT Pushy WITH LISA BROWN

SCAN HERE

The Power of Being Around Passionate People

One of the greatest joys in both life and business is surrounding yourself with people who truly love what they do. Shawn and I are fortunate to be part of several industry-leading organizations, and last month I had the pleasure of attending an event that reminded me just how powerful it is to be in a room full of passionate, like-minded peers.

There's an energy that can't be replicated when you spend time with people who care deeply about their work. These are individuals who don't just "do a job", they live their purpose, they show up fully, and they bring that spark into every conversation. As a technology and cybersecurity leader, it's inspiring to connect with others who are just as driven to innovate, protect, and lead in their industries.

Here's what struck me most: passion is contagious. When you're around people who are truly lit up by what they do, it pushes you to think bigger, dream bolder, and take action with renewed clarity. It's not about competing, it's about collaborating, sharing, and celebrating each other's wins.

For me, this is the heart of Passionate Not Pushy. It's not about forcing your voice into the room, it's about letting your authentic enthusiasm shine so brightly that others can't help but feel it too. And when passionate people come together, they raise the bar for everyone creating new opportunities, fresh ideas, and stronger communities.

So this month, my encouragement to you is simple: seek out the people who fuel your fire. Spend time with those who inspire you, challenge you, and remind you why you love what you do. Because when passion meets passion, incredible things happen.

And here's the key: being passionate about what you believe in doesn't mean closing the door on other perspectives. True passion leaves room for curiosity. It allows us to stand firmly in our values while also listening, learning, and respecting the experiences of others. Sometimes disagreement can be the very thing that broadens our understanding, sharpens our thinking, and helps us grow.

In times when the world feels divided, choosing to listen is one of the most powerful acts of leadership we can offer.

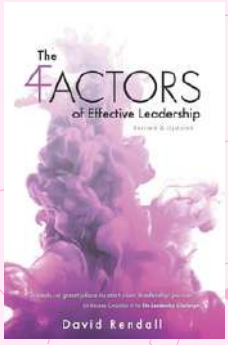
If you are passionate about what you do, I'd love to have you share that passion with our listeners on the Passionate Not Pushy Podcast. Reach out to Sara at sara@cstsupport.com to get on the PnP Podcast Schedule.

"passionate NOT pushy"
Lisa

<BOOK> <OF_THE> <MONTH>

WHAT I'M READING...

This month I'm recommending a book by my friend and mentor, David Rendall. *The 4 Factors of Effective Leadership* is a practical guide built around influence, integrity, inspiration, and improvement. It's a powerful reminder that leadership isn't about authority, it's about the impact you have on others. A quick but meaningful read that will challenge you to lead with purpose.



....Tech Talk Continued from Front Page

is a must so please ensure you have encryption capabilities and managed detection and response on all email accounts. Looking for assistance? CST can help so give us a call. The conversation is always free!

Trick: Weak or Reused Passwords
Using the same password for every account is like giving away your house key to every stranger who asks. Once one account is cracked, the rest are easy targets.

Treat: Use a password manager to create strong, unique passwords for each account. Add multi-factor authentication (MFA) for an extra layer of protection. CST offers a password manager that allows administrative control, so you protect your business along with your employees. Want to know if you are already on the dark web? Give Sara a call and request a FREE Dark Web Scan – 518-483-4100.

Trick: Unpatched Software
Hackers are like trick-or-treaters who know exactly which houses keep their doors unlocked. Outdated software leaves the door wide open.

Treat: Keep your systems and devices updated. Those pesky pop-ups asking for updates? They're really candy wrappers hiding the sweetest protection. Automating updates and patches will save time and provide peace of mind.

Trick: Public Wi-Fi Without Protection
Logging into sensitive accounts on open Wi-Fi is like sharing your candy bag with the whole block—anyone can reach in and take what they want.

Treat: Use a VPN (Virtual Private Network) or stick to trusted, secure connections when handling sensitive work or personal data.When in the office, be sure "outsiders" are using a guest WiFi that is separate from your organization. You do not want to risk getting someone else's cold (aka virus).

Cybersecurity doesn't have to be scary. By trading a few tricks for proven treats, like MFA, updates, and smarter habits, you can keep your business, your employees, and your community safe. Remember, it's much better to hand out the candy than to become the victim of a cyber trick!

And Speaking of Treats…

This month, we've added something even sweeter to the CST family – a new team member! Victor Ortiz has joined our technical team and will be assisting Shawn, Carrie, Tyler and Michelle with helping our clients. We couldn't be more excited.

Just like strong passwords and updates keep your systems secure, the right people keep our company strong. We look forward to the value that Victor will bring to our clients and our team.

Welcome Victor to the CST family!

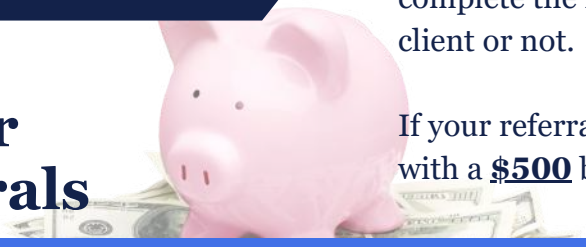
I also want to thank our clients as we celebrate CST's 25th Anniversary! I started Computer Support & Training in October 2000 and we have grown from a small break/fix IT company to a cybersecurity powerhouse! I am so grateful to all of you who have trusted CST as your premier IT provider. We will continue to keep you safe, secure and informed.

Stay safe, stay secure, and have a Safe Cybersecurity Awareness Month!

Lisa

BIG REWARDS

For Your Referrals



We'll offer you **$50** as a gesture of appreciation, once you introduce CST Group to a qualified colleague and they complete the initial appointment whether they become a client or not.

If your referral becomes a managed client, we'll provide you with a **$500** bonus at the end of their first month of service.

SO, YOU MIGHT BE WONDERING – WHO MAKES AN IDEAL REFERRAL?

- **Any business with 5 or more computers**
- **Needs help with its network, backup, compliancy, support, and security**
- **Wants 24x7x365 peace of mind**

Full Details Here: https://www.cstsupport.com/about-us/referral-program/
or call us at 1-877-954-4100

October is Cybersecurity Awareness Month!

But Why Does It Matter?

Every October, organizations nationwide observe Cybersecurity Awareness Month — a reminder that protecting sensitive data and critical systems is everyone's responsibility. While large corporations make headlines when they're attacked, small businesses and local governments are actually among the most common targets and yet we never hear about it. A single successful phishing attempt or ransomware infection can cost hundreds of thousands of dollars and disrupt critical services. Why? Because attackers know these organizations often have fewer resources, but still manage highly valuable information: employee records, financial data, and even resident services.

For small businesses, a successful cyberattack can lead to financial loss, downtime, and reputational damage. For local governments, it could mean disrupted public services like billing, permitting, or even emergency response systems.

Cybersecurity Awareness Month is the perfect time to double check your defenses, review your digital habits and reinforce safe practices with your staff. Security is strongest when everyone takes part. Investing in security today protects your business, your employees, and your community tomorrow.

Need some help? We offer training to help your team stay on top of Cybersecurity and out of the headlines. Email Jessica@cstsupport.com to set up trainings.

AND AS ALWAYS,
#STAYCYBERSAFE

=Jessica=

Passionate NOT Pushy
WITH LISA BROWN

SUBSCRIBE

New Podcast Episode Alert!

No Tricks, Just Treats with Missy Vega

This month, Lisa sits down with Missy Vega, Director of Business Development at Technology Marketing Toolkit—a mentor, leader, and lover of all things Halloween. Together, they dive into mentorship, women in leadership, and how to bring passion (and a little spooky flair) into your career and life.

Missy Vega

OCTOBER EVENTS

-CYBERSECURITY AWARENESS MONTH-

5TH SHAWN'S BIRTHDAY
8TH LISA'S BIRTHDAY
13TH INDIGENOUS PEOPLE'S DAY (OFFICE CLOSED)
16TH BOSS'S DAY
26TH NATIONAL BLACK CAT DAY
31ST HALLOWEEN

CONCERNED ABOUT THE SAFETY AND SECURITY OF YOUR ONLINE IDENTITY? YOU SHOULD BE!

If you've been following the latest news in cybersecurity, you know that attacks have only continued to grow in both size and sophistication. However, you might not be aware that small and mid-sized businesses like yours are the most targeted by Dark Web criminals. Would you be among the 60% of SMBs that would be bankrupted by the average cost of a data breach?

If you are reading this, you are eligible for a free and comprehensive Dark Web scan to identify how many of your credentials (DOB, SSN, User ID's and Passwords) have been compromised. To get your FREE Scan instantly, contact us today at 518-483-4100 or 941-249-3520 or email sara@cstsupport.com.