CETech
IT Hassle Free
1425 Mount Read Blvd Suite 125
Rochester, NY 14606

Who Else Wants To Win A $25 Gift Card?

The Grand Prize Winners of last month's Trivia Challenge Quiz were Norm St. John from the Town of Hamlin and Padam Ghimirey from Tru Care. They were the first two people to correctly answer our quiz question from last month.

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! The first two people to correctly answer this month's trivia question will receive a $25 Amazon gift card. One winner per company per quarter.

What technology is used to record cryptocurrency transactions?

A) Digital wallet
B) Mining
C) Blockchain
D) Token

Email us at **chill@cetechno.com** or call us now with your answer! **585-441-0055**

Do These Things To Protect Your Business From Getting Hacked

1. Train Employees. Your team needs to know how to identify and handle today's IT security threats. Cybercriminals often rely on your employees' lack of training to break into your network. Ongoing training gives employees tools and resources to overcome this and many other IT security challenges. Make training a top priority!

2. Hold Employees (And Yourself) Accountable. Training and company guidelines don't mean much without accountability. When you set rules, follow them, just as you follow industry and government rules and regulations when operating your business. Be willing to hold anyone accountable.

3. Have A Disaster Recovery Plan. Things happen. When you store sensitive data, you need to have a plan in place to recover and restore that data should anything happen. This doesn't just include data loss from malicious attacks but other types of disasters, including hardware failure, fire and flood. How is your data being backed up and saved? Who do you notify in the event of a breach? Who do your employees call in the event of disaster?

SmallBiz Technology, Dec. 26, 2019

4 TIPS TO GET PROJECTS DONE ON TIME WITH A SMALL TEAM

Give Them The Tools And Resources They Need — We all need tools to get things done – project management software, content creation tools, messaging apps, virtual private network access and more. Have a conversation about what each team member needs to maximize productivity and work closely with them to meet that need.

Set Aside Time For Proper Research Don't jump headfirst into a project without jumping into research first. Information is a powerful tool to get things done efficiently and effectively.

Assign Accordingly —Before the team goes to work, make sure assignments or responsibilities are delegated properly and check in with everyone on a regular basis to make sure things are going smoothly (or to see if they need help).

Plan And Plan Again —Plan out the project before you set to work. Give yourself and your team a map to follow as you work through the project. As with any project, expect obstacles along the way and be willing to update your map accordingly.

Small Business Trends, July 4, 2020

CE BITS & BYTES
INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY
October 2020

WHAT'S NEW

OCTOBER IS NATIONAL CYBERSECURITY AWARENESS MONTH

October is National Cybersecurity Awareness Month created by the US Department of Homeland Security and the National Cyber Security Alliance. The purpose is to ensure people and businesses are taking proactive steps to enhance cybersecurity to stay safe online.

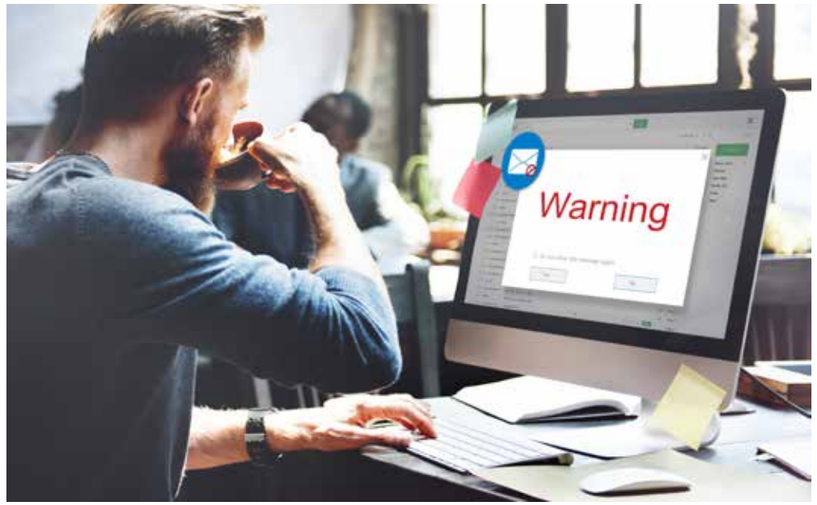
This year's theme is "**Do Your Part. #BeCyberSmart."** "If you connect it, protect it." If everyone does their part implementing stronger security practices, raising community awareness, educating, or training employees - our interconnected world will be safer and more resilient for everyone.

Securing Devices at Home and Work- With the emergence of telemedicine, digital health records, internet-connected medical devices, and patient wellness apps, many benefits have been created, but have also exposed the industry to vulnerabilites that cyber-criminals regularly attempt to exploit.

The future of Connected Devices- Technological innovations, such as 5G, might impact consumers' and business' online experiences, as well as how people and businesses can adapt to the continuous evolution of the connected devices moving forward. No matter what the future holds, every user needs to be empowered to do their part.

National Cybersecurity Awareness Month is an ideal time to become cyber aware. We have lots of options to help you out. Stay vigilant with cybersecurity. Give us a call, your cybersecurity experts. **585-441-0055.**

585-441-0055



Employees Are Letting Hackers Into Your Network ...

What You Can Do To Stop It

Cyberthreats are everywhere these days. Hackers, scammers and cybercriminals are working overtime to break into your network – and the network of just about every business out there. They have a huge arsenal of tools at their disposal, from automated bots to malicious advertising networks, to make it possible.

But there is one "tool" that you may be putting directly into their hands: your employees. Specifically, **your employees' lack of IT security training.**

While most of us expect hackers to attack from the outside using malware or brute-force attacks (hacking, in a more traditional sense), the truth is that most hackers love it when they can get others to do their work for them. In other words, if they can fool your employees into clicking on a link in an e-mail or downloading unapproved software onto a company device, all the hackers have to do is sit back while your employees wreak havoc. The worst part is that your employees may not even realize that their actions are compromising your network. And that's a problem.

Even if you have other forms of network security in place – malware protection, firewalls, secure cloud backup, etc. – it won't be enough if your employees lack good IT security training. In fact, a lack of training is the single biggest threat to your network!

It's time to do something about it. Comprehensive network security training accomplishes several things, including:

1. Identifying Phishing E-Mails Phishing e-mails are constantly evolving. It used to be that the average phishing e-mail included a message littered with bad grammar and misspelled words. Plus, it was generally from someone you'd never heard of.These days, phishing e-mails are a lot more clever. Hackers can spoof legitimate e-mail

-- Continued on page 2

... continued from page 1

addresses and websites and make their e-mails look like they're coming from a sender you actually know. They can disguise these e-mails as messages from your bank or other employees within your business.

You can still identify these fake e-mails by paying attention to little details that give them away, such as inconsistencies in URLs in the body of the e-mail. Inconsistencies can include odd strings of numbers in the web address or links to YourBank.net instead of YourBank.com. Good training can help your employees recognize these types of red flags.

2. Avoiding Malware Or Ransomware Attacks One reason why malware attacks work is because an employee clicks a link or downloads a program they shouldn't. They might think they're about to download a useful new program to their company computer, but the reality is very different. Malware comes from many different sources. It can come from phishing e-mails, but it also comes from malicious ads on the Internet or by connecting an infected device to your network. For example, an employee might be using their USB thumb drive from home to transfer files (don't let this happen!), and that thumb drive happens to be carrying a virus. The next thing you know, it's on your network and spreading.

"Every device on your network should be firewalled and have updated malware and ransomware protectection in place."

This is why endpoint protection across the board is so important. Every device on your network should be firewalled and have updated malware and ransomware protection in place. If you have remote employees, they should only use verified and protected devices to connect to your network. (They should also be using a VPN, or virtual private network, for even more security.) But more importantly, your employees should be trained on this security. They should understand why it's in place and why they should only connect to your network using secured devices.

3. Updating Poor Or Outdated Passwords If you want to make a hacker's job easier than ever, all you have to do is never change your password. Or use a weak password, like "QWERTY" or "PASSWORD." Even in enterprise, people still use bad passwords that never get changed. Don't let this be you!

A good IT security training program stresses the importance of updating passwords regularly. Even better, it shows employees the best practices in updating the passwords and in choosing secure passwords that will offer an extra layer of protection between your business and the outside world. If you or your employees haven't updated their passwords recently, a good rule of thumb is to consider all current passwords compromised. When hackers attack your network, two of the big things they look for are usernames and passwords. It doesn't matter what they're for – hackers just want this information. Why? Because most people do not change their passwords regularly, and because many people are in the habit of reusing passwords for multiple applications, hackers will try to use these passwords in other places, including bank accounts.

Don't let your employees become your biggest liability. These are just a few examples of how comprehensive IT and network security training can give your employees the knowledge and resources they need to help protect themselves and your business. **Just remember, you do not have to do this by yourself! Good IT training programs are hard to find, and we are here to help.**

"Our organization recently engaged with CE Tech and I have been super impressed with their level of professionalism and knowledge.Their responses have been efficient and on-point.Their support has been crucial to our operation in a time of transition. A shout out to Reed who has been our primary contact thus far and has done a great job!"

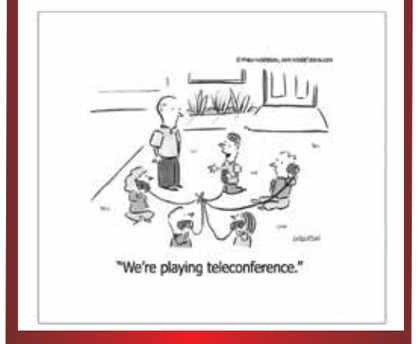
Scott Keyes
New York Farm Bureau

FREE Report: The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks

Eighty-two thousand NEW malware threats are being released every day, and businesses (and their bank accounts) are the #1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious damage to reputation, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyberattack, you MUST read this report and act on the information we're providing.

Claim your FREE copy today at www.cetechno.com/cybercrime

CARTOON of the MONTH



SHINY NEW GADGET OF THE MONTH

Ovo Portable Steam Iron And Garment Steamer

The **Ovo Portable Steam Iron And Garment Steamer** is much smaller than your average iron and yet capable of so much more. It's an iron and a steamer and the perfect companion for when you're traveling and want to look sharp. Or keep the Ovo at home to save space!

The Ovo fits easily in your hand. It's lightweight and won't take up much space in your luggage. Plus, it holds enough water to create up to 10 minutes of steam. You can quickly switch from the metal ironing plate to the brush attachment to add finishing touches to delicate fabrics (and remove any lint or pet hair). It even comes with a heat-resistant travel case. Learn more about this minimarvel at **bit.ly/2CgQzJG!**

Do Smartphone Apps Listen To Your Conversations?

We've all seen this: you scroll down Facebook or Google search results and see an ad for a restaurant or product you were just talking about the other day. How can this be? Was your phone "spying" on you? According to Consumer Reports, not exactly.

Instead, what you're seeing is a personalized ad created by your search habits. Google, Facebook and others collect data as you enter search terms and click on various results or other ads. They know you, and as a result, you are likely to see ads regarding things you just talked about last week. The best way to get around this is to turn off app permission, browse in "incognito mode" or uninstall intrusive apps.

CETech's Client Spotlight:

MASLINE ELECTRONICS INC.

A Family Affair Since 1932

Maslines Electronics is a premiere OEM industrial electronics reseller in the Mid-Atlantic region. "We sell passive electromechanical components, principally board and chassis level, so stuff that goes on a printed circuit board and chassis level parts, such as pilot lights on the front of a panel or an on off switch or a circuit breaker" explains Masline Electronics Co-President, Glenn Masline. "My father started the business in 1932. It was a completely different industry as you can appreciate. I think the primary business in 1932 was lamp repair."

The company continued to grow and offer a broader range of services. Glenn recalls "During the Korean war electronics kind of came of age in the 50s, and if you could buy parts you could sell them. My father would go to Chicago and New York and buy and sell them parts." With the passing of his father in 1964, Glenn's mother took the reins and made the company into what it is today.

Glenn has been involved in every aspect of the business, from dusting and stocking shelves, sales and purchasing to now Co-President, with his sister Sheila Gerling. In addition to working with his sister, Glenn's nephew is the sales manager and his wife works with accounts payable. It's not all family, Masline has over 30 long term employees as well. "Our strength is people-to-people and the relationships we build and maintain." says Glenn. "We've been around for a lot of years and we have a lot of friends in the industry." Being a smaller agile business, Masline can adapt quickly to customers' needs, be it stocking inventory, hold pricing steady or offering just in time order fulfilment. Additionally, Masline offers a wide array of value added services such as kitting, custom assembly work, lead forming and a host of others. This allows their customers to only handle components once and ultimately makes them more efficient, productive and profitable. "We sell on to tier ones obviously, the Carestream, Welch Allen, Siemens, Phillips and a whole bunch of other Dow Jones names, but we also sell to a lot of 20 - 50 person shops as well, where they may not be able to get our level of attention from other suppliers." Masline emphasizes the importance of family and its partnerships with its customers and suppliers. Glenn advises everyone, "Tell us what you want, and we will make adjustments, we are here to work with you."

For more information visit masline.com

CETech has been supporting Masline Electronics for 4 years and really appreciate having them as our customer.