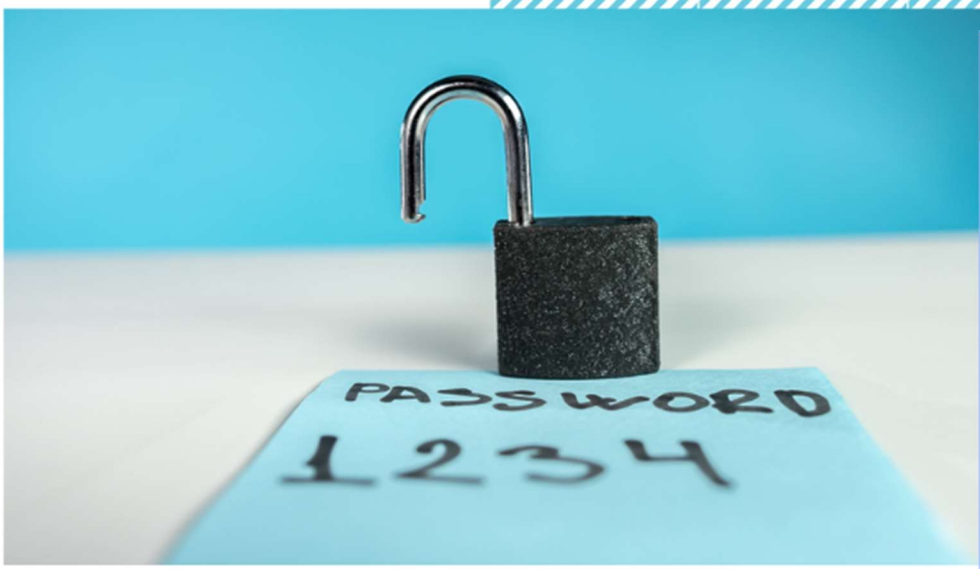
CST TECHNOLOGY TIMES

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



"passionate NOT pushy" about your technology

By Lisa Brown, CEO & Founder

When you live a busy life, you prioritize based on "need" and "noise" but even those things you consider low maintenance or low priority need attention eventually.

Let me explain. Shawn is crazy about our yard. He doesn't necessarily love to mow, weed whack, and fertilize, but he loves the outcome and takes pride in making sure our home looks amazing. This is why I surrounded our home with perennial plants, perennial flowers, and a solid base of mulch because this girl does not want to weed, pull or maintain any of it. I want it to look beautiful without a huge amount of maintenance.

However, low maintenance does not mean NO maintenance.

Last weekend, as Shawn was mowing the grass, I took a walk around our home only to realize there were more weeds than plants.

(CONTINUED ON PAGE 3)

HOW TO SAFELY SHARE PASSWORDS WITH EMPLOYEES

If you ask a security professional, you get by-the-book advice about sharing passwords: "Don't share passwords." But we know, in reality, that doesn't work. Your office might be sharing a single password for apps like SurveyMonkey right now to save cash on buying additional users, and some social media accounts don't even give you the option to have multiple log-ins.

Sharing passwords in your office is sometimes necessary for collaboration, and the best way to do this is by using a password manager. Affordable (some platforms even offer free versions), layered with security and simple to use, password managers are the safest and easiest way to store and share your company's private passwords.

Reasons You Would Need To Share Your Passwords

Share accounts are the biggest reason businesses share passwords, whether their employees work from a physical office or at home. It improves collaboration and makes employees' jobs a lot easier.

Medical leaves, turnover, vacations and "Bob isn't coming in because he ate bad fish last night but has our Amazon log-in" are other reasons passwords get handed around like a plate of turkey at Thanksgiving dinner.

However, unsafe sharing habits will put your private passwords in the hands of reedy hackers, who can fetch a high price for your data in dark web markets. IBM Security reported that in 2022, 19% of all breaches were caused by stolen or compromised credentials.

So, how do you share passwords safely?

continued on page 2...

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 that specializes in helping municipalities and compliance-driven industries to SECURE, PROTECT and MANAGE their technology.

...continued from cover

First, Avoid These Common Password-Sharing Mistakes

When it comes to password sharing, remember:

1. **Don't send passwords via e-mail:** E-mail is the #1 target of hackers, and many e-mail services aren't encrypted. Those that are encrypted are still risky because e-mails are stored in several servers on their way to or from your account. That means your e-mail is sitting in a Sent folder, ripe for the taking by anyone who gets into your e-mail account, encrypted or not.
2. **Never text or chat passwords:** Like e-mails, SMS messages or messaging apps like Slack aren't secure. Once a text is sent, it's available for anyone to see.
3. **Stay away from storing passwords using pen and paper and shared documents:** Sticky notes, memo pads, Google Docs – NEVER write down your passwords.
4. **Avoid the temptation to store passwords on your device:** If your device gets hacked, nothing stops that perp from taking every password you saved.

The Best Way To SAFELY Share And Store Your Passwords

We recommend using reliable password managers because they have multiple layers of encryption so only those with a key (your master password) can see it, AND they include more robust security and sharing features like:

> **IBM Security reported that in 2022, 19% of all breaches were caused by stolen or compromised credentials.**

- **Zero-knowledge architecture:** Not even your password manager service can see the information you save in your vault.
- **Multifactor authentication (MFA):** For added log-in security.
- **Unique password generation:** Creates strong, random passwords to improve log-in security.
- **Fake log-in page warnings:** Warns you if a page is spoofed by hackers.
- **Breach or weak password notification:** Alerts you if one of your passwords was leaked or if your current password is weak.
- **Simple, secure built-in password sharing:** Some password managers let you choose which passwords your employees can see and keep others in a private vault. Others, like Keeper, let you share documents or records without exposing credentials.

To use password managers, you only need to remember one password – the master password. One downside is that whomever you share a password with needs an account for the same service. However, most password managers have corporate accounts, so this shouldn't be a problem.

A Word To The Wise: Look out for password managers with a bad security track record, like LastPass, which was breached in 2022, 2021, 2016 *and* 2015.

Smart Businesses Use Password Managers

It's a good idea to avoid sharing passwords as much as possible, but when you have to, use a reliable password manager to ensure you have control over exactly who sees your credentials. Talk to your employees about safe password hygiene, host regular security-awareness training for employees and use MFA with every account. It's not just safe business – it's smart business.
If you're not sure which password manager to use, give us a call and we'll get you set up with one.

"Free Up Coming Webinar"

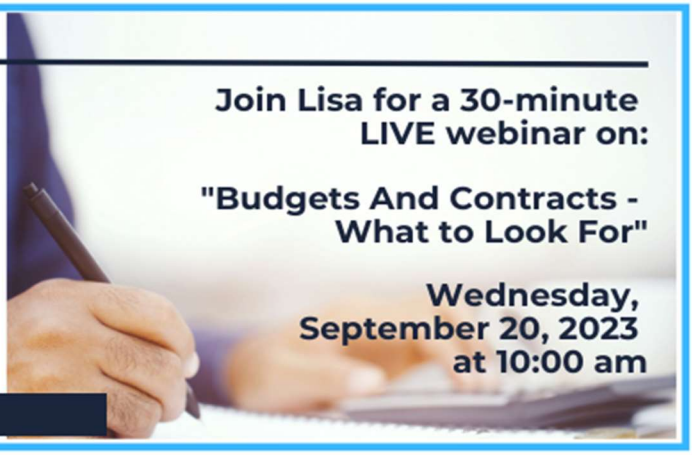
During the webinar, you'll learn...

- Technology requirements that need to be included in 2024's budget
- Contract Do's and Don'ts
- You can't forget these things… Especially compliance.

Who should attend...

All Small Business Owners who are working on next year's budget and need to consider technology changes, contracts, and compliance.

Secure your place by registering now at www.cstsupport.com/webinar



...passionate NOT pushy...continued from cover

So, I got busy with our four-wheeler, wagon and garden tools. Four hours later, I had a full wagon of weeds and grass stains on my knees.

How did I let it go unattended for this long without noticing? Because those weeds didn't make noise or call out to me or complain. They simply grew with no care of where they were or how they were affecting my beautiful flowers. I didn't realize how intrusive they were until I started to pay attention to them.

This is how I feel about protecting clients from cyber security risks. Hackers are lurking in the background, quiet, silent, not intrusive at all. Most of you have no idea they are even there stealing your data and planting files that will one day corrupt your data. It isn't until they make noise that you pay attention. Even with the state and federal government barking at you to implement cyber security precautions, you still don't. Your insurance provider should be prompting you to get cyber liability insurance which requires all sorts of safety measures and yet, you don't act.

So, what must happen for you to put cyber security at the top of your priority list? Instead of waiting for your data to disappear or a hacker to infiltrate, this is me….making NOISE and asking you to prioritize cyber security precautions right NOW.

To make this easy for you, here is a list of seven cyber security precautions that should be in place now to ensure you are meeting the compliance guidelines and protecting your business.

Remember, even if you are a client, you may not have authorized us to implement everything on this list. I will discuss the new regulations with you in our next quarterly business review. For now, here is what every business should have in place:

1. Proactive monitoring and maintenance – not just antivirus/anti ransom software.
2. Endpoint Detection and Response Software - a watchdog to "bark" if something gets in.
3. Automatic updates, scans, and patches – the Windows environment gets constant updates and patches. Make sure those are downloaded and installed.
4. Security Awareness Training – this is a must for cyber insurance and should be automated and reportable.
5. Password management – complex passwords are a must to keep your accounts safe and writing it down on a post-it or notebook is no longer acceptable.
6. MFA – Two Factor Authentication on ALL Accounts.
7. Hardware Managed Firewall – you should have a wall between your internet connection and your computers, and this hardware needs to be monitored for malicious access.

These seven things are the MINIMUM of what you should have in place NOW! Depending on your industry and needs, there are a few other things you should have in place. Reach out if you need additional information.

If you are wondering how susceptible your company is to risk, CST offers penetration tests to determine risk levels. Reach out if you want to learn more.

I want to welcome Mary Boyea as our newest member of the CST Team. Mary is our receptionist/front desk clerk and the first voice you hear if you call our offices. Please be patient as she gets to know you. If you're wondering what happen to Michelle, no worries, she is still with us but moving into our Marketing Department.

As always,
"passionate NOT pushy"
Lisa

Create The Healthy Work-Life Balance Your Mind And Body Need

Business owners and entrepreneurs are some of the hardest-working individuals in our country. They're constantly sacrificing for their business, but eventually this behavior takes its toll on their bodies and minds. If you own a business, it's important to dedicate some time every day to your hobbies, interests and passions – all it takes is a concentrated effort.

One great strategy to create a healthier work-life balance is adding your personal activities to your calendar. Adding items like family dinners or golf rounds to your calendar helps ensure you actually participate in these activities. It's also helpful to set some boundaries. Determine how many hours you're allowed to work each day and what activities you're not willing to miss. Once you establish a boundary and get into a strong routine, you'll feel much happier, and your business will still get the attention it deserves.

WILL THE REAL FRED BONES PLEASE STAND UP

September can only mean one thing....Fred is back baby!! Our loveable, under-fed, seasonal worker is awake and back at the office for his fourth year with us.

Of course all of our long time clients know that when fall season starts, Fred wakes from his slumber to check up on the office. As usual Fred is ready to get started.

Fred will be accompanying our Tech Manager, Carrie, on all of her onsite visits. Also, he may join her in the mornings to drop her two girls off at school, but no worries he is a professional. He wont be carrying any equipment but he is an excellent supervisor while Carrie works. Take a picture, or slap a company sticker on him to mark the occasion.

We know that when September hits, there are only a handful of weeks before the snow flies at our headquarters in Northern New York, so Carrie likes to make as many visits as possible before the weather gets unpredictable. This gives her some time to check in with many of you and Fred will get some much needed fresh air before his winter slumber.

Keep a look out for Carrie and Fred this fall season. Fred looks forward to some quality time with his favorite people.

Remember where Carrie goes Fred will follow! #followfred