CST Tech News

What's New

It's time to talk about the Leprechaun (in honor of St. Patrick's Day) in the room!

Want to know the ONE thing my office works on EVERYDAY? Multiple times a day? All of which we believe is simple, common sense and yet hundreds of thousands of dollars are lost every day by ordinary people like you and me.

EMAIL PHISHING! How many emails are you getting in a day and how many of those emails are actually relevant emails with valuable content from people you want to get an email from? I get over 100 emails a day — which is why I only check email twice a day — because I would spend ALL day, everyday, checking darn email. If you guessed about 10% you would be correct. I would bet my hard-earned money that is about the same for you.

Now, how many emails are advising you of a package that could not be delivered, a client asking for money or credentials, a vendor asking for verification of your account information, even your bank, credit card company or PayPal asking for account information? How many emails are trying to sell you something? What about Amazon, Microsoft or Apple locking you out of your account?

It is absolutely out of control and that is why Business Email Compromise (BEC) makes up 89% of virus, ransomware, phishing attacks and financial loss and it continues to rise.

It may be helpful to explain how your email can get compromised. NOTE: It is significantly more complicated that this, but this is an easy way to think about it:

(Continued on page 3)

March 2023

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

CST Group Inc.

Our Mission:

To provide outstanding technology services to our customers allowing them to focus on their business.

Improve Your Cyber Security Awareness

Learn About Today's Most Common Types Of Cyber-Attacks

If you've turned on the news sometime during the past few years, you've probably heard of more than one instance where a business closed due to a cyber-attack. You may think your business is small enough and hackers won't target you, but this couldn't be further from the truth. Every business is at risk of experiencing a cyber-attack and should be well-prepared to defend against these threats. With the right type of attack, a cybercriminal can gain valuable information about your business, customers and employees, which can be used to damage your reputation and hurt you financially.

If you're a business owner or leader and you want to ensure your business is well-protected, check out the most common cyber-attacks that are affecting companies today. From there, you can implement cyber security plans and tactics to ensure your business is protected from cybercriminals.

Phishing Scams

Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure. Phishing scams can wreak havoc on your business and personal life. You may have seen an e-mail from someone claiming to be Amazon or your credit card company asking for specific sensitive information. Often, the e-mail address does not line up with who the person is claiming to be.

When a phishing scam targets your business, they'll likely request valuable information from your employees such as passwords or customer data. If your employees fall for the scam, they could give a cybercriminal unprecedented access to your network and systems. This may also allow the cybercriminal to steal private employee and customer information, leaving your employees

Continued on pg.2

Continued from pg.1

vulnerable to identity theft. Phishing scams can be averted by using common sense and providing cyber security training to your employees. Most companies will not request private information over e-mail. That being said, if an employee receives a suspicious e-mail, they should do their due diligence to ensure the e-mail is genuine before responding in any way.

Malware

Malware is software installed on a computer without the user's consent that performs malicious actions, such as stealing passwords or money. There are many types of malware, including spyware, viruses, ransomware and adware. You can accidentally download malware onto your computer by clicking on sketchy links within e-mails or websites. You might not even notice you have malware on your computer right now. If your computer is operating more slowly than usual, web browsers are taking you to random sites or you have frequent pop-ups, you should scan your computer for malware.

Prevention is key in stopping malware from affecting your business. Hiring and utilizing a managed services provider is the best way to protect your business, as they will continually monitor your network for exploitable holes. With malware, it's always better to play it safe than sorry. If a cybercriminal is able to use ransomware on your network, your business could be stuck at a standstill until you pay the ransom. Even if you can pay the ransom, your reputation will still take a hit, and your business could be greatly affected. Be careful where you click on your phone, too, since malware attacks on cellphones have become more common over the past few years.

> "Every business is at risk of experiencing a cyber-attack and should be well-prepared to defend against these threats."

Attacks Involving Passwords

How do your employees access your network or computer systems? They most likely use a password to log in to their computer, access their e-mail and much more. What would happen if someone with bad intentions gained access to one of your employee's passwords? Depending on the individual's access, they could obtain sensitive information about your business, customers and employees.

Your team should be using long, complex passwords for their accounts, and each password for every account should be different. We encourage you to implement a password management tool that will allow you and your employees some control over complex passwords and it provides a means for you to keep track of them more easily. You should also incorporate multifactor authentication to ensure nobody can steal a password and gain access immediately.

If your business falls victim to a cyber-attack, it could have lasting consequences for everyone involved. Now that you know the most common types of cyber-attacks, you can start implementing plans to ensure you and your business stay protected. Please call us if you have any questions or are looking for some guidance.

FREE 30-MINUTE WEBINAR

Join Lisa for a 30-Minutes LIVE Webinar on

Wednesday, March 15th at 2pm

Data Protection and Backups—What and Where!

Small Business Owners or Decision Makers who want to protect their business information in a secure and efficient way should attend this webinar. You need to understand what and where your data is and it all needs to be tested regularly. Even your Cloud data needs to be protected. Take 30 minutes and learn how.

Register NOW to reserve your spot:

Register at: www.cstsupport.com/webinar

(Continued from page 1)

1. You create an email and hit the SEND button
2. That email leaves your computer and enters the world of the Internet – THIS IS WHERE THE PROBLEM ARISES.
3. Your email can be intercepted at any point during its travels as it bounces from server to server. Matter of fact, hackers have written code that scans and analyzes data that may contain key words like routing numbers, bank numbers, SSN, DOB, EFT, financial institution names, etc. If the program flags any of these key words (along with thousands of others), it will advise the hacker where he/she can gain access to it, spoof it (copy it) and then communicate as if they are you to the recipient.

So, what can you do about it? Here are some tips to help you through the copious amounts of email rubbish in your inbox:

1. Use a professional email – not Gmail, Yahoo, or any other public email domain.
2. Activate Multi-Factor Authentication – this two-factor setting will prevent unauthorized access to your email by sending a code to your phone. This alone will cut down on email breaches and compromises by 99%.
3. NEVER (and I cannot stress this enough) – NEVER, send money to anyone, EVER, without confirming via telephone. Make sure you actually talk to someone BEFORE you initiate any electronic funds transfers. Now this does NOT apply to paying bills online.
4. NEVER send confidential data via email. So never email an account number, PIN, date of birth, social security number, bank information, credit card information, etc., without encrypting the email first.
5. Speaking of encryption, if you absolutely need to send confidential information, be sure to have the ability to encrypt it. Adding an encryption feature to your email is easy and worth the investment.
6. Initiate some Security Awareness Training to ensure your employees understand the risk.

I will be hosting a webinar regarding managing email June 21st . Please register for that event to learn how to identify spam email along with some other valuable information.

I want to thank those of you who attended February's webinar on Compliancy. It was a huge success, and we believe these webinars will allow us to educate and communicate. They are always the third Wednesday of every month. If you want our schedule, please call the office and talk to Michelle. She can get you a copy of the entire years' webinar schedule.

As always "**Passionate NOT Pushy**"

Lisa

Don't Come Back To Work

Don't come back to work. Instead, move forward in leading your company and managing your career by embracing remote work. Even though ghSMART has been remote-only for over 26 years, I never fully realized how enthusiastic I am about remote work until I heard that many companies are forcing workers to come back into offices.

Before the COVID-19 pandemic, "work where you want" was a rare concept – but during the pandemic, basically every company that could function with people working remotely shifted to that mode out of necessity. I thought that mode would stick, and we'd see the landscape of cities shift from "places people go to work every day" to "places people go to work sometimes, eat, shop, learn and play." But it seems I was wrong.

There isn't a great argument against the idea of remote work, but there is one *for* it. Remote work improves financial and operating performance and productivity for companies while also improving job and life satisfaction for employees. A 2015 Stanford University study published in the *Quarterly Journal of Economics* showed a 13% performance increase from remote working, and employee attrition rates fell by 50%.

Even with all of the research and information available that shows remote work is beneficial, there are still some myths floating around. For example, many say you can't build a great company culture when your business operates remotely. This is entirely false. I think an excellent culture begins with doing what's best for people. Making people commute to offices daily does not seem to be in anybody's best interests.

Another common myth states that people don't work as hard remotely as they do in an office. I believe that if you have a transparent culture where performance is measured, you can pay people according to the value they are creating. They will be incentivized to work productively and not lollygag – even if they are working remotely. But I guess many companies have not yet figured out how to pay employees based on a scorecard of measurable results and instead pay based on hours worked. They should be worried about lollygagging anyway, both in the office and for people who work remotely.

If you run or own a company, please continue to experiment with allowing your people to work remotely when possible. I believe this is the future of work, both because of the demonstrable benefits to companies in operating and financial performance and the benefits to workers due to having more control over their time.

Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times *bestsellers. He stays active in his community and has advised many government officials.*

TYLER'S TECH TIPS

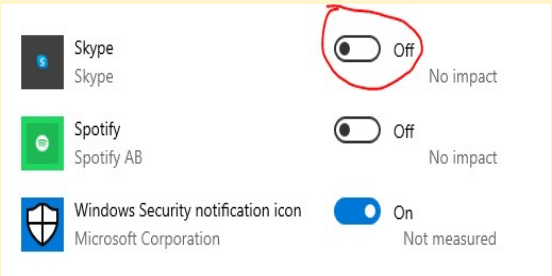
Does your computer take a long time to start up?

You might want to check to see if there are too many start up apps slowing it down.

1. Simply type "start" in your windows search bar and click "Startup Apps"
2. Then go through and turn off any apps that don't need to open when you first turn on your computer.

Programs and Apps like Spotify and Skype can be turned off at start up, which then frees up memory on your computer resulting in a faster experience.

Remember, you can always call the office if you need assistance. We'd be happy to take care of this for you.



HAPPY MARCH!

As we end the first quarter of 2023, we begin the spring season. The first day of spring is quickly approaching and the team here at CST are looking forward to the sunshine. Soon the snow will melt and you can bet we will be pulling out the grill and picnic table so we can enjoy some team lunches outside. Most of us spend 8 hours at our job 5 days a week so we feel it is important to find as much enjoyment as we can while we are here.

Protecting your technology is a passion of ours but it can be stressful for us as well. Because of that we like to make sure we take time to check in with each other. Sometimes that can be a little coffee talk in the morning or a nice team lunch together. Having a good office life makes a huge difference in the enjoyment of your job. What do you do to find joy in your workday?

-Jessica

Working Remotely? Improve Your Work-Life Balance In 3 Steps

As many businesses continue to utilize remote workers, some employees are struggling to find a proper work-life balance. They constantly find themselves drawn back to their work after completing all tasks for the day, which takes away from their ability to enjoy hobbies or spend time with their families. Maintaining a proper work-life balance is beneficial to all aspects of our lives, including productivity and overall happiness. If you're struggling to maintain your work-life balance, here are three ways to include more personal time in your daily routine.

Set Boundaries: Don't allow yourself to be pulled back into work. Turn off your work phone and e-mail when your shift has ended for the day.

Create A Workspace: Do not work in the same areas you use for relaxation. This will make it more difficult to relax when you've finished working.

Dress Professionally: It might be tempting to wear sweatpants while working from home, but try to wear the same clothes you would wear if you had to go into an office. When the workday comes to a close, you can dress in more comfortable clothing, allowing you to easily unwind.